SHA-3 submission – Tweaked version: 2009-09-15

SIMD Is a Message Digest

Principal submitter:

Gaëtan Leurent

École Normale Supérieure
Département d'Informatique
45, rue d'Ulm
75005 Paris
France

`Gaetan.Leurent@ens.fr`
Tel: +33.1.44.32.20.47
Fax: +33.1.44.32.21.51

Auxiliary submitters:

Charles Bouillaguet, Pierre-Alain Fouque

Algorithm inventors/developers:

Gaëtan Leurent, Charles Bouillaguet, Pierre-Alain Fouque

Backup contact:

Pierre-Alain Fouque
École Normale Supérieure
Département d'Informatique
45, rue d'Ulm
75005 Paris
France

`Pierre-Alain.Fouque@ens.fr`
Tel: +33.1.44.32.20.48
Fax: +33.1.44.32.21.51

Last revision: 2009-09-15

About the tweak

This document defines the version 1.1 of SIMD. The following modifications have been made since version 1.0:

- The permutations $p^{(i)}$ have been optimized to provide a better security.
- The rotations $r^{(i)}$ and $s^{(i)}$ have been optimized to provide a better security.
- We introduce a new family of strengthened versions SIMD+ with more rounds than SIMD. These versions can be used if strong security margins are needed.
- We introduce a new family of reduced versions SISD which can be used in constrained environment when only a short tag is needed. These versions can also be useful to develop cryptanalysis techniques.
- The IV and the test vectors have been updated.

The tweak has essentially no effect on the performances of SIMD.

This tweak is motivated by the discovery of a differential distinguisher on the compression function of SIMD-512 1.0 by Nad and Mendel [21]. This distinguishing attack has complexity 2^{427} and is a based on a differential trail where no difference is introduced in the message, but a specific difference Δ_{in} in the chaining value can go to a difference Δ_{out} with probability 2^{-507}. The attack is possible because the diffusion in the compression function is relatively slow and the permutations and rotations of SIMD 1.0 have some bad properties that allow good differential paths.

The tweak prevents the attack in its current form by removing unwanted properties of the permutations and rotations, but it is possible that future improvements give a distinguisher based on similar ideas. However, we decided to not increase the number of rounds of SIMD because we believe that such distinguishers do not threaten the security of SIMD.

The compression function of SIMD was designed with the idea that the message input and the chaining value input of the compression function have a different role. An attacker can easily control the message input, but the chaining value can only be chosen by hashing a previous block. That is why we use a strong message expansion step, and the chaining value undergoes less transformations. Moreover, since SIMD is using a wide-pipe design, attacks on the compression function which require control of the chaining value are very unlikely to be transferable to the full hash function. For instance a free-start preimage attack on the compression compression can not be used to break the hash function, even if it is only has unit cost.

Therefore, we believe that it not worth increase the number of rounds to avoid potential free-start distinguishers, but we provide a strengthened version SIMD+ for those who feel otherwise.

Introduction

The SIMD hash function is quite similar to members of the MD/SHA family. It is based on a familiar Merkle-Damgård design, where the compression function is built from a Feistel-like cipher in Davies-Meyer mode. However there are some innovations in this design: the internal state is twice as big as the output size, we use a strong message expansion, and we use a modified feed-forward in the compression function. The main design criteria was to follow the MD/SHA designs principle which are quite well understood, and to add some elements to avoid all known attacks.

SIMD is particularly efficient on platforms with vector instructions (SIMD) which are available on many processors. Such instructions have been proposed since 1997 and are now widely deployed. Moreover, it is also possible to use two cores on multicore processors to boost the performance with a factor 1.8 by splitting the message expansion function and the hashing process.

Contents

Chapter 1

Algorithm Specification and Rationale

This document defines the SIMD family of hash functions. This family is based on two functions SIMD-256 and SIMD-512; we define SIMD-n with $n \leq 256$ as a truncation of SIMD-256, and SIMD-n with $256 < n \leq 512$ as a truncation of SIMD-512.

Each function SIMD-n takes as input a message of arbitrary size, and outputs a digest of n bits.

1.1 Mathematical Preliminaries and Notations

The design of SIMD uses a number of different operations with useful mathematical properties. In this section, we introduce the operations that will be used through this document, and detail their properties.

1.1.1 The Field $\mathbb{F}_{257}$

Since 257 is a prime, the ring $\mathbb{Z}_{257}$ of the integers modulo 257 is a field $\mathbb{F}_{257}$. The operations in this field are denoted with $\pmod{257}$. We chose this field because we can easily map a byte to an element of the field, and the operations in $\mathbb{F}_{257}$ can be computed efficiently in software and in hardware.

1.1.2 The Number-Theoretic Transform

The Number-theoretic transform of size n in $\mathbb{F}_{257}$ is defined as:

$$\begin{aligned} \mathsf{NTT}_n : \mathbb{F}_{257}^n &\to \mathbb{F}_{257}^n \\ (x_j)_{j=0}^{n-1} &\mapsto (y_i)_{i=0}^{n-1} : \quad y_i = \sum_{j=0}^{n-1} x_j \omega^{ij} \pmod{257}. \end{aligned}$$

where $n \leq 256$, and ω is a n-th root of unity in $\mathbb{F}_{257}$. We can see it as a polynomial evaluation: if the sequence $(x_j)_{j=0}^{n-1}$ is interpreted as a polynomial $P(X) = \sum_{j=0}^{n-1} x_j X^j$, then we have $y_i = P(\omega^i)$.

This transform is identical to the Discrete Fourier Transform but it operates on a finite field instead of the field of complex numbers. It is a bijection of $\mathbb{F}_{257}^n$. It can be computed efficiently by the same algorithm as the Fast Fourier Transform, which has a complexity of $\mathcal{O}(n \log n)$ field operations.

1.1.3 The Rings $\mathbb{Z}_{2^{16}}$ and $\mathbb{Z}_{2^{32}}$

$\mathbb{Z}_{2^{16}}$ denotes the ring of integers modulo 2^{16}, and $\mathbb{Z}_{2^{32}}$ denotes the ring of the integers modulo 2^{32}. We use $\boxplus$ and $\boxtimes$ to represent the modular addition and multiplication in these rings. (Actually, we only use $\boxplus$ in $\mathbb{Z}_{2^{32}}$ and $\boxtimes$ in $\mathbb{Z}_{2^{16}}$).

We can represent elements of $\mathbb{Z}_{2^{16}}$ by 16-bit words, and elements of $\mathbb{Z}_{2^{32}}$ by 32-bit words. Thus, we define the following bitwise boolean functions on 32-bit words:

$$\begin{aligned}\mathsf{IF}(A,B,C) &= (A \wedge B) \ \vee (\neg A \wedge C)\\ \mathsf{MAJ}(A,B,C) &= (A \wedge B) \ \vee (A \wedge C) \vee (B \wedge C)\end{aligned}$$

where $\vee$ denotes the boolean OR, $\wedge$ denotes AND, and $\neg$ denotes NOT. We also use $\oplus$ for the exclusive or (XOR). IF acts as a conditional, and MAJ is the majority function. These function are already used in some hash functions because they have good properties: the output is unbiased, and no input bit has a linear effect on the output.

We also use bitwise rotations on 32-bit words: x rotated to the left by s bits is denoted by $x^{\lll s}$.

1.1.4 Superscripts and Subscripts

Since the compression function consists of the repetition of a simple round function, we use $X^{(i)}$ to denote the variable X associated with round i. Meanwhile, many variable can be seen as vectors, and we use $X_{[0..k]}$ to denote the vector $[X_0, X_1, ...X_k]$ (or its transpose, depending on the context).

1.2 Description of the Algorithm

SIMD is an iterative hash function that follows the Merkle-Damgård design. The main component of a Merkle-Damgård hash function h is a compression function $C : \{0,1\}^p \times \{0,1\}^m \to \{0,1\}^p$. To compute $h(M)$, the message M is first divided into k chunks M_i's of m bits. Then the compression function is used to compress the message chunks and the internal state: $H_{i+1} = C(H_i, M_i)$. There is a padding rule to fill the last m-bit blocks, and the padding usually includes the message size (this is known as the Merkle-Damgård strengthening). The initial value of the internal state H_{i-1} is called IV and is fixed in the description of the hash function. The output of the hash function is given by computing a finalization function $D : \{0,1\}^p \to \{0,1\}^n$ on the last internal state H_{k-1}.

The Davies-Meyer mode is a common way to build a compression function C from a block cipher E: it is defined as $C(h,m) = E_m(h) \oplus h$. Many hash functions use a custom block cipher, designed with a message expansion step, and a Feistel ladder.

The SIMD family uses a similar design, and the size parameters are as follows:

	Output size n	Message block size m	Internal state size p
SIMD-256	256	512	512
SIMD-512	512	1024	1024

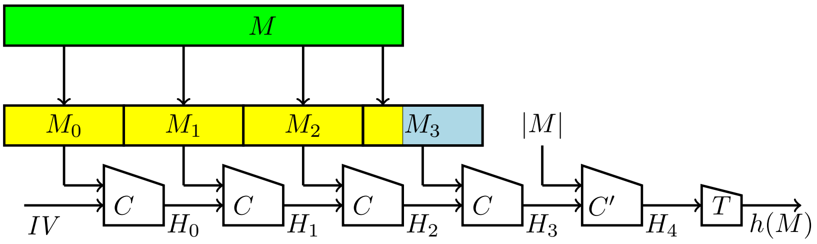

Figure 1.1: The iteration used in SIMD

The inner state is represented as a matrix of 32-bit words. For SIMD-256, it is a 4×4 matrix, while SIMD-512 has a 8×4 inner state:

$$\mathcal{S}_{256} = \begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \end{bmatrix} \qquad \mathcal{S}_{512} = \begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \\ A_4 & B_4 & C_4 & D_4 \\ A_5 & B_5 & C_5 & D_5 \\ A_6 & B_6 & C_6 & D_6 \\ A_7 & B_7 & C_7 & D_7 \end{bmatrix}$$

In this section, we will describe more precisely the operating mode of SIMD, and the inside of the compression function: the message expansion and the Feistel ladder.

1.2.1 Mode of Operation

Iteration

Our mode of operation is similar to the wide-pipe construction of Lucks [18] and to Chop-MD [6]. The internal state is twice as large as the output, and we use a truncation T to compute the hash value from the last internal state. The padding rule is quite simple: the last message block is filled with zeros if it is smaller than m bits, and an extra block containing the size of the message in bits is added. This extra block is compressed with a slightly modified compression function C', and the output is truncated. This is described by Figure 1.1.

The size of the message input to SIMD is not limited, and the number of bits of the message included in the last block is taken modulo 2^m. We believe that it is not necessary to limit the message size in the description of the algorithm, but for all practical purpose it can be considered to be below 2^{64}. Therefore, the message input in the last message block is quite constrained. The last compression function C' acts as kind of blank round, and makes it harder to use the truncation to find a collision.

Modified Davies-Meyer

To build our compression from a Feistel-like block cipher, we will use a technique similar to the well known Davies-Meyer construction, but with a few variations.

First, we have a message block size that is equal to the internal state size, so we can use $C(h, m) = E_m(h \oplus m) \oplus h$ instead of $C(h, m) = E_m(h) \oplus h$. This is construction 8 from [4] (and construction 41 from [24]). It enjoys the same provable security guarantees than the original

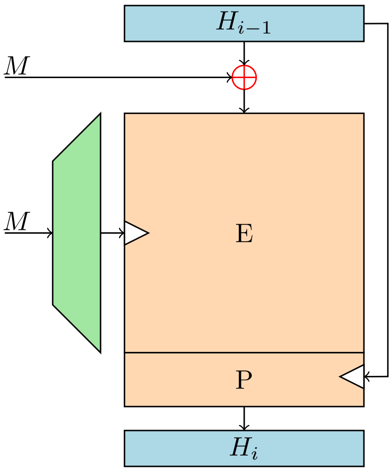

Figure 1.2: Modified Davies-Meyer

Davies-Meyer construction. Note that this is natural, because the former can be seen as a special case of the later, with a block cipher E' defined as $E'_k(x) = E_k(x \oplus k)$. The fact that $h \oplus m$ goes into the block cipher means that the adversary has to "commit" to a given value of m before starting to evaluate $E_m(h \oplus m)$. This prevents, for example, to construct the message m "on the fly", and complicates message modification techniques.

Second, instead of using a simple XOR to combine $E_m(h \oplus m)$ and h, we will use a few extra Feistel rounds, with h entering as the key. This makes a function $P : \{0,1\}^p \times \{0,1\}^p \to \{0,1\}^p$, and the compression function is defined as $P(h, E_m(h \oplus m))$. The security proofs of the Davies-Meyer mode can easily be adapted to the modified Davies-Meyer because P is a quasigroup operation:

- for all y, $x \mapsto P(x,y)$ is a permutation;
- for all x, $y \mapsto P(x,y)$ is a permutation;
- for all z, $x \mapsto y$ s.t. $P(x,y) = z$ is a permutation;
- for all z, $y \mapsto x$ s.t. $P(x,y) = z$ is a permutation.

Moreover, this modified mode prevents some kind of multi-block attacks, and does not allow to find trivial fixed points used in some second preimage attacks [17]. Our modified Davies-Meyer mode is described in Figure 1.2.

1.2.2 The Message Expansion

The message expansion is a very important part of our design. It seems that all the attacks against hash functions of the MD/SHA family use the fact that in order to modify a small part of the expanded message, one can modify the original message block without too much effect on other parts of the full expanded message. Therefore, we choose to view the message expansion as an error correcting code, and we try to build a code with a high minimal distance. This is similar to the approach of [16], but our message expansion is very different from the MD/SHA one.

The message expansion is composed of three layers, which can each be considered as a code in some vector space. For SIMD-256 (resp. SIMD-512), it expands a 512-bit (resp. 1024-bit) message block into a 4096-bit (resp. 8192) expanded message, with a minimal distance of 520 (resp. 1032).

	Message block	Expanded message	Minimal distance
SIMD-256	512 bits	4096 bits	520 bits
SIMD-512	1024 bits	8192 bits	1032 bits

First Layer: Number-Theoretic Transform

The first layer of the message expansion is computationally expensive, but it a very important part of our design. The basic idea is to consider the message as a polynomial P of degree 63 (resp. 127) in $\mathbb{F}_{257}[X]$, and to evaluate this polynomial over 128 (resp. 256) points of the field $\mathbb{F}_{257}$ using a Number-Theoretic Transform[1]. This is essentially a truncated Reed-Solomon code, and it has an optimal minimal distance: two different polynomials will match on at most 63 (resp. 127) points. It reaches the Singleton bound, and therefore is a linear MDS code.

However, this code has some unwanted properties, that would allow to build very specific expanded messages:

- The Reed-Solomon code is cyclic: for any polynomial P, if $(y_i) = \mathsf{NTT}(P(X))$ and $(z_i) = \mathsf{NTT}(P(\omega X))$ with ω a n-th root of the unity, then $z_i = y_{i+1 \pmod n}$.
- The NTT of a constant polynomial k is uniform ($\forall i,\ y_i = k$). In particular, $\mathsf{NTT}(0) = 0$.

To avoid those properties, we will actually compute the NTT of the polynomial $P + X^{127}$ (resp. $P + X^{255}$). This is equivalent to adding some constants (actually the NTT of X^{127} or X^{255}) to the NTT of P. This makes the code affine, instead of just linear.

More precisely, the first message expansion step of SIMD-256 is defined as:

$$\begin{aligned} O : (\mathbb{Z}_{2^8})^{64} &\to (\mathbb{F}_{257})^{128} \\ (x_j)_{j=0}^{63} &\mapsto (y_i)_{i=0}^{127} : \quad y_i = \sum_{j=0}^{63} x_j \alpha^{ij} + \alpha^{127i} \pmod{257}. \end{aligned}$$

where $\alpha = 139$ is a 128th root of unity in $\mathbb{F}_{257}$.

For SIMD-512, the first message expansion step is defined as:

$$\begin{aligned} O : (\mathbb{Z}_{2^8})^{128} &\to (\mathbb{F}_{257})^{256} \\ (x_j)_{j=0}^{127} &\mapsto (y_i)_{i=0}^{255} : \quad y_i = \sum_{j=0}^{127} x_j \beta^{ij} + \beta^{255i} \pmod{257}. \end{aligned}$$

where $\beta = 41$ is a 256th root of unity in $\mathbb{F}_{257}$, and a square root of α.

---

[1] The NTT is a bijection, but we use it with half of the input set to zero, which makes it an injection.

This affine code has the same *differential* properties than the Reed-Solomon code: two different messages will match on at most 63 (resp. 127) y_i's. Moreover, we still have a good number of non-zero *values*. Let us consider SIMD-256, and an i such that $y_i = 0$. Then we have

$$\begin{aligned} y_i = 0 &= P(\alpha^i) + \alpha^{127i} \\ 0 &= \alpha^i P(\alpha^i) + 1. \end{aligned}$$

α^i is a root of $X.P + 1$, which is a polynomial of degree 64. Thus there are at least 64 non-zero y_i's in SIMD-256. Similarly, we can show there are at least 128 non-zero y_i's in SIMD-512

To map the x_j's from $\mathbb{Z}_{2^8}$ to $\mathbb{F}_{257}$, we take them as integers between 0 and 255.

Second Layer: Concatenated Code

In order to output a sequence of bytes (rather than elements of $\mathbb{F}_{257}$) and to increase the minimal distance of our message expansion, each symbol of $O(M)$ will be encoded through an inner code $I : \mathbb{F}_{257} \to \mathbb{Z}_{2^{16}}$. We use a class of very efficient codes, implemented with only a single multiplication modulo 2^{16}: $I_C : x \mapsto C \boxtimes x$ for some constant C. We ran an exhaustive search over the constant C, and we found four values that give a minimal Hamming distance of 4 bits: $C = 185$, $C = 233$, and their opposites. Thus, we will use the two following inner codes:

$$\begin{aligned} I_{185} : \mathbb{F}_{257} &\to \mathbb{Z}_{2^{16}} \\ x &\mapsto 185 \boxtimes \widetilde{x} \qquad \text{where } -128 \le \widetilde{x} \le 128 \text{ and } \widetilde{x} = x \pmod{257} \\ I_{233} : \mathbb{F}_{257} &\to \mathbb{Z}_{2^{16}} \\ x &\mapsto 233 \boxtimes \widetilde{x} \qquad \text{where } -128 \le \widetilde{x} \le 128 \text{ and } \widetilde{x} = x \pmod{257} \end{aligned}$$

x is lifted to the integers with $-128 \le \widetilde{x} \le 128$ because lifting to $\{-128, ...128\}$ is easier than to $\{0, ...257\}$. We will use both $I_{185}(O(M))$ and $I_{233}(O(M))$ in the expanded message (*i.e.*, we will have two copies of $O(M)$ encoded through two different inner codes).

Theses codes also have a minimal distance of 4 when we measure the weigh of the Non Adjacent Form (NAF) of the modular difference. The NAF is an optimal signed binary representation, so this means that from modular difference point of view, the code also has a distance of 4. We cannot express the 4 Hamming difference with less than 4 modular differences.

Third Layer : Permutation

The expanded message will be used as a sequence of 32-bit words, so we have to pack two 16-bit words together. The 32-bit word with $I_C(x)$ in his lower 16 bits and $I_C(y)$ in its higher 16 bits is denoted by $I_C(x, y)$. If $I_C(x)$ and $I_C(y)$ are seen as integers between 0 and $2^{16} - 1$, we have $I_C(x, y) = I_C(x) + 2^{16} I_C(y)$.

To make the message expansion stronger we permute the message words so that if an attacker wants to cancel some expanded message words, he will have to choose them quite far away. We first define an intermediate 32×4 (resp. 32×8) matrix of 32-bit words. For SIMD-256, we have (with $0 \le j \le 3$):

$$Z_j^{(i)} = \begin{cases} I_{185}\big(y[8i + 2j], & y[8i + 2j + 1]\big) & \text{when } 0 \le i \le 15 \\ I_{233}\big(y[8i + 2j - 128], & y[8i + 2j - 64]\big) & \text{when } 16 \le i \le 23 \\ I_{233}\big(y[8i + 2j - 191], & y[8i + 2j - 127]\big) & \text{when } 24 \le i \le 31 \end{cases}$$

For SIMD-512, we have (with $0 \le j \le 7$):

$$Z_j^{(i)} = \begin{cases} I_{185}\big(y[16i + 2j], & y[16i + 2j + 1]\big) & \text{when } 0 \le i \le 15 \\ I_{233}\big(y[16i + 2j - 256], & y[16i + 2j - 128]\big) & \text{when } 16 \le i \le 23 \\ I_{233}\big(y[16i + 2j - 383], & y[16i + 2j - 255]\big) & \text{when } 24 \le i \le 31 \end{cases}$$

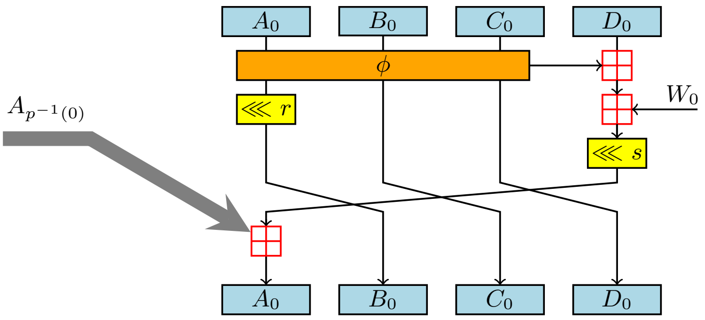

Figure 1.3: Step update of a single Feistel

Lastly, we permute the lines of the matrix Z. Let $W_j^{(i)} = Z_j^{(P(i))}$ with the following permutation:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	4	6	0	2	7	5	3	1	15	11	12	8	9	13	10	14

i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	17	18	23	20	22	21	16	19	30	24	25	31	27	29	28	26

The full message expansion for SIMD-256 is given in Table 1.1.

1.2.3 The Feistel Ladder

The compression function is based on a Feistel structure, with a step function similar to the step functions of the MD/SHA family:

$$\begin{aligned} A_j^{(i)} &= \left(D_j^{(i-1)} \boxplus W_j^{(i)} \boxplus \phi^{(i)}(A_j^{(i-1)}, B_j^{(i-1)}, C_j^{(i-1)})\right)^{\lll s^{(i)}} \boxplus A_{p^{(i)}(j)}^{(i-1)\ \lll r^{(i)}} \\ B_j^{(i)} &= A_j^{(i-1)\lll r^{(i)}} \\ C_j^{(i)} &= B_j^{(i-1)} \\ D_j^{(i)} &= C_j^{(i-1)} \end{aligned}$$

where $\phi^{(i)}$ is a boolean function, $\boxplus$ is the addition modulo 2^{32} and $\lll s^{(i)}$ denotes rotation to the left by an amount of $s^{(i)}$ bits. This step function is shown in Figure 1.4. Note that all the values used to compute the new $A_j^{(i+1)}$'s go through a rotation. That should prevent differential trails active only on the most-significant bit, as was found in MD5 [9].

Alternatively, we can write an equivalent description of the step update involving only the A_j registers:

$$\begin{aligned} B_j^{(i)} &= A_j^{(i-1)\lll r_{i-1}} \\ C_j^{(i)} &= A_j^{(i-2)\lll r_{i-2}} \\ D_j^{(i)} &= A_j^{(i-3)\lll r_{i-3}} \\ A_j^{(i)} &= \left(A_j^{(i-4)\lll r_{i-4}} \boxplus W_j^{(i)} \boxplus \phi^{(i)}(A_j^{(i-1)}, A_j^{(i-2)\lll r_{i-2}}, A_j^{(i-3)\lll r_{i-3}})\right)^{\lll s^{(i)}} \boxplus A_{p^{(i)}(j)}^{(i-1)\ \lll r^{(i)}} \end{aligned}$$

i	$W_0^{(i)}$	$W_1^{(i)}$	$W_2^{(i)}$	$W_3^{(i)}$
0	$I_{185}(y_{32}, y_{33})$	$I_{185}(y_{34}, y_{35})$	$I_{185}(y_{36}, y_{37})$	$I_{185}(y_{38}, y_{39})$
1	$I_{185}(y_{48}, y_{49})$	$I_{185}(y_{50}, y_{51})$	$I_{185}(y_{52}, y_{53})$	$I_{185}(y_{54}, y_{55})$
2	$I_{185}(y_{0}, y_{1})$	$I_{185}(y_{2}, y_{3})$	$I_{185}(y_{4}, y_{5})$	$I_{185}(y_{6}, y_{7})$
3	$I_{185}(y_{16}, y_{17})$	$I_{185}(y_{18}, y_{19})$	$I_{185}(y_{20}, y_{21})$	$I_{185}(y_{22}, y_{23})$
4	$I_{185}(y_{56}, y_{57})$	$I_{185}(y_{58}, y_{59})$	$I_{185}(y_{60}, y_{61})$	$I_{185}(y_{62}, y_{63})$
5	$I_{185}(y_{40}, y_{41})$	$I_{185}(y_{42}, y_{43})$	$I_{185}(y_{44}, y_{45})$	$I_{185}(y_{46}, y_{47})$
6	$I_{185}(y_{24}, y_{25})$	$I_{185}(y_{26}, y_{27})$	$I_{185}(y_{28}, y_{29})$	$I_{185}(y_{30}, y_{31})$
7	$I_{185}(y_{8}, y_{9})$	$I_{185}(y_{10}, y_{11})$	$I_{185}(y_{12}, y_{13})$	$I_{185}(y_{14}, y_{15})$
8	$I_{185}(y_{120}, y_{121})$	$I_{185}(y_{122}, y_{123})$	$I_{185}(y_{124}, y_{125})$	$I_{185}(y_{126}, y_{127})$
9	$I_{185}(y_{88}, y_{89})$	$I_{185}(y_{90}, y_{91})$	$I_{185}(y_{92}, y_{93})$	$I_{185}(y_{94}, y_{95})$
10	$I_{185}(y_{96}, y_{97})$	$I_{185}(y_{98}, y_{99})$	$I_{185}(y_{100}, y_{101})$	$I_{185}(y_{102}, y_{103})$
11	$I_{185}(y_{64}, y_{65})$	$I_{185}(y_{66}, y_{67})$	$I_{185}(y_{68}, y_{69})$	$I_{185}(y_{70}, y_{71})$
12	$I_{185}(y_{72}, y_{73})$	$I_{185}(y_{74}, y_{75})$	$I_{185}(y_{76}, y_{77})$	$I_{185}(y_{78}, y_{79})$
13	$I_{185}(y_{104}, y_{105})$	$I_{185}(y_{106}, y_{107})$	$I_{185}(y_{108}, y_{109})$	$I_{185}(y_{110}, y_{111})$
14	$I_{185}(y_{80}, y_{81})$	$I_{185}(y_{82}, y_{83})$	$I_{185}(y_{84}, y_{85})$	$I_{185}(y_{86}, y_{87})$
15	$I_{185}(y_{112}, y_{113})$	$I_{185}(y_{114}, y_{115})$	$I_{185}(y_{116}, y_{117})$	$I_{185}(y_{118}, y_{119})$
16	$I_{233}(y_{8}, y_{72})$	$I_{233}(y_{10}, y_{74})$	$I_{233}(y_{12}, y_{76})$	$I_{233}(y_{14}, y_{78})$
17	$I_{233}(y_{16}, y_{80})$	$I_{233}(y_{18}, y_{82})$	$I_{233}(y_{20}, y_{84})$	$I_{233}(y_{22}, y_{86})$
18	$I_{233}(y_{56}, y_{120})$	$I_{233}(y_{58}, y_{122})$	$I_{233}(y_{60}, y_{124})$	$I_{233}(y_{62}, y_{126})$
19	$I_{233}(y_{32}, y_{96})$	$I_{233}(y_{34}, y_{98})$	$I_{233}(y_{36}, y_{100})$	$I_{233}(y_{38}, y_{102})$
20	$I_{233}(y_{48}, y_{112})$	$I_{233}(y_{50}, y_{114})$	$I_{233}(y_{52}, y_{116})$	$I_{233}(y_{54}, y_{118})$
21	$I_{233}(y_{40}, y_{104})$	$I_{233}(y_{42}, y_{106})$	$I_{233}(y_{44}, y_{108})$	$I_{233}(y_{46}, y_{110})$
22	$I_{233}(y_{0}, y_{64})$	$I_{233}(y_{2}, y_{66})$	$I_{233}(y_{4}, y_{68})$	$I_{233}(y_{6}, y_{70})$
23	$I_{233}(y_{24}, y_{88})$	$I_{233}(y_{26}, y_{90})$	$I_{233}(y_{28}, y_{92})$	$I_{233}(y_{30}, y_{94})$
24	$I_{233}(y_{49}, y_{113})$	$I_{233}(y_{51}, y_{115})$	$I_{233}(y_{53}, y_{117})$	$I_{233}(y_{55}, y_{119})$
25	$I_{233}(y_{1}, y_{65})$	$I_{233}(y_{3}, y_{67})$	$I_{233}(y_{5}, y_{69})$	$I_{233}(y_{7}, y_{71})$
26	$I_{233}(y_{9}, y_{73})$	$I_{233}(y_{11}, y_{75})$	$I_{233}(y_{13}, y_{77})$	$I_{233}(y_{15}, y_{79})$
27	$I_{233}(y_{57}, y_{121})$	$I_{233}(y_{59}, y_{123})$	$I_{233}(y_{61}, y_{125})$	$I_{233}(y_{63}, y_{127})$
28	$I_{233}(y_{25}, y_{89})$	$I_{233}(y_{27}, y_{91})$	$I_{233}(y_{29}, y_{93})$	$I_{233}(y_{31}, y_{95})$
29	$I_{233}(y_{41}, y_{105})$	$I_{233}(y_{43}, y_{107})$	$I_{233}(y_{45}, y_{109})$	$I_{233}(y_{47}, y_{111})$
30	$I_{233}(y_{33}, y_{97})$	$I_{233}(y_{35}, y_{99})$	$I_{233}(y_{37}, y_{101})$	$I_{233}(y_{39}, y_{103})$
31	$I_{233}(y_{17}, y_{81})$	$I_{233}(y_{19}, y_{83})$	$I_{233}(y_{21}, y_{85})$	$I_{233}(y_{23}, y_{87})$

Table 1.1: Full Message Expansion for SIMD-256

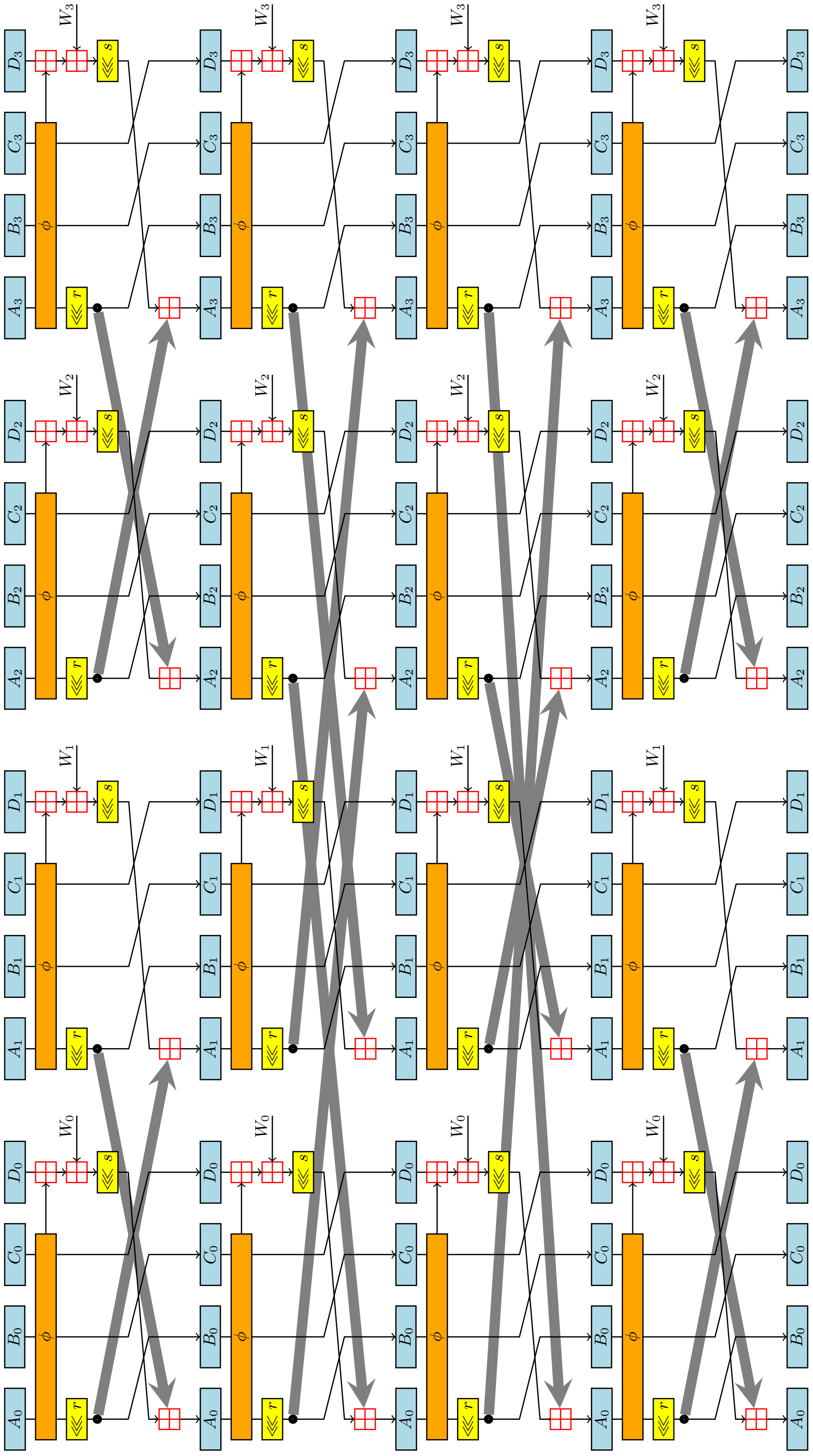

Figure 1.4: A few step updates of SIMD-256

We basically have 4 parallel Feistel ladders for SIMD-256 (resp. 8 for SIMD-512), and they interact together because of the permutations $p^{(i)}$'s. At each round, a new value is computed in each Feistel ladder, and this new value is sent to another Feistel ladder at the following round. The $p^{(i)}$'s are chosen to ensure a good diffusion. For SIMD-256, we define the following permutations:

$$p^{(0)}(j) = j \oplus 1$$
$$p^{(1)}(j) = j \oplus 2$$
$$p^{(2)}(j) = j \oplus 3$$

j	0	1	2	3
$p^{(0)}(j)$	1	0	3	2
$p^{(1)}(j)$	2	3	0	1
$p^{(2)}(j)$	3	2	1	0

The permutation used at step i is $p^{(i \bmod 3)}$. If a difference is introduced in one Feistel at round i, it will have propagated to all the Feistels at round $i+2$.

For SIMD-512, we define seven permutations:

$$p^{(0)}(j) = j \oplus 1$$
$$p^{(1)}(j) = j \oplus 6$$
$$p^{(2)}(j) = j \oplus 2$$
$$p^{(3)}(j) = j \oplus 3$$
$$p^{(4)}(j) = j \oplus 5$$
$$p^{(5)}(j) = j \oplus 7$$
$$p^{(6)}(j) = j \oplus 4$$

j	0	1	2	3	4	5	6	7
$p^{(0)}(j)$	1	0	3	2	5	4	7	6
$p^{(1)}(j)$	6	7	4	5	2	3	0	1
$p^{(2)}(j)$	2	3	0	1	6	7	4	5
$p^{(3)}(j)$	3	2	1	0	7	6	5	4
$p^{(4)}(j)$	5	4	7	6	1	0	3	2
$p^{(5)}(j)$	7	6	5	4	3	2	1	0
$p^{(6)}(j)$	4	5	6	7	0	1	2	3

The permutation used at step i is $p^{(i \bmod 7)}$. If a difference is introduced in one Feistel at round i, it will have propagated to all the Feistels at round $i+3$. The Figure 1.4 shows the repetition of a few round functions, with the permutations of SIMD-256.

More precisely, the step update function of SIMD-256 is:

$$\begin{aligned}\mathsf{Step}\left(\begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \end{bmatrix}, \begin{bmatrix} W_0 \\ W_1 \\ W_2 \\ W_3 \end{bmatrix}, \phi, r, s, p\right) \\ = \begin{bmatrix} (D_0 \boxplus W_0 \boxplus \phi(A_0, B_0, C_0))^{\lll s} \boxplus A_{p(0)}^{\lll r} & A_0^{\lll r} & B_0 & C_0 \\ (D_1 \boxplus W_1 \boxplus \phi(A_1, B_1, C_1))^{\lll s} \boxplus A_{p(1)}^{\lll r} & A_1^{\lll r} & B_1 & C_1 \\ (D_2 \boxplus W_2 \boxplus \phi(A_2, B_2, C_2))^{\lll s} \boxplus A_{p(2)}^{\lll r} & A_2^{\lll r} & B_2 & C_2 \\ (D_3 \boxplus W_3 \boxplus \phi(A_3, B_3, C_3))^{\lll s} \boxplus A_{p(3)}^{\lll r} & A_3^{\lll r} & B_3 & C_3 \end{bmatrix}\end{aligned} \tag{1.1}$$

and the step update function of SIMD-512 is:

$$\mathsf{Step}\left(\begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \\ A_4 & B_4 & C_4 & D_4 \\ A_5 & B_5 & C_5 & D_5 \\ A_6 & B_6 & C_6 & D_6 \\ A_7 & B_7 & C_7 & D_7 \end{bmatrix}, \begin{bmatrix} W_0 \\ W_1 \\ W_2 \\ W_3 \\ W_4 \\ W_5 \\ W_6 \\ W_7 \end{bmatrix}, \phi, r, s, p\right) \tag{1.2}$$

$$= \begin{bmatrix} (D_0 \boxplus W_0 \boxplus \phi(A_0, B_0, C_0))^{\lll s} \boxplus A_{p(0)}^{\lll r} & A_0^{\lll r} & B_0 & C_0 \\ (D_1 \boxplus W_1 \boxplus \phi(A_1, B_1, C_1))^{\lll s} \boxplus A_{p(1)}^{\lll r} & A_1^{\lll r} & B_1 & C_1 \\ (D_2 \boxplus W_2 \boxplus \phi(A_2, B_2, C_2))^{\lll s} \boxplus A_{p(2)}^{\lll r} & A_2^{\lll r} & B_2 & C_2 \\ (D_3 \boxplus W_3 \boxplus \phi(A_3, B_3, C_3))^{\lll s} \boxplus A_{p(3)}^{\lll r} & A_3^{\lll r} & B_3 & C_3 \\ (D_4 \boxplus W_4 \boxplus \phi(A_4, B_4, C_4))^{\lll s} \boxplus A_{p(4)}^{\lll r} & A_4^{\lll r} & B_4 & C_4 \\ (D_5 \boxplus W_5 \boxplus \phi(A_5, B_5, C_5))^{\lll s} \boxplus A_{p(5)}^{\lll r} & A_5^{\lll r} & B_5 & C_5 \\ (D_6 \boxplus W_6 \boxplus \phi(A_6, B_6, C_6))^{\lll s} \boxplus A_{p(6)}^{\lll r} & A_6^{\lll r} & B_6 & C_6 \\ (D_7 \boxplus W_7 \boxplus \phi(A_7, B_7, C_7))^{\lll s} \boxplus A_{p(7)}^{\lll r} & A_7^{\lll r} & B_7 & C_7 \end{bmatrix}$$

A block of eight steps, is called a round, and it is parametrized by a set of rotation constants $\pi_{[0..3]}$. The boolean functions and the rotation constants are used as follows:

$\phi^{(i)}$	$r^{(i)}$	$s^{(i)}$
IF	π_0	π_1
IF	π_1	π_2
IF	π_2	π_3
IF	π_3	π_0
MAJ	π_0	π_1
MAJ	π_1	π_2
MAJ	π_2	π_3
MAJ	π_3	π_0

Round	π_0	π_1	π_2	π_3
0	3	23	17	27
1	28	19	22	7
2	29	9	15	5
3	4	13	10	25

The whole compression function is made of 4 rounds, plus four final steps to mix the initial chaining value to the initial state (this is our feed-forward). A graphical representation of the compression function is given in Figure 1.5, and Algorithm 1 gives a pseudo-code description of the full SIMD hash function, with the chosen of constants and boolean functions.

1.2.4 The Final Compression Function

After all the message blocks have been compressed, there is an extra call to the compression function, with the message length as input. The message length is counted in bits, modulo 2^m if needed. It is written as a sequence of bytes using the little endian convention, *i.e.* the low order byte of the counter will be the first message byte.

For this final compression function, we use a slightly different message expansion, with a tweaked outer code. In SIMD-256, instead of using $O(M) = \mathsf{NTT}_{128}(M + X^{127})$, we use $O'(M) = \mathsf{NTT}_{128}(M + X^{127} + X^{125})$. In SIMD-512, instead of using $O(M) = \mathsf{NTT}_{256}(M + X^{255})$, we use $O'(M) = \mathsf{NTT}_{256}(M + X^{255} + X^{253})$. The range of this modified message expansion is

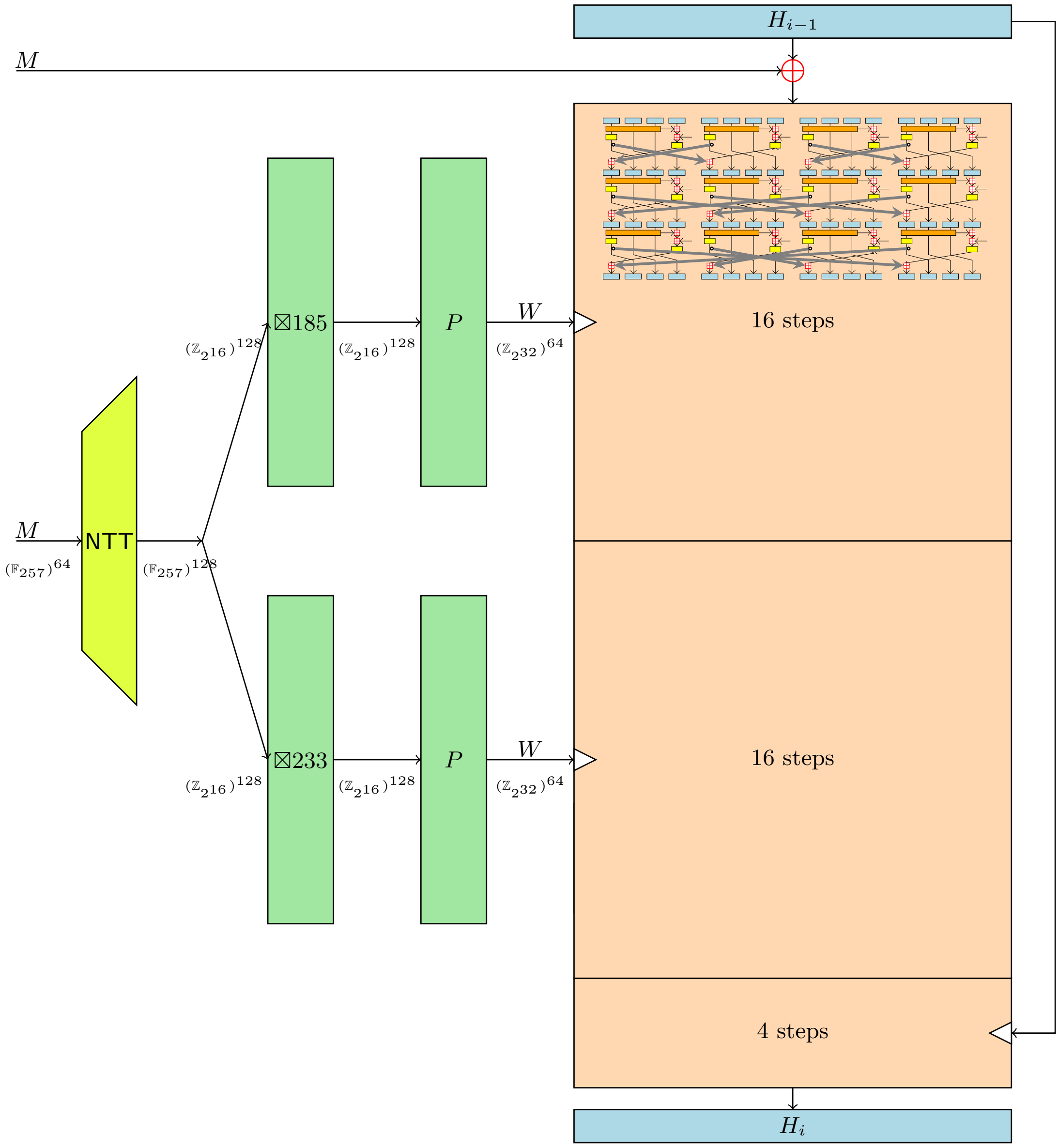
H_{i-1}
M
16 steps
W
$(\mathbb{Z}_{2^{32}})^{64}$
P
$(\mathbb{Z}_{2^{16}})^{128}$
⊠185
$(\mathbb{Z}_{2^{16}})^{128}$
M
NTT
$(\mathbb{F}_{257})^{64}$
$(\mathbb{F}_{257})^{128}$
16 steps
⊠233
$(\mathbb{Z}_{2^{16}})^{128}$
P
$(\mathbb{Z}_{2^{16}})^{128}$
W
$(\mathbb{Z}_{2^{32}})^{64}$
4 steps
H_i

Figure 1.5: Compression function of SIMD-256

distinct from the range of the main message expansion. Alternatively, we can consider that the compression function takes an extra input bit, and that the message is encoded in a prefix-free way by setting the extra bit only in the final block.

After that step, the output is defined as follows:

- For SIMD-256, output the bit-string representation of:
  A_0, A_1, A_2, A_3, B_0, B_1, B_2, B_3.
- For SIMD-n with $n \leq 256$, output the n-bit prefix of the SIMD-256 output. For instance, SIMD-224's output is the bit-string representation of:
  A_0, A_1, A_2, A_3, B_0, B_1, B_2.
- For SIMD-512, output the bit-string representation of:
  A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7, B_0, B_1, B_2, B_3, B_4, B_5, B_6, B_7.
- For SIMD-n with $256 < n \leq 512$, output the n-bit prefix of the SIMD-512 output. For instance, SIMD-384's output is the bit-string representation of:
  A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7, B_0, B_1, B_2, B_3.

1.2.5 Initialization Vector

Each SIMD-n function will use a distinct Initialization Vector, so as to avoid relations between the outputs of different members of the family. The IV of SIMD-n is defined as

$$IV\text{-}n = \textsf{SIMD-Compress}(0, \texttt{"SIMD-}\langle n\rangle\texttt{ v1.1"})$$

where:

- the chaining value has all its bits set to zero;
- the string `"SIMD-`$\langle n\rangle$` v1.1"` is written in ASCII and padded with zeros;
- $\langle n\rangle$ is the decimal representation of n in ASCII without any extra zero;
- there is a single space between the last digit of $\langle n\rangle$ and the `"v"`.

The IV of SIMD-224, SIMD-256, SIMD-384 and SIMD-512 are given in Table 1.2.

1.2.6 Input and Output

To defines the set of functions SIMD-$n : \{0,1\}^* \rightarrow \{0,1\}^n$, we still have to define how to map a bit-string to the input of SIMD, and how to map the output of SIMD to a bit-string. We will use a little-endian mapping, following the convention of MD4.

Input mapping

The input sequence of bits is interpreted in a natural manner as a sequence of bytes, where each consecutive group of eight bits is interpreted as a byte with the high-order (most significant) bit of each byte listed first.

Each byte represents an integer between 0 and 255, and we use the canonical mapping from $\mathbb{Z}$ to $\mathbb{Z}_{257} = \mathbb{F}_{257}$ to construct the inputs of the NTT step of the message expansion. Note that the NTT will never receive the input value 256.

Algorithm 1 Pseudo-code description of SIMD.

```
function MessageExpansion($M$, $f$)    ▷ $f$ marks the final compression function
    if $f = 0$ then
        $(y_i) \leftarrow \mathsf{NTT}_{128}(M + X^{127})$    ▷ resp. $X^{255}$ for SIMD-512
    else
        $(y_i) \leftarrow \mathsf{NTT}_{128}(M + X^{127} + X^{125})$    ▷ resp. $X^{255} + X^{253}$ for SIMD-512
    end if
    Compute the $Z_j^{(i)}$'s by applying the inner codes $I_{185}$ and $I_{233}$ to the $y_i$'s.
    Compute the $W_j^{(i)}$'s by permuting the $Z_i^{(j)}$'s.
    return the $W_j^{(i)}$'s.
end function

function Round($\mathcal{S}$, $i$, $\pi_{[0..3]}$)
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+0)}, \mathsf{IF}, \pi_0, \pi_1)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+1)}, \mathsf{IF}, \pi_1, \pi_2)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+2)}, \mathsf{IF}, \pi_2, \pi_3)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+3)}, \mathsf{IF}, \pi_3, \pi_0)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+4)}, \mathsf{MAJ}, \pi_0, \pi_1)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+5)}, \mathsf{MAJ}, \pi_1, \pi_2)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+6)}, \mathsf{MAJ}, \pi_2, \pi_3)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{[0..3]}^{(8i+7)}, \mathsf{MAJ}, \pi_3, \pi_0)$
    return $\mathcal{S}$
end function

function SIMD-Compress($IV$, $M$, $f$)
    $W \leftarrow \mathsf{MessageExpansion}(M, f)$
    $\mathcal{S} \leftarrow IV \oplus M$
    $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 0, [\ 3, 23, 17, 27])$
    $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 1, [28, 19, 22,\ 7])$
    $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 2, [29,\ 9, 15,\ 5])$
    $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 3, [\ 4, 13, 10, 25])$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, IV_{[0..3]}^{(0)}, \mathsf{IF},\ 4, 13)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, IV_{[0..3]}^{(1)}, \mathsf{IF}, 13, 10)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, IV_{[0..3]}^{(2)}, \mathsf{IF}, 10, 25)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, IV_{[0..3]}^{(3)}, \mathsf{IF}, 24,\ 4)$
    return $\mathcal{S}$
end function

function SIMD($M$)
    Split the message $M$ into chunks $M_i, 0 \leq i < k$.
    $M_{k-1}$ is padded with zeros.
    $\mathcal{S} \leftarrow IV$
    for $0 \leq i < k$ do
        $\mathcal{S} \leftarrow \mathsf{SIMD\text{-}Compress}(\mathcal{S}, M_i, 0)$
    end for
    $\mathcal{S} \leftarrow \mathsf{SIMD\text{-}Compress}(\mathcal{S}, |M|, 1)$
    return Truncate($\mathcal{S}$)
end function
```

SIMD-224 IV				
$A_{0..3}$	33586e9f	12fff033	b2d9f64d	6f8fea53
$B_{0..3}$	de943106	2742e439	4fbab5ac	62b9ff96
$C_{0..3}$	22e7b0af	c862b3a8	33e00cdc	236b86a6
$D_{0..3}$	f64ae77c	fa373b76	7dc1ee5b	7fb29ce8

SIMD-256 IV				
$A_{0..3}$	4d567983	07190ba9	8474577b	39d726e9
$B_{0..3}$	aaf3d925	3ee20b03	afd5e751	c96006d3
$C_{0..3}$	c2c2ba14	49b3bcb4	f67caf46	668626c9
$D_{0..3}$	e2eaa8d2	1ff47833	d0c661a5	55693de1

SIMD-384 IV				
$A_{0..3}$	8a36eebc	94a3bd90	d1537b83	b25b070b
$A_{4..7}$	f463f1b5	b6f81e20	0055c339	b4d144d1
$B_{0..3}$	7360ca61	18361a03	17dcb4b9	3414c45a
$B_{4..7}$	a699a9d2	e39e9664	468bfe77	51d062f8
$C_{0..3}$	b9e3bfe8	63bece2a	8fe506b9	f8cc4ac2
$C_{4..7}$	7ae11542	b1aadda1	64b06794	28d2f462
$D_{0..3}$	e64071ec	1deb91a8	8ac8db23	3f782ab5
$D_{4..7}$	039b5cb8	71ddd962	fade2cea	1416df71

SIMD-512 IV				
$A_{0..3}$	0ba16b95	72f999ad	9fecc2ae	ba3264fc
$A_{4..7}$	5e894929	8e9f30e5	2f1daa37	f0f2c558
$B_{0..3}$	ac506643	a90635a5	e25b878b	aab7878f
$B_{4..7}$	88817f7a	0a02892b	559a7550	598f657e
$C_{0..3}$	7eef60a1	6b70e3e8	9c1714d1	b958e2a8
$C_{4..7}$	ab02675e	ed1c014f	cd8d65bb	fdb7a257
$D_{0..3}$	09254899	d699c7bc	9019b6dc	2b9022e4
$D_{4..7}$	8fa14956	21bf9bd3	b94d0943	6ffddc22

Table 1.2: Initialization Vector for common versions of SIMD.

The message also needs to be interpreted as a matrix of 32-bit words to compute $IV \oplus M$. Each consecutive group of four bytes is interpreted as a word with the low-order (least significant) byte given first. The first word of IV and the first word of M are xored together to produce A_0, the second words are xored to compute A_1, and so on.

In the feed-forward, we need to see the IV as four vectors. The first vector IV_0 corresponds to the A vector of the state, IV_1 to the B vector, IV_2 to the C vector, and IV_3 to the D vector.

In the final compression function, we use a counter as the message input. The counter is taken modulo 2^m, so that it fits in one message block. The counter is converted to a sequence of bit using the same little endian convention: the first byte is the low-order byte. Note that the reference implementation only keeps a counter modulo 2^{64}, and is therefore unable to compute the hash of a message of more than 2^{64} bits, but this not a limitation of the algorithm.

Output Mapping

The output of SIMD is made of 32-bit words, which will be converted to bytes in a little-endian fashion: the first output byte is the low-order byte.

1.3 Rationale

The SIMD hash function follows the spirit of the MD/SHA family, but it should be protected against known attacks on members of this family.

1.3.1 Iteration Mode

We believe that Merkle-Damgård construction is now well understood, thanks to all previous attacks which have shown where weaknesses can be found. In particular the Merkle-Damgård iteration without no finalization function is sensible to some generic attacks:

- the extension attack;
- the second preimage attack on long messages [17];
- the multi-collision attack [15];
- various meet-in-the-middle attacks: building expandable messages from fixed point[8], preimages.

Those weakness can be tolerated, but we believe it is better to avoid them. This is why we use an internal state larger than the output size, and a modified compression function for the last block, (which is equivalent to a prefix-free encoding of the message).

1.3.2 Davies-Meyer

The Davies-Meyer mode is also well studied, and suffers the following problems:

- It is easy to find fixed-points, which can be used to build expandable messages. If we choose a message M, then $E_M^{-1}(0)$ is a fixed point as seen in Figure 1.6.
- In collision attacks, the feed-forward makes it quite easy to transform pseudo-collision into collisions. If we have a linear characteristic that gives a message difference Δ, we can use two non-linear characteristic to build a differential path $0 \rightsquigarrow \Delta$ and $\Delta \rightsquigarrow \Delta$ in the Feistel part. Figure 1.7 shows that this allows to find a collision when the input difference

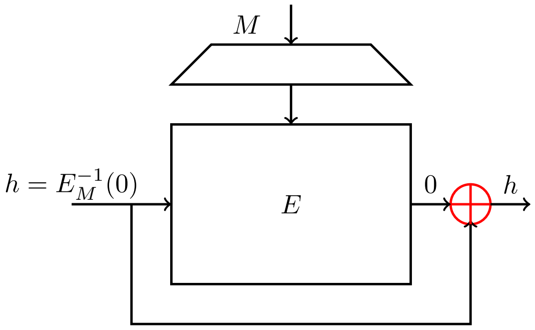

Figure 1.6: Finding fixed points in a Devies-Meyer compression function

Δ cancels the output difference Δ in the feed-forward. This property was used to break MD5 [27] and SHA-1 [26].

Our non-linear feedback should avoid these attacks.

However, it was pointed out by Gauravaram and Bagheri [14] that the modified Davies-Meyer used in SIMD is still easy to differentiate from a random function. Indeed, one can use a technique very similar to the fixed-point attack on the regular Davies-Meyer:

- Start with a state $\mathcal{S}^{(31)}$ (the output of the block cipher) so that the registers satisfy $A_j^{(31)} = 0$ and $D_j^{(31)} = \boxminus\phi^{(32)}(A_j^{(31)}, B_j^{(31)}, C_j^{(31)})$.
- The computation at step 32 is the first step of the feed-forward permutation P, and the computation will give back one IV word, up to a rotation:

$$\begin{aligned} A_j^{(32)} &= \left(D_j^{(31)} \boxplus IV_j \boxplus \phi^{(32)}(A_j^{(31)}, B_j^{(31)}, C_j^{(31)})\right)^{\lll s^{(32)}} \boxplus A_{p^{(32)}(j)}^{(31)} {}^{\lll r^{(32)}} \\ &= IV_j^{\lll s^{(32)}}. \end{aligned}$$

- Then, we have in the output of the compression function:

$$D_j^{(35)} = A_j^{(32)\lll r^{(33)}} = IV_j^{\lll s^{(32)} + r^{(33)}}$$

.

This gives some kind of partial fixed-points, where 128 bits of the output (256 for SIMD-512) are bits of the IV up to some rotation. This property is weaker than the fixed-points of a Davies-Meyer compression function, but it show that the compression function of SIMD is not a perfect function.

Note that is has no implication on the security of the SIMD hash function: many designs are based on the plain Davies-Meyer which has a stronger distinguisher, but the only known attacks based on fixed-points use this property to build expandable messages. In the case of SIMD, expandable messages can not be build from fixed points because the chaining value is twice as large as the output size. In fact, the security proofs of Coron *et al.* [6] show that the iteration of a Davies-Meyer based compression function is indifferentiable from a random oracle under the assumption that the block cipher is an ideal cipher.

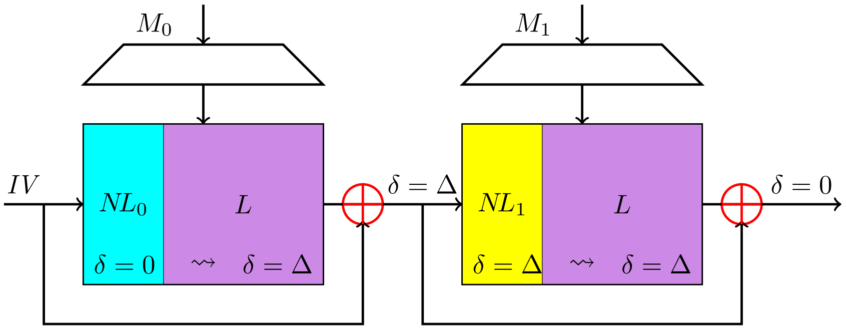

Figure 1.7: Multi-block attack using the Davies-Meyer feed-forward.

1.3.3 The Message Expansion

When a block cipher is used to build hash function in Davies-Meyer mode, the key of the block cipher is under control of the attacker. This setting is quite different from the regular use of a block cipher, since an attack against the hash function usually translates to a related-key attack on the block cipher. Therefore, the block cipher should be designed with a strong key expansion (the key expansion of the block cipher become the message expansion of the hash function).

Indeed, most attacks against Davies-Meyer based hash functions take advantage of the weak message expansion. For the members of the MD/SHA family, the message expansion can be seen as a linear code and the minimal distance of this code seems to play a very important role. This minimal distance is only 3 and 4 for MD4 and MD5, so the attacker has a lot of control. In SHA-1, the minimal distance is no more than 44, and is exactly 25 in the last 60 words [16]. Additionally, it is easy to shift a differential pattern one round down. This allows to build local collisions.

In our design, we follow the approach of Jutla and Patthak [16], who designed a better message expansion for SHA-1 with a minimal distance of 82, and 75 on the last 60 words. In [16], the authors used a code with a structure similar to the code of SHA-1 for efficiency reasons, and ruled out various algebraic codes. They consider Reed-Solomon codes over $\mathbb{F}_{2^8}$ which have a very good minimal distance, but they conclude they are unsuitable for a software implementation. In SIMD, we do use a Reed-Solomon code, but we use the field $\mathbb{F}_{257}$ for an efficient software implementation. This field was already used in the design of SWIFFT [19] for the same reason. Finally using concatenated codes, we can increase the minimal distance without adding much computations.

Our message expansion is designed to avoid related key attacks on the block cipher. It has a provable minimal distance of 520 for SIMD-256, and 1032 for SIMD-512. After the NTT layer of SIMD-256, any pair of distinct message are mapped to a sequence of 128 elements in $\mathbb{F}_{257}$, with at least 65 distinct components (resp. 256 elements with 129 distinct elements). The concatenated code maps the elements of $\mathbb{F}_{257}$ to 16-bit words, so that two distinct elements are mapped to words with a Hamming distance of at least 4. We have two copies of the concatenated code (with two different inner codes), so this makes a minimal hamming distance of $2 \times 4 \times 65 = 520$ for the message expansion of SIMD-256 (resp. $2 \times 4 \times 129 = 1032$ for SIMD-512).

Chapter 2

Implementation Aspect and Performances

The design of SIMD is highly parallellisable due to the choice of the components: the NTT and the parallel Feistel ladders. This should allow efficient hardware implementations. As far as software is concerned, we can use SIMD instructions (Single Instructions, Multiple Data) to compute some operations in parallel.

2.1 Software Implementation

2.1.1 SIMD Instructions

SIMD instructions allow to compute a given operation on multiple data in parallel. Processors that supports SIMD instructions usually come with a set of dedicated registers, which can contain a vector of integers or floating point data. For instance the SSE registers in x86 processors are 128-bit wide and can be used to store 16 8-bit values, 8 16-bit values, 4 32-bit values, or 2 64-bit values. The SIMD instruction set allows to compute in parallel some arithmetic operations on those vectors: addition, multiplication, bitwise operations, ...

SIMD instructions were introduced in personal computers to improve the efficiency of multimedia computations, and are now very widely available. The x86 family offers MMX since 1997 and SSE since 1999 and the PPC family has AltiVec since 1998. For embedded systems, Intel has introduced IwMMXt to its PXA family of ARM processors, and is now promoting the Atom, an x86 processor which supports SSE. We believe that SIMD support will become even more widespread in the future. We also note that the efficiency of SIMD implementations is constantly improving: the SSE units of Intel Core micro-architecture based processors is much faster than in the older NetBurst micro-architecture. Similarly, the new AMD K10 processors feature a much better SSE units than AMD K8 ones.

Another advantage of SIMD instructions is that they usually come with a relatively large set of registers, even on CISC processors. The x86 architecture has only 8 general purpose 32-bit registers but SSE instructions comes with 8 extra 128-bit registers (on x86-64 we have 16 general purpose 64-bit registers, and 16 128-bit SSE registers). In most cases, the full state of the Feistel ladder can be kept inside those registers, which is good for performances. The NTT can also be computed mostly inside the registers.

2.1.2 Optimized Implementation

The NTT is the main component of the message expansion, and the high minimal distance is mainly due to the NTT. However the NTT is quite expensive and has to be carefully optimized to make an efficient implementation of SIMD.

Field Operations

An element of $\mathbb{F}_{257}$ will be stored in a signed 16-bit word. The choice of the field $\mathbb{F}_{257}$ allows an efficient implementation of the field operations, because 257 is a prime and $256 = -1 \pmod{257}$.

To reduce x modulo 257, we let q and r be the quotient and the remainder of the division of x by 256, and we have $x = r - q \pmod{257}$. This can be written as `(x&0xff) - (x>>8)` in C, provided that the integers are represented in a two's-complement arithmetic, and that the right shift operation preserves the sign bit (which is an implementation defined behaviour). The result is not fully reduced and will be between -127 and 383. When a full reduction is needed, we substract 257 to values over 128, and get a result between -128 and 128. This reduction is quite fast to compute because it only uses bitwise operations, and no division. Moreover, these operation are available in most SIMD instruction sets.

To compute a multiplication in $\mathbb{F}_{257}$, we reduce both operands to $\{-128, ...128\}$, and the result can be computed with a single multiplication modulo 2^{16} with no overflow.

Note that it is not necessary to perform a reduction after each field operation, because we have some extra bits in a 16-bit word. We have to study the NTT algorithm to find out where reductions are needed.

NTT Computation

Because SIMD instructions compute the same operation on each element of the vectors, we can't use the classical radix-2 FFT algorithm. Instead, we will rewrite the one-dimensional NTT as a two-dimensional one. In our implementation, we rewrite the NTT of size 64 as a two-dimensional NTT of size 8×8. The input data is seen as a 8×8 matrix, and the computation of the NTT_{64} is done in three steps:

- First we compute 8 NTT_8 on the columns of the matrix using a decimation in time algorithm.
- We multiply by the twiddle factors, transpose the matrix, and permute the row and the columns following the bit reversal order.
- Then we compute 8 NTT_8 on the columns of the matrix using a decimation in frequency algorithm.

The first and the last step are easy to parallelize with SIMD instruction. Moreover, the root of unity used in the NTT_8 will be 4, so the multiplications will only be bit shifts. The transposition can be implemented using the merge operation that is available on most SIMD instruction sets (`punpcklwd/punpckhwd` in SSE, `vmrghh/vmrglh` in Altivec, `wunpckilh/wunpckihh` in IwMMXt).

For more details on the NTT and FFT algorithms, see [22].

Computation of the Feistel Ladder

The computation of the Feistel Ladder can also be parallelized with SIMD instruction. We store each row of the state matrix in a vector register, and the step functions can be computed in parallel.

					Scalar		Vector	
Architecture		SHA-1/256/512			SIMD-256/512		SIMD-256/512	
Core2	32 bits	261	140	45	31	24	245	220
	64 bits	323	176	223	45	33	270	250
K10	32 bits	207	135	39	30	20	145	145
	64 bits	301	147	193	38	29	160	160
P4	32 bits	147	89	19	16	13	85	65
K8	32 bits	174	107	31	23	15	80	?
	64 bits	238	111	148	30	22	78	?
Atom	32 bits	66	35	12	7.2	5.7	64	50
G4	32 bits	102	55	16	10	7.5	78	55
ARM		19	11	3.0	2.1	1.6	9	?

Table 2.1: Performances of SIMD compared to the SHA family. The figures are in megabyte per second (MB/s).

2.1.3 Multi-core

Our design can also exploit multi-core processors: the most expensive part of the algorithm is the message expansion, and it can be done in parallel for different message blocks. When using two cores, we gain a factor 1.8 on the performance.

The synchronisation cost can be made very low if each core computes the message expansion on many message block before waiting for the chaining value from the other core.

2.1.4 Performance

SIMD-512 and SIMD-256 offer comparable performances: one SIMD-512 compression function need roughly twice the number of operations of one SIMD-256 compression function, but it also take a message block twice as big. SIMD-512 is still somewhat slower because of the higher memory requirement, and the slightly more expensive NTT (because of the $\log n$ factor). As a general rule, the message expansion of SIMD takes half of the computing time.

The memory requirement of SIMD is essentially the internal state (64 bytes for SIMD-256 and 128 bytes for SIMD-512) and the output of the NTT ($4 \times 64 = 256$ bytes for SIMD-256 and $4 \times 128 = 256$ bytes for SIMD-512).

The performance for SHA-1, SHA-256 and SHA-512 have been obtained using the implementation from sphlib [25]. We used the same compiler for SHA and SIMD.

We stress that the *optimized* versions are not really optimized since they are written in pure C, and only use scalar instructions. The natural way to write an optimized version of SIMD is to write a vectorized implementation using SIMD instructions, which are available on many platforms.

Performances on a range of computers are given in Table 2.1 and Table 2.2. We compare two implementations of SIMD, a scalar one written in pure C and a vectorized one written in C using compiler extensions to access the SIMD instructions. Our vector implementation runs on x86 with SSE2, on PowerPC with Altivec, and on ARM with IwMMXt. More extensive benchmarks are available from the eBASH project [11].

					Scalar		Vector	
Architecture		SHA-1/256/512			SIMD-256/512		SIMD-256/512	
Core2	32 bits	11	21	63	90	118	12	13
	64 bits	9	16	13	63	85	11	12
K10	32 bits	12	18	64	80	125	17	17
	64 bits	9	17	13	65	85	16	16
P4	32 bits	19	89	147	170	210	32	43
K8	32 bits	12	19	65	90	135	25	?
	64 bits	9	18	14	66	88	26	?
Atom	32 bits	24	46	133	220	280	25	32
G4	32 bits	12	23	78	125	166	16	23
ARM		22	38	138	200	260	46	?

Table 2.2: Performances of SIMD compared to the SHA family. The figures are in cycles per byte (c/B).

Software Platforms

Here is a brief description of the test platforms:
Core2: Intel Xeon E5440 running at 2.83 GHz; compiled with gcc 4.1.2.
K10: AMD Phenom 9850 running at 2.5 GHz; compiled with gcc 4.2.4.
P4: Intel Pentium 4 running at 2.8 GHz; compiled with gcc 4.1.2.
K8: AMD Athlon64 X2 3800+ running at 2 GHz; compiled with gcc 4.2.3.
Atom: Intel Atom N270 running at 1.6 GHz; compiled with gcc 4.1.3.
G4: PowerPC 7447 running at 1.25 GHz; compiled with gcc 4.1.2.
ARM: Intel XScale PXA270 running at 416 MHz; compiled with gcc 4.1.3.

2.2 8-bit Implementation

We also tested SIMD on a 8-bit platform. We used gcc to compile the optimized code to an Atmel AVR AtMega8, and we ran it in the simularv simulator. We optimized some part of the code with inline assembly to handle efficiently some 32-bits operations on the 8-bit architecture. Our code ran at approximately 1300 cycles/byte.

2.3 Hardware Implementation

We did a preliminary study to implement SIMD on a FPGA. The Feistel part of SIMD can be implemented in the same way as the Feistel part of other hash functions of the MD/SHA family, and we would include the hardware to compute the four Feistels in parallel (resp. eight for SIMD-512). Since SIMD has less steps than SHA-1 and SHA-2, this part will run faster, but requires more gates to computes the four Feistels. To compute the NTT, we propose to include the hardware to compute a size 8 NTT, which will be called 32 times to compute the size 128 NTT of SIMD-256. It should run at about the same speed as the Feistel part.

Chapter 3

Expected Strength

We conjecture that no non-random properties of an instance of SIMD-224 or SIMD-256 (indexed by the IV) can be identified with less than 2^{256} calls to the compression function.

Similarly we conjecture that no non-random properties of an instance of SIMD-384 or SIMD-512 can be identified with less than 2^{512} calls to the compression function.

In particular this means that we believe that a collision attack on SIMD-n has a complexity of $2^{n/2}$, and a preimage or second preimage attack has a complexity of 2^n. There should be neither shortcut multi-collision attack nor shortcut second preimage against long messages.

3.1 Security of the compression function

The compression function of SIMD has a relatively slow diffusion, and it might be possible to build free-start distinguishers that do not introduce differences in the message. This was the case in SIMD 1.0, as shown by [21]. However, this kind of distinguisher is very unlikely to be useful against the full hash function because of the wide-pipe design of SIMD. The compression function was designed assuming that the chaining value is hard to control, which is the case when the compression function is iterated to build the hash function.

In Section 4.4, we introduce a strengthened version of SIMD, SIMD+, which is designed to avoid this kind of distinguisher by using of more compression rounds.

Chapter 4

Security Analysis

4.1 Mode of Operation

4.1.1 Mode of Operation for the Hash Function

Since we use a modified message expansion for the final compression function, the expanded message will be prefix free. This allow better security proofs of the iteration mode. Alternatively, we can model the compression function C and the final compression C' as two independent random oracles and see our construction as an instance of the wide-pipe design of Lucks [18].

Thus, following proofs from [5, 20, 18], our iteration mode is indifferentiable from a random oracle if the compression function is a random oracle. These proofs show that there is no generic attack against the mode of operation. Moreover, the security proved is up to 2^n queries, where n is the length of the hash function. Consequently, there are no generic attack against collision, second-preimage attack or preimage attack.

Furthermore, Coron *et al.* [6] showed that the same results can be obtained under the assumption that the underlying block cipher is an ideal cipher. This result is important and shows that distinguisher based on fixed-point that can be found against the Davies-Meyer mode and our modified Davies-Meyer mode do not affect the security of the hash function.

4.1.2 Security Results for Some Hash Based Constructions

The security proof for ChopMD has been provided in [5] by Chang and Nandi at FSE 2008 and the security proof for ChopMD with prefix-free message by Maurer and Tessaro at Crypto 2007 in [20, Section 5] in the indifferentiablity framework. Such results show that there is no generic attack against the mode of operation. Moreover, since the security is above the birthday barrier and in 2^n if n is the hash length, then there is no better collision, second or preimage attack.

Moreover, the fact that messages are *prefix-free* allows to prove that the cascade construction of a PRF function is also a PRF [2]. This can also be used to prove the security of MAC function.

MAC Function

We propose two distinct ways to build a Message Authentication Code from the SIMD hash function.

First, as any Merkle-Damgård based hash function, SIMD can be used with the HMAC construction. We define HMAC-SIMD as:

$$\text{HMAC-}\mathsf{SIMD}_k(M) = \mathsf{SIMD}(\bar{k} \oplus \text{opad}\,\|\mathsf{SIMD}(\bar{k} \oplus \text{ipad}\,\|M)).$$

The security proof of Bellare in [1] can be used to prove the security of HMAC-SIMD.

Second, we can simply compute $\text{MAC}_k(M) = \mathsf{SIMD}(k\|M)$ where $\|$ denotes the concatenation. The key can be padded to a full block to allow more efficient implementations. Thanks to the security proof in the indifferentiability framework, there are no generic shortcut attack on this construction. This means that one has to find a weakness in the compression function in order to break this MAC.

Key Derivation

If SIMD is a PRF assuming that the compression function is a good PRF, then it is easy to prove that SIMD is a good randomness extractor that can be plugged in a key derivation function. Such results have been provided in [12]. The important point to construct a good randomness extractor already pointed out in [10] is the fact that we need to truncate the output of the function.

4.1.3 Mode of Operation for the Compression Function

The mode of operation for the compression function does not follow directly from the Davies-Meyer mode of operation. This mode presents some weaknesses we want to avoid : fix points can be easily found for example. The mode we used can be seen as a variant of the construction 8 of paper [4] (and construction 41 from [24]). Finally, the proofs provided in [4] can be extended to our construction in the ideal cipher model.

4.2 Security of the Compression Function

4.2.1 Resistance to Differential Cryptanalysis

The SIMD-family is provably secure against a class of differential attacks. This is based on the fact that the message expansion has a high minimal distance: any pair of distinct messages gives expanded messages with a least 520 bit differences for SIMD-256, resp. 1032 for SIMD-512.

If we assume that the attacker does not control the positions of the differences in the expanded message, each difference in the expanded message will introduce a difference in the state, and the attacker has to control its propagation. The attacker must at least control the effect of the carry, which will be good with a probability of 2^{-1}. As a comparison, in SHA-1, it is quite easy to control the error propagation because the perturbation vector can shifted to correct the errors, but the success probability is only $2^{-2.5}$. We expect that it will actually be more difficult to control the propagation of differences in SIMD.

Even if the adversary can use message-modification techniques to control the non-linearity in one half of the hash function for free, he still has to deal with 260 differences, resp. 516 for SIMD-512. Note that our compression function construction forces the adversary to choose the message from the beginning, so we do not expect message modification techniques to work.

4.2.2 The Step Update Function

The step update function of SIMD is defined as:

$$A_j^{(i)} = \left(A_j^{(i-4)^{\lll r_{i-4}}} \boxplus W_j^{(i)} \boxplus \phi^{(i)}(A_j^{(i-1)}, A_j^{(i-2)^{\lll r_{i-2}}}, A_j^{(i-3)^{\lll r_{i-3}}})\right)^{\lll s^{(i)}} \boxplus A_{p^{(i)}(j)}^{(i-1)^{\lll r^{(i)}}}$$

It is quite similar to the step update functions of members of the MD/SHA family, and has been built with previous attacks on these functions in mind.

Our function is of form $A^{(i)} = F(A^{(i-4)}, A^{(i-3)}, A^{(i-2)}, A^{(i-1)}) \boxplus A^{(i-1)}$, like in MD5. This gives a good avalanche effect, since a difference in $A^{(i-1)}$ will most likely be propagated to $A^{(i)}$ and can not be easily absorbed. Most attacks on MD4 are based on the fact that the step update allows to easily absorb a difference in the internal state.

Den Boer and Bosselaers discovered an other kind of weakness in the step update function of MD5 [9]. If there is some differential pattern in $A^{(i-4)}, A^{(i-3)}, A^{(i-2)}, A^{(i-1)}$, that can be cancelled through F, then the addition of $A^{(i-1)}$ will reintroduce this pattern and it will propagate in the compression function. To avoid this kind of attack, we added a rotation on $A^{(i-1)}$ in the design of SIMD.

4.3 Reduced Versions

We define two kind of reduced versions of SIMD. The first one, SISD is very similar to SIMD but has only one or two parallel Feistels, and can only produce short digests (less than 128 bits). We believe SISD can be useful to try cryptanalytic techniques on a smaller scale. It could also be used instead of the full SIMD in some constrained environments where only a small amount of memory is available.

In the second section, we define round-reduced version to be used as an easier target for cryptanalysis.

4.3.1 SISD-n

We first define the family SISD, which is a short digest constructed as a reduced version of SIMD. SISD-n is defined for $n \leq 128$, and the family is based on two designs: SISD-128 and SISD-64. SISD-n with $n \leq 64$ is a truncation of SIMD-64, and SISD-n with $64 < n \leq 128$ as a truncation of SISD-128. SISD is essentially similar to SIMD, but uses fewer parallel Feistels: SISD-64 has a single one, and SISD-128 has two.

The first message expansion step of SISD-128 is defined as:

$$\begin{aligned} O : (\mathbb{Z}_{2^8})^{32} &\to (\mathbb{F}_{257})^{64} \\ (x_j)_{j=0}^{31} &\mapsto (y_i)_{i=0}^{63} : \quad y_i = \sum_{j=0}^{31} x_j \alpha^{ij} + \alpha^{63i} \pmod{257}. \end{aligned}$$

where $\alpha = 46$ is a 64th root of unity in $\mathbb{F}_{257}$. And similarly for SISD-64:

$$\begin{aligned} O : (\mathbb{Z}_{2^8})^{16} &\to (\mathbb{F}_{257})^{32} \\ (x_j)_{j=0}^{15} &\mapsto (y_i)_{i=0}^{31} : \quad y_i = \sum_{j=0}^{15} x_j \alpha^{ij} + \alpha^{31i} \pmod{257}. \end{aligned}$$

where $\alpha = 60$ is a 32th root of unity in $\mathbb{F}_{257}$. Then we have in SISD-128:

$$Z_j^{(i)} = \begin{cases} I_{185}\big(y[4i+2j], & y[4i+2j+1]\big) \quad \text{when } 0 \leq i \leq 15 \\ I_{233}\big(y[4i+2j-64], & y[4i+2j-32]\big) \quad \text{when } 16 \leq i \leq 23 \\ I_{233}\big(y[4i+2j-95], & y[4i+2j-63]\big) \quad \text{when } 24 \leq i \leq 31 \end{cases}$$

and in SISD-64:

$$Z_j^{(i)} = \begin{cases} I_{185}\big(y[2i+2j], & y[2i+2j+1]\big) \quad \text{when } 0 \le i \le 15 \\ I_{233}\big(y[2i+2j-32], & y[2i+2j-16]\big) \quad \text{when } 16 \le i \le 23 \\ I_{233}\big(y[2i+2j-47], & y[2i+2j-31]\big) \quad \text{when } 24 \le i \le 31 \end{cases}$$

Finally, the expanded message is defined as $W_j^{(i)} = Z_j^{(P(i))}$. In the Feistel part, SISD-128 uses the permutation $p(x) = x \oplus 1$ while SISD-64 uses the identity.

SISD can be used to compute short digest, and we expected it to be as strong as SIMD. However we do not recommend using it as a general purpose hash function because it is less parallelizable than SIMD. The performances of SISD are expected to be lower than that of SIMD on high-end architecture, but it should perform well in low-end machines which have no SIMD instructions and where little memory is available.

We also define two sets of reduced version of SIMD for security analysis, with a reduced number of steps, and a weaker message expansion. We encourage cryptographers to try and break them. Note that these round-reduced versions can also be defined for SISD.

4.3.2 SIMD-$n/2.k$

We let SIMD-$n/2.k$ be a reduced version of SIMD-n with $2k$ steps in the main part of the Feistel instead of 2×16. The steps of SIMD-$n/2.k$ are the steps 0, 1, ... $k-1$, and 16, 17, ... $15+k$ of SIMD-n, plus the feed-forward steps. For SIMD-256/2.k, the reduced message expansion is defined as:

$$W_j^{(i)} = \begin{cases} I_{185}\big(y[8i+2j], & y[8i+2j+1]\big) \quad \text{when } 0 \le i < k \\ I_{233}\big(y[8i+2j-128], & y[8i+2j-127]\big) \quad \text{when } 16 \le i < 16+k \end{cases}$$

and for SIMD-512/k:

$$W_j^{(i)} = \begin{cases} I_{185}\big(y[16i+2j], & y[16i+2j+1]\big) \quad \text{when } 0 \le i < k \\ I_{233}\big(y[16i+2j-256], & y[16i+2j-255]\big) \quad \text{when } 16 \le i < 16+k \end{cases}$$

SIMD-$n/2.k$ is defined for k between 8 and 16 (with $k < 8$, the message expansion would not be injective).

4.3.3 SIMD-n/k

We let SIMD-n/k be a reduced version of SIMD-n with only k steps in the main part of the Feistel. The steps of SIMD-n/k are the steps 0, 1, ... $k-1$ of SIMD-n. For SIMD-256/k, the reduced message expansion is defined as:

$$W_j^{(i)} = I_{185}\big(y[8i+2j], y[8i+2j+1]\big)$$

and for SIMD-512/k:

$$W_j^{(i)} = I_{185}\big(y[16i+2j], y[16i+2j+1]\big)$$

SIMD-n/k is defined for k between 8 and 16.

There are no permutations is these reduced versions, and the message expansion of SIMD-256/2.k and SIMD-256/k only uses $8k$ outputs of the NTT ($16k$ for SIMD-512/k). SIMD-$n/2.16$ and SIMD-$n/16$ uses the full NTT, while in SIMD-$n/8$ SIMD-$n/2.8$, the NTT does not expand the message at all, which should greatly reduce the security.

Note that SIMD-$n/2.8$ and SIMD-$n/16$ both have 16 steps, but the message expansion of SIMD-$n/2.8$ is much weaker than the message expansion of SIMD-$n/16$.

4.4 Strengthened Versions

Finally, we define a strengthened version of SIMD with more rounds in the Feistel part, called SIMD+. SIMD+ is designed to have a big security margin, while being somewhat less efficient that SIMD. The compression function of SIMD+ is expected to be very strong, and we conjecture that no non-random property of the implicit block cipher of SIMD+n can not be detected using less than 2^n operations. SIMD+ has twice the number of rounds of SIMD, and the throughput is around 25% lower than that of SIMD because the message expansion still costs the same (SIMD+ runs between 15 and 17 cycles per byte on a Core2).

SIMD+ uses two new inner codes:

$$\begin{aligned}
I_{-185} : \mathbb{F}_{257} &\to \mathbb{Z}_{2^{16}} \\
x &\mapsto (2^{16} - 185) \boxtimes \widetilde{x} \qquad \text{where } -128 \leq \widetilde{x} \leq 128 \text{ and } \widetilde{x} = x \pmod{257} \\
I_{-233} : \mathbb{F}_{257} &\to \mathbb{Z}_{2^{16}} \\
x &\mapsto (2^{16} - 233) \boxtimes \widetilde{x} \qquad \text{where } -128 \leq \widetilde{x} \leq 128 \text{ and } \widetilde{x} = x \pmod{257}
\end{aligned}$$

These codes have the same properties as I_{185} and I_{233}: they are efficient and achieve a minimal distance of 4.

The intermediate expanded message is defined by taking four copies of the message, encoded with the four inner codes. For SIMD+256, we have (with $0 \leq j \leq 3$):

$$Z_j^{(i)} = \left\{ \begin{array}{lll}
I_{185}\big(y[8i+2j], & y[8i+2j+1]\big) & \text{when } 0 \leq i \leq 15 \\
I_{233}\big(y[8i+2j-128], & y[8i+2j-64]\big) & \text{when } 16 \leq i \leq 23 \\
I_{233}\big(y[8i+2j-191], & y[8i+2j-127]\big) & \text{when } 24 \leq i \leq 31 \\
I_{-185}\big(y[8i+2j-256], & y[8i+2j-255]\big) & \text{when } 32 \leq i \leq 47 \\
I_{-233}\big(y[8i+2j-384], & y[8i+2j-320]\big) & \text{when } 48 \leq i \leq 55 \\
I_{-233}\big(y[8i+2j-447], & y[8i+2j-383]\big) & \text{when } 56 \leq i \leq 63
\end{array} \right.$$

For SIMD+512, we have (with $0 \leq j \leq 7$):

$$Z_j^{(i)} = \left\{ \begin{array}{lll}
I_{185}\big(y[16i+2j], & y[16i+2j+1]\big) & \text{when } 0 \leq i \leq 15 \\
I_{233}\big(y[16i+2j-256], & y[16i+2j-128]\big) & \text{when } 16 \leq i \leq 23 \\
I_{233}\big(y[16i+2j-383], & y[16i+2j-255]\big) & \text{when } 24 \leq i \leq 31 \\
I_{-185}\big(y[16i+2j-512], & y[16i+2j-511]\big) & \text{when } 32 \leq i \leq 47 \\
I_{-233}\big(y[16i+2j-768], & y[16i+2j-640]\big) & \text{when } 48 \leq i \leq 55 \\
I_{-233}\big(y[16i+2j-895], & y[16i+2j-767]\big) & \text{when } 56 \leq i \leq 63
\end{array} \right.$$

Then, the expended message is defined using the same permutation as in SIMD:

$$W_j^{(i)} = Z_j^{(P(i \bmod 32))}.$$

The rotations used in the rounds 4, 5, 6 and 7 are the same as those in rounds 0, 1, 2 and 3 respectively.

Chapter 5

Advantages and Limitations

5.1 Parallelism

SIMD features a small scale parallelism. The compression function itself can be parallelized to some extend. This can be used to improve hardware efficiency, and allows an efficient software implementation using SIMD instructions. The fact that about half the time required to compute the hash function is spent in the message expansion also allows a second level of parallelism: the message expansion of the message block $i+1$ can be computed while the Feistel part is compressing the message block i.

We believe that this level of parallelism is sufficient for a general purpose hash function. If a specific application require an extremely fast hash function, it can use SIMD in a custom parallel mode. For instance, given a parallelization parameter k, one can split the message into k independent parts, hash the k parts with SIMD, and use an extra call to SIMD to rehash the concatenation of the k hash values.

5.2 Security

We believe that the internal block cipher in a hash function does not have the same security requirement than a block cipher used to encrypt a message. In particular, the block cipher inside a Davies-Meyer hash function should be secure under related key attacks. This is why the message expansion of SIMD is very strong. The security of the hash function is mainly based on its very high minimal distance. Of course, this also means that the message expansion is quite expensive: it accounts for about half the time spent in the hash function. However, there are some cases where we can reduce this cost and improve the efficiency of SIMD. If there is only a small of the message block that is variable, we can precompute the NTT of the fixed part, and add the variable part when it is known. This trick can be used to speed up the hashing of small messages (the counter in the final compression function has at most two active byte), or when SIMD is used in counter mode.

5.3 Performance

The performances of SIMD are very good on high-end desktop computers. SIMD-256 only needs 11 cycles per byte on one core of a Core2 processor, and we can go down to 6 cycles per byte if we use two cores. More generally, SIMD is efficient on architectures which include a set of SIMD instructions.

On the other hand, it should also be noted than a fast implementation of the SIMD hash function has to use SIMD instructions, and can be written in pure C. Similarly, the performances are not very good if there is no SIMD support on the target platform.

Bibliography

[1] Bellare, M.: New Proofs for NMAC and HMAC: Security without Collision-Resistance. In Dwork, C., ed.: CRYPTO. Volume 4117 of Lecture Notes in Computer Science., Springer (2006) 602–619

[2] Bellare, M., Canetti, R., Krawczyk, H.: Pseudorandom Functions Revisited: The Cascade Construction and Its Concrete Security. In: FOCS. (1996) 514–523

[3] Biham, E., Youssef, A.M., eds.: Selected Areas in Cryptography, 13th International Workshop, SAC 2006, Montreal, Canada, August 17-18, 2006 Revised Selected Papers. In Biham, E., Youssef, A.M., eds.: Selected Areas in Cryptography. Volume 4356 of Lecture Notes in Computer Science., Springer (2007)

[4] Black, J., Rogaway, P., Shrimpton, T.: Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV. In Yung, M., ed.: CRYPTO. Volume 2442 of Lecture Notes in Computer Science., Springer (2002) 320–335

[5] Chang, D., Nandi, M.: Improved Indifferentiability Security Analysis of chopMD Hash Function. [23] 429–443

[6] Coron, J.S., Dodis, Y., Malinaud, C., Puniya, P.: Merkle-Damgård Revisited: How to Construct a Hash Function. In: CRYPTO'05. (2005) 430–448

[7] Cramer, R., ed.: Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings. In Cramer, R., ed.: EUROCRYPT'05. Volume 3494 of Lecture Notes in Computer Science., Springer (2005)

[8] Dean, R.D.: Formal Aspects of Mobile Code Security. PhD thesis, Princeton University (January 1999)

[9] den Boer, B., Bosselaers, A.: Collisions for the Compression Function of MD5. In: EUROCRYPT. (1993) 293–304

[10] Dodis, Y., Gennaro, R., Håstad, J., Krawczyk, H., Rabin, T.: Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes. [13] 494–510

[11] Bernstein, D.J., Lange, T., eds.: eBACS: ECRYPT Benchmarking of Cryptographic Systems. `http://bench.cr.yp.to`

[12] Fouque, P.A., Pointcheval, D., Zimmer, S.: HMAC is a randomness extractor and applications to TLS. In Abe, M., Gligor, V.D., eds.: ASIACCS, ACM (2008) 21–32

[13] Franklin, M.K., ed.: Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings. In Franklin, M.K., ed.: CRYPTO'04. Volume 3152 of Lecture Notes in Computer Science., Springer (2004)

[14] Gauravaram, P., Bagheri, N. Private communication (July 2009)

[15] Joux, A.: Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions. [13] 306–316

[16] Jutla, C.S., Patthak, A.C.: Provably Good Codes for Hash Function Design. [3] 376–393

[17] Kelsey, J., Schneier, B.: Second Preimages on n-Bit Hash Functions for Much Less than 2^n Work. [7] 474–490

[18] Lucks, S.: A Failure-Friendly Design Principle for Hash Functions. In Roy, B.K., ed.: ASIACRYPT'05. Volume 3788 of Lecture Notes in Computer Science., Springer (2005) 474–494

[19] Lyubashevsky, V., Micciancio, D., Peikert, C., Rosen, A.: SWIFFT: A Modest Proposal for FFT Hashing. [23] 54–72

[20] Maurer, U.M., Tessaro, S.: Domain Extension of Public Random Functions: Beyond the Birthday Barrier. In Menezes, A., ed.: CRYPTO. Volume 4622 of Lecture Notes in Computer Science., Springer (2007) 187–204

[21] Nad, T., Mendel, F. Private communication (August 2009)

[22] Nussbaumer, H.: Fast Fourier Transform and Convolution Algorithms. Springer-Verlag (1982)

[23] Nyberg, K., ed.: Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers. In Nyberg, K., ed.: FSE. Volume 5086 of Lecture Notes in Computer Science., Springer (2008)

[24] Preneel, B., Govaerts, R., Vandewalle, J.: Differential Cryptanalysis of Hash Functions Based on Block Ciphers. In: ACM Conference on Computer and Communications Security. (1993) 183–188

[25] Projet RNRT SAPHIR: sphlib 1.0. `http://www.crypto-hash.fr/modules/wfdownloads/singlefile.php?cid=9&lid=5`

[26] Wang, X., Yin, Y.L., Yu, H.: Finding Collisions in the Full SHA-1. In Shoup, V., ed.: CRYPTO. Volume 3621 of Lecture Notes in Computer Science., Springer (2005) 17–36

[27] Wang, X., Yu, H.: How to Break MD5 and Other Hash Functions. [7] 19–35

Appendix A

Test Vectors

In this section we give test vectors and intermediate value during the computations. This should help implementors to make a correct implementation.

The hash values of the test-vectors are:

M	SIMD-224(M)
Empty message	`43e1d53656d7b85d10d5499e28afdef90bb497730d2853c8609b534b`
`0x00`, `0x01`, `0x02`, ...`0x3f`	`cbb4f8a9304b4b043093a94b7059ee36e43ff94a21dc46611f1a7769`
700 1 bits	`19499a44b7541c7f27b867b207f87269d7351d2cbb405f7c0cb491aa`

M	SIMD-256(M)
Empty message	`8029e81e7320e13ed9001dc3d8021fec695b7a25cd43ad805260181c35fcaea8`
`0x00`, `0x01`, `0x02`, ...`0x3f`	`5bebdb816cd3e6c8c2b5a42867a6f41570c4b917f1d3b15aabc17f24679e6acd`
700 1 bits	`e80b4eeb8a370e6ca918e7810400441f6dd0da1eb4559cade791c314f82d524a`

M	SIMD-384(M)

Empty message	`5fdd62778fc213221890ad3bac742a4af107ce2692d6112e`
	`795b54b25dcd5e0f4bf3ef1b770ab34b38f074a5e0ecfcb5`

`0x00`, `0x01`, `0x02`, ...`0x7f`	`5e02e645868ef837f535f44609a268a0a146476584d50f83`
	`683ce3e7cb355caaf7e8eb81cb28db3ccf40d25313f16950`

1079 1 bits	`e999b35b42301eca3a9c648fef39635b13059b2ac3be16f5` `c9372d3e773a716f1b2a23b784f3c1e231e42d87d2c950f3`

M	SIMD-512(M)

Empty message	`51a5af7e243cd9a5989f7792c880c4c3168c3d60c4518725fe5757d1f7a69c63`
	`66977eaba7905ce2da5d7cfd07773725f0935b55f3efb954996689a49b6d29e0`

`0x00`, `0x01`, `0x02`, ...`0x7f`	`8851ad0a57426b4af57af3294706c0448fa6accf24683fc239871be58ca913fb`
	`ee53e35c1dedd88016ebd131f2eb0761e97a3048de6e696787fd5f54981d6f2c`

1079 1 bits	`c060fa9aae2414715a3a27c5df22dbd41469e3d09056b093861f0f6b9bdc311a`
	`24ac743811e88358dc69094ad444036bbbf7708ed8bdeaf1e8ed871dfb79c218`

A.1 SIMD-224

A.1.1 Empty Message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    2  156  118  107   45  212  111  162
y[  8.. 15] =   97  249  211    3   49  101  151  223
y[ 16.. 23] =  189  178  253  204   76   82  232   65
y[ 24.. 31] =   96  176  161   47  189   61  248  107
y[ 32.. 39] =    0  131  133  113   17   33   12  111
y[ 40.. 47] =  251  103   57  148   47   65  249  143
y[ 48.. 55] =  189    8  204  230  205  151  187  227
y[ 56.. 63] =  247  111  140    6   77   10   21  149
y[ 64.. 71] =  255  101  139  150  212   45  146   95
y[ 72.. 79] =  160    8   46  254  208  156  106   34
y[ 80.. 87] =   68   79    4   53  181  175   25  192
y[ 88.. 95] =  161   81   96  210   68  196    9  150
y[ 96..103] =    0  126  124  144  240  224  245  146
y[104..111] =    6  154  200  109  210  192    8  114
y[112..119] =   68  249   53   27   52  106   70   30
y[120..127] =   10  146  117  251  180  247  236  108
```

Intermediate Expanded Message

```
Z[ 0] = b7030172  4d535546  df7b2085  bb595037
Z[ 1] = fa384619  022bdec2  48fd2369  e76eb366
Z[ 2] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
Z[ 3] = c5774560  21f7baa0  2c15cedc  4d53f97f
Z[ 4] = a4f20000  51a9a664  17d90c49  503708ac
Z[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
Z[ 6] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
Z[ 7] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
Z[ 8] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
Z[ 9] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
Z[10] = 39173124  264d02e4  c4bec914  d1071211
```

```
Z[11] = 3a89baa0  de094560  d3eb3124  b2ad0681
Z[12] = 5b0e0000  ae57599c  e827f3b7  afc9f754
Z[13] = b5910456  4ec5d6cf  d107de09  526205c8
Z[14] = fa383124  1383264d  4c9a2594  15ae3296
Z[15] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
Z[16] = fe2e01d2  949a6b66  d70b28f5  9af96507
Z[17] = a7b75849  29ded622  d3672c99  607a9f86
Z[18] = 3de4c21c  03a4fc5c  bad4452c  16c1e93f
Z[19] = a8a05760  5760a8a0  3de4c21c  0831f7cf
Z[20] = 00000000  70dc8f24  f0870f79  f5140aec
Z[21] = 0576fa8a  cc1f33e1  d5392ac7  0748f8b8
Z[22] = 3de4c21c  303dcfc3  2f54d0ac  3fb6c04a
Z[23] = 091af6e6  6a7d9583  b9eb4615  ece3131d
Z[24] = 5beda413  9e9d6163  28f5d70b  5677a989
Z[25] = 0748f8b8  fd4502bb  a4135bed  1ef2e10e
Z[26] = 47e7b819  303dcfc3  b55e4aa2  c4d73b29
Z[27] = 49b9b647  d5392ac7  c87b3785  9e9d6163
Z[28] = 72ae8d52  992766d9  e1f71e09  9af96507
Z[29] = a2415dbf  63359ccb  c4d73b29  67c2983e
Z[30] = f8b80748  1893e76d  607a9f86  1b4ee4b2
Z[31] = 9af96507  fa8a0576  f6e6091a  624c9db4
```

Expanded Message

```
W[ 0] = a4f20000  51a9a664  17d90c49  503708ac
W[ 1] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
W[ 2] = b7030172  4d535546  df7b2085  bb595037
W[ 3] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
W[ 4] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
W[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
W[ 6] = c5774560  21f7baa0  2c15cedc  4d53f97f
W[ 7] = fa384619  022bdec2  48fd2369  e76eb366
W[ 8] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
W[ 9] = 3a89baa0  de094560  d3eb3124  b2ad0681
W[10] = 5b0e0000  ae57599c  e827f3b7  afc9f754
W[11] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
W[12] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
W[13] = b5910456  4ec5d6cf  d107de09  526205c8
W[14] = 39173124  264d02e4  c4bec914  d1071211
W[15] = fa383124  1383264d  4c9a2594  15ae3296
W[16] = a7b75849  29ded622  d3672c99  607a9f86
W[17] = 3de4c21c  03a4fc5c  bad4452c  16c1e93f
W[18] = 091af6e6  6a7d9583  b9eb4615  ece3131d
W[19] = 00000000  70dc8f24  f0870f79  f5140aec
W[20] = 3de4c21c  303dcfc3  2f54d0ac  3fb6c04a
W[21] = 0576fa8a  cc1f33e1  d5392ac7  0748f8b8
W[22] = fe2e01d2  949a6b66  d70b28f5  9af96507
W[23] = a8a05760  5760a8a0  3de4c21c  0831f7cf
W[24] = f8b80748  1893e76d  607a9f86  1b4ee4b2
```

```
W[25] = 5beda413  9e9d6163  28f5d70b  5677a989
W[26] = 0748f8b8  fd4502bb  a4135bed  1ef2e10e
W[27] = 9af96507  fa8a0576  f6e6091a  624c9db4
W[28] = 49b9b647  d5392ac7  c87b3785  9e9d6163
W[29] = a2415dbf  63359ccb  c4d73b29  67c2983e
W[30] = 72ae8d52  992766d9  e1f71e09  9af96507
W[31] = 47e7b819  303dcfc3  b55e4aa2  c4d73b29
```

Feistel Steps

```
IV :
A[0]=33586e9f  B[0]=de943106  C[0]=22e7b0af  D[0]=f64ae77c
A[1]=12fff033  B[1]=2742e439  C[1]=c862b3a8  D[1]=fa373b76
A[2]=b2d9f64d  B[2]=4fbab5ac  C[2]=33e00cdc  D[2]=7dc1ee5b
A[3]=6f8fea53  B[3]=62b9ff96  C[3]=236b86a6  D[3]=7fb29ce8

IV XOR M :
A[0]=33586e9f  B[0]=de943106  C[0]=22e7b0af  D[0]=f64ae77c
A[1]=12fff033  B[1]=2742e439  C[1]=c862b3a8  D[1]=fa373b76
A[2]=b2d9f64d  B[2]=4fbab5ac  C[2]=33e00cdc  D[2]=7dc1ee5b
A[3]=6f8fea53  B[3]=62b9ff96  C[3]=236b86a6  D[3]=7fb29ce8

Step  0: (r= 3, s=23)
A[0]=69567be3  B[0]=9ac374f9  C[0]=de943106  D[0]=22e7b0af
A[1]=644e86db  B[1]=97ff8198  C[1]=2742e439  D[1]=c862b3a8
A[2]=1ccbfc76  B[2]=96cfb26d  C[2]=4fbab5ac  D[2]=33e00cdc
A[3]=bbe91c37  B[3]=7c7f529b  C[3]=62b9ff96  D[3]=236b86a6

Step  1: (r=23, s=17)
A[0]=1beff4e3  B[0]=f1b4ab3d  C[0]=9ac374f9  D[0]=de943106
A[1]=f8056cec  B[1]=6db22743  C[1]=97ff8198  D[1]=2742e439
A[2]=241d29c2  B[2]=3b0e65fe  C[2]=96cfb26d  D[2]=4fbab5ac
A[3]=fcf933b3  B[3]=1bddf48e  C[3]=7c7f529b  D[3]=62b9ff96

Step  2: (r=17, s=27)
A[0]=f0a1d887  B[0]=e9c637df  C[0]=f1b4ab3d  D[0]=9ac374f9
A[1]=d2a8cf30  B[1]=d9d9f00a  C[1]=6db22743  D[1]=97ff8198
A[2]=e0ea145b  B[2]=5384483a  C[2]=3b0e65fe  D[2]=96cfb26d
A[3]=a37dcde1  B[3]=6767f9f2  C[3]=1bddf48e  D[3]=7c7f529b

Step  3: (r=27, s= 3)
A[0]=a0a1031b  B[0]=3f850ec4  C[0]=e9c637df  D[0]=f1b4ab3d
A[1]=b9f8067f  B[1]=86954679  C[1]=d9d9f00a  D[1]=6db22743
A[2]=79ce4728  B[2]=df0750a2  C[2]=5384483a  D[2]=3b0e65fe
A[3]=1a012469  B[3]=0d1bee6f  C[3]=6767f9f2  D[3]=1bddf48e

Step  4: (r= 3, s=23)
A[0]=bfe7f218  B[0]=050818dd  C[0]=3f850ec4  D[0]=e9c637df
A[1]=688f1454  B[1]=cfc033fd  C[1]=86954679  D[1]=d9d9f00a
```

```
A[2]=ebd7004b  B[2]=ce723943  C[2]=df0750a2  D[2]=5384483a
A[3]=e32e9ef5  B[3]=d0092348  C[3]=0d1bee6f  D[3]=6767f9f2

Step  5: (r=23, s=17)
A[0]=17bc7ec5  B[0]=0c5ff3f9  C[0]=050818dd  D[0]=3f850ec4
A[1]=85669eb4  B[1]=2a34478a  C[1]=cfc033fd  D[1]=86954679
A[2]=1f1ceb32  B[2]=25f5eb80  C[2]=ce723943  D[2]=df0750a2
A[3]=518fa01e  B[3]=7af1974f  C[3]=d0092348  D[3]=0d1bee6f

Step  6: (r=17, s=27)
A[0]=45b9d145  B[0]=fd8a2f78  C[0]=0c5ff3f9  D[0]=050818dd
A[1]=a749b83e  B[1]=3d690acd  C[1]=2a34478a  D[1]=cfc033fd
A[2]=41113373  B[2]=d6643e39  C[2]=25f5eb80  D[2]=ce723943
A[3]=bbbc0a92  B[3]=403ca31f  C[3]=7af1974f  D[3]=d0092348

Step  7: (r=27, s= 3)
A[0]=00eb1d15  B[0]=2a2dce8a  C[0]=fd8a2f78  D[0]=0c5ff3f9
A[1]=a086cabc  B[1]=f53a4dc1  C[1]=3d690acd  D[1]=2a34478a
A[2]=11528d74  B[2]=9a08899b  C[2]=d6643e39  D[2]=25f5eb80
A[3]=86dd1c2a  B[3]=95dde054  C[3]=403ca31f  D[3]=7af1974f

Step  8: (r=28, s=19)
A[0]=f54b9c53  B[0]=500eb1d1  C[0]=2a2dce8a  D[0]=fd8a2f78
A[1]=67dc4326  B[1]=ca086cab  C[1]=f53a4dc1  D[1]=3d690acd
A[2]=41b013b6  B[2]=411528d7  C[2]=9a08899b  D[2]=d6643e39
A[3]=a9cb21b2  B[3]=a86dd1c2  C[3]=95dde054  D[3]=403ca31f

Step  9: (r=19, s=22)
A[0]=5597cf91  B[0]=e29faa5c  C[0]=500eb1d1  D[0]=2a2dce8a
A[1]=26db1183  B[1]=19333ee2  C[1]=ca086cab  D[1]=f53a4dc1
A[2]=0cb6a856  B[2]=9db20d80  C[2]=411528d7  D[2]=9a08899b
A[3]=775ddf5a  B[3]=0d954e59  C[3]=a86dd1c2  D[3]=95dde054

Step 10: (r=22, s= 7)
A[0]=03479b0c  B[0]=e45565f3  C[0]=e29faa5c  D[0]=500eb1d1
A[1]=a92fdb2c  B[1]=60c9b6c4  C[1]=19333ee2  D[1]=ca086cab
A[2]=d6184fda  B[2]=15832daa  C[2]=9db20d80  D[2]=411528d7
A[3]=cf5cf72d  B[3]=d69dd777  C[3]=0d954e59  D[3]=a86dd1c2

Step 11: (r= 7, s=28)
A[0]=a61a3401  B[0]=a3cd8601  C[0]=e45565f3  D[0]=e29faa5c
A[1]=c6f4ea4d  B[1]=97ed9654  C[1]=60c9b6c4  D[1]=19333ee2
A[2]=5fe167b1  B[2]=0c27ed6b  C[2]=15832daa  D[2]=9db20d80
A[3]=af08bc11  B[3]=ae7b96e7  C[3]=d69dd777  D[3]=0d954e59

Step 12: (r=28, s=19)
A[0]=1e93c4d0  B[0]=1a61a340  C[0]=a3cd8601  D[0]=e45565f3
A[1]=cd8892f0  B[1]=dc6f4ea4  C[1]=97ed9654  D[1]=60c9b6c4
A[2]=d9041e8b  B[2]=15fe167b  C[2]=0c27ed6b  D[2]=15832daa
```

```
A[3]=a154b884  B[3]=1af08bc1  C[3]=ae7b96e7  D[3]=d69dd777

Step 13: (r=19, s=22)
A[0]=16cbf21c  B[0]=2680f49e  C[0]=1a61a340  D[0]=a3cd8601
A[1]=e60869ee  B[1]=97866c44  C[1]=dc6f4ea4  D[1]=97ed9654
A[2]=ae01e0e8  B[2]=f45ec820  C[2]=15fe167b  D[2]=0c27ed6b
A[3]=98bb4862  B[3]=c4250aa5  C[3]=1af08bc1  D[3]=ae7b96e7

Step 14: (r=22, s= 7)
A[0]=ebfacfcb  B[0]=8705b2fc  C[0]=2680f49e  D[0]=1a61a340
A[1]=5eae8ec2  B[1]=7bb9821a  C[1]=97866c44  D[1]=dc6f4ea4
A[2]=1e74f5dc  B[2]=3a2b8078  C[2]=f45ec820  D[2]=15fe167b
A[3]=a0df9f88  B[3]=18a62ed2  C[3]=c4250aa5  D[3]=1af08bc1

Step 15: (r= 7, s=28)
A[0]=83090de3  B[0]=fd67e5f5  C[0]=8705b2fc  D[0]=2680f49e
A[1]=3261f628  B[1]=5747612f  C[1]=7bb9821a  D[1]=97866c44
A[2]=e9e13418  B[2]=3a7aee0f  C[2]=3a2b8078  D[2]=f45ec820
A[3]=b58f4adc  B[3]=6fcfc450  C[3]=18a62ed2  D[3]=c4250aa5

Step 16: (r=29, s= 9)
A[0]=9945ef29  B[0]=706121bc  C[0]=fd67e5f5  D[0]=8705b2fc
A[1]=13f72995  B[1]=064c3ec5  C[1]=5747612f  D[1]=7bb9821a
A[2]=d19363c0  B[2]=1d3c2683  C[2]=3a7aee0f  D[2]=3a2b8078
A[3]=a4693969  B[3]=96b1e95b  C[3]=6fcfc450  D[3]=18a62ed2

Step 17: (r= 9, s=15)
A[0]=9dfcefee  B[0]=8bde5332  C[0]=706121bc  D[0]=fd67e5f5
A[1]=9a5a6474  B[1]=ee532a27  C[1]=064c3ec5  D[1]=5747612f
A[2]=286cc263  B[2]=26c781a3  C[2]=1d3c2683  D[2]=3a7aee0f
A[3]=8e93d2ba  B[3]=d272d348  C[3]=96b1e95b  D[3]=6fcfc450

Step 18: (r=15, s= 5)
A[0]=3e3e4eeb  B[0]=77f74efe  C[0]=8bde5332  D[0]=706121bc
A[1]=7b5d79e8  B[1]=323a4d2d  C[1]=ee532a27  D[1]=064c3ec5
A[2]=20b8602e  B[2]=61319436  C[2]=26c781a3  D[2]=1d3c2683
A[3]=3debeb13  B[3]=e95d4749  C[3]=d272d348  D[3]=96b1e95b

Step 19: (r= 5, s=29)
A[0]=dc16f5fa  B[0]=c7c9dd67  C[0]=77f74efe  D[0]=8bde5332
A[1]=c325c58a  B[1]=6baf3d0f  C[1]=323a4d2d  D[1]=ee532a27
A[2]=2e51345b  B[2]=170c05c4  C[2]=61319436  D[2]=26c781a3
A[3]=7a932601  B[3]=bd7d6267  C[3]=e95d4749  D[3]=d272d348

Step 20: (r=29, s= 9)
A[0]=6538fe03  B[0]=5b82debf  C[0]=c7c9dd67  D[0]=77f74efe
A[1]=e658198e  B[1]=5864b8b1  C[1]=6baf3d0f  D[1]=323a4d2d
A[2]=b33203ab  B[2]=65ca268b  C[2]=170c05c4  D[2]=61319436
A[3]=697684d6  B[3]=2f5264c0  C[3]=bd7d6267  D[3]=e95d4749
```

```
Step 21: (r= 9, s=15)
A[0]=440b0047  B[0]=71fc06ca  C[0]=5b82debf  D[0]=c7c9dd67
A[1]=4f4abb2c  B[1]=b0331dcc  C[1]=5864b8b1  D[1]=6baf3d0f
A[2]=504de38c  B[2]=64075766  C[2]=65ca268b  D[2]=170c05c4
A[3]=b66ae674  B[3]=ed09acd2  C[3]=2f5264c0  D[3]=bd7d6267

Step 22: (r=15, s= 5)
A[0]=e202e928  B[0]=8023a205  C[0]=71fc06ca  D[0]=5b82debf
A[1]=88c69f60  B[1]=5d9627a5  C[1]=b0331dcc  D[1]=5864b8b1
A[2]=ccf66aef  B[2]=f1c62826  C[2]=64075766  D[2]=65ca268b
A[3]=55cbaf65  B[3]=733a5b35  C[3]=ed09acd2  D[3]=2f5264c0

Step 23: (r= 5, s=29)
A[0]=b5fea7ae  B[0]=405d251c  C[0]=8023a205  D[0]=71fc06ca
A[1]=47d8ce1f  B[1]=18d3ec11  C[1]=5d9627a5  D[1]=b0331dcc
A[2]=c9e29672  B[2]=9ecd5df9  C[2]=f1c62826  D[2]=64075766
A[3]=d5ef269c  B[3]=b975ecaa  C[3]=733a5b35  D[3]=ed09acd2

Step 24: (r= 4, s=13)
A[0]=a3f0cf56  B[0]=5fea7aeb  C[0]=405d251c  D[0]=8023a205
A[1]=1e47d71e  B[1]=7d8ce1f4  C[1]=18d3ec11  D[1]=5d9627a5
A[2]=255e7975  B[2]=9e29672c  C[2]=9ecd5df9  D[2]=f1c62826
A[3]=600f1ea5  B[3]=5ef269cd  C[3]=b975ecaa  D[3]=733a5b35

Step 25: (r=13, s=10)
A[0]=c9f02d2a  B[0]=19ead47e  C[0]=5fea7aeb  D[0]=405d251c
A[1]=059d2064  B[1]=fae3c3c8  C[1]=7d8ce1f4  D[1]=18d3ec11
A[2]=2f7e4b63  B[2]=cf2ea4ab  C[2]=9e29672c  D[2]=9ecd5df9
A[3]=8e98fa54  B[3]=e3d4ac01  C[3]=5ef269cd  D[3]=b975ecaa

Step 26: (r=10, s=25)
A[0]=e2b87323  B[0]=c0b4ab27  C[0]=19ead47e  D[0]=5fea7aeb
A[1]=324ac21e  B[1]=74819016  C[1]=fae3c3c8  D[1]=7d8ce1f4
A[2]=a045afd2  B[2]=f92d8cbd  C[2]=cf2ea4ab  D[2]=9e29672c
A[3]=440b6215  B[3]=63e9523a  C[3]=e3d4ac01  D[3]=5ef269cd

Step 27: (r=25, s= 4)
A[0]=89cd0ca1  B[0]=47c570e6  C[0]=c0b4ab27  D[0]=19ead47e
A[1]=534c04ed  B[1]=3c649584  C[1]=74819016  D[1]=fae3c3c8
A[2]=6e77e6bc  B[2]=a5408b5f  C[2]=f92d8cbd  D[2]=cf2ea4ab
A[3]=f70de479  B[3]=2a8816c4  C[3]=63e9523a  D[3]=e3d4ac01

Step 28: (r= 4, s=13)
A[0]=1debf073  B[0]=9cd0ca18  C[0]=47c570e6  D[0]=c0b4ab27
A[1]=a140b02b  B[1]=34c04ed5  C[1]=3c649584  D[1]=74819016
A[2]=8a2e7ab9  B[2]=e77e6bc6  C[2]=a5408b5f  D[2]=f92d8cbd
A[3]=a13beb94  B[3]=70de479f  C[3]=2a8816c4  D[3]=63e9523a
```

```
Step 29: (r=13, s=10)
A[0]=5d57f629  B[0]=7e0e63bd  C[0]=9cd0ca18  D[0]=47c570e6
A[1]=ae5cc974  B[1]=16057428  C[1]=34c04ed5  D[1]=3c649584
A[2]=e2d489bd  B[2]=cf573145  C[2]=e77e6bc6  D[2]=a5408b5f
A[3]=96d6976e  B[3]=7d729427  C[3]=70de479f  D[3]=2a8816c4

Step 30: (r=10, s=25)
A[0]=55536879  B[0]=5fd8a575  C[0]=7e0e63bd  D[0]=9cd0ca18
A[1]=01f04606  B[1]=7325d2b9  C[1]=16057428  D[1]=34c04ed5
A[2]=b53ad601  B[2]=5226f78b  C[2]=cf573145  D[2]=e77e6bc6
A[3]=469ba7b0  B[3]=5a5dba5b  C[3]=7d729427  D[3]=70de479f

Step 31: (r=25, s= 4)
A[0]=4498b090  B[0]=f2aaa6d0  C[0]=5fd8a575  D[0]=7e0e63bd
A[1]=e2c48356  B[1]=0c03e08c  C[1]=7325d2b9  D[1]=16057428
A[2]=33e57d67  B[2]=036a75ac  C[2]=5226f78b  D[2]=cf573145
A[3]=4d177045  B[3]=608d374f  C[3]=5a5dba5b  D[3]=7d729427

Feed-Forward Step 32: (r= 4, s=13)
A[0]=c08125f9  B[0]=498b0904  C[0]=f2aaa6d0  D[0]=5fd8a575
A[1]=24f8ddb7  B[1]=2c48356e  C[1]=0c03e08c  D[1]=7325d2b9
A[2]=b0300e20  B[2]=3e57d673  C[2]=036a75ac  D[2]=5226f78b
A[3]=50a630ee  B[3]=d1770454  C[3]=608d374f  D[3]=5a5dba5b

Feed-Forward Step 33: (r=13, s=10)
A[0]=7d1cd363  B[0]=24bf3810  C[0]=498b0904  D[0]=f2aaa6d0
A[1]=f46fbb2a  B[1]=1bb6e49f  C[1]=2c48356e  D[1]=0c03e08c
A[2]=b6b15968  B[2]=01c41606  C[2]=3e57d673  D[2]=036a75ac
A[3]=1cc8eebb  B[3]=c61dca14  C[3]=d1770454  D[3]=608d374f

Feed-Forward Step 34: (r=10, s=25)
A[0]=cbda05b9  B[0]=734d8df4  C[0]=24bf3810  D[0]=498b0904
A[1]=299406e4  B[1]=beecabd1  C[1]=1bb6e49f  D[1]=2c48356e
A[2]=a9cdb025  B[2]=c565a2da  C[2]=01c41606  D[2]=3e57d673
A[3]=517f1ce1  B[3]=23baec73  C[3]=c61dca14  D[3]=d1770454

Feed-Forward Step 35: (r=25, s= 4)
A[0]=36d5e143  B[0]=7397b40b  C[0]=734d8df4  D[0]=24bf3810
A[1]=5db8d756  B[1]=c853280d  C[1]=beecabd1  D[1]=1bb6e49f
A[2]=9e49d510  B[2]=4b539b60  C[2]=c565a2da  D[2]=01c41606
A[3]=f9deaf28  B[3]=c2a2fe39  C[3]=23baec73  D[3]=c61dca14
```

Compression Function Output

```
A[0]=36d5e143  B[0]=7397b40b  C[0]=734d8df4  D[0]=24bf3810
A[1]=5db8d756  B[1]=c853280d  C[1]=beecabd1  D[1]=1bb6e49f
A[2]=9e49d510  B[2]=4b539b60  C[2]=c565a2da  D[2]=01c41606
A[3]=f9deaf28  B[3]=c2a2fe39  C[3]=23baec73  D[3]=c61dca14
```

Hash Function Output

```
43e1d53656d7b85d10d5499e28afdef90bb497730d2853c8609b534b
```

A.1.2 One-block Message

We use the message block `0x00 0x01 0x02` ... as an example.

First block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
```

NTT Output

```
y[  0..  7] =  218   26   85  204   79  131  143   82
y[  8.. 15] =  193  132  188  176  130  214  229  177
y[ 16.. 23] =   43    9  233   73  161  207  236  155
y[ 24.. 31] =  124   92  110  120  191  202  211   82
y[ 32.. 39] =  211  215  163   35    7   33  156  212
y[ 40.. 47] =  135  222  249   69  206   55  208  212
y[ 48.. 55] =   99   87  170   98  133  188   63  177
y[ 56.. 63] =   41   50  150   31   54  204   39  220
y[ 64.. 71] =  224    7   13   81   49  160   87  256
y[ 72.. 79] =   21  231  119  191  182  247   17  196
y[ 80.. 87] =  154   34  227   51  125  130  142  149
y[ 88.. 95] =   82   92  139  202  152   85   17  226
y[ 96..103] =  239   47  252  198   36    9  238  244
y[104..111] =   45  236   16   63  151  237  232    9
y[112..119] =   90   90  227  241  198  200   16  123
y[120..127] =  131    1    6  179  204  175  249  158
```

Intermediate Expanded Message

```
Z[ 0] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
Z[ 1] = a5abd1c0  c577ce23  e0eda439  c630ebc4
Z[ 2] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
Z[ 3] = 427c599c  56b84f7e  d841d04e  3b42dec2
Z[ 4] = e1a6dec2  194bbc12  17d9050f  df7bb703
Z[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
Z[ 6] = 3edf478b  46d2c121  ce23a664  c6302d87
Z[ 7] = 24221da1  1667b2ad  d9b32706  e5431c2f
Z[ 8] = 050fe827  3a890965  b9e72369  ff473edf
Z[ 9] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
```

```
Z[10] = 1892b591  24dbea52  a4395a55  b1f4ace5
Z[11] = 427c3b42  d841aaba  3d6db41f  e9990c49
Z[12] = 21f7f2fe  d55dfc63  06811a04  f69bf245
Z[13] = f0d32085  2d870b90  f18cb366  0681edef
Z[14] = 410a410a  f470ea52  d6cfd55d  58e30b90
Z[15] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
Z[16] = e1f7dc81  0bd54d5d  2c9947e7  4f2f983e
Z[17] = 131dc5c0  6c4fc133  bbbd8c69  0f79e684
Z[18] = a2412723  e4b2ea28  71c5a8a0  9755ece3
Z[19] = 4aa270dc  949a641e  a06fc3ee  0f79d622
Z[20] = ef9ed622  fb73aa72  20c4065f  eeb5a413
Z[21] = 28f590f6  0e90f8b8  9f86d195  e93fd367
Z[22] = 51ea5a1b  e4b2b0d1  ca4d8f24  0e903957
Z[23] = 8d522551  05769e9d  cfc33126  f8b8237f
Z[24] = 065f17aa  49b9cfc3  a7b78d52  ff174aa2
Z[25] = e8568e3b  c3eeb647  f6e6d8dd  c87bb730
Z[26] = 1ef20831  2e6b4271  8c69d27e  9db4a32a
Z[27] = 53bc53bc  cdf16d38  4d5dcdf1  e3c94aa2
Z[28] = 2ac7d9c6  ca4d1fdb  08311e09  f42bd70b
Z[29] = ece3e025  39573ecd  edcc320f  0831d70b
Z[30] = 51ea4f2f  f1705932  cc1fc133  6ff3b730
Z[31] = 00e92d82  b9021c37  b55ecfc3  a5e5de53
```

Expanded Message

```
W[ 0] = e1a6dec2  194bbc12  17d9050f  df7bb703
W[ 1] = 3edf478b  46d2c121  ce23a664  c6302d87
W[ 2] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
W[ 3] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
W[ 4] = 24221da1  1667b2ad  d9b32706  e5431c2f
W[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
W[ 6] = 427c599c  56b84f7e  d841d04e  3b42dec2
W[ 7] = a5abd1c0  c577ce23  e0eda439  c630ebc4
W[ 8] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
W[ 9] = 427c3b42  d841aaba  3d6db41f  e9990c49
W[10] = 21f7f2fe  d55dfc63  06811a04  f69bf245
W[11] = 050fe827  3a890965  b9e72369  ff473edf
W[12] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
W[13] = f0d32085  2d870b90  f18cb366  0681edef
W[14] = 1892b591  24dbea52  a4395a55  b1f4ace5
W[15] = 410a410a  f470ea52  d6cfd55d  58e30b90
W[16] = 131dc5c0  6c4fc133  bbbd8c69  0f79e684
W[17] = a2412723  e4b2ea28  71c5a8a0  9755ece3
W[18] = 8d522551  05769e9d  cfc33126  f8b8237f
W[19] = ef9ed622  fb73aa72  20c4065f  eeb5a413
W[20] = 51ea5a1b  e4b2b0d1  ca4d8f24  0e903957
W[21] = 28f590f6  0e90f8b8  9f86d195  e93fd367
W[22] = e1f7dc81  0bd54d5d  2c9947e7  4f2f983e
W[23] = 4aa270dc  949a641e  a06fc3ee  0f79d622
```

```
W[24] = 51ea4f2f  f1705932  cc1fc133  6ff3b730
W[25] = 065f17aa  49b9cfc3  a7b78d52  ff174aa2
W[26] = e8568e3b  c3eeb647  f6e6d8dd  c87bb730
W[27] = 00e92d82  b9021c37  b55ecfc3  a5e5de53
W[28] = 53bc53bc  cdf16d38  4d5dcdf1  e3c94aa2
W[29] = ece3e025  39573ecd  edcc320f  0831d70b
W[30] = 2ac7d9c6  ca4d1fdb  08311e09  f42bd70b
W[31] = 1ef20831  2e6b4271  8c69d27e  9db4a32a
```

Feistel Steps

```
IV :
A[0]=33586e9f  B[0]=de943106  C[0]=22e7b0af  D[0]=f64ae77c
A[1]=12fff033  B[1]=2742e439  C[1]=c862b3a8  D[1]=fa373b76
A[2]=b2d9f64d  B[2]=4fbab5ac  C[2]=33e00cdc  D[2]=7dc1ee5b
A[3]=6f8fea53  B[3]=62b9ff96  C[3]=236b86a6  D[3]=7fb29ce8

IV XOR M :
A[0]=305a6f9f  B[0]=cd862016  C[0]=01c5918f  D[0]=c578d64c
A[1]=15f9f537  B[1]=3054f12d  C[1]=ef44968c  D[1]=cd010e42
A[2]=b9d3ff45  B[2]=54a0acb4  C[2]=18ca25f4  D[2]=46fbd763
A[3]=6081e75f  B[3]=7da7e28a  C[3]=0c45ab8a  D[3]=408ca1d4

Step  0: (r= 3, s=23)
A[0]=4223fd6a  B[0]=82d37cf9  C[0]=cd862016  D[0]=01c5918f
A[1]=83c3cdd8  B[1]=afcfa9b8  C[1]=3054f12d  D[1]=ef44968c
A[2]=9746e9bf  B[2]=ce9ffa2d  C[2]=54a0acb4  D[2]=18ca25f4
A[3]=7f66614e  B[3]=040f3afb  C[3]=7da7e28a  D[3]=0c45ab8a

Step  1: (r=23, s=17)
A[0]=8af943cc  B[0]=b52111fe  C[0]=82d37cf9  D[0]=cd862016
A[1]=ca15870e  B[1]=ec41e1e6  C[1]=afcfa9b8  D[1]=3054f12d
A[2]=262c6d27  B[2]=dfcba374  C[2]=ce9ffa2d  D[2]=54a0acb4
A[3]=e3f98fe0  B[3]=a73fb330  C[3]=040f3afb  D[3]=7da7e28a

Step  2: (r=17, s=27)
A[0]=42c56a02  B[0]=879915f2  C[0]=b52111fe  D[0]=82d37cf9
A[1]=620ceb1a  B[1]=0e1d942b  C[1]=ec41e1e6  D[1]=afcfa9b8
A[2]=cc5f08f2  B[2]=da4e4c58  C[2]=dfcba374  D[2]=ce9ffa2d
A[3]=a29a680d  B[3]=1fc1c7f3  C[3]=a73fb330  D[3]=040f3afb

Step  3: (r=27, s= 3)
A[0]=dabdd7aa  B[0]=12162b50  C[0]=879915f2  D[0]=b52111fe
A[1]=a90ef5c3  B[1]=d3106758  C[1]=0e1d942b  D[1]=ec41e1e6
A[2]=9f7fd44c  B[2]=9662f847  C[2]=da4e4c58  D[2]=dfcba374
A[3]=a662f045  B[3]=6d14d340  C[3]=1fc1c7f3  D[3]=a73fb330

Step  4: (r= 3, s=23)
A[0]=c4b49287  B[0]=d5eebd56  C[0]=12162b50  D[0]=879915f2
```

```
A[1]=225e6571  B[1]=4877ae1d  C[1]=d3106758  D[1]=0e1d942b
A[2]=391ab429  B[2]=fbfea264  C[2]=9662f847  D[2]=da4e4c58
A[3]=98d58fee  B[3]=3317822d  C[3]=6d14d340  D[3]=1fc1c7f3

Step  5: (r=23, s=17)
A[0]=e988f0d1  B[0]=43e25a49  C[0]=d5eebd56  D[0]=12162b50
A[1]=001591fd  B[1]=b8912f32  C[1]=4877ae1d  D[1]=d3106758
A[2]=6856aa43  B[2]=149c8d5a  C[2]=fbfea264  D[2]=9662f847
A[3]=93cecaef  B[3]=f74c6ac7  C[3]=3317822d  D[3]=6d14d340

Step  6: (r=17, s=27)
A[0]=0cadec14  B[0]=e1a3d311  C[0]=43e25a49  D[0]=d5eebd56
A[1]=7b32c641  B[1]=23fa002b  C[1]=b8912f32  D[1]=4877ae1d
A[2]=551b4333  B[2]=5486d0ad  C[2]=149c8d5a  D[2]=fbfea264
A[3]=df640494  B[3]=95df279d  C[3]=f74c6ac7  D[3]=3317822d

Step  7: (r=27, s= 3)
A[0]=849c2356  B[0]=a0656f60  C[0]=e1a3d311  D[0]=43e25a49
A[1]=f407333e  B[1]=0bd99632  C[1]=23fa002b  D[1]=b8912f32
A[2]=2cbdae21  B[2]=9aa8da19  C[2]=5486d0ad  D[2]=149c8d5a
A[3]=907e3a68  B[3]=a6fb2024  C[3]=95df279d  D[3]=f74c6ac7

Step  8: (r=28, s=19)
A[0]=1ce911c5  B[0]=6849c235  C[0]=a0656f60  D[0]=e1a3d311
A[1]=40a7fc44  B[1]=ef407333  C[1]=0bd99632  D[1]=23fa002b
A[2]=fc120365  B[2]=12cbdae2  C[2]=9aa8da19  D[2]=5486d0ad
A[3]=bdeb7021  B[3]=8907e3a6  C[3]=a6fb2024  D[3]=95df279d

Step  9: (r=19, s=22)
A[0]=0055209e  B[0]=8e28e748  C[0]=6849c235  D[0]=a0656f60
A[1]=d3facc4f  B[1]=e222053f  C[1]=ef407333  D[1]=0bd99632
A[2]=52371732  B[2]=1b2fe090  C[2]=12cbdae2  D[2]=9aa8da19
A[3]=1db28375  B[3]=810def5b  C[3]=8907e3a6  D[3]=a6fb2024

Step 10: (r=22, s= 7)
A[0]=ffb6d15a  B[0]=27801548  C[0]=8e28e748  D[0]=6849c235
A[1]=8a2c5707  B[1]=13f4feb3  C[1]=e222053f  D[1]=ef407333
A[2]=345e8c22  B[2]=cc948dc5  C[2]=1b2fe090  D[2]=12cbdae2
A[3]=62701cc2  B[3]=dd476ca0  C[3]=810def5b  D[3]=8907e3a6

Step 11: (r= 7, s=28)
A[0]=815c7f4b  B[0]=db68ad7f  C[0]=27801548  D[0]=8e28e748
A[1]=68050e47  B[1]=162b83c5  C[1]=13f4feb3  D[1]=e222053f
A[2]=d3ea1272  B[2]=2f46111a  C[2]=cc948dc5  D[2]=1b2fe090
A[3]=c0027ea0  B[3]=380e6131  C[3]=dd476ca0  D[3]=810def5b

Step 12: (r=28, s=19)
A[0]=1488461d  B[0]=b815c7f4  C[0]=db68ad7f  D[0]=27801548
A[1]=0843eca3  B[1]=768050e4  C[1]=162b83c5  D[1]=13f4feb3
```

```
A[2]=e97f45cf  B[2]=2d3ea127  C[2]=2f46111a  D[2]=cc948dc5
A[3]=6f600922  B[3]=0c0027ea  C[3]=380e6131  D[3]=dd476ca0

Step 13: (r=19, s=22)
A[0]=812b62f9  B[0]=30e8a442  C[0]=b815c7f4  D[0]=db68ad7f
A[1]=13295af2  B[1]=6518421f  C[1]=768050e4  D[1]=162b83c5
A[2]=bfa38c12  B[2]=2e7f4bfa  C[2]=2d3ea127  D[2]=2f46111a
A[3]=515c347d  B[3]=49137b00  C[3]=0c0027ea  D[3]=380e6131

Step 14: (r=22, s= 7)
A[0]=31f9575f  B[0]=be604ad8  C[0]=30e8a442  D[0]=b815c7f4
A[1]=0c906fbc  B[1]=bc84ca56  C[1]=6518421f  D[1]=768050e4
A[2]=1bff1ad7  B[2]=04afe8e3  C[2]=2e7f4bfa  D[2]=2d3ea127
A[3]=480309f1  B[3]=1f54570d  C[3]=49137b00  D[3]=0c0027ea

Step 15: (r= 7, s=28)
A[0]=cad862fb  B[0]=fcabaf98  C[0]=be604ad8  D[0]=30e8a442
A[1]=4623c7ed  B[1]=4837de06  C[1]=bc84ca56  D[1]=6518421f
A[2]=72b5d4bb  B[2]=ff8d6b8d  C[2]=04afe8e3  D[2]=2e7f4bfa
A[3]=ba6cd474  B[3]=0184f8a4  C[3]=1f54570d  D[3]=49137b00

Step 16: (r=29, s= 9)
A[0]=cb7fef18  B[0]=795b0c5f  C[0]=fcabaf98  D[0]=be604ad8
A[1]=b6f06c22  B[1]=a8c478fd  C[1]=4837de06  D[1]=bc84ca56
A[2]=11dd6520  B[2]=6e56ba97  C[2]=ff8d6b8d  D[2]=04afe8e3
A[3]=ed2ddbb8  B[3]=974d9a8e  C[3]=0184f8a4  D[3]=1f54570d

Step 17: (r= 9, s=15)
A[0]=9b016118  B[0]=ffde3196  C[0]=795b0c5f  D[0]=fcabaf98
A[1]=921b8522  B[1]=e0d8456d  C[1]=a8c478fd  D[1]=4837de06
A[2]=bee077d1  B[2]=baca4023  C[2]=6e56ba97  D[2]=ff8d6b8d
A[3]=ff1c4fb1  B[3]=5bb771da  C[3]=974d9a8e  D[3]=0184f8a4

Step 18: (r=15, s= 5)
A[0]=6d91911d  B[0]=b08c4d80  C[0]=ffde3196  D[0]=795b0c5f
A[1]=81eba19e  B[1]=c291490d  C[1]=e0d8456d  D[1]=a8c478fd
A[2]=6cc596e7  B[2]=3be8df70  C[2]=baca4023  D[2]=6e56ba97
A[3]=ee46979a  B[3]=27d8ff8e  C[3]=5bb771da  D[3]=974d9a8e

Step 19: (r= 5, s=29)
A[0]=fc2bdd6d  B[0]=b23223ad  C[0]=b08c4d80  D[0]=ffde3196
A[1]=596c2078  B[1]=3d7433d0  C[1]=c291490d  D[1]=e0d8456d
A[2]=7b6ed697  B[2]=98b2dced  C[2]=3be8df70  D[2]=baca4023
A[3]=b532da9d  B[3]=c8d2f35d  C[3]=27d8ff8e  D[3]=5bb771da

Step 20: (r=29, s= 9)
A[0]=9c591756  B[0]=bf857bad  C[0]=b23223ad  D[0]=b08c4d80
A[1]=ed9d070f  B[1]=0b2d840f  C[1]=3d7433d0  D[1]=c291490d
A[2]=1089fd91  B[2]=ef6ddad2  C[2]=98b2dced  D[2]=3be8df70
```

```
A[3]=f4d317cd  B[3]=b6a65b53  C[3]=c8d2f35d  D[3]=27d8ff8e

Step 21: (r= 9, s=15)
A[0]=c31feba4  B[0]=b22ead38  C[0]=bf857bad  D[0]=b23223ad
A[1]=56992c67  B[1]=3a0e1fdb  C[1]=0b2d840f  D[1]=3d7433d0
A[2]=6d1ad5f5  B[2]=13fb2221  C[2]=ef6ddad2  D[2]=98b2dced
A[3]=a7242516  B[3]=a62f9be9  C[3]=b6a65b53  D[3]=c8d2f35d

Step 22: (r=15, s= 5)
A[0]=523831d5  B[0]=f5d2618f  C[0]=b22ead38  D[0]=bf857bad
A[1]=7d5d031e  B[1]=9633ab4c  C[1]=3a0e1fdb  D[1]=0b2d840f
A[2]=8ed15a35  B[2]=6afab68d  C[2]=13fb2221  D[2]=ef6ddad2
A[3]=5b488923  B[3]=128b5392  C[3]=a62f9be9  D[3]=b6a65b53

Step 23: (r= 5, s=29)
A[0]=489d662f  B[0]=47063aaa  C[0]=f5d2618f  D[0]=b22ead38
A[1]=55e82522  B[1]=aba063cf  C[1]=9633ab4c  D[1]=3a0e1fdb
A[2]=5efb7deb  B[2]=da2b46b1  C[2]=6afab68d  D[2]=13fb2221
A[3]=620bb44d  B[3]=6911246b  C[3]=128b5392  D[3]=a62f9be9

Step 24: (r= 4, s=13)
A[0]=42849150  B[0]=89d662f4  C[0]=47063aaa  D[0]=f5d2618f
A[1]=ce61d8da  B[1]=5e825225  C[1]=aba063cf  D[1]=9633ab4c
A[2]=f5fa701e  B[2]=efb7deb5  C[2]=da2b46b1  D[2]=6afab68d
A[3]=87166f89  B[3]=20bb44d6  C[3]=6911246b  D[3]=128b5392

Step 25: (r=13, s=10)
A[0]=2c94aac5  B[0]=922a0850  C[0]=89d662f4  D[0]=47063aaa
A[1]=85a9821f  B[1]=3b1b59cc  C[1]=5e825225  D[1]=aba063cf
A[2]=28945859  B[2]=4e03debf  C[2]=efb7deb5  D[2]=da2b46b1
A[3]=12a7b3b2  B[3]=cdf130e2  C[3]=20bb44d6  D[3]=6911246b

Step 26: (r=10, s=25)
A[0]=4a30066c  B[0]=52ab14b2  C[0]=922a0850  D[0]=89d662f4
A[1]=d6f69976  B[1]=a6087e16  C[1]=3b1b59cc  D[1]=5e825225
A[2]=3d48ea12  B[2]=516164a2  C[2]=4e03debf  D[2]=efb7deb5
A[3]=554fa153  B[3]=9ecec84a  C[3]=cdf130e2  D[3]=20bb44d6

Step 27: (r=25, s= 4)
A[0]=bc47b797  B[0]=d894600c  C[0]=52ab14b2  D[0]=922a0850
A[1]=4170cfb8  B[1]=edaded32  C[1]=a6087e16  D[1]=3b1b59cc
A[2]=2c4cd1c1  B[2]=247a91d4  C[2]=516164a2  D[2]=4e03debf
A[3]=5e75d28a  B[3]=a6aa9f42  C[3]=9ecec84a  D[3]=cdf130e2

Step 28: (r= 4, s=13)
A[0]=76e173df  B[0]=c47b797b  C[0]=d894600c  D[0]=52ab14b2
A[1]=9e24066b  B[1]=170cfb84  C[1]=edaded32  D[1]=a6087e16
A[2]=14499174  B[2]=c4cd1c12  C[2]=247a91d4  D[2]=516164a2
A[3]=41c6c599  B[3]=e75d28a5  C[3]=a6aa9f42  D[3]=9ecec84a
```

```
Step 29: (r=13, s=10)
A[0]=da4c008a  B[0]=2e7beedc  C[0]=c47b797b  D[0]=d894600c
A[1]=64de9883  B[1]=80cd73c4  C[1]=170cfb84  D[1]=edaded32
A[2]=5d6d88d1  B[2]=322e8289  C[2]=c4cd1c12  D[2]=247a91d4
A[3]=6b2f4917  B[3]=d8b32838  C[3]=e75d28a5  D[3]=a6aa9f42

Step 30: (r=10, s=25)
A[0]=d405bcd8  B[0]=30022b69  C[0]=2e7beedc  D[0]=c47b797b
A[1]=537bbb7a  B[1]=7a620d93  C[1]=80cd73c4  D[1]=170cfb84
A[2]=9a26901c  B[2]=b6234575  C[2]=322e8289  D[2]=c4cd1c12
A[3]=bb2f70b2  B[3]=bd245dac  C[3]=d8b32838  D[3]=e75d28a5

Step 31: (r=25, s= 4)
A[0]=b0475561  B[0]=b1a80b79  C[0]=30022b69  D[0]=2e7beedc
A[1]=e3adfb5a  B[1]=f4a6f776  C[1]=7a620d93  D[1]=80cd73c4
A[2]=e77ef649  B[2]=39344d20  C[2]=b6234575  D[2]=322e8289
A[3]=d83b3fe9  B[3]=65765ee1  C[3]=bd245dac  D[3]=d8b32838

Feed-Forward Step 32: (r= 4, s=13)
A[0]=14d080d7  B[0]=0475561b  C[0]=b1a80b79  D[0]=30022b69
A[1]=0368b634  B[1]=3adfb5ae  C[1]=f4a6f776  D[1]=7a620d93
A[2]=f2a0f875  B[2]=77ef649e  C[2]=39344d20  D[2]=b6234575
A[3]=32a36bca  B[3]=83b3fe9d  C[3]=65765ee1  D[3]=bd245dac

Feed-Forward Step 33: (r=13, s=10)
A[0]=50652b3d  B[0]=101ae29a  C[0]=0475561b  D[0]=b1a80b79
A[1]=dfb7acfb  B[1]=16c6806d  C[1]=3adfb5ae  D[1]=f4a6f776
A[2]=b6fa1c5a  B[2]=1f0ebe54  C[2]=77ef649e  D[2]=39344d20
A[3]=767e6bf3  B[3]=6d794654  C[3]=83b3fe9d  D[3]=65765ee1

Feed-Forward Step 34: (r=10, s=25)
A[0]=6e42ab3f  B[0]=94acf541  C[0]=101ae29a  D[0]=0475561b
A[1]=11977e52  B[1]=deb3ef7e  C[1]=16c6806d  D[1]=3adfb5ae
A[2]=36353cee  B[2]=e8716adb  C[2]=1f0ebe54  D[2]=77ef649e
A[3]=a591a6f5  B[3]=f9afcdd9  C[3]=6d794654  D[3]=83b3fe9d

Feed-Forward Step 35: (r=25, s= 4)
A[0]=d8dd14cd  B[0]=7edc8556  C[0]=94acf541  D[0]=101ae29a
A[1]=9b1a64ad  B[1]=a4232efc  C[1]=deb3ef7e  D[1]=16c6806d
A[2]=92f30c2d  B[2]=dc6c6a79  C[2]=e8716adb  D[2]=1f0ebe54
A[3]=53e28ac4  B[3]=eb4b234d  C[3]=f9afcdd9  D[3]=6d794654
```

Compression Function Output

```
A[0]=d8dd14cd  B[0]=7edc8556  C[0]=94acf541  D[0]=101ae29a
A[1]=9b1a64ad  B[1]=a4232efc  C[1]=deb3ef7e  D[1]=16c6806d
A[2]=92f30c2d  B[2]=dc6c6a79  C[2]=e8716adb  D[2]=1f0ebe54
A[3]=53e28ac4  B[3]=eb4b234d  C[3]=f9afcdd9  D[3]=6d794654
```

Final block

```
M[  0..  7] = 00 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    4  177  210   45  165  187  234   40
y[  8.. 15] =  101   34  138  136   32   51  140  236
y[ 16.. 23] =  197    5  107  213   42  239  210   91
y[ 24.. 31] =  112   87  126   65  121  118  204  159
y[ 32.. 39] =   32  210   63  149  138  147  181  215
y[ 40.. 47] =   58    4  174  220   32   36   73   94
y[ 48.. 55] =   60   67  181  117  175   93   92  129
y[ 56.. 63] =  246  229   94   37   17  151   88  210
y[ 64.. 71] =  253   80   47  212   92   70   23  217
y[ 72.. 79] =  156  223  119  121  225  206  117   21
y[ 80.. 87] =   60  252  150   44  215   18   47  166
y[ 88.. 95] =  145  170  131  192  136  139   53   98
y[ 96..103] =  225   47  194  108  119  110   76   42
y[104..111] =  199  253   83   37  225  221  184  163
y[112..119] =  197  190   76  140   82  164  165  128
y[120..127] =   11   28  163  220  240  106  169   47
```

Intermediate Expanded Message

```
Z[ 0] = c63002e4  2085de09  cd6abd84  1ce8ef61
Z[ 1] = 189248fd  a88faa01  24db1720  f0d3ab73
Z[ 2] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
Z[ 3] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
Z[ 4] = de091720  b1f42d87  b082aa01  e1a6c914
Z[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
Z[ 6] = 306b2b5c  548dc914  4335c4be  a380427c
Z[ 7] = ebc4f80d  1abd43ee  b3660c49  de093f98
Z[ 8] = 39d0fd1c  df7b21f7  3296427c  e318109f
Z[ 9] = e76eb703  577155ff  db25e8e0  0f2d548d
Z[10] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
Z[11] = c121af10  d107a4f2  aabaa88f  46d2264d
Z[12] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
Z[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
Z[14] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
Z[15] = 143c07f3  e543bc12  4c9af3b7  21f7c068
Z[16] = fc5c03a4  2ac7d539  53bcac44  14efeb11
Z[17] = a4135bed  6c4f93b1  e2e01d20  6a7d9583
```

```
Z[18] = 369cc964  9e9d6163  d9c6263a  2ac7d539
Z[19] = 9a1065f0  8d5272ae  91df6e21  303dcfc3
Z[20] = e2e01d20  c6a93957  6c4f93b1  452cbad4
Z[21] = cb3634ca  4b8bb475  e2e01d20  bd8f4271
Z[22] = c964369c  452cbad4  4aa2b55e  ac4453bc
Z[23] = 0a03f5fd  aa72558e  f0870f79  afe85018
Z[24] = 48d0b730  d70b28f5  3fb6c04a  db982468
Z[25] = e10e1ef2  6e2191df  d1952e6b  131dece3
Z[26] = fb73048d  280cd7f4  1062ef9e  ad2d52d3
Z[27] = b0d14f2f  c4d73b29  949a6b66  5932a6ce
Z[28] = 2ac7d539  624c9db4  641e9be2  263ad9c6
Z[29] = fc5c03a4  21adde53  df3c20c4  aa72558e
Z[30] = c3053cfb  95836a7d  ab5b54a5  74808b80
Z[31] = 197ce684  de5321ad  607a9f86  2ac7d539
```

Expanded Message

```
W[ 0] = de091720  b1f42d87  b082aa01  e1a6c914
W[ 1] = 306b2b5c  548dc914  4335c4be  a380427c
W[ 2] = c63002e4  2085de09  cd6abd84  1ce8ef61
W[ 3] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
W[ 4] = ebc4f80d  1abd43ee  b3660c49  de093f98
W[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
W[ 6] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
W[ 7] = 189248fd  a88faa01  24db1720  f0d3ab73
W[ 8] = 143c07f3  e543bc12  4c9af3b7  21f7c068
W[ 9] = c121af10  d107a4f2  aabaa88f  46d2264d
W[10] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
W[11] = 39d0fd1c  df7b21f7  3296427c  e318109f
W[12] = e76eb703  577155ff  db25e8e0  0f2d548d
W[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
W[14] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
W[15] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
W[16] = a4135bed  6c4f93b1  e2e01d20  6a7d9583
W[17] = 369cc964  9e9d6163  d9c6263a  2ac7d539
W[18] = 0a03f5fd  aa72558e  f0870f79  afe85018
W[19] = e2e01d20  c6a93957  6c4f93b1  452cbad4
W[20] = c964369c  452cbad4  4aa2b55e  ac4453bc
W[21] = cb3634ca  4b8bb475  e2e01d20  bd8f4271
W[22] = fc5c03a4  2ac7d539  53bcac44  14efeb11
W[23] = 9a1065f0  8d5272ae  91df6e21  303dcfc3
W[24] = c3053cfb  95836a7d  ab5b54a5  74808b80
W[25] = 48d0b730  d70b28f5  3fb6c04a  db982468
W[26] = e10e1ef2  6e2191df  d1952e6b  131dece3
W[27] = 197ce684  de5321ad  607a9f86  2ac7d539
W[28] = b0d14f2f  c4d73b29  949a6b66  5932a6ce
W[29] = fc5c03a4  21adde53  df3c20c4  aa72558e
W[30] = 2ac7d539  624c9db4  641e9be2  263ad9c6
W[31] = fb73048d  280cd7f4  1062ef9e  ad2d52d3
```

Feistel Steps

```
IV :
A[0]=d8dd14cd  B[0]=7edc8556  C[0]=94acf541  D[0]=101ae29a
A[1]=9b1a64ad  B[1]=a4232efc  C[1]=deb3ef7e  D[1]=16c6806d
A[2]=92f30c2d  B[2]=dc6c6a79  C[2]=e8716adb  D[2]=1f0ebe54
A[3]=53e28ac4  B[3]=eb4b234d  C[3]=f9afcdd9  D[3]=6d794654

IV XOR M :
A[0]=d8dd16cd  B[0]=7edc8556  C[0]=94acf541  D[0]=101ae29a
A[1]=9b1a64ad  B[1]=a4232efc  C[1]=deb3ef7e  D[1]=16c6806d
A[2]=92f30c2d  B[2]=dc6c6a79  C[2]=e8716adb  D[2]=1f0ebe54
A[3]=53e28ac4  B[3]=eb4b234d  C[3]=f9afcdd9  D[3]=6d794654

Step  0: (r= 3, s=23)
A[0]=57f8b5db  B[0]=c6e8b66e  C[0]=7edc8556  D[0]=94acf541
A[1]=c02f659c  B[1]=d8d3256c  C[1]=a4232efc  D[1]=deb3ef7e
A[2]=47784f0b  B[2]=9798616c  C[2]=dc6c6a79  D[2]=e8716adb
A[3]=fa359917  B[3]=9f145622  C[3]=eb4b234d  D[3]=f9afcdd9

Step  1: (r=23, s=17)
A[0]=2f7a2430  B[0]=edabfc5a  C[0]=c6e8b66e  D[0]=7edc8556
A[1]=5bf94955  B[1]=ce6017b2  C[1]=d8d3256c  D[1]=a4232efc
A[2]=0fcf91e1  B[2]=85a3bc27  C[2]=9798616c  D[2]=dc6c6a79
A[3]=539e88ce  B[3]=8bfd1acc  C[3]=9f145622  D[3]=eb4b234d

Step  2: (r=17, s=27)
A[0]=d3326131  B[0]=48605ef4  C[0]=edabfc5a  D[0]=c6e8b66e
A[1]=103a7930  B[1]=92aab7f2  C[1]=ce6017b2  D[1]=d8d3256c
A[2]=e4a610b3  B[2]=23c21f9f  C[2]=85a3bc27  D[2]=9798616c
A[3]=1d1ee280  B[3]=119ca73d  C[3]=8bfd1acc  D[3]=9f145622

Step  3: (r=27, s= 3)
A[0]=3a05102a  B[0]=8e999309  C[0]=48605ef4  D[0]=edabfc5a
A[1]=4a26e695  B[1]=8081d3c9  C[1]=92aab7f2  D[1]=ce6017b2
A[2]=61bada01  B[2]=9f253085  C[2]=23c21f9f  D[2]=85a3bc27
A[3]=45d4a440  B[3]=00e8f714  C[3]=119ca73d  D[3]=8bfd1acc

Step  4: (r= 3, s=23)
A[0]=55c8890e  B[0]=d0288151  C[0]=8e999309  D[0]=48605ef4
A[1]=e75b022b  B[1]=513734aa  C[1]=8081d3c9  D[1]=92aab7f2
A[2]=4ad6d742  B[2]=0dd6d00b  C[2]=9f253085  D[2]=23c21f9f
A[3]=0d6d262a  B[3]=2ea52202  C[3]=00e8f714  D[3]=119ca73d

Step  5: (r=23, s=17)
A[0]=28d4f62d  B[0]=872ae444  C[0]=d0288151  D[0]=8e999309
A[1]=be69dd6e  B[1]=15f3ad81  C[1]=513734aa  D[1]=8081d3c9
A[2]=237848bb  B[2]=a1256b6b  C[2]=0dd6d00b  D[2]=9f253085
A[3]=8b2ba934  B[3]=1506b693  C[3]=2ea52202  D[3]=00e8f714
```

```
Step  6: (r=17, s=27)
A[0]=ad4a8b14  B[0]=ec5a51a9  C[0]=872ae444  D[0]=d0288151
A[1]=fa81c90d  B[1]=badd7cd3  C[1]=15f3ad81  D[1]=513734aa
A[2]=5b1814d8  B[2]=917646f0  C[2]=a1256b6b  D[2]=0dd6d00b
A[3]=5fc04286  B[3]=52691657  C[3]=1506b693  D[3]=2ea52202

Step  7: (r=27, s= 3)
A[0]=73051b3a  B[0]=a56a5458  C[0]=ec5a51a9  D[0]=872ae444
A[1]=d7c46379  B[1]=6fd40e48  C[1]=badd7cd3  D[1]=15f3ad81
A[2]=c49bc576  B[2]=c2d8c0a6  C[2]=917646f0  D[2]=a1256b6b
A[3]=259b2eab  B[3]=32fe0214  C[3]=52691657  D[3]=1506b693

Step  8: (r=28, s=19)
A[0]=98dbf8f3  B[0]=a73051b3  C[0]=a56a5458  D[0]=ec5a51a9
A[1]=af3514fb  B[1]=9d7c4637  C[1]=6fd40e48  D[1]=badd7cd3
A[2]=abc24420  B[2]=6c49bc57  C[2]=c2d8c0a6  D[2]=917646f0
A[3]=f1ada177  B[3]=b259b2ea  C[3]=32fe0214  D[3]=52691657

Step  9: (r=19, s=22)
A[0]=04f224bd  B[0]=c79cc6df  C[0]=a73051b3  D[0]=a56a5458
A[1]=c5b33d2a  B[1]=a7dd79a8  C[1]=9d7c4637  D[1]=6fd40e48
A[2]=0d28afca  B[2]=21055e12  C[2]=6c49bc57  D[2]=c2d8c0a6
A[3]=e29843c9  B[3]=0bbf8d6d  C[3]=b259b2ea  D[3]=32fe0214

Step 10: (r=22, s= 7)
A[0]=6bccb5e2  B[0]=2f413c89  C[0]=c79cc6df  D[0]=a73051b3
A[1]=d1a6a53d  B[1]=4ab16ccf  C[1]=a7dd79a8  D[1]=9d7c4637
A[2]=fb5b9ac2  B[2]=f2834a2b  C[2]=21055e12  D[2]=6c49bc57
A[3]=63a6a281  B[3]=f278a610  C[3]=0bbf8d6d  D[3]=b259b2ea

Step 11: (r= 7, s=28)
A[0]=9c565d07  B[0]=e65af135  C[0]=2f413c89  D[0]=c79cc6df
A[1]=6c0c6fc8  B[1]=d3529ee8  C[1]=4ab16ccf  D[1]=a7dd79a8
A[2]=2c6113b6  B[2]=adcd617d  C[2]=f2834a2b  D[2]=21055e12
A[3]=4655a864  B[3]=d35140b1  C[3]=f278a610  D[3]=0bbf8d6d

Step 12: (r=28, s=19)
A[0]=5dfbb1eb  B[0]=79c565d0  C[0]=e65af135  D[0]=2f413c89
A[1]=6d3fb0c9  B[1]=86c0c6fc  C[1]=d3529ee8  D[1]=4ab16ccf
A[2]=95f2a1ea  B[2]=62c6113b  C[2]=adcd617d  D[2]=f2834a2b
A[3]=741d7b2f  B[3]=44655a86  C[3]=d35140b1  D[3]=f278a610

Step 13: (r=19, s=22)
A[0]=337f3e16  B[0]=8f5aefdd  C[0]=79c565d0  D[0]=e65af135
A[1]=c606d13a  B[1]=864b69fd  C[1]=86c0c6fc  D[1]=d3529ee8
A[2]=b0fa8172  B[2]=0f54af95  C[2]=62c6113b  D[2]=adcd617d
A[3]=83cc222f  B[3]=d97ba0eb  C[3]=44655a86  D[3]=d35140b1

Step 14: (r=22, s= 7)
```

```
A[0]=9aa72597  B[0]=858cdfcf  C[0]=8f5aefdd  D[0]=79c565d0
A[1]=0db6075c  B[1]=4eb181b4  C[1]=864b69fd  D[1]=86c0c6fc
A[2]=2213ad22  B[2]=5cac3ea0  C[2]=0f54af95  D[2]=62c6113b
A[3]=034f8b78  B[3]=8be0f308  C[3]=d97ba0eb  D[3]=44655a86

Step 15: (r= 7, s=28)
A[0]=189250ab  B[0]=5392cbcd  C[0]=858cdfcf  D[0]=8f5aefdd
A[1]=97a13bcb  B[1]=db03ae06  C[1]=4eb181b4  D[1]=864b69fd
A[2]=7aa01bc2  B[2]=09d69111  C[2]=5cac3ea0  D[2]=0f54af95
A[3]=2c9bacc8  B[3]=a7c5bc01  C[3]=8be0f308  D[3]=d97ba0eb

Step 16: (r=29, s= 9)
A[0]=698b330a  B[0]=63124a15  C[0]=5392cbcd  D[0]=858cdfcf
A[1]=5ee33f34  B[1]=72f42779  C[1]=db03ae06  D[1]=4eb181b4
A[2]=e515f612  B[2]=4f540378  C[2]=09d69111  D[2]=5cac3ea0
A[3]=295f0550  B[3]=05937599  C[3]=a7c5bc01  D[3]=8be0f308

Step 17: (r= 9, s=15)
A[0]=f806b7f0  B[0]=166614d3  C[0]=63124a15  D[0]=5392cbcd
A[1]=f1110661  B[1]=c67e68bd  C[1]=72f42779  D[1]=db03ae06
A[2]=fa742ae1  B[2]=2bec25ca  C[2]=4f540378  D[2]=09d69111
A[3]=590f33f1  B[3]=be0aa052  C[3]=05937599  D[3]=a7c5bc01

Step 18: (r=15, s= 5)
A[0]=98d4cc76  B[0]=5bf87c03  C[0]=166614d3  D[0]=63124a15
A[1]=693d15ac  B[1]=8330f888  C[1]=c67e68bd  D[1]=72f42779
A[2]=d230f8cc  B[2]=1570fd3a  C[2]=2bec25ca  D[2]=4f540378
A[3]=9e7f0b68  B[3]=99f8ac87  C[3]=be0aa052  D[3]=05937599

Step 19: (r= 5, s=29)
A[0]=52bbb211  B[0]=1a998ed3  C[0]=5bf87c03  D[0]=166614d3
A[1]=08036840  B[1]=27a2b58d  C[1]=8330f888  D[1]=c67e68bd
A[2]=994da159  B[2]=461f199a  C[2]=1570fd3a  D[2]=2bec25ca
A[3]=0809d09c  B[3]=cfe16d13  C[3]=99f8ac87  D[3]=be0aa052

Step 20: (r=29, s= 9)
A[0]=89143e88  B[0]=2a577642  C[0]=1a998ed3  D[0]=5bf87c03
A[1]=cf61e648  B[1]=01006d08  C[1]=27a2b58d  D[1]=8330f888
A[2]=da28f21f  B[2]=3329b42b  C[2]=461f199a  D[2]=1570fd3a
A[3]=9c18c22a  B[3]=81013a13  C[3]=cfe16d13  D[3]=99f8ac87

Step 21: (r= 9, s=15)
A[0]=bb942a3f  B[0]=287d1112  C[0]=2a577642  D[0]=1a998ed3
A[1]=f17ffc00  B[1]=c3cc919e  C[1]=01006d08  D[1]=27a2b58d
A[2]=96befa75  B[2]=51e43fb4  C[2]=3329b42b  D[2]=461f199a
A[3]=fe6a31f8  B[3]=31845538  C[3]=81013a13  D[3]=cfe16d13

Step 22: (r=15, s= 5)
A[0]=a6935c87  B[0]=151fddca  C[0]=287d1112  D[0]=2a577642
```

```
A[1]=8fed78f7  B[1]=fe0078bf  C[1]=c3cc919e  D[1]=01006d08
A[2]=c630603f  B[2]=7d3acb5f  C[2]=51e43fb4  D[2]=3329b42b
A[3]=b831a451  B[3]=18fc7f35  C[3]=31845538  D[3]=81013a13

Step 23: (r= 5, s=29)
A[0]=a345716d  B[0]=d26b90f4  C[0]=151fddca  D[0]=287d1112
A[1]=71cff306  B[1]=fdaf1ef1  C[1]=fe0078bf  D[1]=c3cc919e
A[2]=60f650a2  B[2]=c60c07f8  C[2]=7d3acb5f  D[2]=51e43fb4
A[3]=cfaa00d4  B[3]=06348a37  C[3]=18fc7f35  D[3]=31845538

Step 24: (r= 4, s=13)
A[0]=da5da0a2  B[0]=345716da  C[0]=d26b90f4  D[0]=151fddca
A[1]=1731a1f5  B[1]=1cff3067  C[1]=fdaf1ef1  D[1]=fe0078bf
A[2]=7eaad895  B[2]=0f650a26  C[2]=c60c07f8  D[2]=7d3acb5f
A[3]=3b62c1b5  B[3]=faa00d4c  C[3]=06348a37  D[3]=18fc7f35

Step 25: (r=13, s=10)
A[0]=f9a9f18e  B[0]=b4145b4b  C[0]=345716da  D[0]=d26b90f4
A[1]=83b70eb3  B[1]=343ea2e6  C[1]=1cff3067  D[1]=fdaf1ef1
A[2]=0a80b077  B[2]=5b12afd5  C[2]=0f650a26  D[2]=c60c07f8
A[3]=56f92fb1  B[3]=5836a76c  C[3]=faa00d4c  D[3]=06348a37

Step 26: (r=10, s=25)
A[0]=658e6569  B[0]=a7c63be6  C[0]=b4145b4b  D[0]=345716da
A[1]=6fd279f1  B[1]=dc3ace0e  C[1]=343ea2e6  D[1]=1cff3067
A[2]=4d88dbcf  B[2]=02c1dc2a  C[2]=5b12afd5  D[2]=0f650a26
A[3]=b3e94123  B[3]=e4bec55b  C[3]=5836a76c  D[3]=faa00d4c

Step 27: (r=25, s= 4)
A[0]=198330f3  B[0]=d2cb1cca  C[0]=a7c63be6  D[0]=b4145b4b
A[1]=4bdcde6f  B[1]=e2dfa4f3  C[1]=dc3ace0e  D[1]=343ea2e6
A[2]=6e922eea  B[2]=9e9b11b7  C[2]=02c1dc2a  D[2]=5b12afd5
A[3]=8107aef7  B[3]=4767d282  C[3]=e4bec55b  D[3]=5836a76c

Step 28: (r= 4, s=13)
A[0]=058e8dbb  B[0]=98330f31  C[0]=d2cb1cca  D[0]=a7c63be6
A[1]=a60ac7f6  B[1]=bdcde6f4  C[1]=e2dfa4f3  D[1]=dc3ace0e
A[2]=9f2fcef9  B[2]=e922eea6  C[2]=9e9b11b7  D[2]=02c1dc2a
A[3]=e06f95c6  B[3]=107aef78  C[3]=4767d282  D[3]=e4bec55b

Step 29: (r=13, s=10)
A[0]=a7edf0df  B[0]=d1b760b1  C[0]=98330f31  D[0]=d2cb1cca
A[1]=dc2c9277  B[1]=58fed4c1  C[1]=bdcde6f4  D[1]=e2dfa4f3
A[2]=002d6ac5  B[2]=f9df33e5  C[2]=e922eea6  D[2]=9e9b11b7
A[3]=55820fef  B[3]=f2b8dc0d  C[3]=107aef78  D[3]=4767d282

Step 30: (r=10, s=25)
A[0]=1b687415  B[0]=b7c37e9f  C[0]=d1b760b1  D[0]=98330f31
A[1]=f007b0d2  B[1]=b249df70  C[1]=58fed4c1  D[1]=bdcde6f4
```

```
A[2]=06178f86  B[2]=b5ab1400  C[2]=f9df33e5  D[2]=e922eea6
A[3]=2127cef7  B[3]=083fbd56  C[3]=f2b8dc0d  D[3]=107aef78

Step 31: (r=25, s= 4)
A[0]=84a4b451  B[0]=2a36d0e8  C[0]=b7c37e9f  D[0]=d1b760b1
A[1]=50eb8b2a  B[1]=a5e00f61  C[1]=b249df70  D[1]=58fed4c1
A[2]=1c862d72  B[2]=0c0c2f1f  C[2]=b5ab1400  D[2]=f9df33e5
A[3]=8461f98e  B[3]=ee424f9d  C[3]=083fbd56  D[3]=f2b8dc0d

Feed-Forward Step 32: (r= 4, s=13)
A[0]=d02934a7  B[0]=4a4b4518  C[0]=2a36d0e8  D[0]=b7c37e9f
A[1]=fb7eaa00  B[1]=0eb8b2a5  C[1]=a5e00f61  D[1]=b249df70
A[2]=fe5d39e4  B[2]=c862d721  C[2]=0c0c2f1f  D[2]=b5ab1400
A[3]=80e0ff77  B[3]=461f98e8  C[3]=ee424f9d  D[3]=083fbd56

Feed-Forward Step 33: (r=13, s=10)
A[0]=d46115f1  B[0]=2694fa05  C[0]=4a4b4518  D[0]=2a36d0e8
A[1]=bd6c2f99  B[1]=d5401f6f  C[1]=0eb8b2a5  D[1]=a5e00f61
A[2]=7e45c185  B[2]=a73c9fcb  C[2]=c862d721  D[2]=0c0c2f1f
A[3]=dd22cd51  B[3]=1feef01c  C[3]=461f98e8  D[3]=ee424f9d

Feed-Forward Step 34: (r=10, s=25)
A[0]=7c9ff225  B[0]=8457c751  C[0]=2694fa05  D[0]=4a4b4518
A[1]=a36e10b0  B[1]=b0be66f5  C[1]=d5401f6f  D[1]=0eb8b2a5
A[2]=bb8d0fb4  B[2]=170615f9  C[2]=a73c9fcb  D[2]=c862d721
A[3]=0ccccad1  B[3]=8b354774  C[3]=1feef01c  D[3]=461f98e8

Feed-Forward Step 35: (r=25, s= 4)
A[0]=a9f8b4cb  B[0]=4af93fe4  C[0]=8457c751  D[0]=2694fa05
A[1]=044b4b30  B[1]=6146dc21  C[1]=b0be66f5  D[1]=d5401f6f
A[2]=4ba99330  B[2]=69771a1f  C[2]=170615f9  D[2]=a73c9fcb
A[3]=36ee5970  B[3]=a2199995  C[3]=8b354774  D[3]=1feef01c
```

Compression Function Output

```
A[0]=a9f8b4cb  B[0]=4af93fe4  C[0]=8457c751  D[0]=2694fa05
A[1]=044b4b30  B[1]=6146dc21  C[1]=b0be66f5  D[1]=d5401f6f
A[2]=4ba99330  B[2]=69771a1f  C[2]=170615f9  D[2]=a73c9fcb
A[3]=36ee5970  B[3]=a2199995  C[3]=8b354774  D[3]=1feef01c
```

Hash Function Output

```
cbb4f8a9304b4b043093a94b7059ee36e43ff94a21dc46611f1a7769
```

A.1.3 Two-block Message

We use the message made of 700 `1` bits.

First block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =  130  139   95   90   30    8   23   57
y[  8.. 15] =  129  152  176  135   15   86  140   53
y[ 16.. 23] =  193   34   88   34  136  231   70    7
y[ 24.. 31] =  225   75   44   72   68  127   35  120
y[ 32.. 39] =  241  151   22   70   34  193  146  163
y[ 40.. 47] =  249   20   11  219   17   74   73  235
y[ 48.. 55] =  253   50  134  235  137   79  165   92
y[ 56.. 63] =  255  194   67  159  197   44  211   92
y[ 64.. 71] =  256  181  162  182  227  122  234  179
y[ 72.. 79] =  128   91   81  207  242  115  117  226
y[ 80.. 87] =   64   80  169  160  121  120  187   42
y[ 88.. 95] =   32   58  213  108  189   44  222  244
y[ 96..103] =   16  248  235    8  223  133  111  210
y[104..111] =    8  180  246  193  240  238  184  157
y[112..119] =    4  177  123   70  120   85   92  171
y[120..127] =    2   76  190  217   60  190   46   94
```

Intermediate Expanded Message

```
Z[ 0] = aabaa439  410a44a7  05c815ae  2931109f
Z[ 1] = b41fa380  a7d6c577  3e260ad7  264dab73
Z[ 2] = 1892d1c0  18923f98  ed36a88f  050f3296
Z[ 3] = 3633e8e0  34081fcc  5bc73124  56b8194b
Z[ 4] = b366f470  32960fe6  d1c01892  bc12afc9
Z[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
Z[ 6] = 2422fd1c  f01aa71d  3917a948  427cbd84
Z[ 7] = d279fe8e  b92e306b  1fccd4a4  427cdec2
Z[ 8] = c914ff47  c9cdbb59  582aea52  c7a2ef61
Z[ 9] = 41c35c80  dbde3a89  531bf529  e999548d
Z[10] = 39d02e40  b9e7c068  56b85771  1e5acd6a
Z[11] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
Z[12] = f97f0b90  05c8f01a  a664e76e  de095037
Z[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
Z[14] = c63002e4  329658e3  3d6d56b8  c1da427c
Z[15] = 36ec0172  e318cf95  cf952b5c  43ee213e
Z[16] = ff178c69  a9895677  e4b21b4e  eb1114ef
Z[17] = 74808b80  49b9b647  f2590da7  6a7d9583
```

```
Z[18] = 3a40c5c0  afe85018  6e2191df  c04a3fb6
Z[19] = 1d20e2e0  d7f4280c  c21c3de4  e0251fdb
Z[20] = 0e90f170  ebfa1406  e10e1ef2  65079af9
Z[21] = 0748f8b8  f5fd0a03  f0870f79  bd8f4271
Z[22] = 03a4fc5c  6ff3900d  6d3892c8  53bcac44
Z[23] = 01d2fe2e  c3053cfb  369cc964  29ded622
Z[24] = bad4949a  bbbd51ea  6f0a0748  b90233e1
Z[25] = 52d3a06f  d27e90f6  68ab4e46  e3c9303d
Z[26] = 48d01ef2  a7b71ef2  6d38e856  263a065f
Z[27] = 34ca4443  624c4188  280c7397  f42b6d38
Z[28] = f7cf9f86  07483fb6  8f24c5c0  d539aa72
Z[29] = b9eb1234  c5c0dd6a  eeb5435a  a4fcebfa
Z[30] = b7302d82  3fb6ebfa  4d5d47e7  b1ba53bc
Z[31] = 452cc6a9  db98a6ce  c305280c  558e53bc
```

Expanded Message

```
W[ 0] = b366f470  32960fe6  d1c01892  bc12afc9
W[ 1] = 2422fd1c  f01aa71d  3917a948  427cbd84
W[ 2] = aabaa439  410a44a7  05c815ae  2931109f
W[ 3] = 1892d1c0  18923f98  ed36a88f  050f3296
W[ 4] = d279fe8e  b92e306b  1fccd4a4  427cdec2
W[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
W[ 6] = 3633e8e0  34081fcc  5bc73124  56b8194b
W[ 7] = b41fa380  a7d6c577  3e260ad7  264dab73
W[ 8] = 36ec0172  e318cf95  cf952b5c  43ee213e
W[ 9] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
W[10] = f97f0b90  05c8f01a  a664e76e  de095037
W[11] = c914ff47  c9cdbb59  582aea52  c7a2ef61
W[12] = 41c35c80  dbde3a89  531bf529  e999548d
W[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
W[14] = 39d02e40  b9e7c068  56b85771  1e5acd6a
W[15] = c63002e4  329658e3  3d6d56b8  c1da427c
W[16] = 74808b80  49b9b647  f2590da7  6a7d9583
W[17] = 3a40c5c0  afe85018  6e2191df  c04a3fb6
W[18] = 01d2fe2e  c3053cfb  369cc964  29ded622
W[19] = 0e90f170  ebfa1406  e10e1ef2  65079af9
W[20] = 03a4fc5c  6ff3900d  6d3892c8  53bcac44
W[21] = 0748f8b8  f5fd0a03  f0870f79  bd8f4271
W[22] = ff178c69  a9895677  e4b21b4e  eb1114ef
W[23] = 1d20e2e0  d7f4280c  c21c3de4  e0251fdb
W[24] = b7302d82  3fb6ebfa  4d5d47e7  b1ba53bc
W[25] = bad4949a  bbbd51ea  6f0a0748  b90233e1
W[26] = 52d3a06f  d27e90f6  68ab4e46  e3c9303d
W[27] = 452cc6a9  db98a6ce  c305280c  558e53bc
W[28] = 34ca4443  624c4188  280c7397  f42b6d38
W[29] = b9eb1234  c5c0dd6a  eeb5435a  a4fcebfa
W[30] = f7cf9f86  07483fb6  8f24c5c0  d539aa72
W[31] = 48d01ef2  a7b71ef2  6d38e856  263a065f
```

Feistel Steps

```
IV :
A[0]=33586e9f  B[0]=de943106  C[0]=22e7b0af  D[0]=f64ae77c
A[1]=12fff033  B[1]=2742e439  C[1]=c862b3a8  D[1]=fa373b76
A[2]=b2d9f64d  B[2]=4fbab5ac  C[2]=33e00cdc  D[2]=7dc1ee5b
A[3]=6f8fea53  B[3]=62b9ff96  C[3]=236b86a6  D[3]=7fb29ce8

IV XOR M :
A[0]=cca79160  B[0]=216bcef9  C[0]=dd184f50  D[0]=09b51883
A[1]=ed000fcc  B[1]=d8bd1bc6  C[1]=379d4c57  D[1]=05c8c489
A[2]=4d2609b2  B[2]=b0454a53  C[2]=cc1ff323  D[2]=823e11a4
A[3]=907015ac  B[3]=9d460069  C[3]=dc947959  D[3]=804d6317

Step  0: (r= 3, s=23)
A[0]=19e7aa54  B[0]=653c8b06  C[0]=216bcef9  D[0]=dd184f50
A[1]=88460916  B[1]=68007e67  C[1]=d8bd1bc6  D[1]=379d4c57
A[2]=a86abb76  B[2]=69304d92  C[2]=b0454a53  D[2]=cc1ff323
A[3]=15bcdfcf  B[3]=8380ad64  C[3]=9d460069  D[3]=dc947959

Step  1: (r=23, s=17)
A[0]=f1867a2d  B[0]=2a0cf3d5  C[0]=653c8b06  D[0]=216bcef9
A[1]=03ffdf51  B[1]=8b442304  C[1]=68007e67  D[1]=d8bd1bc6
A[2]=f5096e8e  B[2]=bb54355d  C[2]=69304d92  D[2]=b0454a53
A[3]=13c774ab  B[3]=e78ade6f  C[3]=8380ad64  D[3]=9d460069

Step  2: (r=17, s=27)
A[0]=b8d942bf  B[0]=f45be30c  C[0]=2a0cf3d5  D[0]=653c8b06
A[1]=7946462e  B[1]=bea207ff  C[1]=8b442304  D[1]=68007e67
A[2]=aa1bf427  B[2]=dd1dea12  C[2]=bb54355d  D[2]=69304d92
A[3]=aeabb27f  B[3]=e956278e  C[3]=e78ade6f  D[3]=8380ad64

Step  3: (r=27, s= 3)
A[0]=f534b2c2  B[0]=fdc6ca15  C[0]=f45be30c  D[0]=2a0cf3d5
A[1]=d26df37e  B[1]=73ca3231  C[1]=bea207ff  D[1]=8b442304
A[2]=7b9c1972  B[2]=3d50dfa1  C[2]=dd1dea12  D[2]=bb54355d
A[3]=c9e34fe4  B[3]=fd755d93  C[3]=e956278e  D[3]=e78ade6f

Step  4: (r= 3, s=23)
A[0]=10d9ba7d  B[0]=a9a59617  C[0]=fdc6ca15  D[0]=f45be30c
A[1]=c6362d69  B[1]=936f9bf6  C[1]=73ca3231  D[1]=bea207ff
A[2]=4351b509  B[2]=dce0cb93  C[2]=3d50dfa1  D[2]=dd1dea12
A[3]=eef95b7c  B[3]=4f1a7f26  C[3]=fd755d93  D[3]=e956278e

Step  5: (r=23, s=17)
A[0]=ad2af5d9  B[0]=3e886cdd  C[0]=a9a59617  D[0]=fdc6ca15
A[1]=1b68960e  B[1]=b4e31b16  C[1]=936f9bf6  D[1]=73ca3231
A[2]=609bfae7  B[2]=84a1a8da  C[2]=dce0cb93  D[2]=3d50dfa1
A[3]=b593feb0  B[3]=be777cad  C[3]=4f1a7f26  D[3]=fd755d93
```

```
Step  6: (r=17, s=27)
A[0]=c329540f  B[0]=ebb35a55  C[0]=3e886cdd  D[0]=a9a59617
A[1]=858d49bd  B[1]=2c1c36d1  C[1]=b4e31b16  D[1]=936f9bf6
A[2]=c04f3b03  B[2]=f5cec137  C[2]=84a1a8da  D[2]=dce0cb93
A[3]=0668c8e3  B[3]=fd616b27  C[3]=be777cad  D[3]=4f1a7f26

Step  7: (r=27, s= 3)
A[0]=6977297a  B[0]=7e194aa0  C[0]=ebb35a55  D[0]=3e886cdd
A[1]=16cf2e5d  B[1]=ec2c6a4d  C[1]=2c1c36d1  D[1]=b4e31b16
A[2]=7ccd468e  B[2]=1e0279d8  C[2]=f5cec137  D[2]=84a1a8da
A[3]=8a79044e  B[3]=18334647  C[3]=fd616b27  D[3]=be777cad

Step  8: (r=28, s=19)
A[0]=2c4a9072  B[0]=a6977297  C[0]=7e194aa0  D[0]=ebb35a55
A[1]=1392f529  B[1]=d16cf2e5  C[1]=ec2c6a4d  D[1]=2c1c36d1
A[2]=80ec7cb1  B[2]=e7ccd468  C[2]=1e0279d8  D[2]=f5cec137
A[3]=112b6f4f  B[3]=e8a79044  C[3]=18334647  D[3]=fd616b27

Step  9: (r=19, s=22)
A[0]=ab2b88ca  B[0]=83916254  C[0]=a6977297  D[0]=7e194aa0
A[1]=de2f37d8  B[1]=a9489c97  C[1]=d16cf2e5  D[1]=ec2c6a4d
A[2]=d965a3d4  B[2]=e58c0763  C[2]=e7ccd468  D[2]=1e0279d8
A[3]=6dcb1377  B[3]=7a78895b  C[3]=e8a79044  D[3]=18334647

Step 10: (r=22, s= 7)
A[0]=8c1a9c67  B[0]=32aacae2  C[0]=83916254  D[0]=a6977297
A[1]=7cf30101  B[1]=f6378bcd  C[1]=a9489c97  D[1]=d16cf2e5
A[2]=2c872237  B[2]=f5365968  C[2]=e58c0763  D[2]=e7ccd468
A[3]=4ac374bc  B[3]=dddb72c4  C[3]=7a78895b  D[3]=e8a79044

Step 11: (r= 7, s=28)
A[0]=68ede3ea  B[0]=0d4e33c6  C[0]=32aacae2  D[0]=83916254
A[1]=9c988053  B[1]=798080be  C[1]=f6378bcd  D[1]=a9489c97
A[2]=1bd0dcff  B[2]=43911b96  C[2]=f5365968  D[2]=e58c0763
A[3]=cfe29b5c  B[3]=61ba5e25  C[3]=dddb72c4  D[3]=7a78895b

Step 12: (r=28, s=19)
A[0]=4f80fa22  B[0]=a68ede3e  C[0]=0d4e33c6  D[0]=32aacae2
A[1]=668aebf8  B[1]=39c98805  C[1]=798080be  D[1]=f6378bcd
A[2]=81528b77  B[2]=f1bd0dcf  C[2]=43911b96  D[2]=f5365968
A[3]=b31e9e30  B[3]=ccfe29b5  C[3]=61ba5e25  D[3]=dddb72c4

Step 13: (r=19, s=22)
A[0]=0fbeafc6  B[0]=d1127c07  C[0]=a68ede3e  D[0]=0d4e33c6
A[1]=1715f937  B[1]=5fc33457  C[1]=39c98805  D[1]=798080be
A[2]=0ebcbf5d  B[2]=5bbc0a94  C[2]=f1bd0dcf  D[2]=43911b96
A[3]=6de109ee  B[3]=f18598f4  C[3]=ccfe29b5  D[3]=61ba5e25

Step 14: (r=22, s= 7)
```

```
A[0]=da4b7ea9  B[0]=f183efab  C[0]=d1127c07  D[0]=a68ede3e
A[1]=6c404dd8  B[1]=4dc5c57e  C[1]=5fc33457  D[1]=39c98805
A[2]=508737f9  B[2]=d743af2f  C[2]=5bbc0a94  D[2]=f1bd0dcf
A[3]=ee9eb161  B[3]=7b9b7842  C[3]=f18598f4  D[3]=ccfe29b5

Step 15: (r= 7, s=28)
A[0]=f4031232  B[0]=25bf54ed  C[0]=f183efab  D[0]=d1127c07
A[1]=91616751  B[1]=2026ec36  C[1]=4dc5c57e  D[1]=5fc33457
A[2]=9783ca3b  B[2]=439bfca8  C[2]=d743af2f  D[2]=5bbc0a94
A[3]=5c437ef1  B[3]=4f58b0f7  C[3]=7b9b7842  D[3]=f18598f4

Step 16: (r=29, s= 9)
A[0]=a0fada1d  B[0]=5e806246  C[0]=25bf54ed  D[0]=f183efab
A[1]=6f2629ca  B[1]=322c2cea  C[1]=2026ec36  D[1]=4dc5c57e
A[2]=108b3169  B[2]=72f07947  C[2]=439bfca8  D[2]=d743af2f
A[3]=e8eb0281  B[3]=2b886fde  C[3]=4f58b0f7  D[3]=7b9b7842

Step 17: (r= 9, s=15)
A[0]=d42c9c75  B[0]=f5b43b41  C[0]=5e806246  D[0]=25bf54ed
A[1]=97ace20a  B[1]=4c5394de  C[1]=322c2cea  D[1]=2026ec36
A[2]=6bbb6159  B[2]=1662d221  C[2]=72f07947  D[2]=439bfca8
A[3]=2b2b7100  B[3]=d60503d1  C[3]=2b886fde  D[3]=4f58b0f7

Step 18: (r=15, s= 5)
A[0]=37def796  B[0]=4e3aea16  C[0]=f5b43b41  D[0]=5e806246
A[1]=33d1ad76  B[1]=71054bd6  C[1]=4c5394de  D[1]=322c2cea
A[2]=4be3d806  B[2]=b0acb5dd  C[2]=1662d221  D[2]=72f07947
A[3]=27bf94cc  B[3]=b8801595  C[3]=d60503d1  D[3]=2b886fde

Step 19: (r= 5, s=29)
A[0]=22e4888a  B[0]=fbdef2c6  C[0]=4e3aea16  D[0]=f5b43b41
A[1]=cb57c4dd  B[1]=7a35aec6  C[1]=71054bd6  D[1]=4c5394de
A[2]=c8f2d811  B[2]=7c7b00c9  C[2]=b0acb5dd  D[2]=1662d221
A[3]=0a57b313  B[3]=f7f29984  C[3]=b8801595  D[3]=d60503d1

Step 20: (r=29, s= 9)
A[0]=118f3d2a  B[0]=445c9111  C[0]=fbdef2c6  D[0]=4e3aea16
A[1]=f305dd70  B[1]=b96af89b  C[1]=7a35aec6  D[1]=71054bd6
A[2]=e5567d94  B[2]=391e5b02  C[2]=7c7b00c9  D[2]=b0acb5dd
A[3]=6cdfe6da  B[3]=614af662  C[3]=f7f29984  D[3]=b8801595

Step 21: (r= 9, s=15)
A[0]=55a33597  B[0]=1e7a5423  C[0]=445c9111  D[0]=fbdef2c6
A[1]=47d00537  B[1]=0bbae1e6  C[1]=b96af89b  D[1]=7a35aec6
A[2]=cf38c422  B[2]=acfb29ca  C[2]=391e5b02  D[2]=7c7b00c9
A[3]=d45f97bf  B[3]=bfcdb4d9  C[3]=614af662  D[3]=f7f29984

Step 22: (r=15, s= 5)
A[0]=5023efe5  B[0]=9acbaad1  C[0]=1e7a5423  D[0]=445c9111
```

```
A[1]=c31cc8b4  B[1]=029ba3e8  C[1]=0bbae1e6  D[1]=b96af89b
A[2]=67b84df2  B[2]=6211679c  C[2]=acfb29ca  D[2]=391e5b02
A[3]=0d0851c3  B[3]=cbdfea2f  C[3]=bfcdb4d9  D[3]=614af662

Step 23: (r= 5, s=29)
A[0]=f08764bb  B[0]=047dfcaa  C[0]=9acbaad1  D[0]=1e7a5423
A[1]=69a8fe9d  B[1]=63991698  C[1]=029ba3e8  D[1]=0bbae1e6
A[2]=6fd79770  B[2]=f709be4c  C[2]=6211679c  D[2]=acfb29ca
A[3]=1ea5bd8b  B[3]=a10a3861  C[3]=cbdfea2f  D[3]=bfcdb4d9

Step 24: (r= 4, s=13)
A[0]=a8a1e5d5  B[0]=08764bbf  C[0]=047dfcaa  D[0]=9acbaad1
A[1]=a53161a0  B[1]=9a8fe9d6  C[1]=63991698  D[1]=029ba3e8
A[2]=376b84dc  B[2]=fd797706  C[2]=f709be4c  D[2]=6211679c
A[3]=4dd0bd62  B[3]=ea5bd8b1  C[3]=a10a3861  D[3]=cbdfea2f

Step 25: (r=13, s=10)
A[0]=e3003075  B[0]=3cbab514  C[0]=08764bbf  D[0]=047dfcaa
A[1]=a161f3bd  B[1]=2c3414a6  C[1]=9a8fe9d6  D[1]=63991698
A[2]=4f6e582e  B[2]=709b86ed  C[2]=fd797706  D[2]=f709be4c
A[3]=1f0cda5a  B[3]=17ac49ba  C[3]=ea5bd8b1  D[3]=a10a3861

Step 26: (r=10, s=25)
A[0]=a268f8ad  B[0]=00c1d78c  C[0]=3cbab514  D[0]=08764bbf
A[1]=a24244bd  B[1]=87cef685  C[1]=2c3414a6  D[1]=9a8fe9d6
A[2]=046e96ec  B[2]=b960b93d  C[2]=709b86ed  D[2]=fd797706
A[3]=b3ba3cee  B[3]=3369687c  C[3]=17ac49ba  D[3]=ea5bd8b1

Step 27: (r=25, s= 4)
A[0]=22a304cf  B[0]=5b44d1f1  C[0]=00c1d78c  D[0]=3cbab514
A[1]=a53324a1  B[1]=7b448489  C[1]=87cef685  D[1]=2c3414a6
A[2]=f46a686c  B[2]=d808dd2d  C[2]=b960b93d  D[2]=709b86ed
A[3]=49723bc4  B[3]=dd677479  C[3]=3369687c  D[3]=17ac49ba

Step 28: (r= 4, s=13)
A[0]=208b1557  B[0]=2a304cf2  C[0]=5b44d1f1  D[0]=00c1d78c
A[1]=7679a2fc  B[1]=53324a1a  C[1]=7b448489  D[1]=87cef685
A[2]=48a67f14  B[2]=46a686cf  C[2]=d808dd2d  D[2]=b960b93d
A[3]=b92016c1  B[3]=9723bc44  C[3]=dd677479  D[3]=3369687c

Step 29: (r=13, s=10)
A[0]=b7d706b6  B[0]=62aae411  C[0]=2a304cf2  D[0]=5b44d1f1
A[1]=d13ca818  B[1]=345f8ecf  C[1]=53324a1a  D[1]=7b448489
A[2]=27ce2291  B[2]=cfe28914  C[2]=46a686cf  D[2]=d808dd2d
A[3]=88cdc1e7  B[3]=02d83724  C[3]=9723bc44  D[3]=dd677479

Step 30: (r=10, s=25)
A[0]=458bf0b0  B[0]=5c1adadf  C[0]=62aae411  D[0]=2a304cf2
A[1]=0fc2717b  B[1]=f2a06344  C[1]=345f8ecf  D[1]=53324a1a
```

```
A[2]=3c65c66e  B[2]=388a449f  C[2]=cfe28914  D[2]=46a686cf
A[3]=d6f51a47  B[3]=37079e23  C[3]=02d83724  D[3]=9723bc44

Step 31: (r=25, s= 4)
A[0]=552e92e7  B[0]=608b17e1  C[0]=5c1adadf  D[0]=62aae411
A[1]=aa6aafe7  B[1]=f61f84e2  C[1]=f2a06344  D[1]=345f8ecf
A[2]=6cae4c20  B[2]=dc78cb8c  C[2]=388a449f  D[2]=cfe28914
A[3]=394d918f  B[3]=8fadea34  C[3]=37079e23  D[3]=02d83724

Feed-Forward Step 32: (r= 4, s=13)
A[0]=4a8e54b6  B[0]=52e92e75  C[0]=608b17e1  D[0]=5c1adadf
A[1]=13614943  B[1]=a6aafe7a  C[1]=f61f84e2  D[1]=f2a06344
A[2]=3fab1a56  B[2]=cae4c206  C[2]=dc78cb8c  D[2]=388a449f
A[3]=48dc9ea3  B[3]=94d918f3  C[3]=8fadea34  D[3]=37079e23

Feed-Forward Step 33: (r=13, s=10)
A[0]=0975cce0  B[0]=ca96c951  C[0]=52e92e75  D[0]=608b17e1
A[1]=52e84551  B[1]=2928626c  C[1]=a6aafe7a  D[1]=f61f84e2
A[2]=6acbce67  B[2]=634ac7f5  C[2]=cae4c206  D[2]=dc78cb8c
A[3]=4fa4887b  B[3]=93d4691b  C[3]=94d918f3  D[3]=8fadea34

Feed-Forward Step 34: (r=10, s=25)
A[0]=faf5bd10  B[0]=d7338025  C[0]=ca96c951  D[0]=52e92e75
A[1]=7ae747a3  B[1]=a115454b  C[1]=2928626c  D[1]=a6aafe7a
A[2]=73190f62  B[2]=2f399dab  C[2]=634ac7f5  D[2]=cae4c206
A[3]=8ba3325d  B[3]=9221ed3e  C[3]=93d4691b  D[3]=94d918f3

Feed-Forward Step 35: (r=25, s= 4)
A[0]=7194a985  B[0]=21f5eb7a  C[0]=d7338025  D[0]=ca96c951
A[1]=e3e0261a  B[1]=46f5ce8f  C[1]=a115454b  D[1]=2928626c
A[2]=071db015  B[2]=c4e6321e  C[2]=2f399dab  D[2]=634ac7f5
A[3]=9207db14  B[3]=bb174664  C[3]=9221ed3e  D[3]=93d4691b
```

Compression Function Output

```
A[0]=7194a985  B[0]=21f5eb7a  C[0]=d7338025  D[0]=ca96c951
A[1]=e3e0261a  B[1]=46f5ce8f  C[1]=a115454b  D[1]=2928626c
A[2]=071db015  B[2]=c4e6321e  C[2]=2f399dab  D[2]=634ac7f5
A[3]=9207db14  B[3]=bb174664  C[3]=9221ed3e  D[3]=93d4691b
```

Second block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff f0
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  195  145  230   47   52  203  238  249
y[  8.. 15] =   12   96  215  134  192  149   97   86
y[ 16.. 23] =  125   71  253   29   78  108  111   14
y[ 24.. 31] =   76   62  254  175   50   20  235   16
y[ 32.. 39] =  224   33  108  228   44  109  107   42
y[ 40.. 47] =  154  246  148  136  113  117   81  174
y[ 48.. 55] =   56  126  148   62  151   51  153  212
y[ 56.. 63] =   51  141  153   14    7  209  219   46
y[ 64.. 71] =   14   20   75  104   16  215  142  205
y[ 72.. 79] =  162   98  256  209  240   66   86   20
y[ 80.. 87] =  132   44   30    5   90   44  223  126
y[ 88.. 95] =  226  151   51  249  247   44  154   79
y[ 96..103] =   33  241  111  146   19  101   97  216
y[104..111] =   50  140   61  172   65  117   52  126
y[112..119] =  201  236  251   10   65  247  201  209
y[120..127] =   24   46  196   55  113   95   83  196
```

Intermediate Expanded Message

```
Z[ 0] = af10d332  21f7ec7d  d8fa2594  fa38f245
Z[ 1] = 456008ac  a71de1a6  b1f4d107  3e264619
Z[ 2] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
Z[ 3] = 2cce36ec  c4befdd5  0e742422  0b90f01a
Z[ 4] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
Z[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
Z[ 6] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
Z[ 7] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
Z[ 8] = 0e740a1e  4b283633  e1a60b90  da6cace5
Z[ 9] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
Z[10] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
Z[11] = b366e999  fa3824db  1fccf8c6  3917b591
Z[12] = f47017d9  afc95037  48fd0dbb  e25f4619
Z[13] = ab732422  c2932c15  548d2ef9  5b0e2594
Z[14] = f0d3d788  073afbaa  f8c62ef9  dd50d788
Z[15] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
Z[16] = 0cbec792  4443e76d  0e902f54  9755eeb5
Z[17] = a9890aec  ff17d9c6  f087c4d7  4e465849
Z[18] = 8e3b71c5  1b4efc5c  51ea46fe  e10e6507
Z[19] = e3c9452c  2e6bfd45  f6e62d82  a241ebfa
Z[20] = 1e09e1f7  6507624c  114b280c  58496163
Z[21] = 2d82a241  37859ccb  3b2966d9  2f5449b9
Z[22] = cd0832f8  fa8a9ccb  3b299f86  cd08a158
Z[23] = 15d82e6b  c87ba158  66d9065f  4b8bdd6a
Z[24] = 12349a10  5ea82ac7  d9c6ceda  d0acf8b8
Z[25] = 59325760  d450900d  3c129db4  12344e46
Z[26] = 280c409f  048d1a65  280c624c  72ae0cbe
Z[27] = 9f86386e  f8b8b55e  280c1234  47e70e90
Z[28] = f1701e09  9af9e59b  5bed6335  daaf263a
```

```
Z[29] = 9583f5fd  b2a391df  6a7d6a7d  72aeb475
Z[30] = ece372ae  091a386e  f6e62e6b  d450d70b
Z[31] = 29de966c  320f0cbe  5677d450  c87b29de
```

Expanded Message

```
W[ 0] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
W[ 1] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
W[ 2] = af10d332  21f7ec7d  d8fa2594  fa38f245
W[ 3] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
W[ 4] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
W[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
W[ 6] = 2cce36ec  c4befdd5  0e742422  0b90f01a
W[ 7] = 456008ac  a71de1a6  b1f4d107  3e264619
W[ 8] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
W[ 9] = b366e999  fa3824db  1fccf8c6  3917b591
W[10] = f47017d9  afc95037  48fd0dbb  e25f4619
W[11] = 0e740a1e  4b283633  e1a60b90  da6cace5
W[12] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
W[13] = ab732422  c2932c15  548d2ef9  5b0e2594
W[14] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
W[15] = f0d3d788  073afbaa  f8c62ef9  dd50d788
W[16] = a9890aec  ff17d9c6  f087c4d7  4e465849
W[17] = 8e3b71c5  1b4efc5c  51ea46fe  e10e6507
W[18] = 15d82e6b  c87ba158  66d9065f  4b8bdd6a
W[19] = 1e09e1f7  6507624c  114b280c  58496163
W[20] = cd0832f8  fa8a9ccb  3b299f86  cd08a158
W[21] = 2d82a241  37859ccb  3b2966d9  2f5449b9
W[22] = 0cbec792  4443e76d  0e902f54  9755eeb5
W[23] = e3c9452c  2e6bfd45  f6e62d82  a241ebfa
W[24] = ece372ae  091a386e  f6e62e6b  d450d70b
W[25] = 12349a10  5ea82ac7  d9c6ceda  d0acf8b8
W[26] = 59325760  d450900d  3c129db4  12344e46
W[27] = 29de966c  320f0cbe  5677d450  c87b29de
W[28] = 9f86386e  f8b8b55e  280c1234  47e70e90
W[29] = 9583f5fd  b2a391df  6a7d6a7d  72aeb475
W[30] = f1701e09  9af9e59b  5bed6335  daaf263a
W[31] = 280c409f  048d1a65  280c624c  72ae0cbe
```

Feistel Steps

```
IV :
A[0]=7194a985  B[0]=21f5eb7a  C[0]=d7338025  D[0]=ca96c951
A[1]=e3e0261a  B[1]=46f5ce8f  C[1]=a115454b  D[1]=2928626c
A[2]=071db015  B[2]=c4e6321e  C[2]=2f399dab  D[2]=634ac7f5
A[3]=9207db14  B[3]=bb174664  C[3]=9221ed3e  D[3]=93d4691b

IV XOR M :
A[0]=8e6b567a  B[0]=de0a1485  C[0]=d7338025  D[0]=ca96c951
A[1]=1c1fd9e5  B[1]=b60a3170  C[1]=a115454b  D[1]=2928626c
```

```
A[2]=f8e24fea  B[2]=c4e6321e  C[2]=2f399dab  D[2]=634ac7f5
A[3]=6df824eb  B[3]=bb174664  C[3]=9221ed3e  D[3]=93d4691b

Step  0: (r= 3, s=23)
A[0]=9fdf94ca  B[0]=735ab3d4  C[0]=de0a1485  D[0]=d7338025
A[1]=64bf52b6  B[1]=e0fecf28  C[1]=b60a3170  D[1]=a115454b
A[2]=55fe2d17  B[2]=c7127f57  C[2]=c4e6321e  D[2]=2f399dab
A[3]=b8491f98  B[3]=6fc1275b  C[3]=bb174664  D[3]=9221ed3e

Step  1: (r=23, s=17)
A[0]=fe700a4e  B[0]=654fefca  C[0]=735ab3d4  D[0]=de0a1485
A[1]=8029a5d3  B[1]=5b325fa9  C[1]=e0fecf28  D[1]=b60a3170
A[2]=85b02219  B[2]=8baaff16  C[2]=c7127f57  D[2]=c4e6321e
A[3]=2e579992  B[3]=cc5c248f  C[3]=6fc1275b  D[3]=bb174664

Step  2: (r=17, s=27)
A[0]=c2b789cb  B[0]=149dfce0  C[0]=654fefca  D[0]=735ab3d4
A[1]=f5facecc  B[1]=4ba70053  C[1]=5b325fa9  D[1]=e0fecf28
A[2]=8eb3170b  B[2]=44330b60  C[2]=8baaff16  D[2]=c7127f57
A[3]=b4b71fdb  B[3]=33245caf  C[3]=cc5c248f  D[3]=6fc1275b

Step  3: (r=27, s= 3)
A[0]=cbefbdc4  B[0]=5e15bc4e  C[0]=149dfce0  D[0]=654fefca
A[1]=6acca978  B[1]=67afd676  C[1]=4ba70053  D[1]=5b325fa9
A[2]=b07acf46  B[2]=5c7598b8  C[2]=44330b60  D[2]=8baaff16
A[3]=eed339c7  B[3]=dda5b8fe  C[3]=33245caf  D[3]=cc5c248f

Step  4: (r= 3, s=23)
A[0]=388e871d  B[0]=5f7dee26  C[0]=5e15bc4e  D[0]=149dfce0
A[1]=f0824e89  B[1]=56654bc3  C[1]=67afd676  D[1]=4ba70053
A[2]=225ca56d  B[2]=83d67a35  C[2]=5c7598b8  D[2]=44330b60
A[3]=5adbebe4  B[3]=7699ce3f  C[3]=dda5b8fe  D[3]=33245caf

Step  5: (r=23, s=17)
A[0]=b32c4387  B[0]=8e9c4743  C[0]=5f7dee26  D[0]=5e15bc4e
A[1]=b734040e  B[1]=44f84127  C[1]=56654bc3  D[1]=67afd676
A[2]=6f857751  B[2]=b6912e52  C[2]=83d67a35  D[2]=5c7598b8
A[3]=9308f2ca  B[3]=f22d6df5  C[3]=7699ce3f  D[3]=dda5b8fe

Step  6: (r=17, s=27)
A[0]=116e703a  B[0]=870f6658  C[0]=8e9c4743  D[0]=5f7dee26
A[1]=1b267f02  B[1]=081d6e68  C[1]=44f84127  D[1]=56654bc3
A[2]=3e291fea  B[2]=eea2df0a  C[2]=b6912e52  D[2]=83d67a35
A[3]=ad7ce3ca  B[3]=e5952611  C[3]=f22d6df5  D[3]=7699ce3f

Step  7: (r=27, s= 3)
A[0]=b1543260  B[0]=d08b7381  C[0]=870f6658  D[0]=8e9c4743
A[1]=8368cb76  B[1]=10d933f8  C[1]=081d6e68  D[1]=44f84127
A[2]=73eec7b8  B[2]=51f148ff  C[2]=eea2df0a  D[2]=b6912e52
```

```
A[3]=e0c51544  B[3]=556be71e  C[3]=e5952611  D[3]=f22d6df5

Step  8: (r=28, s=19)
A[0]=c3a68082  B[0]=0b154326  C[0]=d08b7381  D[0]=870f6658
A[1]=6b929524  B[1]=68368cb7  C[1]=10d933f8  D[1]=081d6e68
A[2]=2de5557d  B[2]=873eec7b  C[2]=51f148ff  D[2]=eea2df0a
A[3]=933d9e74  B[3]=4e0c5154  C[3]=556be71e  D[3]=e5952611

Step  9: (r=19, s=22)
A[0]=6636bd84  B[0]=04161d34  C[0]=0b154326  D[0]=d08b7381
A[1]=93f4c982  B[1]=a9235c94  C[1]=68368cb7  D[1]=10d933f8
A[2]=267d82f5  B[2]=abe96f2a  C[2]=873eec7b  D[2]=51f148ff
A[3]=ec02adfd  B[3]=f3a499ec  C[3]=4e0c5154  D[3]=556be71e

Step 10: (r=22, s= 7)
A[0]=c6bedfc9  B[0]=61198daf  C[0]=04161d34  D[0]=0b154326
A[1]=61e372ff  B[1]=60a4fd32  C[1]=a9235c94  D[1]=68368cb7
A[2]=8dfbffce  B[2]=bd499f60  C[2]=abe96f2a  D[2]=873eec7b
A[3]=4ca88ebe  B[3]=7f7b00ab  C[3]=f3a499ec  D[3]=4e0c5154

Step 11: (r= 7, s=28)
A[0]=69e17cd6  B[0]=5f6fe4e3  C[0]=61198daf  D[0]=04161d34
A[1]=c7bfdb37  B[1]=f1b97fb0  C[1]=60a4fd32  D[1]=a9235c94
A[2]=a33c6926  B[2]=fdffe746  C[2]=bd499f60  D[2]=abe96f2a
A[3]=91ea35e5  B[3]=54475f26  C[3]=7f7b00ab  D[3]=f3a499ec

Step 12: (r=28, s=19)
A[0]=a821a049  B[0]=669e17cd  C[0]=5f6fe4e3  D[0]=61198daf
A[1]=3f09595f  B[1]=7c7bfdb3  C[1]=f1b97fb0  D[1]=60a4fd32
A[2]=eb5b6c30  B[2]=6a33c692  C[2]=fdffe746  D[2]=bd499f60
A[3]=d7fe82b1  B[3]=591ea35e  C[3]=54475f26  D[3]=7f7b00ab

Step 13: (r=19, s=22)
A[0]=082609f0  B[0]=024d410d  C[0]=669e17cd  D[0]=5f6fe4e3
A[1]=d436dc5d  B[1]=caf9f84a  C[1]=7c7bfdb3  D[1]=f1b97fb0
A[2]=1d4c95ba  B[2]=61875adb  C[2]=6a33c692  D[2]=fdffe746
A[3]=2845f234  B[3]=158ebff4  C[3]=591ea35e  D[3]=54475f26

Step 14: (r=22, s= 7)
A[0]=32503f3c  B[0]=7c020982  C[0]=024d410d  D[0]=669e17cd
A[1]=57d0300d  B[1]=17750db7  C[1]=caf9f84a  D[1]=7c7bfdb3
A[2]=817482fa  B[2]=6e875325  C[2]=61875adb  D[2]=6a33c692
A[3]=ae7f0de6  B[3]=8d0a117c  C[3]=158ebff4  D[3]=591ea35e

Step 15: (r= 7, s=28)
A[0]=00b32631  B[0]=281f9e19  C[0]=7c020982  D[0]=024d410d
A[1]=f5da212f  B[1]=e81806ab  C[1]=17750db7  D[1]=caf9f84a
A[2]=abcf07df  B[2]=ba417d40  C[2]=6e875325  D[2]=61875adb
A[3]=667956cd  B[3]=3f86f357  C[3]=8d0a117c  D[3]=158ebff4
```

```
Step 16: (r=29, s= 9)
A[0]=c830f94a  B[0]=201664c6  C[0]=281f9e19  D[0]=7c020982
A[1]=4a8cc231  B[1]=febb4425  C[1]=e81806ab  D[1]=17750db7
A[2]=c1008946  B[2]=f579e0fb  C[2]=ba417d40  D[2]=6e875325
A[3]=ad92a84a  B[3]=accf2ad9  C[3]=3f86f357  D[3]=8d0a117c

Step 17: (r= 9, s=15)
A[0]=961daa89  B[0]=61f29590  C[0]=201664c6  D[0]=281f9e19
A[1]=28719c30  B[1]=19846295  C[1]=febb4425  D[1]=e81806ab
A[2]=e0b7406e  B[2]=01128d82  C[2]=f579e0fb  D[2]=ba417d40
A[3]=dae2abdf  B[3]=2550955b  C[3]=accf2ad9  D[3]=3f86f357

Step 18: (r=15, s= 5)
A[0]=8f6a3d83  B[0]=d544cb0e  C[0]=61f29590  D[0]=201664c6
A[1]=b901ce1f  B[1]=ce181438  C[1]=19846295  D[1]=febb4425
A[2]=249473b7  B[2]=a037705b  C[2]=01128d82  D[2]=f579e0fb
A[3]=8c41b3f0  B[3]=55efed71  C[3]=2550955b  D[3]=accf2ad9

Step 19: (r= 5, s=29)
A[0]=770c90dd  B[0]=ed47b071  C[0]=d544cb0e  D[0]=61f29590
A[1]=c5bf5772  B[1]=2039c3f7  C[1]=ce181438  D[1]=19846295
A[2]=32433114  B[2]=928e76e4  C[2]=a037705b  D[2]=01128d82
A[3]=05870a2d  B[3]=88367e11  C[3]=55efed71  D[3]=2550955b

Step 20: (r=29, s= 9)
A[0]=1f62ab8d  B[0]=aee1921b  C[0]=ed47b071  D[0]=d544cb0e
A[1]=16f60bd2  B[1]=58b7eaee  C[1]=2039c3f7  D[1]=ce181438
A[2]=dff2a4ca  B[2]=86486622  C[2]=928e76e4  D[2]=a037705b
A[3]=b02b5c0b  B[3]=a0b0e145  C[3]=88367e11  D[3]=55efed71

Step 21: (r= 9, s=15)
A[0]=7bcbfd42  B[0]=c5571a3e  C[0]=aee1921b  D[0]=ed47b071
A[1]=83d3a568  B[1]=ec17a42d  C[1]=58b7eaee  D[1]=2039c3f7
A[2]=f5c35075  B[2]=e54995bf  C[2]=86486622  D[2]=928e76e4
A[3]=3edf287a  B[3]=56b81760  C[3]=a0b0e145  D[3]=88367e11

Step 22: (r=15, s= 5)
A[0]=e17d3e9e  B[0]=fea13de5  C[0]=c5571a3e  D[0]=aee1921b
A[1]=36e71974  B[1]=d2b441e9  C[1]=ec17a42d  D[1]=58b7eaee
A[2]=cba08bd5  B[2]=a83afae1  C[2]=e54995bf  D[2]=86486622
A[3]=9b4606b3  B[3]=943d1f6f  C[3]=56b81760  D[3]=a0b0e145

Step 23: (r= 5, s=29)
A[0]=17c4d933  B[0]=2fa7d3dc  C[0]=fea13de5  D[0]=c5571a3e
A[1]=83ccd7ed  B[1]=dce32e86  C[1]=d2b441e9  D[1]=ec17a42d
A[2]=09ae1479  B[2]=74117ab9  C[2]=a83afae1  D[2]=e54995bf
A[3]=8acdb070  B[3]=68c0d673  C[3]=943d1f6f  D[3]=56b81760
```

```
Step 24: (r= 4, s=13)
A[0]=4d259314  B[0]=7c4d9331  C[0]=2fa7d3dc  D[0]=fea13de5
A[1]=b8b18bf5  B[1]=3ccd7ed8  C[1]=dce32e86  D[1]=d2b441e9
A[2]=c4b77690  B[2]=9ae14790  C[2]=74117ab9  D[2]=a83afae1
A[3]=cc9e908f  B[3]=acdb0708  C[3]=68c0d673  D[3]=943d1f6f

Step 25: (r=13, s=10)
A[0]=65814e93  B[0]=b26289a4  C[0]=7c4d9331  D[0]=2fa7d3dc
A[1]=5080044b  B[1]=317eb716  C[1]=3ccd7ed8  D[1]=dce32e86
A[2]=3ec45a6e  B[2]=eed21896  C[2]=9ae14790  D[2]=74117ab9
A[3]=42f9335d  B[3]=d211f993  C[3]=acdb0708  D[3]=68c0d673

Step 26: (r=10, s=25)
A[0]=9e4fc294  B[0]=053a4d96  C[0]=b26289a4  D[0]=7c4d9331
A[1]=5d44bb75  B[1]=00112d42  C[1]=317eb716  D[1]=3ccd7ed8
A[2]=06cf37ae  B[2]=1169b8fb  C[2]=eed21896  D[2]=9ae14790
A[3]=9a0c5e49  B[3]=e4cd750b  C[3]=d211f993  D[3]=acdb0708

Step 27: (r=25, s= 4)
A[0]=9021be92  B[0]=293c9f85  C[0]=053a4d96  D[0]=b26289a4
A[1]=1aa82d0d  B[1]=eaba8976  C[1]=00112d42  D[1]=317eb716
A[2]=2e596269  B[2]=5c0d9e6f  C[2]=1169b8fb  D[2]=eed21896
A[3]=b3500682  B[3]=933418bc  C[3]=e4cd750b  D[3]=d211f993

Step 28: (r= 4, s=13)
A[0]=11cb30f6  B[0]=021be929  C[0]=293c9f85  D[0]=053a4d96
A[1]=2837aec8  B[1]=aa82d0d1  C[1]=eaba8976  D[1]=00112d42
A[2]=fec28f8d  B[2]=e5962692  C[2]=5c0d9e6f  D[2]=1169b8fb
A[3]=4e188a7a  B[3]=3500682b  C[3]=933418bc  D[3]=e4cd750b

Step 29: (r=13, s=10)
A[0]=79442c32  B[0]=661ec239  C[0]=021be929  D[0]=293c9f85
A[1]=ef11854d  B[1]=f5d90506  C[1]=aa82d0d1  D[1]=eaba8976
A[2]=aca122e7  B[2]=51f1bfd8  C[2]=e5962692  D[2]=5c0d9e6f
A[3]=96e5abf3  B[3]=114f49c3  C[3]=3500682b  D[3]=933418bc

Step 30: (r=10, s=25)
A[0]=d50ecf07  B[0]=10b0c9e5  C[0]=661ec239  D[0]=021be929
A[1]=bd9b55cd  B[1]=461537bc  C[1]=f5d90506  D[1]=aa82d0d1
A[2]=83eb26ab  B[2]=848b9eb2  C[2]=51f1bfd8  D[2]=e5962692
A[3]=3791f003  B[3]=96afce5b  C[3]=114f49c3  D[3]=3500682b

Step 31: (r=25, s= 4)
A[0]=3b772524  B[0]=0faa1d9e  C[0]=10b0c9e5  D[0]=661ec239
A[1]=50ff300a  B[1]=9b7b36ab  C[1]=461537bc  D[1]=f5d90506
A[2]=088e9726  B[2]=5707d64d  C[2]=848b9eb2  D[2]=51f1bfd8
A[3]=8f5f0976  B[3]=066f23e0  C[3]=96afce5b  D[3]=114f49c3

Feed-Forward Step 32: (r= 4, s=13)
```

```
A[0]=bd2113d2  B[0]=b7725243  C[0]=0faa1d9e  D[0]=10b0c9e5
A[1]=15455066  B[1]=0ff300a5  C[1]=9b7b36ab  D[1]=461537bc
A[2]=f1c33c47  B[2]=88e97260  C[2]=5707d64d  D[2]=848b9eb2
A[3]=94fa698b  B[3]=f5f09768  C[3]=066f23e0  D[3]=96afce5b

Feed-Forward Step 33: (r=13, s=10)
A[0]=ed5b7a51  B[0]=227a57a4  C[0]=b7725243  D[0]=0faa1d9e
A[1]=3b2e3816  B[1]=aa0cc2a8  C[1]=0ff300a5  D[1]=9b7b36ab
A[2]=2c3dd5df  B[2]=6788fe38  C[2]=88e97260  D[2]=5707d64d
A[3]=57e99dda  B[3]=4d31729f  C[3]=f5f09768  D[3]=066f23e0

Feed-Forward Step 34: (r=10, s=25)
A[0]=818a2c8f  B[0]=6de947b5  C[0]=227a57a4  D[0]=b7725243
A[1]=d54e4458  B[1]=b8e058ec  C[1]=aa0cc2a8  D[1]=0ff300a5
A[2]=ce3f5c89  B[2]=f7577cb0  C[2]=6788fe38  D[2]=88e97260
A[3]=69dbdd33  B[3]=a677695f  C[3]=4d31729f  D[3]=f5f09768

Feed-Forward Step 35: (r=25, s= 4)
A[0]=c6eaeb54  B[0]=1f031459  C[0]=6de947b5  D[0]=227a57a4
A[1]=495ede58  B[1]=b1aa9c88  C[1]=b8e058ec  D[1]=aa0cc2a8
A[2]=ee6e2ce5  B[2]=139c7eb9  C[2]=f7577cb0  D[2]=6788fe38
A[3]=0289d683  B[3]=66d3b7ba  C[3]=a677695f  D[3]=4d31729f
```

Compression Function Output

```
A[0]=c6eaeb54  B[0]=1f031459  C[0]=6de947b5  D[0]=227a57a4
A[1]=495ede58  B[1]=b1aa9c88  C[1]=b8e058ec  D[1]=aa0cc2a8
A[2]=ee6e2ce5  B[2]=139c7eb9  C[2]=f7577cb0  D[2]=6788fe38
A[3]=0289d683  B[3]=66d3b7ba  C[3]=a677695f  D[3]=4d31729f
```

Final block

```
M[  0..  7] = bc 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  192  108  141  233   96  118  165  228
y[  8.. 15] =   32  222   69   67  220  239   71  167
y[ 16.. 23] =  128  193   38  144  230  170  141   22
y[ 24.. 31] =   43   18   57  253   52   49  135   90
y[ 32.. 39] =  220  141  251   80   69   78  112  146
y[ 40.. 47] =  246  192  105  151  220  224    4   25
y[ 48.. 55] =  248  255  112   48  106   24   23   60
```

```
y[ 56.. 63] =  177  160   25  225  205   82   19  141
y[ 64.. 71] =  184   11  235  143   23    1  211  148
y[ 72.. 79] =   87  154   50   52  156  137   48  209
y[ 80.. 87] =  248  183   81  232  146  206  235   97
y[ 88.. 95] =   76  101   62  123   67   70  241   29
y[ 96..103] =  156  235  125   39   50   41    7  230
y[104..111] =  130  184   14  225  156  152  115   94
y[112..119] =  128  121    7   71   13   95   96   59
y[120..127] =  199  216   94  151  171   37  100  235
```

Intermediate Expanded Message

```
Z[ 0] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
Z[ 1] = e6b51720  306b31dd  f2fee543  bef6334f
Z[ 2] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
Z[ 3] = 0d021f13  fd1c2931  23692594  410aa7d6
Z[ 4] = ac2ce543  39d0fbaa  385e31dd  afc950f0
Z[ 5] = d107f80d  b3664be1  e827e543  121102e4
Z[ 6] = fe8ef97f  22b050f0  11584c9a  2b5c109f
Z[ 7] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
Z[ 8] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
Z[ 9] = b5913edf  25942422  a948b703  dd5022b0
Z[10] = ca86f97f  edef3a89  db25afc9  4619f01a
Z[11] = 48fd36ec  58e32cce  3296306b  14f5f470
Z[12] = f01ab703  1c2f5a55  1da12422  ec7d050f
Z[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
Z[14] = 57715c80  334f050f  44a70965  2aa34560
Z[15] = e25fd616  b36643ee  1abdc1da  f01a4844
Z[16] = bd8fc4d7  ebfa966c  14ef5760  d622ac44
Z[17] = 4f2f1d20  2d823ecd  a413de53  2bb0409f
Z[18] = f7cf7480  49b92296  9af9e76d  ebfa966c
Z[19] = 452c2723  386e33e1  3cfb2f54  f17090f6
Z[20] = a413de53  71c5fa8a  2d823ecd  065f65f0
Z[21] = 8c69f5fd  0cbe5f91  a413de53  68ab03a4
Z[22] = 7480f7cf  065f65f0  0bd5607a  576014ef
Z[23] = cb36b730  558e16c1  b1bad0ac  5b04114b
Z[24] = 0a03624c  983eea28  00e96b66  9ccbe59b
Z[25] = a241e025  2f543cfb  92c8ef9e  d450ae16
Z[26] = bca6c5c0  e93f9927  d195b0d1  58491406
Z[27] = 5bed1062  6ff3fc5c  3fb62c99  1a6551ea
Z[28] = ebfa966c  237f48d0  255146fe  e76d9af9
Z[29] = bd8fc4d7  e2e09f86  a06fe1f7  558e16c1
Z[30] = 6e21fe2e  409f2bb0  567715d8  35b3369c
Z[31] = daafa7b7  9f86e2e0  21ad4aa2  ebfa966c
```

Expanded Message

```
W[ 0] = ac2ce543  39d0fbaa  385e31dd  afc950f0
W[ 1] = fe8ef97f  22b050f0  11584c9a  2b5c109f
W[ 2] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
```

```
W[ 3] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
W[ 4] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
W[ 5] = d107f80d  b3664be1  e827e543  121102e4
W[ 6] = 0d021f13  fd1c2931  23692594  410aa7d6
W[ 7] = e6b51720  306b31dd  f2fee543  bef6334f
W[ 8] = e25fd616  b36643ee  1abdc1da  f01a4844
W[ 9] = 48fd36ec  58e32cce  3296306b  14f5f470
W[10] = f01ab703  1c2f5a55  1da12422  ec7d050f
W[11] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
W[12] = b5913edf  25942422  a948b703  dd5022b0
W[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
W[14] = ca86f97f  edef3a89  db25afc9  4619f01a
W[15] = 57715c80  334f050f  44a70965  2aa34560
W[16] = 4f2f1d20  2d823ecd  a413de53  2bb0409f
W[17] = f7cf7480  49b92296  9af9e76d  ebfa966c
W[18] = cb36b730  558e16c1  b1bad0ac  5b04114b
W[19] = a413de53  71c5fa8a  2d823ecd  065f65f0
W[20] = 7480f7cf  065f65f0  0bd5607a  576014ef
W[21] = 8c69f5fd  0cbe5f91  a413de53  68ab03a4
W[22] = bd8fc4d7  ebfa966c  14ef5760  d622ac44
W[23] = 452c2723  386e33e1  3cfb2f54  f17090f6
W[24] = 6e21fe2e  409f2bb0  567715d8  35b3369c
W[25] = 0a03624c  983eea28  00e96b66  9ccbe59b
W[26] = a241e025  2f543cfb  92c8ef9e  d450ae16
W[27] = daafa7b7  9f86e2e0  21ad4aa2  ebfa966c
W[28] = 5bed1062  6ff3fc5c  3fb62c99  1a6551ea
W[29] = bd8fc4d7  e2e09f86  a06fe1f7  558e16c1
W[30] = ebfa966c  237f48d0  255146fe  e76d9af9
W[31] = bca6c5c0  e93f9927  d195b0d1  58491406
```

Feistel Steps

```
IV :
A[0]=c6eaeb54  B[0]=1f031459  C[0]=6de947b5  D[0]=227a57a4
A[1]=495ede58  B[1]=b1aa9c88  C[1]=b8e058ec  D[1]=aa0cc2a8
A[2]=ee6e2ce5  B[2]=139c7eb9  C[2]=f7577cb0  D[2]=6788fe38
A[3]=0289d683  B[3]=66d3b7ba  C[3]=a677695f  D[3]=4d31729f

IV XOR M :
A[0]=c6eae9e8  B[0]=1f031459  C[0]=6de947b5  D[0]=227a57a4
A[1]=495ede58  B[1]=b1aa9c88  C[1]=b8e058ec  D[1]=aa0cc2a8
A[2]=ee6e2ce5  B[2]=139c7eb9  C[2]=f7577cb0  D[2]=6788fe38
A[3]=0289d683  B[3]=66d3b7ba  C[3]=a677695f  D[3]=4d31729f

Step  0: (r= 3, s=23)
A[0]=ed75c7e3  B[0]=37574f46  C[0]=1f031459  D[0]=6de947b5
A[1]=b6a21373  B[1]=4af6f2c2  C[1]=b1aa9c88  D[1]=b8e058ec
A[2]=77a8366e  B[2]=7371672f  C[2]=139c7eb9  D[2]=f7577cb0
A[3]=2a436070  B[3]=144eb418  C[3]=66d3b7ba  D[3]=a677695f
```

```
Step  1: (r=23, s=17)
A[0]=68591bba  B[0]=f1f6bae3  C[0]=37574f46  D[0]=1f031459
A[1]=c962e026  B[1]=b9db5109  C[1]=4af6f2c2  D[1]=b1aa9c88
A[2]=6209b2ab  B[2]=373bd41b  C[2]=7371672f  D[2]=139c7eb9
A[3]=1d0b7e55  B[3]=381521b0  C[3]=144eb418  D[3]=66d3b7ba

Step  2: (r=17, s=27)
A[0]=33cd6c38  B[0]=3774d0b2  C[0]=f1f6bae3  D[0]=37574f46
A[1]=06b810ee  B[1]=c04d92c5  C[1]=b9db5109  D[1]=4af6f2c2
A[2]=0530778e  B[2]=6556c413  C[2]=373bd41b  D[2]=7371672f
A[3]=eac5f95c  B[3]=fcaa3a16  C[3]=381521b0  D[3]=144eb418

Step  3: (r=27, s= 3)
A[0]=54a9b656  B[0]=c19e6b61  C[0]=3774d0b2  D[0]=f1f6bae3
A[1]=56696b4e  B[1]=7035c087  C[1]=c04d92c5  D[1]=b9db5109
A[2]=44ceedc5  B[2]=702983bc  C[2]=6556c413  D[2]=373bd41b
A[3]=56564b7c  B[3]=e7562fca  C[3]=fcaa3a16  D[3]=381521b0

Step  4: (r= 3, s=23)
A[0]=e8f83be3  B[0]=a54db2b2  C[0]=c19e6b61  D[0]=3774d0b2
A[1]=a3abf074  B[1]=b34b5a72  C[1]=7035c087  D[1]=c04d92c5
A[2]=b3b9196c  B[2]=26776e2a  C[2]=702983bc  D[2]=6556c413
A[3]=1838a61f  B[3]=b2b25be2  C[3]=e7562fca  D[3]=fcaa3a16

Step  5: (r=23, s=17)
A[0]=18d1f105  B[0]=f1f47c1d  C[0]=a54db2b2  D[0]=c19e6b61
A[1]=14922a4b  B[1]=3a51d5f8  C[1]=b34b5a72  D[1]=7035c087
A[2]=a356d567  B[2]=b659dc8c  C[2]=26776e2a  D[2]=702983bc
A[3]=cb7dfdf7  B[3]=0f8c1c53  C[3]=b2b25be2  D[3]=e7562fca

Step  6: (r=17, s=27)
A[0]=a099dcf8  B[0]=e20a31a3  C[0]=f1f47c1d  D[0]=a54db2b2
A[1]=77075bc4  B[1]=54962924  C[1]=3a51d5f8  D[1]=b34b5a72
A[2]=edbeeb26  B[2]=aacf46ad  C[2]=b659dc8c  D[2]=26776e2a
A[3]=48703059  B[3]=fbef96fb  C[3]=0f8c1c53  D[3]=b2b25be2

Step  7: (r=27, s= 3)
A[0]=9c482bb4  B[0]=c504cee7  C[0]=e20a31a3  D[0]=f1f47c1d
A[1]=98b2b31c  B[1]=23b83ade  C[1]=54962924  D[1]=3a51d5f8
A[2]=07b5dfb5  B[2]=376df759  C[2]=aacf46ad  D[2]=b659dc8c
A[3]=105d5743  B[3]=ca438182  C[3]=fbef96fb  D[3]=0f8c1c53

Step  8: (r=28, s=19)
A[0]=97dba827  B[0]=49c482bb  C[0]=c504cee7  D[0]=e20a31a3
A[1]=f18cf15d  B[1]=c98b2b31  C[1]=23b83ade  D[1]=54962924
A[2]=75872f6c  B[2]=507b5dfb  C[2]=376df759  D[2]=aacf46ad
A[3]=7c53df0a  B[3]=3105d574  C[3]=ca438182  D[3]=fbef96fb
```

```
Step  9: (r=19, s=22)
A[0]=678abf72  B[0]=413cbedd  C[0]=49c482bb  D[0]=c504cee7
A[1]=a2990b3d  B[1]=8aef8c67  C[1]=c98b2b31  D[1]=23b83ade
A[2]=1c9fd6f3  B[2]=7b63ac39  C[2]=507b5dfb  D[2]=376df759
A[3]=b6546611  B[3]=f853e29e  C[3]=3105d574  D[3]=ca438182

Step 10: (r=22, s= 7)
A[0]=f2e989f4  B[0]=dc99e2af  C[0]=413cbedd  D[0]=49c482bb
A[1]=3dcc411e  B[1]=cf68a642  C[1]=8aef8c67  D[1]=c98b2b31
A[2]=95ee3d05  B[2]=bcc727f5  C[2]=7b63ac39  D[2]=507b5dfb
A[3]=d8a5a8f6  B[3]=846d9519  C[3]=f853e29e  D[3]=3105d574

Step 11: (r= 7, s=28)
A[0]=c509dbb6  B[0]=74c4fa79  C[0]=dc99e2af  D[0]=413cbedd
A[1]=d787dd44  B[1]=e6208f1e  C[1]=cf68a642  D[1]=8aef8c67
A[2]=5b20505b  B[2]=f71e82ca  C[2]=bcc727f5  D[2]=7b63ac39
A[3]=5cf091dd  B[3]=52d47b6c  C[3]=846d9519  D[3]=f853e29e

Step 12: (r=28, s=19)
A[0]=1156d893  B[0]=6c509dbb  C[0]=74c4fa79  D[0]=dc99e2af
A[1]=6acc5adc  B[1]=4d787dd4  C[1]=e6208f1e  D[1]=cf68a642
A[2]=068826b0  B[2]=b5b20505  C[2]=f71e82ca  D[2]=bcc727f5
A[3]=6b0b59c9  B[3]=d5cf091d  C[3]=52d47b6c  D[3]=846d9519

Step 13: (r=19, s=22)
A[0]=1e473fd8  B[0]=c4988ab6  C[0]=6c509dbb  D[0]=74c4fa79
A[1]=dd55049e  B[1]=d6e35662  C[1]=4d787dd4  D[1]=e6208f1e
A[2]=22a2aaef  B[2]=35803441  C[2]=b5b20505  D[2]=f71e82ca
A[3]=372a6132  B[3]=ce4b585a  C[3]=d5cf091d  D[3]=52d47b6c

Step 14: (r=22, s= 7)
A[0]=1ad7a3dd  B[0]=f60791cf  C[0]=c4988ab6  D[0]=6c509dbb
A[1]=7c57e782  B[1]=27b75541  C[1]=d6e35662  D[1]=4d787dd4
A[2]=1ae2c144  B[2]=bbc8a8aa  C[2]=35803441  D[2]=b5b20505
A[3]=12e1e207  B[3]=4c8dca98  C[3]=ce4b585a  D[3]=d5cf091d

Step 15: (r= 7, s=28)
A[0]=d599591f  B[0]=6bd1ee8d  C[0]=f60791cf  D[0]=c4988ab6
A[1]=cb4ddc2f  B[1]=2bf3c13e  C[1]=27b75541  D[1]=d6e35662
A[2]=14529e73  B[2]=7160a20d  C[2]=bbc8a8aa  D[2]=35803441
A[3]=e6546396  B[3]=70f10389  C[3]=4c8dca98  D[3]=ce4b585a

Step 16: (r=29, s= 9)
A[0]=216b9abc  B[0]=fab32b23  C[0]=6bd1ee8d  D[0]=f60791cf
A[1]=8f77c6da  B[1]=f969bb85  C[1]=2bf3c13e  D[1]=27b75541
A[2]=b41d664d  B[2]=628a53ce  C[2]=7160a20d  D[2]=bbc8a8aa
A[3]=a3b2be4a  B[3]=dcca8c72  C[3]=70f10389  D[3]=4c8dca98

Step 17: (r= 9, s=15)
```

```
A[0]=9fb4c18c  B[0]=d7357842  C[0]=fab32b23  D[0]=6bd1ee8d
A[1]=388a2910  B[1]=ef8db51e  C[1]=f969bb85  D[1]=2bf3c13e
A[2]=98bf9133  B[2]=3acc9b68  C[2]=628a53ce  D[2]=7160a20d
A[3]=ce98fce7  B[3]=657c9547  C[3]=dcca8c72  D[3]=70f10389

Step 18: (r=15, s= 5)
A[0]=dc8a184a  B[0]=60c64fda  C[0]=d7357842  D[0]=fab32b23
A[1]=ce37c267  B[1]=14881c45  C[1]=ef8db51e  D[1]=f969bb85
A[2]=337cbbff  B[2]=c899cc5f  C[2]=3acc9b68  D[2]=628a53ce
A[3]=d28ef1c3  B[3]=7e73e74c  C[3]=657c9547  D[3]=dcca8c72

Step 19: (r= 5, s=29)
A[0]=8be74e1e  B[0]=9143095b  C[0]=60c64fda  D[0]=d7357842
A[1]=e3f535e7  B[1]=c6f84cf9  C[1]=14881c45  D[1]=ef8db51e
A[2]=e457acba  B[2]=6f977fe6  C[2]=c899cc5f  D[2]=3acc9b68
A[3]=924be7ed  B[3]=51de387a  C[3]=7e73e74c  D[3]=657c9547

Step 20: (r=29, s= 9)
A[0]=adc85497  B[0]=d17ce9c3  C[0]=9143095b  D[0]=60c64fda
A[1]=26fadd10  B[1]=fc7ea6bc  C[1]=c6f84cf9  D[1]=14881c45
A[2]=70506722  B[2]=5c8af597  C[2]=6f977fe6  D[2]=c899cc5f
A[3]=42a02de1  B[3]=b2497cfd  C[3]=51de387a  D[3]=7e73e74c

Step 21: (r= 9, s=15)
A[0]=3d8f5f89  B[0]=90a92f5b  C[0]=d17ce9c3  D[0]=9143095b
A[1]=34f0337b  B[1]=f5ba204d  C[1]=fc7ea6bc  D[1]=c6f84cf9
A[2]=51883725  B[2]=a0ce44e0  C[2]=5c8af597  D[2]=6f977fe6
A[3]=34c2e1d3  B[3]=405bc285  C[3]=b2497cfd  D[3]=51de387a

Step 22: (r=15, s= 5)
A[0]=2b9a6880  B[0]=afc49ec7  C[0]=90a92f5b  D[0]=d17ce9c3
A[1]=6e8a56b5  B[1]=19bd9a78  C[1]=f5ba204d  D[1]=fc7ea6bc
A[2]=51ee3c41  B[2]=1b92a8c4  C[2]=a0ce44e0  D[2]=5c8af597
A[3]=23564ce3  B[3]=70e99a61  C[3]=405bc285  D[3]=b2497cfd

Step 23: (r= 5, s=29)
A[0]=a30fc459  B[0]=734d1005  C[0]=afc49ec7  D[0]=90a92f5b
A[1]=941c65cd  B[1]=d14ad6ad  C[1]=19bd9a78  D[1]=f5ba204d
A[2]=46b560e2  B[2]=3dc7882a  C[2]=1b92a8c4  D[2]=a0ce44e0
A[3]=f3cfcb1f  B[3]=6ac99c64  C[3]=70e99a61  D[3]=405bc285

Step 24: (r= 4, s=13)
A[0]=4ac862ac  B[0]=30fc459a  C[0]=734d1005  D[0]=afc49ec7
A[1]=96539f9a  B[1]=41c65cd9  C[1]=d14ad6ad  D[1]=19bd9a78
A[2]=d9587498  B[2]=6b560e24  C[2]=3dc7882a  D[2]=1b92a8c4
A[3]=7d86c943  B[3]=3cfcb1ff  C[3]=6ac99c64  D[3]=70e99a61

Step 25: (r=13, s=10)
A[0]=63d98ed9  B[0]=0c558959  C[0]=30fc459a  D[0]=734d1005
```

```
A[1]=f4ade77d  B[1]=73f352ca  C[1]=41c65cd9  D[1]=d14ad6ad
A[2]=5ad6bb82  B[2]=0e931b2b  C[2]=6b560e24  D[2]=3dc7882a
A[3]=8048dffc  B[3]=d9286fb0  C[3]=3cfcb1ff  D[3]=6ac99c64

Step 26: (r=10, s=25)
A[0]=2dcbfb74  B[0]=663b658f  C[0]=0c558959  D[0]=30fc459a
A[1]=3bd30e47  B[1]=b79df7d2  C[1]=73f352ca  D[1]=41c65cd9
A[2]=95963cff  B[2]=5aee096b  C[2]=0e931b2b  D[2]=6b560e24
A[3]=c2331303  B[3]=237ff201  C[3]=d9286fb0  D[3]=3cfcb1ff

Step 27: (r=25, s= 4)
A[0]=8b2c8bfe  B[0]=e85b97f6  C[0]=663b658f  D[0]=0c558959
A[1]=3845002b  B[1]=8e77a61c  C[1]=b79df7d2  D[1]=73f352ca
A[2]=802aa940  B[2]=ff2b2c79  C[2]=5aee096b  D[2]=0e931b2b
A[3]=42579e3d  B[3]=07846626  C[3]=237ff201  D[3]=d9286fb0

Step 28: (r= 4, s=13)
A[0]=c6e1be57  B[0]=b2c8bfe8  C[0]=e85b97f6  D[0]=663b658f
A[1]=c421f81b  B[1]=845002b3  C[1]=8e77a61c  D[1]=b79df7d2
A[2]=20ee64f6  B[2]=02aa9408  C[2]=ff2b2c79  D[2]=5aee096b
A[3]=3b48018f  B[3]=2579e3d4  C[3]=07846626  D[3]=237ff201

Step 29: (r=13, s=10)
A[0]=53db5783  B[0]=37caf8dc  C[0]=b2c8bfe8  D[0]=e85b97f6
A[1]=8d849098  B[1]=3f037884  C[1]=845002b3  D[1]=8e77a61c
A[2]=5f42e0fc  B[2]=cc9ec41d  C[2]=02aa9408  D[2]=ff2b2c79
A[3]=917c1b5d  B[3]=0031e769  C[3]=2579e3d4  D[3]=07846626

Step 30: (r=10, s=25)
A[0]=6652a492  B[0]=6d5e0d4f  C[0]=37caf8dc  D[0]=b2c8bfe8
A[1]=65dbfb4d  B[1]=12426236  C[1]=3f037884  D[1]=845002b3
A[2]=175384b4  B[2]=0b83f17d  C[2]=cc9ec41d  D[2]=02aa9408
A[3]=0564c945  B[3]=f06d7645  C[3]=0031e769  D[3]=2579e3d4

Step 31: (r=25, s= 4)
A[0]=d4d1cf76  B[0]=24cca549  C[0]=6d5e0d4f  D[0]=37caf8dc
A[1]=d73c277c  B[1]=9acbb7f6  C[1]=12426236  D[1]=3f037884
A[2]=620d36b7  B[2]=682ea709  C[2]=0b83f17d  D[2]=cc9ec41d
A[3]=7d59a9ed  B[3]=8a0ac992  C[3]=f06d7645  D[3]=0031e769

Feed-Forward Step 32: (r= 4, s=13)
A[0]=62c9c467  B[0]=4d1cf76d  C[0]=24cca549  D[0]=6d5e0d4f
A[1]=b89daecb  B[1]=73c277cd  C[1]=9acbb7f6  D[1]=12426236
A[2]=eecbdc60  B[2]=20d36b76  C[2]=682ea709  D[2]=0b83f17d
A[3]=60ca88ca  B[3]=d59a9ed7  C[3]=8a0ac992  D[3]=f06d7645

Feed-Forward Step 33: (r=13, s=10)
A[0]=6df5ce54  B[0]=388cec59  C[0]=4d1cf76d  D[0]=24cca549
A[1]=f567dc33  B[1]=b5d97713  C[1]=73c277cd  D[1]=9acbb7f6
```

```
A[2]=7087c919  B[2]=7b8c1dd9  C[2]=20d36b76  D[2]=682ea709
A[3]=ab6b6260  B[3]=51194c19  C[3]=d59a9ed7  D[3]=8a0ac992

Feed-Forward Step 34: (r=10, s=25)
A[0]=0e9aeb96  B[0]=d73951b7  C[0]=388cec59  D[0]=4d1cf76d
A[1]=2fa05dbe  B[1]=9f70cfd5  C[1]=b5d97713  D[1]=73c277cd
A[2]=48da0655  B[2]=1f2465c2  C[2]=7b8c1dd9  D[2]=20d36b76
A[3]=b07d07f4  B[3]=ad8982ad  C[3]=51194c19  D[3]=d59a9ed7

Feed-Forward Step 35: (r=25, s= 4)
A[0]=449a4919  B[0]=2c1d35d7  C[0]=d73951b7  D[0]=388cec59
A[1]=7f1c54b7  B[1]=7c5f40bb  C[1]=9f70cfd5  D[1]=b5d97713
A[2]=b267b827  B[2]=aa91b40c  C[2]=1f2465c2  D[2]=7b8c1dd9
A[3]=6972f807  B[3]=e960fa0f  C[3]=ad8982ad  D[3]=51194c19
```

Compression Function Output

```
A[0]=449a4919  B[0]=2c1d35d7  C[0]=d73951b7  D[0]=388cec59
A[1]=7f1c54b7  B[1]=7c5f40bb  C[1]=9f70cfd5  D[1]=b5d97713
A[2]=b267b827  B[2]=aa91b40c  C[2]=1f2465c2  D[2]=7b8c1dd9
A[3]=6972f807  B[3]=e960fa0f  C[3]=ad8982ad  D[3]=51194c19
```

Hash Function Output

```
19499a44b7541c7f27b867b207f87269d7351d2cbb405f7c0cb491aa
```

A.2 SIMD-256

A.2.1 Empty Message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    2  156  118  107   45  212  111  162
y[  8.. 15] =   97  249  211    3   49  101  151  223
y[ 16.. 23] =  189  178  253  204   76   82  232   65
y[ 24.. 31] =   96  176  161   47  189   61  248  107
```

```
y[ 32.. 39] =    0  131  133  113   17   33   12  111
y[ 40.. 47] =  251  103   57  148   47   65  249  143
y[ 48.. 55] =  189    8  204  230  205  151  187  227
y[ 56.. 63] =  247  111  140    6   77   10   21  149
y[ 64.. 71] =  255  101  139  150  212   45  146   95
y[ 72.. 79] =  160    8   46  254  208  156  106   34
y[ 80.. 87] =   68   79    4   53  181  175   25  192
y[ 88.. 95] =  161   81   96  210   68  196    9  150
y[ 96..103] =    0  126  124  144  240  224  245  146
y[104..111] =    6  154  200  109  210  192    8  114
y[112..119] =   68  249   53   27   52  106   70   30
y[120..127] =   10  146  117  251  180  247  236  108
```

Intermediate Expanded Message

```
Z[ 0] = b7030172  4d535546  df7b2085  bb595037
Z[ 1] = fa384619  022bdec2  48fd2369  e76eb366
Z[ 2] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
Z[ 3] = c5774560  21f7baa0  2c15cedc  4d53f97f
Z[ 4] = a4f20000  51a9a664  17d90c49  503708ac
Z[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
Z[ 6] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
Z[ 7] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
Z[ 8] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
Z[ 9] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
Z[10] = 39173124  264d02e4  c4bec914  d1071211
Z[11] = 3a89baa0  de094560  d3eb3124  b2ad0681
Z[12] = 5b0e0000  ae57599c  e827f3b7  afc9f754
Z[13] = b5910456  4ec5d6cf  d107de09  526205c8
Z[14] = fa383124  1383264d  4c9a2594  15ae3296
Z[15] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
Z[16] = fe2e01d2  949a6b66  d70b28f5  9af96507
Z[17] = a7b75849  29ded622  d3672c99  607a9f86
Z[18] = 3de4c21c  03a4fc5c  bad4452c  16c1e93f
Z[19] = a8a05760  5760a8a0  3de4c21c  0831f7cf
Z[20] = 00000000  70dc8f24  f0870f79  f5140aec
Z[21] = 0576fa8a  cc1f33e1  d5392ac7  0748f8b8
Z[22] = 3de4c21c  303dcfc3  2f54d0ac  3fb6c04a
Z[23] = 091af6e6  6a7d9583  b9eb4615  ece3131d
Z[24] = 5beda413  9e9d6163  28f5d70b  5677a989
Z[25] = 0748f8b8  fd4502bb  a4135bed  1ef2e10e
Z[26] = 47e7b819  303dcfc3  b55e4aa2  c4d73b29
Z[27] = 49b9b647  d5392ac7  c87b3785  9e9d6163
Z[28] = 72ae8d52  992766d9  e1f71e09  9af96507
Z[29] = a2415dbf  63359ccb  c4d73b29  67c2983e
Z[30] = f8b80748  1893e76d  607a9f86  1b4ee4b2
Z[31] = 9af96507  fa8a0576  f6e6091a  624c9db4
```

Expanded Message

```
W[ 0] = a4f20000  51a9a664  17d90c49  503708ac
W[ 1] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
W[ 2] = b7030172  4d535546  df7b2085  bb595037
W[ 3] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
W[ 4] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
W[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
W[ 6] = c5774560  21f7baa0  2c15cedc  4d53f97f
W[ 7] = fa384619  022bdec2  48fd2369  e76eb366
W[ 8] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
W[ 9] = 3a89baa0  de094560  d3eb3124  b2ad0681
W[10] = 5b0e0000  ae57599c  e827f3b7  afc9f754
W[11] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
W[12] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
W[13] = b5910456  4ec5d6cf  d107de09  526205c8
W[14] = 39173124  264d02e4  c4bec914  d1071211
W[15] = fa383124  1383264d  4c9a2594  15ae3296
W[16] = a7b75849  29ded622  d3672c99  607a9f86
W[17] = 3de4c21c  03a4fc5c  bad4452c  16c1e93f
W[18] = 091af6e6  6a7d9583  b9eb4615  ece3131d
W[19] = 00000000  70dc8f24  f0870f79  f5140aec
W[20] = 3de4c21c  303dcfc3  2f54d0ac  3fb6c04a
W[21] = 0576fa8a  cc1f33e1  d5392ac7  0748f8b8
W[22] = fe2e01d2  949a6b66  d70b28f5  9af96507
W[23] = a8a05760  5760a8a0  3de4c21c  0831f7cf
W[24] = f8b80748  1893e76d  607a9f86  1b4ee4b2
W[25] = 5beda413  9e9d6163  28f5d70b  5677a989
W[26] = 0748f8b8  fd4502bb  a4135bed  1ef2e10e
W[27] = 9af96507  fa8a0576  f6e6091a  624c9db4
W[28] = 49b9b647  d5392ac7  c87b3785  9e9d6163
W[29] = a2415dbf  63359ccb  c4d73b29  67c2983e
W[30] = 72ae8d52  992766d9  e1f71e09  9af96507
W[31] = 47e7b819  303dcfc3  b55e4aa2  c4d73b29
```

Feistel Steps

```
IV :
A[0]=4d567983  B[0]=aaf3d925  C[0]=c2c2ba14  D[0]=e2eaa8d2
A[1]=07190ba9  B[1]=3ee20b03  C[1]=49b3bcb4  D[1]=1ff47833
A[2]=8474577b  B[2]=afd5e751  C[2]=f67caf46  D[2]=d0c661a5
A[3]=39d726e9  B[3]=c96006d3  C[3]=668626c9  D[3]=55693de1

IV XOR M :
A[0]=4d567983  B[0]=aaf3d925  C[0]=c2c2ba14  D[0]=e2eaa8d2
A[1]=07190ba9  B[1]=3ee20b03  C[1]=49b3bcb4  D[1]=1ff47833
A[2]=8474577b  B[2]=afd5e751  C[2]=f67caf46  D[2]=d0c661a5
A[3]=39d726e9  B[3]=c96006d3  C[3]=668626c9  D[3]=55693de1

Step  0: (r= 3, s=23)
A[0]=2c51b509  B[0]=6ab3cc1a  C[0]=aaf3d925  D[0]=c2c2ba14
```

```
A[1]=4113ec88  B[1]=38c85d48  C[1]=3ee20b03  D[1]=49b3bcb4
A[2]=70a8b577  B[2]=23a2bbdc  C[2]=afd5e751  D[2]=f67caf46
A[3]=cb1d2c02  B[3]=ceb93749  C[3]=c96006d3  D[3]=668626c9

Step  1: (r=23, s=17)
A[0]=65f13ad8  B[0]=849628da  C[0]=6ab3cc1a  D[0]=aaf3d925
A[1]=cc4a78b9  B[1]=442089f6  C[1]=38c85d48  D[1]=3ee20b03
A[2]=7ea2dc8c  B[2]=bbb8545a  C[2]=23a2bbdc  D[2]=afd5e751
A[3]=7a28c09a  B[3]=01658e96  C[3]=ceb93749  D[3]=c96006d3

Step  2: (r=17, s=27)
A[0]=0cb9428c  B[0]=75b0cbe2  C[0]=849628da  D[0]=6ab3cc1a
A[1]=811ea8b6  B[1]=f1739894  C[1]=442089f6  D[1]=38c85d48
A[2]=67cb248d  B[2]=b918fd45  C[2]=bbb8545a  D[2]=23a2bbdc
A[3]=5dfc2458  B[3]=8134f451  C[3]=01658e96  D[3]=ceb93749

Step  3: (r=27, s= 3)
A[0]=66a9238a  B[0]=6065ca14  C[0]=75b0cbe2  D[0]=849628da
A[1]=1ddcebda  B[1]=b408f545  C[1]=f1739894  D[1]=442089f6
A[2]=83db1a1a  B[2]=6b3e5924  C[2]=b918fd45  D[2]=bbb8545a
A[3]=6284f99b  B[3]=c2efe122  C[3]=8134f451  D[3]=01658e96

Step  4: (r= 3, s=23)
A[0]=aff588ca  B[0]=35491c53  C[0]=6065ca14  D[0]=75b0cbe2
A[1]=b326b4f2  B[1]=eee75ed0  C[1]=b408f545  D[1]=f1739894
A[2]=b70022c5  B[2]=1ed8d0d4  C[2]=6b3e5924  D[2]=b918fd45
A[3]=5a225e17  B[3]=1427ccdb  C[3]=c2efe122  D[3]=8134f451

Step  5: (r=23, s=17)
A[0]=ab6adc3b  B[0]=6557fac4  C[0]=35491c53  D[0]=6065ca14
A[1]=d00631bc  B[1]=7959935a  C[1]=eee75ed0  D[1]=b408f545
A[2]=5959e1ae  B[2]=62db8011  C[2]=1ed8d0d4  D[2]=6b3e5924
A[3]=da90fcbb  B[3]=0bad112f  C[3]=1427ccdb  D[3]=c2efe122

Step  6: (r=17, s=27)
A[0]=9dd2e76a  B[0]=b87756d5  C[0]=6557fac4  D[0]=35491c53
A[1]=a6e994f2  B[1]=6379a00c  C[1]=7959935a  D[1]=eee75ed0
A[2]=a1092465  B[2]=c35cb2b3  C[2]=62db8011  D[2]=1ed8d0d4
A[3]=a4b4006d  B[3]=f977b521  C[3]=0bad112f  D[3]=1427ccdb

Step  7: (r=27, s= 3)
A[0]=93d312aa  B[0]=54ee973b  C[0]=b87756d5  D[0]=6557fac4
A[1]=118c0f65  B[1]=95374ca7  C[1]=6379a00c  D[1]=7959935a
A[2]=ae6b3aad  B[2]=2d084923  C[2]=c35cb2b3  D[2]=62db8011
A[3]=bf93d81c  B[3]=6d25a003  C[3]=f977b521  D[3]=0bad112f

Step  8: (r=28, s=19)
A[0]=8fe3adbb  B[0]=a93d312a  C[0]=54ee973b  D[0]=b87756d5
A[1]=7b8df776  B[1]=5118c0f6  C[1]=95374ca7  D[1]=6379a00c
```

```
A[2]=d61706ec  B[2]=dae6b3aa  C[2]=2d084923  D[2]=c35cb2b3
A[3]=e25b6a27  B[3]=cbf93d81  C[3]=6d25a003  D[3]=f977b521

Step  9: (r=19, s=22)
A[0]=e3a6e800  B[0]=6ddc7f1d  C[0]=a93d312a  D[0]=54ee973b
A[1]=06a22e88  B[1]=bbb3dc6f  C[1]=5118c0f6  D[1]=95374ca7
A[2]=31e3a866  B[2]=3766b0b8  C[2]=dae6b3aa  D[2]=2d084923
A[3]=20459950  B[3]=513f12db  C[3]=cbf93d81  D[3]=6d25a003

Step 10: (r=22, s= 7)
A[0]=e694ab76  B[0]=0038e9ba  C[0]=6ddc7f1d  D[0]=a93d312a
A[1]=f8c17231  B[1]=a201a88b  C[1]=bbb3dc6f  D[1]=5118c0f6
A[2]=4bb12ac2  B[2]=198c78ea  C[2]=3766b0b8  D[2]=dae6b3aa
A[3]=f867bcff  B[3]=54081166  C[3]=513f12db  D[3]=cbf93d81

Step 11: (r= 7, s=28)
A[0]=7397c2cb  B[0]=4a55bb73  C[0]=0038e9ba  D[0]=6ddc7f1d
A[1]=d30502a4  B[1]=60b918fc  C[1]=a201a88b  D[1]=bbb3dc6f
A[2]=544c4dbd  B[2]=d8956125  C[2]=198c78ea  D[2]=3766b0b8
A[3]=50714b6e  B[3]=33de7ffc  C[3]=54081166  D[3]=513f12db

Step 12: (r=28, s=19)
A[0]=752dfe03  B[0]=b7397c2c  C[0]=4a55bb73  D[0]=0038e9ba
A[1]=ea06587c  B[1]=4d30502a  C[1]=60b918fc  D[1]=a201a88b
A[2]=9ce94c6d  B[2]=d544c4db  C[2]=d8956125  D[2]=198c78ea
A[3]=ac629628  B[3]=e50714b6  C[3]=33de7ffc  D[3]=54081166

Step 13: (r=19, s=22)
A[0]=70382945  B[0]=f01ba96f  C[0]=b7397c2c  D[0]=4a55bb73
A[1]=a6dba109  B[1]=c3e75032  C[1]=4d30502a  D[1]=60b918fc
A[2]=c84d7fd5  B[2]=636ce74a  C[2]=d544c4db  D[2]=d8956125
A[3]=3e7a3c3d  B[3]=b1456314  C[3]=e50714b6  D[3]=33de7ffc

Step 14: (r=22, s= 7)
A[0]=e25aa0c8  B[0]=515c0e0a  C[0]=f01ba96f  D[0]=b7397c2c
A[1]=72281886  B[1]=4269b6e8  C[1]=c3e75032  D[1]=4d30502a
A[2]=92f2c117  B[2]=f572135f  C[2]=636ce74a  D[2]=d544c4db
A[3]=67bf2ee7  B[3]=0f4f9e8f  C[3]=b1456314  D[3]=e50714b6

Step 15: (r= 7, s=28)
A[0]=be290892  B[0]=2d506471  C[0]=515c0e0a  D[0]=f01ba96f
A[1]=c7822ce2  B[1]=140c4339  C[1]=4269b6e8  D[1]=c3e75032
A[2]=c0ec8e8f  B[2]=79608bc9  C[2]=f572135f  D[2]=636ce74a
A[3]=ab80d326  B[3]=df9773b3  C[3]=0f4f9e8f  D[3]=b1456314

Step 16: (r=29, s= 9)
A[0]=462d31db  B[0]=57c52112  C[0]=2d506471  D[0]=515c0e0a
A[1]=34e11448  B[1]=58f0459c  C[1]=140c4339  D[1]=4269b6e8
A[2]=e5249a6a  B[2]=f81d91d1  C[2]=79608bc9  D[2]=f572135f
```

```
A[3]=77b4d0df  B[3]=d5701a64  C[3]=df9773b3  D[3]=0f4f9e8f

Step 17: (r= 9, s=15)
A[0]=844e3e3a  B[0]=5a63b68c  C[0]=57c52112  D[0]=2d506471
A[1]=c6738147  B[1]=c2289069  C[1]=58f0459c  D[1]=140c4339
A[2]=374ee4ae  B[2]=4934d5ca  C[2]=f81d91d1  D[2]=79608bc9
A[3]=b7fcb82e  B[3]=69a1beef  C[3]=d5701a64  D[3]=df9773b3

Step 18: (r=15, s= 5)
A[0]=06762f2a  B[0]=1f1d4227  C[0]=5a63b68c  D[0]=57c52112
A[1]=4470f4d2  B[1]=c0a3e339  C[1]=c2289069  D[1]=58f0459c
A[2]=e84c533d  B[2]=72571ba7  C[2]=4934d5ca  D[2]=f81d91d1
A[3]=35bf436c  B[3]=5c175bfe  C[3]=69a1beef  D[3]=d5701a64

Step 19: (r= 5, s=29)
A[0]=2045be34  B[0]=cec5e540  C[0]=1f1d4227  D[0]=5a63b68c
A[1]=e9672425  B[1]=8e1e9a48  C[1]=c0a3e339  D[1]=c2289069
A[2]=f8090c66  B[2]=098a67bd  C[2]=72571ba7  D[2]=4934d5ca
A[3]=72f21eef  B[3]=b7e86d86  C[3]=5c175bfe  D[3]=69a1beef

Step 20: (r=29, s= 9)
A[0]=0b1bdd2a  B[0]=8408b7c6  C[0]=cec5e540  D[0]=1f1d4227
A[1]=fb05cd01  B[1]=bd2ce484  C[1]=8e1e9a48  D[1]=c0a3e339
A[2]=e6992065  B[2]=df01218c  C[2]=098a67bd  D[2]=72571ba7
A[3]=19c70606  B[3]=ee5e43dd  C[3]=b7e86d86  D[3]=5c175bfe

Step 21: (r= 9, s=15)
A[0]=2493dd45  B[0]=37ba5416  C[0]=8408b7c6  D[0]=cec5e540
A[1]=294779fd  B[1]=0b9a03f6  C[1]=bd2ce484  D[1]=8e1e9a48
A[2]=421997bf  B[2]=3240cbcd  C[2]=df01218c  D[2]=098a67bd
A[3]=805edd64  B[3]=8e0c0c33  C[3]=ee5e43dd  D[3]=b7e86d86

Step 22: (r=15, s= 5)
A[0]=fdb72c2a  B[0]=eea29249  C[0]=37ba5416  D[0]=8408b7c6
A[1]=e79f3478  B[1]=bcfe94a3  C[1]=0b9a03f6  D[1]=bd2ce484
A[2]=41851a2f  B[2]=cbdfa10c  C[2]=3240cbcd  D[2]=df01218c
A[3]=e50294ff  B[3]=6eb2402f  C[3]=8e0c0c33  D[3]=ee5e43dd

Step 23: (r= 5, s=29)
A[0]=a5de0462  B[0]=b6e5855f  C[0]=eea29249  D[0]=37ba5416
A[1]=0928ba2a  B[1]=f3e68f1c  C[1]=bcfe94a3  D[1]=0b9a03f6
A[2]=9ffbfcf2  B[2]=30a345e8  C[2]=cbdfa10c  D[2]=3240cbcd
A[3]=3377cd5c  B[3]=a0529ffc  C[3]=6eb2402f  D[3]=8e0c0c33

Step 24: (r= 4, s=13)
A[0]=70c0c68a  B[0]=5de0462a  C[0]=b6e5855f  D[0]=eea29249
A[1]=ed1de16e  B[1]=928ba2a0  C[1]=f3e68f1c  D[1]=bcfe94a3
A[2]=8da4d22f  B[2]=ffbfcf29  C[2]=30a345e8  D[2]=cbdfa10c
A[3]=af8c51ee  B[3]=377cd5c3  C[3]=a0529ffc  D[3]=6eb2402f
```

```
Step 25: (r=13, s=10)
A[0]=703cde39  B[0]=18d14e18  C[0]=5de0462a  D[0]=b6e5855f
A[1]=a8ceb1ab  B[1]=bc2ddda3  C[1]=928ba2a0  D[1]=f3e68f1c
A[2]=0dd150e1  B[2]=9a45f1b4  C[2]=ffbfcf29  D[2]=30a345e8
A[3]=df540955  B[3]=8a3dd5f1  C[3]=377cd5c3  D[3]=a0529ffc

Step 26: (r=10, s=25)
A[0]=b3dd5515  B[0]=f378e5c0  C[0]=18d14e18  D[0]=5de0462a
A[1]=3a99f681  B[1]=3ac6aea3  C[1]=bc2ddda3  D[1]=928ba2a0
A[2]=3664fba5  B[2]=45438437  C[2]=9a45f1b4  D[2]=ffbfcf29
A[3]=ae4bea6d  B[3]=5025577d  C[3]=8a3dd5f1  D[3]=377cd5c3

Step 27: (r=25, s= 4)
A[0]=4594d788  B[0]=2b67baaa  C[0]=f378e5c0  D[0]=18d14e18
A[1]=e70d363e  B[1]=027533ed  C[1]=3ac6aea3  D[1]=bc2ddda3
A[2]=09d21f5c  B[2]=4a6cc9f7  C[2]=45438437  D[2]=9a45f1b4
A[3]=ea598140  B[3]=db5c97d4  C[3]=5025577d  D[3]=8a3dd5f1

Step 28: (r= 4, s=13)
A[0]=9c9eee7f  B[0]=594d7884  C[0]=2b67baaa  D[0]=f378e5c0
A[1]=2d7b4a83  B[1]=70d363ee  C[1]=027533ed  D[1]=3ac6aea3
A[2]=d0238e04  B[2]=9d21f5c0  C[2]=4a6cc9f7  D[2]=45438437
A[3]=8aa86455  B[3]=a598140e  C[3]=db5c97d4  D[3]=5025577d

Step 29: (r=13, s=10)
A[0]=35836811  B[0]=ddcff393  C[0]=594d7884  D[0]=2b67baaa
A[1]=307e10fd  B[1]=695065af  C[1]=70d363ee  D[1]=027533ed
A[2]=5b84f937  B[2]=71c09a04  C[2]=9d21f5c0  D[2]=4a6cc9f7
A[3]=dde030a1  B[3]=0c8ab155  C[3]=a598140e  D[3]=db5c97d4

Step 30: (r=10, s=25)
A[0]=143bc042  B[0]=0da044d6  C[0]=ddcff393  D[0]=594d7884
A[1]=77b822cf  B[1]=f843f4c1  C[1]=695065af  D[1]=70d363ee
A[2]=89ce5139  B[2]=13e4dd6e  C[2]=71c09a04  D[2]=9d21f5c0
A[3]=d3ec99c7  B[3]=80c28777  C[3]=0c8ab155  D[3]=a598140e

Step 31: (r=25, s= 4)
A[0]=6122b39d  B[0]=84287780  C[0]=0da044d6  D[0]=ddcff393
A[1]=35c16134  B[1]=9eef7045  C[1]=f843f4c1  D[1]=695065af
A[2]=c87a1066  B[2]=73139ca2  C[2]=13e4dd6e  D[2]=71c09a04
A[3]=528d7933  B[3]=8fa7d933  C[3]=80c28777  D[3]=0c8ab155

Feed-Forward Step 32: (r= 4, s=13)
A[0]=05729a2d  B[0]=122b39d6  C[0]=84287780  D[0]=0da044d6
A[1]=3464b011  B[1]=5c161343  C[1]=9eef7045  D[1]=f843f4c1
A[2]=d5eb3c7c  B[2]=87a1066c  C[2]=73139ca2  D[2]=13e4dd6e
A[3]=4921f2fb  B[3]=28d79335  C[3]=8fa7d933  D[3]=80c28777
```

```
Feed-Forward Step 33: (r=13, s=10)
A[0]=9070236e  B[0]=5345a0ae  C[0]=122b39d6  D[0]=84287780
A[1]=2885c804  B[1]=9602268c  C[1]=5c161343  D[1]=9eef7045
A[2]=ef861ed1  B[2]=678f9abd  C[2]=87a1066c  D[2]=73139ca2
A[3]=10358a1f  B[3]=3e5f6924  C[3]=28d79335  D[3]=8fa7d933

Feed-Forward Step 34: (r=10, s=25)
A[0]=bd2db492  B[0]=c08dba41  C[0]=5345a0ae  D[0]=122b39d6
A[1]=56a1e6c0  B[1]=172010a2  C[1]=9602268c  D[1]=5c161343
A[2]=0c30290e  B[2]=187b47be  C[2]=678f9abd  D[2]=87a1066c
A[3]=577e1ad4  B[3]=d6287c40  C[3]=3e5f6924  D[3]=28d79335

Feed-Forward Step 35: (r=25, s= 4)
A[0]=1ee82980  B[0]=257a5b69  C[0]=c08dba41  D[0]=5345a0ae
A[1]=3ee12073  B[1]=80ad43cd  C[1]=172010a2  D[1]=9602268c
A[2]=c31d00d9  B[2]=1c186052  C[2]=187b47be  D[2]=678f9abd
A[3]=ec1f02d8  B[3]=a8aefc35  C[3]=d6287c40  D[3]=3e5f6924
```

Compression Function Output

```
A[0]=1ee82980  B[0]=257a5b69  C[0]=c08dba41  D[0]=5345a0ae
A[1]=3ee12073  B[1]=80ad43cd  C[1]=172010a2  D[1]=9602268c
A[2]=c31d00d9  B[2]=1c186052  C[2]=187b47be  D[2]=678f9abd
A[3]=ec1f02d8  B[3]=a8aefc35  C[3]=d6287c40  D[3]=3e5f6924
```

Hash Function Output

```
8029e81e7320e13ed9001dc3d8021fec695b7a25cd43ad805260181c35fcaea8
```

A.2.2 One-block Message

We use the message block `0x00 0x01 0x02` ... as an example.

First block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
```

NTT Output

```
y[  0..  7] =  218   26   85  204   79  131  143   82
y[  8.. 15] =  193  132  188  176  130  214  229  177
y[ 16.. 23] =   43    9  233   73  161  207  236  155
y[ 24.. 31] =  124   92  110  120  191  202  211   82
```

```
y[ 32.. 39] =  211  215  163   35    7   33  156  212
y[ 40.. 47] =  135  222  249   69  206   55  208  212
y[ 48.. 55] =   99   87  170   98  133  188   63  177
y[ 56.. 63] =   41   50  150   31   54  204   39  220
y[ 64.. 71] =  224    7   13   81   49  160   87  256
y[ 72.. 79] =   21  231  119  191  182  247   17  196
y[ 80.. 87] =  154   34  227   51  125  130  142  149
y[ 88.. 95] =   82   92  139  202  152   85   17  226
y[ 96..103] =  239   47  252  198   36    9  238  244
y[104..111] =   45  236   16   63  151  237  232    9
y[112..119] =   90   90  227  241  198  200   16  123
y[120..127] =  131    1    6  179  204  175  249  158
```

Intermediate Expanded Message

```
Z[ 0] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
Z[ 1] = a5abd1c0  c577ce23  e0eda439  c630ebc4
Z[ 2] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
Z[ 3] = 427c599c  56b84f7e  d841d04e  3b42dec2
Z[ 4] = e1a6dec2  194bbc12  17d9050f  df7bb703
Z[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
Z[ 6] = 3edf478b  46d2c121  ce23a664  c6302d87
Z[ 7] = 24221da1  1667b2ad  d9b32706  e5431c2f
Z[ 8] = 050fe827  3a890965  b9e72369  ff473edf
Z[ 9] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
Z[10] = 1892b591  24dbea52  a4395a55  b1f4ace5
Z[11] = 427c3b42  d841aaba  3d6db41f  e9990c49
Z[12] = 21f7f2fe  d55dfc63  06811a04  f69bf245
Z[13] = f0d32085  2d870b90  f18cb366  0681edef
Z[14] = 410a410a  f470ea52  d6cfd55d  58e30b90
Z[15] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
Z[16] = e1f7dc81  0bd54d5d  2c9947e7  4f2f983e
Z[17] = 131dc5c0  6c4fc133  bbbd8c69  0f79e684
Z[18] = a2412723  e4b2ea28  71c5a8a0  9755ece3
Z[19] = 4aa270dc  949a641e  a06fc3ee  0f79d622
Z[20] = ef9ed622  fb73aa72  20c4065f  eeb5a413
Z[21] = 28f590f6  0e90f8b8  9f86d195  e93fd367
Z[22] = 51ea5a1b  e4b2b0d1  ca4d8f24  0e903957
Z[23] = 8d522551  05769e9d  cfc33126  f8b8237f
Z[24] = 065f17aa  49b9cfc3  a7b78d52  ff174aa2
Z[25] = e8568e3b  c3eeb647  f6e6d8dd  c87bb730
Z[26] = 1ef20831  2e6b4271  8c69d27e  9db4a32a
Z[27] = 53bc53bc  cdf16d38  4d5dcdf1  e3c94aa2
Z[28] = 2ac7d9c6  ca4d1fdb  08311e09  f42bd70b
Z[29] = ece3e025  39573ecd  edcc320f  0831d70b
Z[30] = 51ea4f2f  f1705932  cc1fc133  6ff3b730
Z[31] = 00e92d82  b9021c37  b55ecfc3  a5e5de53
```

Expanded Message

```
W[ 0] = e1a6dec2  194bbc12  17d9050f  df7bb703
W[ 1] = 3edf478b  46d2c121  ce23a664  c6302d87
W[ 2] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
W[ 3] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
W[ 4] = 24221da1  1667b2ad  d9b32706  e5431c2f
W[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
W[ 6] = 427c599c  56b84f7e  d841d04e  3b42dec2
W[ 7] = a5abd1c0  c577ce23  e0eda439  c630ebc4
W[ 8] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
W[ 9] = 427c3b42  d841aaba  3d6db41f  e9990c49
W[10] = 21f7f2fe  d55dfc63  06811a04  f69bf245
W[11] = 050fe827  3a890965  b9e72369  ff473edf
W[12] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
W[13] = f0d32085  2d870b90  f18cb366  0681edef
W[14] = 1892b591  24dbea52  a4395a55  b1f4ace5
W[15] = 410a410a  f470ea52  d6cfd55d  58e30b90
W[16] = 131dc5c0  6c4fc133  bbbd8c69  0f79e684
W[17] = a2412723  e4b2ea28  71c5a8a0  9755ece3
W[18] = 8d522551  05769e9d  cfc33126  f8b8237f
W[19] = ef9ed622  fb73aa72  20c4065f  eeb5a413
W[20] = 51ea5a1b  e4b2b0d1  ca4d8f24  0e903957
W[21] = 28f590f6  0e90f8b8  9f86d195  e93fd367
W[22] = e1f7dc81  0bd54d5d  2c9947e7  4f2f983e
W[23] = 4aa270dc  949a641e  a06fc3ee  0f79d622
W[24] = 51ea4f2f  f1705932  cc1fc133  6ff3b730
W[25] = 065f17aa  49b9cfc3  a7b78d52  ff174aa2
W[26] = e8568e3b  c3eeb647  f6e6d8dd  c87bb730
W[27] = 00e92d82  b9021c37  b55ecfc3  a5e5de53
W[28] = 53bc53bc  cdf16d38  4d5dcdf1  e3c94aa2
W[29] = ece3e025  39573ecd  edcc320f  0831d70b
W[30] = 2ac7d9c6  ca4d1fdb  08311e09  f42bd70b
W[31] = 1ef20831  2e6b4271  8c69d27e  9db4a32a
```

Feistel Steps

```
IV :
A[0]=4d567983  B[0]=aaf3d925  C[0]=c2c2ba14  D[0]=e2eaa8d2
A[1]=07190ba9  B[1]=3ee20b03  C[1]=49b3bcb4  D[1]=1ff47833
A[2]=8474577b  B[2]=afd5e751  C[2]=f67caf46  D[2]=d0c661a5
A[3]=39d726e9  B[3]=c96006d3  C[3]=668626c9  D[3]=55693de1

IV XOR M :
A[0]=4e547883  B[0]=b9e1c835  C[0]=e1e09b34  D[0]=d1d899e2
A[1]=001f0ead  B[1]=29f41e17  C[1]=6e959990  D[1]=28c24d07
A[2]=8f7e5e73  B[2]=b4cffe49  C[2]=dd56866e  D[2]=ebfc589d
A[3]=36d92be5  B[3]=d67e1bcf  C[3]=49a80be5  D[3]=6a5700dd

Step  0: (r= 3, s=23)
A[0]=eda72589  B[0]=72a3c41a  C[0]=b9e1c835  D[0]=e1e09b34
```

```
A[1]=89fc156e  B[1]=00f87568  C[1]=29f41e17  D[1]=6e959990
A[2]=b3b57146  B[2]=7bf2f39c  C[2]=b4cffe49  D[2]=dd56866e
A[3]=4ec798fd  B[3]=b6c95f29  C[3]=d67e1bcf  D[3]=49a80be5

Step  1: (r=23, s=17)
A[0]=0150fdff  B[0]=c4f6d392  C[0]=72a3c41a  D[0]=b9e1c835
A[1]=72fd108c  B[1]=b744fe0a  C[1]=00f87568  D[1]=29f41e17
A[2]=1cb69a7c  B[2]=a359dab8  C[2]=7bf2f39c  D[2]=b4cffe49
A[3]=60744bac  B[3]=7ea763cc  C[3]=b6c95f29  D[3]=d67e1bcf

Step  2: (r=17, s=27)
A[0]=5955c4d4  B[0]=fbfe02a1  C[0]=c4f6d392  D[0]=72a3c41a
A[1]=96a797f4  B[1]=2118e5fa  C[1]=b744fe0a  D[1]=00f87568
A[2]=e7017f92  B[2]=34f8396d  C[2]=a359dab8  D[2]=7bf2f39c
A[3]=cc4173a8  B[3]=9758c0e8  C[3]=7ea763cc  D[3]=b6c95f29

Step  3: (r=27, s= 3)
A[0]=5d8cf239  B[0]=a2caae26  C[0]=fbfe02a1  D[0]=c4f6d392
A[1]=5aa53e78  B[1]=a4b53cbf  C[1]=2118e5fa  D[1]=b744fe0a
A[2]=27b546c0  B[2]=97380bfc  C[2]=34f8396d  D[2]=a359dab8
A[3]=b70c933d  B[3]=46620b9d  C[3]=9758c0e8  D[3]=7ea763cc

Step  4: (r= 3, s=23)
A[0]=e81ca9ca  B[0]=ec6791ca  C[0]=a2caae26  D[0]=fbfe02a1
A[1]=915bcae3  B[1]=d529f3c2  C[1]=a4b53cbf  D[1]=2118e5fa
A[2]=c1c1f450  B[2]=3daa3601  C[2]=97380bfc  D[2]=34f8396d
A[3]=b1a78d43  B[3]=b86499ed  C[3]=46620b9d  D[3]=9758c0e8

Step  5: (r=23, s=17)
A[0]=4a5c69ca  B[0]=e5740e54  C[0]=ec6791ca  D[0]=a2caae26
A[1]=de8cb15b  B[1]=71c8ade5  C[1]=d529f3c2  D[1]=a4b53cbf
A[2]=078e92a5  B[2]=2860e0fa  C[2]=3daa3601  D[2]=97380bfc
A[3]=340c5cca  B[3]=a1d8d3c6  C[3]=b86499ed  D[3]=46620b9d

Step  6: (r=17, s=27)
A[0]=c94595a5  B[0]=d39494b8  C[0]=e5740e54  D[0]=ec6791ca
A[1]=da1c46a8  B[1]=62b7bd19  C[1]=71c8ade5  D[1]=d529f3c2
A[2]=167d8c8f  B[2]=254a0f1d  C[2]=2860e0fa  D[2]=3daa3601
A[3]=8ed99d3e  B[3]=b9946818  C[3]=a1d8d3c6  D[3]=b86499ed

Step  7: (r=27, s= 3)
A[0]=13f3ae56  B[0]=2e4a2cad  C[0]=d39494b8  D[0]=e5740e54
A[1]=5e6a4959  B[1]=46d0e235  C[1]=62b7bd19  D[1]=71c8ade5
A[2]=464d6377  B[2]=78b3ec64  C[2]=254a0f1d  D[2]=2860e0fa
A[3]=8a43d8ae  B[3]=f476cce9  C[3]=b9946818  D[3]=a1d8d3c6

Step  8: (r=28, s=19)
A[0]=68398129  B[0]=613f3ae5  C[0]=2e4a2cad  D[0]=d39494b8
A[1]=a6c9d83c  B[1]=95e6a495  C[1]=46d0e235  D[1]=62b7bd19
```

```
A[2]=ceb115ae  B[2]=7464d637  C[2]=78b3ec64  D[2]=254a0f1d
A[3]=16ef9c12  B[3]=e8a43d8a  C[3]=f476cce9  D[3]=b9946818

Step  9: (r=19, s=22)
A[0]=e9c4594d  B[0]=094b41cc  C[0]=613f3ae5  D[0]=2e4a2cad
A[1]=838b344e  B[1]=c1e5364e  C[1]=95e6a495  D[1]=46d0e235
A[2]=c9466e2b  B[2]=ad767588  C[2]=7464d637  D[2]=78b3ec64
A[3]=00976dfc  B[3]=e090b77c  C[3]=e8a43d8a  D[3]=f476cce9

Step 10: (r=22, s= 7)
A[0]=69b41d47  B[0]=537a7116  C[0]=094b41cc  D[0]=613f3ae5
A[1]=8949e1b4  B[1]=13a0e2cd  C[1]=c1e5364e  D[1]=95e6a495
A[2]=a177b334  B[2]=8af2519b  C[2]=ad767588  D[2]=7464d637
A[3]=f51b3936  B[3]=7f0025db  C[3]=e090b77c  D[3]=e8a43d8a

Step 11: (r= 7, s=28)
A[0]=381942c3  B[0]=da0ea3b4  C[0]=537a7116  D[0]=094b41cc
A[1]=3cfae49c  B[1]=a4f0da44  C[1]=13a0e2cd  D[1]=c1e5364e
A[2]=309cbf37  B[2]=bbd99a50  C[2]=8af2519b  D[2]=ad767588
A[3]=0fe565f0  B[3]=8d9c9b7a  C[3]=7f0025db  D[3]=e090b77c

Step 12: (r=28, s=19)
A[0]=684a3326  B[0]=3381942c  C[0]=da0ea3b4  D[0]=537a7116
A[1]=ac4fcd4f  B[1]=c3cfae49  C[1]=a4f0da44  D[1]=13a0e2cd
A[2]=d4415f0d  B[2]=7309cbf3  C[2]=bbd99a50  D[2]=8af2519b
A[3]=c107ebf2  B[3]=00fe565f  C[3]=8d9c9b7a  D[3]=7f0025db

Step 13: (r=19, s=22)
A[0]=285e381b  B[0]=99334251  C[0]=3381942c  D[0]=da0ea3b4
A[1]=8a4f862e  B[1]=6a7d627e  C[1]=c3cfae49  D[1]=a4f0da44
A[2]=adcf3489  B[2]=f86ea20a  C[2]=7309cbf3  D[2]=bbd99a50
A[3]=3b7f2ab9  B[3]=5f96083f  C[3]=00fe565f  D[3]=8d9c9b7a

Step 14: (r=22, s= 7)
A[0]=88838edf  B[0]=06ca178e  C[0]=99334251  D[0]=3381942c
A[1]=30a0f617  B[1]=8ba293e1  C[1]=6a7d627e  D[1]=c3cfae49
A[2]=3cee2c0d  B[2]=226b73cd  C[2]=f86ea20a  D[2]=7309cbf3
A[3]=ce7366bb  B[3]=ae4edfca  C[3]=5f96083f  D[3]=00fe565f

Step 15: (r= 7, s=28)
A[0]=b04bf959  B[0]=41c76fc4  C[0]=06ca178e  D[0]=99334251
A[1]=6ff58875  B[1]=507b0b98  C[1]=8ba293e1  D[1]=6a7d627e
A[2]=11d7da1c  B[2]=7716069e  C[2]=226b73cd  D[2]=f86ea20a
A[3]=199981a8  B[3]=39b35de7  C[3]=ae4edfca  D[3]=5f96083f

Step 16: (r=29, s= 9)
A[0]=ab2aaaa9  B[0]=36097f2b  C[0]=41c76fc4  D[0]=06ca178e
A[1]=83b1b363  B[1]=adfeb10e  C[1]=507b0b98  D[1]=8ba293e1
A[2]=0aae20f9  B[2]=823afb43  C[2]=7716069e  D[2]=226b73cd
```

```
A[3]=7c9bfb6b  B[3]=03333035  C[3]=39b35de7  D[3]=ae4edfca

Step 17: (r= 9, s=15)
A[0]=8f05dce5  B[0]=55555356  C[0]=36097f2b  D[0]=41c76fc4
A[1]=7813933d  B[1]=6366c707  C[1]=adfeb10e  D[1]=507b0b98
A[2]=04c0ccbc  B[2]=5c41f215  C[2]=823afb43  D[2]=7716069e
A[3]=55fe76c2  B[3]=37f6d6f9  C[3]=03333035  D[3]=39b35de7

Step 18: (r=15, s= 5)
A[0]=4e7fc869  B[0]=ee72c782  C[0]=55555356  D[0]=36097f2b
A[1]=6a7c6f09  B[1]=c99ebc09  C[1]=6366c707  D[1]=adfeb10e
A[2]=e5e68e78  B[2]=665e0260  C[2]=5c41f215  D[2]=823afb43
A[3]=b2b90dc9  B[3]=3b612aff  C[3]=37f6d6f9  D[3]=03333035

Step 19: (r= 5, s=29)
A[0]=2d753428  B[0]=cff90d29  C[0]=ee72c782  D[0]=55555356
A[1]=5573da27  B[1]=4f8de12d  C[1]=c99ebc09  D[1]=6366c707
A[2]=b3e1dba9  B[2]=bcd1cf1c  C[2]=665e0260  D[2]=5c41f215
A[3]=74b7f715  B[3]=5721b936  C[3]=3b612aff  D[3]=37f6d6f9

Step 20: (r=29, s= 9)
A[0]=0ffc320f  B[0]=05aea685  C[0]=cff90d29  D[0]=ee72c782
A[1]=a95c46a0  B[1]=eaae7b44  C[1]=4f8de12d  D[1]=c99ebc09
A[2]=ad473efe  B[2]=367c3b75  C[2]=bcd1cf1c  D[2]=665e0260
A[3]=5745b600  B[3]=ae96fee2  C[3]=5721b936  D[3]=3b612aff

Step 21: (r= 9, s=15)
A[0]=f7cfd504  B[0]=f8641e1f  C[0]=05aea685  D[0]=cff90d29
A[1]=0456fffd  B[1]=b88d4152  C[1]=eaae7b44  D[1]=4f8de12d
A[2]=9524e1cb  B[2]=8e7dfd5a  C[2]=367c3b75  D[2]=bcd1cf1c
A[3]=ecc23b2d  B[3]=8b6c00ae  C[3]=ae96fee2  D[3]=5721b936

Step 22: (r=15, s= 5)
A[0]=6cd5c086  B[0]=ea827be7  C[0]=f8641e1f  D[0]=05aea685
A[1]=9bcc3221  B[1]=7ffe822b  C[1]=b88d4152  D[1]=eaae7b44
A[2]=e78487b6  B[2]=70e5ca92  C[2]=8e7dfd5a  D[2]=367c3b75
A[3]=22f00675  B[3]=1d96f661  C[3]=8b6c00ae  D[3]=ae96fee2

Step 23: (r= 5, s=29)
A[0]=65237ce1  B[0]=9ab810cd  C[0]=ea827be7  D[0]=f8641e1f
A[1]=97f3930c  B[1]=79864433  C[1]=7ffe822b  D[1]=b88d4152
A[2]=31407e11  B[2]=f090f6dc  C[2]=70e5ca92  D[2]=8e7dfd5a
A[3]=d3f8ac3a  B[3]=5e00cea4  C[3]=1d96f661  D[3]=8b6c00ae

Step 24: (r= 4, s=13)
A[0]=4f5beb66  B[0]=5237ce16  C[0]=9ab810cd  D[0]=ea827be7
A[1]=c58cb287  B[1]=7f3930c9  C[1]=79864433  D[1]=7ffe822b
A[2]=b62ebd15  B[2]=1407e113  C[2]=f090f6dc  D[2]=70e5ca92
A[3]=e6cfcc3f  B[3]=3f8ac3ad  C[3]=5e00cea4  D[3]=1d96f661
```

```
Step 25: (r=13, s=10)
A[0]=2d5b39d3  B[0]=7d6cc9eb  C[0]=5237ce16  D[0]=9ab810cd
A[1]=04a279f4  B[1]=9650f8b1  C[1]=7f3930c9  D[1]=79864433
A[2]=4e5bbf9f  B[2]=d7a2b6c5  C[2]=1407e113  D[2]=f090f6dc
A[3]=7a5fba1d  B[3]=f987fcd9  C[3]=3f8ac3ad  D[3]=5e00cea4

Step 26: (r=10, s=25)
A[0]=1ced6cc6  B[0]=6ce74cb5  C[0]=7d6cc9eb  D[0]=5237ce16
A[1]=d6779a1f  B[1]=89e7d012  C[1]=9650f8b1  D[1]=7f3930c9
A[2]=0662cd9e  B[2]=6efe7d39  C[2]=d7a2b6c5  D[2]=1407e113
A[3]=882f55b4  B[3]=7ee875e9  C[3]=f987fcd9  D[3]=3f8ac3ad

Step 27: (r=25, s= 4)
A[0]=50198390  B[0]=8c39dad9  C[0]=6ce74cb5  D[0]=7d6cc9eb
A[1]=166db604  B[1]=3facef34  C[1]=89e7d012  D[1]=9650f8b1
A[2]=7da361a5  B[2]=3c0cc59b  C[2]=6efe7d39  D[2]=d7a2b6c5
A[3]=2da6c430  B[3]=69105eab  C[3]=7ee875e9  D[3]=f987fcd9

Step 28: (r= 4, s=13)
A[0]=373d1e03  B[0]=01983905  C[0]=8c39dad9  D[0]=6ce74cb5
A[1]=e5ebf388  B[1]=66db6041  C[1]=3facef34  D[1]=89e7d012
A[2]=dee62d3a  B[2]=da361a57  C[2]=3c0cc59b  D[2]=6efe7d39
A[3]=9a5fe99f  B[3]=da6c4302  C[3]=69105eab  D[3]=7ee875e9

Step 29: (r=13, s=10)
A[0]=0e4f60c7  B[0]=a3c066e7  C[0]=01983905  D[0]=8c39dad9
A[1]=716ed888  B[1]=7e711cbd  C[1]=66db6041  D[1]=3facef34
A[2]=4162a9a8  B[2]=c5a75bdc  C[2]=da361a57  D[2]=3c0cc59b
A[3]=7e22646c  B[3]=fd33f34b  C[3]=da6c4302  D[3]=69105eab

Step 30: (r=10, s=25)
A[0]=88d7b5ef  B[0]=3d831c39  C[0]=a3c066e7  D[0]=01983905
A[1]=6e840708  B[1]=bb6221c5  C[1]=7e711cbd  D[1]=66db6041
A[2]=899c79f7  B[2]=8aa6a105  C[2]=c5a75bdc  D[2]=da361a57
A[3]=8b5d5e37  B[3]=8991b1f8  C[3]=fd33f34b  D[3]=da6c4302

Step 31: (r=25, s= 4)
A[0]=93ea9b4f  B[0]=df11af6b  C[0]=3d831c39  D[0]=a3c066e7
A[1]=a9813ead  B[1]=10dd080e  C[1]=bb6221c5  D[1]=7e711cbd
A[2]=e3781a1a  B[2]=ef1338f3  C[2]=8aa6a105  D[2]=c5a75bdc
A[3]=240aa27e  B[3]=6f16babc  C[3]=8991b1f8  D[3]=fd33f34b

Feed-Forward Step 32: (r= 4, s=13)
A[0]=4ea6dde5  B[0]=3ea9b4f9  C[0]=df11af6b  D[0]=3d831c39
A[1]=ddb7f4bb  B[1]=9813eada  C[1]=10dd080e  D[1]=bb6221c5
A[2]=e5a1b190  B[2]=3781a1ae  C[2]=ef1338f3  D[2]=8aa6a105
A[3]=1867d18c  B[3]=40aa27e2  C[3]=6f16babc  D[3]=8991b1f8
```

```
Feed-Forward Step 33: (r=13, s=10)
A[0]=a148a1d6  B[0]=dbbca9d4  C[0]=3ea9b4f9  D[0]=df11af6b
A[1]=5c12441e  B[1]=fe977bb6  C[1]=9813eada  D[1]=10dd080e
A[2]=3afa68b4  B[2]=36321cb4  C[2]=3781a1ae  D[2]=ef1338f3
A[3]=c5c40b9c  B[3]=fa31830c  C[3]=40aa27e2  D[3]=6f16babc

Feed-Forward Step 34: (r=10, s=25)
A[0]=e225cd29  B[0]=22875a85  C[0]=dbbca9d4  D[0]=3ea9b4f9
A[1]=409bbc76  B[1]=49107970  C[1]=fe977bb6  D[1]=9813eada
A[2]=10c0e168  B[2]=e9a2d0eb  C[2]=36321cb4  D[2]=3781a1ae
A[3]=303c0781  B[3]=102e7317  C[3]=fa31830c  D[3]=40aa27e2

Feed-Forward Step 35: (r=25, s= 4)
A[0]=d57ce214  B[0]=53c44b9a  C[0]=22875a85  D[0]=dbbca9d4
A[1]=31ef719d  B[1]=ec813778  C[1]=49107970  D[1]=fe977bb6
A[2]=dc2f3c6a  B[2]=d02181c2  C[2]=e9a2d0eb  D[2]=36321cb4
A[3]=57d2d8a1  B[3]=0260780f  C[3]=102e7317  D[3]=fa31830c
```

Compression Function Output

```
A[0]=d57ce214  B[0]=53c44b9a  C[0]=22875a85  D[0]=dbbca9d4
A[1]=31ef719d  B[1]=ec813778  C[1]=49107970  D[1]=fe977bb6
A[2]=dc2f3c6a  B[2]=d02181c2  C[2]=e9a2d0eb  D[2]=36321cb4
A[3]=57d2d8a1  B[3]=0260780f  C[3]=102e7317  D[3]=fa31830c
```

Final block

```
M[  0..  7] = 00 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    4  177  210   45  165  187  234   40
y[  8.. 15] =  101   34  138  136   32   51  140  236
y[ 16.. 23] =  197    5  107  213   42  239  210   91
y[ 24.. 31] =  112   87  126   65  121  118  204  159
y[ 32.. 39] =   32  210   63  149  138  147  181  215
y[ 40.. 47] =   58    4  174  220   32   36   73   94
y[ 48.. 55] =   60   67  181  117  175   93   92  129
y[ 56.. 63] =  246  229   94   37   17  151   88  210
y[ 64.. 71] =  253   80   47  212   92   70   23  217
y[ 72.. 79] =  156  223  119  121  225  206  117   21
y[ 80.. 87] =   60  252  150   44  215   18   47  166
y[ 88.. 95] =  145  170  131  192  136  139   53   98
```

```
y[ 96..103] =  225   47  194  108  119  110   76   42
y[104..111] =  199  253   83   37  225  221  184  163
y[112..119] =  197  190   76  140   82  164  165  128
y[120..127] =   11   28  163  220  240  106  169   47
```

Intermediate Expanded Message

```
Z[ 0] = c63002e4  2085de09  cd6abd84  1ce8ef61
Z[ 1] = 189248fd  a88faa01  24db1720  f0d3ab73
Z[ 2] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
Z[ 3] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
Z[ 4] = de091720  b1f42d87  b082aa01  e1a6c914
Z[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
Z[ 6] = 306b2b5c  548dc914  4335c4be  a380427c
Z[ 7] = ebc4f80d  1abd43ee  b3660c49  de093f98
Z[ 8] = 39d0fd1c  df7b21f7  3296427c  e318109f
Z[ 9] = e76eb703  577155ff  db25e8e0  0f2d548d
Z[10] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
Z[11] = c121af10  d107a4f2  aabaa88f  46d2264d
Z[12] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
Z[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
Z[14] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
Z[15] = 143c07f3  e543bc12  4c9af3b7  21f7c068
Z[16] = fc5c03a4  2ac7d539  53bcac44  14efeb11
Z[17] = a4135bed  6c4f93b1  e2e01d20  6a7d9583
Z[18] = 369cc964  9e9d6163  d9c6263a  2ac7d539
Z[19] = 9a1065f0  8d5272ae  91df6e21  303dcfc3
Z[20] = e2e01d20  c6a93957  6c4f93b1  452cbad4
Z[21] = cb3634ca  4b8bb475  e2e01d20  bd8f4271
Z[22] = c964369c  452cbad4  4aa2b55e  ac4453bc
Z[23] = 0a03f5fd  aa72558e  f0870f79  afe85018
Z[24] = 48d0b730  d70b28f5  3fb6c04a  db982468
Z[25] = e10e1ef2  6e2191df  d1952e6b  131dece3
Z[26] = fb73048d  280cd7f4  1062ef9e  ad2d52d3
Z[27] = b0d14f2f  c4d73b29  949a6b66  5932a6ce
Z[28] = 2ac7d539  624c9db4  641e9be2  263ad9c6
Z[29] = fc5c03a4  21adde53  df3c20c4  aa72558e
Z[30] = c3053cfb  95836a7d  ab5b54a5  74808b80
Z[31] = 197ce684  de5321ad  607a9f86  2ac7d539
```

Expanded Message

```
W[ 0] = de091720  b1f42d87  b082aa01  e1a6c914
W[ 1] = 306b2b5c  548dc914  4335c4be  a380427c
W[ 2] = c63002e4  2085de09  cd6abd84  1ce8ef61
W[ 3] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
W[ 4] = ebc4f80d  1abd43ee  b3660c49  de093f98
W[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
W[ 6] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
W[ 7] = 189248fd  a88faa01  24db1720  f0d3ab73
```

```
W[ 8] = 143c07f3  e543bc12  4c9af3b7  21f7c068
W[ 9] = c121af10  d107a4f2  aabaa88f  46d2264d
W[10] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
W[11] = 39d0fd1c  df7b21f7  3296427c  e318109f
W[12] = e76eb703  577155ff  db25e8e0  0f2d548d
W[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
W[14] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
W[15] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
W[16] = a4135bed  6c4f93b1  e2e01d20  6a7d9583
W[17] = 369cc964  9e9d6163  d9c6263a  2ac7d539
W[18] = 0a03f5fd  aa72558e  f0870f79  afe85018
W[19] = e2e01d20  c6a93957  6c4f93b1  452cbad4
W[20] = c964369c  452cbad4  4aa2b55e  ac4453bc
W[21] = cb3634ca  4b8bb475  e2e01d20  bd8f4271
W[22] = fc5c03a4  2ac7d539  53bcac44  14efeb11
W[23] = 9a1065f0  8d5272ae  91df6e21  303dcfc3
W[24] = c3053cfb  95836a7d  ab5b54a5  74808b80
W[25] = 48d0b730  d70b28f5  3fb6c04a  db982468
W[26] = e10e1ef2  6e2191df  d1952e6b  131dece3
W[27] = 197ce684  de5321ad  607a9f86  2ac7d539
W[28] = b0d14f2f  c4d73b29  949a6b66  5932a6ce
W[29] = fc5c03a4  21adde53  df3c20c4  aa72558e
W[30] = 2ac7d539  624c9db4  641e9be2  263ad9c6
W[31] = fb73048d  280cd7f4  1062ef9e  ad2d52d3
```

Feistel Steps

```
IV :
A[0]=d57ce214  B[0]=53c44b9a  C[0]=22875a85  D[0]=dbbca9d4
A[1]=31ef719d  B[1]=ec813778  C[1]=49107970  D[1]=fe977bb6
A[2]=dc2f3c6a  B[2]=d02181c2  C[2]=e9a2d0eb  D[2]=36321cb4
A[3]=57d2d8a1  B[3]=0260780f  C[3]=102e7317  D[3]=fa31830c

IV XOR M :
A[0]=d57ce014  B[0]=53c44b9a  C[0]=22875a85  D[0]=dbbca9d4
A[1]=31ef719d  B[1]=ec813778  C[1]=49107970  D[1]=fe977bb6
A[2]=dc2f3c6a  B[2]=d02181c2  C[2]=e9a2d0eb  D[2]=36321cb4
A[3]=57d2d8a1  B[3]=0260780f  C[3]=102e7317  D[3]=fa31830c

Step  0: (r= 3, s=23)
A[0]=52125376  B[0]=abe700a6  C[0]=53c44b9a  D[0]=22875a85
A[1]=06738f17  B[1]=8f7b8ce9  C[1]=ec813778  D[1]=49107970
A[2]=7b02f04d  B[2]=e179e356  C[2]=d02181c2  D[2]=e9a2d0eb
A[3]=7d6905b9  B[3]=be96c50a  C[3]=0260780f  D[3]=102e7317

Step  1: (r=23, s=17)
A[0]=43dc2ee9  B[0]=bb290929  C[0]=abe700a6  D[0]=53c44b9a
A[1]=da99cda5  B[1]=8b8339c7  C[1]=8f7b8ce9  D[1]=ec813778
A[2]=aa07251d  B[2]=26bd8178  C[2]=e179e356  D[2]=d02181c2
```

```
A[3]=f0c71d25  B[3]=dcbeb482  C[3]=be96c50a  D[3]=0260780f

Step  2: (r=17, s=27)
A[0]=a874dc43  B[0]=5dd287b8  C[0]=bb290929  D[0]=abe700a6
A[1]=bf22a508  B[1]=9b4bb533  C[1]=8b8339c7  D[1]=8f7b8ce9
A[2]=9b540548  B[2]=4a3b540e  C[2]=26bd8178  D[2]=e179e356
A[3]=35c18993  B[3]=3a4be18e  C[3]=dcbeb482  D[3]=be96c50a

Step  3: (r=27, s= 3)
A[0]=9cebe8be  B[0]=1d43a6e2  C[0]=5dd287b8  D[0]=bb290929
A[1]=76e066fa  B[1]=45f91528  C[1]=9b4bb533  D[1]=8b8339c7
A[2]=b33a3b8c  B[2]=44daa02a  C[2]=4a3b540e  D[2]=26bd8178
A[3]=0bad64d9  B[3]=99ae0c4c  C[3]=3a4be18e  D[3]=dcbeb482

Step  4: (r= 3, s=23)
A[0]=92343538  B[0]=e75f45f4  C[0]=1d43a6e2  D[0]=5dd287b8
A[1]=d56a3ba1  B[1]=b70337d3  C[1]=45f91528  D[1]=9b4bb533
A[2]=ceed74d2  B[2]=99d1dc65  C[2]=44daa02a  D[2]=4a3b540e
A[3]=2a6e737f  B[3]=5d6b26c8  C[3]=99ae0c4c  D[3]=3a4be18e

Step  5: (r=23, s=17)
A[0]=6ebb2754  B[0]=9c491a1a  C[0]=e75f45f4  D[0]=1d43a6e2
A[1]=cb1a22af  B[1]=d0eab51d  C[1]=b70337d3  D[1]=45f91528
A[2]=900b174f  B[2]=696776ba  C[2]=99d1dc65  D[2]=44daa02a
A[3]=1580496a  B[3]=bf953739  C[3]=5d6b26c8  D[3]=99ae0c4c

Step  6: (r=17, s=27)
A[0]=77b3862d  B[0]=4ea8dd76  C[0]=9c491a1a  D[0]=e75f45f4
A[1]=f8e8c2b4  B[1]=455f9634  C[1]=d0eab51d  D[1]=b70337d3
A[2]=e46f4d70  B[2]=2e9f2016  C[2]=696776ba  D[2]=99d1dc65
A[3]=6a221081  B[3]=92d42b00  C[3]=bf953739  D[3]=5d6b26c8

Step  7: (r=27, s= 3)
A[0]=7bfce3e5  B[0]=6bbd9c31  C[0]=4ea8dd76  D[0]=9c491a1a
A[1]=8f3cd0c5  B[1]=a7c74615  C[1]=455f9634  D[1]=d0eab51d
A[2]=c4a059ea  B[2]=87237a6b  C[2]=2e9f2016  D[2]=696776ba
A[3]=ee5f6ff5  B[3]=0b511084  C[3]=92d42b00  D[3]=bf953739

Step  8: (r=28, s=19)
A[0]=50e6f90c  B[0]=57bfce3e  C[0]=6bbd9c31  D[0]=4ea8dd76
A[1]=676df14b  B[1]=58f3cd0c  C[1]=a7c74615  D[1]=455f9634
A[2]=706eef1b  B[2]=ac4a059e  C[2]=87237a6b  D[2]=2e9f2016
A[3]=18efb12d  B[3]=5ee5f6ff  C[3]=0b511084  D[3]=92d42b00

Step  9: (r=19, s=22)
A[0]=bb3e1e05  B[0]=c8628737  C[0]=57bfce3e  D[0]=6bbd9c31
A[1]=591859f7  B[1]=8a5b3b6f  C[1]=58f3cd0c  D[1]=a7c74615
A[2]=1148f0b4  B[2]=78db8377  C[2]=ac4a059e  D[2]=87237a6b
A[3]=f798ea77  B[3]=8968c77d  C[3]=5ee5f6ff  D[3]=0b511084
```

```
Step 10: (r=22, s= 7)
A[0]=59a9fa69  B[0]=816ecf87  C[0]=c8628737  D[0]=57bfce3e
A[1]=05d8e539  B[1]=7dd64616  C[1]=8a5b3b6f  D[1]=58f3cd0c
A[2]=f799a3d0  B[2]=2d04523c  C[2]=78db8377  D[2]=ac4a059e
A[3]=0a657cef  B[3]=9dfde63a  C[3]=8968c77d  D[3]=5ee5f6ff

Step 11: (r= 7, s=28)
A[0]=43ee312c  B[0]=d4fd34ac  C[0]=816ecf87  D[0]=c8628737
A[1]=69560d50  B[1]=ec729c82  C[1]=7dd64616  D[1]=8a5b3b6f
A[2]=fd34c127  B[2]=ccd1e87b  C[2]=2d04523c  D[2]=78db8377
A[3]=61b3f399  B[3]=32be7785  C[3]=9dfde63a  D[3]=8968c77d

Step 12: (r=28, s=19)
A[0]=a5c8eed0  B[0]=c43ee312  C[0]=d4fd34ac  D[0]=816ecf87
A[1]=b0415c26  B[1]=069560d5  C[1]=ec729c82  D[1]=7dd64616
A[2]=facd47ea  B[2]=7fd34c12  C[2]=ccd1e87b  D[2]=2d04523c
A[3]=1cf19ec2  B[3]=961b3f39  C[3]=32be7785  D[3]=9dfde63a

Step 13: (r=19, s=22)
A[0]=4aa8b88d  B[0]=76852e47  C[0]=c43ee312  D[0]=d4fd34ac
A[1]=9be020c3  B[1]=e135820a  C[1]=069560d5  D[1]=ec729c82
A[2]=5c09a2e8  B[2]=3f57d66a  C[2]=7fd34c12  D[2]=ccd1e87b
A[3]=1fd1b506  B[3]=f610e78c  C[3]=961b3f39  D[3]=32be7785

Step 14: (r=22, s= 7)
A[0]=480cfbf9  B[0]=2352aa2e  C[0]=76852e47  D[0]=c43ee312
A[1]=b44efbaf  B[1]=30e6f808  C[1]=e135820a  D[1]=069560d5
A[2]=c52f3db4  B[2]=ba170268  C[2]=3f57d66a  D[2]=7fd34c12
A[3]=a9faee71  B[3]=4187f46d  C[3]=f610e78c  D[3]=961b3f39

Step 15: (r= 7, s=28)
A[0]=86db6dfc  B[0]=067dfca4  C[0]=2352aa2e  D[0]=76852e47
A[1]=bca4f5c0  B[1]=277dd7da  C[1]=30e6f808  D[1]=e135820a
A[2]=cd3292af  B[2]=979eda62  C[2]=ba170268  D[2]=3f57d66a
A[3]=44e1c894  B[3]=fd7738d4  C[3]=4187f46d  D[3]=f610e78c

Step 16: (r=29, s= 9)
A[0]=de9806d8  B[0]=90db6dbf  C[0]=067dfca4  D[0]=2352aa2e
A[1]=60833ff5  B[1]=17949eb8  C[1]=277dd7da  D[1]=30e6f808
A[2]=2fe74771  B[2]=f9a65255  C[2]=979eda62  D[2]=ba170268
A[3]=0308b803  B[3]=889c3912  C[3]=fd7738d4  D[3]=4187f46d

Step 17: (r= 9, s=15)
A[0]=c9977b7c  B[0]=300db1bd  C[0]=90db6dbf  D[0]=067dfca4
A[1]=6aa1ce1f  B[1]=067feac1  C[1]=17949eb8  D[1]=277dd7da
A[2]=07fa918f  B[2]=ce8ee25f  C[2]=f9a65255  D[2]=979eda62
A[3]=b14be624  B[3]=11700606  C[3]=889c3912  D[3]=fd7738d4
```

```
Step 18: (r=15, s= 5)
A[0]=00f4c154  B[0]=bdbe64cb  C[0]=300db1bd  D[0]=90db6dbf
A[1]=e27f6608  B[1]=e70fb550  C[1]=067feac1  D[1]=17949eb8
A[2]=c9a7dff5  B[2]=48c783fd  C[2]=ce8ee25f  D[2]=f9a65255
A[3]=2f3c8455  B[3]=f31258a5  C[3]=11700606  D[3]=889c3912

Step 19: (r= 5, s=29)
A[0]=498b1e32  B[0]=1e982a80  C[0]=bdbe64cb  D[0]=300db1bd
A[1]=001a3b3f  B[1]=4fecc11c  C[1]=e70fb550  D[1]=067feac1
A[2]=d528dbc0  B[2]=34fbfeb9  C[2]=48c783fd  D[2]=ce8ee25f
A[3]=f00fdfd9  B[3]=e7908aa5  C[3]=f31258a5  D[3]=11700606

Step 20: (r=29, s= 9)
A[0]=562fb229  B[0]=493163c6  C[0]=1e982a80  D[0]=bdbe64cb
A[1]=91527e9d  B[1]=e0034767  C[1]=4fecc11c  D[1]=e70fb550
A[2]=1aeab443  B[2]=1aa51b78  C[2]=34fbfeb9  D[2]=48c783fd
A[3]=d79a3327  B[3]=3e01fbfb  C[3]=e7908aa5  D[3]=f31258a5

Step 21: (r= 9, s=15)
A[0]=83082eb8  B[0]=5f6452ac  C[0]=493163c6  D[0]=1e982a80
A[1]=37d5cc9a  B[1]=a4fd3b22  C[1]=e0034767  D[1]=4fecc11c
A[2]=e43172f8  B[2]=d5688635  C[2]=1aa51b78  D[2]=34fbfeb9
A[3]=00c75a4e  B[3]=34664faf  C[3]=3e01fbfb  D[3]=e7908aa5

Step 22: (r=15, s= 5)
A[0]=7c0e8c24  B[0]=175c4184  C[0]=5f6452ac  D[0]=493163c6
A[1]=9e63af46  B[1]=e64d1bea  C[1]=a4fd3b22  D[1]=e0034767
A[2]=b293f02f  B[2]=b97c7218  C[2]=d5688635  D[2]=1aa51b78
A[3]=ff475090  B[3]=ad270063  C[3]=34664faf  D[3]=3e01fbfb

Step 23: (r= 5, s=29)
A[0]=313bd36a  B[0]=81d1848f  C[0]=175c4184  D[0]=5f6452ac
A[1]=34f664a4  B[1]=cc75e8d3  C[1]=e64d1bea  D[1]=a4fd3b22
A[2]=9835984d  B[2]=527e05f6  C[2]=b97c7218  D[2]=d5688635
A[3]=a746661b  B[3]=e8ea121f  C[3]=ad270063  D[3]=34664faf

Step 24: (r= 4, s=13)
A[0]=316cef7a  B[0]=13bd36a3  C[0]=81d1848f  D[0]=175c4184
A[1]=d7ea56c2  B[1]=4f664a43  C[1]=cc75e8d3  D[1]=e64d1bea
A[2]=7c0c3802  B[2]=835984d9  C[2]=527e05f6  D[2]=b97c7218
A[3]=bf0ecf02  B[3]=746661ba  C[3]=e8ea121f  D[3]=ad270063

Step 25: (r=13, s=10)
A[0]=2f7dbf48  B[0]=9def462d  C[0]=13bd36a3  D[0]=81d1848f
A[1]=1a9d2014  B[1]=4ad85afd  C[1]=4f664a43  D[1]=cc75e8d3
A[2]=52d0a21b  B[2]=87004f81  C[2]=835984d9  D[2]=527e05f6
A[3]=e0b006f3  B[3]=d9e057e1  C[3]=746661ba  D[3]=e8ea121f

Step 26: (r=10, s=25)
```

```
A[0]=191d68d6  B[0]=f6fd20bd  C[0]=9def462d  D[0]=13bd36a3
A[1]=559d90d5  B[1]=7480506a  C[1]=4ad85afd  D[1]=4f664a43
A[2]=b9ce88e0  B[2]=42886d4b  C[2]=87004f81  D[2]=835984d9
A[3]=ce9efd8a  B[3]=c01bcf82  C[3]=d9e057e1  D[3]=746661ba

Step 27: (r=25, s= 4)
A[0]=ce3f796d  B[0]=ac323ad1  C[0]=f6fd20bd  D[0]=9def462d
A[1]=73cea059  B[1]=aaab3b21  C[1]=7480506a  D[1]=4ad85afd
A[2]=bb647809  B[2]=c1739d11  C[2]=42886d4b  D[2]=87004f81
A[3]=cc040a78  B[3]=159d3dfb  C[3]=c01bcf82  D[3]=d9e057e1

Step 28: (r= 4, s=13)
A[0]=b012a83a  B[0]=e3f796dc  C[0]=ac323ad1  D[0]=f6fd20bd
A[1]=f91297d3  B[1]=3cea0597  C[1]=aaab3b21  D[1]=7480506a
A[2]=4af5b2bb  B[2]=b647809b  C[2]=c1739d11  D[2]=42886d4b
A[3]=3ebf447d  B[3]=c040a78c  C[3]=159d3dfb  D[3]=c01bcf82

Step 29: (r=13, s=10)
A[0]=180c8e25  B[0]=55075602  C[0]=e3f796dc  D[0]=ac323ad1
A[1]=1770aa99  B[1]=52fa7f22  C[1]=3cea0597  D[1]=aaab3b21
A[2]=43752ab2  B[2]=b657695e  C[2]=b647809b  D[2]=c1739d11
A[3]=02338bfe  B[3]=e88fa7d7  C[3]=c040a78c  D[3]=159d3dfb

Step 30: (r=10, s=25)
A[0]=defa67a9  B[0]=32389460  C[0]=55075602  D[0]=e3f796dc
A[1]=02807870  B[1]=c2aa645d  C[1]=52fa7f22  D[1]=3cea0597
A[2]=e9e7cacb  B[2]=d4aac90d  C[2]=b657695e  D[2]=b647809b
A[3]=14a2808c  B[3]=ce2ff808  C[3]=e88fa7d7  D[3]=c040a78c

Step 31: (r=25, s= 4)
A[0]=f222e828  B[0]=53bdf4cf  C[0]=32389460  D[0]=55075602
A[1]=923ee4bb  B[1]=e00500f0  C[1]=c2aa645d  D[1]=52fa7f22
A[2]=0ce18d5a  B[2]=97d3cf95  C[2]=d4aac90d  D[2]=b657695e
A[3]=81deafa3  B[3]=18294501  C[3]=ce2ff808  D[3]=e88fa7d7

Feed-Forward Step 32: (r= 4, s=13)
A[0]=c376c9cf  B[0]=222e828f  C[0]=53bdf4cf  D[0]=32389460
A[1]=8c4f3e4d  B[1]=23ee4bb9  C[1]=e00500f0  D[1]=c2aa645d
A[2]=7249f8a3  B[2]=ce18d5a0  C[2]=97d3cf95  D[2]=d4aac90d
A[3]=9cdeb460  B[3]=1deafa38  C[3]=18294501  D[3]=ce2ff808

Feed-Forward Step 33: (r=13, s=10)
A[0]=9a1bd7eb  B[0]=d939f86e  C[0]=222e828f  D[0]=53bdf4cf
A[1]=bfd430ab  B[1]=e7c9b189  C[1]=23ee4bb9  D[1]=e00500f0
A[2]=7316214c  B[2]=3f146e49  C[2]=ce18d5a0  D[2]=97d3cf95
A[3]=309951fe  B[3]=d68c139b  C[3]=1deafa38  D[3]=18294501

Feed-Forward Step 34: (r=10, s=25)
A[0]=dce2380b  B[0]=6f5fae68  C[0]=d939f86e  D[0]=222e828f
```

```
A[1]=58e9f8ad  B[1]=50c2aeff  C[1]=e7c9b189  D[1]=23ee4bb9
A[2]=3fe0d592  B[2]=588531cc  C[2]=3f146e49  D[2]=ce18d5a0
A[3]=b54f33e6  B[3]=6547f8c2  C[3]=d68c139b  D[3]=1deafa38

Feed-Forward Step 35: (r=25, s= 4)
A[0]=81dbeb5b  B[0]=17b9c470  C[0]=6f5fae68  D[0]=d939f86e
A[1]=c8e6d36c  B[1]=5ab1d3f1  C[1]=50c2aeff  D[1]=e7c9b189
A[2]=28a4b5c2  B[2]=247fc1ab  C[2]=588531cc  D[2]=3f146e49
A[3]=15f4a667  B[3]=cd6a9e67  C[3]=6547f8c2  D[3]=d68c139b
```

Compression Function Output

```
A[0]=81dbeb5b  B[0]=17b9c470  C[0]=6f5fae68  D[0]=d939f86e
A[1]=c8e6d36c  B[1]=5ab1d3f1  C[1]=50c2aeff  D[1]=e7c9b189
A[2]=28a4b5c2  B[2]=247fc1ab  C[2]=588531cc  D[2]=3f146e49
A[3]=15f4a667  B[3]=cd6a9e67  C[3]=6547f8c2  D[3]=d68c139b
```

Hash Function Output

```
5bebdb816cd3e6c8c2b5a42867a6f41570c4b917f1d3b15aabc17f24679e6acd
```

A.2.3 Two-block Message

We use the message made of 700 `1` bits.

First block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =  130  139   95   90   30    8   23   57
y[  8.. 15] =  129  152  176  135   15   86  140   53
y[ 16.. 23] =  193   34   88   34  136  231   70    7
y[ 24.. 31] =  225   75   44   72   68  127   35  120
y[ 32.. 39] =  241  151   22   70   34  193  146  163
y[ 40.. 47] =  249   20   11  219   17   74   73  235
y[ 48.. 55] =  253   50  134  235  137   79  165   92
y[ 56.. 63] =  255  194   67  159  197   44  211   92
y[ 64.. 71] =  256  181  162  182  227  122  234  179
y[ 72.. 79] =  128   91   81  207  242  115  117  226
y[ 80.. 87] =   64   80  169  160  121  120  187   42
y[ 88.. 95] =   32   58  213  108  189   44  222  244
```

```
y[ 96..103] =   16  248  235    8  223  133  111  210
y[104..111] =    8  180  246  193  240  238  184  157
y[112..119] =    4  177  123   70  120   85   92  171
y[120..127] =    2   76  190  217   60  190   46   94
```

Intermediate Expanded Message

```
Z[ 0] = aabaa439  410a44a7  05c815ae  2931109f
Z[ 1] = b41fa380  a7d6c577  3e260ad7  264dab73
Z[ 2] = 1892d1c0  18923f98  ed36a88f  050f3296
Z[ 3] = 3633e8e0  34081fcc  5bc73124  56b8194b
Z[ 4] = b366f470  32960fe6  d1c01892  bc12afc9
Z[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
Z[ 6] = 2422fd1c  f01aa71d  3917a948  427cbd84
Z[ 7] = d279fe8e  b92e306b  1fccd4a4  427cdec2
Z[ 8] = c914ff47  c9cdbb59  582aea52  c7a2ef61
Z[ 9] = 41c35c80  dbde3a89  531bf529  e999548d
Z[10] = 39d02e40  b9e7c068  56b85771  1e5acd6a
Z[11] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
Z[12] = f97f0b90  05c8f01a  a664e76e  de095037
Z[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
Z[14] = c63002e4  329658e3  3d6d56b8  c1da427c
Z[15] = 36ec0172  e318cf95  cf952b5c  43ee213e
Z[16] = ff178c69  a9895677  e4b21b4e  eb1114ef
Z[17] = 74808b80  49b9b647  f2590da7  6a7d9583
Z[18] = 3a40c5c0  afe85018  6e2191df  c04a3fb6
Z[19] = 1d20e2e0  d7f4280c  c21c3de4  e0251fdb
Z[20] = 0e90f170  ebfa1406  e10e1ef2  65079af9
Z[21] = 0748f8b8  f5fd0a03  f0870f79  bd8f4271
Z[22] = 03a4fc5c  6ff3900d  6d3892c8  53bcac44
Z[23] = 01d2fe2e  c3053cfb  369cc964  29ded622
Z[24] = bad4949a  bbbd51ea  6f0a0748  b90233e1
Z[25] = 52d3a06f  d27e90f6  68ab4e46  e3c9303d
Z[26] = 48d01ef2  a7b71ef2  6d38e856  263a065f
Z[27] = 34ca4443  624c4188  280c7397  f42b6d38
Z[28] = f7cf9f86  07483fb6  8f24c5c0  d539aa72
Z[29] = b9eb1234  c5c0dd6a  eeb5435a  a4fcebfa
Z[30] = b7302d82  3fb6ebfa  4d5d47e7  b1ba53bc
Z[31] = 452cc6a9  db98a6ce  c305280c  558e53bc
```

Expanded Message

```
W[ 0] = b366f470  32960fe6  d1c01892  bc12afc9
W[ 1] = 2422fd1c  f01aa71d  3917a948  427cbd84
W[ 2] = aabaa439  410a44a7  05c815ae  2931109f
W[ 3] = 1892d1c0  18923f98  ed36a88f  050f3296
W[ 4] = d279fe8e  b92e306b  1fccd4a4  427cdec2
W[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
W[ 6] = 3633e8e0  34081fcc  5bc73124  56b8194b
W[ 7] = b41fa380  a7d6c577  3e260ad7  264dab73
```

```
W[ 8] = 36ec0172  e318cf95  cf952b5c  43ee213e
W[ 9] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
W[10] = f97f0b90  05c8f01a  a664e76e  de095037
W[11] = c914ff47  c9cdbb59  582aea52  c7a2ef61
W[12] = 41c35c80  dbde3a89  531bf529  e999548d
W[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
W[14] = 39d02e40  b9e7c068  56b85771  1e5acd6a
W[15] = c63002e4  329658e3  3d6d56b8  c1da427c
W[16] = 74808b80  49b9b647  f2590da7  6a7d9583
W[17] = 3a40c5c0  afe85018  6e2191df  c04a3fb6
W[18] = 01d2fe2e  c3053cfb  369cc964  29ded622
W[19] = 0e90f170  ebfa1406  e10e1ef2  65079af9
W[20] = 03a4fc5c  6ff3900d  6d3892c8  53bcac44
W[21] = 0748f8b8  f5fd0a03  f0870f79  bd8f4271
W[22] = ff178c69  a9895677  e4b21b4e  eb1114ef
W[23] = 1d20e2e0  d7f4280c  c21c3de4  e0251fdb
W[24] = b7302d82  3fb6ebfa  4d5d47e7  b1ba53bc
W[25] = bad4949a  bbbd51ea  6f0a0748  b90233e1
W[26] = 52d3a06f  d27e90f6  68ab4e46  e3c9303d
W[27] = 452cc6a9  db98a6ce  c305280c  558e53bc
W[28] = 34ca4443  624c4188  280c7397  f42b6d38
W[29] = b9eb1234  c5c0dd6a  eeb5435a  a4fcebfa
W[30] = f7cf9f86  07483fb6  8f24c5c0  d539aa72
W[31] = 48d01ef2  a7b71ef2  6d38e856  263a065f
```

Feistel Steps

```
IV :
A[0]=4d567983  B[0]=aaf3d925  C[0]=c2c2ba14  D[0]=e2eaa8d2
A[1]=07190ba9  B[1]=3ee20b03  C[1]=49b3bcb4  D[1]=1ff47833
A[2]=8474577b  B[2]=afd5e751  C[2]=f67caf46  D[2]=d0c661a5
A[3]=39d726e9  B[3]=c96006d3  C[3]=668626c9  D[3]=55693de1

IV XOR M :
A[0]=b2a9867c  B[0]=550c26da  C[0]=3d3d45eb  D[0]=1d15572d
A[1]=f8e6f456  B[1]=c11df4fc  C[1]=b64c434b  D[1]=e00b87cc
A[2]=7b8ba884  B[2]=502a18ae  C[2]=098350b9  D[2]=2f399e5a
A[3]=c628d916  B[3]=369ff92c  C[3]=9979d936  D[3]=aa96c21e

Step  0: (r= 3, s=23)
A[0]=83ae6f00  B[0]=954c33e5  C[0]=550c26da  D[0]=3d3d45eb
A[1]=1d388b2c  B[1]=c737a2b7  C[1]=c11df4fc  D[1]=b64c434b
A[2]=05ef4abd  B[2]=dc5d4423  C[2]=502a18ae  D[2]=098350b9
A[3]=622045c8  B[3]=3146c8b6  C[3]=369ff92c  D[3]=9979d936

Step  1: (r=23, s=17)
A[0]=2c45647d  B[0]=8041d737  C[0]=954c33e5  D[0]=550c26da
A[1]=a6e9e75b  B[1]=960e9c45  C[1]=c737a2b7  D[1]=c11df4fc
A[2]=148b0507  B[2]=5e82f7a5  C[2]=dc5d4423  D[2]=502a18ae
```

```
A[3]=b4cabd72  B[3]=e4311022  C[3]=3146c8b6  D[3]=369ff92c

Step  2: (r=17, s=27)
A[0]=bf6deaab  B[0]=c8fa588a  C[0]=8041d737  D[0]=954c33e5
A[1]=50585f0a  B[1]=ceb74dd3  C[1]=960e9c45  D[1]=c737a2b7
A[2]=d84d916f  B[2]=0a0e2916  C[2]=5e82f7a5  D[2]=dc5d4423
A[3]=5121035d  B[3]=7ae56995  C[3]=e4311022  D[3]=3146c8b6

Step  3: (r=27, s= 3)
A[0]=04bddd11  B[0]=5dfb6f55  C[0]=c8fa588a  D[0]=8041d737
A[1]=8d00ec0a  B[1]=5282c2f8  C[1]=ceb74dd3  D[1]=960e9c45
A[2]=ab9ba9e0  B[2]=7ec26c8b  C[2]=0a0e2916  D[2]=5e82f7a5
A[3]=d2fad0a4  B[3]=ea89081a  C[3]=7ae56995  D[3]=e4311022

Step  4: (r= 3, s=23)
A[0]=c82d2a9e  B[0]=25eee888  C[0]=5dfb6f55  D[0]=c8fa588a
A[1]=5ce564f2  B[1]=68076054  C[1]=5282c2f8  D[1]=ceb74dd3
A[2]=0bc35582  B[2]=5cdd4f05  C[2]=7ec26c8b  D[2]=0a0e2916
A[3]=24182bef  B[3]=97d68526  C[3]=ea89081a  D[3]=7ae56995

Step  5: (r=23, s=17)
A[0]=724e56d2  B[0]=4f641695  C[0]=25eee888  D[0]=5dfb6f55
A[1]=2e71f93b  B[1]=792e72b2  C[1]=68076054  D[1]=5282c2f8
A[2]=7ef3af49  B[2]=c105e1aa  C[2]=5cdd4f05  D[2]=7ec26c8b
A[3]=9e6c39c4  B[3]=f7920c15  C[3]=97d68526  D[3]=ea89081a

Step  6: (r=17, s=27)
A[0]=22534a59  B[0]=ada4e49c  C[0]=4f641695  D[0]=25eee888
A[1]=651a7733  B[1]=f2765ce3  C[1]=792e72b2  D[1]=68076054
A[2]=3544393d  B[2]=5e92fde7  C[2]=c105e1aa  D[2]=5cdd4f05
A[3]=ad5bb75a  B[3]=73893cd8  C[3]=f7920c15  D[3]=97d68526

Step  7: (r=27, s= 3)
A[0]=3540b6f1  B[0]=c9129a52  C[0]=ada4e49c  D[0]=4f641695
A[1]=de4fc1ae  B[1]=9b28d3b9  C[1]=f2765ce3  D[1]=792e72b2
A[2]=495536b1  B[2]=e9aa21c9  C[2]=5e92fde7  D[2]=c105e1aa
A[3]=49243b46  B[3]=d56addba  C[3]=73893cd8  D[3]=f7920c15

Step  8: (r=28, s=19)
A[0]=b7aac35b  B[0]=13540b6f  C[0]=c9129a52  D[0]=ada4e49c
A[1]=1616076c  B[1]=ede4fc1a  C[1]=9b28d3b9  D[1]=f2765ce3
A[2]=a4547d09  B[2]=1495536b  C[2]=e9aa21c9  D[2]=5e92fde7
A[3]=6ac184b9  B[3]=649243b4  C[3]=d56addba  D[3]=73893cd8

Step  9: (r=19, s=22)
A[0]=fd2d5875  B[0]=1addbd56  C[0]=13540b6f  D[0]=c9129a52
A[1]=8711295a  B[1]=3b60b0b0  C[1]=ede4fc1a  D[1]=9b28d3b9
A[2]=c8fe5d93  B[2]=e84d22a3  C[2]=1495536b  D[2]=e9aa21c9
A[3]=38251682  B[3]=25cb560c  C[3]=649243b4  D[3]=d56addba
```

```
Step 10: (r=22, s= 7)
A[0]=dc52e005  B[0]=1d7f4b56  C[0]=1addbd56  D[0]=13540b6f
A[1]=0be9facb  B[1]=56a1c44a  C[1]=3b60b0b0  D[1]=ede4fc1a
A[2]=4b855c8c  B[2]=64f23f97  C[2]=e84d22a3  D[2]=1495536b
A[3]=5a6456d6  B[3]=a08e0945  C[3]=25cb560c  D[3]=649243b4

Step 11: (r= 7, s=28)
A[0]=01dff1ad  B[0]=297002ee  C[0]=1d7f4b56  D[0]=1addbd56
A[1]=a1538da3  B[1]=f4fd6585  C[1]=56a1c44a  D[1]=3b60b0b0
A[2]=39d5ed4b  B[2]=c2ae4625  C[2]=64f23f97  D[2]=e84d22a3
A[3]=3e8c4624  B[3]=322b6b2d  C[3]=a08e0945  D[3]=25cb560c

Step 12: (r=28, s=19)
A[0]=283869dc  B[0]=d01dff1a  C[0]=297002ee  D[0]=1d7f4b56
A[1]=55fe609f  B[1]=3a1538da  C[1]=f4fd6585  D[1]=56a1c44a
A[2]=7a85a75e  B[2]=b39d5ed4  C[2]=c2ae4625  D[2]=64f23f97
A[3]=618f6e6b  B[3]=43e8c462  C[3]=322b6b2d  D[3]=a08e0945

Step 13: (r=19, s=22)
A[0]=79f758dc  B[0]=4ee141c3  C[0]=d01dff1a  D[0]=297002ee
A[1]=b1026482  B[1]=04faaff3  C[1]=3a1538da  D[1]=f4fd6585
A[2]=b773b321  B[2]=3af3d42d  C[2]=b39d5ed4  D[2]=c2ae4625
A[3]=c0e9ad83  B[3]=735b0c7b  C[3]=43e8c462  D[3]=322b6b2d

Step 14: (r=22, s= 7)
A[0]=7bb5bec9  B[0]=371e7dd6  C[0]=4ee141c3  D[0]=d01dff1a
A[1]=44173cdb  B[1]=20ac4099  C[1]=04faaff3  D[1]=3a1538da
A[2]=cde61e7f  B[2]=c86ddcec  C[2]=3af3d42d  D[2]=b39d5ed4
A[3]=6f00fb20  B[3]=60f03a6b  C[3]=735b0c7b  D[3]=43e8c462

Step 15: (r= 7, s=28)
A[0]=1cfea59e  B[0]=dadf64bd  C[0]=371e7dd6  D[0]=4ee141c3
A[1]=61f600a6  B[1]=0b9e6da2  C[1]=20ac4099  D[1]=04faaff3
A[2]=1c1cb956  B[2]=f30f3fe6  C[2]=c86ddcec  D[2]=3af3d42d
A[3]=89a073fa  B[3]=807d9037  C[3]=60f03a6b  D[3]=735b0c7b

Step 16: (r=29, s= 9)
A[0]=4417d728  B[0]=c39fd4b3  C[0]=dadf64bd  D[0]=371e7dd6
A[1]=f681f91f  B[1]=cc3ec014  C[1]=0b9e6da2  D[1]=20ac4099
A[2]=385f5aae  B[2]=c383972a  C[2]=f30f3fe6  D[2]=c86ddcec
A[3]=5db32390  B[3]=51340e7f  C[3]=807d9037  D[3]=60f03a6b

Step 17: (r= 9, s=15)
A[0]=026cc6da  B[0]=2fae5088  C[0]=c39fd4b3  D[0]=dadf64bd
A[1]=69682b49  B[1]=03f23fed  C[1]=cc3ec014  D[1]=0b9e6da2
A[2]=570d3cb6  B[2]=beb55c70  C[2]=c383972a  D[2]=f30f3fe6
A[3]=b5dac9e3  B[3]=664720bb  C[3]=51340e7f  D[3]=807d9037
```

```
Step 18: (r=15, s= 5)
A[0]=23db2748  B[0]=636d0136  C[0]=2fae5088  D[0]=c39fd4b3
A[1]=e6bfc080  B[1]=15a4b4b4  C[1]=03f23fed  D[1]=cc3ec014
A[2]=6b66eb45  B[2]=9e5b2b86  C[2]=beb55c70  D[2]=c383972a
A[3]=76a8ce87  B[3]=64f1daed  C[3]=664720bb  D[3]=51340e7f

Step 19: (r= 5, s=29)
A[0]=cd112ba1  B[0]=7b64e904  C[0]=636d0136  D[0]=2fae5088
A[1]=ccdd836e  B[1]=d7f8101c  C[1]=15a4b4b4  D[1]=03f23fed
A[2]=83d187ae  B[2]=6cdd68ad  C[2]=9e5b2b86  D[2]=beb55c70
A[3]=7b5c82a2  B[3]=d519d0ee  C[3]=64f1daed  D[3]=664720bb

Step 20: (r=29, s= 9)
A[0]=c057a191  B[0]=39a22574  C[0]=7b64e904  D[0]=636d0136
A[1]=953a9d88  B[1]=d99bb06d  C[1]=d7f8101c  D[1]=15a4b4b4
A[2]=67d17de2  B[2]=d07a30f5  C[2]=6cdd68ad  D[2]=9e5b2b86
A[3]=f4e1ffd2  B[3]=4f6b9054  C[3]=d519d0ee  D[3]=64f1daed

Step 21: (r= 9, s=15)
A[0]=c2bc8338  B[0]=af432380  C[0]=39a22574  D[0]=7b64e904
A[1]=d6a5142e  B[1]=753b112a  C[1]=d99bb06d  D[1]=d7f8101c
A[2]=9df21fc6  B[2]=a2fbc4cf  C[2]=d07a30f5  D[2]=6cdd68ad
A[3]=1a1640c4  B[3]=c3ffa5e9  C[3]=4f6b9054  D[3]=d519d0ee

Step 22: (r=15, s= 5)
A[0]=d3b6629d  B[0]=419c615e  C[0]=af432380  D[0]=39a22574
A[1]=07f0e535  B[1]=8a176b52  C[1]=753b112a  D[1]=d99bb06d
A[2]=92cf79ba  B[2]=0fe34ef9  C[2]=a2fbc4cf  D[2]=d07a30f5
A[3]=ff643f73  B[3]=20620d0b  C[3]=c3ffa5e9  D[3]=4f6b9054

Step 23: (r= 5, s=29)
A[0]=efd31bfd  B[0]=76cc53ba  C[0]=419c615e  D[0]=af432380
A[1]=d1079e87  B[1]=fe1ca6a0  C[1]=8a176b52  D[1]=753b112a
A[2]=80ccde1a  B[2]=59ef3752  C[2]=0fe34ef9  D[2]=a2fbc4cf
A[3]=b92b2f6d  B[3]=ec87ee7f  C[3]=20620d0b  D[3]=c3ffa5e9

Step 24: (r= 4, s=13)
A[0]=09118224  B[0]=fd31bfde  C[0]=76cc53ba  D[0]=419c615e
A[1]=d9d051be  B[1]=1079e87d  C[1]=fe1ca6a0  D[1]=8a176b52
A[2]=972816e4  B[2]=0ccde1a8  C[2]=59ef3752  D[2]=0fe34ef9
A[3]=b1d06567  B[3]=92b2f6db  C[3]=ec87ee7f  D[3]=20620d0b

Step 25: (r=13, s=10)
A[0]=3e02ecd6  B[0]=30448122  C[0]=fd31bfde  D[0]=76cc53ba
A[1]=d33ad82a  B[1]=0a37db3a  C[1]=1079e87d  D[1]=fe1ca6a0
A[2]=22245050  B[2]=02dc92e5  C[2]=0ccde1a8  D[2]=59ef3752
A[3]=faf4fa11  B[3]=0cacf63a  C[3]=92b2f6db  D[3]=ec87ee7f

Step 26: (r=10, s=25)
```

```
A[0]=3b5deaf9  B[0]=0bb358f8  C[0]=30448122  D[0]=fd31bfde
A[1]=bce75ee8  B[1]=eb60ab4c  C[1]=0a37db3a  D[1]=1079e87d
A[2]=ed037bbb  B[2]=91414088  C[2]=02dc92e5  D[2]=0ccde1a8
A[3]=39654923  B[3]=d3e847eb  C[3]=0cacf63a  D[3]=92b2f6db

Step 27: (r=25, s= 4)
A[0]=a876d6d1  B[0]=f276bbd5  C[0]=0bb358f8  D[0]=30448122
A[1]=5aa8662e  B[1]=d179cebd  C[1]=eb60ab4c  D[1]=0a37db3a
A[2]=817f7297  B[2]=77da06f7  C[2]=91414088  D[2]=02dc92e5
A[3]=5a7e2426  B[3]=4672ca92  C[3]=d3e847eb  D[3]=0cacf63a

Step 28: (r= 4, s=13)
A[0]=cbfdeb68  B[0]=876d6d1a  C[0]=f276bbd5  D[0]=0bb358f8
A[1]=49400b62  B[1]=aa8662e5  C[1]=d179cebd  D[1]=eb60ab4c
A[2]=108fe4a2  B[2]=17f72978  C[2]=77da06f7  D[2]=91414088
A[3]=ffc8ed4f  B[3]=a7e24265  C[3]=4672ca92  D[3]=d3e847eb

Step 29: (r=13, s=10)
A[0]=8f04121d  B[0]=bd6d197f  C[0]=876d6d1a  D[0]=f276bbd5
A[1]=83e2affa  B[1]=016c4928  C[1]=aa8662e5  D[1]=d179cebd
A[2]=580f9b87  B[2]=fc944211  C[2]=17f72978  D[2]=77da06f7
A[3]=dd65cb02  B[3]=1da9fff9  C[3]=a7e24265  D[3]=4672ca92

Step 30: (r=10, s=25)
A[0]=7fb350f7  B[0]=1048763c  C[0]=bd6d197f  D[0]=876d6d1a
A[1]=c701c730  B[1]=8abfea0f  C[1]=016c4928  D[1]=aa8662e5
A[2]=27f33724  B[2]=3e6e1d60  C[2]=fc944211  D[2]=17f72978
A[3]=09e139e0  B[3]=972c0b75  C[3]=1da9fff9  D[3]=a7e24265

Step 31: (r=25, s= 4)
A[0]=22bdaf1e  B[0]=eeff66a1  C[0]=1048763c  D[0]=bd6d197f
A[1]=16c89270  B[1]=618e038e  C[1]=8abfea0f  D[1]=016c4928
A[2]=3161f58d  B[2]=484fe66e  C[2]=3e6e1d60  D[2]=fc944211
A[3]=1de64eec  B[3]=c013c273  C[3]=972c0b75  D[3]=1da9fff9

Feed-Forward Step 32: (r= 4, s=13)
A[0]=ff893679  B[0]=2bdaf1e2  C[0]=eeff66a1  D[0]=1048763c
A[1]=adfb6afb  B[1]=6c892701  C[1]=618e038e  D[1]=8abfea0f
A[2]=7d4838ec  B[2]=161f58d3  C[2]=484fe66e  D[2]=3e6e1d60
A[3]=99256d13  B[3]=de64eec1  C[3]=c013c273  D[3]=972c0b75

Feed-Forward Step 33: (r=13, s=10)
A[0]=58607d5b  B[0]=26cf3ff1  C[0]=2bdaf1e2  D[0]=eeff66a1
A[1]=e32f9cc9  B[1]=6d5f75bf  C[1]=6c892701  D[1]=618e038e
A[2]=fd303f2d  B[2]=071d8fa9  C[2]=161f58d3  D[2]=484fe66e
A[3]=1320348c  B[3]=ada27324  C[3]=de64eec1  D[3]=c013c273

Feed-Forward Step 34: (r=10, s=25)
A[0]=0ea7f1b1  B[0]=81f56d61  C[0]=26cf3ff1  D[0]=2bdaf1e2
```

```
A[1]=1703d23b  B[1]=be73278c  C[1]=6d5f75bf  D[1]=6c892701
A[2]=e081452c  B[2]=c0fcb7f4  C[2]=071d8fa9  D[2]=161f58d3
A[3]=c25b2553  B[3]=80d2304c  C[3]=ada27324  D[3]=de64eec1

Feed-Forward Step 35: (r=25, s= 4)
A[0]=a2b5579c  B[0]=621d4fe3  C[0]=81f56d61  D[0]=26cf3ff1
A[1]=078d6e8a  B[1]=762e07a4  C[1]=be73278c  D[1]=6d5f75bf
A[2]=5e52a97e  B[2]=59c1028a  C[2]=c0fcb7f4  D[2]=071d8fa9
A[3]=7e274051  B[3]=a784b64a  C[3]=80d2304c  D[3]=ada27324
```

Compression Function Output

```
A[0]=a2b5579c  B[0]=621d4fe3  C[0]=81f56d61  D[0]=26cf3ff1
A[1]=078d6e8a  B[1]=762e07a4  C[1]=be73278c  D[1]=6d5f75bf
A[2]=5e52a97e  B[2]=59c1028a  C[2]=c0fcb7f4  D[2]=071d8fa9
A[3]=7e274051  B[3]=a784b64a  C[3]=80d2304c  D[3]=ada27324
```

Second block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff f0
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  195  145  230   47   52  203  238  249
y[  8.. 15] =   12   96  215  134  192  149   97   86
y[ 16.. 23] =  125   71  253   29   78  108  111   14
y[ 24.. 31] =   76   62  254  175   50   20  235   16
y[ 32.. 39] =  224   33  108  228   44  109  107   42
y[ 40.. 47] =  154  246  148  136  113  117   81  174
y[ 48.. 55] =   56  126  148   62  151   51  153  212
y[ 56.. 63] =   51  141  153   14    7  209  219   46
y[ 64.. 71] =   14   20   75  104   16  215  142  205
y[ 72.. 79] =  162   98  256  209  240   66   86   20
y[ 80.. 87] =  132   44   30    5   90   44  223  126
y[ 88.. 95] =  226  151   51  249  247   44  154   79
y[ 96..103] =   33  241  111  146   19  101   97  216
y[104..111] =   50  140   61  172   65  117   52  126
y[112..119] =  201  236  251   10   65  247  201  209
y[120..127] =   24   46  196   55  113   95   83  196
```

Intermediate Expanded Message

```
Z[ 0] = af10d332  21f7ec7d  d8fa2594  fa38f245
Z[ 1] = 456008ac  a71de1a6  b1f4d107  3e264619
Z[ 2] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
Z[ 3] = 2cce36ec  c4befdd5  0e742422  0b90f01a
Z[ 4] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
Z[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
Z[ 6] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
Z[ 7] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
Z[ 8] = 0e740a1e  4b283633  e1a60b90  da6cace5
Z[ 9] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
Z[10] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
Z[11] = b366e999  fa3824db  1fccf8c6  3917b591
Z[12] = f47017d9  afc95037  48fd0dbb  e25f4619
Z[13] = ab732422  c2932c15  548d2ef9  5b0e2594
Z[14] = f0d3d788  073afbaa  f8c62ef9  dd50d788
Z[15] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
Z[16] = 0cbec792  4443e76d  0e902f54  9755eeb5
Z[17] = a9890aec  ff17d9c6  f087c4d7  4e465849
Z[18] = 8e3b71c5  1b4efc5c  51ea46fe  e10e6507
Z[19] = e3c9452c  2e6bfd45  f6e62d82  a241ebfa
Z[20] = 1e09e1f7  6507624c  114b280c  58496163
Z[21] = 2d82a241  37859ccb  3b2966d9  2f5449b9
Z[22] = cd0832f8  fa8a9ccb  3b299f86  cd08a158
Z[23] = 15d82e6b  c87ba158  66d9065f  4b8bdd6a
Z[24] = 12349a10  5ea82ac7  d9c6ceda  d0acf8b8
Z[25] = 59325760  d450900d  3c129db4  12344e46
Z[26] = 280c409f  048d1a65  280c624c  72ae0cbe
Z[27] = 9f86386e  f8b8b55e  280c1234  47e70e90
Z[28] = f1701e09  9af9e59b  5bed6335  daaf263a
Z[29] = 9583f5fd  b2a391df  6a7d6a7d  72aeb475
Z[30] = ece372ae  091a386e  f6e62e6b  d450d70b
Z[31] = 29de966c  320f0cbe  5677d450  c87b29de
```

Expanded Message

```
W[ 0] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
W[ 1] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
W[ 2] = af10d332  21f7ec7d  d8fa2594  fa38f245
W[ 3] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
W[ 4] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
W[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
W[ 6] = 2cce36ec  c4befdd5  0e742422  0b90f01a
W[ 7] = 456008ac  a71de1a6  b1f4d107  3e264619
W[ 8] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
W[ 9] = b366e999  fa3824db  1fccf8c6  3917b591
W[10] = f47017d9  afc95037  48fd0dbb  e25f4619
W[11] = 0e740a1e  4b283633  e1a60b90  da6cace5
W[12] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
W[13] = ab732422  c2932c15  548d2ef9  5b0e2594
```

```
W[14] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
W[15] = f0d3d788  073afbaa  f8c62ef9  dd50d788
W[16] = a9890aec  ff17d9c6  f087c4d7  4e465849
W[17] = 8e3b71c5  1b4efc5c  51ea46fe  e10e6507
W[18] = 15d82e6b  c87ba158  66d9065f  4b8bdd6a
W[19] = 1e09e1f7  6507624c  114b280c  58496163
W[20] = cd0832f8  fa8a9ccb  3b299f86  cd08a158
W[21] = 2d82a241  37859ccb  3b2966d9  2f5449b9
W[22] = 0cbec792  4443e76d  0e902f54  9755eeb5
W[23] = e3c9452c  2e6bfd45  f6e62d82  a241ebfa
W[24] = ece372ae  091a386e  f6e62e6b  d450d70b
W[25] = 12349a10  5ea82ac7  d9c6ceda  d0acf8b8
W[26] = 59325760  d450900d  3c129db4  12344e46
W[27] = 29de966c  320f0cbe  5677d450  c87b29de
W[28] = 9f86386e  f8b8b55e  280c1234  47e70e90
W[29] = 9583f5fd  b2a391df  6a7d6a7d  72aeb475
W[30] = f1701e09  9af9e59b  5bed6335  daaf263a
W[31] = 280c409f  048d1a65  280c624c  72ae0cbe
```

Feistel Steps

```
IV :
A[0]=a2b5579c  B[0]=621d4fe3  C[0]=81f56d61  D[0]=26cf3ff1
A[1]=078d6e8a  B[1]=762e07a4  C[1]=be73278c  D[1]=6d5f75bf
A[2]=5e52a97e  B[2]=59c1028a  C[2]=c0fcb7f4  D[2]=071d8fa9
A[3]=7e274051  B[3]=a784b64a  C[3]=80d2304c  D[3]=ada27324

IV XOR M :
A[0]=5d4aa863  B[0]=9de2b01c  C[0]=81f56d61  D[0]=26cf3ff1
A[1]=f8729175  B[1]=86d1f85b  C[1]=be73278c  D[1]=6d5f75bf
A[2]=a1ad5681  B[2]=59c1028a  C[2]=c0fcb7f4  D[2]=071d8fa9
A[3]=81d8bfae  B[3]=a784b64a  C[3]=80d2304c  D[3]=ada27324

Step  0: (r= 3, s=23)
A[0]=5002dc35  B[0]=ea55431a  C[0]=9de2b01c  D[0]=81f56d61
A[1]=3cc4a157  B[1]=c3948baf  C[1]=86d1f85b  D[1]=be73278c
A[2]=c391d79d  B[2]=0d6ab40d  C[2]=59c1028a  D[2]=c0fcb7f4
A[3]=6e1173c8  B[3]=0ec5fd74  C[3]=a784b64a  D[3]=80d2304c

Step  1: (r=23, s=17)
A[0]=bac51eb2  B[0]=1aa8016e  C[0]=ea55431a  D[0]=9de2b01c
A[1]=47e3e468  B[1]=ab9e6250  C[1]=c3948baf  D[1]=86d1f85b
A[2]=197bff9f  B[2]=cee1c8eb  C[2]=0d6ab40d  D[2]=59c1028a
A[3]=606c41f7  B[3]=e43708b9  C[3]=0ec5fd74  D[3]=a784b64a

Step  2: (r=17, s=27)
A[0]=492adefb  B[0]=3d65758a  C[0]=1aa8016e  D[0]=ea55431a
A[1]=f8a1357b  B[1]=c8d08fc7  C[1]=ab9e6250  D[1]=c3948baf
A[2]=12c9774c  B[2]=ff3e32f7  C[2]=cee1c8eb  D[2]=0d6ab40d
```

```
A[3]=3de890b4  B[3]=83eec0d8  C[3]=e43708b9  D[3]=0ec5fd74

Step  3: (r=27, s= 3)
A[0]=a9eca194  B[0]=da4956f7  C[0]=3d65758a  D[0]=1aa8016e
A[1]=fb8fd76c  B[1]=dfc509ab  C[1]=c8d08fc7  D[1]=ab9e6250
A[2]=6eec7f16  B[2]=60964bba  C[2]=ff3e32f7  D[2]=cee1c8eb
A[3]=37b4fde0  B[3]=a1ef4485  C[3]=83eec0d8  D[3]=e43708b9

Step  4: (r= 3, s=23)
A[0]=67241980  B[0]=4f650ca5  C[0]=da4956f7  D[0]=3d65758a
A[1]=4970b054  B[1]=dc7ebb67  C[1]=dfc509ab  D[1]=c8d08fc7
A[2]=277284c9  B[2]=7763f8b3  C[2]=60964bba  D[2]=ff3e32f7
A[3]=de536dc0  B[3]=bda7ef01  C[3]=a1ef4485  D[3]=83eec0d8

Step  5: (r=23, s=17)
A[0]=6ff03366  B[0]=c033920c  C[0]=4f650ca5  D[0]=da4956f7
A[1]=596656eb  B[1]=2a24b858  C[1]=dc7ebb67  D[1]=dfc509ab
A[2]=c4dc2ed4  B[2]=6493b942  C[2]=7763f8b3  D[2]=60964bba
A[3]=91f79dc2  B[3]=e06f29b6  C[3]=bda7ef01  D[3]=a1ef4485

Step  6: (r=17, s=27)
A[0]=e88af7cc  B[0]=66ccdfe0  C[0]=c033920c  D[0]=4f650ca5
A[1]=c6b435ef  B[1]=add6b2cc  C[1]=2a24b858  D[1]=dc7ebb67
A[2]=b2241534  B[2]=5da989b8  C[2]=6493b942  D[2]=7763f8b3
A[3]=68a4c8c9  B[3]=3b8523ef  C[3]=e06f29b6  D[3]=bda7ef01

Step  7: (r=27, s= 3)
A[0]=50108994  B[0]=674457be  C[0]=66ccdfe0  D[0]=c033920c
A[1]=ddcf950f  B[1]=7e35a1af  C[1]=add6b2cc  D[1]=2a24b858
A[2]=57176f12  B[2]=a59120a9  C[2]=5da989b8  D[2]=6493b942
A[3]=a1d099fa  B[3]=4b452646  C[3]=3b8523ef  D[3]=e06f29b6

Step  8: (r=28, s=19)
A[0]=84df4b8e  B[0]=45010899  C[0]=674457be  D[0]=66ccdfe0
A[1]=a607e6c2  B[1]=fddcf950  C[1]=7e35a1af  D[1]=add6b2cc
A[2]=5a7ab0f5  B[2]=257176f1  C[2]=a59120a9  D[2]=5da989b8
A[3]=84c78595  B[3]=aa1d099f  C[3]=4b452646  D[3]=3b8523ef

Step  9: (r=19, s=22)
A[0]=c2757d78  B[0]=5c7426fa  C[0]=45010899  D[0]=674457be
A[1]=a19d37e8  B[1]=3615303f  C[1]=fddcf950  D[1]=7e35a1af
A[2]=0a750028  B[2]=87aad3d5  C[2]=257176f1  D[2]=a59120a9
A[3]=dd7abc54  B[3]=2cac263c  C[3]=aa1d099f  D[3]=4b452646

Step 10: (r=22, s= 7)
A[0]=9e4ce590  B[0]=5e309d5f  C[0]=5c7426fa  D[0]=45010899
A[1]=3fac6e04  B[1]=fa28674d  C[1]=3615303f  D[1]=fddcf950
A[2]=358337e9  B[2]=0a029d40  C[2]=87aad3d5  D[2]=257176f1
A[3]=e2f1667a  B[3]=15375eaf  C[3]=2cac263c  D[3]=aa1d099f
```

```
Step 11: (r= 7, s=28)
A[0]=93cd9714  B[0]=2672c84f  C[0]=5e309d5f  D[0]=5c7426fa
A[1]=e9cfdef6  B[1]=d637021f  C[1]=fa28674d  D[1]=3615303f
A[2]=2ecb279c  B[2]=c19bf49a  C[2]=0a029d40  D[2]=87aad3d5
A[3]=4f7f381a  B[3]=78b33d71  C[3]=15375eaf  D[3]=2cac263c

Step 12: (r=28, s=19)
A[0]=6c32cbaa  B[0]=493cd971  C[0]=2672c84f  D[0]=5e309d5f
A[1]=f865461c  B[1]=6e9cfdef  C[1]=d637021f  D[1]=fa28674d
A[2]=8e1e02cc  B[2]=c2ecb279  C[2]=c19bf49a  D[2]=0a029d40
A[3]=c7d97536  B[3]=a4f7f381  C[3]=78b33d71  D[3]=15375eaf

Step 13: (r=19, s=22)
A[0]=d181e692  B[0]=5d536196  C[0]=493cd971  D[0]=2672c84f
A[1]=0a24fb01  B[1]=30e7c32a  C[1]=6e9cfdef  D[1]=d637021f
A[2]=219bad35  B[2]=166470f0  C[2]=c2ecb279  D[2]=c19bf49a
A[3]=8dfd1168  B[3]=a9b63ecb  C[3]=a4f7f381  D[3]=78b33d71

Step 14: (r=22, s= 7)
A[0]=02cb4593  B[0]=a4b46079  C[0]=5d536196  D[0]=493cd971
A[1]=89d1e2ed  B[1]=c042893e  C[1]=30e7c32a  D[1]=6e9cfdef
A[2]=eab59430  B[2]=4d4866eb  C[2]=166470f0  D[2]=c2ecb279
A[3]=8160b4b9  B[3]=5a237f44  C[3]=a9b63ecb  D[3]=a4f7f381

Step 15: (r= 7, s=28)
A[0]=acdfb7ec  B[0]=65a2c981  C[0]=a4b46079  D[0]=5d536196
A[1]=e50c854d  B[1]=e8f176c4  C[1]=c042893e  D[1]=30e7c32a
A[2]=d0fbd226  B[2]=5aca1875  C[2]=4d4866eb  D[2]=166470f0
A[3]=7b80c912  B[3]=b05a5cc0  C[3]=5a237f44  D[3]=a9b63ecb

Step 16: (r=29, s= 9)
A[0]=d87ba09a  B[0]=959bf6fd  C[0]=65a2c981  D[0]=a4b46079
A[1]=d2c2e542  B[1]=bca190a9  C[1]=e8f176c4  D[1]=c042893e
A[2]=02715fc6  B[2]=da1f7a44  C[2]=5aca1875  D[2]=4d4866eb
A[3]=fccc40f9  B[3]=4f701922  C[3]=b05a5cc0  D[3]=5a237f44

Step 17: (r= 9, s=15)
A[0]=766de83e  B[0]=f74135b0  C[0]=959bf6fd  D[0]=65a2c981
A[1]=6eced625  B[1]=85ca85a5  C[1]=bca190a9  D[1]=e8f176c4
A[2]=89fa028c  B[2]=e2bf8c04  C[2]=da1f7a44  D[2]=5aca1875
A[3]=f776f972  B[3]=9881f3f9  C[3]=4f701922  D[3]=b05a5cc0

Step 18: (r=15, s= 5)
A[0]=d4d89315  B[0]=f41f3b36  C[0]=f74135b0  D[0]=959bf6fd
A[1]=bf32d45e  B[1]=6b12b767  C[1]=85ca85a5  D[1]=bca190a9
A[2]=090c5ecd  B[2]=014644fd  C[2]=e2bf8c04  D[2]=da1f7a44
A[3]=7e2bb84f  B[3]=7cb97bbb  C[3]=9881f3f9  D[3]=4f701922
```

```
Step 19: (r= 5, s=29)
A[0]=36e3bbb6  B[0]=9b1262ba  C[0]=f41f3b36  D[0]=f74135b0
A[1]=4f277b0a  B[1]=e65a8bd7  C[1]=6b12b767  D[1]=85ca85a5
A[2]=54f6af9d  B[2]=218bd9a1  C[2]=014644fd  D[2]=e2bf8c04
A[3]=fae6ea9f  B[3]=c57709ef  C[3]=7cb97bbb  D[3]=9881f3f9

Step 20: (r=29, s= 9)
A[0]=b8a59a47  B[0]=c6dc7776  C[0]=9b1262ba  D[0]=f41f3b36
A[1]=7a5a45d1  B[1]=49e4ef61  C[1]=e65a8bd7  D[1]=6b12b767
A[2]=a9d77da0  B[2]=aa9ed5f3  C[2]=218bd9a1  D[2]=014644fd
A[3]=cade983b  B[3]=ff5cdd53  C[3]=c57709ef  D[3]=7cb97bbb

Step 21: (r= 9, s=15)
A[0]=dc82810f  B[0]=4b348f71  C[0]=c6dc7776  D[0]=9b1262ba
A[1]=dd3615ea  B[1]=b48ba2f4  C[1]=49e4ef61  D[1]=e65a8bd7
A[2]=81ec6a9c  B[2]=aefb4153  C[2]=aa9ed5f3  D[2]=218bd9a1
A[3]=de72ff09  B[3]=bd307795  C[3]=ff5cdd53  D[3]=c57709ef

Step 22: (r=15, s= 5)
A[0]=02047964  B[0]=4087ee41  C[0]=4b348f71  D[0]=c6dc7776
A[1]=882853ba  B[1]=0af56e9b  C[1]=b48ba2f4  D[1]=49e4ef61
A[2]=a3d1475c  B[2]=354e40f6  C[2]=aefb4153  D[2]=aa9ed5f3
A[3]=92b46546  B[3]=7f84ef39  C[3]=bd307795  D[3]=ff5cdd53

Step 23: (r= 5, s=29)
A[0]=d421fe52  B[0]=408f2c80  C[0]=4087ee41  D[0]=4b348f71
A[1]=7a483580  B[1]=050a7751  C[1]=0af56e9b  D[1]=b48ba2f4
A[2]=6e367fea  B[2]=7a28eb94  C[2]=354e40f6  D[2]=aefb4153
A[3]=8cb9928c  B[3]=568ca8d2  C[3]=7f84ef39  D[3]=bd307795

Step 24: (r= 4, s=13)
A[0]=8a47671a  B[0]=421fe52d  C[0]=408f2c80  D[0]=4087ee41
A[1]=ad6f9cf9  B[1]=a4835807  C[1]=050a7751  D[1]=0af56e9b
A[2]=07036cf1  B[2]=e367fea6  C[2]=7a28eb94  D[2]=354e40f6
A[3]=aaf21fc7  B[3]=cb9928c8  C[3]=568ca8d2  D[3]=7f84ef39

Step 25: (r=13, s=10)
A[0]=9d758735  B[0]=ece35148  C[0]=421fe52d  D[0]=408f2c80
A[1]=c84a8194  B[1]=f39f35ad  C[1]=a4835807  D[1]=050a7751
A[2]=f0e12371  B[2]=6d9e20e0  C[2]=e367fea6  D[2]=7a28eb94
A[3]=2de23a68  B[3]=43f8f55e  C[3]=cb9928c8  D[3]=568ca8d2

Step 26: (r=10, s=25)
A[0]=59b9fa80  B[0]=d61cd675  C[0]=ece35148  D[0]=421fe52d
A[1]=50099484  B[1]=2a065321  C[1]=f39f35ad  D[1]=a4835807
A[2]=8639d82d  B[2]=848dc7c3  C[2]=6d9e20e0  D[2]=e367fea6
A[3]=96764ac4  B[3]=88e9a0b7  C[3]=43f8f55e  D[3]=cb9928c8

Step 27: (r=25, s= 4)
```

```
A[0]=0e35013f  B[0]=00b373f5  C[0]=d61cd675  D[0]=ece35148
A[1]=a33cd2dc  B[1]=08a01329  C[1]=2a065321  D[1]=f39f35ad
A[2]=00282807  B[2]=5b0c73b0  C[2]=848dc7c3  D[2]=6d9e20e0
A[3]=badcf7f5  B[3]=892cec95  C[3]=88e9a0b7  D[3]=43f8f55e

Step 28: (r= 4, s=13)
A[0]=de27f2c3  B[0]=e35013f0  C[0]=00b373f5  D[0]=d61cd675
A[1]=3596022a  B[1]=33cd2dca  C[1]=08a01329  D[1]=2a065321
A[2]=b62306a6  B[2]=02828070  C[2]=5b0c73b0  D[2]=848dc7c3
A[3]=d0e19063  B[3]=adcf7f5b  C[3]=892cec95  D[3]=88e9a0b7

Step 29: (r=13, s=10)
A[0]=830e06d3  B[0]=fe587bc4  C[0]=e35013f0  D[0]=00b373f5
A[1]=18757efc  B[1]=c04546b2  C[1]=33cd2dca  D[1]=08a01329
A[2]=f51906b6  B[2]=60d4d6c4  C[2]=02828070  D[2]=5b0c73b0
A[3]=179e79da  B[3]=320c7a1c  C[3]=adcf7f5b  D[3]=892cec95

Step 30: (r=10, s=25)
A[0]=73a6e7ac  B[0]=381b4e0c  C[0]=fe587bc4  D[0]=e35013f0
A[1]=b5830cdb  B[1]=d5fbf061  C[1]=c04546b2  D[1]=33cd2dca
A[2]=2c167d19  B[2]=641adbd4  C[2]=60d4d6c4  D[2]=02828070
A[3]=b751b0f0  B[3]=79e7685e  C[3]=320c7a1c  D[3]=adcf7f5b

Step 31: (r=25, s= 4)
A[0]=89c46eb2  B[0]=58e74dcf  C[0]=381b4e0c  D[0]=fe587bc4
A[1]=c3477581  B[1]=b76b0619  C[1]=d5fbf061  D[1]=c04546b2
A[2]=434376d7  B[2]=32582cfa  C[2]=641adbd4  D[2]=60d4d6c4
A[3]=f39b4d6e  B[3]=e16ea361  C[3]=79e7685e  D[3]=320c7a1c

Feed-Forward Step 32: (r= 4, s=13)
A[0]=ddb2b22c  B[0]=9c46eb28  C[0]=58e74dcf  D[0]=381b4e0c
A[1]=fb6b196d  B[1]=3477581c  C[1]=b76b0619  D[1]=d5fbf061
A[2]=3a39f4cc  B[2]=34376d74  C[2]=32582cfa  D[2]=641adbd4
A[3]=d7c29e5c  B[3]=39b4d6ef  C[3]=e16ea361  D[3]=79e7685e

Feed-Forward Step 33: (r=13, s=10)
A[0]=65652847  B[0]=56459bb6  C[0]=9c46eb28  D[0]=58e74dcf
A[1]=8a9e21b8  B[1]=632dbf6d  C[1]=3477581c  D[1]=b76b0619
A[2]=88f6eeb1  B[2]=3e998747  C[2]=34376d74  D[2]=32582cfa
A[3]=a1f1dc93  B[3]=53cb9af8  C[3]=39b4d6ef  D[3]=e16ea361

Feed-Forward Step 34: (r=10, s=25)
A[0]=99290f2f  B[0]=94a11d95  C[0]=56459bb6  D[0]=9c46eb28
A[1]=6acae5d4  B[1]=7886e22a  C[1]=632dbf6d  D[1]=3477581c
A[2]=fb00ea6d  B[2]=dbbac623  C[2]=3e998747  D[2]=34376d74
A[3]=cb7eef07  B[3]=c7724e87  C[3]=53cb9af8  D[3]=39b4d6ef

Feed-Forward Step 35: (r=25, s= 4)
A[0]=a75388c7  B[0]=5f32521e  C[0]=94a11d95  D[0]=56459bb6
```

```
A[1]=93e28214  B[1]=a8d595cb  C[1]=7886e22a  D[1]=632dbf6d
A[2]=57c1d9cc  B[2]=dbf601d4  C[2]=dbbac623  D[2]=3e998747
A[3]=13dce349  B[3]=0f96fdde  C[3]=c7724e87  D[3]=53cb9af8
```

Compression Function Output

```
A[0]=a75388c7  B[0]=5f32521e  C[0]=94a11d95  D[0]=56459bb6
A[1]=93e28214  B[1]=a8d595cb  C[1]=7886e22a  D[1]=632dbf6d
A[2]=57c1d9cc  B[2]=dbf601d4  C[2]=dbbac623  D[2]=3e998747
A[3]=13dce349  B[3]=0f96fdde  C[3]=c7724e87  D[3]=53cb9af8
```

Final block

```
M[  0..  7] = bc 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  192  108  141  233   96  118  165  228
y[  8.. 15] =   32  222   69   67  220  239   71  167
y[ 16.. 23] =  128  193   38  144  230  170  141   22
y[ 24.. 31] =   43   18   57  253   52   49  135   90
y[ 32.. 39] =  220  141  251   80   69   78  112  146
y[ 40.. 47] =  246  192  105  151  220  224    4   25
y[ 48.. 55] =  248  255  112   48  106   24   23   60
y[ 56.. 63] =  177  160   25  225  205   82   19  141
y[ 64.. 71] =  184   11  235  143   23    1  211  148
y[ 72.. 79] =   87  154   50   52  156  137   48  209
y[ 80.. 87] =  248  183   81  232  146  206  235   97
y[ 88.. 95] =   76  101   62  123   67   70  241   29
y[ 96..103] =  156  235  125   39   50   41    7  230
y[104..111] =  130  184   14  225  156  152  115   94
y[112..119] =  128  121    7   71   13   95   96   59
y[120..127] =  199  216   94  151  171   37  100  235
```

Intermediate Expanded Message

```
Z[ 0] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
Z[ 1] = e6b51720  306b31dd  f2fee543  bef6334f
Z[ 2] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
Z[ 3] = 0d021f13  fd1c2931  23692594  410aa7d6
Z[ 4] = ac2ce543  39d0fbaa  385e31dd  afc950f0
Z[ 5] = d107f80d  b3664be1  e827e543  121102e4
Z[ 6] = fe8ef97f  22b050f0  11584c9a  2b5c109f
```

```
Z[ 7] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
Z[ 8] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
Z[ 9] = b5913edf  25942422  a948b703  dd5022b0
Z[10] = ca86f97f  edef3a89  db25afc9  4619f01a
Z[11] = 48fd36ec  58e32cce  3296306b  14f5f470
Z[12] = f01ab703  1c2f5a55  1da12422  ec7d050f
Z[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
Z[14] = 57715c80  334f050f  44a70965  2aa34560
Z[15] = e25fd616  b36643ee  1abdc1da  f01a4844
Z[16] = bd8fc4d7  ebfa966c  14ef5760  d622ac44
Z[17] = 4f2f1d20  2d823ecd  a413de53  2bb0409f
Z[18] = f7cf7480  49b92296  9af9e76d  ebfa966c
Z[19] = 452c2723  386e33e1  3cfb2f54  f17090f6
Z[20] = a413de53  71c5fa8a  2d823ecd  065f65f0
Z[21] = 8c69f5fd  0cbe5f91  a413de53  68ab03a4
Z[22] = 7480f7cf  065f65f0  0bd5607a  576014ef
Z[23] = cb36b730  558e16c1  b1bad0ac  5b04114b
Z[24] = 0a03624c  983eea28  00e96b66  9ccbe59b
Z[25] = a241e025  2f543cfb  92c8ef9e  d450ae16
Z[26] = bca6c5c0  e93f9927  d195b0d1  58491406
Z[27] = 5bed1062  6ff3fc5c  3fb62c99  1a6551ea
Z[28] = ebfa966c  237f48d0  255146fe  e76d9af9
Z[29] = bd8fc4d7  e2e09f86  a06fe1f7  558e16c1
Z[30] = 6e21fe2e  409f2bb0  567715d8  35b3369c
Z[31] = daafa7b7  9f86e2e0  21ad4aa2  ebfa966c
```

Expanded Message

```
W[ 0] = ac2ce543  39d0fbaa  385e31dd  afc950f0
W[ 1] = fe8ef97f  22b050f0  11584c9a  2b5c109f
W[ 2] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
W[ 3] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
W[ 4] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
W[ 5] = d107f80d  b3664be1  e827e543  121102e4
W[ 6] = 0d021f13  fd1c2931  23692594  410aa7d6
W[ 7] = e6b51720  306b31dd  f2fee543  bef6334f
W[ 8] = e25fd616  b36643ee  1abdc1da  f01a4844
W[ 9] = 48fd36ec  58e32cce  3296306b  14f5f470
W[10] = f01ab703  1c2f5a55  1da12422  ec7d050f
W[11] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
W[12] = b5913edf  25942422  a948b703  dd5022b0
W[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
W[14] = ca86f97f  edef3a89  db25afc9  4619f01a
W[15] = 57715c80  334f050f  44a70965  2aa34560
W[16] = 4f2f1d20  2d823ecd  a413de53  2bb0409f
W[17] = f7cf7480  49b92296  9af9e76d  ebfa966c
W[18] = cb36b730  558e16c1  b1bad0ac  5b04114b
W[19] = a413de53  71c5fa8a  2d823ecd  065f65f0
W[20] = 7480f7cf  065f65f0  0bd5607a  576014ef
```

```
W[21] = 8c69f5fd  0cbe5f91  a413de53  68ab03a4
W[22] = bd8fc4d7  ebfa966c  14ef5760  d622ac44
W[23] = 452c2723  386e33e1  3cfb2f54  f17090f6
W[24] = 6e21fe2e  409f2bb0  567715d8  35b3369c
W[25] = 0a03624c  983eea28  00e96b66  9ccbe59b
W[26] = a241e025  2f543cfb  92c8ef9e  d450ae16
W[27] = daafa7b7  9f86e2e0  21ad4aa2  ebfa966c
W[28] = 5bed1062  6ff3fc5c  3fb62c99  1a6551ea
W[29] = bd8fc4d7  e2e09f86  a06fe1f7  558e16c1
W[30] = ebfa966c  237f48d0  255146fe  e76d9af9
W[31] = bca6c5c0  e93f9927  d195b0d1  58491406
```

Feistel Steps

```
IV :
A[0]=a75388c7  B[0]=5f32521e  C[0]=94a11d95  D[0]=56459bb6
A[1]=93e28214  B[1]=a8d595cb  C[1]=7886e22a  D[1]=632dbf6d
A[2]=57c1d9cc  B[2]=dbf601d4  C[2]=dbbac623  D[2]=3e998747
A[3]=13dce349  B[3]=0f96fdde  C[3]=c7724e87  D[3]=53cb9af8

IV XOR M :
A[0]=a7538a7b  B[0]=5f32521e  C[0]=94a11d95  D[0]=56459bb6
A[1]=93e28214  B[1]=a8d595cb  C[1]=7886e22a  D[1]=632dbf6d
A[2]=57c1d9cc  B[2]=dbf601d4  C[2]=dbbac623  D[2]=3e998747
A[3]=13dce349  B[3]=0f96fdde  C[3]=c7724e87  D[3]=53cb9af8

Step  0: (r= 3, s=23)
A[0]=eaa122f0  B[0]=3a9c53dd  C[0]=5f32521e  D[0]=94a11d95
A[1]=db5f35aa  B[1]=9f1410a4  C[1]=a8d595cb  D[1]=7886e22a
A[2]=24909328  B[2]=be0ece62  C[2]=dbf601d4  D[2]=dbbac623
A[3]=9974744e  B[3]=9ee71a48  C[3]=0f96fdde  D[3]=c7724e87

Step  1: (r=23, s=17)
A[0]=67f7edcd  B[0]=78755091  C[0]=3a9c53dd  D[0]=5f32521e
A[1]=af4367d1  B[1]=d56daf9a  C[1]=9f1410a4  D[1]=a8d595cb
A[2]=a3d92984  B[2]=94124849  C[2]=be0ece62  D[2]=dbf601d4
A[3]=c76ad303  B[3]=274cba3a  C[3]=9ee71a48  D[3]=0f96fdde

Step  2: (r=17, s=27)
A[0]=57357282  B[0]=db9acfef  C[0]=78755091  D[0]=3a9c53dd
A[1]=ac6fe37f  B[1]=cfa35e86  C[1]=d56daf9a  D[1]=9f1410a4
A[2]=860df732  B[2]=530947b2  C[2]=94124849  D[2]=be0ece62
A[3]=3c6e529c  B[3]=a6078ed5  C[3]=274cba3a  D[3]=9ee71a48

Step  3: (r=27, s= 3)
A[0]=3acb169f  B[0]=12b9ab94  C[0]=db9acfef  D[0]=78755091
A[1]=672d8095  B[1]=fd637f1b  C[1]=cfa35e86  D[1]=d56daf9a
A[2]=6c43c568  B[2]=94306fb9  C[2]=530947b2  D[2]=94124849
A[3]=42d3f90f  B[3]=e1e37294  C[3]=a6078ed5  D[3]=274cba3a
```

```
Step  4: (r= 3, s=23)
A[0]=9244a796  B[0]=d658b4f9  C[0]=12b9ab94  D[0]=db9acfef
A[1]=37f6810a  B[1]=396c04ab  C[1]=fd637f1b  D[1]=cfa35e86
A[2]=0cea602e  B[2]=621e2b43  C[2]=94306fb9  D[2]=530947b2
A[3]=7ec7230c  B[3]=169fc87a  C[3]=e1e37294  D[3]=a6078ed5

Step  5: (r=23, s=17)
A[0]=655fe187  B[0]=cb492253  C[0]=d658b4f9  D[0]=12b9ab94
A[1]=75ebf60f  B[1]=851bfb40  C[1]=396c04ab  D[1]=fd637f1b
A[2]=b55c7a17  B[2]=17067530  C[2]=621e2b43  D[2]=94306fb9
A[3]=b2f38012  B[3]=863f6391  C[3]=169fc87a  D[3]=e1e37294

Step  6: (r=17, s=27)
A[0]=c3579732  B[0]=c30ecabf  C[0]=cb492253  D[0]=d658b4f9
A[1]=7c8e27b1  B[1]=ec1eebd7  C[1]=851bfb40  D[1]=396c04ab
A[2]=079b266a  B[2]=f42f6ab8  C[2]=17067530  D[2]=621e2b43
A[3]=d9fcd98b  B[3]=002565e7  C[3]=863f6391  D[3]=169fc87a

Step  7: (r=27, s= 3)
A[0]=53274b97  B[0]=961abcb9  C[0]=c30ecabf  D[0]=cb492253
A[1]=0e80f996  B[1]=8be4713d  C[1]=ec1eebd7  D[1]=851bfb40
A[2]=f77e72ac  B[2]=503cd933  C[2]=f42f6ab8  D[2]=17067530
A[3]=3a7f5b9f  B[3]=5ecfe6cc  C[3]=002565e7  D[3]=863f6391

Step  8: (r=28, s=19)
A[0]=fcb9f355  B[0]=753274b9  C[0]=961abcb9  D[0]=c30ecabf
A[1]=6391002f  B[1]=60e80f99  C[1]=8be4713d  D[1]=ec1eebd7
A[2]=dabc1fa5  B[2]=cf77e72a  C[2]=503cd933  D[2]=f42f6ab8
A[3]=0b3efa01  B[3]=f3a7f5b9  C[3]=5ecfe6cc  D[3]=002565e7

Step  9: (r=19, s=22)
A[0]=9a9bac27  B[0]=9aafe5cf  C[0]=753274b9  D[0]=961abcb9
A[1]=0a3b5f71  B[1]=017b1c88  C[1]=60e80f99  D[1]=8be4713d
A[2]=6584988f  B[2]=fd2ed5e0  C[2]=cf77e72a  D[2]=503cd933
A[3]=c64a16b3  B[3]=d00859f7  C[3]=f3a7f5b9  D[3]=5ecfe6cc

Step 10: (r=22, s= 7)
A[0]=148d8ee8  B[0]=09e6a6eb  C[0]=9aafe5cf  D[0]=753274b9
A[1]=34659f89  B[1]=dc428ed7  C[1]=017b1c88  D[1]=60e80f99
A[2]=b4e12199  B[2]=23d96126  C[2]=fd2ed5e0  D[2]=cf77e72a
A[3]=59b159f5  B[3]=acf19285  C[3]=d00859f7  D[3]=f3a7f5b9

Step 11: (r= 7, s=28)
A[0]=4929cd2a  B[0]=46c7740a  C[0]=09e6a6eb  D[0]=9aafe5cf
A[1]=b2cee5bd  B[1]=32cfc49a  C[1]=dc428ed7  D[1]=017b1c88
A[2]=c66fd36c  B[2]=7090ccda  C[2]=23d96126  D[2]=fd2ed5e0
A[3]=69a1425a  B[3]=d8acfaac  C[3]=acf19285  D[3]=d00859f7
```

```
Step 12: (r=28, s=19)
A[0]=21f1bfa3  B[0]=a4929cd2  C[0]=46c7740a  D[0]=09e6a6eb
A[1]=cee16bc2  B[1]=db2cee5b  C[1]=32cfc49a  D[1]=dc428ed7
A[2]=19225eaf  B[2]=cc66fd36  C[2]=7090ccda  D[2]=23d96126
A[3]=4603ad08  B[3]=a69a1425  C[3]=d8acfaac  D[3]=acf19285

Step 13: (r=19, s=22)
A[0]=df374793  B[0]=fd190f8d  C[0]=a4929cd2  D[0]=46c7740a
A[1]=5c2a343e  B[1]=5e16770b  C[1]=db2cee5b  D[1]=32cfc49a
A[2]=36e5168a  B[2]=f578c912  C[2]=cc66fd36  D[2]=7090ccda
A[3]=d14451b3  B[3]=6842301d  C[3]=a69a1425  D[3]=d8acfaac

Step 14: (r=22, s= 7)
A[0]=9db2df1b  B[0]=e4f7cdd1  C[0]=fd190f8d  D[0]=a4929cd2
A[1]=19485884  B[1]=0f970a8d  C[1]=5e16770b  D[1]=db2cee5b
A[2]=1d43e52d  B[2]=a28db945  C[2]=f578c912  D[2]=cc66fd36
A[3]=69754bd0  B[3]=6cf45114  C[3]=6842301d  D[3]=a69a1425

Step 15: (r= 7, s=28)
A[0]=63c7be9a  B[0]=d96f8dce  C[0]=e4f7cdd1  D[0]=fd190f8d
A[1]=4c48b2ad  B[1]=a42c420c  C[1]=0f970a8d  D[1]=5e16770b
A[2]=c70b672e  B[2]=a1f2968e  C[2]=a28db945  D[2]=f578c912
A[3]=358db137  B[3]=baa5e834  C[3]=6cf45114  D[3]=6842301d

Step 16: (r=29, s= 9)
A[0]=58d65d08  B[0]=4c78f7d3  C[0]=d96f8dce  D[0]=e4f7cdd1
A[1]=56317f4c  B[1]=a9891655  C[1]=a42c420c  D[1]=0f970a8d
A[2]=73046049  B[2]=d8e16ce5  C[2]=a1f2968e  D[2]=a28db945
A[3]=7a2af66e  B[3]=e6b1b626  C[3]=baa5e834  D[3]=6cf45114

Step 17: (r= 9, s=15)
A[0]=e1f8b014  B[0]=acba10b1  C[0]=4c78f7d3  D[0]=d96f8dce
A[1]=aa748f94  B[1]=62fe98ac  C[1]=a9891655  D[1]=a42c420c
A[2]=aebb1fe9  B[2]=08c092e6  C[2]=d8e16ce5  D[2]=a1f2968e
A[3]=ff952e7b  B[3]=55ecdcf4  C[3]=e6b1b626  D[3]=baa5e834

Step 18: (r=15, s= 5)
A[0]=739def64  B[0]=580a70fc  C[0]=acba10b1  D[0]=4c78f7d3
A[1]=0f08a33f  B[1]=47ca553a  C[1]=62fe98ac  D[1]=a9891655
A[2]=24f9439f  B[2]=8ff4d75d  C[2]=08c092e6  D[2]=d8e16ce5
A[3]=f9c795ca  B[3]=973dffca  C[3]=55ecdcf4  D[3]=e6b1b626

Step 19: (r= 5, s=29)
A[0]=18bf5cc7  B[0]=73bdec8e  C[0]=580a70fc  D[0]=acba10b1
A[1]=695c5eb2  B[1]=e11467e1  C[1]=47ca553a  D[1]=62fe98ac
A[2]=56287c73  B[2]=9f2873e4  C[2]=8ff4d75d  D[2]=08c092e6
A[3]=715c4723  B[3]=38f2b95f  C[3]=973dffca  D[3]=55ecdcf4

Step 20: (r=29, s= 9)
```

```
A[0]=633625d7  B[0]=e317eb98  C[0]=73bdec8e  D[0]=580a70fc
A[1]=df71ad23  B[1]=4d2b8bd6  C[1]=e11467e1  D[1]=47ca553a
A[2]=ca01373d  B[2]=6ac50f8e  C[2]=9f2873e4  D[2]=8ff4d75d
A[3]=76fa4955  B[3]=6e2b88e4  C[3]=38f2b95f  D[3]=973dffca

Step 21: (r= 9, s=15)
A[0]=0da5eb94  B[0]=6c4baec6  C[0]=e317eb98  D[0]=73bdec8e
A[1]=9ea2bfa3  B[1]=e35a47be  C[1]=4d2b8bd6  D[1]=e11467e1
A[2]=eb4129f1  B[2]=026e7b94  C[2]=6ac50f8e  D[2]=9f2873e4
A[3]=c8d03b05  B[3]=f492aaed  C[3]=6e2b88e4  D[3]=38f2b95f

Step 22: (r=15, s= 5)
A[0]=5fac94d3  B[0]=f5ca06d2  C[0]=6c4baec6  D[0]=e317eb98
A[1]=a4b4a4db  B[1]=5fd1cf51  C[1]=e35a47be  D[1]=4d2b8bd6
A[2]=c168e1d5  B[2]=94f8f5a0  C[2]=026e7b94  D[2]=6ac50f8e
A[3]=d4d3e070  B[3]=1d82e468  C[3]=f492aaed  D[3]=6e2b88e4

Step 23: (r= 5, s=29)
A[0]=4f3de14b  B[0]=f5929a6b  C[0]=f5ca06d2  D[0]=6c4baec6
A[1]=7ac98baa  B[1]=96949b74  C[1]=5fd1cf51  D[1]=e35a47be
A[2]=5b99c182  B[2]=2d1c3ab8  C[2]=94f8f5a0  D[2]=026e7b94
A[3]=3c1879b3  B[3]=9a7c0e1a  C[3]=1d82e468  D[3]=f492aaed

Step 24: (r= 4, s=13)
A[0]=b312b4af  B[0]=f3de14b4  C[0]=f5929a6b  D[0]=f5ca06d2
A[1]=3c39fc25  B[1]=ac98baa7  C[1]=96949b74  D[1]=5fd1cf51
A[2]=7a4937fe  B[2]=b99c1825  C[2]=2d1c3ab8  D[2]=94f8f5a0
A[3]=c75880a1  B[3]=c1879b33  C[3]=9a7c0e1a  D[3]=1d82e468

Step 25: (r=13, s=10)
A[0]=a51fdb26  B[0]=5695f662  C[0]=f3de14b4  D[0]=f5929a6b
A[1]=c5e7f385  B[1]=3f84a787  C[1]=ac98baa7  D[1]=96949b74
A[2]=507aa1ad  B[2]=26ffcf49  C[2]=b99c1825  D[2]=2d1c3ab8
A[3]=0ce5a1d4  B[3]=101438eb  C[3]=c1879b33  D[3]=9a7c0e1a

Step 26: (r=10, s=25)
A[0]=1c64a4d5  B[0]=7f6c9a94  C[0]=5695f662  D[0]=f3de14b4
A[1]=186dc049  B[1]=9fce1717  C[1]=3f84a787  D[1]=ac98baa7
A[2]=5ea1de9d  B[2]=ea86b541  C[2]=26ffcf49  D[2]=b99c1825
A[3]=a5cc4082  B[3]=96875033  C[3]=101438eb  D[3]=c1879b33

Step 27: (r=25, s= 4)
A[0]=6a69cd92  B[0]=aa38c949  C[0]=7f6c9a94  D[0]=5695f662
A[1]=68f51a31  B[1]=9230db80  C[1]=9fce1717  D[1]=3f84a787
A[2]=67cb1905  B[2]=3abd43bd  C[2]=ea86b541  D[2]=26ffcf49
A[3]=5c27e461  B[3]=054b9881  C[3]=96875033  D[3]=101438eb

Step 28: (r= 4, s=13)
A[0]=f6bc13f3  B[0]=a69cd926  C[0]=aa38c949  D[0]=7f6c9a94
```

```
A[1]=5a5ccf62  B[1]=8f51a316  C[1]=9230db80  D[1]=9fce1717
A[2]=4839d34e  B[2]=7cb19056  C[2]=3abd43bd  D[2]=ea86b541
A[3]=bab06ae6  B[3]=c27e4615  C[3]=054b9881  D[3]=96875033

Step 29: (r=13, s=10)
A[0]=f24012e4  B[0]=827e7ed7  C[0]=a69cd926  D[0]=aa38c949
A[1]=3870457a  B[1]=99ec4b4b  C[1]=8f51a316  D[1]=9230db80
A[2]=5b96a359  B[2]=3a69c907  C[2]=7cb19056  D[2]=3abd43bd
A[3]=c1446491  B[3]=0d5cd756  C[3]=c27e4615  D[3]=054b9881

Step 30: (r=10, s=25)
A[0]=f7870856  B[0]=004b93c9  C[0]=827e7ed7  D[0]=a69cd926
A[1]=54e9d498  B[1]=c115e8e1  C[1]=99ec4b4b  D[1]=8f51a316
A[2]=3747c71d  B[2]=5a8d656e  C[2]=3a69c907  D[2]=7cb19056
A[3]=79e99061  B[3]=11924705  C[3]=0d5cd756  D[3]=c27e4615

Step 31: (r=25, s= 4)
A[0]=939a2b6c  B[0]=adef0e10  C[0]=004b93c9  D[0]=827e7ed7
A[1]=6ae42384  B[1]=30a9d3a9  C[1]=c115e8e1  D[1]=99ec4b4b
A[2]=373f7178  B[2]=3a6e8f8e  C[2]=5a8d656e  D[2]=3a69c907
A[3]=7aace9ac  B[3]=c2f3d320  C[3]=11924705  D[3]=0d5cd756

Feed-Forward Step 32: (r= 4, s=13)
A[0]=5f12903a  B[0]=39a2b6c9  C[0]=adef0e10  D[0]=004b93c9
A[1]=871f3173  B[1]=ae423846  C[1]=30a9d3a9  D[1]=c115e8e1
A[2]=e33e59e1  B[2]=73f71783  C[2]=3a6e8f8e  D[2]=5a8d656e
A[3]=c9dac366  B[3]=aace9ac7  C[3]=c2f3d320  D[3]=11924705

Feed-Forward Step 33: (r=13, s=10)
A[0]=9c3e2d48  B[0]=52074be2  C[0]=39a2b6c9  D[0]=adef0e10
A[1]=8bcd2464  B[1]=e62e70e3  C[1]=ae423846  D[1]=30a9d3a9
A[2]=40682002  B[2]=cb3c3c67  C[2]=73f71783  D[2]=3a6e8f8e
A[3]=1e98e317  B[3]=586cd93b  C[3]=aace9ac7  D[3]=c2f3d320

Feed-Forward Step 34: (r=10, s=25)
A[0]=6d68368f  B[0]=f8b52270  C[0]=52074be2  D[0]=39a2b6c9
A[1]=ce2ada56  B[1]=3491922f  C[1]=e62e70e3  D[1]=ae423846
A[2]=61c8f38a  B[2]=a0800901  C[2]=cb3c3c67  D[2]=73f71783
A[3]=2916fc25  B[3]=638c5c7a  C[3]=586cd93b  D[3]=aace9ac7

Feed-Forward Step 35: (r=25, s= 4)
A[0]=eb4e0be8  B[0]=1edad06d  C[0]=f8b52270  D[0]=52074be2
A[1]=6c0e378a  B[1]=ad9c55b4  C[1]=3491922f  D[1]=e62e70e3
A[2]=81e718a9  B[2]=14c391e7  C[2]=a0800901  D[2]=cb3c3c67
A[3]=1f440004  B[3]=4a522df8  C[3]=638c5c7a  D[3]=586cd93b
```

Compression Function Output

```
A[0]=eb4e0be8  B[0]=1edad06d  C[0]=f8b52270  D[0]=52074be2
```

```
A[1]=6c0e378a  B[1]=ad9c55b4  C[1]=3491922f  D[1]=e62e70e3
A[2]=81e718a9  B[2]=14c391e7  C[2]=a0800901  D[2]=cb3c3c67
A[3]=1f440004  B[3]=4a522df8  C[3]=638c5c7a  D[3]=586cd93b
```

Hash Function Output

```
e80b4eeb8a370e6ca918e7810400441f6dd0da1eb4559cade791c314f82d524a
```

A.3 SIMD-384

A.3.1 Empty Message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    2  203  156   47  118  214  107  106
y[  8.. 15] =   45   93  212   20  111   73  162  251
y[ 16.. 23] =   97  215  249   53  211   19    3   89
y[ 24.. 31] =   49  207  101   67  151  130  223   23
y[ 32.. 39] =  189  202  178  239  253  127  204   49
y[ 40.. 47] =   76  236   82  137  232  157   65   79
y[ 48.. 55] =   96  161  176  130  161   30   47    9
y[ 56.. 63] =  189  247   61  226  248   90  107   64
y[ 64.. 71] =    0   88  131  243  133   59  113  115
y[ 72.. 79] =   17  236   33  213   12  191  111   19
y[ 80.. 87] =  251   61  103  208   57   35  148  248
y[ 88.. 95] =   47  116   65  119  249  178  143   40
y[ 96..103] =  189  129    8  163  204  227  230  196
y[104..111] =  205  122  151   45  187   19  227   72
```

```
y[112..119] =  247  125  111  121  140  220    6  107
y[120..127] =   77   69   10  101   21   65  149  171
y[128..135] =  255   54  101  210  139   43  150  151
y[136..143] =  212  164   45  237  146  184   95    6
y[144..151] =  160   42    8  204   46  238  254  168
y[152..159] =  208   50  156  190  106  127   34  234
y[160..167] =   68   55   79   18    4  130   53  208
y[168..175] =  181   21  175  120   25  100  192  178
y[176..183] =  161   96   81  127   96  227  210  248
y[184..191] =   68   10  196   31    9  167  150  193
y[192..199] =    0  169  126   14  124  198  144  142
y[200..207] =  240   21  224   44  245   66  146  238
y[208..215] =    6  196  154   49  200  222  109    9
y[216..223] =  210  141  192  138    8   79  114  217
y[224..231] =   68  128  249   94   53   30   27   61
y[232..239] =   52  135  106  212   70  238   30  185
y[240..247] =   10  132  146  136  117   37  251  150
y[248..255] =  180  188  247  156  236  192  108   86
```

Intermediate Expanded Message

```
Z[ 0] = d8fa0172  21f7b703  e0ed5546  4c9a4d53
        43352085  0e74df7b  34c15037  fbaabb59
Z[ 1] = e1a64619  264dfa38  0dbbdec2  4051022b
        dbde2369  306b48fd  a439b366  109fe76e
Z[ 2] = d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
        f0d336ec  a9483b42  b7bcedef  39172ef9
Z[ 3] = baa04560  a439c577  15aebaa0  068121f7
        f8c6cedc  e9992c15  410af97f  2e404d53
Z[ 4] = 3f980000  f5e2a4f2  2aa3a664  531b51a9
        f0d30c49  e03417d9  d04e08ac  0dbb5037
Z[ 5] = 2c15fbaa  dc974a6f  194b2931  f97fb13b
        53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
Z[ 6] = a380cedc  bc1205c8  ea52d9b3  d3ebec7d
        582ada6c  2085b366  0dbbcd6a  3408ea52
Z[ 7] = 5a55f8c6  57715037  e543ab73  4d530456
        31dd37a5  48fd073a  2ef90f2d  c1dab1f4
Z[ 8] = 2706fe8e  de0948fd  1f13aaba  b366b2ad
        bccbdf7b  f18c2085  cb3fafc9  045644a7
Z[ 9] = 1e5ab9e7  d9b305c8  f245213e  bfaffdd5
        2422dc97  cf95b703  5bc74c9a  ef611892
Z[10] = 27bf3124  0d023917  a43902e4  dc97264d
        0f2dc914  56b8c4be  48441211  c6e9d107
Z[11] = 4560baa0  5bc73a89  ea524560  f97fde09
        073a3124  1667d3eb  bef60681  d1c0b2ad
Z[12] = c0680000  0a1e5b0e  d55d599c  ace5ae57
        0f2df3b7  1fcce827  2fb2f754  f245afc9
Z[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
        ac2cde09  aa01d107  391705c8  e3185262
```

```
Z[14] = 5c803124  43eefa38  15ae264d  2c151383
        a7d62594  df7b4c9a  f2453296  cbf815ae
Z[15] = a5ab073a  a88fafc9  1abd548d  b2adfbaa
        ce23c85b  b703f8c6  d107f0d3  3e264e0c
Z[16] = fe2e01d2  5beda413  949a6b66  9e9d6163
        d70b28f5  28f5d70b  9af96507  5677a989
Z[17] = a7b75849  0748f8b8  29ded622  fd4502bb
        d3672c99  a4135bed  607a9f86  1ef2e10e
Z[18] = 3de4c21c  47e7b819  03a4fc5c  303dcfc3
        bad4452c  b55e4aa2  16c1e93f  c4d73b29
Z[19] = a8a05760  49b9b647  5760a8a0  d5392ac7
        3de4c21c  c87b3785  0831f7cf  9e9d6163
Z[20] = 00000000  72ae8d52  70dc8f24  992766d9
        f0870f79  e1f71e09  f5140aec  9af96507
Z[21] = 0576fa8a  a2415dbf  cc1f33e1  63359ccb
        d5392ac7  c4d73b29  0748f8b8  67c2983e
Z[22] = 3de4c21c  f8b80748  303dcfc3  1893e76d
        2f54d0ac  607a9f86  3fb6c04a  1b4ee4b2
Z[23] = 091af6e6  9af96507  6a7d9583  fa8a0576
        b9eb4615  f6e6091a  ece3131d  624c9db4
Z[24] = 3126ceda  d5392ac7  2723d8dd  9f86607a
        ab5b54a5  edcc1234  bd8f4271  0576fa8a
Z[25] = 263ad9c6  cfc3303d  eeb5114b  aeff5101
        2d82d27e  c3053cfb  73978c69  eb1114ef
Z[26] = 320fcdf1  1062ef9e  8c697397  d3672c99
        131dece3  6d3892c8  5b04a4fc  b81947e7
Z[27] = 5760a8a0  73978c69  e4b21b4e  f7cf0831
        091af6e6  1c37e3c9  ae1651ea  c5c03a40
Z[28] = afe85018  0cbef342  ca4d35b3  975568ab
        131dece3  280cd7f4  3c12c3ee  eeb5114b
Z[29] = c87b3785  2c99d367  e0251fdb  0831f7cf
        966c6994  93b16c4f  47e7b819  db982468
Z[30] = 74808b80  558eaa72  1b4ee4b2  3785c87b
        90f66f0a  d70b28f5  eeb5114b  be784188
Z[31] = 8e3b71c5  91df6e21  21adde53  9e9d6163
        c1333ecd  a4135bed  c4d73b29  4e46b1ba
```

Expanded Message

```
W[ 0] = 3f980000  f5e2a4f2  2aa3a664  531b51a9
        f0d30c49  e03417d9  d04e08ac  0dbb5037
W[ 1] = a380cedc  bc1205c8  ea52d9b3  d3ebec7d
        582ada6c  2085b366  0dbbcd6a  3408ea52
W[ 2] = d8fa0172  21f7b703  e0ed5546  4c9a4d53
        43352085  0e74df7b  34c15037  fbaabb59
W[ 3] = d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
        f0d336ec  a9483b42  b7bcedef  39172ef9
W[ 4] = 5a55f8c6  57715037  e543ab73  4d530456
        31dd37a5  48fd073a  2ef90f2d  c1dab1f4
```

```
W[ 5] = 2c15fbaa  dc974a6f  194b2931  f97fb13b
        53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
W[ 6] = baa04560  a439c577  15aebaa0  068121f7
        f8c6cedc  e9992c15  410af97f  2e404d53
W[ 7] = e1a64619  264dfa38  0dbbdec2  4051022b
        dbde2369  306b48fd  a439b366  109fe76e
W[ 8] = a5ab073a  a88fafc9  1abd548d  b2adfbaa
        ce23c85b  b703f8c6  d107f0d3  3e264e0c
W[ 9] = 4560baa0  5bc73a89  ea524560  f97fde09
        073a3124  1667d3eb  bef60681  d1c0b2ad
W[10] = c0680000  0a1e5b0e  d55d599c  ace5ae57
        0f2df3b7  1fcce827  2fb2f754  f245afc9
W[11] = 2706fe8e  de0948fd  1f13aaba  b366b2ad
        bccbdf7b  f18c2085  cb3fafc9  045644a7
W[12] = 1e5ab9e7  d9b305c8  f245213e  bfaffdd5
        2422dc97  cf95b703  5bc74c9a  ef611892
W[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
        ac2cde09  aa01d107  391705c8  e3185262
W[14] = 27bf3124  0d023917  a43902e4  dc97264d
        0f2dc914  56b8c4be  48441211  c6e9d107
W[15] = 5c803124  43eefa38  15ae264d  2c151383
        a7d62594  df7b4c9a  f2453296  cbf815ae
W[16] = a7b75849  0748f8b8  29ded622  fd4502bb
        d3672c99  a4135bed  607a9f86  1ef2e10e
W[17] = 3de4c21c  47e7b819  03a4fc5c  303dcfc3
        bad4452c  b55e4aa2  16c1e93f  c4d73b29
W[18] = 091af6e6  9af96507  6a7d9583  fa8a0576
        b9eb4615  f6e6091a  ece3131d  624c9db4
W[19] = 00000000  72ae8d52  70dc8f24  992766d9
        f0870f79  e1f71e09  f5140aec  9af96507
W[20] = 3de4c21c  f8b80748  303dcfc3  1893e76d
        2f54d0ac  607a9f86  3fb6c04a  1b4ee4b2
W[21] = 0576fa8a  a2415dbf  cc1f33e1  63359ccb
        d5392ac7  c4d73b29  0748f8b8  67c2983e
W[22] = fe2e01d2  5beda413  949a6b66  9e9d6163
        d70b28f5  28f5d70b  9af96507  5677a989
W[23] = a8a05760  49b9b647  5760a8a0  d5392ac7
        3de4c21c  c87b3785  0831f7cf  9e9d6163
W[24] = 74808b80  558eaa72  1b4ee4b2  3785c87b
        90f66f0a  d70b28f5  eeb5114b  be784188
W[25] = 3126ceda  d5392ac7  2723d8dd  9f86607a
        ab5b54a5  edcc1234  bd8f4271  0576fa8a
W[26] = 263ad9c6  cfc3303d  eeb5114b  aeff5101
        2d82d27e  c3053cfb  73978c69  eb1114ef
W[27] = 8e3b71c5  91df6e21  21adde53  9e9d6163
        c1333ecd  a4135bed  c4d73b29  4e46b1ba
W[28] = 5760a8a0  73978c69  e4b21b4e  f7cf0831
        091af6e6  1c37e3c9  ae1651ea  c5c03a40
W[29] = c87b3785  2c99d367  e0251fdb  0831f7cf
```

```
        966c6994  93b16c4f  47e7b819  db982468
W[30] = afe85018  0cbef342  ca4d35b3  975568ab
        131dece3  280cd7f4  3c12c3ee  eeb5114b
W[31] = 320fcdf1  1062ef9e  8c697397  d3672c99
        131dece3  6d3892c8  5b04a4fc  b81947e7
```

Feistel Steps

```
IV :
A[0]=8a36eebc  B[0]=7360ca61  C[0]=b9e3bfe8  D[0]=e64071ec
A[1]=94a3bd90  B[1]=18361a03  C[1]=63bece2a  D[1]=1deb91a8
A[2]=d1537b83  B[2]=17dcb4b9  C[2]=8fe506b9  D[2]=8ac8db23
A[3]=b25b070b  B[3]=3414c45a  C[3]=f8cc4ac2  D[3]=3f782ab5
A[4]=f463f1b5  B[4]=a699a9d2  C[4]=7ae11542  D[4]=039b5cb8
A[5]=b6f81e20  B[5]=e39e9664  C[5]=b1aadda1  D[5]=71ddd962
A[6]=0055c339  B[6]=468bfe77  C[6]=64b06794  D[6]=fade2cea
A[7]=b4d144d1  B[7]=51d062f8  C[7]=28d2f462  D[7]=1416df71

IV XOR M :
A[0]=8a36eebc  B[0]=7360ca61  C[0]=b9e3bfe8  D[0]=e64071ec
A[1]=94a3bd90  B[1]=18361a03  C[1]=63bece2a  D[1]=1deb91a8
A[2]=d1537b83  B[2]=17dcb4b9  C[2]=8fe506b9  D[2]=8ac8db23
A[3]=b25b070b  B[3]=3414c45a  C[3]=f8cc4ac2  D[3]=3f782ab5
A[4]=f463f1b5  B[4]=a699a9d2  C[4]=7ae11542  D[4]=039b5cb8
A[5]=b6f81e20  B[5]=e39e9664  C[5]=b1aadda1  D[5]=71ddd962
A[6]=0055c339  B[6]=468bfe77  C[6]=64b06794  D[6]=fade2cea
A[7]=b4d144d1  B[7]=51d062f8  C[7]=28d2f462  D[7]=1416df71

Step  0: (r= 3, s=23)
A[0]=4b4ac9aa  B[0]=51b775e4  C[0]=7360ca61  D[0]=b9e3bfe8
A[1]=b3fafc2c  B[1]=a51dec84  C[1]=18361a03  D[1]=63bece2a
A[2]=b342e8b8  B[2]=8a9bdc1e  C[2]=17dcb4b9  D[2]=8fe506b9
A[3]=1ea17002  B[3]=92d8385d  C[3]=3414c45a  D[3]=f8cc4ac2
A[4]=2192690c  B[4]=a31f8daf  C[4]=a699a9d2  D[4]=7ae11542
A[5]=119a6413  B[5]=b7c0f105  C[5]=e39e9664  D[5]=b1aadda1
A[6]=cc220d9b  B[6]=02ae19c8  C[6]=468bfe77  D[6]=64b06794
A[7]=4fcb6c58  B[7]=a68a268d  C[7]=51d062f8  D[7]=28d2f462

Step  1: (r=23, s=17)
A[0]=7331ae13  B[0]=d525a564  C[0]=51b775e4  D[0]=7360ca61
A[1]=b01b7791  B[1]=1659fd7e  C[1]=a51dec84  D[1]=18361a03
A[2]=ff1acae1  B[2]=5c59a174  C[2]=8a9bdc1e  D[2]=17dcb4b9
A[3]=e0b8cbcb  B[3]=010f50b8  C[3]=92d8385d  D[3]=3414c45a
A[4]=4f7295c2  B[4]=8610c934  C[4]=a31f8daf  D[4]=a699a9d2
A[5]=07e8dc23  B[5]=0988cd32  C[5]=b7c0f105  D[5]=e39e9664
A[6]=36fa8f94  B[6]=cde61106  C[6]=02ae19c8  D[6]=468bfe77
A[7]=2112e46a  B[7]=2c27e5b6  C[7]=a68a268d  D[7]=51d062f8

Step  2: (r=17, s=27)
```

```
A[0]=52b41442  B[0]=5c26e663  C[0]=d525a564  D[0]=51b775e4
A[1]=6a121fe1  B[1]=ef236036  C[1]=1659fd7e  D[1]=a51dec84
A[2]=46d20356  B[2]=95c3fe35  C[2]=5c59a174  D[2]=8a9bdc1e
A[3]=3bbb1c48  B[3]=9797c171  C[3]=010f50b8  D[3]=92d8385d
A[4]=43a7d091  B[4]=2b849ee5  C[4]=8610c934  D[4]=a31f8daf
A[5]=f5f1253d  B[5]=b8460fd1  C[5]=0988cd32  D[5]=b7c0f105
A[6]=ff8639e4  B[6]=1f286df5  C[6]=cde61106  D[6]=02ae19c8
A[7]=7fe63ff8  B[7]=c8d44225  C[7]=2c27e5b6  D[7]=a68a268d

Step  3: (r=27, s= 3)
A[0]=3ad52a19  B[0]=1295a0a2  C[0]=5c26e663  D[0]=d525a564
A[1]=657b2d72  B[1]=0b5090ff  C[1]=ef236036  D[1]=1659fd7e
A[2]=24cc6c6f  B[2]=b236901a  C[2]=95c3fe35  D[2]=5c59a174
A[3]=616038a8  B[3]=41ddd8e2  C[3]=9797c171  D[3]=010f50b8
A[4]=a03a23ff  B[4]=8a1d3e84  C[4]=2b849ee5  D[4]=8610c934
A[5]=f28bfc9f  B[5]=efaf8929  C[5]=b8460fd1  D[5]=0988cd32
A[6]=be091617  B[6]=27fc31cf  C[6]=1f286df5  D[6]=cde61106
A[7]=cd55fbe5  B[7]=c3ff31ff  C[7]=c8d44225  D[7]=2c27e5b6

Step  4: (r= 3, s=23)
A[0]=bb04ed9f  B[0]=d6a950c9  C[0]=1295a0a2  D[0]=5c26e663
A[1]=17bfbf34  B[1]=2bd96b93  C[1]=0b5090ff  D[1]=ef236036
A[2]=fe2b1152  B[2]=26636379  C[2]=b236901a  D[2]=95c3fe35
A[3]=e790ccd3  B[3]=0b01c543  C[3]=41ddd8e2  D[3]=9797c171
A[4]=0b0a70b2  B[4]=01d11ffd  C[4]=8a1d3e84  D[4]=2b849ee5
A[5]=d94fdb7a  B[5]=945fe4ff  C[5]=efaf8929  D[5]=b8460fd1
A[6]=101fc8ee  B[6]=f048b0bd  C[6]=27fc31cf  D[6]=1f286df5
A[7]=ee3f4f7e  B[7]=6aafdf2e  C[7]=c3ff31ff  D[7]=c8d44225

Step  5: (r=23, s=17)
A[0]=44a7552c  B[0]=cfdd8276  C[0]=d6a950c9  D[0]=1295a0a2
A[1]=43c1bf0c  B[1]=9a0bdfdf  C[1]=2bd96b93  D[1]=0b5090ff
A[2]=2eed7251  B[2]=a97f1588  C[2]=26636379  D[2]=b236901a
A[3]=d7e52e8a  B[3]=69f3c866  C[3]=0b01c543  D[3]=41ddd8e2
A[4]=6914dd49  B[4]=59058538  C[4]=01d11ffd  D[4]=8a1d3e84
A[5]=ba0aecb2  B[5]=bd6ca7ed  C[5]=945fe4ff  D[5]=efaf8929
A[6]=cc440cbd  B[6]=77080fe4  C[6]=f048b0bd  D[6]=27fc31cf
A[7]=6e61236e  B[7]=bf771fa7  C[7]=6aafdf2e  D[7]=c3ff31ff

Step  6: (r=17, s=27)
A[0]=2f31ebdc  B[0]=aa58894e  C[0]=cfdd8276  D[0]=d6a950c9
A[1]=874016c5  B[1]=7e188783  C[1]=9a0bdfdf  D[1]=2bd96b93
A[2]=b92e3e78  B[2]=e4a25dda  C[2]=a97f1588  D[2]=26636379
A[3]=237ee2fa  B[3]=5d15afca  C[3]=69f3c866  D[3]=0b01c543
A[4]=78b856a4  B[4]=ba92d229  C[4]=59058538  D[4]=01d11ffd
A[5]=6ac54454  B[5]=d9657415  C[5]=bd6ca7ed  D[5]=945fe4ff
A[6]=3f8cd79a  B[6]=197b9888  C[6]=77080fe4  D[6]=f048b0bd
A[7]=601ae4be  B[7]=46dcdcc2  C[7]=bf771fa7  D[7]=6aafdf2e
```

```
Step  7: (r=27, s= 3)
A[0]=698312b9  B[0]=e1798f5e  C[0]=aa58894e  D[0]=cfdd8276
A[1]=62f97bf5  B[1]=2c3a00b6  C[1]=7e188783  D[1]=9a0bdfdf
A[2]=bb86f7b5  B[2]=c5c971f3  C[2]=e4a25dda  D[2]=a97f1588
A[3]=6c1f04b8  B[3]=d11bf717  C[3]=5d15afca  D[3]=69f3c866
A[4]=5556f694  B[4]=23c5c2b5  C[4]=ba92d229  D[4]=59058538
A[5]=154a5542  B[5]=a3562a22  C[5]=d9657415  D[5]=bd6ca7ed
A[6]=8f58f483  B[6]=d1fc66bc  C[6]=197b9888  D[6]=77080fe4
A[7]=df7180d3  B[7]=f300d725  C[7]=46dcdcc2  D[7]=bf771fa7

Step  8: (r=28, s=19)
A[0]=e1685658  B[0]=9698312b  C[0]=e1798f5e  D[0]=aa58894e
A[1]=e0eb0ead  B[1]=562f97bf  C[1]=2c3a00b6  D[1]=7e188783
A[2]=65d9be50  B[2]=5bb86f7b  C[2]=c5c971f3  D[2]=e4a25dda
A[3]=bc68133f  B[3]=86c1f04b  C[3]=d11bf717  D[3]=5d15afca
A[4]=de3f06eb  B[4]=45556f69  C[4]=23c5c2b5  D[4]=ba92d229
A[5]=8d13df09  B[5]=2154a554  C[5]=a3562a22  D[5]=d9657415
A[6]=0096fd86  B[6]=38f58f48  C[6]=d1fc66bc  D[6]=197b9888
A[7]=a3d62111  B[7]=3df7180d  C[7]=f300d725  D[7]=46dcdcc2

Step  9: (r=19, s=22)
A[0]=319f2384  B[0]=b2c70b42  C[0]=9698312b  D[0]=e1798f5e
A[1]=ccc769f2  B[1]=756f0758  C[1]=562f97bf  D[1]=2c3a00b6
A[2]=7e2b2e86  B[2]=f2832ecd  C[2]=5bb86f7b  D[2]=c5c971f3
A[3]=ecf601b8  B[3]=99fde340  C[3]=86c1f04b  D[3]=d11bf717
A[4]=5eb9ed69  B[4]=375ef1f8  C[4]=45556f69  D[4]=23c5c2b5
A[5]=5111e72c  B[5]=f84c689e  C[5]=2154a554  D[5]=a3562a22
A[6]=c7c98d83  B[6]=ec3004b7  C[6]=38f58f48  D[6]=d1fc66bc
A[7]=5d6f05b7  B[7]=088d1eb1  C[7]=3df7180d  D[7]=f300d725

Step 10: (r=22, s= 7)
A[0]=a28c822c  B[0]=e10c67c8  C[0]=b2c70b42  D[0]=9698312b
A[1]=05991b91  B[1]=7cb331da  C[1]=756f0758  D[1]=562f97bf
A[2]=d9d0f7e1  B[2]=a19f8acb  C[2]=f2832ecd  D[2]=5bb86f7b
A[3]=5cd7c04c  B[3]=6e3b3d80  C[3]=99fde340  D[3]=86c1f04b
A[4]=962445e6  B[4]=5a57ae7b  C[4]=375ef1f8  D[4]=45556f69
A[5]=14ab44fc  B[5]=cb144479  C[5]=f84c689e  D[5]=2154a554
A[6]=bcc6b277  B[6]=60f1f263  C[6]=ec3004b7  D[6]=38f58f48
A[7]=4c298201  B[7]=6dd75bc1  C[7]=088d1eb1  D[7]=3df7180d

Step 11: (r= 7, s=28)
A[0]=8c8161ba  B[0]=46411651  C[0]=e10c67c8  D[0]=b2c70b42
A[1]=5cb5f2b4  B[1]=cc8dc882  C[1]=7cb331da  D[1]=756f0758
A[2]=36a6faf6  B[2]=e87bf0ec  C[2]=a19f8acb  D[2]=f2832ecd
A[3]=e3cf783d  B[3]=6be0262e  C[3]=6e3b3d80  D[3]=99fde340
A[4]=afe5c8b7  B[4]=1222f34b  C[4]=5a57ae7b  D[4]=375ef1f8
A[5]=85f36976  B[5]=55a27e0a  C[5]=cb144479  D[5]=f84c689e
A[6]=b232858d  B[6]=63593bde  C[6]=60f1f263  D[6]=ec3004b7
A[7]=416918a2  B[7]=14c100a6  C[7]=6dd75bc1  D[7]=088d1eb1
```

```
Step 12: (r=28, s=19)
A[0]=8c233aa3  B[0]=a8c8161b  C[0]=46411651  D[0]=e10c67c8
A[1]=c8b88717  B[1]=45cb5f2b  C[1]=cc8dc882  D[1]=7cb331da
A[2]=c02b62d9  B[2]=636a6faf  C[2]=e87bf0ec  D[2]=a19f8acb
A[3]=650c8953  B[3]=de3cf783  C[3]=6be0262e  D[3]=6e3b3d80
A[4]=a690a6d0  B[4]=7afe5c8b  C[4]=1222f34b  D[4]=5a57ae7b
A[5]=c446dc53  B[5]=685f3697  C[5]=55a27e0a  D[5]=cb144479
A[6]=6ed0b273  B[6]=db232858  C[6]=63593bde  D[6]=60f1f263
A[7]=27f20395  B[7]=2416918a  C[7]=14c100a6  D[7]=6dd75bc1

Step 13: (r=19, s=22)
A[0]=c2d582a5  B[0]=d51c6119  C[0]=a8c8161b  D[0]=46411651
A[1]=7e394be3  B[1]=38be45c4  C[1]=45cb5f2b  D[1]=cc8dc882
A[2]=b575a6b6  B[2]=16ce015b  C[2]=636a6faf  D[2]=e87bf0ec
A[3]=eee239dc  B[3]=4a9b2864  C[3]=de3cf783  D[3]=6be0262e
A[4]=a8eaaef9  B[4]=36853485  C[4]=7afe5c8b  D[4]=1222f34b
A[5]=1dac9ce8  B[5]=e29e2236  C[5]=685f3697  D[5]=55a27e0a
A[6]=b80f57e7  B[6]=939b7685  C[6]=db232858  D[6]=63593bde
A[7]=34f898cf  B[7]=1ca93f90  C[7]=2416918a  D[7]=14c100a6

Step 14: (r=22, s= 7)
A[0]=67045569  B[0]=a970b560  C[0]=d51c6119  D[0]=a8c8161b
A[1]=cf19738b  B[1]=f8df8e52  C[1]=38be45c4  D[1]=45cb5f2b
A[2]=88c98070  B[2]=adad5d69  C[2]=16ce015b  D[2]=636a6faf
A[3]=46707cf4  B[3]=773bb88e  C[3]=4a9b2864  D[3]=de3cf783
A[4]=5983df55  B[4]=be6a3aab  C[4]=36853485  D[4]=7afe5c8b
A[5]=3b26f9b5  B[5]=3a076b27  C[5]=e29e2236  D[5]=685f3697
A[6]=882f9849  B[6]=f9ee03d5  C[6]=939b7685  D[6]=db232858
A[7]=2ba39f5d  B[7]=33cd3e26  C[7]=1ca93f90  D[7]=2416918a

Step 15: (r= 7, s=28)
A[0]=a671f08e  B[0]=822ab4b3  C[0]=a970b560  D[0]=d51c6119
A[1]=29f548a7  B[1]=8cb9c5e7  C[1]=f8df8e52  D[1]=38be45c4
A[2]=124e0423  B[2]=64c03844  C[2]=adad5d69  D[2]=16ce015b
A[3]=3885aedb  B[3]=383e7a23  C[3]=773bb88e  D[3]=4a9b2864
A[4]=aad5b44e  B[4]=c1efaaac  C[4]=be6a3aab  D[4]=36853485
A[5]=c05c8909  B[5]=937cda9d  C[5]=3a076b27  D[5]=e29e2236
A[6]=b89c2b8e  B[6]=17cc24c4  C[6]=f9ee03d5  D[6]=939b7685
A[7]=4f75444b  B[7]=d1cfae95  C[7]=33cd3e26  D[7]=1ca93f90

Step 16: (r=29, s= 9)
A[0]=4b284893  B[0]=d4ce3e11  C[0]=822ab4b3  D[0]=a970b560
A[1]=ed1b9c0c  B[1]=e53ea914  C[1]=8cb9c5e7  D[1]=f8df8e52
A[2]=f12fc9ee  B[2]=6249c084  C[2]=64c03844  D[2]=adad5d69
A[3]=2208f6a2  B[3]=6710b5db  C[3]=383e7a23  D[3]=773bb88e
A[4]=8f2b1cae  B[4]=d55ab689  C[4]=c1efaaac  D[4]=be6a3aab
A[5]=8cbf4d0b  B[5]=380b9121  C[5]=937cda9d  D[5]=3a076b27
A[6]=ddc87715  B[6]=d7138571  C[6]=17cc24c4  D[6]=f9ee03d5
```

```
A[7]=0ac9187b  B[7]=69eea889  C[7]=d1cfae95  D[7]=33cd3e26

Step 17: (r= 9, s=15)
A[0]=2bc417f4  B[0]=50912696  C[0]=d4ce3e11  D[0]=822ab4b3
A[1]=67bcf123  B[1]=373819da  C[1]=e53ea914  D[1]=8cb9c5e7
A[2]=5c5ca4e8  B[2]=5f93dde2  C[2]=6249c084  D[2]=64c03844
A[3]=72fb976e  B[3]=11ed4444  C[3]=6710b5db  D[3]=383e7a23
A[4]=2d60959b  B[4]=56395d1e  C[4]=d55ab689  D[4]=c1efaaac
A[5]=359d3113  B[5]=7e9a1719  C[5]=380b9121  D[5]=937cda9d
A[6]=780d0af2  B[6]=90ee2bbb  C[6]=d7138571  D[6]=17cc24c4
A[7]=ea27c657  B[7]=9230f615  C[7]=69eea889  D[7]=d1cfae95

Step 18: (r=15, s= 5)
A[0]=9284e099  B[0]=0bfa15e2  C[0]=50912696  D[0]=d4ce3e11
A[1]=28761749  B[1]=7891b3de  C[1]=373819da  D[1]=e53ea914
A[2]=8d1e4a7c  B[2]=52742e2e  C[2]=5f93dde2  D[2]=6249c084
A[3]=9badc9cf  B[3]=cbb7397d  C[3]=11ed4444  D[3]=6710b5db
A[4]=7b36af48  B[4]=4acd96b0  C[4]=56395d1e  D[4]=d55ab689
A[5]=eba8b2fa  B[5]=98899ace  C[5]=7e9a1719  D[5]=380b9121
A[6]=45702c10  B[6]=85793c06  C[6]=90ee2bbb  D[6]=d7138571
A[7]=531b8b05  B[7]=e32bf513  C[7]=9230f615  D[7]=69eea889

Step 19: (r= 5, s=29)
A[0]=465d493c  B[0]=509c1332  C[0]=0bfa15e2  D[0]=50912696
A[1]=c0e62c50  B[1]=0ec2e925  C[1]=7891b3de  D[1]=373819da
A[2]=39cddd47  B[2]=a3c94f91  C[2]=52742e2e  D[2]=5f93dde2
A[3]=98598e4f  B[3]=75b939f3  C[3]=cbb7397d  D[3]=11ed4444
A[4]=78372d76  B[4]=66d5e90f  C[4]=4acd96b0  D[4]=56395d1e
A[5]=5a9cf86f  B[5]=75165f5d  C[5]=98899ace  D[5]=7e9a1719
A[6]=1b07a126  B[6]=ae058208  C[6]=85793c06  D[6]=90ee2bbb
A[7]=899e9386  B[7]=637160aa  C[7]=e32bf513  D[7]=9230f615

Step 20: (r=29, s= 9)
A[0]=72faaf50  B[0]=88cba927  C[0]=509c1332  D[0]=0bfa15e2
A[1]=50e88bfe  B[1]=181cc58a  C[1]=0ec2e925  D[1]=7891b3de
A[2]=015a4dab  B[2]=e739bba8  C[2]=a3c94f91  D[2]=52742e2e
A[3]=45fe3278  B[3]=f30b31c9  C[3]=75b939f3  D[3]=cbb7397d
A[4]=5081ab07  B[4]=cf06e5ae  C[4]=66d5e90f  D[4]=4acd96b0
A[5]=7b3ea1f9  B[5]=eb539f0d  C[5]=75165f5d  D[5]=98899ace
A[6]=3c51d267  B[6]=c360f424  C[6]=ae058208  D[6]=85793c06
A[7]=6aa3c4ea  B[7]=d133d270  C[7]=637160aa  D[7]=e32bf513

Step 21: (r= 9, s=15)
A[0]=aee72dc6  B[0]=f55ea0e5  C[0]=88cba927  D[0]=509c1332
A[1]=e3043ab2  B[1]=d117fca1  C[1]=181cc58a  D[1]=0ec2e925
A[2]=55415181  B[2]=b49b5602  C[2]=e739bba8  D[2]=a3c94f91
A[3]=b8bc2856  B[3]=fc64f08b  C[3]=f30b31c9  D[3]=75b939f3
A[4]=d287263c  B[4]=03560ea1  C[4]=cf06e5ae  D[4]=66d5e90f
A[5]=be007adc  B[5]=7d43f2f6  C[5]=eb539f0d  D[5]=75165f5d
```

```
A[6]=4afaf257  B[6]=a3a4ce78  C[6]=c360f424  D[6]=ae058208
A[7]=cac2a589  B[7]=4789d4d5  C[7]=d133d270  D[7]=637160aa

Step 22: (r=15, s= 5)
A[0]=ec6382fc  B[0]=96e35773  C[0]=f55ea0e5  D[0]=88cba927
A[1]=cb7620a8  B[1]=1d597182  C[1]=d117fca1  D[1]=181cc58a
A[2]=42c03828  B[2]=a8c0aaa0  C[2]=b49b5602  D[2]=e739bba8
A[3]=cdc7e321  B[3]=142b5c5e  C[3]=fc64f08b  D[3]=f30b31c9
A[4]=c5a7c0a0  B[4]=931e6943  C[4]=03560ea1  D[4]=cf06e5ae
A[5]=be3184f1  B[5]=3d6e5f00  C[5]=7d43f2f6  D[5]=eb539f0d
A[6]=32df07d4  B[6]=792ba57d  C[6]=a3a4ce78  D[6]=c360f424
A[7]=caf55211  B[7]=52c4e561  C[7]=4789d4d5  D[7]=d133d270

Step 23: (r= 5, s=29)
A[0]=dcc0f577  B[0]=8c705f9d  C[0]=96e35773  D[0]=f55ea0e5
A[1]=e06221c7  B[1]=6ec41519  C[1]=1d597182  D[1]=d117fca1
A[2]=a85bb36a  B[2]=58070508  C[2]=a8c0aaa0  D[2]=b49b5602
A[3]=e3599eac  B[3]=b8fc6439  C[3]=142b5c5e  D[3]=fc64f08b
A[4]=cde13893  B[4]=b4f81418  C[4]=931e6943  D[4]=03560ea1
A[5]=bcd097e9  B[5]=c6309e37  C[5]=3d6e5f00  D[5]=7d43f2f6
A[6]=b4e06285  B[6]=5be0fa86  C[6]=792ba57d  D[6]=a3a4ce78
A[7]=5c837f3b  B[7]=5eaa4239  C[7]=52c4e561  D[7]=4789d4d5

Step 24: (r= 4, s=13)
A[0]=860949d6  B[0]=cc0f577d  C[0]=8c705f9d  D[0]=96e35773
A[1]=84bdcb29  B[1]=06221c7e  C[1]=6ec41519  D[1]=1d597182
A[2]=aea9b78b  B[2]=85bb36aa  C[2]=58070508  D[2]=a8c0aaa0
A[3]=6bbf7489  B[3]=3599eace  C[3]=b8fc6439  D[3]=142b5c5e
A[4]=2217591e  B[4]=de13893c  C[4]=b4f81418  D[4]=931e6943
A[5]=0d47c38c  B[5]=cd097e9b  C[5]=c6309e37  D[5]=3d6e5f00
A[6]=86017c23  B[6]=4e06285b  C[6]=5be0fa86  D[6]=792ba57d
A[7]=f92e55d5  B[7]=c837f3b5  C[7]=5eaa4239  D[7]=52c4e561

Step 25: (r=13, s=10)
A[0]=06682afa  B[0]=293ad0c1  C[0]=cc0f577d  D[0]=8c705f9d
A[1]=b605c9c5  B[1]=b9653097  C[1]=06221c7e  D[1]=6ec41519
A[2]=19a2ddb7  B[2]=36f175d5  C[2]=85bb36aa  D[2]=58070508
A[3]=5bfab256  B[3]=ee912d77  C[3]=3599eace  D[3]=b8fc6439
A[4]=8c9143ec  B[4]=eb23c442  C[4]=de13893c  D[4]=b4f81418
A[5]=d87a90aa  B[5]=f87181a8  C[5]=cd097e9b  D[5]=c6309e37
A[6]=5cdb03d1  B[6]=2f8470c0  C[6]=4e06285b  D[6]=5be0fa86
A[7]=bfc01670  B[7]=cababf25  C[7]=c837f3b5  D[7]=5eaa4239

Step 26: (r=10, s=25)
A[0]=514f781d  B[0]=a0abe819  C[0]=293ad0c1  D[0]=cc0f577d
A[1]=97eca227  B[1]=172716d8  C[1]=b9653097  D[1]=06221c7e
A[2]=cbf9967c  B[2]=8b76dc66  C[2]=36f175d5  D[2]=85bb36aa
A[3]=76bccc6e  B[3]=eac9596f  C[3]=ee912d77  D[3]=3599eace
A[4]=b84256cc  B[4]=450fb232  C[4]=eb23c442  D[4]=de13893c
```

```
A[5]=62442bf9  B[5]=ea42ab61  C[5]=f87181a8  D[5]=cd097e9b
A[6]=8ae31037  B[6]=6c0f4573  C[6]=2f8470c0  D[6]=4e06285b
A[7]=3ad4ceb6  B[7]=0059c2ff  C[7]=cababf25  D[7]=c837f3b5

Step 27: (r=25, s= 4)
A[0]=c1dba665  B[0]=3aa29ef0  C[0]=a0abe819  D[0]=293ad0c1
A[1]=652e5b54  B[1]=4f2fd944  C[1]=172716d8  D[1]=b9653097
A[2]=dcb67446  B[2]=f997f32c  C[2]=8b76dc66  D[2]=36f175d5
A[3]=588104a8  B[3]=dced7998  C[3]=eac9596f  D[3]=ee912d77
A[4]=61483fae  B[4]=997084ad  C[4]=450fb232  D[4]=eb23c442
A[5]=081837da  B[5]=f2c48857  C[5]=ea42ab61  D[5]=f87181a8
A[6]=f7e43a9f  B[6]=6f15c620  C[6]=6c0f4573  D[6]=2f8470c0
A[7]=4c870c05  B[7]=6c75a99d  C[7]=0059c2ff  D[7]=cababf25

Step 28: (r= 4, s=13)
A[0]=37dff96e  B[0]=1dba665c  C[0]=3aa29ef0  D[0]=a0abe819
A[1]=a0c4f4e1  B[1]=52e5b546  C[1]=4f2fd944  D[1]=172716d8
A[2]=d8c18930  B[2]=cb67446d  C[2]=f997f32c  D[2]=8b76dc66
A[3]=fd515c52  B[3]=88104a85  C[3]=dced7998  D[3]=eac9596f
A[4]=6fbe4450  B[4]=1483fae6  C[4]=997084ad  D[4]=450fb232
A[5]=569c9ac3  B[5]=81837da0  C[5]=f2c48857  D[5]=ea42ab61
A[6]=c98c69e8  B[6]=7e43a9ff  C[6]=6f15c620  D[6]=6c0f4573
A[7]=8e840599  B[7]=c870c054  C[7]=6c75a99d  D[7]=0059c2ff

Step 29: (r=13, s=10)
A[0]=15b583d4  B[0]=ff2dc6fb  C[0]=1dba665c  D[0]=3aa29ef0
A[1]=1c313fea  B[1]=9e9c3418  C[1]=52e5b546  D[1]=4f2fd944
A[2]=577fc30c  B[2]=31261b18  C[2]=cb67446d  D[2]=f997f32c
A[3]=c5ffa610  B[3]=2b8a5faa  C[3]=88104a85  D[3]=dced7998
A[4]=eca8c6fc  B[4]=c88a0df7  C[4]=1483fae6  D[4]=997084ad
A[5]=0e4c2ceb  B[5]=93586ad3  C[5]=81837da0  D[5]=f2c48857
A[6]=f2cb9786  B[6]=8d3d1931  C[6]=7e43a9ff  D[6]=6f15c620
A[7]=384046b9  B[7]=80b331d0  C[7]=c870c054  D[7]=6c75a99d

Step 30: (r=10, s=25)
A[0]=c71cc2c8  B[0]=d60f5056  C[0]=ff2dc6fb  D[0]=1dba665c
A[1]=9f8d8b1a  B[1]=c4ffa870  C[1]=9e9c3418  D[1]=52e5b546
A[2]=ac3de92d  B[2]=ff0c315d  C[2]=31261b18  D[2]=cb67446d
A[3]=4cfb62d1  B[3]=fe984317  C[3]=2b8a5faa  D[3]=88104a85
A[4]=3b504e4c  B[4]=a31bf3b2  C[4]=c88a0df7  D[4]=1483fae6
A[5]=5e57187b  B[5]=30b3ac39  C[5]=93586ad3  D[5]=81837da0
A[6]=2e6edbf9  B[6]=2e5e1bcb  C[6]=8d3d1931  D[6]=7e43a9ff
A[7]=a27ae230  B[7]=011ae4e1  C[7]=80b331d0  D[7]=c870c054

Step 31: (r=25, s= 4)
A[0]=10196937  B[0]=918e3985  C[0]=d60f5056  D[0]=ff2dc6fb
A[1]=79bd4b92  B[1]=353f1b16  C[1]=c4ffa870  D[1]=9e9c3418
A[2]=850e2d27  B[2]=5b587bd2  C[2]=ff0c315d  D[2]=31261b18
A[3]=32a9e4a1  B[3]=a299f6c5  C[3]=fe984317  D[3]=2b8a5faa
```

```
A[4]=8d0871c1  B[4]=9876a09c  C[4]=a31bf3b2  D[4]=c88a0df7
A[5]=03506be7  B[5]=f6bcae30  C[5]=30b3ac39  D[5]=93586ad3
A[6]=73235d70  B[6]=f25cddb7  C[6]=2e5e1bcb  D[6]=8d3d1931
A[7]=a4c5334c  B[7]=6144f5c4  C[7]=011ae4e1  D[7]=80b331d0

Feed-Forward Step 32: (r= 4, s=13)
A[0]=92e64a5e  B[0]=01969371  C[0]=918e3985  D[0]=d60f5056
A[1]=c42a792f  B[1]=9bd4b927  C[1]=353f1b16  D[1]=c4ffa870
A[2]=8651e47a  B[2]=50e2d278  C[2]=5b587bd2  D[2]=ff0c315d
A[3]=1bff7096  B[3]=2a9e4a13  C[3]=a299f6c5  D[3]=fe984317
A[4]=d0208607  B[4]=d0871c18  C[4]=9876a09c  D[4]=a31bf3b2
A[5]=887c0311  B[5]=3506be70  C[5]=f6bcae30  D[5]=30b3ac39
A[6]=1222eb90  B[6]=3235d707  C[6]=f25cddb7  D[6]=2e5e1bcb
A[7]=be739d54  B[7]=4c5334ca  C[7]=6144f5c4  D[7]=011ae4e1

Feed-Forward Step 33: (r=13, s=10)
A[0]=6ce4b8f9  B[0]=c94bd25c  C[0]=01969371  D[0]=918e3985
A[1]=8968ac7d  B[1]=4f25f885  C[1]=9bd4b927  D[1]=353f1b16
A[2]=476a6acf  B[2]=3c8f50ca  C[2]=50e2d278  D[2]=5b587bd2
A[3]=3ff80d79  B[3]=ee12c37f  C[3]=2a9e4a13  D[3]=a299f6c5
A[4]=1d1b3407  B[4]=10c0fa04  C[4]=d0871c18  D[4]=9876a09c
A[5]=985286f5  B[5]=8062310f  C[5]=3506be70  D[5]=f6bcae30
A[6]=eaeb9e22  B[6]=5d720244  C[6]=3235d707  D[6]=f25cddb7
A[7]=d43e38dd  B[7]=73aa97ce  C[7]=4c5334ca  D[7]=6144f5c4

Feed-Forward Step 34: (r=10, s=25)
A[0]=f7f9a58d  B[0]=92e3e5b3  C[0]=c94bd25c  D[0]=01969371
A[1]=d9853ba5  B[1]=a2b1f625  C[1]=4f25f885  D[1]=9bd4b927
A[2]=ba781c52  B[2]=a9ab3d1d  C[2]=3c8f50ca  D[2]=50e2d278
A[3]=fe76705a  B[3]=e035e4ff  C[3]=ee12c37f  D[3]=2a9e4a13
A[4]=88ab9d8e  B[4]=6cd01c74  C[4]=10c0fa04  D[4]=d0871c18
A[5]=4f4d51ac  B[5]=4a1bd661  C[5]=8062310f  D[5]=3506be70
A[6]=4b0a442d  B[6]=ae788bab  C[6]=5d720244  D[6]=3235d707
A[7]=c9faeafc  B[7]=f8e37750  C[7]=73aa97ce  D[7]=4c5334ca

Feed-Forward Step 35: (r=25, s= 4)
A[0]=7762dd5f  B[0]=1beff34b  C[0]=92e3e5b3  D[0]=c94bd25c
A[1]=2213c28f  B[1]=4bb30a77  C[1]=a2b1f625  D[1]=4f25f885
A[2]=3bad9018  B[2]=a574f038  C[2]=a9ab3d1d  D[2]=3c8f50ca
A[3]=4a2a74ac  B[3]=b5fcece0  C[3]=e035e4ff  D[3]=ee12c37f
A[4]=26ce07f1  B[4]=1d11573b  C[4]=6cd01c74  D[4]=10c0fa04
A[5]=2e11d692  B[5]=589e9aa3  C[5]=4a1bd661  D[5]=8062310f
A[6]=b2545b79  B[6]=5a961488  C[6]=ae788bab  D[6]=5d720244
A[7]=0f5ecd5d  B[7]=f993f5d5  C[7]=f8e37750  D[7]=73aa97ce
```

Compression Function Output

```
A[0]=7762dd5f  B[0]=1beff34b  C[0]=92e3e5b3  D[0]=c94bd25c
A[1]=2213c28f  B[1]=4bb30a77  C[1]=a2b1f625  D[1]=4f25f885
```

```
A[2]=3bad9018  B[2]=a574f038  C[2]=a9ab3d1d  D[2]=3c8f50ca
A[3]=4a2a74ac  B[3]=b5fcece0  C[3]=e035e4ff  D[3]=ee12c37f
A[4]=26ce07f1  B[4]=1d11573b  C[4]=6cd01c74  D[4]=10c0fa04
A[5]=2e11d692  B[5]=589e9aa3  C[5]=4a1bd661  D[5]=8062310f
A[6]=b2545b79  B[6]=5a961488  C[6]=ae788bab  D[6]=5d720244
A[7]=0f5ecd5d  B[7]=f993f5d5  C[7]=f8e37750  D[7]=73aa97ce
```

Hash Function Output

```
5fdd62778fc213221890ad3bac742a4af107ce2692d6112e795b54b25dcd5e0f4bf3ef1b770ab34b38f074a5e0ecfcb5
```

A.3.2 One-block Message

We use the message block `0x00 0x01 0x02` ... as an example.

First block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
M[ 64.. 71] = 40 41 42 43 44 45 46 47
M[ 72.. 79] = 48 49 4a 4b 4c 4d 4e 4f
M[ 80.. 87] = 50 51 52 53 54 55 56 57
M[ 88.. 95] = 58 59 5a 5b 5c 5d 5e 5f
M[ 96..103] = 60 61 62 63 64 65 66 67
M[104..111] = 68 69 6a 6b 6c 6d 6e 6f
M[112..119] = 70 71 72 73 74 75 76 77
M[120..127] = 78 79 7a 7b 7c 7d 7e 7f
```

NTT Output

```
y[  0..  7] =  162   85  125  159   75  219   54   22
y[  8.. 15] =  128  171   94  185    6   71   55   63
y[ 16.. 23] =    0  203    4  152  200   45   80  133
y[ 24.. 31] =  245  117  101  152   61   77  169  230
y[ 32.. 39] =  150  100  200  254  121   31  253   22
y[ 40.. 47] =  186  171   27   59  145   41  103  177
y[ 48.. 55] =   23   10  157    5  176   84  216   88
y[ 56.. 63] =   57   20  253    9  130  255   53   84
y[ 64.. 71] =  181  160  241   61   47  252  168   18
y[ 72.. 79] =  237   26   30   19  166   18  110  113
y[ 80.. 87] =   21  240   15  103  230   72   61  142
y[ 88.. 95] =  138  119   66   45   86   29   84  243
y[ 96..103] =  202   33  131  121  206  189   63   26
y[104..111] =  129  171   92   61  218   92  254   87
```

```
y[112..119] =  84  189  205  152  233    8  203  182
y[120..127] = 168  207  190  143  124  129   57   30
y[128..135] = 192  141   92  168  121  110  169   28
y[136..143] = 128  161  211  146  197   45   44  249
y[144..151] = 171  249   62   82  157  156   70   32
y[152..159] = 122  202  163   42  174   32   21  256
y[160..167] = 244   93  107    0   28  137   44  134
y[168..175] = 129  255  154   17   97  197  180   68
y[176..183] = 132  107  244   30   65  163  147  190
y[184..191] = 115  193   79   65   69  180   30   67
y[192..199] = 205    3  191  238   12   69   15  256
y[200..207] = 106   66  122   90  108  168    4   39
y[208..215] =  82  251  217  159   43   47   16  138
y[216..223] =  62   41  152   21   23  239  124  246
y[224..231] = 176   51  194   43   74   68  188  100
y[232..239] =  19  207   16  134  197   67  195   38
y[240..247] =   3  145  211  141   79   12    7  226
y[248..255] =  91   41  102  109  195  181  241   46
```

Intermediate Expanded Message

```
Z[ 0] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
Z[ 1] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
Z[ 2] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
Z[ 3] = 073a109f  039db7bc  3cb4c577  3f98e25f
        0e742931  0681fd1c  fe8ea439  3cb4264d
Z[ 4] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
        12caf18c  0dbb15ae  0d02be3d  51a94f7e
Z[ 5] = f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
        55ffaa01  20852fb2  14f53e26  f5e23cb4
Z[ 6] = 17d9d841  5771a4f2  cedcdb25  12ca2d87
        c1daa380  2c15427c  427ce3d1  3edffdd5
Z[ 7] = cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
        dbdebfaf  ad9ecf95  a380599c  15ae2931
Z[ 8] = ac2cd107  bfaf427c  4f7e5771  143cc068
        baa05c80  afc9dec2  2085d4a4  fa381fcc
Z[ 9] = fa38c1da  3b422cce  b703b7bc  17203296
        d841582a  1e5abc12  1720c405  ff470f2d
Z[10] = 4335f69b  00004d53  a948143c  a71d1fcc
        fe8ea380  0c49b591  d4a44619  3124c85b
Z[11] = 4d53a5ab  15aef69b  bc122ef9  cf95b082
        d1c0531b  2ef93917  c85b31dd  306b15ae
Z[12] = 022bda6c  f245d04e  31dd08ac  ff470ad7
        2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
Z[13] = fbaa3b42  b92ee318  21f71f13  aa010b90
        1da12cce  0f2db41f  f2fe109f  f80d599c
```

```
Z[14] = 24dbc577  1f13d279  3124357a  4844ce23
        dbde0dbb  a71d0b90  306bd4a4  1b76d332
Z[15] = af10022b  ac2cdec2  08ac3917  e999050f
        1da141c3  4ec549b6  c914d332  213ef470
Z[16] = c4d7a989  53bc71c5  6e214443  afe83126
        74807480  d622558e  c9640576  280c320f
Z[17] = b1ba0000  386e03a4  a4fccc1f  3fb648d0
        6f0af514  aa725bed  b4753785  131dafe8
Z[18] = f42b9e9d  6163cc1f  197c6e21  280cfc5c
        8b80bf61  a2411893  58499a10  b9eb5dbf
Z[19] = 8e3b14ef  f42ba4fc  3b29b647  9be2daaf
        68ab33e1  47e7fc5c  3ecd8c69  1b4e303d
Z[20] = d0acbad4  c3eef170  0aec2ac7  0da7aeff
        607aedcc  6f0a1b4e  624cad2d  03a4641e
Z[21] = 4aa2131d  db980da7  2723e76d  0e903785
        386e93b1  a06f3c12  14ef4e46  70dc4c74
Z[22] = b647cdf1  c6a98d52  435ad195  c1333957
        114b8b80  0e9053bc  c964dc81  c792fd45
Z[23] = 02bb4c74  d622d0ac  47e7ea28  065fceda
        52d3aeff  5cd6c305  c79270dc  f17033e1
Z[24] = 966c4d5d  aeffa6ce  641edd6a  197c1406
        a8a0b1ba  9af9be78  28f5409f  f8b83957
Z[25] = f8b8ceda  4aa2a06f  a41328f5  1d208f24
        cdf16a7d  263aa06f  1d204615  ff17e76d
Z[26] = 54a55b04  0000fd45  92c81c37  900d1406
        fe2eb1ba  0f7935b3  c9642551  3de4b730
Z[27] = 6163091a  1b4e048d  aa724c74  c3055018
        c5c01234  3b290831  b9ebfe2e  3cfb4c74
Z[28] = 02bba7b7  eeb53785  3ecdfb73  ff171062
        3c1217aa  51ea114b  aeff1062  237f66d9
Z[29] = fa8af087  a6ce5dbf  2ac74188  93b19755
        25516c4f  131d28f5  ef9e1a65  f5fdf342
Z[30] = 2e6b1e09  27236e21  3de4c21c  5b0417aa
        d27eb1ba  900d3785  3cfb53bc  22964f2f
Z[31] = 9a10c21c  966ca06f  0aec0748  e3c9bbbd
        2551d27e  6335983e  bad48b80  29de1b4e
```

Expanded Message

```
W[ 0] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
        12caf18c  0dbb15ae  0d02be3d  51a94f7e
W[ 1] = 17d9d841  5771a4f2  cedcdb25  12ca2d87
        c1daa380  2c15427c  427ce3d1  3edffdd5
W[ 2] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
W[ 3] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
W[ 4] = cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
        dbdebfaf  ad9ecf95  a380599c  15ae2931
```

```
W[ 5] = f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
        55ffaa01  20852fb2  14f53e26  f5e23cb4
W[ 6] = 073a109f  039db7bc  3cb4c577  3f98e25f
        0e742931  0681fd1c  fe8ea439  3cb4264d
W[ 7] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
W[ 8] = af10022b  ac2cdec2  08ac3917  e999050f
        1da141c3  4ec549b6  c914d332  213ef470
W[ 9] = 4d53a5ab  15aef69b  bc122ef9  cf95b082
        d1c0531b  2ef93917  c85b31dd  306b15ae
W[10] = 022bda6c  f245d04e  31dd08ac  ff470ad7
        2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
W[11] = ac2cd107  bfaf427c  4f7e5771  143cc068
        baa05c80  afc9dec2  2085d4a4  fa381fcc
W[12] = fa38c1da  3b422cce  b703b7bc  17203296
        d841582a  1e5abc12  1720c405  ff470f2d
W[13] = fbaa3b42  b92ee318  21f71f13  aa010b90
        1da12cce  0f2db41f  f2fe109f  f80d599c
W[14] = 4335f69b  00004d53  a948143c  a71d1fcc
        fe8ea380  0c49b591  d4a44619  3124c85b
W[15] = 24dbc577  1f13d279  3124357a  4844ce23
        dbde0dbb  a71d0b90  306bd4a4  1b76d332
W[16] = b1ba0000  386e03a4  a4fccc1f  3fb648d0
        6f0af514  aa725bed  b4753785  131dafe8
W[17] = f42b9e9d  6163cc1f  197c6e21  280cfc5c
        8b80bf61  a2411893  58499a10  b9eb5dbf
W[18] = 02bb4c74  d622d0ac  47e7ea28  065fceda
        52d3aeff  5cd6c305  c79270dc  f17033e1
W[19] = d0acbad4  c3eef170  0aec2ac7  0da7aeff
        607aedcc  6f0a1b4e  624cad2d  03a4641e
W[20] = b647cdf1  c6a98d52  435ad195  c1333957
        114b8b80  0e9053bc  c964dc81  c792fd45
W[21] = 4aa2131d  db980da7  2723e76d  0e903785
        386e93b1  a06f3c12  14ef4e46  70dc4c74
W[22] = c4d7a989  53bc71c5  6e214443  afe83126
        74807480  d622558e  c9640576  280c320f
W[23] = 8e3b14ef  f42ba4fc  3b29b647  9be2daaf
        68ab33e1  47e7fc5c  3ecd8c69  1b4e303d
W[24] = 2e6b1e09  27236e21  3de4c21c  5b0417aa
        d27eb1ba  900d3785  3cfb53bc  22964f2f
W[25] = 966c4d5d  aeffa6ce  641edd6a  197c1406
        a8a0b1ba  9af9be78  28f5409f  f8b83957
W[26] = f8b8ceda  4aa2a06f  a41328f5  1d208f24
        cdf16a7d  263aa06f  1d204615  ff17e76d
W[27] = 9a10c21c  966ca06f  0aec0748  e3c9bbbd
        2551d27e  6335983e  bad48b80  29de1b4e
W[28] = 6163091a  1b4e048d  aa724c74  c3055018
        c5c01234  3b290831  b9ebfe2e  3cfb4c74
W[29] = fa8af087  a6ce5dbf  2ac74188  93b19755
```

```
        25516c4f  131d28f5  ef9e1a65  f5fdf342
W[30] = 02bba7b7  eeb53785  3ecdfb73  ff171062
        3c1217aa  51ea114b  aeff1062  237f66d9
W[31] = 54a55b04  0000fd45  92c81c37  900d1406
        fe2eb1ba  0f7935b3  c9642551  3de4b730
```

Feistel Steps

```
IV :
A[0]=8a36eebc  B[0]=7360ca61  C[0]=b9e3bfe8  D[0]=e64071ec
A[1]=94a3bd90  B[1]=18361a03  C[1]=63bece2a  D[1]=1deb91a8
A[2]=d1537b83  B[2]=17dcb4b9  C[2]=8fe506b9  D[2]=8ac8db23
A[3]=b25b070b  B[3]=3414c45a  C[3]=f8cc4ac2  D[3]=3f782ab5
A[4]=f463f1b5  B[4]=a699a9d2  C[4]=7ae11542  D[4]=039b5cb8
A[5]=b6f81e20  B[5]=e39e9664  C[5]=b1aadda1  D[5]=71ddd962
A[6]=0055c339  B[6]=468bfe77  C[6]=64b06794  D[6]=fade2cea
A[7]=b4d144d1  B[7]=51d062f8  C[7]=28d2f462  D[7]=1416df71

IV XOR M :
A[0]=8934efbc  B[0]=5042eb41  C[0]=faa1fea8  D[0]=8522108c
A[1]=93a5b894  B[1]=3f103f27  C[1]=24f88b6e  D[1]=7a8df4cc
A[2]=da59728b  B[2]=3cf69d91  C[2]=c4af4ff1  D[2]=e1a2b24b
A[3]=bd550a07  B[3]=1b3ae976  C[3]=b782078e  D[3]=501647d9
A[4]=e771e0a5  B[4]=95ab98e2  C[4]=29b34412  D[4]=70e92dc8
A[5]=a1ee0b34  B[5]=d4a8a350  C[5]=e6fc88f5  D[5]=06abac16
A[6]=1b4fda21  B[6]=7db1c74f  C[6]=3fea3ecc  D[6]=81a45592
A[7]=abcf59cd  B[7]=6eee5fc4  C[7]=778ca93e  D[7]=6b68a20d

Step  0: (r= 3, s=23)
A[0]=ed868a8e  B[0]=49a77de4  C[0]=5042eb41  D[0]=faa1fea8
A[1]=9f167bf6  B[1]=9d2dc4a4  C[1]=3f103f27  D[1]=24f88b6e
A[2]=04a5ce36  B[2]=d2cb945e  C[2]=3cf69d91  D[2]=c4af4ff1
A[3]=5e07e9e8  B[3]=eaa8503d  C[3]=1b3ae976  D[3]=b782078e
A[4]=12790577  B[4]=3b8f052f  C[4]=95ab98e2  D[4]=29b34412
A[5]=067c94d1  B[5]=0f7059a5  C[5]=d4a8a350  D[5]=e6fc88f5
A[6]=ace0f2ea  B[6]=da7ed108  C[6]=7db1c74f  D[6]=3fea3ecc
A[7]=9b1cc17d  B[7]=5e7ace6d  C[7]=6eee5fc4  D[7]=778ca93e

Step  1: (r=23, s=17)
A[0]=f6b348fd  B[0]=4776c345  C[0]=49a77de4  D[0]=5042eb41
A[1]=a8d8013c  B[1]=fb4f8b3d  C[1]=9d2dc4a4  D[1]=3f103f27
A[2]=3ce4d541  B[2]=1b0252e7  C[2]=d2cb945e  D[2]=3cf69d91
A[3]=53296952  B[3]=f42f03f4  C[3]=eaa8503d  D[3]=1b3ae976
A[4]=2575591a  B[4]=bb893c82  C[4]=3b8f052f  D[4]=95ab98e2
A[5]=f214d7f7  B[5]=68833e4a  C[5]=0f7059a5  D[5]=d4a8a350
A[6]=36cb7af6  B[6]=75567079  C[6]=da7ed108  D[6]=7db1c74f
A[7]=074ff60c  B[7]=becd8e60  C[7]=5e7ace6d  D[7]=6eee5fc4

Step  2: (r=17, s=27)
```

```
A[0]=a969b2a7  B[0]=91fbed66  C[0]=4776c345  D[0]=49a77de4
A[1]=9852094b  B[1]=027951b0  C[1]=fb4f8b3d  D[1]=9d2dc4a4
A[2]=b1d84e87  B[2]=aa8279c9  C[2]=1b0252e7  D[2]=d2cb945e
A[3]=cb97a2bf  B[3]=d2a4a652  C[3]=f42f03f4  D[3]=eaa8503d
A[4]=4284f622  B[4]=b2344aea  C[4]=bb893c82  D[4]=3b8f052f
A[5]=ec8816cb  B[5]=afefe429  C[5]=68833e4a  D[5]=0f7059a5
A[6]=9fa008d2  B[6]=f5ec6d96  C[6]=75567079  D[6]=da7ed108
A[7]=d7c77cd8  B[7]=ec180e9f  C[7]=becd8e60  D[7]=5e7ace6d

Step  3: (r=27, s= 3)
A[0]=c9bd4ccf  B[0]=3d4b4d95  C[0]=91fbed66  D[0]=4776c345
A[1]=3097b7b3  B[1]=5cc2904a  C[1]=027951b0  D[1]=fb4f8b3d
A[2]=fa6cb5ce  B[2]=3d8ec274  C[2]=aa8279c9  D[2]=1b0252e7
A[3]=c72ad2f4  B[3]=fe5cbd15  C[3]=d2a4a652  D[3]=f42f03f4
A[4]=8a771ffb  B[4]=121427b1  C[4]=b2344aea  D[4]=bb893c82
A[5]=c9f1c9d5  B[5]=5f6440b6  C[5]=afefe429  D[5]=68833e4a
A[6]=d01c0755  B[6]=94fd0046  C[6]=f5ec6d96  D[6]=75567079
A[7]=97b16451  B[7]=c6be3be6  C[7]=ec180e9f  D[7]=becd8e60

Step  4: (r= 3, s=23)
A[0]=2fe675d4  B[0]=4dea667e  C[0]=3d4b4d95  D[0]=91fbed66
A[1]=01992157  B[1]=84bdbd99  C[1]=5cc2904a  D[1]=027951b0
A[2]=6b78cfa5  B[2]=d365ae77  C[2]=3d8ec274  D[2]=aa8279c9
A[3]=222a4f77  B[3]=395697a6  C[3]=fe5cbd15  D[3]=d2a4a652
A[4]=9ad28b9f  B[4]=53b8ffdc  C[4]=121427b1  D[4]=b2344aea
A[5]=985d6a65  B[5]=4f8e4eae  C[5]=5f6440b6  D[5]=afefe429
A[6]=ef4d810d  B[6]=80e03aae  C[6]=94fd0046  D[6]=f5ec6d96
A[7]=07b3486a  B[7]=bd8b228c  C[7]=c6be3be6  D[7]=ec180e9f

Step  5: (r=23, s=17)
A[0]=f9d340de  B[0]=ea17f33a  C[0]=4dea667e  D[0]=3d4b4d95
A[1]=a2bc49c4  B[1]=ab80cc90  C[1]=84bdbd99  D[1]=5cc2904a
A[2]=9c42e2a5  B[2]=d2b5bc67  C[2]=d365ae77  D[2]=3d8ec274
A[3]=b30add15  B[3]=bb911527  C[3]=395697a6  D[3]=fe5cbd15
A[4]=04a14ab0  B[4]=cfcd6945  C[4]=53b8ffdc  D[4]=121427b1
A[5]=8fb81be9  B[5]=32cc2eb5  C[5]=4f8e4eae  D[5]=5f6440b6
A[6]=0315ec2d  B[6]=86f7a6c0  C[6]=80e03aae  D[6]=94fd0046
A[7]=d69ac6a4  B[7]=3503d9a4  C[7]=bd8b228c  D[7]=c6be3be6

Step  6: (r=17, s=27)
A[0]=26d2cf47  B[0]=81bdf3a6  C[0]=ea17f33a  D[0]=4dea667e
A[1]=e7ec081c  B[1]=93894578  C[1]=ab80cc90  D[1]=84bdbd99
A[2]=6abf4fdd  B[2]=c54b3885  C[2]=d2b5bc67  D[2]=d365ae77
A[3]=6d11eed9  B[3]=ba2b6615  C[3]=bb911527  D[3]=395697a6
A[4]=34ff818b  B[4]=95600942  C[4]=cfcd6945  D[4]=53b8ffdc
A[5]=8f34d7db  B[5]=37d31f70  C[5]=32cc2eb5  D[5]=4f8e4eae
A[6]=1dff431e  B[6]=d85a062b  C[6]=86f7a6c0  D[6]=80e03aae
A[7]=77f3573b  B[7]=8d49ad35  C[7]=3503d9a4  D[7]=bd8b228c
```

```
Step  7: (r=27, s= 3)
A[0]=33222d66  B[0]=3936967a  C[0]=81bdf3a6  D[0]=ea17f33a
A[1]=1c5efb28  B[1]=e73f6040  C[1]=93894578  D[1]=ab80cc90
A[2]=80be9fd3  B[2]=eb55fa7e  C[2]=c54b3885  D[2]=d2b5bc67
A[3]=c1b7b6da  B[3]=cb688f76  C[3]=ba2b6615  D[3]=bb911527
A[4]=ce19aa57  B[4]=59a7fc0c  C[4]=95600942  D[4]=cfcd6945
A[5]=35b5b8ed  B[5]=dc79a6be  C[5]=37d31f70  D[5]=32cc2eb5
A[6]=87e30123  B[6]=f0effa18  C[6]=d85a062b  D[6]=86f7a6c0
A[7]=eb55fb66  B[7]=dbbf9ab9  C[7]=8d49ad35  D[7]=3503d9a4

Step  8: (r=28, s=19)
A[0]=9ab88750  B[0]=633222d6  C[0]=3936967a  D[0]=81bdf3a6
A[1]=ebcc5a1e  B[1]=81c5efb2  C[1]=e73f6040  D[1]=93894578
A[2]=fb86a062  B[2]=380be9fd  C[2]=eb55fa7e  D[2]=c54b3885
A[3]=d7c85e25  B[3]=ac1b7b6d  C[3]=cb688f76  D[3]=ba2b6615
A[4]=d86e207f  B[4]=7ce19aa5  C[4]=59a7fc0c  D[4]=95600942
A[5]=ad583b96  B[5]=d35b5b8e  C[5]=dc79a6be  D[5]=37d31f70
A[6]=63036b11  B[6]=387e3012  C[6]=f0effa18  D[6]=d85a062b
A[7]=e3ef1ab5  B[7]=6eb55fb6  C[7]=dbbf9ab9  D[7]=8d49ad35

Step  9: (r=19, s=22)
A[0]=f6146e1f  B[0]=3a84d5c4  C[0]=633222d6  D[0]=3936967a
A[1]=8a7a8a2b  B[1]=d0f75e62  C[1]=81c5efb2  D[1]=e73f6040
A[2]=b933421c  B[2]=0317dc35  C[2]=380be9fd  D[2]=eb55fa7e
A[3]=547cd8de  B[3]=f12ebe42  C[3]=ac1b7b6d  D[3]=cb688f76
A[4]=793b58a9  B[4]=03fec371  C[4]=7ce19aa5  D[4]=59a7fc0c
A[5]=e2fd30f6  B[5]=dcb56ac1  C[5]=d35b5b8e  D[5]=dc79a6be
A[6]=0c132c6b  B[6]=588b181b  C[6]=387e3012  D[6]=f0effa18
A[7]=44838558  B[7]=d5af1f78  C[7]=6eb55fb6  D[7]=dbbf9ab9

Step 10: (r=22, s= 7)
A[0]=7beff46d  B[0]=87fd851b  C[0]=3a84d5c4  D[0]=633222d6
A[1]=457e6cfd  B[1]=8ae29ea2  C[1]=d0f75e62  D[1]=81c5efb2
A[2]=b2592e31  B[2]=872e4cd0  C[2]=0317dc35  D[2]=380be9fd
A[3]=f7a85d7c  B[3]=37951f36  C[3]=f12ebe42  D[3]=ac1b7b6d
A[4]=009686a8  B[4]=2a5e4ed6  C[4]=03fec371  D[4]=7ce19aa5
A[5]=b8785d42  B[5]=3db8bf4c  C[5]=dcb56ac1  D[5]=d35b5b8e
A[6]=c4e8df40  B[6]=1ac304cb  C[6]=588b181b  D[6]=387e3012
A[7]=7d5d1c89  B[7]=561120e1  C[7]=d5af1f78  D[7]=6eb55fb6

Step 11: (r= 7, s=28)
A[0]=9d6368f2  B[0]=f7fa36bd  C[0]=87fd851b  D[0]=3a84d5c4
A[1]=5868d90d  B[1]=bf367ea2  C[1]=8ae29ea2  D[1]=d0f75e62
A[2]=cf37d696  B[2]=2c9718d9  C[2]=872e4cd0  D[2]=0317dc35
A[3]=33ed9012  B[3]=d42ebe7b  C[3]=37951f36  D[3]=f12ebe42
A[4]=22e68291  B[4]=4b435400  C[4]=2a5e4ed6  D[4]=03fec371
A[5]=17f85e5e  B[5]=3c2ea15c  C[5]=3db8bf4c  D[5]=dcb56ac1
A[6]=eb4b2f0c  B[6]=746fa062  C[6]=1ac304cb  D[6]=588b181b
A[7]=60712110  B[7]=ae8e44be  C[7]=561120e1  D[7]=d5af1f78
```

```
Step 12: (r=28, s=19)
A[0]=e8d577d6  B[0]=29d6368f  C[0]=f7fa36bd  D[0]=87fd851b
A[1]=1d49e7d3  B[1]=d5868d90  C[1]=bf367ea2  D[1]=8ae29ea2
A[2]=6789d07c  B[2]=6cf37d69  C[2]=2c9718d9  D[2]=872e4cd0
A[3]=8a80680d  B[3]=233ed901  C[3]=d42ebe7b  D[3]=37951f36
A[4]=34970d34  B[4]=122e6829  C[4]=4b435400  D[4]=2a5e4ed6
A[5]=9e6d43b0  B[5]=e17f85e5  C[5]=3c2ea15c  D[5]=3db8bf4c
A[6]=d8dddd48  B[6]=ceb4b2f0  C[6]=746fa062  D[6]=1ac304cb
A[7]=a4800ec9  B[7]=06071211  C[7]=ae8e44be  D[7]=561120e1

Step 13: (r=19, s=22)
A[0]=28bd0435  B[0]=beb746ab  C[0]=29d6368f  D[0]=f7fa36bd
A[1]=70bd3986  B[1]=3e98ea4f  C[1]=d5868d90  D[1]=bf367ea2
A[2]=014c351f  B[2]=83e33c4e  C[2]=6cf37d69  D[2]=2c9718d9
A[3]=2a261548  B[3]=406c5403  C[3]=233ed901  D[3]=d42ebe7b
A[4]=afcdc85c  B[4]=69a1a4b8  C[4]=122e6829  D[4]=4b435400
A[5]=965b3fcc  B[5]=1d84f36a  C[5]=e17f85e5  D[5]=3c2ea15c
A[6]=f69debff  B[6]=ea46c6ee  C[6]=ceb4b2f0  D[6]=746fa062
A[7]=86297d23  B[7]=764d2400  C[7]=06071211  D[7]=ae8e44be

Step 14: (r=22, s= 7)
A[0]=553632ff  B[0]=0d4a2f41  C[0]=beb746ab  D[0]=29d6368f
A[1]=f704ecda  B[1]=619c2f4e  C[1]=3e98ea4f  D[1]=d5868d90
A[2]=333fbbf0  B[2]=47c0530d  C[2]=83e33c4e  D[2]=6cf37d69
A[3]=04d9f75b  B[3]=520a8985  C[3]=406c5403  D[3]=233ed901
A[4]=b3157309  B[4]=172bf372  C[4]=69a1a4b8  D[4]=122e6829
A[5]=03336060  B[5]=f32596cf  C[5]=1d84f36a  D[5]=e17f85e5
A[6]=1d4646fa  B[6]=fffda77a  C[6]=ea46c6ee  D[6]=ceb4b2f0
A[7]=e01e34ec  B[7]=48e18a5f  C[7]=764d2400  D[7]=06071211

Step 15: (r= 7, s=28)
A[0]=b9e1ff3d  B[0]=9b197faa  C[0]=0d4a2f41  D[0]=beb746ab
A[1]=85ddeb55  B[1]=82766d7b  C[1]=619c2f4e  D[1]=3e98ea4f
A[2]=84d933bb  B[2]=9fddf819  C[2]=47c0530d  D[2]=83e33c4e
A[3]=146cf7c3  B[3]=6cfbad82  C[3]=520a8985  D[3]=406c5403
A[4]=61f0deaa  B[4]=8ab984d9  C[4]=172bf372  D[4]=69a1a4b8
A[5]=66b7d5bf  B[5]=99b03001  C[5]=f32596cf  D[5]=1d84f36a
A[6]=8afff492  B[6]=a3237d0e  C[6]=fffda77a  D[6]=ea46c6ee
A[7]=7a931e13  B[7]=0f1a7670  C[7]=48e18a5f  D[7]=764d2400

Step 16: (r=29, s= 9)
A[0]=6a274c91  B[0]=b73c3fe7  C[0]=9b197faa  D[0]=0d4a2f41
A[1]=19443ba6  B[1]=b0bbbd6a  C[1]=82766d7b  D[1]=619c2f4e
A[2]=2a2d55c8  B[2]=709b2677  C[2]=9fddf819  D[2]=47c0530d
A[3]=cb5070f7  B[3]=628d9ef8  C[3]=6cfbad82  D[3]=520a8985
A[4]=21df4870  B[4]=4c3e1bd5  C[4]=8ab984d9  D[4]=172bf372
A[5]=be159475  B[5]=ecd6fab7  C[5]=99b03001  D[5]=f32596cf
A[6]=0b29d700  B[6]=515ffe92  C[6]=a3237d0e  D[6]=fffda77a
```

```
A[7]=a7ab83de  B[7]=6f5263c2  C[7]=0f1a7670  D[7]=48e18a5f

Step 17: (r= 9, s=15)
A[0]=a7a6c9ef  B[0]=4e9922d4  C[0]=b73c3fe7  D[0]=9b197faa
A[1]=971fbaed  B[1]=88774c32  C[1]=b0bbbd6a  D[1]=82766d7b
A[2]=bf36d7bd  B[2]=5aab9054  C[2]=709b2677  D[2]=9fddf819
A[3]=e0821335  B[3]=a0e1ef96  C[3]=628d9ef8  D[3]=6cfbad82
A[4]=f6ddd3c4  B[4]=be90e043  C[4]=4c3e1bd5  D[4]=8ab984d9
A[5]=0379a1a3  B[5]=2b28eb7c  C[5]=ecd6fab7  D[5]=99b03001
A[6]=caf56825  B[6]=53ae0016  C[6]=515ffe92  D[6]=a3237d0e
A[7]=6e90f932  B[7]=5707bd4f  C[7]=6f5263c2  D[7]=0f1a7670

Step 18: (r=15, s= 5)
A[0]=5e71de12  B[0]=64f7d3d3  C[0]=4e9922d4  D[0]=b73c3fe7
A[1]=13ebe4ad  B[1]=dd76cb8f  C[1]=88774c32  D[1]=b0bbbd6a
A[2]=cacb8a30  B[2]=6bdedf9b  C[2]=5aab9054  D[2]=709b2677
A[3]=71346c7c  B[3]=099af041  C[3]=a0e1ef96  D[3]=628d9ef8
A[4]=657650c2  B[4]=e9e27b6e  C[4]=be90e043  D[4]=4c3e1bd5
A[5]=2bb59b2f  B[5]=d0d181bc  C[5]=2b28eb7c  D[5]=ecd6fab7
A[6]=d62b8058  B[6]=b412e57a  C[6]=53ae0016  D[6]=515ffe92
A[7]=658ba203  B[7]=7c993748  C[7]=5707bd4f  D[7]=6f5263c2

Step 19: (r= 5, s=29)
A[0]=eb109e1e  B[0]=ce3bc24b  C[0]=64f7d3d3  D[0]=4e9922d4
A[1]=e7343a09  B[1]=7d7c95a2  C[1]=dd76cb8f  D[1]=88774c32
A[2]=d181a357  B[2]=59714619  C[2]=6bdedf9b  D[2]=5aab9054
A[3]=ed0afe83  B[3]=268d8f8e  C[3]=099af041  D[3]=a0e1ef96
A[4]=bba10eca  B[4]=aeca184c  C[4]=e9e27b6e  D[4]=be90e043
A[5]=8500a509  B[5]=76b365e5  C[5]=d0d181bc  D[5]=2b28eb7c
A[6]=26a2fb25  B[6]=c5700b1a  C[6]=b412e57a  D[6]=53ae0016
A[7]=6b6c4330  B[7]=b174406c  C[7]=7c993748  D[7]=5707bd4f

Step 20: (r=29, s= 9)
A[0]=80fa63bf  B[0]=dd6213c3  C[0]=ce3bc24b  D[0]=64f7d3d3
A[1]=5b8a333a  B[1]=3ce68741  C[1]=7d7c95a2  D[1]=dd76cb8f
A[2]=55266953  B[2]=fa30346a  C[2]=59714619  D[2]=6bdedf9b
A[3]=4dbc6985  B[3]=7da15fd0  C[3]=268d8f8e  D[3]=099af041
A[4]=5a6e36ba  B[4]=577421d9  C[4]=aeca184c  D[4]=e9e27b6e
A[5]=d2b0515d  B[5]=30a014a1  C[5]=76b365e5  D[5]=d0d181bc
A[6]=85bfd7ec  B[6]=a4d45f64  C[6]=c5700b1a  D[6]=b412e57a
A[7]=ab9d5900  B[7]=0d6d8866  C[7]=b174406c  D[7]=7c993748

Step 21: (r= 9, s=15)
A[0]=29c432c1  B[0]=f4c77f01  C[0]=dd6213c3  D[0]=ce3bc24b
A[1]=acf39a7f  B[1]=146674b7  C[1]=3ce68741  D[1]=7d7c95a2
A[2]=0e8500b4  B[2]=4cd2a6aa  C[2]=fa30346a  D[2]=59714619
A[3]=8877e996  B[3]=78d30a9b  C[3]=7da15fd0  D[3]=268d8f8e
A[4]=009e7c04  B[4]=dc6d74b4  C[4]=577421d9  D[4]=aeca184c
A[5]=664766ac  B[5]=60a2bba5  C[5]=30a014a1  D[5]=76b365e5
```

```
A[6]=844828d2  B[6]=7fafd90b  C[6]=a4d45f64  D[6]=c5700b1a
A[7]=e5c02484  B[7]=3ab20157  C[7]=0d6d8866  D[7]=b174406c

Step 22: (r=15, s= 5)
A[0]=2f9d34d6  B[0]=196094e2  C[0]=f4c77f01  D[0]=dd6213c3
A[1]=d6362ea1  B[1]=cd3fd679  C[1]=146674b7  D[1]=3ce68741
A[2]=0257e111  B[2]=805a0742  C[2]=4cd2a6aa  D[2]=fa30346a
A[3]=a077bbec  B[3]=f4cb443b  C[3]=78d30a9b  D[3]=7da15fd0
A[4]=793a3350  B[4]=3e02004f  C[4]=dc6d74b4  D[4]=577421d9
A[5]=a3c98750  B[5]=b3563323  C[5]=60a2bba5  D[5]=30a014a1
A[6]=8d6dcf28  B[6]=14694224  C[6]=7fafd90b  D[6]=a4d45f64
A[7]=b94e2e99  B[7]=124272e0  C[7]=3ab20157  D[7]=0d6d8866

Step 23: (r= 5, s=29)
A[0]=e0286dce  B[0]=f3a69ac5  C[0]=196094e2  D[0]=f4c77f01
A[1]=cfa091f1  B[1]=c6c5d43a  C[1]=cd3fd679  D[1]=146674b7
A[2]=5a5c2cfb  B[2]=4afc2220  C[2]=805a0742  D[2]=4cd2a6aa
A[3]=0810bce1  B[3]=0ef77d94  C[3]=f4cb443b  D[3]=78d30a9b
A[4]=754315d2  B[4]=27466a0f  C[4]=3e02004f  D[4]=dc6d74b4
A[5]=ed4f2bba  B[5]=7930ea14  C[5]=b3563323  D[5]=60a2bba5
A[6]=c76860ed  B[6]=adb9e511  C[6]=14694224  D[6]=7fafd90b
A[7]=0590a582  B[7]=29c5d337  C[7]=124272e0  D[7]=3ab20157

Step 24: (r= 4, s=13)
A[0]=e7c991a2  B[0]=0286dcee  C[0]=f3a69ac5  D[0]=196094e2
A[1]=dce4cffa  B[1]=fa091f1c  C[1]=c6c5d43a  D[1]=cd3fd679
A[2]=ab85e9be  B[2]=a5c2cfb5  C[2]=4afc2220  D[2]=805a0742
A[3]=5662d704  B[3]=810bce10  C[3]=0ef77d94  D[3]=f4cb443b
A[4]=1dda13e5  B[4]=54315d27  C[4]=27466a0f  D[4]=3e02004f
A[5]=7c2d7c54  B[5]=d4f2bbae  C[5]=7930ea14  D[5]=b3563323
A[6]=66cbc5e8  B[6]=76860edc  C[6]=adb9e511  D[6]=14694224
A[7]=b8ae6b48  B[7]=590a5820  C[7]=29c5d337  D[7]=124272e0

Step 25: (r=13, s=10)
A[0]=7d7f2a8e  B[0]=32345cf9  C[0]=0286dcee  D[0]=f3a69ac5
A[1]=44ee2114  B[1]=99ff5b9c  C[1]=fa091f1c  D[1]=c6c5d43a
A[2]=942a9a2e  B[2]=bd37d570  C[2]=a5c2cfb5  D[2]=4afc2220
A[3]=f5d85134  B[3]=5ae08acc  C[3]=810bce10  D[3]=0ef77d94
A[4]=76ac3c0e  B[4]=427ca3bb  C[4]=54315d27  D[4]=27466a0f
A[5]=34e2db87  B[5]=af8a8f85  C[5]=d4f2bbae  D[5]=7930ea14
A[6]=9d7efb80  B[6]=78bd0cd9  C[6]=76860edc  D[6]=adb9e511
A[7]=d7498e01  B[7]=cd691715  C[7]=590a5820  D[7]=29c5d337

Step 26: (r=10, s=25)
A[0]=34762fea  B[0]=fcaa39f5  C[0]=32345cf9  D[0]=0286dcee
A[1]=8786b19c  B[1]=b8845113  C[1]=99ff5b9c  D[1]=fa091f1c
A[2]=18b80114  B[2]=aa68ba50  C[2]=bd37d570  D[2]=a5c2cfb5
A[3]=29e9f10f  B[3]=6144d3d7  C[3]=5ae08acc  D[3]=810bce10
A[4]=cfb3be42  B[4]=b0f039da  C[4]=427ca3bb  D[4]=54315d27
```

```
A[5]=0b70b6bc  B[5]=8b6e1cd3  C[5]=af8a8f85  D[5]=d4f2bbae
A[6]=bd0f7d83  B[6]=fbee0275  C[6]=78bd0cd9  D[6]=76860edc
A[7]=88968c16  B[7]=2638075d  C[7]=cd691715  D[7]=590a5820

Step 27: (r=25, s= 4)
A[0]=b140f739  B[0]=d468ec5f  C[0]=fcaa39f5  D[0]=32345cf9
A[1]=0f488b1f  B[1]=390f0d63  C[1]=b8845113  D[1]=99ff5b9c
A[2]=e564d5d0  B[2]=28317002  C[2]=aa68ba50  D[2]=bd37d570
A[3]=ae778665  B[3]=1e53d3e2  C[3]=6144d3d7  D[3]=5ae08acc
A[4]=7c5f866e  B[4]=859f677c  C[4]=b0f039da  D[4]=427ca3bb
A[5]=ba362541  B[5]=7816e16d  C[5]=8b6e1cd3  D[5]=af8a8f85
A[6]=d9bb1b54  B[6]=077a1efb  C[6]=fbee0275  D[6]=78bd0cd9
A[7]=a46c7c1e  B[7]=2d112d18  C[7]=2638075d  D[7]=cd691715

Step 28: (r= 4, s=13)
A[0]=00fac2f0  B[0]=140f739b  C[0]=d468ec5f  D[0]=fcaa39f5
A[1]=41371166  B[1]=f488b1f0  C[1]=390f0d63  D[1]=b8845113
A[2]=49bee85b  B[2]=564d5d0e  C[2]=28317002  D[2]=aa68ba50
A[3]=0c26c695  B[3]=e778665a  C[3]=1e53d3e2  D[3]=6144d3d7
A[4]=1f100bbe  B[4]=c5f866e7  C[4]=859f677c  D[4]=b0f039da
A[5]=fd975b84  B[5]=a362541b  C[5]=7816e16d  D[5]=8b6e1cd3
A[6]=ab7743be  B[6]=9bb1b54d  C[6]=077a1efb  D[6]=fbee0275
A[7]=2dc65b20  B[7]=46c7c1ea  C[7]=2d112d18  D[7]=2638075d

Step 29: (r=13, s=10)
A[0]=68ad319c  B[0]=585e001f  C[0]=140f739b  D[0]=d468ec5f
A[1]=5264d8f9  B[1]=e22cc826  C[1]=f488b1f0  D[1]=390f0d63
A[2]=b7474c57  B[2]=dd0b6937  C[2]=564d5d0e  D[2]=28317002
A[3]=903897bf  B[3]=d8d2a184  C[3]=e778665a  D[3]=1e53d3e2
A[4]=454406a6  B[4]=0177c3e2  C[4]=c5f866e7  D[4]=859f677c
A[5]=5f2df7e2  B[5]=eb709fb2  C[5]=a362541b  D[5]=7816e16d
A[6]=553165fa  B[6]=e877d56e  C[6]=9bb1b54d  D[6]=077a1efb
A[7]=d73be54d  B[7]=cb6405b8  C[7]=46c7c1ea  D[7]=2d112d18

Step 30: (r=10, s=25)
A[0]=878fc668  B[0]=b4c671a2  C[0]=585e001f  D[0]=140f739b
A[1]=9292e07b  B[1]=9363e549  C[1]=e22cc826  D[1]=f488b1f0
A[2]=cd430f13  B[2]=1d315edd  C[2]=dd0b6937  D[2]=564d5d0e
A[3]=593fac60  B[3]=e25efe40  C[3]=d8d2a184  D[3]=e778665a
A[4]=dda634e0  B[4]=101a9915  C[4]=0177c3e2  D[4]=c5f866e7
A[5]=c4fffaf0  B[5]=b7df897c  C[5]=eb709fb2  D[5]=a362541b
A[6]=a739ef5e  B[6]=c597e954  C[6]=e877d56e  D[6]=9bb1b54d
A[7]=6a0f7a2f  B[7]=ef95375c  C[7]=cb6405b8  D[7]=46c7c1ea

Step 31: (r=25, s= 4)
A[0]=98e36bf7  B[0]=d10f1f8c  C[0]=b4c671a2  D[0]=585e001f
A[1]=92638026  B[1]=f72525c0  C[1]=9363e549  D[1]=e22cc826
A[2]=58b1ab8c  B[2]=279a861e  C[2]=1d315edd  D[2]=dd0b6937
A[3]=cf518990  B[3]=c0b27f58  C[3]=e25efe40  D[3]=d8d2a184
```

```
A[4]=b4aec711  B[4]=c1bb4c69  C[4]=101a9915  D[4]=0177c3e2
A[5]=6b00cfc7  B[5]=e189fff5  C[5]=b7df897c  D[5]=eb709fb2
A[6]=86667fb9  B[6]=bd4e73de  C[6]=c597e954  D[6]=e877d56e
A[7]=bcd651cf  B[7]=5ed41ef4  C[7]=ef95375c  D[7]=cb6405b8

Feed-Forward Step 32: (r= 4, s=13)
A[0]=3158ef49  B[0]=8e36bf79  C[0]=d10f1f8c  D[0]=b4c671a2
A[1]=884c5259  B[1]=26380269  C[1]=f72525c0  D[1]=9363e549
A[2]=c4c81378  B[2]=8b1ab8c5  C[2]=279a861e  D[2]=1d315edd
A[3]=eb63e901  B[3]=f518990c  C[3]=c0b27f58  D[3]=e25efe40
A[4]=e86b913b  B[4]=4aec711b  C[4]=c1bb4c69  D[4]=101a9915
A[5]=9ff0b282  B[5]=b00cfc76  C[5]=e189fff5  D[5]=b7df897c
A[6]=a6a90ee0  B[6]=6667fb98  C[6]=bd4e73de  D[6]=c597e954
A[7]=db4674c6  B[7]=cd651cfb  C[7]=5ed41ef4  D[7]=ef95375c

Feed-Forward Step 33: (r=13, s=10)
A[0]=ca881f08  B[0]=1de9262b  C[0]=8e36bf79  D[0]=d10f1f8c
A[1]=2e786960  B[1]=8a4b3109  C[1]=26380269  D[1]=f72525c0
A[2]=b8efc75e  B[2]=026f1899  C[2]=8b1ab8c5  D[2]=279a861e
A[3]=83af48ed  B[3]=7d203d6c  C[3]=f518990c  D[3]=c0b27f58
A[4]=2fa1456e  B[4]=72277d0d  C[4]=4aec711b  D[4]=c1bb4c69
A[5]=22e476c7  B[5]=165053fe  C[5]=b00cfc76  D[5]=e189fff5
A[6]=b7d8d637  B[6]=21dc14d5  C[6]=6667fb98  D[6]=bd4e73de
A[7]=04ce3e67  B[7]=ce98db68  C[7]=cd651cfb  D[7]=5ed41ef4

Feed-Forward Step 34: (r=10, s=25)
A[0]=60451bc9  B[0]=207c232a  C[0]=1de9262b  D[0]=8e36bf79
A[1]=78a574b8  B[1]=e1a580b9  C[1]=8a4b3109  D[1]=26380269
A[2]=44cedc69  B[2]=bf1d7ae3  C[2]=026f1899  D[2]=8b1ab8c5
A[3]=4556fada  B[3]=bd23b60e  C[3]=7d203d6c  D[3]=f518990c
A[4]=b1ba36d7  B[4]=8515b8be  C[4]=72277d0d  D[4]=4aec711b
A[5]=f9f07c2a  B[5]=91db1c8b  C[5]=165053fe  D[5]=b00cfc76
A[6]=de257715  B[6]=6358dedf  C[6]=21dc14d5  D[6]=6667fb98
A[7]=59ce566a  B[7]=38f99c13  C[7]=ce98db68  D[7]=cd651cfb

Feed-Forward Step 35: (r=25, s= 4)
A[0]=9726d3e4  B[0]=92c08a37  C[0]=207c232a  D[0]=1de9262b
A[1]=03e9e6d9  B[1]=70f14ae9  C[1]=e1a580b9  D[1]=8a4b3109
A[2]=75997b86  B[2]=d2899db8  C[2]=bf1d7ae3  D[2]=026f1899
A[3]=edc14caf  B[3]=b48aadf5  C[3]=bd23b60e  D[3]=7d203d6c
A[4]=6fc85809  B[4]=af63746d  C[4]=8515b8be  D[4]=72277d0d
A[5]=4b12cfd8  B[5]=55f3e0f8  C[5]=91db1c8b  D[5]=165053fe
A[6]=269b9228  B[6]=2bbc4aee  C[6]=6358dedf  D[6]=21dc14d5
A[7]=3105e1d6  B[7]=d4b39cac  C[7]=38f99c13  D[7]=ce98db68
```

Compression Function Output

```
A[0]=9726d3e4  B[0]=92c08a37  C[0]=207c232a  D[0]=1de9262b
A[1]=03e9e6d9  B[1]=70f14ae9  C[1]=e1a580b9  D[1]=8a4b3109
```

```
A[2]=75997b86  B[2]=d2899db8  C[2]=bf1d7ae3  D[2]=026f1899
A[3]=edc14caf  B[3]=b48aadf5  C[3]=bd23b60e  D[3]=7d203d6c
A[4]=6fc85809  B[4]=af63746d  C[4]=8515b8be  D[4]=72277d0d
A[5]=4b12cfd8  B[5]=55f3e0f8  C[5]=91db1c8b  D[5]=165053fe
A[6]=269b9228  B[6]=2bbc4aee  C[6]=6358dedf  D[6]=21dc14d5
A[7]=3105e1d6  B[7]=d4b39cac  C[7]=38f99c13  D[7]=ce98db68
```

Final block

```
M[  0..  7] = 00 04 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    6  110  198  227   45   48  240  162
y[  8.. 15] =   28  167  162   26  100  136  175   13
y[ 16.. 23] =  105   29   76  156   65  201   12  201
y[ 24.. 31] =   15   98    1   79  129  256  249   61
y[ 32.. 39] =  205   87   89  188  218  234  222   16
y[ 40.. 47] =    8   18  139  161  188  152  117  155
y[ 48.. 55] =  128  188  255   28   91  244   83  200
y[ 56.. 63] =   53   68  175   17  160   80  211  216
y[ 64.. 71] =   64  142   32   39  250  230  185  240
y[ 72.. 79] =    2  135    4   52   93  171   62   66
y[ 80.. 87] =  122  169  162   57   34  120   35  241
y[ 88.. 95] =   17  171    7   54  154  138   45  134
y[ 96..103] =  188   88  126  118  158  140    4  182
y[104..111] =  145  232   35  172  254  196   31    3
y[112..119] =  245   43   90   31   48   46   68   79
y[120..127] =  214   32   35   98  155  162   14   33
y[128..135] =  251  147   59   30  212  209   17   95
y[136..143] =  229   90   95  231  157  121   82  244
y[144..151] =  152  228  181  101  192   56  245   56
y[152..159] =  242  159  256  178  128    1    8  196
y[160..167] =   52  170  168   69   39   23   35  241
y[168..175] =  249  239  118   96   69  105  140  102
```

```
y[176..183] =  129   69    2  229  166   13  174   57
y[184..191] =  204  189   82  240   97  177   46   41
y[192..199] =  193  115  225  218    7   27   72   17
y[200..207] =  255  122  253  205  164   86  195  191
y[208..215] =  135   88   95  200  223  137  222   16
y[216..223] =  240   86  250  203  103  119  212  123
y[224..231] =   69  169  131  139   99  117  253   75
y[232..239] =  112   25  222   85    3   61  226  254
y[240..247] =   12  214  167  226  209  211  189  178
y[248..255] =   43  225  222  159  102   95  243  224
```

Intermediate Expanded Message

```
Z[ 0] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
Z[ 1] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
Z[ 2] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
Z[ 3] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
Z[ 4] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
        a7d60172  259402e4  c1da4335  2fb22cce
Z[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
Z[ 6] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
Z[ 7] = 1f13f754  1667410a  213e22b0  39173124
        1720e0ed  46d2194b  bb59b64a  17d90a1e
Z[ 8] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
        410aebc4  ed3644a7  5771b7bc  f69b3b42
Z[ 9] = eb0bb41f  48fdc914  2878d107  2878f754
        b92ef529  c6e9ff47  00b95c80  d3eb05c8
Z[10] = c1212594  31ddbfaf  109f1c2f  f470194b
        f2fefa38  45605546  4be131dd  49b6ab73
Z[11] = 31dda380  ebc40172  0965be3d  2931c405
        cedcd9b3  f3b73b42  c6304619  1da1213e
Z[12] = 531bd1c0  e3d1e8e0  1383050f  0c493408
        582afe8e  da6cfd1c  3e26bccb  d04ed332
Z[13] = 3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
        3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
Z[14] = c06831dd  aabaa4f2  548d478b  3633fd1c
        121150f0  3d6de6b5  2c15022b  fdd5e999
Z[15] = e0ed08ac  e999bef6  dec2dd50  c6e9cedc
        e8e01f13  b92ee6b5  44a749b6  e827f5e2
Z[16] = fa8a0576  35b3ca4d  d70b28f5  0f79f087
        e684197c  5677a989  a4fc5b04  4aa2b55e
Z[17] = a06f5f91  bad4452c  c4d73b29  f5140aec
        f2590da7  ff1700e9  74808b80  0748f8b8
```

```
Z[18] = 2f54d0ac  aeff5101  237fdc81  1fdbe025
        f8b80748  6b66949a  3ecdc133  95836a7d
Z[19] = 8b807480  01d2fe2e  ad2d52d3  b4754b8b
        cfc3303d  4aa2b55e  5849a7b7  29ded622
Z[20] = c5c03a40  e2e01d20  065ff9a1  4188be78
        fe2e01d2  fc5c03a4  ab5b54a5  c792386e
Z[21] = 90f66f0a  5677a989  e10e1ef2  e0251fdb
        f0870f79  f9a1065f  5dbfa241  d70b28f5
Z[22] = 3ecdc133  8d5272ae  5a1ba5e5  fc5c03a4
        65f09a10  e0251fdb  02bbfd45  e3c91c37
Z[23] = 0aecf514  ae1651ea  d4502bb0  c21c3de4
        2723d8dd  e0251fdb  5cd6a32a  f3420cbe
Z[24] = 9be2641e  1b4ee4b2  d4502bb0  5677a989
        51eaae16  e85617aa  6e2191df  f42b0bd5
Z[25] = e59b1a65  5beda413  32f8cd08  32f8cd08
        a6ce5932  b81947e7  00e9ff17  c87b3785
Z[26] = b0d14f2f  3ecdc133  14efeb11  f1700e90
        ef9e1062  5760a8a0  5f91a06f  5cd6a32a
Z[27] = 3ecdc133  e684197c  0bd5f42b  33e1cc1f
        c21c3de4  f0870f79  b73048d0  2551daaf
Z[28] = 68ab9755  dc81237f  1893e76d  0f79f087
        6f0a90f6  d0ac2f54  4e46b1ba  c3ee3c12
Z[29] = 5018afe8  cc1f33e1  92c86d38  0e90f170
        4e46b1ba  ceda3126  6c4f93b1  6ff3900d
Z[30] = afe85018  949a6b66  6a7d9583  4443bbbd
        16c1e93f  4d5db2a3  3785c87b  fd4502bb
Z[31] = d8dd2723  e3c91c37  d62229de  b81947e7
        e2e01d20  a6ce5932  5677a989  e1f71e09
```

Expanded Message

```
W[ 0] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
        a7d60172  259402e4  c1da4335  2fb22cce
W[ 1] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
W[ 2] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
W[ 3] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
W[ 4] = 1f13f754  1667410a  213e22b0  39173124
        1720e0ed  46d2194b  bb59b64a  17d90a1e
W[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
W[ 6] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
W[ 7] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
W[ 8] = e0ed08ac  e999bef6  dec2dd50  c6e9cedc
        e8e01f13  b92ee6b5  44a749b6  e827f5e2
```

```
W[ 9] = 31dda380  ebc40172  0965be3d  2931c405
        cedcd9b3  f3b73b42  c6304619  1da1213e
W[10] = 531bd1c0  e3d1e8e0  1383050f  0c493408
        582afe8e  da6cfd1c  3e26bccb  d04ed332
W[11] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
        410aebc4  ed3644a7  5771b7bc  f69b3b42
W[12] = eb0bb41f  48fdc914  2878d107  2878f754
        b92ef529  c6e9ff47  00b95c80  d3eb05c8
W[13] = 3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
        3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
W[14] = c1212594  31ddbfaf  109f1c2f  f470194b
        f2fefa38  45605546  4be131dd  49b6ab73
W[15] = c06831dd  aabaa4f2  548d478b  3633fd1c
        121150f0  3d6de6b5  2c15022b  fdd5e999
W[16] = a06f5f91  bad4452c  c4d73b29  f5140aec
        f2590da7  ff1700e9  74808b80  0748f8b8
W[17] = 2f54d0ac  aeff5101  237fdc81  1fdbe025
        f8b80748  6b66949a  3ecdc133  95836a7d
W[18] = 0aecf514  ae1651ea  d4502bb0  c21c3de4
        2723d8dd  e0251fdb  5cd6a32a  f3420cbe
W[19] = c5c03a40  e2e01d20  065ff9a1  4188be78
        fe2e01d2  fc5c03a4  ab5b54a5  c792386e
W[20] = 3ecdc133  8d5272ae  5a1ba5e5  fc5c03a4
        65f09a10  e0251fdb  02bbfd45  e3c91c37
W[21] = 90f66f0a  5677a989  e10e1ef2  e0251fdb
        f0870f79  f9a1065f  5dbfa241  d70b28f5
W[22] = fa8a0576  35b3ca4d  d70b28f5  0f79f087
        e684197c  5677a989  a4fc5b04  4aa2b55e
W[23] = 8b807480  01d2fe2e  ad2d52d3  b4754b8b
        cfc3303d  4aa2b55e  5849a7b7  29ded622
W[24] = afe85018  949a6b66  6a7d9583  4443bbbd
        16c1e93f  4d5db2a3  3785c87b  fd4502bb
W[25] = 9be2641e  1b4ee4b2  d4502bb0  5677a989
        51eaae16  e85617aa  6e2191df  f42b0bd5
W[26] = e59b1a65  5beda413  32f8cd08  32f8cd08
        a6ce5932  b81947e7  00e9ff17  c87b3785
W[27] = d8dd2723  e3c91c37  d62229de  b81947e7
        e2e01d20  a6ce5932  5677a989  e1f71e09
W[28] = 3ecdc133  e684197c  0bd5f42b  33e1cc1f
        c21c3de4  f0870f79  b73048d0  2551daaf
W[29] = 5018afe8  cc1f33e1  92c86d38  0e90f170
        4e46b1ba  ceda3126  6c4f93b1  6ff3900d
W[30] = 68ab9755  dc81237f  1893e76d  0f79f087
        6f0a90f6  d0ac2f54  4e46b1ba  c3ee3c12
W[31] = b0d14f2f  3ecdc133  14efeb11  f1700e90
        ef9e1062  5760a8a0  5f91a06f  5cd6a32a
```

Feistel Steps

```
IV :
```

```
A[0]=9726d3e4  B[0]=92c08a37  C[0]=207c232a  D[0]=1de9262b
A[1]=03e9e6d9  B[1]=70f14ae9  C[1]=e1a580b9  D[1]=8a4b3109
A[2]=75997b86  B[2]=d2899db8  C[2]=bf1d7ae3  D[2]=026f1899
A[3]=edc14caf  B[3]=b48aadf5  C[3]=bd23b60e  D[3]=7d203d6c
A[4]=6fc85809  B[4]=af63746d  C[4]=8515b8be  D[4]=72277d0d
A[5]=4b12cfd8  B[5]=55f3e0f8  C[5]=91db1c8b  D[5]=165053fe
A[6]=269b9228  B[6]=2bbc4aee  C[6]=6358dedf  D[6]=21dc14d5
A[7]=3105e1d6  B[7]=d4b39cac  C[7]=38f99c13  D[7]=ce98db68

IV XOR M :
A[0]=9726d7e4  B[0]=92c08a37  C[0]=207c232a  D[0]=1de9262b
A[1]=03e9e6d9  B[1]=70f14ae9  C[1]=e1a580b9  D[1]=8a4b3109
A[2]=75997b86  B[2]=d2899db8  C[2]=bf1d7ae3  D[2]=026f1899
A[3]=edc14caf  B[3]=b48aadf5  C[3]=bd23b60e  D[3]=7d203d6c
A[4]=6fc85809  B[4]=af63746d  C[4]=8515b8be  D[4]=72277d0d
A[5]=4b12cfd8  B[5]=55f3e0f8  C[5]=91db1c8b  D[5]=165053fe
A[6]=269b9228  B[6]=2bbc4aee  C[6]=6358dedf  D[6]=21dc14d5
A[7]=3105e1d6  B[7]=d4b39cac  C[7]=38f99c13  D[7]=ce98db68

Step  0: (r= 3, s=23)
A[0]=6c0dca43  B[0]=b936bf24  C[0]=92c08a37  D[0]=207c232a
A[1]=427a6ee9  B[1]=1f4f36c8  C[1]=70f14ae9  D[1]=e1a580b9
A[2]=23ef2295  B[2]=accbdc33  C[2]=d2899db8  D[2]=bf1d7ae3
A[3]=b15e9997  B[3]=6e0a657f  C[3]=b48aadf5  D[3]=bd23b60e
A[4]=f7fb2879  B[4]=7e42c04b  C[4]=af63746d  D[4]=8515b8be
A[5]=5cc9a05e  B[5]=58967ec2  C[5]=55f3e0f8  D[5]=91db1c8b
A[6]=0cd2d604  B[6]=34dc9141  C[6]=2bbc4aee  D[6]=6358dedf
A[7]=92683393  B[7]=882f0eb1  C[7]=d4b39cac  D[7]=38f99c13

Step  1: (r=23, s=17)
A[0]=f9089f1d  B[0]=21b606e5  C[0]=b936bf24  D[0]=92c08a37
A[1]=cee80787  B[1]=74a13d37  C[1]=1f4f36c8  D[1]=70f14ae9
A[2]=de1eb44d  B[2]=4a91f791  C[2]=accbdc33  D[2]=d2899db8
A[3]=ec01bbc5  B[3]=cbd8af4c  C[3]=6e0a657f  D[3]=b48aadf5
A[4]=c2c9da20  B[4]=3cfbfd94  C[4]=7e42c04b  D[4]=af63746d
A[5]=f94a0b8d  B[5]=2f2e64d0  C[5]=58967ec2  D[5]=55f3e0f8
A[6]=0cf2c567  B[6]=0206696b  C[6]=34dc9141  D[6]=2bbc4aee
A[7]=f7113cf7  B[7]=c9c93419  C[7]=882f0eb1  D[7]=d4b39cac

Step  2: (r=17, s=27)
A[0]=f8b761e2  B[0]=3e3bf211  C[0]=21b606e5  D[0]=b936bf24
A[1]=251332af  B[1]=0f0f9dd0  C[1]=74a13d37  D[1]=1f4f36c8
A[2]=c13c4fe4  B[2]=689bbc3d  C[2]=4a91f791  D[2]=accbdc33
A[3]=60df1a59  B[3]=778bd803  C[3]=cbd8af4c  D[3]=6e0a657f
A[4]=302744ec  B[4]=b4418593  C[4]=3cfbfd94  D[4]=7e42c04b
A[5]=1682d6aa  B[5]=171bf294  C[5]=2f2e64d0  D[5]=58967ec2
A[6]=5c6454b7  B[6]=8ace19e5  C[6]=0206696b  D[6]=34dc9141
A[7]=f456374f  B[7]=79efee22  C[7]=c9c93419  D[7]=882f0eb1
```

```
Step  3: (r=27, s= 3)
A[0]=5556f57b  B[0]=17c5bb0f  C[0]=3e3bf211  D[0]=21b606e5
A[1]=3eb687c9  B[1]=79289995  C[1]=0f0f9dd0  D[1]=74a13d37
A[2]=af647b64  B[2]=2609e27f  C[2]=689bbc3d  D[2]=4a91f791
A[3]=40fe04da  B[3]=cb06f8d2  C[3]=778bd803  D[3]=cbd8af4c
A[4]=c096ced8  B[4]=61813a27  C[4]=b4418593  D[4]=3cfbfd94
A[5]=4e140507  B[5]=50b416b5  C[5]=171bf294  D[5]=2f2e64d0
A[6]=eac8e144  B[6]=bae322a5  C[6]=8ace19e5  D[6]=0206696b
A[7]=23c584ac  B[7]=7fa2b1ba  C[7]=79efee22  D[7]=c9c93419

Step  4: (r= 3, s=23)
A[0]=1acc3932  B[0]=aab7abda  C[0]=17c5bb0f  D[0]=3e3bf211
A[1]=0e1b9254  B[1]=f5b43e49  C[1]=79289995  D[1]=0f0f9dd0
A[2]=7d79126b  B[2]=7b23db25  C[2]=2609e27f  D[2]=689bbc3d
A[3]=f76b4983  B[3]=07f026d2  C[3]=cb06f8d2  D[3]=778bd803
A[4]=7fce8d7f  B[4]=04b676c6  C[4]=61813a27  D[4]=b4418593
A[5]=031db624  B[5]=70a0283a  C[5]=50b416b5  D[5]=171bf294
A[6]=d5243bf2  B[6]=56470a27  C[6]=bae322a5  D[6]=8ace19e5
A[7]=ebd2a016  B[7]=1e2c2561  C[7]=7fa2b1ba  D[7]=79efee22

Step  5: (r=23, s=17)
A[0]=16201c24  B[0]=990d661c  C[0]=aab7abda  D[0]=17c5bb0f
A[1]=e067fd10  B[1]=2a070dc9  C[1]=f5b43e49  D[1]=79289995
A[2]=607e0bd6  B[2]=35bebc89  C[2]=7b23db25  D[2]=2609e27f
A[3]=74004e02  B[3]=c1fbb5a4  C[3]=07f026d2  D[3]=cb06f8d2
A[4]=62836ce7  B[4]=bfbfe746  C[4]=04b676c6  D[4]=61813a27
A[5]=916dda35  B[5]=12018edb  C[5]=70a0283a  D[5]=50b416b5
A[6]=1e412436  B[6]=f96a921d  C[6]=56470a27  D[6]=bae322a5
A[7]=f8c0a77b  B[7]=0b75e950  C[7]=1e2c2561  D[7]=7fa2b1ba

Step  6: (r=17, s=27)
A[0]=35cf3733  B[0]=38482c40  C[0]=990d661c  D[0]=aab7abda
A[1]=17d78986  B[1]=fa21c0cf  C[1]=2a070dc9  D[1]=f5b43e49
A[2]=84db5a80  B[2]=17acc0fc  C[2]=35bebc89  D[2]=7b23db25
A[3]=ce36245b  B[3]=9c04e800  C[3]=c1fbb5a4  D[3]=07f026d2
A[4]=0e131279  B[4]=d9cec506  C[4]=bfbfe746  D[4]=04b676c6
A[5]=6d8abbfc  B[5]=b46b22db  C[5]=12018edb  D[5]=70a0283a
A[6]=324477f2  B[6]=486c3c82  C[6]=f96a921d  D[6]=56470a27
A[7]=07e821af  B[7]=4ef7f181  C[7]=0b75e950  D[7]=1e2c2561

Step  7: (r=27, s= 3)
A[0]=f88faaab  B[0]=99ae79b9  C[0]=38482c40  D[0]=990d661c
A[1]=cfa671e0  B[1]=30bebc4c  C[1]=fa21c0cf  D[1]=2a070dc9
A[2]=21c8c655  B[2]=0426dad4  C[2]=17acc0fc  D[2]=35bebc89
A[3]=619d76c9  B[3]=de71b122  C[3]=9c04e800  D[3]=c1fbb5a4
A[4]=3cae9cfe  B[4]=c8709893  C[4]=d9cec506  D[4]=bfbfe746
A[5]=b6873709  B[5]=e36c55df  C[5]=b46b22db  D[5]=12018edb
A[6]=e81662db  B[6]=919223bf  C[6]=486c3c82  D[6]=f96a921d
A[7]=63522c91  B[7]=783f410d  C[7]=4ef7f181  D[7]=0b75e950
```

```
Step  8: (r=28, s=19)
A[0]=9c09fc71  B[0]=bf88faaa  C[0]=99ae79b9  D[0]=38482c40
A[1]=fea7450c  B[1]=0cfa671e  C[1]=30bebc4c  D[1]=fa21c0cf
A[2]=ca743f01  B[2]=521c8c65  C[2]=0426dad4  D[2]=17acc0fc
A[3]=7f6b9b29  B[3]=9619d76c  C[3]=de71b122  D[3]=9c04e800
A[4]=51781c6b  B[4]=e3cae9cf  C[4]=c8709893  D[4]=d9cec506
A[5]=f1754450  B[5]=9b687370  C[5]=e36c55df  D[5]=b46b22db
A[6]=92feef0a  B[6]=be81662d  C[6]=919223bf  D[6]=486c3c82
A[7]=8e9569cb  B[7]=163522c9  C[7]=783f410d  D[7]=4ef7f181

Step  9: (r=19, s=22)
A[0]=521048d3  B[0]=e38ce04f  C[0]=bf88faaa  D[0]=99ae79b9
A[1]=bcc8a38b  B[1]=2867f53a  C[1]=0cfa671e  D[1]=30bebc4c
A[2]=e726aaa2  B[2]=f80e53a1  C[2]=521c8c65  D[2]=0426dad4
A[3]=f43ec951  B[3]=d94bfb5c  C[3]=9619d76c  D[3]=de71b122
A[4]=5d711500  B[4]=e35a8bc0  C[4]=e3cae9cf  D[4]=c8709893
A[5]=4d6b5756  B[5]=22878baa  C[5]=9b687370  D[5]=e36c55df
A[6]=398312fa  B[6]=785497f7  C[6]=be81662d  D[6]=919223bf
A[7]=05c041b6  B[7]=4e5c74ab  C[7]=163522c9  D[7]=783f410d

Step 10: (r=22, s= 7)
A[0]=7e1c0220  B[0]=34d48412  C[0]=e38ce04f  D[0]=bf88faaa
A[1]=2a7eeec8  B[1]=e2ef3228  C[1]=2867f53a  D[1]=0cfa671e
A[2]=c6e2962b  B[2]=a8b9c9aa  C[2]=f80e53a1  D[2]=521c8c65
A[3]=9836d770  B[3]=547d0fb2  C[3]=d94bfb5c  D[3]=9619d76c
A[4]=a8c1e812  B[4]=40175c45  C[4]=e35a8bc0  D[4]=e3cae9cf
A[5]=acc96f6b  B[5]=d5935ad5  C[5]=22878baa  D[5]=9b687370
A[6]=b23f1b9b  B[6]=be8e60c4  C[6]=785497f7  D[6]=be81662d
A[7]=c1d2f174  B[7]=6d817010  C[7]=4e5c74ab  D[7]=163522c9

Step 11: (r= 7, s=28)
A[0]=9711c340  B[0]=0e01103f  C[0]=34d48412  D[0]=e38ce04f
A[1]=154585a3  B[1]=3f776415  C[1]=e2ef3228  D[1]=2867f53a
A[2]=97fa5d38  B[2]=714b15e3  C[2]=a8b9c9aa  D[2]=f80e53a1
A[3]=3251af08  B[3]=1b6bb84c  C[3]=547d0fb2  D[3]=d94bfb5c
A[4]=75f6762a  B[4]=60f40954  C[4]=40175c45  D[4]=e35a8bc0
A[5]=8ef3786c  B[5]=64b7b5d6  C[5]=d5935ad5  D[5]=22878baa
A[6]=ec6fd278  B[6]=1f8dcdd9  C[6]=be8e60c4  D[6]=785497f7
A[7]=d710e30d  B[7]=e978ba60  C[7]=6d817010  D[7]=4e5c74ab

Step 12: (r=28, s=19)
A[0]=81783380  B[0]=09711c34  C[0]=0e01103f  D[0]=34d48412
A[1]=a244438e  B[1]=3154585a  C[1]=3f776415  D[1]=e2ef3228
A[2]=db85cb9a  B[2]=897fa5d3  C[2]=714b15e3  D[2]=a8b9c9aa
A[3]=b5200957  B[3]=83251af0  C[3]=1b6bb84c  D[3]=547d0fb2
A[4]=6c9506ee  B[4]=a75f6762  C[4]=60f40954  D[4]=40175c45
A[5]=a7ad16fb  B[5]=c8ef3786  C[5]=64b7b5d6  D[5]=d5935ad5
A[6]=dbce1547  B[6]=8ec6fd27  C[6]=1f8dcdd9  D[6]=be8e60c4
```

```
A[7]=6d0996f7  B[7]=dd710e30  C[7]=e978ba60  D[7]=6d817010

Step 13: (r=19, s=22)
A[0]=3e92dc37  B[0]=9c040bc1  C[0]=09711c34  D[0]=0e01103f
A[1]=73588215  B[1]=1c751222  C[1]=3154585a  D[1]=3f776415
A[2]=6509b2fd  B[2]=5cd6dc2e  C[2]=897fa5d3  D[2]=714b15e3
A[3]=66b8340f  B[3]=4abda900  C[3]=83251af0  D[3]=1b6bb84c
A[4]=74bcd096  B[4]=377364a8  C[4]=a75f6762  D[4]=60f40954
A[5]=8399e185  B[5]=b7dd3d68  C[5]=c8ef3786  D[5]=64b7b5d6
A[6]=7b83f350  B[6]=aa3ede70  C[6]=8ec6fd27  D[6]=1f8dcdd9
A[7]=c9aaa0bb  B[7]=b7bb684c  C[7]=dd710e30  D[7]=e978ba60

Step 14: (r=22, s= 7)
A[0]=1e85da95  B[0]=0dcfa4b7  C[0]=9c040bc1  D[0]=09711c34
A[1]=626a9008  B[1]=855cd620  C[1]=1c751222  D[1]=3154585a
A[2]=a8cd36f4  B[2]=bf59426c  C[2]=5cd6dc2e  D[2]=897fa5d3
A[3]=0bde0e15  B[3]=03d9ae0d  C[3]=4abda900  D[3]=83251af0
A[4]=1a94fdbd  B[4]=259d2f34  C[4]=377364a8  D[4]=a75f6762
A[5]=203d7f4a  B[5]=6160e678  C[5]=b7dd3d68  D[5]=c8ef3786
A[6]=29f1fdb2  B[6]=d41ee0fc  C[6]=aa3ede70  D[6]=8ec6fd27
A[7]=4965e684  B[7]=2ef26aa8  C[7]=b7bb684c  D[7]=dd710e30

Step 15: (r= 7, s=28)
A[0]=6764c69e  B[0]=42ed4a8f  C[0]=0dcfa4b7  D[0]=9c040bc1
A[1]=80fbfb1a  B[1]=35480431  C[1]=855cd620  D[1]=1c751222
A[2]=f42d82c9  B[2]=669b7a54  C[2]=bf59426c  D[2]=5cd6dc2e
A[3]=3b131171  B[3]=ef070a85  C[3]=03d9ae0d  D[3]=4abda900
A[4]=55abdcb4  B[4]=4a7ede8d  C[4]=259d2f34  D[4]=377364a8
A[5]=2184b45f  B[5]=1ebfa510  C[5]=6160e678  D[5]=b7dd3d68
A[6]=691efa53  B[6]=f8fed914  C[6]=d41ee0fc  D[6]=aa3ede70
A[7]=85fbaa56  B[7]=b2f34224  C[7]=2ef26aa8  D[7]=b7bb684c

Step 16: (r=29, s= 9)
A[0]=0421b367  B[0]=ccec98d3  C[0]=42ed4a8f  D[0]=0dcfa4b7
A[1]=52195fe7  B[1]=501f7f63  C[1]=35480431  D[1]=855cd620
A[2]=dba00ff5  B[2]=3e85b059  C[2]=669b7a54  D[2]=bf59426c
A[3]=8ae3723a  B[3]=2762622e  C[3]=ef070a85  D[3]=03d9ae0d
A[4]=8407865e  B[4]=8ab57b96  C[4]=4a7ede8d  D[4]=259d2f34
A[5]=83087939  B[5]=e430968b  C[5]=1ebfa510  D[5]=6160e678
A[6]=473ad3cb  B[6]=6d23df4a  C[6]=f8fed914  D[6]=d41ee0fc
A[7]=d377f75e  B[7]=d0bf754a  C[7]=b2f34224  D[7]=2ef26aa8

Step 17: (r= 9, s=15)
A[0]=6dfbb71d  B[0]=4366ce08  C[0]=ccec98d3  D[0]=42ed4a8f
A[1]=036a4091  B[1]=32bfcea4  C[1]=501f7f63  D[1]=35480431
A[2]=7a5edf5e  B[2]=401febb7  C[2]=3e85b059  D[2]=669b7a54
A[3]=3fd79395  B[3]=c6e47515  C[3]=2762622e  D[3]=ef070a85
A[4]=3878b20f  B[4]=0f0cbd08  C[4]=8ab57b96  D[4]=4a7ede8d
A[5]=fd354b4d  B[5]=10f27306  C[5]=e430968b  D[5]=1ebfa510
```

```
A[6]=cfb8fb6f  B[6]=75a7968e  C[6]=6d23df4a  D[6]=f8fed914
A[7]=b454979e  B[7]=efeebda6  C[7]=d0bf754a  D[7]=b2f34224

Step 18: (r=15, s= 5)
A[0]=8dc0cc3b  B[0]=db8eb6fd  C[0]=4366ce08  D[0]=ccec98d3
A[1]=0cc25be2  B[1]=204881b5  C[1]=32bfcea4  D[1]=501f7f63
A[2]=3d417d99  B[2]=6faf3d2f  C[2]=401febb7  D[2]=3e85b059
A[3]=7eaf1cf3  B[3]=c9ca9feb  C[3]=c6e47515  D[3]=2762622e
A[4]=a65ea214  B[4]=59079c3c  C[4]=0f0cbd08  D[4]=8ab57b96
A[5]=be42451e  B[5]=a5a6fe9a  C[5]=10f27306  D[5]=e430968b
A[6]=38ece982  B[6]=7db7e7dc  C[6]=75a7968e  D[6]=6d23df4a
A[7]=d457d240  B[7]=4bcf5a2a  C[7]=efeebda6  D[7]=d0bf754a

Step 19: (r= 5, s=29)
A[0]=16c4b343  B[0]=b8198771  C[0]=db8eb6fd  D[0]=4366ce08
A[1]=0a4cd48b  B[1]=984b7c41  C[1]=204881b5  D[1]=32bfcea4
A[2]=fe8950fc  B[2]=a82fb327  C[2]=6faf3d2f  D[2]=401febb7
A[3]=720af665  B[3]=d5e39e6f  C[3]=c9ca9feb  D[3]=c6e47515
A[4]=6820e1bf  B[4]=cbd44294  C[4]=59079c3c  D[4]=0f0cbd08
A[5]=d8d79530  B[5]=c848a3d7  C[5]=a5a6fe9a  D[5]=10f27306
A[6]=0b1061b0  B[6]=1d9d3047  C[6]=7db7e7dc  D[6]=75a7968e
A[7]=78a1ad1c  B[7]=8afa481a  C[7]=4bcf5a2a  D[7]=efeebda6

Step 20: (r=29, s= 9)
A[0]=6f917470  B[0]=62d89668  C[0]=b8198771  D[0]=db8eb6fd
A[1]=d1469a36  B[1]=61499a91  C[1]=984b7c41  D[1]=204881b5
A[2]=d6e7a347  B[2]=9fd12a1f  C[2]=a82fb327  D[2]=6faf3d2f
A[3]=a54286cd  B[3]=ae415ecc  C[3]=d5e39e6f  D[3]=c9ca9feb
A[4]=67083fe4  B[4]=ed041c37  C[4]=cbd44294  D[4]=59079c3c
A[5]=1dde8204  B[5]=1b1af2a6  C[5]=c848a3d7  D[5]=a5a6fe9a
A[6]=91bc794a  B[6]=01620c36  C[6]=1d9d3047  D[6]=7db7e7dc
A[7]=f4854d09  B[7]=8f1435a3  C[7]=8afa481a  D[7]=4bcf5a2a

Step 21: (r= 9, s=15)
A[0]=eb705931  B[0]=22e8e0df  C[0]=62d89668  D[0]=b8198771
A[1]=059084e4  B[1]=8d346da2  C[1]=61499a91  D[1]=984b7c41
A[2]=04a2131c  B[2]=cf468fad  C[2]=9fd12a1f  D[2]=a82fb327
A[3]=7e903746  B[3]=850d9b4a  C[3]=ae415ecc  D[3]=d5e39e6f
A[4]=2238a484  B[4]=107fc8ce  C[4]=ed041c37  D[4]=cbd44294
A[5]=643fa51f  B[5]=bd04083b  C[5]=1b1af2a6  D[5]=c848a3d7
A[6]=ebcc0a82  B[6]=78f29523  C[6]=01620c36  D[6]=1d9d3047
A[7]=e107edda  B[7]=0a9a13e9  C[7]=8f1435a3  D[7]=8afa481a

Step 22: (r=15, s= 5)
A[0]=b8cd21e8  B[0]=2c98f5b8  C[0]=22e8e0df  D[0]=62d89668
A[1]=58e7d65d  B[1]=427202c8  C[1]=8d346da2  D[1]=61499a91
A[2]=31def83d  B[2]=098e0251  C[2]=cf468fad  D[2]=9fd12a1f
A[3]=3e657ab1  B[3]=1ba33f48  C[3]=850d9b4a  D[3]=ae415ecc
A[4]=5c2b152b  B[4]=5242111c  C[4]=107fc8ce  D[4]=ed041c37
```

```
A[5]=9780f333  B[5]=d28fb21f  C[5]=bd04083b  D[5]=1b1af2a6
A[6]=bc0be35d  B[6]=054175e6  C[6]=78f29523  D[6]=01620c36
A[7]=58d86f34  B[7]=f6ed7083  C[7]=0a9a13e9  D[7]=8f1435a3

Step 23: (r= 5, s=29)
A[0]=3ec34542  B[0]=19a43d17  C[0]=2c98f5b8  D[0]=22e8e0df
A[1]=c221b217  B[1]=1cfacbab  C[1]=427202c8  D[1]=8d346da2
A[2]=047dddfc  B[2]=3bdf07a6  C[2]=098e0251  D[2]=cf468fad
A[3]=0d36485e  B[3]=ccaf5627  C[3]=1ba33f48  D[3]=850d9b4a
A[4]=c322b767  B[4]=8562a56b  C[4]=5242111c  D[4]=107fc8ce
A[5]=1ab631d2  B[5]=f01e6672  C[5]=d28fb21f  D[5]=bd04083b
A[6]=18209a95  B[6]=817c6bb7  C[6]=054175e6  D[6]=78f29523
A[7]=b297d65e  B[7]=1b0de68b  C[7]=f6ed7083  D[7]=0a9a13e9

Step 24: (r= 4, s=13)
A[0]=103ac34d  B[0]=ec345423  C[0]=19a43d17  D[0]=2c98f5b8
A[1]=73584408  B[1]=221b217c  C[1]=1cfacbab  D[1]=427202c8
A[2]=87b5c9f0  B[2]=47dddfc0  C[2]=3bdf07a6  D[2]=098e0251
A[3]=05f61122  B[3]=d36485e0  C[3]=ccaf5627  D[3]=1ba33f48
A[4]=b46e7cff  B[4]=322b767c  C[4]=8562a56b  D[4]=5242111c
A[5]=adb164a1  B[5]=ab631d21  C[5]=f01e6672  D[5]=d28fb21f
A[6]=e515d3dc  B[6]=8209a951  C[6]=817c6bb7  D[6]=054175e6
A[7]=d1d16245  B[7]=297d65eb  C[7]=1b0de68b  D[7]=f6ed7083

Step 25: (r=13, s=10)
A[0]=ebebdcfe  B[0]=5869a207  C[0]=ec345423  D[0]=19a43d17
A[1]=bd6c8cbe  B[1]=08810e6b  C[1]=221b217c  D[1]=1cfacbab
A[2]=243fd6b0  B[2]=b93e10f6  C[2]=47dddfc0  D[2]=3bdf07a6
A[3]=db3b7590  B[3]=c22440be  C[3]=d36485e0  D[3]=ccaf5627
A[4]=6753c9c0  B[4]=cf9ff68d  C[4]=322b767c  D[4]=8562a56b
A[5]=abaa94d7  B[5]=2c9435b6  C[5]=ab631d21  D[5]=f01e6672
A[6]=f4e9248d  B[6]=ba7b9ca2  C[6]=8209a951  D[6]=817c6bb7
A[7]=92c2a0cf  B[7]=2c48ba3a  C[7]=297d65eb  D[7]=1b0de68b

Step 26: (r=10, s=25)
A[0]=111ab7fa  B[0]=af73fbaf  C[0]=5869a207  D[0]=ec345423
A[1]=f5982f0d  B[1]=b232faf5  C[1]=08810e6b  D[1]=221b217c
A[2]=e7f90a8b  B[2]=ff5ac090  C[2]=b93e10f6  D[2]=47dddfc0
A[3]=8eab1b65  B[3]=edd6436c  C[3]=c22440be  D[3]=d36485e0
A[4]=a0dd1d56  B[4]=4f27019d  C[4]=cf9ff68d  D[4]=322b767c
A[5]=1efcb228  B[5]=aa535eae  C[5]=2c9435b6  D[5]=ab631d21
A[6]=ee9c9ae6  B[6]=a49237d3  C[6]=ba7b9ca2  D[6]=8209a951
A[7]=238e09b5  B[7]=0a833e4b  C[7]=2c48ba3a  D[7]=297d65eb

Step 27: (r=25, s= 4)
A[0]=9594a98a  B[0]=f422356f  C[0]=af73fbaf  D[0]=5869a207
A[1]=2f947b0f  B[1]=1beb305e  C[1]=b232faf5  D[1]=08810e6b
A[2]=a3bee256  B[2]=17cff215  C[2]=ff5ac090  D[2]=b93e10f6
A[3]=ea883868  B[3]=cb1d5636  C[3]=edd6436c  D[3]=c22440be
```

```
A[4]=3559a905  B[4]=ad41ba3a  C[4]=4f27019d  D[4]=cf9ff68d
A[5]=e4041175  B[5]=503df964  C[5]=aa535eae  D[5]=2c9435b6
A[6]=ef168bdd  B[6]=cddd3935  C[6]=a49237d3  D[6]=ba7b9ca2
A[7]=6e913627  B[7]=6a471c13  C[7]=0a833e4b  D[7]=2c48ba3a

Step 28: (r= 4, s=13)
A[0]=3ce4da7f  B[0]=594a98a9  C[0]=f422356f  D[0]=af73fbaf
A[1]=4d935dff  B[1]=f947b0f2  C[1]=1beb305e  D[1]=b232faf5
A[2]=056a362c  B[2]=3bee256a  C[2]=17cff215  D[2]=ff5ac090
A[3]=87d7619e  B[3]=a883868e  C[3]=cb1d5636  D[3]=edd6436c
A[4]=fbf2ef3d  B[4]=559a9053  C[4]=ad41ba3a  D[4]=4f27019d
A[5]=696d0ff9  B[5]=4041175e  C[5]=503df964  D[5]=aa535eae
A[6]=2d3c4e5e  B[6]=f168bdde  C[6]=cddd3935  D[6]=a49237d3
A[7]=abc65561  B[7]=e9136276  C[7]=6a471c13  D[7]=0a833e4b

Step 29: (r=13, s=10)
A[0]=46dbdf96  B[0]=9b4fe79c  C[0]=594a98a9  D[0]=f422356f
A[1]=202b88d8  B[1]=6bbfe9b2  C[1]=f947b0f2  D[1]=1beb305e
A[2]=a3779226  B[2]=46c580ad  C[2]=3bee256a  D[2]=17cff215
A[3]=9bed174c  B[3]=ec33d0fa  C[3]=a883868e  D[3]=cb1d5636
A[4]=487bcb1a  B[4]=5de7bf7e  C[4]=559a9053  D[4]=ad41ba3a
A[5]=56f113e0  B[5]=a1ff2d2d  C[5]=4041175e  D[5]=503df964
A[6]=13737395  B[6]=89cbc5a7  C[6]=f168bdde  D[6]=cddd3935
A[7]=644b1748  B[7]=caac3578  C[7]=e9136276  D[7]=6a471c13

Step 30: (r=10, s=25)
A[0]=9fb8cde5  B[0]=6f7e591b  C[0]=9b4fe79c  D[0]=594a98a9
A[1]=53206a68  B[1]=ae236080  C[1]=6bbfe9b2  D[1]=f947b0f2
A[2]=d026efce  B[2]=de489a8d  C[2]=46c580ad  D[2]=3bee256a
A[3]=c529d63b  B[3]=b45d326f  C[3]=ec33d0fa  D[3]=a883868e
A[4]=e2c2e41a  B[4]=ef2c6921  C[4]=5de7bf7e  D[4]=559a9053
A[5]=7520d811  B[5]=c44f815b  C[5]=a1ff2d2d  D[5]=4041175e
A[6]=fc8788e2  B[6]=cdce544d  C[6]=89cbc5a7  D[6]=f168bdde
A[7]=fe7c027a  B[7]=2c5d2191  C[7]=caac3578  D[7]=e9136276

Step 31: (r=25, s= 4)
A[0]=1135ab06  B[0]=cb3f719b  C[0]=6f7e591b  D[0]=9b4fe79c
A[1]=d12dfa39  B[1]=d0a640d4  C[1]=ae236080  D[1]=6bbfe9b2
A[2]=42cff156  B[2]=9da04ddf  C[2]=de489a8d  D[2]=46c580ad
A[3]=ae15eb32  B[3]=778a53ac  C[3]=b45d326f  D[3]=ec33d0fa
A[4]=47f5d6f7  B[4]=35c585c8  C[4]=ef2c6921  D[4]=5de7bf7e
A[5]=970da088  B[5]=22ea41b0  C[5]=c44f815b  D[5]=a1ff2d2d
A[6]=0f8c74f1  B[6]=c5f90f11  C[6]=cdce544d  D[6]=89cbc5a7
A[7]=7c27f74b  B[7]=f5fcf804  C[7]=2c5d2191  D[7]=caac3578

Feed-Forward Step 32: (r= 4, s=13)
A[0]=366d7cc7  B[0]=135ab061  C[0]=cb3f719b  D[0]=6f7e591b
A[1]=8180dd2e  B[1]=12dfa39d  C[1]=d0a640d4  D[1]=ae236080
A[2]=ab81bfd2  B[2]=2cff1564  C[2]=9da04ddf  D[2]=de489a8d
```

```
A[3]=a6ea1117  B[3]=e15eb32a  C[3]=778a53ac  D[3]=b45d326f
A[4]=cb88930c  B[4]=7f5d6f74  C[4]=35c585c8  D[4]=ef2c6921
A[5]=9335b64c  B[5]=70da0889  C[5]=22ea41b0  D[5]=c44f815b
A[6]=0cdc41f0  B[6]=f8c74f10  C[6]=c5f90f11  D[6]=cdce544d
A[7]=0dfae369  B[7]=c27f74b7  C[7]=f5fcf804  D[7]=2c5d2191

Feed-Forward Step 33: (r=13, s=10)
A[0]=c0bfd135  B[0]=af98e6cd  C[0]=135ab061  D[0]=cb3f719b
A[1]=74f31759  B[1]=1ba5d030  C[1]=12dfa39d  D[1]=d0a640d4
A[2]=84ffde1b  B[2]=37fa5570  C[2]=2cff1564  D[2]=9da04ddf
A[3]=db31d2d9  B[3]=4222f4dd  C[3]=e15eb32a  D[3]=778a53ac
A[4]=b5b83d54  B[4]=12619971  C[4]=7f5d6f74  D[4]=35c585c8
A[5]=ae8a829c  B[5]=b6c99266  C[5]=70da0889  D[5]=22ea41b0
A[6]=db5f033d  B[6]=883e019b  C[6]=f8c74f10  D[6]=c5f90f11
A[7]=ec727293  B[7]=5c6d21bf  C[7]=c27f74b7  D[7]=f5fcf804

Feed-Forward Step 34: (r=10, s=25)
A[0]=f5f47bc0  B[0]=ff44d702  C[0]=af98e6cd  D[0]=135ab061
A[1]=6d94659e  B[1]=cc5d65d3  C[1]=1ba5d030  D[1]=12dfa39d
A[2]=e92067a9  B[2]=ff786e13  C[2]=37fa5570  D[2]=2cff1564
A[3]=34f889a8  B[3]=c74b676c  C[3]=4222f4dd  D[3]=e15eb32a
A[4]=eb6f5835  B[4]=e0f552d6  C[4]=12619971  D[4]=7f5d6f74
A[5]=4db4a1a3  B[5]=2a0a72ba  C[5]=b6c99266  D[5]=70da0889
A[6]=131c4e89  B[6]=7c0cf76d  C[6]=883e019b  D[6]=f8c74f10
A[7]=64462edd  B[7]=c9ca4fb1  C[7]=5c6d21bf  D[7]=c27f74b7

Feed-Forward Step 35: (r=25, s= 4)
A[0]=45e6025e  B[0]=81ebe8f7  C[0]=ff44d702  D[0]=af98e6cd
A[1]=37f88e86  B[1]=3cdb28cb  C[1]=cc5d65d3  D[1]=1ba5d030
A[2]=46f435f5  B[2]=53d240cf  C[2]=ff786e13  D[2]=37fa5570
A[3]=a068a209  B[3]=5069f113  C[3]=c74b676c  D[3]=4222f4dd
A[4]=654746a1  B[4]=6bd6deb0  C[4]=e0f552d6  D[4]=12619971
A[5]=830fd584  B[5]=469b6943  C[5]=2a0a72ba  D[5]=b6c99266
A[6]=e7e33c68  B[6]=1226389d  C[6]=7c0cf76d  D[6]=883e019b
A[7]=aa5c35cb  B[7]=bac88c5d  C[7]=c9ca4fb1  D[7]=5c6d21bf
```

Compression Function Output

```
A[0]=45e6025e  B[0]=81ebe8f7  C[0]=ff44d702  D[0]=af98e6cd
A[1]=37f88e86  B[1]=3cdb28cb  C[1]=cc5d65d3  D[1]=1ba5d030
A[2]=46f435f5  B[2]=53d240cf  C[2]=ff786e13  D[2]=37fa5570
A[3]=a068a209  B[3]=5069f113  C[3]=c74b676c  D[3]=4222f4dd
A[4]=654746a1  B[4]=6bd6deb0  C[4]=e0f552d6  D[4]=12619971
A[5]=830fd584  B[5]=469b6943  C[5]=2a0a72ba  D[5]=b6c99266
A[6]=e7e33c68  B[6]=1226389d  C[6]=7c0cf76d  D[6]=883e019b
A[7]=aa5c35cb  B[7]=bac88c5d  C[7]=c9ca4fb1  D[7]=5c6d21bf
```

Hash Function Output

```
5e02e645868ef837f535f44609a268a0a146476584d50f83683ce3e7cb355caaf7e8eb81cb28db3ccf40d25313f16950
```

A.3.3 Two-block Message

We use the message made of 1079 `1` bits.

First block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
M[ 64.. 71] = ff ff ff ff ff ff ff ff
M[ 72.. 79] = ff ff ff ff ff ff ff ff
M[ 80.. 87] = ff ff ff ff ff ff ff ff
M[ 88.. 95] = ff ff ff ff ff ff ff ff
M[ 96..103] = ff ff ff ff ff ff ff ff
M[104..111] = ff ff ff ff ff ff ff ff
M[112..119] = ff ff ff ff ff ff ff ff
M[120..127] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =    2   86   98  227   95   77   58  143
y[  8.. 15] =   30   88  113  180   23   99  198   13
y[ 16.. 23] =  129   99   49  124  176  112   29   25
y[ 24.. 31] =   15   75  185   88  140  162   99  143
y[ 32.. 39] =  193   12  153  234   88   32  143  123
y[ 40.. 47] =  136  228  221  198   70  243  178  116
y[ 48.. 55] =  225  137  205    0   44    3  200  137
y[ 56.. 63] =   68   61  239  127   35  160   89  129
y[ 64.. 71] =  241   24  231  210   22  182  100  124
y[ 72.. 79] =   34   91  248   64  146  239  173   25
y[ 80.. 87] =  249   80  244  174   11   64   50   18
y[ 88.. 95] =   17  161  124   95   73  100  215  156
y[ 96..103] =  253  250  122   18  134  251   25  162
y[104..111] =  137  234   62   10  165  228  236   41
y[112..119] =  255  140   61   62   67  176  141  238
y[120..127] =  197  205   31  131  211   74  118   53
y[128..135] =  256  253  159   94  162  227  199   89
y[136..143] =  227  118  144   32  234  217   59  152
y[144..151] =  128  177  208  172   81  165  228  147
y[152..159] =  242  179   72  170  117  128  158  176
y[160..167] =   64   85  104  220  169  115  114  114
y[168..175] =  121   95   36  140  187  171   79  181
y[176..183] =   32  233   52  163  213   31   57   89
y[184..191] =  189  205   18  166  222  123  168   76
y[192..199] =   16   20   26   13  235   31  157  116
```

```
y[200..207] =  223  189    9  151  111  104   84  111
y[208..215] =    8  129   13  175  246  104  207  165
y[216..223] =  240  108  133    7  184  209   42  253
y[224..231] =    4  194  135  198  123  254  232   90
y[232..239] =  120  100  195  219   92  239   21  189
y[240..247] =    2  201  196  128  190  118  116   62
y[248..255] =   60   69  226   71   46  111  139  114
```

Intermediate Expanded Message

```
Z[ 0] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
Z[ 1] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
Z[ 2] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
Z[ 3] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
Z[ 4] = 1158f470  de09ed36  c9cd0fe6  599c4844
        41c31892  2e40f97f  f2feafc9  1211c34c
Z[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
        baa00c49  44a7599c  484434c1  b703e1a6
Z[ 6] = faf1fd1c  0d02582a  fbaaa71d  bb591211
        ef61a948  073a2cce  eb0bbd84  1da1f0d3
Z[ 7] = ab73fe8e  2cce2c15  c577306b  f245ac2c
        da6cd4a4  a4f21667  357adec2  264d5546
Z[ 8] = fd1cff47  43eeb92e  ea52bb59  4051d616
        5546ea52  1720ae57  e318ef61  b41f2aa3
Z[ 9] = c6305c80  c293dc97  bd843a89  b082eb0b
        c7a2f529  c1213408  5c80548d  c577b875
Z[10] = 3d6d2e40  e5434b28  531bc068  52625262
        44a75771  ab731a04  c1dacd6a  c9143917
Z[11] = eea81720  bc122594  1667e034  40512931
        da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
Z[12] = 0e740b90  096512ca  1667f01a  53d4b7bc
        cedce76e  b3660681  4b285037  50373cb4
Z[13] = a38005c8  c4be0965  4b28f80d  bd84dbde
        4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
Z[14] = d27902e4  d55da7d6  fdd558e3  410aedef
        484456b8  e48ad332  f2fe427c  cedc0f2d
Z[15] = d7880172  5c80d3eb  5546cf95  2cce53d4
        31dd2b5c  334fe999  5037213e  5262aaba
Z[16] = ff1701d2  a6ce5932  a9895677  cb3634ca
        e4b21b4e  992766d9  eb1114ef  35b3ca4d
Z[17] = 74808b80  d3672c99  49b9b647  e59b1a65
        f2590da7  4188be78  6a7d9583  a5e55a1b
Z[18] = 3a40c5c0  5ea8a158  afe85018  67c2983e
        6e2191df  20c4df3c  c04a3fb6  47e7b819
Z[19] = 1d20e2e0  2f54d0ac  d7f4280c  33e1cc1f
```

```
        c21c3de4  1062ef9e  e0251fdb  aeff5101
Z[20] = 0e90f170  17aae856  ebfa1406  a4fc5b04
        e10e1ef2  0831f7cf  65079af9  4c74b38c
Z[21] = 0748f8b8  0bd5f42b  f5fd0a03  d27e2d82
        f0870f79  8f2470dc  bd8f4271  263ad9c6
Z[22] = 03a4fc5c  90f66f0a  6ff3900d  e93f16c1
        6d3892c8  c792386e  53bcac44  131dece3
Z[23] = 01d2fe2e  c87b3785  c3053cfb  6994966c
        369cc964  e3c91c37  29ded622  949a6b66
Z[24] = fc5c4e46  558ee4b2  e4b24615  5101983e
        6b665018  1d20b9eb  db985a1b  a06f0bd5
Z[25] = b7305a1b  b2a370dc  ac4465f0  9be216c1
        b9024443  b0d15018  7480a989  b647983e
Z[26] = 4d5d0aec  de53eb11  68ab1d20  67c26ff3
        5677e59b  9583ca4d  b1baf342  bad46994
Z[27] = ea2892c8  aa720000  1c3702bb  510192c8
        d0ac3785  ad2d7397  6ff3a7b7  452c8b80
Z[28] = 123415d8  0bd5d539  1c37bbbd  699470dc
        c21c52d3  9f863a40  5ea8ef9e  650716c1
Z[29] = 8b8048d0  b55eb475  5ea83a40  ac441062
        624ca8a0  065f5677  d4505b04  fc5ca413
Z[30] = c6a9f9a1  ca4d1062  fd45fa8a  51eaa989
        5b04eb11  dd6a091a  ef9ee59b  c21c2551
Z[31] = cd089583  7480386e  6b66b647  386eeeb5
        3ecdd0ac  409f8d52  6507435a  67c2303d
```

Expanded Message

```
W[ 0] = 1158f470  de09ed36  c9cd0fe6  599c4844
        41c31892  2e40f97f  f2feafc9  1211c34c
W[ 1] = faf1fd1c  0d02582a  fbaaa71d  bb591211
        ef61a948  073a2cce  eb0bbd84  1da1f0d3
W[ 2] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
W[ 3] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
W[ 4] = ab73fe8e  2cce2c15  c577306b  f245ac2c
        da6cd4a4  a4f21667  357adec2  264d5546
W[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
        baa00c49  44a7599c  484434c1  b703e1a6
W[ 6] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
W[ 7] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
W[ 8] = d7880172  5c80d3eb  5546cf95  2cce53d4
        31dd2b5c  334fe999  5037213e  5262aaba
W[ 9] = eea81720  bc122594  1667e034  40512931
        da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
W[10] = 0e740b90  096512ca  1667f01a  53d4b7bc
```

```
         cedce76e  b3660681  4b285037  50373cb4
W[11] =  fd1cff47  43eeb92e  ea52bb59  4051d616
         5546ea52  1720ae57  e318ef61  b41f2aa3
W[12] =  c6305c80  c293dc97  bd843a89  b082eb0b
         c7a2f529  c1213408  5c80548d  c577b875
W[13] =  a38005c8  c4be0965  4b28f80d  bd84dbde
         4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
W[14] =  3d6d2e40  e5434b28  531bc068  52625262
         44a75771  ab731a04  c1dacd6a  c9143917
W[15] =  d27902e4  d55da7d6  fdd558e3  410aedef
         484456b8  e48ad332  f2fe427c  cedc0f2d
W[16] =  74808b80  d3672c99  49b9b647  e59b1a65
         f2590da7  4188be78  6a7d9583  a5e55a1b
W[17] =  3a40c5c0  5ea8a158  afe85018  67c2983e
         6e2191df  20c4df3c  c04a3fb6  47e7b819
W[18] =  01d2fe2e  c87b3785  c3053cfb  6994966c
         369cc964  e3c91c37  29ded622  949a6b66
W[19] =  0e90f170  17aae856  ebfa1406  a4fc5b04
         e10e1ef2  0831f7cf  65079af9  4c74b38c
W[20] =  03a4fc5c  90f66f0a  6ff3900d  e93f16c1
         6d3892c8  c792386e  53bcac44  131dece3
W[21] =  0748f8b8  0bd5f42b  f5fd0a03  d27e2d82
         f0870f79  8f2470dc  bd8f4271  263ad9c6
W[22] =  ff1701d2  a6ce5932  a9895677  cb3634ca
         e4b21b4e  992766d9  eb1114ef  35b3ca4d
W[23] =  1d20e2e0  2f54d0ac  d7f4280c  33e1cc1f
         c21c3de4  1062ef9e  e0251fdb  aeff5101
W[24] =  c6a9f9a1  ca4d1062  fd45fa8a  51eaa989
         5b04eb11  dd6a091a  ef9ee59b  c21c2551
W[25] =  fc5c4e46  558ee4b2  e4b24615  5101983e
         6b665018  1d20b9eb  db985a1b  a06f0bd5
W[26] =  b7305a1b  b2a370dc  ac4465f0  9be216c1
         b9024443  b0d15018  7480a989  b647983e
W[27] =  cd089583  7480386e  6b66b647  386eeeb5
         3ecdd0ac  409f8d52  6507435a  67c2303d
W[28] =  ea2892c8  aa720000  1c3702bb  510192c8
         d0ac3785  ad2d7397  6ff3a7b7  452c8b80
W[29] =  8b8048d0  b55eb475  5ea83a40  ac441062
         624ca8a0  065f5677  d4505b04  fc5ca413
W[30] =  123415d8  0bd5d539  1c37bbbd  699470dc
         c21c52d3  9f863a40  5ea8ef9e  650716c1
W[31] =  4d5d0aec  de53eb11  68ab1d20  67c26ff3
         5677e59b  9583ca4d  b1baf342  bad46994
```

Feistel Steps

```
IV :
A[0]=8a36eebc  B[0]=7360ca61  C[0]=b9e3bfe8  D[0]=e64071ec
A[1]=94a3bd90  B[1]=18361a03  C[1]=63bece2a  D[1]=1deb91a8
```

```
A[2]=d1537b83  B[2]=17dcb4b9  C[2]=8fe506b9  D[2]=8ac8db23
A[3]=b25b070b  B[3]=3414c45a  C[3]=f8cc4ac2  D[3]=3f782ab5
A[4]=f463f1b5  B[4]=a699a9d2  C[4]=7ae11542  D[4]=039b5cb8
A[5]=b6f81e20  B[5]=e39e9664  C[5]=b1aadda1  D[5]=71ddd962
A[6]=0055c339  B[6]=468bfe77  C[6]=64b06794  D[6]=fade2cea
A[7]=b4d144d1  B[7]=51d062f8  C[7]=28d2f462  D[7]=1416df71

IV XOR M :
A[0]=75c91143  B[0]=8c9f359e  C[0]=461c4017  D[0]=19bf8e13
A[1]=6b5c426f  B[1]=e7c9e5fc  C[1]=9c4131d5  D[1]=e2146e57
A[2]=2eac847c  B[2]=e8234b46  C[2]=701af946  D[2]=753724dc
A[3]=4da4f8f4  B[3]=cbeb3ba5  C[3]=0733b53d  D[3]=c087d54a
A[4]=0b9c0e4a  B[4]=5966562d  C[4]=851eeabd  D[4]=fc64a347
A[5]=4907e1df  B[5]=1c61699b  C[5]=4e55225e  D[5]=8e22269d
A[6]=ffaa3cc6  B[6]=b9740188  C[6]=9b4f986b  D[6]=0521d315
A[7]=4b2ebb2e  B[7]=ae2f9d07  C[7]=d72d0b9d  D[7]=ebe9208e

Step  0: (r= 3, s=23)
A[0]=277aee64  B[0]=ae488a1b  C[0]=8c9f359e  D[0]=461c4017
A[1]=73243e01  B[1]=5ae2137b  C[1]=e7c9e5fc  D[1]=9c4131d5
A[2]=718362f9  B[2]=756423e1  C[2]=e8234b46  D[2]=701af946
A[3]=13170f8e  B[3]=6d27c7a2  C[3]=cbeb3ba5  D[3]=0733b53d
A[4]=93a4a64b  B[4]=5ce07250  C[4]=5966562d  D[4]=851eeabd
A[5]=38c5cc91  B[5]=483f0efa  C[5]=1c61699b  D[5]=4e55225e
A[6]=1d4e9c73  B[6]=fd51e637  C[6]=b9740188  D[6]=9b4f986b
A[7]=b61ffb75  B[7]=5975d972  C[7]=ae2f9d07  D[7]=d72d0b9d

Step  1: (r=23, s=17)
A[0]=eb2a8705  B[0]=3213bd77  C[0]=ae488a1b  D[0]=8c9f359e
A[1]=76d41057  B[1]=00b9921f  C[1]=5ae2137b  D[1]=e7c9e5fc
A[2]=be5e9c1e  B[2]=7cb8c1b1  C[2]=756423e1  D[2]=e8234b46
A[3]=467f7bdd  B[3]=c7098b87  C[3]=6d27c7a2  D[3]=cbeb3ba5
A[4]=898c5c77  B[4]=25c9d253  C[4]=5ce07250  D[4]=5966562d
A[5]=c0964eef  B[5]=489c62e6  C[5]=483f0efa  D[5]=1c61699b
A[6]=e968450e  B[6]=398ea74e  C[6]=fd51e637  D[6]=b9740188
A[7]=b47dac28  B[7]=badb0ffd  C[7]=5975d972  D[7]=ae2f9d07

Step  2: (r=17, s=27)
A[0]=b7c5bade  B[0]=0e0bd655  C[0]=3213bd77  D[0]=ae488a1b
A[1]=6690fefe  B[1]=20aeeda8  C[1]=00b9921f  D[1]=5ae2137b
A[2]=02f3dff3  B[2]=383d7cbd  C[2]=7cb8c1b1  D[2]=756423e1
A[3]=d7f38551  B[3]=f7ba8cfe  C[3]=c7098b87  D[3]=6d27c7a2
A[4]=019509c1  B[4]=b8ef1318  C[4]=25c9d253  D[4]=5ce07250
A[5]=29bd38ec  B[5]=9ddf812c  C[5]=489c62e6  D[5]=483f0efa
A[6]=eadfd8e3  B[6]=8a1dd2d0  C[6]=398ea74e  D[6]=fd51e637
A[7]=9366f7aa  B[7]=585168fb  C[7]=badb0ffd  D[7]=5975d972

Step  3: (r=27, s= 3)
A[0]=770736af  B[0]=f5be2dd6  C[0]=0e0bd655  D[0]=3213bd77
```

```
A[1]=ef8546e2  B[1]=f33487f7  C[1]=20aeeda8  D[1]=00b9921f
A[2]=39228947  B[2]=98179eff  C[2]=383d7cbd  D[2]=7cb8c1b1
A[3]=e3ee4e8a  B[3]=8ebf9c2a  C[3]=f7ba8cfe  D[3]=c7098b87
A[4]=ba6aa748  B[4]=080ca84e  C[4]=b8ef1318  D[4]=25c9d253
A[5]=5928b7ea  B[5]=614de9c7  C[5]=9ddf812c  D[5]=489c62e6
A[6]=d3de6e93  B[6]=1f56fec7  C[6]=8a1dd2d0  D[6]=398ea74e
A[7]=392cf325  B[7]=549b37bd  C[7]=585168fb  D[7]=badb0ffd

Step  4: (r= 3, s=23)
A[0]=37700acb  B[0]=b839b57b  C[0]=f5be2dd6  D[0]=0e0bd655
A[1]=de5dd088  B[1]=7c2a3717  C[1]=f33487f7  D[1]=20aeeda8
A[2]=5724ccf0  B[2]=c9144a39  C[2]=98179eff  D[2]=383d7cbd
A[3]=cdc3fb80  B[3]=1f727457  C[3]=8ebf9c2a  D[3]=f7ba8cfe
A[4]=9c0689bc  B[4]=d3553a45  C[4]=080ca84e  D[4]=b8ef1318
A[5]=55dd2388  B[5]=c945bf52  C[5]=614de9c7  D[5]=9ddf812c
A[6]=90f7a899  B[6]=9ef3749e  C[6]=1f56fec7  D[6]=8a1dd2d0
A[7]=4930eb25  B[7]=c9679929  C[7]=549b37bd  D[7]=585168fb

Step  5: (r=23, s=17)
A[0]=8f76929e  B[0]=659bb805  C[0]=b839b57b  D[0]=f5be2dd6
A[1]=447e41b6  B[1]=446f2ee8  C[1]=7c2a3717  D[1]=f33487f7
A[2]=6b7d6db5  B[2]=782b9266  C[2]=c9144a39  D[2]=98179eff
A[3]=38932ca5  B[3]=c066e1fd  C[3]=1f727457  D[3]=8ebf9c2a
A[4]=4fc0f924  B[4]=de4e0344  C[4]=d3553a45  D[4]=080ca84e
A[5]=853fda0f  B[5]=c42aee91  C[5]=c945bf52  D[5]=614de9c7
A[6]=4cd0119c  B[6]=4cc87bd4  C[6]=9ef3749e  D[6]=1f56fec7
A[7]=71386917  B[7]=92a49875  C[7]=c9679929  D[7]=549b37bd

Step  6: (r=17, s=27)
A[0]=9caab5b7  B[0]=253d1eed  C[0]=659bb805  D[0]=b839b57b
A[1]=7ddc26cf  B[1]=836c88fc  C[1]=446f2ee8  D[1]=7c2a3717
A[2]=235499e8  B[2]=db6ad6fa  C[2]=782b9266  D[2]=c9144a39
A[3]=44b2b92f  B[3]=594a7126  C[3]=c066e1fd  D[3]=1f727457
A[4]=d5d84f92  B[4]=f2489f81  C[4]=de4e0344  D[4]=d3553a45
A[5]=477eb7d2  B[5]=b41f0a7f  C[5]=c42aee91  D[5]=c945bf52
A[6]=4c9b4b47  B[6]=233899a0  C[6]=4cc87bd4  D[6]=9ef3749e
A[7]=779471b0  B[7]=d22ee270  C[7]=92a49875  D[7]=c9679929

Step  7: (r=27, s= 3)
A[0]=a7f78e37  B[0]=bce555ad  C[0]=253d1eed  D[0]=659bb805
A[1]=9679a10d  B[1]=7beee136  C[1]=836c88fc  D[1]=446f2ee8
A[2]=25a2aa9d  B[2]=411aa4cf  C[2]=db6ad6fa  D[2]=782b9266
A[3]=d04e78aa  B[3]=7a2595c9  C[3]=594a7126  D[3]=c066e1fd
A[4]=90be9aa4  B[4]=96aec27c  C[4]=f2489f81  D[4]=de4e0344
A[5]=ff98936a  B[5]=923bf5be  C[5]=b41f0a7f  D[5]=c42aee91
A[6]=bae8823a  B[6]=3a64da5a  C[6]=233899a0  D[6]=4cc87bd4
A[7]=87bb637c  B[7]=83bca38d  C[7]=d22ee270  D[7]=92a49875

Step  8: (r=28, s=19)
```

```
A[0]=1ed598a9  B[0]=7a7f78e3  C[0]=bce555ad  D[0]=253d1eed
A[1]=2eb9591c  B[1]=d9679a10  C[1]=7beee136  D[1]=836c88fc
A[2]=00612f94  B[2]=d25a2aa9  C[2]=411aa4cf  D[2]=db6ad6fa
A[3]=eae3bb00  B[3]=ad04e78a  C[3]=7a2595c9  D[3]=594a7126
A[4]=80824376  B[4]=490be9aa  C[4]=96aec27c  D[4]=f2489f81
A[5]=3851345d  B[5]=aff98936  C[5]=923bf5be  D[5]=b41f0a7f
A[6]=3fe63c64  B[6]=abae8823  C[6]=3a64da5a  D[6]=233899a0
A[7]=0b45602f  B[7]=c87bb637  C[7]=83bca38d  D[7]=d22ee270

Step  9: (r=19, s=22)
A[0]=695399ad  B[0]=c548f6ac  C[0]=7a7f78e3  D[0]=bce555ad
A[1]=88ad90b6  B[1]=c8e175ca  C[1]=d9679a10  D[1]=7beee136
A[2]=4395c204  B[2]=7ca00309  C[2]=d25a2aa9  D[2]=411aa4cf
A[3]=50f5ddda  B[3]=d807571d  C[3]=ad04e78a  D[3]=7a2595c9
A[4]=c51ab83c  B[4]=1bb40412  C[4]=490be9aa  D[4]=96aec27c
A[5]=4f3f9021  B[5]=a2e9c289  C[5]=aff98936  D[5]=923bf5be
A[6]=bf9df4e4  B[6]=e321ff31  C[6]=abae8823  D[6]=3a64da5a
A[7]=148e47da  B[7]=01785a2b  C[7]=c87bb637  D[7]=83bca38d

Step 10: (r=22, s= 7)
A[0]=d9bd5306  B[0]=6b5a54e6  C[0]=c548f6ac  D[0]=7a7f78e3
A[1]=1c98269f  B[1]=2da22b64  C[1]=c8e175ca  D[1]=d9679a10
A[2]=5401f478  B[2]=8110e570  C[2]=7ca00309  D[2]=d25a2aa9
A[3]=eb3ca3cb  B[3]=76943d77  C[3]=d807571d  D[3]=ad04e78a
A[4]=44fae1c8  B[4]=0f3146ae  C[4]=1bb40412  D[4]=490be9aa
A[5]=7ef292f1  B[5]=0853cfe4  C[5]=a2e9c289  D[5]=aff98936
A[6]=60e729f8  B[6]=392fe77d  C[6]=e321ff31  D[6]=abae8823
A[7]=461a7efc  B[7]=f6852391  C[7]=01785a2b  D[7]=c87bb637

Step 11: (r= 7, s=28)
A[0]=0598cf8c  B[0]=dea9836c  C[0]=6b5a54e6  D[0]=c548f6ac
A[1]=ac14608a  B[1]=4c134f8e  C[1]=2da22b64  D[1]=c8e175ca
A[2]=4b945afa  B[2]=00fa3c2a  C[2]=8110e570  D[2]=7ca00309
A[3]=e98bdf5f  B[3]=9e51e5f5  C[3]=76943d77  D[3]=d807571d
A[4]=b7ebc117  B[4]=7d70e422  C[4]=0f3146ae  D[4]=1bb40412
A[5]=33a0e313  B[5]=794978bf  C[5]=0853cfe4  D[5]=a2e9c289
A[6]=7170dce4  B[6]=7394fc30  C[6]=392fe77d  D[6]=e321ff31
A[7]=dd39ec60  B[7]=0d3f7e23  C[7]=f6852391  D[7]=01785a2b

Step 12: (r=28, s=19)
A[0]=e69a7756  B[0]=c0598cf8  C[0]=dea9836c  D[0]=6b5a54e6
A[1]=3694ca0b  B[1]=aac14608  C[1]=4c134f8e  D[1]=2da22b64
A[2]=039bebd6  B[2]=a4b945af  C[2]=00fa3c2a  D[2]=8110e570
A[3]=787af4f2  B[3]=fe98bdf5  C[3]=9e51e5f5  D[3]=76943d77
A[4]=e9a1d43a  B[4]=7b7ebc11  C[4]=7d70e422  D[4]=0f3146ae
A[5]=b6fe3016  B[5]=333a0e31  C[5]=794978bf  D[5]=0853cfe4
A[6]=2c56ccc2  B[6]=47170dce  C[6]=7394fc30  D[6]=392fe77d
A[7]=c666ae64  B[7]=0dd39ec6  C[7]=0d3f7e23  D[7]=f6852391
```

```
Step 13: (r=19, s=22)
A[0]=2c8caa06  B[0]=bab734d3  C[0]=c0598cf8  D[0]=dea9836c
A[1]=357df451  B[1]=5059b4a6  C[1]=aac14608  D[1]=4c134f8e
A[2]=3104a008  B[2]=5eb01cdf  C[2]=a4b945af  D[2]=00fa3c2a
A[3]=45b2cfb8  B[3]=a793c3d7  C[3]=fe98bdf5  D[3]=9e51e5f5
A[4]=60ace09e  B[4]=a1d74d0e  C[4]=7b7ebc11  D[4]=7d70e422
A[5]=f029ec11  B[5]=80b5b7f1  C[5]=333a0e31  D[5]=794978bf
A[6]=3e4f82be  B[6]=661162b6  C[6]=47170dce  D[6]=7394fc30
A[7]=bbd40a17  B[7]=73263335  C[7]=0dd39ec6  D[7]=0d3f7e23

Step 14: (r=22, s= 7)
A[0]=6e7c9edf  B[0]=818b232a  C[0]=bab734d3  D[0]=c0598cf8
A[1]=59d27e5a  B[1]=144d5f7d  C[1]=5059b4a6  D[1]=aac14608
A[2]=5111fd77  B[2]=020c4128  C[2]=5eb01cdf  D[2]=a4b945af
A[3]=25906794  B[3]=ee116cb3  C[3]=a793c3d7  D[3]=fe98bdf5
A[4]=100fe30d  B[4]=27982b38  C[4]=a1d74d0e  D[4]=7b7ebc11
A[5]=a2b8a5a2  B[5]=047c0a7b  C[5]=80b5b7f1  D[5]=333a0e31
A[6]=4955214f  B[6]=af8f93e0  C[6]=661162b6  D[6]=47170dce
A[7]=c4783c69  B[7]=85eef502  C[7]=73263335  D[7]=0dd39ec6

Step 15: (r= 7, s=28)
A[0]=1e69c40f  B[0]=3e4f6fb7  C[0]=818b232a  D[0]=bab734d3
A[1]=0925bba7  B[1]=e93f2d2c  C[1]=144d5f7d  D[1]=5059b4a6
A[2]=273b7649  B[2]=88febba8  C[2]=020c4128  D[2]=5eb01cdf
A[3]=1ac62288  B[3]=c833ca12  C[3]=ee116cb3  D[3]=a793c3d7
A[4]=e754e385  B[4]=07f18688  C[4]=27982b38  D[4]=a1d74d0e
A[5]=31bbe2a7  B[5]=5c52d151  C[5]=047c0a7b  D[5]=80b5b7f1
A[6]=48e216fa  B[6]=aa90a7a4  C[6]=af8f93e0  D[6]=661162b6
A[7]=33610b5d  B[7]=3c1e34e2  C[7]=85eef502  D[7]=73263335

Step 16: (r=29, s= 9)
A[0]=2b366467  B[0]=e3cd3881  C[0]=3e4f6fb7  D[0]=818b232a
A[1]=5ff63ad3  B[1]=e124b774  C[1]=e93f2d2c  D[1]=144d5f7d
A[2]=33d9d5d2  B[2]=24e76ec9  C[2]=88febba8  D[2]=020c4128
A[3]=657d9666  B[3]=0358c451  C[3]=c833ca12  D[3]=ee116cb3
A[4]=5ae71e17  B[4]=bcea9c70  C[4]=07f18688  D[4]=27982b38
A[5]=d0e9a718  B[5]=e6377c54  C[5]=5c52d151  D[5]=047c0a7b
A[6]=f5ea4f70  B[6]=491c42df  C[6]=aa90a7a4  D[6]=af8f93e0
A[7]=1b3aa1ef  B[7]=a66c216b  C[7]=3c1e34e2  D[7]=85eef502

Step 17: (r= 9, s=15)
A[0]=856ac656  B[0]=6cc8ce56  C[0]=e3cd3881  D[0]=3e4f6fb7
A[1]=4fd44e78  B[1]=ec75a6bf  C[1]=e124b774  D[1]=e93f2d2c
A[2]=ec89d42d  B[2]=b3aba467  C[2]=24e76ec9  D[2]=88febba8
A[3]=d569bded  B[3]=fb2cccca  C[3]=0358c451  D[3]=c833ca12
A[4]=a21bb80c  B[4]=ce3c2eb5  C[4]=bcea9c70  D[4]=07f18688
A[5]=03a35aa5  B[5]=d34e31a1  C[5]=e6377c54  D[5]=5c52d151
A[6]=2e838f1a  B[6]=d49ee1eb  C[6]=491c42df  D[6]=aa90a7a4
A[7]=3f7fa8b6  B[7]=7543de36  C[7]=a66c216b  D[7]=3c1e34e2
```

```
Step 18: (r=15, s= 5)
A[0]=8b601965  B[0]=632b42b5  C[0]=6cc8ce56  D[0]=e3cd3881
A[1]=a1e9cec0  B[1]=273c27ea  C[1]=ec75a6bf  D[1]=e124b774
A[2]=72d010dc  B[2]=ea16f644  C[2]=b3aba467  D[2]=24e76ec9
A[3]=67b2c201  B[3]=def6eab4  C[3]=fb2cccca  D[3]=0358c451
A[4]=d80bb405  B[4]=dc06510d  C[4]=ce3c2eb5  D[4]=bcea9c70
A[5]=496f91d9  B[5]=ad5281d1  C[5]=d34e31a1  D[5]=e6377c54
A[6]=20bedd57  B[6]=c78d1741  C[6]=d49ee1eb  D[6]=491c42df
A[7]=a99c2f34  B[7]=d45b1fbf  C[7]=7543de36  D[7]=a66c216b

Step 19: (r= 5, s=29)
A[0]=3ec6c49a  B[0]=6c032cb1  C[0]=632b42b5  D[0]=6cc8ce56
A[1]=449d23bd  B[1]=3d39d814  C[1]=273c27ea  D[1]=ec75a6bf
A[2]=0c75e20f  B[2]=5a021b8e  C[2]=ea16f644  D[2]=b3aba467
A[3]=f258fe7e  B[3]=f658402c  C[3]=def6eab4  D[3]=fb2cccca
A[4]=e5de1aee  B[4]=017680bb  C[4]=dc06510d  D[4]=ce3c2eb5
A[5]=eb379e50  B[5]=2df23b29  C[5]=ad5281d1  D[5]=d34e31a1
A[6]=6d8fda8c  B[6]=17dbaae4  C[6]=c78d1741  D[6]=d49ee1eb
A[7]=24eac336  B[7]=3385e695  C[7]=d45b1fbf  D[7]=7543de36

Step 20: (r=29, s= 9)
A[0]=beda8b19  B[0]=47d8d893  C[0]=6c032cb1  D[0]=632b42b5
A[1]=6fd9ff0f  B[1]=a893a477  C[1]=3d39d814  D[1]=273c27ea
A[2]=f9ff002c  B[2]=e18ebc41  C[2]=5a021b8e  D[2]=ea16f644
A[3]=4e38e81b  B[3]=de4b1fcf  C[3]=f658402c  D[3]=def6eab4
A[4]=dd7d3094  B[4]=dcbbc35d  C[4]=017680bb  D[4]=dc06510d
A[5]=4e9e6507  B[5]=1d66f3ca  C[5]=2df23b29  D[5]=ad5281d1
A[6]=b7e0a320  B[6]=8db1fb51  C[6]=17dbaae4  D[6]=c78d1741
A[7]=3970c149  B[7]=c49d5866  C[7]=3385e695  D[7]=d45b1fbf

Step 21: (r= 9, s=15)
A[0]=15fd8b86  B[0]=b516337d  C[0]=47d8d893  D[0]=6c032cb1
A[1]=c12c63d3  B[1]=b3fe1edf  C[1]=a893a477  D[1]=3d39d814
A[2]=7dfa236d  B[2]=fe0059f3  C[2]=e18ebc41  D[2]=5a021b8e
A[3]=ae2321d9  B[3]=71d0369c  C[3]=de4b1fcf  D[3]=f658402c
A[4]=ad5be3a3  B[4]=fa6129ba  C[4]=dcbbc35d  D[4]=017680bb
A[5]=ad3d4ef0  B[5]=3cca0e9d  C[5]=1d66f3ca  D[5]=2df23b29
A[6]=e40ba0f9  B[6]=c146416f  C[6]=8db1fb51  D[6]=17dbaae4
A[7]=9e2b5784  B[7]=e1829272  C[7]=c49d5866  D[7]=3385e695

Step 22: (r=15, s= 5)
A[0]=ef563555  B[0]=c5c30afe  C[0]=b516337d  D[0]=47d8d893
A[1]=648d52c5  B[1]=31e9e096  C[1]=b3fe1edf  D[1]=a893a477
A[2]=1487436d  B[2]=11b6befd  C[2]=fe0059f3  D[2]=e18ebc41
A[3]=a1adf115  B[3]=90ecd711  C[3]=71d0369c  D[3]=de4b1fcf
A[4]=6646b799  B[4]=f1d1d6ad  C[4]=fa6129ba  D[4]=dcbbc35d
A[5]=21eaf251  B[5]=a778569e  C[5]=3cca0e9d  D[5]=1d66f3ca
A[6]=c3d73496  B[6]=d07cf205  C[6]=c146416f  D[6]=8db1fb51
```

```
A[7]=ea8a499b  B[7]=abc24f15  C[7]=e1829272  D[7]=c49d5866

Step 23: (r= 5, s=29)
A[0]=9a326b80  B[0]=eac6aabd  C[0]=c5c30afe  D[0]=b516337d
A[1]=76f8dbb3  B[1]=91aa58ac  C[1]=31e9e096  D[1]=b3fe1edf
A[2]=4487d2c6  B[2]=90e86da2  C[2]=11b6befd  D[2]=fe0059f3
A[3]=0a2d950c  B[3]=35be22b4  C[3]=90ecd711  D[3]=71d0369c
A[4]=cd09c9f7  B[4]=c8d6f32c  C[4]=f1d1d6ad  D[4]=fa6129ba
A[5]=fbbfbabd  B[5]=3d5e4a24  C[5]=a778569e  D[5]=3cca0e9d
A[6]=2ebca492  B[6]=7ae692d8  C[6]=d07cf205  D[6]=c146416f
A[7]=894228b3  B[7]=5149337d  C[7]=abc24f15  D[7]=e1829272

Step 24: (r= 4, s=13)
A[0]=0ddcda30  B[0]=a326b809  C[0]=eac6aabd  D[0]=c5c30afe
A[1]=dd79de62  B[1]=6f8dbb37  C[1]=91aa58ac  D[1]=31e9e096
A[2]=47b4bcd5  B[2]=487d2c64  C[2]=90e86da2  D[2]=11b6befd
A[3]=876e029d  B[3]=a2d950c0  C[3]=35be22b4  D[3]=90ecd711
A[4]=71a174fe  B[4]=d09c9f7c  C[4]=c8d6f32c  D[4]=f1d1d6ad
A[5]=3885f414  B[5]=bbfbabdf  C[5]=3d5e4a24  D[5]=a778569e
A[6]=fb2fa158  B[6]=ebca4922  C[6]=7ae692d8  D[6]=d07cf205
A[7]=b47bb867  B[7]=94228b38  C[7]=5149337d  D[7]=abc24f15

Step 25: (r=13, s=10)
A[0]=56c9cda4  B[0]=9b4601bb  C[0]=a326b809  D[0]=eac6aabd
A[1]=401fa988  B[1]=3bcc5baf  C[1]=6f8dbb37  D[1]=91aa58ac
A[2]=0cd6d9aa  B[2]=979aa8f6  C[2]=487d2c64  D[2]=90e86da2
A[3]=0e6addb8  B[3]=c053b0ed  C[3]=a2d950c0  D[3]=35be22b4
A[4]=76c56087  B[4]=2e9fce34  C[4]=d09c9f7c  D[4]=c8d6f32c
A[5]=6e30f5c4  B[5]=be828710  C[5]=bbfbabdf  D[5]=3d5e4a24
A[6]=3dd2334c  B[6]=f42b1f65  C[6]=ebca4922  D[6]=7ae692d8
A[7]=e733317b  B[7]=770cf68f  C[7]=94228b38  D[7]=5149337d

Step 26: (r=10, s=25)
A[0]=cf70aa09  B[0]=2736915b  C[0]=9b4601bb  D[0]=a326b809
A[1]=d7b4e4c1  B[1]=7ea62100  C[1]=3bcc5baf  D[1]=6f8dbb37
A[2]=b4dae2b8  B[2]=5b66a833  C[2]=979aa8f6  D[2]=487d2c64
A[3]=d067056f  B[3]=ab76e039  C[3]=c053b0ed  D[3]=a2d950c0
A[4]=81c7ce66  B[4]=15821ddb  C[4]=2e9fce34  D[4]=d09c9f7c
A[5]=0ac29e85  B[5]=c3d711b8  C[5]=be828710  D[5]=bbfbabdf
A[6]=0e71042f  B[6]=48cd30f7  C[6]=f42b1f65  D[6]=ebca4922
A[7]=b433b466  B[7]=ccc5ef9c  C[7]=770cf68f  D[7]=94228b38

Step 27: (r=25, s= 4)
A[0]=43608414  B[0]=139ee154  C[0]=2736915b  D[0]=9b4601bb
A[1]=39b87273  B[1]=83af69c9  C[1]=7ea62100  D[1]=3bcc5baf
A[2]=d0859424  B[2]=7169b5c5  C[2]=5b66a833  D[2]=979aa8f6
A[3]=8957694d  B[3]=dfa0ce0a  C[3]=ab76e039  D[3]=c053b0ed
A[4]=03e6a8f7  B[4]=cd038f9c  C[4]=15821ddb  D[4]=2e9fce34
A[5]=b98415e4  B[5]=0a15853d  C[5]=c3d711b8  D[5]=be828710
```

```
A[6]=033433f9  B[6]=5e1ce208  C[6]=48cd30f7  D[6]=f42b1f65
A[7]=0ecaee36  B[7]=cd686768  C[7]=ccc5ef9c  D[7]=770cf68f

Step 28: (r= 4, s=13)
A[0]=3e421847  B[0]=36084144  C[0]=139ee154  D[0]=2736915b
A[1]=cda64581  B[1]=9b872733  C[1]=83af69c9  D[1]=7ea62100
A[2]=8171557e  B[2]=0859424d  C[2]=7169b5c5  D[2]=5b66a833
A[3]=8dd115e6  B[3]=957694d8  C[3]=dfa0ce0a  D[3]=ab76e039
A[4]=6ab45ee4  B[4]=3e6a8f70  C[4]=cd038f9c  D[4]=15821ddb
A[5]=e0770e58  B[5]=98415e4b  C[5]=0a15853d  D[5]=c3d711b8
A[6]=4bf19927  B[6]=33433f90  C[6]=5e1ce208  D[6]=48cd30f7
A[7]=816cb0b0  B[7]=ecaee360  C[7]=cd686768  D[7]=ccc5ef9c

Step 29: (r=13, s=10)
A[0]=3792a921  B[0]=4308e7c8  C[0]=36084144  D[0]=139ee154
A[1]=4701eb2b  B[1]=c8b039b4  C[1]=9b872733  D[1]=83af69c9
A[2]=acbb9044  B[2]=2aafd02e  C[2]=0859424d  D[2]=7169b5c5
A[3]=8fe0b3e4  B[3]=22bcd1ba  C[3]=957694d8  D[3]=dfa0ce0a
A[4]=f0098fc5  B[4]=8bdc8d56  C[4]=3e6a8f70  D[4]=cd038f9c
A[5]=5096f304  B[5]=e1cb1c0e  C[5]=98415e4b  D[5]=0a15853d
A[6]=0024d5a9  B[6]=3324e97e  C[6]=33433f90  D[6]=5e1ce208
A[7]=068c780e  B[7]=9616102d  C[7]=ecaee360  D[7]=cd686768

Step 30: (r=10, s=25)
A[0]=c6faca62  B[0]=4aa484de  C[0]=4308e7c8  D[0]=36084144
A[1]=ed859f13  B[1]=07acad1c  C[1]=c8b039b4  D[1]=9b872733
A[2]=e8113f61  B[2]=ee4112b2  C[2]=2aafd02e  D[2]=0859424d
A[3]=c54f00bd  B[3]=82cf923f  C[3]=22bcd1ba  D[3]=957694d8
A[4]=19e974e3  B[4]=263f17c0  C[4]=8bdc8d56  D[4]=3e6a8f70
A[5]=48d4f655  B[5]=5bcc1142  C[5]=e1cb1c0e  D[5]=98415e4b
A[6]=e41eed5e  B[6]=9356a400  C[6]=3324e97e  D[6]=33433f90
A[7]=073e0d1e  B[7]=31e0381a  C[7]=9616102d  D[7]=ecaee360

Step 31: (r=25, s= 4)
A[0]=dc6bcdad  B[0]=c58df594  C[0]=4aa484de  D[0]=4308e7c8
A[1]=3bcd1802  B[1]=27db0b3e  C[1]=07acad1c  D[1]=c8b039b4
A[2]=d8322433  B[2]=c3d0227e  C[2]=ee4112b2  D[2]=2aafd02e
A[3]=c6174e3c  B[3]=7b8a9e01  C[3]=82cf923f  D[3]=22bcd1ba
A[4]=4a0728f4  B[4]=c633d2e9  C[4]=263f17c0  D[4]=8bdc8d56
A[5]=36dc0bc1  B[5]=aa91a9ec  C[5]=5bcc1142  D[5]=e1cb1c0e
A[6]=2be3acf5  B[6]=bdc83dda  C[6]=9356a400  D[6]=3324e97e
A[7]=b1ca2414  B[7]=3c0e7c1a  C[7]=31e0381a  D[7]=9616102d

Feed-Forward Step 32: (r= 4, s=13)
A[0]=214c0e8c  B[0]=c6bcdadd  C[0]=c58df594  D[0]=4aa484de
A[1]=54fedfeb  B[1]=bcd18023  C[1]=27db0b3e  D[1]=07acad1c
A[2]=ac6ebd95  B[2]=8322433d  C[2]=c3d0227e  D[2]=ee4112b2
A[3]=0d13d24e  B[3]=6174e3cc  C[3]=7b8a9e01  D[3]=82cf923f
A[4]=2faefcf2  B[4]=a0728f44  C[4]=c633d2e9  D[4]=263f17c0
```

```
A[5]=313adb67  B[5]=6dc0bc13  C[5]=aa91a9ec  D[5]=5bcc1142
A[6]=3ca5e175  B[6]=be3acf52  C[6]=bdc83dda  D[6]=9356a400
A[7]=b545529f  B[7]=1ca2414b  C[7]=3c0e7c1a  D[7]=31e0381a

Feed-Forward Step 33: (r=13, s=10)
A[0]=f77f64b2  B[0]=81d18429  C[0]=c6bcdadd  D[0]=c58df594
A[1]=8d4c00f2  B[1]=dbfd6a9f  C[1]=bcd18023  D[1]=27db0b3e
A[2]=9a98914e  B[2]=d7b2b58d  C[2]=8322433d  D[2]=c3d0227e
A[3]=d431de9e  B[3]=7a49c1a2  C[3]=6174e3cc  D[3]=7b8a9e01
A[4]=ab893056  B[4]=df9e45f5  C[4]=a0728f44  D[4]=c633d2e9
A[5]=89337d38  B[5]=5b6ce627  C[5]=6dc0bc13  D[5]=aa91a9ec
A[6]=09feb0fc  B[6]=bc2ea794  C[6]=be3acf52  D[6]=bdc83dda
A[7]=6dedfaa7  B[7]=aa53f6a8  C[7]=1ca2414b  D[7]=3c0e7c1a

Feed-Forward Step 34: (r=10, s=25)
A[0]=f6c3e155  B[0]=fd92cbdd  C[0]=81d18429  D[0]=c6bcdadd
A[1]=c47fd0d7  B[1]=3003ca35  C[1]=dbfd6a9f  D[1]=bcd18023
A[2]=e492c01f  B[2]=62453a6a  C[2]=d7b2b58d  D[2]=8322433d
A[3]=c3b5d74c  B[3]=c77a7b50  C[3]=7a49c1a2  D[3]=6174e3cc
A[4]=fd2ceacb  B[4]=24c15aae  C[4]=df9e45f5  D[4]=a0728f44
A[5]=9198050c  B[5]=cdf4e224  C[5]=5b6ce627  D[5]=6dc0bc13
A[6]=6c068994  B[6]=fac3f027  C[6]=bc2ea794  D[6]=be3acf52
A[7]=90b4c618  B[7]=b7ea9db7  C[7]=aa53f6a8  D[7]=1ca2414b

Feed-Forward Step 35: (r=25, s= 4)
A[0]=d88a240b  B[0]=abed87c2  C[0]=fd92cbdd  D[0]=81d18429
A[1]=0ffd4651  B[1]=af88ffa1  C[1]=3003ca35  D[1]=dbfd6a9f
A[2]=aa3caa56  B[2]=3fc92580  C[2]=62453a6a  D[2]=d7b2b58d
A[3]=061f4bb9  B[3]=99876bae  C[3]=c77a7b50  D[3]=7a49c1a2
A[4]=c326ebb6  B[4]=97fa59d5  C[4]=24c15aae  D[4]=df9e45f5
A[5]=5131d39f  B[5]=1923300a  C[5]=cdf4e224  D[5]=5b6ce627
A[6]=455b8d97  B[6]=28d80d13  C[6]=fac3f027  D[6]=bc2ea794
A[7]=e2a563e1  B[7]=3121698c  C[7]=b7ea9db7  D[7]=aa53f6a8
```

Compression Function Output

```
A[0]=d88a240b  B[0]=abed87c2  C[0]=fd92cbdd  D[0]=81d18429
A[1]=0ffd4651  B[1]=af88ffa1  C[1]=3003ca35  D[1]=dbfd6a9f
A[2]=aa3caa56  B[2]=3fc92580  C[2]=62453a6a  D[2]=d7b2b58d
A[3]=061f4bb9  B[3]=99876bae  C[3]=c77a7b50  D[3]=7a49c1a2
A[4]=c326ebb6  B[4]=97fa59d5  C[4]=24c15aae  D[4]=df9e45f5
A[5]=5131d39f  B[5]=1923300a  C[5]=cdf4e224  D[5]=5b6ce627
A[6]=455b8d97  B[6]=28d80d13  C[6]=fac3f027  D[6]=bc2ea794
A[7]=e2a563e1  B[7]=3121698c  C[7]=b7ea9db7  D[7]=aa53f6a8
```

Second block

```
M[  0..  7] = ff ff ff ff ff ff fe 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
```

```
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  243   52  151  163  238  141  176    4
y[  8.. 15] =  180  170  128   28   36   36  157   38
y[ 16.. 23] =   68  208   55  168  117  214   88  115
y[ 24.. 31] =   88   14   70  255  173  206  169   46
y[ 32.. 39] =   81  175  138  212   24   95  231  105
y[ 40.. 47] =  163  164  237  239  114   30  101  108
y[ 48.. 55] =  102  116  229   89  170  203   57    2
y[ 56.. 63] =  150  206  145   68  168   96   16  188
y[ 64.. 71] =  210  224  100   35  104  221  190  234
y[ 72.. 79] =  203  159  117   35  162  121   51  137
y[ 80.. 87] =   97   84   41   28  139  160   93  199
y[ 88.. 95] =  238  155  235   82  216  157   67  105
y[ 96..103] =  229  108  176  114  150  225   87  208
y[104..111] =   58   82  135   16    6  210  241  166
y[112..119] =   89  198  134   39   32  224  244  138
y[120..127] =    9  162  101  242  177   36   78  190
y[128..135] =  253  161   80   99   75   12   46   44
y[136..143] =    1  237  214   23  113   75  160  107
y[144..151] =  235   99   19  146  256   79    1  106
y[152..159] =  146   91   23  147  116  103  187  140
y[160..167] =  208  212  231  175  207  151   95    1
y[168..175] =  232   88  172   20   98   63   73   48
y[176..183] =  192  109  121  224  218  244   52   10
y[184..191] =  169   63  154   13   36   77  121  168
y[192..199] =   49  215  209  231   73  167  162   11
y[200..207] =   90   10  183  251  131  157  153  143
y[208..215] =  235  138  164    2  252   99  127   19
y[216..223] =   36   81   41  145    5  224   66  204
y[224..231] =  253  122  184  240  141    0   25  148
y[232..239] =   85  102   83  143   95   63   76    8
y[240..247] =  251   60  249   59   85   46   93  166
y[248..255] =  176  240  243   60  121  113   51  228
```

Intermediate Expanded Message

```
Z[ 0] = 2594f5e2  bc12b366  ac2cf245  02e4c577
        c121c85b  143c5c80  1a041a04  1b76b7bc
Z[ 1] = dc973124  bfaf27bf  e0ed548d  531b3f98
        0a1e3f98  fe8e3296  db25c34c  213ec068
Z[ 2] = c4be3a89  df7baa01  44a71158  4be1ed36
        bccbbc12  f2fef18c  15ae5262  4e0c48fd
Z[ 3] = 53d449b6  4051ebc4  d8fac121  01722931
        db25b2ad  3124af10  4560bfaf  ce230b90
Z[ 4] = e827de09  194b4844  e5fc4b28  ef61cf95
        b92ed8fa  194b548d  5771bb59  a94824db
Z[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
        b64af245  3b42f01a  b7bce25f  4be1306b
Z[ 6] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
        3b4229ea  0b90a7d6  de090456  be3df470
Z[ 7] = d55d4051  1c2fa71d  e8271720  aa01f69b
        bb590681  f52948fd  1a04c630  cf95385e
Z[ 8] = baa0fd1c  478b39d0  08ac3633  1fcc213e
        f18c00b9  109fe0ed  363351a9  4d53b9e7
Z[ 9] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
        41c3afc9  b082109f  4a6f53d4  ab73cd6a
Z[10] = df7bdc97  c4beed36  b366dbde  00b944a7
        3f98edef  0e74c293  2d8746d2  22b034c1
Z[11] = 4ec5d107  e8275771  f69be3d1  073a2594
        2d87c068  0965b591  37a51a04  bfaf5771
Z[12] = e1a62369  ed36dd50  bef634c1  07f3bb59
        073a410a  fbaaca86  b7bca4f2  ad9eb4d8
Z[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
        3a891a04  af101da1  e827039d  d9b32fb2
Z[14] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
        49b63d6d  ad9e3bfb  2d8744a7  05c836ec
Z[15] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
        f3b7c577  2b5cf5e2  51a95771  eb0b24db
Z[16] = fc5cf342  48d09f86  4443eeb5  29deb647
        00e9b9eb  d8dd7480  66d920c4  a7b7a4fc
Z[17] = ebfa3de4  114b320f  ff176a7d  00e95018
        9af95018  14ef3fb6  6994b38c  c04aafe8
Z[18] = d36749b9  e85693b1  d27e15d8  5677e856
        e93faa72  b2a3edcc  593267c2  42715bed
Z[19] = c4d75cd6  6e21e684  dc81b0d1  2f5433e1
        afe89e9d  a2419a10  20c4aeff  6e210e90
Z[20] = 2c99d539  d4505b04  42715ea8  a989c305
        51eaceda  bca66a7d  8d52a989  a1582e6b
Z[21] = ebfa5849  ab5b2551  fb73949a  739754a5
        20c4eeb5  2551ebfa  048ddaaf  3c123cfb
Z[22] = fc5ce684  bd8fb647  966c9e9d  16c14f2f
        4d5d34ca  4b8b90f6  56770576  452cf170
Z[23] = fa8a5101  f8b8900d  4d5d1d20  54a5f42b
        b6470831  f3425bed  6e21b730  2e6b46fe
```

```
Z[24] = a8a02f54  5a1baa72  0aec966c  280c03a4
        edccb0d1  14ef197c  444320c4  61632296
Z[25] = 5a1bd367  9af9aeff  47e7d8dd  607a68ab
        52d30cbe  9be2fe2e  5dbfd195  958329de
Z[26] = d70bb55e  b55ed70b  9f865677  00e95f91
        5018ab5b  1234ef9e  39571b4e  2bb0624c
Z[27] = 63356994  e1f75101  f42bceda  091a01d2
        3957d195  0bd53de4  46155760  aeffc133
Z[28] = d9c6e1f7  e8561fdb  ae16df3c  0a03eb11
        091aa6ce  fa8a1fdb  a4fc6e21  983e92c8
Z[29] = 93b14c74  01d2197c  5a1ba7b7  114bcb36
        49b9a32a  9a104aa2  e1f7a4fc  cfc35f91
Z[30] = 6f0a624c  f08767c2  0000e2e0  9ccbd367
        5cd64aa2  983e0e90  3957d539  0748ad2d
Z[31] = 369cca4d  35b3237f  29dee1f7  ad2d93b1
        f087a989  369cf259  66d920c4  e59bc305
```

Expanded Message

```
W[ 0] = e827de09  194b4844  e5fc4b28  ef61cf95
        b92ed8fa  194b548d  5771bb59  a94824db
W[ 1] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
        3b4229ea  0b90a7d6  de090456  be3df470
W[ 2] = 2594f5e2  bc12b366  ac2cf245  02e4c577
        c121c85b  143c5c80  1a041a04  1b76b7bc
W[ 3] = c4be3a89  df7baa01  44a71158  4be1ed36
        bccbbc12  f2fef18c  15ae5262  4e0c48fd
W[ 4] = d55d4051  1c2fa71d  e8271720  aa01f69b
        bb590681  f52948fd  1a04c630  cf95385e
W[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
        b64af245  3b42f01a  b7bce25f  4be1306b
W[ 6] = 53d449b6  4051ebc4  d8fac121  01722931
        db25b2ad  3124af10  4560bfaf  ce230b90
W[ 7] = dc973124  bfaf27bf  e0ed548d  531b3f98
        0a1e3f98  fe8e3296  db25c34c  213ec068
W[ 8] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
        f3b7c577  2b5cf5e2  51a95771  eb0b24db
W[ 9] = 4ec5d107  e8275771  f69be3d1  073a2594
        2d87c068  0965b591  37a51a04  bfaf5771
W[10] = e1a62369  ed36dd50  bef634c1  07f3bb59
        073a410a  fbaaca86  b7bca4f2  ad9eb4d8
W[11] = baa0fd1c  478b39d0  08ac3633  1fcc213e
        f18c00b9  109fe0ed  363351a9  4d53b9e7
W[12] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
        41c3afc9  b082109f  4a6f53d4  ab73cd6a
W[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
        3a891a04  af101da1  e827039d  d9b32fb2
W[14] = df7bdc97  c4beed36  b366dbde  00b944a7
        3f98edef  0e74c293  2d8746d2  22b034c1
```

```
W[15] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
        49b63d6d  ad9e3bfb  2d8744a7  05c836ec
W[16] = ebfa3de4  114b320f  ff176a7d  00e95018
        9af95018  14ef3fb6  6994b38c  c04aafe8
W[17] = d36749b9  e85693b1  d27e15d8  5677e856
        e93faa72  b2a3edcc  593267c2  42715bed
W[18] = fa8a5101  f8b8900d  4d5d1d20  54a5f42b
        b6470831  f3425bed  6e21b730  2e6b46fe
W[19] = 2c99d539  d4505b04  42715ea8  a989c305
        51eaceda  bca66a7d  8d52a989  a1582e6b
W[20] = fc5ce684  bd8fb647  966c9e9d  16c14f2f
        4d5d34ca  4b8b90f6  56770576  452cf170
W[21] = ebfa5849  ab5b2551  fb73949a  739754a5
        20c4eeb5  2551ebfa  048ddaaf  3c123cfb
W[22] = fc5cf342  48d09f86  4443eeb5  29deb647
        00e9b9eb  d8dd7480  66d920c4  a7b7a4fc
W[23] = c4d75cd6  6e21e684  dc81b0d1  2f5433e1
        afe89e9d  a2419a10  20c4aeff  6e210e90
W[24] = 6f0a624c  f08767c2  0000e2e0  9ccbd367
        5cd64aa2  983e0e90  3957d539  0748ad2d
W[25] = a8a02f54  5a1baa72  0aec966c  280c03a4
        edccb0d1  14ef197c  444320c4  61632296
W[26] = 5a1bd367  9af9aeff  47e7d8dd  607a68ab
        52d30cbe  9be2fe2e  5dbfd195  958329de
W[27] = 369cca4d  35b3237f  29dee1f7  ad2d93b1
        f087a989  369cf259  66d920c4  e59bc305
W[28] = 63356994  e1f75101  f42bceda  091a01d2
        3957d195  0bd53de4  46155760  aeffc133
W[29] = 93b14c74  01d2197c  5a1ba7b7  114bcb36
        49b9a32a  9a104aa2  e1f7a4fc  cfc35f91
W[30] = d9c6e1f7  e8561fdb  ae16df3c  0a03eb11
        091aa6ce  fa8a1fdb  a4fc6e21  983e92c8
W[31] = d70bb55e  b55ed70b  9f865677  00e95f91
        5018ab5b  1234ef9e  39571b4e  2bb0624c
```

Feistel Steps

```
IV :
A[0]=d88a240b  B[0]=abed87c2  C[0]=fd92cbdd  D[0]=81d18429
A[1]=0ffd4651  B[1]=af88ffa1  C[1]=3003ca35  D[1]=dbfd6a9f
A[2]=aa3caa56  B[2]=3fc92580  C[2]=62453a6a  D[2]=d7b2b58d
A[3]=061f4bb9  B[3]=99876bae  C[3]=c77a7b50  D[3]=7a49c1a2
A[4]=c326ebb6  B[4]=97fa59d5  C[4]=24c15aae  D[4]=df9e45f5
A[5]=5131d39f  B[5]=1923300a  C[5]=cdf4e224  D[5]=5b6ce627
A[6]=455b8d97  B[6]=28d80d13  C[6]=fac3f027  D[6]=bc2ea794
A[7]=e2a563e1  B[7]=3121698c  C[7]=b7ea9db7  D[7]=aa53f6a8

IV XOR M :
A[0]=2775dbf4  B[0]=abed87c2  C[0]=fd92cbdd  D[0]=81d18429
```

```
A[1]=0f03b9ae  B[1]=af88ffa1  C[1]=3003ca35  D[1]=dbfd6a9f
A[2]=aa3caa56  B[2]=3fc92580  C[2]=62453a6a  D[2]=d7b2b58d
A[3]=061f4bb9  B[3]=99876bae  C[3]=c77a7b50  D[3]=7a49c1a2
A[4]=c326ebb6  B[4]=97fa59d5  C[4]=24c15aae  D[4]=df9e45f5
A[5]=5131d39f  B[5]=1923300a  C[5]=cdf4e224  D[5]=5b6ce627
A[6]=455b8d97  B[6]=28d80d13  C[6]=fac3f027  D[6]=bc2ea794
A[7]=e2a563e1  B[7]=3121698c  C[7]=b7ea9db7  D[7]=aa53f6a8

Step  0: (r= 3, s=23)
A[0]=75d0bde2  B[0]=3baedfa1  C[0]=abed87c2  D[0]=fd92cbdd
A[1]=85c90478  B[1]=781dcd70  C[1]=af88ffa1  D[1]=3003ca35
A[2]=9f8e59e0  B[2]=51e552b5  C[2]=3fc92580  D[2]=62453a6a
A[3]=e17adc3b  B[3]=30fa5dc8  C[3]=99876bae  D[3]=c77a7b50
A[4]=cf2ef536  B[4]=19375db6  C[4]=97fa59d5  D[4]=24c15aae
A[5]=8840ac6b  B[5]=898e9cfa  C[5]=1923300a  D[5]=cdf4e224
A[6]=25925b7f  B[6]=2adc6cba  C[6]=28d80d13  D[6]=fac3f027
A[7]=b7a0f0c6  B[7]=152b1f0f  C[7]=3121698c  D[7]=b7ea9db7

Step  1: (r=23, s=17)
A[0]=6e14d7c7  B[0]=f13ae85e  C[0]=3baedfa1  D[0]=abed87c2
A[1]=82972959  B[1]=3c42e482  C[1]=781dcd70  D[1]=af88ffa1
A[2]=5ed69150  B[2]=f04fc72c  C[2]=51e552b5  D[2]=3fc92580
A[3]=a93bda78  B[3]=1df0bd6e  C[3]=30fa5dc8  D[3]=99876bae
A[4]=b56ebb1f  B[4]=9b67977a  C[4]=19375db6  D[4]=97fa59d5
A[5]=6ab9a2c0  B[5]=35c42056  C[5]=898e9cfa  D[5]=1923300a
A[6]=72a8eba8  B[6]=bf92c92d  C[6]=2adc6cba  D[6]=28d80d13
A[7]=92adfb15  B[7]=635bd078  C[7]=152b1f0f  D[7]=3121698c

Step  2: (r=17, s=27)
A[0]=74baa7dd  B[0]=af8edc29  C[0]=f13ae85e  D[0]=3baedfa1
A[1]=f40e8730  B[1]=52b3052e  C[1]=3c42e482  D[1]=781dcd70
A[2]=0179cb04  B[2]=22a0bdad  C[2]=f04fc72c  D[2]=51e552b5
A[3]=c065eba6  B[3]=b4f15277  C[3]=1df0bd6e  D[3]=30fa5dc8
A[4]=2ee58520  B[4]=763f6add  C[4]=9b67977a  D[4]=19375db6
A[5]=1ca253a3  B[5]=4580d573  C[5]=35c42056  D[5]=898e9cfa
A[6]=022cf27f  B[6]=d750e551  C[6]=bf92c92d  D[6]=2adc6cba
A[7]=581df51e  B[7]=f62b255b  C[7]=635bd078  D[7]=152b1f0f

Step  3: (r=27, s= 3)
A[0]=65c2610a  B[0]=eba5d53e  C[0]=af8edc29  D[0]=f13ae85e
A[1]=9eeab6f5  B[1]=87a07439  C[1]=52b3052e  D[1]=3c42e482
A[2]=bd37fe05  B[2]=200bce58  C[2]=22a0bdad  D[2]=f04fc72c
A[3]=c212e09e  B[3]=36032f5d  C[3]=b4f15277  D[3]=1df0bd6e
A[4]=5c1250bc  B[4]=01772c29  C[4]=763f6add  D[4]=9b67977a
A[5]=0aa16780  B[5]=18e5129d  C[5]=4580d573  D[5]=35c42056
A[6]=19d25605  B[6]=f8116793  C[6]=d750e551  D[6]=bf92c92d
A[7]=b58b985f  B[7]=f2c0efa8  C[7]=f62b255b  D[7]=635bd078

Step  4: (r= 3, s=23)
```

```
A[0]=41e64b7e  B[0]=2e130853  C[0]=eba5d53e  D[0]=af8edc29
A[1]=cf0a1041  B[1]=f755b7ac  C[1]=87a07439  D[1]=52b3052e
A[2]=d959106b  B[2]=e9bff02d  C[2]=200bce58  D[2]=22a0bdad
A[3]=02d1b333  B[3]=109704f6  C[3]=36032f5d  D[3]=b4f15277
A[4]=53ab33af  B[4]=e09285e2  C[4]=01772c29  D[4]=763f6add
A[5]=a02ccfb3  B[5]=550b3c00  C[5]=18e5129d  D[5]=4580d573
A[6]=47f078f1  B[6]=ce92b028  C[6]=f8116793  D[6]=d750e551
A[7]=0254ae88  B[7]=ac5cc2fd  C[7]=f2c0efa8  D[7]=f62b255b

Step  5: (r=23, s=17)
A[0]=1b81da2b  B[0]=bf20f325  C[0]=2e130853  D[0]=eba5d53e
A[1]=2694541a  B[1]=20e78508  C[1]=f755b7ac  D[1]=87a07439
A[2]=4b71a1af  B[2]=35ecac88  C[2]=e9bff02d  D[2]=200bce58
A[3]=51f110ce  B[3]=998168d9  C[3]=109704f6  D[3]=36032f5d
A[4]=9f1c4554  B[4]=d7a9d599  C[4]=e09285e2  D[4]=01772c29
A[5]=fe29ce69  B[5]=d9d01667  C[5]=550b3c00  D[5]=18e5129d
A[6]=91aa4044  B[6]=78a3f83c  C[6]=ce92b028  D[6]=f8116793
A[7]=47febbe7  B[7]=44012a57  C[7]=ac5cc2fd  D[7]=f2c0efa8

Step  6: (r=17, s=27)
A[0]=469d1e00  B[0]=b4563703  C[0]=bf20f325  D[0]=2e130853
A[1]=cc4a3bfb  B[1]=a8344d28  C[1]=20e78508  D[1]=f755b7ac
A[2]=b3a144d5  B[2]=435e96e3  C[2]=35ecac88  D[2]=e9bff02d
A[3]=da16c2c8  B[3]=219ca3e2  C[3]=998168d9  D[3]=109704f6
A[4]=e9f7e428  B[4]=8aa93e38  C[4]=d7a9d599  D[4]=e09285e2
A[5]=196ce428  B[5]=9cd3fc53  C[5]=d9d01667  D[5]=550b3c00
A[6]=b40f3f9e  B[6]=80892354  C[6]=78a3f83c  D[6]=ce92b028
A[7]=99c6a913  B[7]=77ce8ffd  C[7]=44012a57  D[7]=ac5cc2fd

Step  7: (r=27, s= 3)
A[0]=e455d5a5  B[0]=0234e8f0  C[0]=b4563703  D[0]=bf20f325
A[1]=fd8c4d8a  B[1]=de6251df  C[1]=a8344d28  D[1]=20e78508
A[2]=3b9f01f5  B[2]=ad9d0a26  C[2]=435e96e3  D[2]=35ecac88
A[3]=97d644dd  B[3]=46d0b616  C[3]=219ca3e2  D[3]=998168d9
A[4]=f3a134b6  B[4]=474fbf21  C[4]=8aa93e38  D[4]=d7a9d599
A[5]=b2a2d6f0  B[5]=40cb6721  C[5]=9cd3fc53  D[5]=d9d01667
A[6]=6eeba9ca  B[6]=f5a079fc  C[6]=80892354  D[6]=78a3f83c
A[7]=10b1efdd  B[7]=9cce3548  C[7]=77ce8ffd  D[7]=44012a57

Step  8: (r=28, s=19)
A[0]=327e8f42  B[0]=5e455d5a  C[0]=0234e8f0  D[0]=b4563703
A[1]=d85c5cdb  B[1]=afd8c4d8  C[1]=de6251df  D[1]=a8344d28
A[2]=70181b8f  B[2]=53b9f01f  C[2]=ad9d0a26  D[2]=435e96e3
A[3]=a54e2229  B[3]=d97d644d  C[3]=46d0b616  D[3]=219ca3e2
A[4]=1d7aa375  B[4]=6f3a134b  C[4]=474fbf21  D[4]=8aa93e38
A[5]=acddf450  B[5]=0b2a2d6f  C[5]=40cb6721  D[5]=9cd3fc53
A[6]=3a92d4c5  B[6]=a6eeba9c  C[6]=f5a079fc  D[6]=80892354
A[7]=54adfbab  B[7]=d10b1efd  C[7]=9cce3548  D[7]=77ce8ffd
```

```
Step  9: (r=19, s=22)
A[0]=5b80d8dd  B[0]=7a1193f4  C[0]=5e455d5a  D[0]=0234e8f0
A[1]=ae94dfeb  B[1]=e6dec2e2  C[1]=afd8c4d8  D[1]=de6251df
A[2]=32d779d6  B[2]=dc7b80c0  C[2]=53b9f01f  D[2]=ad9d0a26
A[3]=4c59efc1  B[3]=114d2a71  C[3]=d97d644d  D[3]=46d0b616
A[4]=1e6bb09d  B[4]=1ba8ebd5  C[4]=6f3a134b  D[4]=474fbf21
A[5]=2ed63665  B[5]=a28566ef  C[5]=0b2a2d6f  D[5]=40cb6721
A[6]=e0d0e012  B[6]=a629d496  C[6]=a6eeba9c  D[6]=f5a079fc
A[7]=38495930  B[7]=dd5aa56f  C[7]=d10b1efd  D[7]=9cce3548

Step 10: (r=22, s= 7)
A[0]=00a42e1c  B[0]=3756e036  C[0]=7a1193f4  D[0]=5e455d5a
A[1]=3085c697  B[1]=faeba537  C[1]=e6dec2e2  D[1]=afd8c4d8
A[2]=024b7d96  B[2]=758cb5de  C[2]=dc7b80c0  D[2]=53b9f01f
A[3]=5024bea6  B[3]=f053167b  C[3]=114d2a71  D[3]=d97d644d
A[4]=2d6013ba  B[4]=27479aec  C[4]=1ba8ebd5  D[4]=6f3a134b
A[5]=15e8bf68  B[5]=994bb58d  C[5]=a28566ef  D[5]=0b2a2d6f
A[6]=5f487bb6  B[6]=04b83438  C[6]=a629d496  D[6]=a6eeba9c
A[7]=02c0a17d  B[7]=4c0e1256  C[7]=dd5aa56f  D[7]=d10b1efd

Step 11: (r= 7, s=28)
A[0]=9d8f74d0  B[0]=52170e00  C[0]=3756e036  D[0]=7a1193f4
A[1]=aeedd547  B[1]=42e34b98  C[1]=faeba537  D[1]=e6dec2e2
A[2]=e3daac43  B[2]=25becb01  C[2]=758cb5de  D[2]=dc7b80c0
A[3]=88e704ee  B[3]=125f5328  C[3]=f053167b  D[3]=114d2a71
A[4]=5c6c3c87  B[4]=b009dd16  C[4]=27479aec  D[4]=1ba8ebd5
A[5]=0f088e3e  B[5]=f45fb40a  C[5]=994bb58d  D[5]=a28566ef
A[6]=6a740f2f  B[6]=a43ddb2f  C[6]=04b83438  D[6]=a629d496
A[7]=d57658d4  B[7]=6050be81  C[7]=4c0e1256  D[7]=dd5aa56f

Step 12: (r=28, s=19)
A[0]=8e4e2b34  B[0]=09d8f74d  C[0]=52170e00  D[0]=3756e036
A[1]=a44b4d8e  B[1]=7aeedd54  C[1]=42e34b98  D[1]=faeba537
A[2]=4b446274  B[2]=3e3daac4  C[2]=25becb01  D[2]=758cb5de
A[3]=826e35ba  B[3]=e88e704e  C[3]=125f5328  D[3]=f053167b
A[4]=a9b2fe1f  B[4]=75c6c3c8  C[4]=b009dd16  D[4]=27479aec
A[5]=9b252d5d  B[5]=e0f088e3  C[5]=f45fb40a  D[5]=994bb58d
A[6]=b7b783fe  B[6]=f6a740f2  C[6]=a43ddb2f  D[6]=04b83438
A[7]=77476071  B[7]=4d57658d  C[7]=6050be81  D[7]=4c0e1256

Step 13: (r=19, s=22)
A[0]=c6383b56  B[0]=59a47271  C[0]=09d8f74d  D[0]=52170e00
A[1]=5284ab94  B[1]=6c75225a  C[1]=7aeedd54  D[1]=42e34b98
A[2]=4170d323  B[2]=13a25a23  C[2]=3e3daac4  D[2]=25becb01
A[3]=deabd173  B[3]=add41371  C[3]=e88e704e  D[3]=125f5328
A[4]=5d294756  B[4]=f0fd4d97  C[4]=75c6c3c8  D[4]=b009dd16
A[5]=4ac356b9  B[5]=6aecd929  C[5]=e0f088e3  D[5]=f45fb40a
A[6]=088b3fe1  B[6]=1ff5bdbc  C[6]=f6a740f2  D[6]=a43ddb2f
A[7]=5036d99a  B[7]=038bba3b  C[7]=4d57658d  D[7]=6050be81
```

```
Step 14: (r=22, s= 7)
A[0]=8ac39767  B[0]=d5b18e0e  C[0]=59a47271  D[0]=09d8f74d
A[1]=19239f4f  B[1]=e514a12a  C[1]=6c75225a  D[1]=7aeedd54
A[2]=88382c6a  B[2]=c8d05c34  C[2]=13a25a23  D[2]=3e3daac4
A[3]=9c44fdb3  B[3]=5cf7aaf4  C[3]=add41371  D[3]=e88e704e
A[4]=765c1e87  B[4]=d5974a51  C[4]=f0fd4d97  D[4]=75c6c3c8
A[5]=b03eed87  B[5]=ae52b0d5  C[5]=6aecd929  D[5]=e0f088e3
A[6]=9cc406ae  B[6]=f84222cf  C[6]=1ff5bdbc  D[6]=f6a740f2
A[7]=04b891b1  B[7]=66940db6  C[7]=038bba3b  D[7]=4d57658d

Step 15: (r= 7, s=28)
A[0]=65bdaffb  B[0]=61cbb3c5  C[0]=d5b18e0e  D[0]=59a47271
A[1]=3a069d3f  B[1]=91cfa78c  C[1]=e514a12a  D[1]=6c75225a
A[2]=5a7e2eec  B[2]=1c163544  C[2]=c8d05c34  D[2]=13a25a23
A[3]=22e0a7bd  B[3]=227ed9ce  C[3]=5cf7aaf4  D[3]=add41371
A[4]=e75bda40  B[4]=2e0f43bb  C[4]=d5974a51  D[4]=f0fd4d97
A[5]=560fb5b4  B[5]=1f76c3d8  C[5]=ae52b0d5  D[5]=6aecd929
A[6]=dddade89  B[6]=6203574e  C[6]=f84222cf  D[6]=1ff5bdbc
A[7]=576b2aee  B[7]=5c48d882  C[7]=66940db6  D[7]=038bba3b

Step 16: (r=29, s= 9)
A[0]=dbf7fa4b  B[0]=6cb7b5ff  C[0]=61cbb3c5  D[0]=d5b18e0e
A[1]=524eff9c  B[1]=e740d3a7  C[1]=91cfa78c  D[1]=e514a12a
A[2]=0d299f55  B[2]=8b4fc5dd  C[2]=1c163544  D[2]=c8d05c34
A[3]=511b7e01  B[3]=a45c14f7  C[3]=227ed9ce  D[3]=5cf7aaf4
A[4]=477add56  B[4]=1ceb7b48  C[4]=2e0f43bb  D[4]=d5974a51
A[5]=3022c5d9  B[5]=8ac1f6b6  C[5]=1f76c3d8  D[5]=ae52b0d5
A[6]=36baa91b  B[6]=3bbb5bd1  C[6]=6203574e  D[6]=f84222cf
A[7]=efb16127  B[7]=caed655d  C[7]=5c48d882  D[7]=66940db6

Step 17: (r= 9, s=15)
A[0]=7bc70b8e  B[0]=eff497b7  C[0]=6cb7b5ff  D[0]=61cbb3c5
A[1]=d76e72b0  B[1]=9dff38a4  C[1]=e740d3a7  D[1]=91cfa78c
A[2]=a9b012db  B[2]=533eaa1a  C[2]=8b4fc5dd  D[2]=1c163544
A[3]=048182ad  B[3]=36fc02a2  C[3]=a45c14f7  D[3]=227ed9ce
A[4]=8b18c582  B[4]=f5baac8e  C[4]=1ceb7b48  D[4]=2e0f43bb
A[5]=27eaee92  B[5]=458bb260  C[5]=8ac1f6b6  D[5]=1f76c3d8
A[6]=3a7f1477  B[6]=7552366d  C[6]=3bbb5bd1  D[6]=6203574e
A[7]=a74eee85  B[7]=62c24fdf  C[7]=caed655d  D[7]=5c48d882

Step 18: (r=15, s= 5)
A[0]=00a0abae  B[0]=85c73de3  C[0]=eff497b7  D[0]=6cb7b5ff
A[1]=619e6d93  B[1]=39586bb7  C[1]=9dff38a4  D[1]=e740d3a7
A[2]=15a603f4  B[2]=096dd4d8  C[2]=533eaa1a  D[2]=8b4fc5dd
A[3]=0a583aa2  B[3]=c1568240  C[3]=36fc02a2  D[3]=a45c14f7
A[4]=8399c286  B[4]=62c1458c  C[4]=f5baac8e  D[4]=1ceb7b48
A[5]=8e617b17  B[5]=774913f5  C[5]=458bb260  D[5]=8ac1f6b6
A[6]=00444ea0  B[6]=8a3b9d3f  C[6]=7552366d  D[6]=3bbb5bd1
```

```
A[7]=bc5bc096  B[7]=7742d3a7  C[7]=62c24fdf  D[7]=caed655d

Step 19: (r= 5, s=29)
A[0]=fc9ccbf4  B[0]=141575c0  C[0]=85c73de3  D[0]=eff497b7
A[1]=57ab290c  B[1]=33cdb26c  C[1]=39586bb7  D[1]=9dff38a4
A[2]=ae4f1c9c  B[2]=b4c07e82  C[2]=096dd4d8  D[2]=533eaa1a
A[3]=03938c0f  B[3]=4b075441  C[3]=c1568240  D[3]=36fc02a2
A[4]=27b68b16  B[4]=733850d0  C[4]=62c1458c  D[4]=f5baac8e
A[5]=c6a6fd17  B[5]=cc2f62f1  C[5]=774913f5  D[5]=458bb260
A[6]=1b91baa4  B[6]=0889d400  C[6]=8a3b9d3f  D[6]=7552366d
A[7]=10768232  B[7]=8b7812d7  C[7]=7742d3a7  D[7]=62c24fdf

Step 20: (r=29, s= 9)
A[0]=92ef0863  B[0]=9f93997e  C[0]=141575c0  D[0]=85c73de3
A[1]=a9090ec0  B[1]=8af56521  C[1]=33cdb26c  D[1]=39586bb7
A[2]=74bcd67f  B[2]=95c9e393  C[2]=b4c07e82  D[2]=096dd4d8
A[3]=ebbaf567  B[3]=e0727181  C[3]=4b075441  D[3]=c1568240
A[4]=2fd972cb  B[4]=c4f6d162  C[4]=733850d0  D[4]=62c1458c
A[5]=1863fbcf  B[5]=f8d4dfa2  C[5]=cc2f62f1  D[5]=774913f5
A[6]=5b79f33f  B[6]=83723754  C[6]=0889d400  D[6]=8a3b9d3f
A[7]=a41a7ef7  B[7]=420ed046  C[7]=8b7812d7  D[7]=7742d3a7

Step 21: (r= 9, s=15)
A[0]=69e4857e  B[0]=de10c725  C[0]=9f93997e  D[0]=141575c0
A[1]=39c50f65  B[1]=121d8152  C[1]=8af56521  D[1]=33cdb26c
A[2]=a5edacac  B[2]=79acfee9  C[2]=95c9e393  D[2]=b4c07e82
A[3]=9fc00ef9  B[3]=75eacfd7  C[3]=e0727181  D[3]=4b075441
A[4]=0a7993ef  B[4]=b2e5965f  C[4]=c4f6d162  D[4]=733850d0
A[5]=30ced0e0  B[5]=c7f79e30  C[5]=f8d4dfa2  D[5]=cc2f62f1
A[6]=ec7f3c69  B[6]=f3e67eb6  C[6]=83723754  D[6]=0889d400
A[7]=a5a3196d  B[7]=34fdef48  C[7]=420ed046  D[7]=8b7812d7

Step 22: (r=15, s= 5)
A[0]=9e92c65d  B[0]=42bf34f2  C[0]=de10c725  D[0]=9f93997e
A[1]=7b21bd43  B[1]=87b29ce2  C[1]=121d8152  D[1]=8af56521
A[2]=a8430151  B[2]=d65652f6  C[2]=79acfee9  D[2]=95c9e393
A[3]=c17b6394  B[3]=077ccfe0  C[3]=75eacfd7  D[3]=e0727181
A[4]=b94a1854  B[4]=c9f7853c  C[4]=b2e5965f  D[4]=c4f6d162
A[5]=c3f39212  B[5]=68701867  C[5]=c7f79e30  D[5]=f8d4dfa2
A[6]=9de59bfc  B[6]=9e34f63f  C[6]=f3e67eb6  D[6]=83723754
A[7]=83a4c0cc  B[7]=8cb6d2d1  C[7]=34fdef48  D[7]=420ed046

Step 23: (r= 5, s=29)
A[0]=30bfe1ce  B[0]=d258cbb3  C[0]=42bf34f2  D[0]=de10c725
A[1]=10f58fb4  B[1]=6437a86f  C[1]=87b29ce2  D[1]=121d8152
A[2]=7fab089d  B[2]=08602a35  C[2]=d65652f6  D[2]=79acfee9
A[3]=2edfd715  B[3]=2f6c7298  C[3]=077ccfe0  D[3]=75eacfd7
A[4]=228c601e  B[4]=29430a97  C[4]=c9f7853c  D[4]=b2e5965f
A[5]=00795c0c  B[5]=7e724258  C[5]=68701867  D[5]=c7f79e30
```

```
A[6]=51c68739  B[6]=bcb37f93  C[6]=9e34f63f  D[6]=f3e67eb6
A[7]=450ed68b  B[7]=74981990  C[7]=8cb6d2d1  D[7]=34fdef48

Step 24: (r= 4, s=13)
A[0]=6de1e538  B[0]=0bfe1ce3  C[0]=d258cbb3  D[0]=42bf34f2
A[1]=8adfdb12  B[1]=0f58fb41  C[1]=6437a86f  D[1]=87b29ce2
A[2]=56e0fb85  B[2]=fab089d7  C[2]=08602a35  D[2]=d65652f6
A[3]=6bc3e527  B[3]=edfd7152  C[3]=2f6c7298  D[3]=077ccfe0
A[4]=3db467d9  B[4]=28c601e2  C[4]=29430a97  D[4]=c9f7853c
A[5]=da0deca9  B[5]=0795c0c0  C[5]=7e724258  D[5]=68701867
A[6]=20f69a3e  B[6]=1c687395  C[6]=bcb37f93  D[6]=9e34f63f
A[7]=fe6ea301  B[7]=50ed68b4  C[7]=74981990  D[7]=8cb6d2d1

Step 25: (r=13, s=10)
A[0]=1b60e15e  B[0]=3ca70dbc  C[0]=0bfe1ce3  D[0]=d258cbb3
A[1]=aa062cf7  B[1]=fb62515b  C[1]=0f58fb41  D[1]=6437a86f
A[2]=622c9cbc  B[2]=1f70aadc  C[2]=fab089d7  D[2]=08602a35
A[3]=ac643e93  B[3]=7ca4ed78  C[3]=edfd7152  D[3]=2f6c7298
A[4]=2861a0dd  B[4]=8cfb27b6  C[4]=28c601e2  D[4]=29430a97
A[5]=9879dc4b  B[5]=bd953b41  C[5]=0795c0c0  D[5]=7e724258
A[6]=e2df4f73  B[6]=d347c41e  C[6]=1c687395  D[6]=bcb37f93
A[7]=782887d8  B[7]=d4603fcd  C[7]=50ed68b4  D[7]=74981990

Step 26: (r=10, s=25)
A[0]=50a9c759  B[0]=8385786d  C[0]=3ca70dbc  D[0]=0bfe1ce3
A[1]=009ae7e0  B[1]=18b3dea8  C[1]=fb62515b  D[1]=0f58fb41
A[2]=cb471f7a  B[2]=b272f188  C[2]=1f70aadc  D[2]=fab089d7
A[3]=ae7ebd32  B[3]=90fa4eb1  C[3]=7ca4ed78  D[3]=edfd7152
A[4]=a8044923  B[4]=868374a1  C[4]=8cfb27b6  D[4]=28c601e2
A[5]=41e6c63a  B[5]=e7712e61  C[5]=bd953b41  D[5]=0795c0c0
A[6]=96a59433  B[6]=7d3dcf8b  C[6]=d347c41e  D[6]=1c687395
A[7]=383b79d3  B[7]=a21f61e0  C[7]=d4603fcd  D[7]=50ed68b4

Step 27: (r=25, s= 4)
A[0]=39730a68  B[0]=b2a1538e  C[0]=8385786d  D[0]=3ca70dbc
A[1]=84732540  B[1]=c00135cf  C[1]=18b3dea8  D[1]=fb62515b
A[2]=174f20d3  B[2]=f5968e3e  C[2]=b272f188  D[2]=1f70aadc
A[3]=68c58ea9  B[3]=655cfd7a  C[3]=90fa4eb1  D[3]=7ca4ed78
A[4]=97327597  B[4]=47500892  C[4]=868374a1  D[4]=8cfb27b6
A[5]=7a405d72  B[5]=7483cd8c  C[5]=e7712e61  D[5]=bd953b41
A[6]=802c14cb  B[6]=672d4b28  C[6]=7d3dcf8b  D[6]=d347c41e
A[7]=13a635cb  B[7]=a67076f3  C[7]=a21f61e0  D[7]=d4603fcd

Step 28: (r= 4, s=13)
A[0]=0169de77  B[0]=9730a683  C[0]=b2a1538e  D[0]=8385786d
A[1]=32353234  B[1]=47325408  C[1]=c00135cf  D[1]=18b3dea8
A[2]=efa303f4  B[2]=74f20d31  C[2]=f5968e3e  D[2]=b272f188
A[3]=ecb28a04  B[3]=8c58ea96  C[3]=655cfd7a  D[3]=90fa4eb1
A[4]=51c1a0d3  B[4]=73275979  C[4]=47500892  D[4]=868374a1
```

```
A[5]=ebf8016e  B[5]=a405d727  C[5]=7483cd8c  D[5]=e7712e61
A[6]=87c48c82  B[6]=02c14cb8  C[6]=672d4b28  D[6]=7d3dcf8b
A[7]=d19db16a  B[7]=3a635cb1  C[7]=a67076f3  D[7]=a21f61e0

Step 29: (r=13, s=10)
A[0]=f3fdf3a1  B[0]=3bcee02d  C[0]=9730a683  D[0]=b2a1538e
A[1]=92de1ba5  B[1]=a6468646  C[1]=47325408  D[1]=c00135cf
A[2]=36bc3641  B[2]=607e9df4  C[2]=74f20d31  D[2]=f5968e3e
A[3]=7c3dd3b9  B[3]=51409d96  C[3]=8c58ea96  D[3]=655cfd7a
A[4]=59011681  B[4]=341a6a38  C[4]=73275979  D[4]=47500892
A[5]=5e39632e  B[5]=002ddd7f  C[5]=a405d727  D[5]=7483cd8c
A[6]=26d39dc8  B[6]=919050f8  C[6]=02c14cb8  D[6]=672d4b28
A[7]=f72016d7  B[7]=b62d5a33  C[7]=3a635cb1  D[7]=a67076f3

Step 30: (r=10, s=25)
A[0]=3d59cf0a  B[0]=f7ce87cf  C[0]=3bcee02d  D[0]=9730a683
A[1]=53ac40c7  B[1]=786e964b  C[1]=a6468646  D[1]=47325408
A[2]=cdffdee4  B[2]=f0d904da  C[2]=607e9df4  D[2]=74f20d31
A[3]=bc0609d3  B[3]=f74ee5f0  C[3]=51409d96  D[3]=8c58ea96
A[4]=81f9fcae  B[4]=045a0564  C[4]=341a6a38  D[4]=73275979
A[5]=ad41d765  B[5]=e58cb978  C[5]=002ddd7f  D[5]=a405d727
A[6]=8677fb90  B[6]=4e77209b  C[6]=919050f8  D[6]=02c14cb8
A[7]=c3765a48  B[7]=805b5fdc  C[7]=b62d5a33  D[7]=3a635cb1

Step 31: (r=25, s= 4)
A[0]=882a3b1d  B[0]=147ab39e  C[0]=f7ce87cf  D[0]=3bcee02d
A[1]=b9971563  B[1]=8ea75881  C[1]=786e964b  D[1]=a6468646
A[2]=e6276250  B[2]=c99bffbd  C[2]=f0d904da  D[2]=607e9df4
A[3]=3d083336  B[3]=a7780c13  C[3]=f74ee5f0  D[3]=51409d96
A[4]=0b2dfcc0  B[4]=5d03f3f9  C[4]=045a0564  D[4]=341a6a38
A[5]=d597341c  B[5]=cb5a83ae  C[5]=e58cb978  D[5]=002ddd7f
A[6]=f4580d9a  B[6]=210ceff7  C[6]=4e77209b  D[6]=919050f8
A[7]=e6358957  B[7]=9186ecb4  C[7]=805b5fdc  D[7]=b62d5a33

Feed-Forward Step 32: (r= 4, s=13)
A[0]=50f61355  B[0]=82a3b1d8  C[0]=147ab39e  D[0]=f7ce87cf
A[1]=1eb3dbe6  B[1]=9971563b  C[1]=8ea75881  D[1]=786e964b
A[2]=393530f0  B[2]=6276250e  C[2]=c99bffbd  D[2]=f0d904da
A[3]=1b450184  B[3]=d0833363  C[3]=a7780c13  D[3]=f74ee5f0
A[4]=426b96cd  B[4]=b2dfcc00  C[4]=5d03f3f9  D[4]=045a0564
A[5]=c9f4f827  B[5]=597341cd  C[5]=cb5a83ae  D[5]=e58cb978
A[6]=32077386  B[6]=4580d9af  C[6]=210ceff7  D[6]=4e77209b
A[7]=960c2832  B[7]=6358957e  C[7]=9186ecb4  D[7]=805b5fdc

Feed-Forward Step 33: (r=13, s=10)
A[0]=200c0162  B[0]=c26aaa1e  C[0]=82a3b1d8  D[0]=147ab39e
A[1]=a2110540  B[1]=7b7cc3d6  C[1]=9971563b  D[1]=8ea75881
A[2]=236a9583  B[2]=a61e0726  C[2]=6276250e  D[2]=c99bffbd
A[3]=b0546d61  B[3]=a0308368  C[3]=d0833363  D[3]=a7780c13
```

```
A[4]=21422a56  B[4]=72d9a84d  C[4]=b2dfcc00  D[4]=5d03f3f9
A[5]=4ed2444e  B[5]=9f04f93e  C[5]=597341cd  D[5]=cb5a83ae
A[6]=dbab59b7  B[6]=ee70c640  C[6]=4580d9af  D[6]=210ceff7
A[7]=e0a324f2  B[7]=850652c1  C[7]=6358957e  D[7]=9186ecb4

Feed-Forward Step 34: (r=10, s=25)
A[0]=33d2cae5  B[0]=30058880  C[0]=c26aaa1e  D[0]=82a3b1d8
A[1]=ad057027  B[1]=44150288  C[1]=7b7cc3d6  D[1]=9971563b
A[2]=1882de2c  B[2]=aa560c8d  C[2]=a61e0726  D[2]=6276250e
A[3]=1732d6b7  B[3]=51b586c1  C[3]=a0308368  D[3]=d0833363
A[4]=066ecef5  B[4]=08a95885  C[4]=72d9a84d  D[4]=b2dfcc00
A[5]=0785e3d6  B[5]=4911393b  C[5]=9f04f93e  D[5]=597341cd
A[6]=f829efcd  B[6]=ad66df6e  C[6]=ee70c640  D[6]=4580d9af
A[7]=c14f1ef9  B[7]=8c93cb82  C[7]=850652c1  D[7]=6358957e

Feed-Forward Step 35: (r=25, s= 4)
A[0]=9937f49f  B[0]=ca67a595  C[0]=30058880  D[0]=c26aaa1e
A[1]=892bf041  B[1]=4f5a0ae0  C[1]=44150288  D[1]=7b7cc3d6
A[2]=f29ce04b  B[2]=583105bc  C[2]=aa560c8d  D[2]=a61e0726
A[3]=1808d2ab  B[3]=6e2e65ad  C[3]=51b586c1  D[3]=a0308368
A[4]=df86b3e7  B[4]=ea0cdd9d  C[4]=08a95885  D[4]=72d9a84d
A[5]=c822f081  B[5]=ac0f0bc7  C[5]=4911393b  D[5]=9f04f93e
A[6]=f587a738  B[6]=9bf053df  C[6]=ad66df6e  D[6]=ee70c640
A[7]=b6edbe48  B[7]=f3829e3d  C[7]=8c93cb82  D[7]=850652c1
```

Compression Function Output

```
A[0]=9937f49f  B[0]=ca67a595  C[0]=30058880  D[0]=c26aaa1e
A[1]=892bf041  B[1]=4f5a0ae0  C[1]=44150288  D[1]=7b7cc3d6
A[2]=f29ce04b  B[2]=583105bc  C[2]=aa560c8d  D[2]=a61e0726
A[3]=1808d2ab  B[3]=6e2e65ad  C[3]=51b586c1  D[3]=a0308368
A[4]=df86b3e7  B[4]=ea0cdd9d  C[4]=08a95885  D[4]=72d9a84d
A[5]=c822f081  B[5]=ac0f0bc7  C[5]=4911393b  D[5]=9f04f93e
A[6]=f587a738  B[6]=9bf053df  C[6]=ad66df6e  D[6]=ee70c640
A[7]=b6edbe48  B[7]=f3829e3d  C[7]=8c93cb82  D[7]=850652c1
```

Final block

```
M[  0..  7] = 37 04 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
```

```
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  61  165  253   25  100  103   38  217
y[  8.. 15] =  83  222  217   81  155  191  230   68
y[ 16.. 23] = 160   84  131  211  120  256   67  256
y[ 24.. 31] =  70  153   56  134  184   54   47  116
y[ 32.. 39] =   3  142  144  243   16   32   20   71
y[ 40.. 47] =  63   73  194  216  243  207  172  210
y[ 48.. 55] = 183  243   53   83  146   42  138  255
y[ 56.. 63] = 108  123  230   72  215  135    9   14
y[ 64.. 71] = 119  197   87   94   48   28  240   38
y[ 72.. 79] =  57  190   59  107  148  226  117  121
y[ 80.. 87] = 177  224  217  112   89  175   90   39
y[ 88.. 95] =  72  226   62  109  209  193  100  189
y[ 96..103] = 243  143  181  173  213  195   59  237
y[104..111] = 200   30   90  227   52  251   86   58
y[112..119] =  43   98  145   86  103  101  123  134
y[120..127] =  12   87   90  153  210  217   69   88
y[128..135] =  49  202  114   85   10    7   72  150
y[136..143] =  27  145  150   29  212  176  137   42
y[144..151] = 207   26  236  156  247  111   43  111
y[152..159] =  40  214   54  233  183   56   63  251
y[160..167] = 107  225  223  124   94   78   90   39
y[168..175] =  47   37  173  151  124  160  195  157
y[176..183] = 184  124   57   27  221   68  229  112
y[184..191] =   2  244  137   38  152  232  101   96
y[192..199] = 248  170   23   16   62   82  127   72
y[200..207] =  53  177   51    3  219  141  250  246
y[208..215] = 190  143  150  255   21  192   20   71
y[216..223] =  38  141   48    1  158  174   10  178
y[224..231] = 124  224  186  194  154  172   51  130
y[232..239] = 167   80   20  140   58  116   24   52
y[240..247] =  67   12  222   24    7    9  244  233
y[248..255] =  98   23   20  214  157  150   41   22
```

Intermediate Expanded Message

```
Z[ 0] = bd842c15  1211fd1c  4a6f4844  e3181b76
        e6b53bfb  3a89e318  d04eb64a  3124ec7d
Z[ 1] = 3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
        b4d83296  a71d2878  2706cb3f  53d421f7
Z[ 2] = ace5022b  f5e2ae57  17200b90  334f0e74
        34c12d87  e25fd279  dbdef5e2  de09c293
Z[ 3] = f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
        58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
```

```
Z[ 4] = d4a455ff  43ee3edf  143c22b0  1b76f3b7
        cf952931  4d532aa3  e999b13b  5771548d
Z[ 5] = e827c630  50f0e318  c4be4051  1c2f410a
        e9993408  4ec52cce  d1c0dd50  cedc4844
Z[ 6] = ad9ef5e2  c34cc914  d332e034  f18c2aa3
        15aed6cf  ea52410a  fbaa2594  29ea3e26
Z[ 7] = 46d21f13  3e26af10  48fd4a6f  a71d58e3
        3edf08ac  b4d8410a  e318de09  3f9831dd
Z[ 8] = d8412369  3d6d5262  050f073a  b2ad3408
        af101383  14f5b2ad  c577df7b  1e5aa948
Z[ 9] = 12cadbde  b703f0d3  5037f8c6  50371f13
        e0ed1ce8  eea82706  2878ca86  fbaa2d87
Z[10] = e8e04d53  599ce76e  385e43ee  1c2f410a
        1abd21f7  b366c34c  b9e7599c  b7bcd332
Z[11] = 599ccb3f  13832931  3124e5fc  50f0ebc4
        f69b0172  1b76a948  edefb41f  456048fd
Z[12] = c121f97f  0b90109f  3b422cce  34085bc7
        c630264d  022b24db  ac2ce48a  f80dfaf1
Z[13] = ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
        ac2c1b76  00b922b0  c405b875  c6e9073a
Z[14] = e827599c  d279ccb1  c293b591  a43924db
        39d0bef6  ab730e74  53d429ea  25941158
Z[15] = 08ac306b  1158e6b5  0681050f  eea8f69b
        109f46d2  e0ed0e74  b2adb7bc  0fe61da1
Z[16] = 2c993785  67c2fc5c  091a5b04  41882296
        18934b8b  9e9ddb98  d70ba32a  92c8e76d
Z[17] = d27ea7b7  ece38d52  f6e66d38  27233cfb
        24683fb6  312632f8  bca6bd8f  39572ac7
Z[18] = 616302bb  e10e9927  558e0e90  51ea1234
        2ac73957  b38cc6a9  70dcf342  c792b2a3
Z[19] = bd8fbca6  33e1303d  df3c9af9  e68493b1
        01d2624c  92c8e76d  a06fd9c6  5bed0831
Z[20] = f7cf6c4f  14ef4f2f  386e2bb0  7397f087
        303d33e1  2e6b35b3  dd6a9ccb  f9a16a7d
Z[21] = c305b730  9e9ddb98  131d5101  123451ea
        22964188  2bb0386e  a5e5d450  091a5b04
Z[22] = 70dcf342  bf61bad4  a241d7f4  2e6b35b3
        ae16cc1f  123451ea  34ca2f54  15d84e46
Z[23] = 3cfb2723  e0259a10  065f5dbf  f42b6ff3
        59320aec  123451ea  a4fcd539  25513ecd
Z[24] = cdf1ac44  4d5d16c1  065f5dbf  9e9ddb98
        9a10e025  1a6549b9  b647c3ee  263a3de4
Z[25] = 17aa4c74  a413d622  6507ff17  6507ff17
        d8dda158  ea28900d  32f83126  fa8a6994
Z[26] = e2e09755  70dcf342  46fe1d20  237f409f
        21ad4271  9f86daaf  a7b7d27e  a4fcd539
Z[27] = 70dcf342  18934b8b  3de4263a  65f0fe2e
        f42b6ff3  22964188  e93f90f6  57600cbe
Z[28] = b0d1c964  0e90558e  4aa2197c  41882296
```

```
         b730c305  02bb6163  966ce3c9  f5fd6e21
Z[29] =  983ee1f7  fe2e65f0  c4d7b55e  409f237f
         966ce3c9  00e96335  b475c5c0  b819c21c
Z[30] =  e1f7983e  c6a9b38c  b2a3c792  8c69edcc
         48d01b4e  9583e4b2  6994fa8a  2f5434ca
Z[31] =  0aec5932  15d84e46  08315bed  ea28900d
         14ef4f2f  d8dda158  9e9ddb98  14065018
```

Expanded Message

```
W[ 0] =  d4a455ff  43ee3edf  143c22b0  1b76f3b7
         cf952931  4d532aa3  e999b13b  5771548d
W[ 1] =  ad9ef5e2  c34cc914  d332e034  f18c2aa3
         15aed6cf  ea52410a  fbaa2594  29ea3e26
W[ 2] =  bd842c15  1211fd1c  4a6f4844  e3181b76
         e6b53bfb  3a89e318  d04eb64a  3124ec7d
W[ 3] =  ace5022b  f5e2ae57  17200b90  334f0e74
         34c12d87  e25fd279  dbdef5e2  de09c293
W[ 4] =  46d21f13  3e26af10  48fd4a6f  a71d58e3
         3edf08ac  b4d8410a  e318de09  3f9831dd
W[ 5] =  e827c630  50f0e318  c4be4051  1c2f410a
         e9993408  4ec52cce  d1c0dd50  cedc4844
W[ 6] =  f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
         58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
W[ 7] =  3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
         b4d83296  a71d2878  2706cb3f  53d421f7
W[ 8] =  08ac306b  1158e6b5  0681050f  eea8f69b
         109f46d2  e0ed0e74  b2adb7bc  0fe61da1
W[ 9] =  599ccb3f  13832931  3124e5fc  50f0ebc4
         f69b0172  1b76a948  edefb41f  456048fd
W[10] =  c121f97f  0b90109f  3b422cce  34085bc7
         c630264d  022b24db  ac2ce48a  f80dfaf1
W[11] =  d8412369  3d6d5262  050f073a  b2ad3408
         af101383  14f5b2ad  c577df7b  1e5aa948
W[12] =  12cadbde  b703f0d3  5037f8c6  50371f13
         e0ed1ce8  eea82706  2878ca86  fbaa2d87
W[13] =  ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
         ac2c1b76  00b922b0  c405b875  c6e9073a
W[14] =  e8e04d53  599ce76e  385e43ee  1c2f410a
         1abd21f7  b366c34c  b9e7599c  b7bcd332
W[15] =  e827599c  d279ccb1  c293b591  a43924db
         39d0bef6  ab730e74  53d429ea  25941158
W[16] =  d27ea7b7  ece38d52  f6e66d38  27233cfb
         24683fb6  312632f8  bca6bd8f  39572ac7
W[17] =  616302bb  e10e9927  558e0e90  51ea1234
         2ac73957  b38cc6a9  70dcf342  c792b2a3
W[18] =  3cfb2723  e0259a10  065f5dbf  f42b6ff3
         59320aec  123451ea  a4fcd539  25513ecd
W[19] =  f7cf6c4f  14ef4f2f  386e2bb0  7397f087
```

```
        303d33e1  2e6b35b3  dd6a9ccb  f9a16a7d
W[20] = 70dcf342  bf61bad4  a241d7f4  2e6b35b3
        ae16cc1f  123451ea  34ca2f54  15d84e46
W[21] = c305b730  9e9ddb98  131d5101  123451ea
        22964188  2bb0386e  a5e5d450  091a5b04
W[22] = 2c993785  67c2fc5c  091a5b04  41882296
        18934b8b  9e9ddb98  d70ba32a  92c8e76d
W[23] = bd8fbca6  33e1303d  df3c9af9  e68493b1
        01d2624c  92c8e76d  a06fd9c6  5bed0831
W[24] = e1f7983e  c6a9b38c  b2a3c792  8c69edcc
        48d01b4e  9583e4b2  6994fa8a  2f5434ca
W[25] = cdf1ac44  4d5d16c1  065f5dbf  9e9ddb98
        9a10e025  1a6549b9  b647c3ee  263a3de4
W[26] = 17aa4c74  a413d622  6507ff17  6507ff17
        d8dda158  ea28900d  32f83126  fa8a6994
W[27] = 0aec5932  15d84e46  08315bed  ea28900d
        14ef4f2f  d8dda158  9e9ddb98  14065018
W[28] = 70dcf342  18934b8b  3de4263a  65f0fe2e
        f42b6ff3  22964188  e93f90f6  57600cbe
W[29] = 983ee1f7  fe2e65f0  c4d7b55e  409f237f
        966ce3c9  00e96335  b475c5c0  b819c21c
W[30] = b0d1c964  0e90558e  4aa2197c  41882296
        b730c305  02bb6163  966ce3c9  f5fd6e21
W[31] = e2e09755  70dcf342  46fe1d20  237f409f
        21ad4271  9f86daaf  a7b7d27e  a4fcd539
```

Feistel Steps

```
IV :
A[0]=9937f49f  B[0]=ca67a595  C[0]=30058880  D[0]=c26aaa1e
A[1]=892bf041  B[1]=4f5a0ae0  C[1]=44150288  D[1]=7b7cc3d6
A[2]=f29ce04b  B[2]=583105bc  C[2]=aa560c8d  D[2]=a61e0726
A[3]=1808d2ab  B[3]=6e2e65ad  C[3]=51b586c1  D[3]=a0308368
A[4]=df86b3e7  B[4]=ea0cdd9d  C[4]=08a95885  D[4]=72d9a84d
A[5]=c822f081  B[5]=ac0f0bc7  C[5]=4911393b  D[5]=9f04f93e
A[6]=f587a738  B[6]=9bf053df  C[6]=ad66df6e  D[6]=ee70c640
A[7]=b6edbe48  B[7]=f3829e3d  C[7]=8c93cb82  D[7]=850652c1

IV XOR M :
A[0]=9937f0a8  B[0]=ca67a595  C[0]=30058880  D[0]=c26aaa1e
A[1]=892bf041  B[1]=4f5a0ae0  C[1]=44150288  D[1]=7b7cc3d6
A[2]=f29ce04b  B[2]=583105bc  C[2]=aa560c8d  D[2]=a61e0726
A[3]=1808d2ab  B[3]=6e2e65ad  C[3]=51b586c1  D[3]=a0308368
A[4]=df86b3e7  B[4]=ea0cdd9d  C[4]=08a95885  D[4]=72d9a84d
A[5]=c822f081  B[5]=ac0f0bc7  C[5]=4911393b  D[5]=9f04f93e
A[6]=f587a738  B[6]=9bf053df  C[6]=ad66df6e  D[6]=ee70c640
A[7]=b6edbe48  B[7]=f3829e3d  C[7]=8c93cb82  D[7]=850652c1

Step  0: (r= 3, s=23)
```

```
A[0]=97ff1d60  B[0]=c9bf8544  C[0]=ca67a595  D[0]=30058880
A[1]=8845c9c6  B[1]=495f820c  C[1]=4f5a0ae0  D[1]=44150288
A[2]=f14feb73  B[2]=94e7025f  C[2]=583105bc  D[2]=aa560c8d
A[3]=98e9b4bd  B[3]=c0469558  C[3]=6e2e65ad  D[3]=51b586c1
A[4]=c29dd263  B[4]=fc359f3e  C[4]=ea0cdd9d  D[4]=08a95885
A[5]=ca7054d4  B[5]=4117840e  C[5]=ac0f0bc7  D[5]=4911393b
A[6]=2426e7ae  B[6]=ac3d39c7  C[6]=9bf053df  D[6]=ad66df6e
A[7]=1888bf0a  B[7]=b76df245  C[7]=f3829e3d  D[7]=8c93cb82

Step  1: (r=23, s=17)
A[0]=1f81623b  B[0]=b04bff8e  C[0]=c9bf8544  D[0]=ca67a595
A[1]=208cf1e1  B[1]=e34422e4  C[1]=495f820c  D[1]=4f5a0ae0
A[2]=19217ae8  B[2]=b9f8a7f5  C[2]=94e7025f  D[2]=583105bc
A[3]=775d8b3b  B[3]=5ecc74da  C[3]=c0469558  D[3]=6e2e65ad
A[4]=581cb4d0  B[4]=31e14ee9  C[4]=fc359f3e  D[4]=ea0cdd9d
A[5]=7165a3df  B[5]=6a65382a  C[5]=4117840e  D[5]=ac0f0bc7
A[6]=1dfed198  B[6]=d7121373  C[6]=ac3d39c7  D[6]=9bf053df
A[7]=5aff75f5  B[7]=850c445f  C[7]=b76df245  D[7]=f3829e3d

Step  2: (r=17, s=27)
A[0]=b8919009  B[0]=c4763f02  C[0]=b04bff8e  D[0]=c9bf8544
A[1]=5ccd0812  B[1]=e3c24119  C[1]=e34422e4  D[1]=495f820c
A[2]=7e7a7289  B[2]=f5d03242  C[2]=b9f8a7f5  D[2]=94e7025f
A[3]=ccfee5c4  B[3]=1676eebb  C[3]=5ecc74da  D[3]=c0469558
A[4]=d7575549  B[4]=69a0b039  C[4]=31e14ee9  D[4]=fc359f3e
A[5]=36233695  B[5]=47bee2cb  C[5]=6a65382a  D[5]=4117840e
A[6]=6aab4255  B[6]=a3303bfd  C[6]=d7121373  D[6]=ac3d39c7
A[7]=c60c8553  B[7]=ebeab5fe  C[7]=850c445f  D[7]=b76df245

Step  3: (r=27, s= 3)
A[0]=de602edd  B[0]=4dc48c80  C[0]=c4763f02  D[0]=b04bff8e
A[1]=64066e4d  B[1]=92e66840  C[1]=e3c24119  D[1]=e34422e4
A[2]=a1a4935d  B[2]=4bf3d394  C[2]=f5d03242  D[2]=b9f8a7f5
A[3]=9e294fb0  B[3]=2667f72e  C[3]=1676eebb  D[3]=5ecc74da
A[4]=32e79f9e  B[4]=4ebabaaa  C[4]=69a0b039  D[4]=31e14ee9
A[5]=3a4163a5  B[5]=a9b119b4  C[5]=47bee2cb  D[5]=6a65382a
A[6]=a41332b5  B[6]=ab555a12  C[6]=a3303bfd  D[6]=d7121373
A[7]=12be8c5c  B[7]=9e30642a  C[7]=ebeab5fe  D[7]=850c445f

Step  4: (r= 3, s=23)
A[0]=62ecde4f  B[0]=f30176ee  C[0]=4dc48c80  D[0]=c4763f02
A[1]=b5bf158e  B[1]=2033726b  C[1]=92e66840  D[1]=e3c24119
A[2]=7266d622  B[2]=0d249aed  C[2]=4bf3d394  D[2]=f5d03242
A[3]=dc27be8b  B[3]=f14a7d84  C[3]=2667f72e  D[3]=1676eebb
A[4]=482123f4  B[4]=973cfcf1  C[4]=4ebabaaa  D[4]=69a0b039
A[5]=5fa6ee5c  B[5]=d20b1d29  C[5]=a9b119b4  D[5]=47bee2cb
A[6]=09f91b9a  B[6]=209995ad  C[6]=ab555a12  D[6]=a3303bfd
A[7]=6a544a7a  B[7]=95f462e0  C[7]=9e30642a  D[7]=ebeab5fe
```

```
Step  5: (r=23, s=17)
A[0]=05354aea  B[0]=27b1766f  C[0]=f30176ee  D[0]=4dc48c80
A[1]=f5fcc762  B[1]=c75adf8a  C[1]=2033726b  D[1]=92e66840
A[2]=b89ddf61  B[2]=1139336b  C[2]=0d249aed  D[2]=4bf3d394
A[3]=58ca5ead  B[3]=45ee13df  C[3]=f14a7d84  D[3]=2667f72e
A[4]=845156c4  B[4]=fa241091  C[4]=973cfcf1  D[4]=4ebabaaa
A[5]=6ae417b9  B[5]=2e2fd377  C[5]=d20b1d29  D[5]=a9b119b4
A[6]=312a1d1e  B[6]=cd04fc8d  C[6]=209995ad  D[6]=ab555a12
A[7]=e90a28e5  B[7]=3d352a25  C[7]=95f462e0  D[7]=9e30642a

Step  6: (r=17, s=27)
A[0]=50dfcf11  B[0]=95d40a6a  C[0]=27b1766f  D[0]=f30176ee
A[1]=ed15b8f7  B[1]=8ec5ebf9  C[1]=c75adf8a  D[1]=2033726b
A[2]=6e58c34a  B[2]=bec3713b  C[2]=1139336b  D[2]=0d249aed
A[3]=3581da19  B[3]=bd5ab194  C[3]=45ee13df  D[3]=f14a7d84
A[4]=cfc29d56  B[4]=ad8908a2  C[4]=fa241091  D[4]=973cfcf1
A[5]=e10534e4  B[5]=2f72d5c8  C[5]=2e2fd377  D[5]=d20b1d29
A[6]=ea651805  B[6]=3a3c6254  C[6]=cd04fc8d  D[6]=209995ad
A[7]=4086c640  B[7]=51cbd214  C[7]=3d352a25  D[7]=95f462e0

Step  7: (r=27, s= 3)
A[0]=ebc4a7c9  B[0]=8a86fe78  C[0]=95d40a6a  D[0]=27b1766f
A[1]=fce7993e  B[1]=bf68adc7  C[1]=8ec5ebf9  D[1]=c75adf8a
A[2]=1fd73752  B[2]=5372c61a  C[2]=bec3713b  D[2]=1139336b
A[3]=8654d27b  B[3]=c9ac0ed0  C[3]=bd5ab194  D[3]=45ee13df
A[4]=03b26a70  B[4]=b67e14ea  C[4]=ad8908a2  D[4]=fa241091
A[5]=f8fef117  B[5]=270829a7  C[5]=2f72d5c8  D[5]=2e2fd377
A[6]=902afdbb  B[6]=2f5328c0  C[6]=3a3c6254  D[6]=cd04fc8d
A[7]=09d55f99  B[7]=02043632  C[7]=51cbd214  D[7]=3d352a25

Step  8: (r=28, s=19)
A[0]=6329276d  B[0]=9ebc4a7c  C[0]=8a86fe78  D[0]=95d40a6a
A[1]=20d20e9e  B[1]=efce7993  C[1]=bf68adc7  D[1]=8ec5ebf9
A[2]=f5e97f0a  B[2]=21fd7375  C[2]=5372c61a  D[2]=bec3713b
A[3]=f2075c3a  B[3]=b8654d27  C[3]=c9ac0ed0  D[3]=bd5ab194
A[4]=e42b3b67  B[4]=003b26a7  C[4]=b67e14ea  D[4]=ad8908a2
A[5]=f636fe4f  B[5]=7f8fef11  C[5]=270829a7  D[5]=2f72d5c8
A[6]=972998c2  B[6]=b902afdb  C[6]=2f5328c0  D[6]=3a3c6254
A[7]=dea362e1  B[7]=909d55f9  C[7]=02043632  D[7]=51cbd214

Step  9: (r=19, s=22)
A[0]=01b63737  B[0]=3b6b1949  C[0]=9ebc4a7c  D[0]=8a86fe78
A[1]=a1301d29  B[1]=74f10690  C[1]=efce7993  D[1]=bf68adc7
A[2]=cd30125b  B[2]=f857af4b  C[2]=21fd7375  D[2]=5372c61a
A[3]=83a304cb  B[3]=e1d7903a  C[3]=b8654d27  D[3]=c9ac0ed0
A[4]=f7026218  B[4]=db3f2159  C[4]=003b26a7  D[4]=b67e14ea
A[5]=c37f7336  B[5]=f27fb1b7  C[5]=7f8fef11  D[5]=270829a7
A[6]=a8b78108  B[6]=c614b94c  C[6]=b902afdb  D[6]=2f5328c0
A[7]=f3899e13  B[7]=170ef51b  C[7]=909d55f9  D[7]=02043632
```

```
Step 10: (r=22, s= 7)
A[0]=9c898936  B[0]=cdc06d8d  C[0]=3b6b1949  D[0]=9ebc4a7c
A[1]=9284c820  B[1]=4a684c07  C[1]=74f10690  D[1]=efce7993
A[2]=139377c2  B[2]=96f34c04  C[2]=f857af4b  D[2]=21fd7375
A[3]=8b9a5068  B[3]=32e0e8c1  C[3]=e1d7903a  D[3]=b8654d27
A[4]=79acdd8e  B[4]=863dc098  C[4]=db3f2159  D[4]=003b26a7
A[5]=5bb00a74  B[5]=cdb0dfdc  C[5]=f27fb1b7  D[5]=7f8fef11
A[6]=180f7292  B[6]=422a2de0  C[6]=c614b94c  D[6]=b902afdb
A[7]=1dc14f9e  B[7]=84fce267  C[7]=170ef51b  D[7]=909d55f9

Step 11: (r= 7, s=28)
A[0]=fa7332a0  B[0]=44c49b4e  C[0]=cdc06d8d  D[0]=3b6b1949
A[1]=2fa998e4  B[1]=42641049  C[1]=4a684c07  D[1]=74f10690
A[2]=62c61379  B[2]=c9bbe109  C[2]=96f34c04  D[2]=f857af4b
A[3]=2496cd24  B[3]=cd283445  C[3]=32e0e8c1  D[3]=e1d7903a
A[4]=757cc1f9  B[4]=d66ec73c  C[4]=863dc098  D[4]=db3f2159
A[5]=9cacf127  B[5]=d8053a2d  C[5]=cdb0dfdc  D[5]=f27fb1b7
A[6]=f17187d7  B[6]=07b9490c  C[6]=422a2de0  D[6]=c614b94c
A[7]=5518501d  B[7]=e0a7cf0e  C[7]=84fce267  D[7]=170ef51b

Step 12: (r=28, s=19)
A[0]=5aea5cb2  B[0]=0fa7332a  C[0]=44c49b4e  D[0]=cdc06d8d
A[1]=fc5acb65  B[1]=42fa998e  C[1]=42641049  D[1]=4a684c07
A[2]=c29b2b29  B[2]=962c6137  C[2]=c9bbe109  D[2]=96f34c04
A[3]=73ea819b  B[3]=42496cd2  C[3]=cd283445  D[3]=32e0e8c1
A[4]=42160219  B[4]=9757cc1f  C[4]=d66ec73c  D[4]=863dc098
A[5]=35824f9d  B[5]=79cacf12  C[5]=d8053a2d  D[5]=cdb0dfdc
A[6]=cfac27c2  B[6]=7f17187d  C[6]=07b9490c  D[6]=422a2de0
A[7]=3535eed9  B[7]=d5518501  C[7]=e0a7cf0e  D[7]=84fce267

Step 13: (r=19, s=22)
A[0]=23fca206  B[0]=e592d752  C[0]=0fa7332a  D[0]=44c49b4e
A[1]=7d4c8878  B[1]=5b2fe2d6  C[1]=42fa998e  D[1]=42641049
A[2]=54a12ad0  B[2]=594e14d9  C[2]=962c6137  D[2]=c9bbe109
A[3]=78f40fb6  B[3]=0cdb9f54  C[3]=42496cd2  D[3]=cd283445
A[4]=7055077a  B[4]=10ca10b0  C[4]=9757cc1f  D[4]=d66ec73c
A[5]=c581ddea  B[5]=7ce9ac12  C[5]=79cacf12  D[5]=d8053a2d
A[6]=41a39014  B[6]=3e167d61  C[6]=7f17187d  D[6]=07b9490c
A[7]=376be642  B[7]=76c9a9af  C[7]=d5518501  D[7]=e0a7cf0e

Step 14: (r=22, s= 7)
A[0]=cbed24cc  B[0]=8188ff28  C[0]=e592d752  D[0]=0fa7332a
A[1]=39494a23  B[1]=1e1f5322  C[1]=5b2fe2d6  D[1]=42fa998e
A[2]=10c1212e  B[2]=b415284a  C[2]=594e14d9  D[2]=962c6137
A[3]=cc57bae3  B[3]=ed9e3d03  C[3]=0cdb9f54  D[3]=42496cd2
A[4]=3c2816f7  B[4]=de9c1541  C[4]=10ca10b0  D[4]=9757cc1f
A[5]=79815ac5  B[5]=7ab16077  C[5]=7ce9ac12  D[5]=79cacf12
A[6]=ec6b6999  B[6]=051068e4  C[6]=3e167d61  D[6]=7f17187d
```

```
A[7]=dc340a6b  B[7]=908ddaf9  C[7]=76c9a9af  D[7]=d5518501

Step 15: (r= 7, s=28)
A[0]=214a4536  B[0]=f6926665  C[0]=8188ff28  D[0]=e592d752
A[1]=2d0d7074  B[1]=a4a5119c  C[1]=1e1f5322  D[1]=5b2fe2d6
A[2]=3a9bcf0f  B[2]=60909708  C[2]=b415284a  D[2]=594e14d9
A[3]=cbe387cb  B[3]=2bdd71e6  C[3]=ed9e3d03  D[3]=0cdb9f54
A[4]=cf6ba108  B[4]=140b7b9e  C[4]=de9c1541  D[4]=10ca10b0
A[5]=05bb6643  B[5]=c0ad62bc  C[5]=7ab16077  D[5]=7ce9ac12
A[6]=86824129  B[6]=35b4ccf6  C[6]=051068e4  D[6]=3e167d61
A[7]=f19c43b0  B[7]=1a0535ee  C[7]=908ddaf9  D[7]=76c9a9af

Step 16: (r=29, s= 9)
A[0]=104de492  B[0]=c42948a6  C[0]=f6926665  D[0]=8188ff28
A[1]=ce82edf5  B[1]=85a1ae0e  C[1]=a4a5119c  D[1]=1e1f5322
A[2]=567bfc8f  B[2]=e75379e1  C[2]=60909708  D[2]=b415284a
A[3]=3dcdd0d5  B[3]=797c70f9  C[3]=2bdd71e6  D[3]=ed9e3d03
A[4]=d3dba6b8  B[4]=19ed7421  C[4]=140b7b9e  D[4]=de9c1541
A[5]=90b604c7  B[5]=60b76cc8  C[5]=c0ad62bc  D[5]=7ab16077
A[6]=b5351c21  B[6]=30d04825  C[6]=35b4ccf6  D[6]=051068e4
A[7]=ad942c48  B[7]=1e338876  C[7]=1a0535ee  D[7]=908ddaf9

Step 17: (r= 9, s=15)
A[0]=3e070f3e  B[0]=9bc92420  C[0]=c42948a6  D[0]=f6926665
A[1]=cc23f095  B[1]=05dbeb9d  C[1]=85a1ae0e  D[1]=a4a5119c
A[2]=5f09a3d8  B[2]=f7f91eac  C[2]=e75379e1  D[2]=60909708
A[3]=fc5e6192  B[3]=9ba1aa7b  C[3]=797c70f9  D[3]=2bdd71e6
A[4]=8e37a0f1  B[4]=b74d71a7  C[4]=19ed7421  D[4]=140b7b9e
A[5]=31447ae8  B[5]=6c098f21  C[5]=60b76cc8  D[5]=c0ad62bc
A[6]=7e986260  B[6]=6a38436a  C[6]=30d04825  D[6]=35b4ccf6
A[7]=8b0eacbf  B[7]=2858915b  C[7]=1e338876  D[7]=1a0535ee

Step 18: (r=15, s= 5)
A[0]=f44e5da3  B[0]=879f1f03  C[0]=9bc92420  D[0]=c42948a6
A[1]=1a4c108c  B[1]=f84ae611  C[1]=05dbeb9d  D[1]=85a1ae0e
A[2]=1fc9b392  B[2]=d1ec2f84  C[2]=f7f91eac  D[2]=e75379e1
A[3]=565289e3  B[3]=30c97e2f  C[3]=9ba1aa7b  D[3]=797c70f9
A[4]=99aa4b71  B[4]=d078c71b  C[4]=b74d71a7  D[4]=19ed7421
A[5]=fa3777c9  B[5]=3d7418a2  C[5]=6c098f21  D[5]=60b76cc8
A[6]=d20710b7  B[6]=31303f4c  C[6]=6a38436a  D[6]=30d04825
A[7]=43ead24f  B[7]=565fc587  C[7]=2858915b  D[7]=1e338876

Step 19: (r= 5, s=29)
A[0]=86cb4827  B[0]=89cbb47e  C[0]=879f1f03  D[0]=9bc92420
A[1]=17efb403  B[1]=49821183  C[1]=f84ae611  D[1]=05dbeb9d
A[2]=e92633e6  B[2]=f9367243  C[2]=d1ec2f84  D[2]=f7f91eac
A[3]=a6281faa  B[3]=ca513c6a  C[3]=30c97e2f  D[3]=9ba1aa7b
A[4]=ea643fdd  B[4]=35496e33  C[4]=d078c71b  D[4]=b74d71a7
A[5]=72a259a6  B[5]=46eef93f  C[5]=3d7418a2  D[5]=6c098f21
```

```
A[6]=d250788a  B[6]=40e216fa  C[6]=31303f4c  D[6]=6a38436a
A[7]=da11aaff  B[7]=7d5a49e8  C[7]=565fc587  D[7]=2858915b

Step 20: (r=29, s= 9)
A[0]=9fb39b23  B[0]=f0d96904  C[0]=89cbb47e  D[0]=879f1f03
A[1]=df093372  B[1]=62fdf680  C[1]=49821183  D[1]=f84ae611
A[2]=1c9edc37  B[2]=dd24c67c  C[2]=f9367243  D[2]=d1ec2f84
A[3]=a77ee637  B[3]=54c503f5  C[3]=ca513c6a  D[3]=30c97e2f
A[4]=8a332baf  B[4]=bd4c87fb  C[4]=35496e33  D[4]=d078c71b
A[5]=ab735a6a  B[5]=ce544b34  C[5]=46eef93f  D[5]=3d7418a2
A[6]=c287d85a  B[6]=5a4a0f11  C[6]=40e216fa  D[6]=31303f4c
A[7]=6e18252e  B[7]=fb42355f  C[7]=7d5a49e8  D[7]=565fc587

Step 21: (r= 9, s=15)
A[0]=5a13d7fe  B[0]=6736473f  C[0]=f0d96904  D[0]=89cbb47e
A[1]=61cc3877  B[1]=1266e5be  C[1]=62fdf680  D[1]=49821183
A[2]=294ad06e  B[2]=3db86e39  C[2]=dd24c67c  D[2]=f9367243
A[3]=b90072e2  B[3]=fdcc6f4e  C[3]=54c503f5  D[3]=ca513c6a
A[4]=02e42d82  B[4]=66575f14  C[4]=bd4c87fb  D[4]=35496e33
A[5]=bc7e7ae1  B[5]=e6b4d556  C[5]=ce544b34  D[5]=46eef93f
A[6]=494569c8  B[6]=0fb0b585  C[6]=5a4a0f11  D[6]=40e216fa
A[7]=32ada4ef  B[7]=304a5cdc  C[7]=fb42355f  D[7]=7d5a49e8

Step 22: (r=15, s= 5)
A[0]=c3ea8cc7  B[0]=ebff2d09  C[0]=6736473f  D[0]=f0d96904
A[1]=58b7ebf8  B[1]=1c3bb0e6  C[1]=1266e5be  D[1]=62fdf680
A[2]=05f379d9  B[2]=683714a5  C[2]=3db86e39  D[2]=dd24c67c
A[3]=71293b00  B[3]=39715c80  C[3]=fdcc6f4e  D[3]=54c503f5
A[4]=ec503eb3  B[4]=16c10172  C[4]=66575f14  D[4]=bd4c87fb
A[5]=b99765fa  B[5]=3d70de3f  C[5]=e6b4d556  D[5]=ce544b34
A[6]=51bc21b5  B[6]=b4e424a2  C[6]=0fb0b585  D[6]=5a4a0f11
A[7]=69e8776e  B[7]=d2779956  C[7]=304a5cdc  D[7]=fb42355f

Step 23: (r= 5, s=29)
A[0]=f0bc2177  B[0]=7d5198f8  C[0]=ebff2d09  D[0]=6736473f
A[1]=9b0a4125  B[1]=16fd7f0b  C[1]=1c3bb0e6  D[1]=1266e5be
A[2]=5a9434bd  B[2]=be6f3b20  C[2]=683714a5  D[2]=3db86e39
A[3]=ed93e1df  B[3]=2527600e  C[3]=39715c80  D[3]=fdcc6f4e
A[4]=5c3237d9  B[4]=8a07d67d  C[4]=16c10172  D[4]=66575f14
A[5]=20e92ed0  B[5]=32ecbf57  C[5]=3d70de3f  D[5]=e6b4d556
A[6]=0c15984c  B[6]=378436aa  C[6]=b4e424a2  D[6]=0fb0b585
A[7]=0bdff2b4  B[7]=3d0eedcd  C[7]=d2779956  D[7]=304a5cdc

Step 24: (r= 4, s=13)
A[0]=f6bcd68e  B[0]=0bc2177f  C[0]=7d5198f8  D[0]=ebff2d09
A[1]=faa509be  B[1]=b0a41259  C[1]=16fd7f0b  D[1]=1c3bb0e6
A[2]=1d6177a9  B[2]=a9434bd5  C[2]=be6f3b20  D[2]=683714a5
A[3]=46e72f72  B[3]=d93e1dfe  C[3]=2527600e  D[3]=39715c80
A[4]=101ae27d  B[4]=c3237d95  C[4]=8a07d67d  D[4]=16c10172
```

```
A[5]=f86a7c06  B[5]=0e92ed02  C[5]=32ecbf57  D[5]=3d70de3f
A[6]=4b2a12c7  B[6]=c15984c0  C[6]=378436aa  D[6]=b4e424a2
A[7]=729104ae  B[7]=bdff2b40  C[7]=3d0eedcd  D[7]=d2779956

Step 25: (r=13, s=10)
A[0]=17600e23  B[0]=9ad1ded7  C[0]=0bc2177f  D[0]=7d5198f8
A[1]=b146a27d  B[1]=a137df54  C[1]=b0a41259  D[1]=16fd7f0b
A[2]=b78d62b9  B[2]=2ef523ac  C[2]=a9434bd5  D[2]=be6f3b20
A[3]=186f4249  B[3]=e5ee48dc  C[3]=d93e1dfe  D[3]=2527600e
A[4]=068e903f  B[4]=5c4fa203  C[4]=c3237d95  D[4]=8a07d67d
A[5]=0f2f0c60  B[5]=4f80df0d  C[5]=0e92ed02  D[5]=32ecbf57
A[6]=c6242c5e  B[6]=4258e965  C[6]=c15984c0  D[6]=378436aa
A[7]=75f71085  B[7]=2095ce52  C[7]=bdff2b40  D[7]=3d0eedcd

Step 26: (r=10, s=25)
A[0]=73a191e0  B[0]=80388c5d  C[0]=9ad1ded7  D[0]=0bc2177f
A[1]=936aeae7  B[1]=1a89f6c5  C[1]=a137df54  D[1]=b0a41259
A[2]=02d5fd08  B[2]=358ae6de  C[2]=2ef523ac  D[2]=a9434bd5
A[3]=80d85794  B[3]=bd092461  C[3]=e5ee48dc  D[3]=d93e1dfe
A[4]=6d594f2b  B[4]=3a40fc1a  C[4]=5c4fa203  D[4]=c3237d95
A[5]=01e43356  B[5]=bc31803c  C[5]=4f80df0d  D[5]=0e92ed02
A[6]=43e5a2e6  B[6]=90b17b18  C[6]=4258e965  D[6]=c15984c0
A[7]=c3f8f962  B[7]=dc4215d7  C[7]=2095ce52  D[7]=bdff2b40

Step 27: (r=25, s= 4)
A[0]=48cea327  B[0]=c0e74323  C[0]=80388c5d  D[0]=9ad1ded7
A[1]=35a94fb5  B[1]=cf26d5d5  C[1]=1a89f6c5  D[1]=a137df54
A[2]=ade0b232  B[2]=1005abfa  C[2]=358ae6de  D[2]=2ef523ac
A[3]=4ed3972c  B[3]=2901b0af  C[3]=bd092461  D[3]=e5ee48dc
A[4]=c682d004  B[4]=56dab29e  C[4]=3a40fc1a  D[4]=5c4fa203
A[5]=283c7d48  B[5]=ac03c866  C[5]=bc31803c  D[5]=4f80df0d
A[6]=1b126190  B[6]=cc87cb45  C[6]=90b17b18  D[6]=4258e965
A[7]=4daadb5a  B[7]=c587f1f2  C[7]=dc4215d7  D[7]=2095ce52

Step 28: (r= 4, s=13)
A[0]=053d14e6  B[0]=8cea3274  C[0]=c0e74323  D[0]=80388c5d
A[1]=2d40cda2  B[1]=5a94fb53  C[1]=cf26d5d5  D[1]=1a89f6c5
A[2]=2ad5870f  B[2]=de0b232a  C[2]=1005abfa  D[2]=358ae6de
A[3]=fd721246  B[3]=ed3972c4  C[3]=2901b0af  D[3]=bd092461
A[4]=440a6969  B[4]=682d004c  C[4]=56dab29e  D[4]=3a40fc1a
A[5]=854d2415  B[5]=83c7d482  C[5]=ac03c866  D[5]=bc31803c
A[6]=575b2e29  B[6]=b1261901  C[6]=cc87cb45  D[6]=90b17b18
A[7]=c6c261b0  B[7]=daadb5a4  C[7]=c587f1f2  D[7]=dc4215d7

Step 29: (r=13, s=10)
A[0]=ffc81560  B[0]=a29cc0a7  C[0]=8cea3274  D[0]=c0e74323
A[1]=41203a76  B[1]=19b445a8  C[1]=5a94fb53  D[1]=cf26d5d5
A[2]=ee2ac0d2  B[2]=b0e1e55a  C[2]=de0b232a  D[2]=1005abfa
A[3]=0a6d4c54  B[3]=4248dfae  C[3]=ed3972c4  D[3]=2901b0af
```

```
A[4]=90e2a1ac  B[4]=4d2d2881  C[4]=682d004c  D[4]=56dab29e
A[5]=cce6bcb7  B[5]=a482b0a9  C[5]=83c7d482  D[5]=ac03c866
A[6]=5bcc250f  B[6]=65c52aeb  C[6]=b1261901  D[6]=cc87cb45
A[7]=a8dad313  B[7]=4c3618d8  C[7]=daadb5a4  D[7]=c587f1f2

Step 30: (r=10, s=25)
A[0]=81444df1  B[0]=205583ff  C[0]=a29cc0a7  D[0]=8cea3274
A[1]=5fa02776  B[1]=80e9d904  C[1]=19b445a8  D[1]=5a94fb53
A[2]=c1072b4c  B[2]=ab034bb8  C[2]=b0e1e55a  D[2]=de0b232a
A[3]=9453bf68  B[3]=b5315029  C[3]=4248dfae  D[3]=ed3972c4
A[4]=8f40ae9b  B[4]=8a86b243  C[4]=4d2d2881  D[4]=682d004c
A[5]=43b35a5f  B[5]=9af2df33  C[5]=a482b0a9  D[5]=83c7d482
A[6]=be3023f3  B[6]=30943d6f  C[6]=65c52aeb  D[6]=b1261901
A[7]=e1fb6716  B[7]=6b4c4ea3  C[7]=4c3618d8  D[7]=daadb5a4

Step 31: (r=25, s= 4)
A[0]=d321637f  B[0]=e302889b  C[0]=205583ff  D[0]=a29cc0a7
A[1]=eaa549f4  B[1]=ecbf404e  C[1]=80e9d904  D[1]=19b445a8
A[2]=4d89fa7a  B[2]=99820e56  C[2]=ab034bb8  D[2]=b0e1e55a
A[3]=33abb155  B[3]=d128a77e  C[3]=b5315029  D[3]=4248dfae
A[4]=bbb2cacf  B[4]=371e815d  C[4]=8a86b243  D[4]=4d2d2881
A[5]=4794f711  B[5]=be8766b4  C[5]=9af2df33  D[5]=a482b0a9
A[6]=95a8dd5c  B[6]=e77c6047  C[6]=30943d6f  D[6]=65c52aeb
A[7]=c9ac185b  B[7]=2dc3f6ce  C[7]=6b4c4ea3  D[7]=4c3618d8

Feed-Forward Step 32: (r= 4, s=13)
A[0]=a00b94f9  B[0]=321637fd  C[0]=e302889b  D[0]=205583ff
A[1]=7bf25e74  B[1]=aa549f4e  C[1]=ecbf404e  D[1]=80e9d904
A[2]=b4f06f9c  B[2]=d89fa7a4  C[2]=99820e56  D[2]=ab034bb8
A[3]=ad0893ba  B[3]=3abb1553  C[3]=d128a77e  D[3]=b5315029
A[4]=fbeb4b47  B[4]=bb2cacfb  C[4]=371e815d  D[4]=8a86b243
A[5]=b401b96e  B[5]=794f7114  C[5]=be8766b4  D[5]=9af2df33
A[6]=610c5564  B[6]=5a8dd5c9  C[6]=e77c6047  D[6]=30943d6f
A[7]=5e60ed80  B[7]=9ac185bc  C[7]=2dc3f6ce  D[7]=6b4c4ea3

Feed-Forward Step 33: (r=13, s=10)
A[0]=1aca4902  B[0]=729f3401  C[0]=321637fd  D[0]=e302889b
A[1]=0eb5561b  B[1]=4bce8f7e  C[1]=aa549f4e  D[1]=ecbf404e
A[2]=5112c0f3  B[2]=0df3969e  C[2]=d89fa7a4  D[2]=99820e56
A[3]=8915b1eb  B[3]=127755a1  C[3]=3abb1553  D[3]=d128a77e
A[4]=52d84270  B[4]=6968ff7d  C[4]=bb2cacfb  D[4]=371e815d
A[5]=337dd0a4  B[5]=372dd680  C[5]=794f7114  D[5]=be8766b4
A[6]=4fe8d5ca  B[6]=8aac8c21  C[6]=5a8dd5c9  D[6]=e77c6047
A[7]=bcb1ee6b  B[7]=1db00bcc  C[7]=9ac185bc  D[7]=2dc3f6ce

Feed-Forward Step 34: (r=10, s=25)
A[0]=91950ddb  B[0]=2924086b  C[0]=729f3401  D[0]=321637fd
A[1]=60f9c271  B[1]=d5586c3a  C[1]=4bce8f7e  D[1]=aa549f4e
A[2]=96f218c3  B[2]=4b03cd44  C[2]=0df3969e  D[2]=d89fa7a4
```

```
A[3]=a864e979  B[3]=56c7ae24  C[3]=127755a1  D[3]=3abb1553
A[4]=e37671fc  B[4]=6109c14b  C[4]=6968ff7d  D[4]=bb2cacfb
A[5]=d45dfd5c  B[5]=f74290cd  C[5]=372dd680  D[5]=794f7114
A[6]=b862eecb  B[6]=a357293f  C[6]=8aac8c21  D[6]=5a8dd5c9
A[7]=b07a3dc0  B[7]=c7b9aef2  C[7]=1db00bcc  D[7]=9ac185bc

Feed-Forward Step 35: (r=25, s= 4)
A[0]=5bb399e9  B[0]=b7232a1b  C[0]=2924086b  D[0]=729f3401
A[1]=ca1e3042  B[1]=e2c1f384  C[1]=d5586c3a  D[1]=4bce8f7e
A[2]=8f649c3a  B[2]=872de431  C[2]=4b03cd44  D[2]=0df3969e
A[3]=5b6339ef  B[3]=f350c9d2  C[3]=56c7ae24  D[3]=127755a1
A[4]=2a9b0513  B[4]=f9c6ece3  C[4]=6109c14b  D[4]=6968ff7d
A[5]=f516bec3  B[5]=b9a8bbfa  C[5]=f74290cd  D[5]=372dd680
A[6]=3e2d37c9  B[6]=9770c5dd  C[6]=a357293f  D[6]=8aac8c21
A[7]=6f713a77  B[7]=8160f47b  C[7]=c7b9aef2  D[7]=1db00bcc
```

Compression Function Output

```
A[0]=5bb399e9  B[0]=b7232a1b  C[0]=2924086b  D[0]=729f3401
A[1]=ca1e3042  B[1]=e2c1f384  C[1]=d5586c3a  D[1]=4bce8f7e
A[2]=8f649c3a  B[2]=872de431  C[2]=4b03cd44  D[2]=0df3969e
A[3]=5b6339ef  B[3]=f350c9d2  C[3]=56c7ae24  D[3]=127755a1
A[4]=2a9b0513  B[4]=f9c6ece3  C[4]=6109c14b  D[4]=6968ff7d
A[5]=f516bec3  B[5]=b9a8bbfa  C[5]=f74290cd  D[5]=372dd680
A[6]=3e2d37c9  B[6]=9770c5dd  C[6]=a357293f  D[6]=8aac8c21
A[7]=6f713a77  B[7]=8160f47b  C[7]=c7b9aef2  D[7]=1db00bcc
```

Hash Function Output

```
e999b35b42301eca3a9c648fef39635b13059b2ac3be16f5c9372d3e773a716f1b2a23b784f3c1e231e42d87d2c950f3
```

A.4 SIMD-512

A.4.1 Empty Message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
```

```
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    2  203  156   47  118  214  107  106
y[  8.. 15] =   45   93  212   20  111   73  162  251
y[ 16.. 23] =   97  215  249   53  211   19    3   89
y[ 24.. 31] =   49  207  101   67  151  130  223   23
y[ 32.. 39] =  189  202  178  239  253  127  204   49
y[ 40.. 47] =   76  236   82  137  232  157   65   79
y[ 48.. 55] =   96  161  176  130  161   30   47    9
y[ 56.. 63] =  189  247   61  226  248   90  107   64
y[ 64.. 71] =    0   88  131  243  133   59  113  115
y[ 72.. 79] =   17  236   33  213   12  191  111   19
y[ 80.. 87] =  251   61  103  208   57   35  148  248
y[ 88.. 95] =   47  116   65  119  249  178  143   40
y[ 96..103] =  189  129    8  163  204  227  230  196
y[104..111] =  205  122  151   45  187   19  227   72
y[112..119] =  247  125  111  121  140  220    6  107
y[120..127] =   77   69   10  101   21   65  149  171
y[128..135] =  255   54  101  210  139   43  150  151
y[136..143] =  212  164   45  237  146  184   95    6
y[144..151] =  160   42    8  204   46  238  254  168
y[152..159] =  208   50  156  190  106  127   34  234
y[160..167] =   68   55   79   18    4  130   53  208
y[168..175] =  181   21  175  120   25  100  192  178
y[176..183] =  161   96   81  127   96  227  210  248
y[184..191] =   68   10  196   31    9  167  150  193
y[192..199] =    0  169  126   14  124  198  144  142
y[200..207] =  240   21  224   44  245   66  146  238
y[208..215] =    6  196  154   49  200  222  109    9
y[216..223] =  210  141  192  138    8   79  114  217
y[224..231] =   68  128  249   94   53   30   27   61
y[232..239] =   52  135  106  212   70  238   30  185
y[240..247] =   10  132  146  136  117   37  251  150
y[248..255] =  180  188  247  156  236  192  108   86
```

Intermediate Expanded Message

```
Z[ 0] = d8fa0172  21f7b703  e0ed5546  4c9a4d53
        43352085  0e74df7b  34c15037  fbaabb59
Z[ 1] = e1a64619  264dfa38  0dbbdec2  4051022b
        dbde2369  306b48fd  a439b366  109fe76e
Z[ 2] = d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
        f0d336ec  a9483b42  b7bcedef  39172ef9
```

```
Z[ 3] = baa04560  a439c577  15aebaa0  068121f7
        f8c6cedc  e9992c15  410af97f  2e404d53
Z[ 4] = 3f980000  f5e2a4f2  2aa3a664  531b51a9
        f0d30c49  e03417d9  d04e08ac  0dbb5037
Z[ 5] = 2c15fbaa  dc974a6f  194b2931  f97fb13b
        53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
Z[ 6] = a380cedc  bc1205c8  ea52d9b3  d3ebec7d
        582ada6c  2085b366  0dbbcd6a  3408ea52
Z[ 7] = 5a55f8c6  57715037  e543ab73  4d530456
        31dd37a5  48fd073a  2ef90f2d  c1dab1f4
Z[ 8] = 2706fe8e  de0948fd  1f13aaba  b366b2ad
        bccbdf7b  f18c2085  cb3fafc9  045644a7
Z[ 9] = 1e5ab9e7  d9b305c8  f245213e  bfaffdd5
        2422dc97  cf95b703  5bc74c9a  ef611892
Z[10] = 27bf3124  0d023917  a43902e4  dc97264d
        0f2dc914  56b8c4be  48441211  c6e9d107
Z[11] = 4560baa0  5bc73a89  ea524560  f97fde09
        073a3124  1667d3eb  bef60681  d1c0b2ad
Z[12] = c0680000  0a1e5b0e  d55d599c  ace5ae57
        0f2df3b7  1fcce827  2fb2f754  f245afc9
Z[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
        ac2cde09  aa01d107  391705c8  e3185262
Z[14] = 5c803124  43eefa38  15ae264d  2c151383
        a7d62594  df7b4c9a  f2453296  cbf815ae
Z[15] = a5ab073a  a88fafc9  1abd548d  b2adfbaa
        ce23c85b  b703f8c6  d107f0d3  3e264e0c
Z[16] = fe2e01d2  5beda413  949a6b66  9e9d6163
        d70b28f5  28f5d70b  9af96507  5677a989
Z[17] = a7b75849  0748f8b8  29ded622  fd4502bb
        d3672c99  a4135bed  607a9f86  1ef2e10e
Z[18] = 3de4c21c  47e7b819  03a4fc5c  303dcfc3
        bad4452c  b55e4aa2  16c1e93f  c4d73b29
Z[19] = a8a05760  49b9b647  5760a8a0  d5392ac7
        3de4c21c  c87b3785  0831f7cf  9e9d6163
Z[20] = 00000000  72ae8d52  70dc8f24  992766d9
        f0870f79  e1f71e09  f5140aec  9af96507
Z[21] = 0576fa8a  a2415dbf  cc1f33e1  63359ccb
        d5392ac7  c4d73b29  0748f8b8  67c2983e
Z[22] = 3de4c21c  f8b80748  303dcfc3  1893e76d
        2f54d0ac  607a9f86  3fb6c04a  1b4ee4b2
Z[23] = 091af6e6  9af96507  6a7d9583  fa8a0576
        b9eb4615  f6e6091a  ece3131d  624c9db4
Z[24] = 3126ceda  d5392ac7  2723d8dd  9f86607a
        ab5b54a5  edcc1234  bd8f4271  0576fa8a
Z[25] = 263ad9c6  cfc3303d  eeb5114b  aeff5101
        2d82d27e  c3053cfb  73978c69  eb1114ef
Z[26] = 320fcdf1  1062ef9e  8c697397  d3672c99
        131dece3  6d3892c8  5b04a4fc  b81947e7
Z[27] = 5760a8a0  73978c69  e4b21b4e  f7cf0831
```

```
        091af6e6  1c37e3c9  ae1651ea  c5c03a40
Z[28] = afe85018  0cbef342  ca4d35b3  975568ab
        131dece3  280cd7f4  3c12c3ee  eeb5114b
Z[29] = c87b3785  2c99d367  e0251fdb  0831f7cf
        966c6994  93b16c4f  47e7b819  db982468
Z[30] = 74808b80  558eaa72  1b4ee4b2  3785c87b
        90f66f0a  d70b28f5  eeb5114b  be784188
Z[31] = 8e3b71c5  91df6e21  21adde53  9e9d6163
        c1333ecd  a4135bed  c4d73b29  4e46b1ba
```

Expanded Message

```
W[ 0] = 3f980000  f5e2a4f2  2aa3a664  531b51a9
        f0d30c49  e03417d9  d04e08ac  0dbb5037
W[ 1] = a380cedc  bc1205c8  ea52d9b3  d3ebec7d
        582ada6c  2085b366  0dbbcd6a  3408ea52
W[ 2] = d8fa0172  21f7b703  e0ed5546  4c9a4d53
        43352085  0e74df7b  34c15037  fbaabb59
W[ 3] = d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
        f0d336ec  a9483b42  b7bcedef  39172ef9
W[ 4] = 5a55f8c6  57715037  e543ab73  4d530456
        31dd37a5  48fd073a  2ef90f2d  c1dab1f4
W[ 5] = 2c15fbaa  dc974a6f  194b2931  f97fb13b
        53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
W[ 6] = baa04560  a439c577  15aebaa0  068121f7
        f8c6cedc  e9992c15  410af97f  2e404d53
W[ 7] = e1a64619  264dfa38  0dbbdec2  4051022b
        dbde2369  306b48fd  a439b366  109fe76e
W[ 8] = a5ab073a  a88fafc9  1abd548d  b2adfbaa
        ce23c85b  b703f8c6  d107f0d3  3e264e0c
W[ 9] = 4560baa0  5bc73a89  ea524560  f97fde09
        073a3124  1667d3eb  bef60681  d1c0b2ad
W[10] = c0680000  0a1e5b0e  d55d599c  ace5ae57
        0f2df3b7  1fcce827  2fb2f754  f245afc9
W[11] = 2706fe8e  de0948fd  1f13aaba  b366b2ad
        bccbdf7b  f18c2085  cb3fafc9  045644a7
W[12] = 1e5ab9e7  d9b305c8  f245213e  bfaffdd5
        2422dc97  cf95b703  5bc74c9a  ef611892
W[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
        ac2cde09  aa01d107  391705c8  e3185262
W[14] = 27bf3124  0d023917  a43902e4  dc97264d
        0f2dc914  56b8c4be  48441211  c6e9d107
W[15] = 5c803124  43eefa38  15ae264d  2c151383
        a7d62594  df7b4c9a  f2453296  cbf815ae
W[16] = a7b75849  0748f8b8  29ded622  fd4502bb
        d3672c99  a4135bed  607a9f86  1ef2e10e
W[17] = 3de4c21c  47e7b819  03a4fc5c  303dcfc3
        bad4452c  b55e4aa2  16c1e93f  c4d73b29
W[18] = 091af6e6  9af96507  6a7d9583  fa8a0576
```

```
          b9eb4615  f6e6091a  ece3131d  624c9db4
W[19] = 00000000  72ae8d52  70dc8f24  992766d9
          f0870f79  e1f71e09  f5140aec  9af96507
W[20] = 3de4c21c  f8b80748  303dcfc3  1893e76d
          2f54d0ac  607a9f86  3fb6c04a  1b4ee4b2
W[21] = 0576fa8a  a2415dbf  cc1f33e1  63359ccb
          d5392ac7  c4d73b29  0748f8b8  67c2983e
W[22] = fe2e01d2  5beda413  949a6b66  9e9d6163
          d70b28f5  28f5d70b  9af96507  5677a989
W[23] = a8a05760  49b9b647  5760a8a0  d5392ac7
          3de4c21c  c87b3785  0831f7cf  9e9d6163
W[24] = 74808b80  558eaa72  1b4ee4b2  3785c87b
          90f66f0a  d70b28f5  eeb5114b  be784188
W[25] = 3126ceda  d5392ac7  2723d8dd  9f86607a
          ab5b54a5  edcc1234  bd8f4271  0576fa8a
W[26] = 263ad9c6  cfc3303d  eeb5114b  aeff5101
          2d82d27e  c3053cfb  73978c69  eb1114ef
W[27] = 8e3b71c5  91df6e21  21adde53  9e9d6163
          c1333ecd  a4135bed  c4d73b29  4e46b1ba
W[28] = 5760a8a0  73978c69  e4b21b4e  f7cf0831
          091af6e6  1c37e3c9  ae1651ea  c5c03a40
W[29] = c87b3785  2c99d367  e0251fdb  0831f7cf
          966c6994  93b16c4f  47e7b819  db982468
W[30] = afe85018  0cbef342  ca4d35b3  975568ab
          131dece3  280cd7f4  3c12c3ee  eeb5114b
W[31] = 320fcdf1  1062ef9e  8c697397  d3672c99
          131dece3  6d3892c8  5b04a4fc  b81947e7
```

Feistel Steps

```
IV :
A[0]=0ba16b95  B[0]=ac506643  C[0]=7eef60a1  D[0]=09254899
A[1]=72f999ad  B[1]=a90635a5  C[1]=6b70e3e8  D[1]=d699c7bc
A[2]=9fecc2ae  B[2]=e25b878b  C[2]=9c1714d1  D[2]=9019b6dc
A[3]=ba3264fc  B[3]=aab7878f  C[3]=b958e2a8  D[3]=2b9022e4
A[4]=5e894929  B[4]=88817f7a  C[4]=ab02675e  D[4]=8fa14956
A[5]=8e9f30e5  B[5]=0a02892b  C[5]=ed1c014f  D[5]=21bf9bd3
A[6]=2f1daa37  B[6]=559a7550  C[6]=cd8d65bb  D[6]=b94d0943
A[7]=f0f2c558  B[7]=598f657e  C[7]=fdb7a257  D[7]=6ffddc22

IV XOR M :
A[0]=0ba16b95  B[0]=ac506643  C[0]=7eef60a1  D[0]=09254899
A[1]=72f999ad  B[1]=a90635a5  C[1]=6b70e3e8  D[1]=d699c7bc
A[2]=9fecc2ae  B[2]=e25b878b  C[2]=9c1714d1  D[2]=9019b6dc
A[3]=ba3264fc  B[3]=aab7878f  C[3]=b958e2a8  D[3]=2b9022e4
A[4]=5e894929  B[4]=88817f7a  C[4]=ab02675e  D[4]=8fa14956
A[5]=8e9f30e5  B[5]=0a02892b  C[5]=ed1c014f  D[5]=21bf9bd3
A[6]=2f1daa37  B[6]=559a7550  C[6]=cd8d65bb  D[6]=b94d0943
A[7]=f0f2c558  B[7]=598f657e  C[7]=fdb7a257  D[7]=6ffddc22
```

```
Step  0: (r= 3, s=23)
A[0]=f52f5340  B[0]=5d0b5ca8  C[0]=ac506643  D[0]=7eef60a1
A[1]=a7061b18  B[1]=97cccd6b  C[1]=a90635a5  D[1]=6b70e3e8
A[2]=df31b45f  B[2]=ff661574  C[2]=e25b878b  D[2]=9c1714d1
A[3]=8bfb2871  B[3]=d19327e5  C[3]=aab7878f  D[3]=b958e2a8
A[4]=038e830e  B[4]=f44a494a  C[4]=88817f7a  D[4]=ab02675e
A[5]=6000c424  B[5]=74f9872c  C[5]=0a02892b  D[5]=ed1c014f
A[6]=4b3dc482  B[6]=78ed51b9  C[6]=559a7550  D[6]=cd8d65bb
A[7]=555af202  B[7]=87962ac7  C[7]=598f657e  D[7]=fdb7a257

Step  1: (r=23, s=17)
A[0]=88269e79  B[0]=a07a97a9  C[0]=5d0b5ca8  D[0]=ac506643
A[1]=2fe61a87  B[1]=8c53830d  C[1]=97cccd6b  D[1]=a90635a5
A[2]=93b2d2e9  B[2]=2fef98da  C[2]=ff661574  D[2]=e25b878b
A[3]=00585e1a  B[3]=38c5fd94  C[3]=d19327e5  D[3]=aab7878f
A[4]=ae78af4b  B[4]=8701c741  C[4]=f44a494a  D[4]=88817f7a
A[5]=bc8eecdc  B[5]=12300062  C[5]=74f9872c  D[5]=0a02892b
A[6]=ea65079a  B[6]=41259ee2  C[6]=78ed51b9  D[6]=559a7550
A[7]=f4a201bc  B[7]=012aad79  C[7]=87962ac7  D[7]=598f657e

Step  2: (r=17, s=27)
A[0]=98a6d957  B[0]=3cf3104d  C[0]=a07a97a9  D[0]=5d0b5ca8
A[1]=676e4650  B[1]=350e5fcc  C[1]=8c53830d  D[1]=97cccd6b
A[2]=a68c8be2  B[2]=a5d32765  C[2]=2fef98da  D[2]=ff661574
A[3]=f3570a62  B[3]=bc3400b0  C[3]=38c5fd94  D[3]=d19327e5
A[4]=1443a004  B[4]=5e975cf1  C[4]=8701c741  D[4]=f44a494a
A[5]=36c12ca4  B[5]=d9b9791d  C[5]=12300062  D[5]=74f9872c
A[6]=b56fa5d2  B[6]=0f35d4ca  C[6]=41259ee2  D[6]=78ed51b9
A[7]=6c7cfb7f  B[7]=0379e944  C[7]=012aad79  D[7]=87962ac7

Step  3: (r=27, s= 3)
A[0]=89d4cbde  B[0]=bcc536ca  C[0]=3cf3104d  D[0]=a07a97a9
A[1]=d48f4168  B[1]=833b7232  C[1]=350e5fcc  D[1]=8c53830d
A[2]=cbc4a272  B[2]=1534645f  C[2]=a5d32765  D[2]=2fef98da
A[3]=2954f12f  B[3]=179ab853  C[3]=bc3400b0  D[3]=38c5fd94
A[4]=dc6a2396  B[4]=20a21d00  C[4]=5e975cf1  D[4]=8701c741
A[5]=0d42d2cf  B[5]=21b60965  C[5]=d9b9791d  D[5]=12300062
A[6]=d034fdb8  B[6]=95ab7d2e  C[6]=0f35d4ca  D[6]=41259ee2
A[7]=31e45526  B[7]=fb63e7db  C[7]=0379e944  D[7]=012aad79

Step  4: (r= 3, s=23)
A[0]=08f26949  B[0]=4ea65ef4  C[0]=bcc536ca  D[0]=3cf3104d
A[1]=398d86c9  B[1]=a47a0b46  C[1]=833b7232  D[1]=350e5fcc
A[2]=f1702ce6  B[2]=5e251396  C[2]=1534645f  D[2]=a5d32765
A[3]=9089849f  B[3]=4aa78979  C[3]=179ab853  D[3]=bc3400b0
A[4]=df84cbd4  B[4]=e3511cb6  C[4]=20a21d00  D[4]=5e975cf1
A[5]=c358cea4  B[5]=6a169678  C[5]=21b60965  D[5]=d9b9791d
A[6]=272a33ce  B[6]=81a7edc6  C[6]=95ab7d2e  D[6]=0f35d4ca
```

```
A[7]=b8204738  B[7]=8f22a931  C[7]=fb63e7db  D[7]=0379e944

Step  5: (r=23, s=17)
A[0]=b1dafc02  B[0]=a4847934  C[0]=4ea65ef4  D[0]=bcc536ca
A[1]=400efada  B[1]=649cc6c3  C[1]=a47a0b46  D[1]=833b7232
A[2]=3d39d50b  B[2]=7378b816  C[2]=5e251396  D[2]=1534645f
A[3]=5efd52e3  B[3]=4fc844c2  C[3]=4aa78979  D[3]=179ab853
A[4]=88c17099  B[4]=ea6fc265  C[4]=e3511cb6  D[4]=20a21d00
A[5]=e06dddb4  B[5]=5261ac67  C[5]=6a169678  D[5]=21b60965
A[6]=fe3d7e59  B[6]=e7139519  C[6]=81a7edc6  D[6]=95ab7d2e
A[7]=a0bc303e  B[7]=9c5c1023  C[7]=8f22a931  D[7]=fb63e7db

Step  6: (r=17, s=27)
A[0]=d2127144  B[0]=f80563b5  C[0]=a4847934  D[0]=4ea65ef4
A[1]=17c660ee  B[1]=f5b4801d  C[1]=649cc6c3  D[1]=a47a0b46
A[2]=aa04e1fa  B[2]=aa167a73  C[2]=7378b816  D[2]=5e251396
A[3]=cbe58a51  B[3]=a5c6bdfa  C[3]=4fc844c2  D[3]=4aa78979
A[4]=8022b599  B[4]=e1331182  C[4]=ea6fc265  D[4]=e3511cb6
A[5]=692226ac  B[5]=bb69c0db  C[5]=5261ac67  D[5]=6a169678
A[6]=e005ee13  B[6]=fcb3fc7a  C[6]=e7139519  D[6]=81a7edc6
A[7]=b375c125  B[7]=607d4178  C[7]=9c5c1023  D[7]=8f22a931

Step  7: (r=27, s= 3)
A[0]=7346e510  B[0]=2690938a  C[0]=f80563b5  D[0]=a4847934
A[1]=2976c5f4  B[1]=70be3307  C[1]=f5b4801d  D[1]=649cc6c3
A[2]=3e0e82a2  B[2]=d550270f  C[2]=aa167a73  D[2]=7378b816
A[3]=ab38eac1  B[3]=8e5f2c52  C[3]=a5c6bdfa  D[3]=4fc844c2
A[4]=5ddf9e39  B[4]=cc0115ac  C[4]=e1331182  D[4]=ea6fc265
A[5]=7b1d38cc  B[5]=63491135  C[5]=bb69c0db  D[5]=5261ac67
A[6]=7d489841  B[6]=9f002f70  C[6]=fcb3fc7a  D[6]=e7139519
A[7]=20febd72  B[7]=2d9bae09  C[7]=607d4178  D[7]=9c5c1023

Step  8: (r=28, s=19)
A[0]=38742b0c  B[0]=07346e51  C[0]=2690938a  D[0]=f80563b5
A[1]=ded7faea  B[1]=42976c5f  C[1]=70be3307  D[1]=f5b4801d
A[2]=cd8f0c17  B[2]=23e0e82a  C[2]=d550270f  D[2]=aa167a73
A[3]=b6e65e2f  B[3]=1ab38eac  C[3]=8e5f2c52  D[3]=a5c6bdfa
A[4]=27360dcf  B[4]=95ddf9e3  C[4]=cc0115ac  D[4]=e1331182
A[5]=c4daf527  B[5]=c7b1d38c  C[5]=63491135  D[5]=bb69c0db
A[6]=9a671cc8  B[6]=17d48984  C[6]=9f002f70  D[6]=fcb3fc7a
A[7]=94514551  B[7]=220febd7  C[7]=2d9bae09  D[7]=607d4178

Step  9: (r=19, s=22)
A[0]=968f732e  B[0]=5861c3a1  C[0]=07346e51  D[0]=2690938a
A[1]=eeeac5fa  B[1]=d756f6bf  C[1]=42976c5f  D[1]=70be3307
A[2]=0fcb51db  B[2]=60be6c78  C[2]=23e0e82a  D[2]=d550270f
A[3]=77457731  B[3]=f17db732  C[3]=1ab38eac  D[3]=8e5f2c52
A[4]=08b233cf  B[4]=6e7939b0  C[4]=95ddf9e3  D[4]=cc0115ac
A[5]=a13afb63  B[5]=a93e26d7  C[5]=c7b1d38c  D[5]=63491135
```

```
A[6]=196df53b  B[6]=e644d338  C[6]=17d48984  D[6]=9f002f70
A[7]=88d5194e  B[7]=2a8ca28a  C[7]=220febd7  D[7]=2d9bae09

Step 10: (r=22, s= 7)
A[0]=e14f4f59  B[0]=cba5a3dc  C[0]=5861c3a1  D[0]=07346e51
A[1]=11015cf4  B[1]=7ebbbab1  C[1]=d756f6bf  D[1]=42976c5f
A[2]=2af04c96  B[2]=76c3f2d4  C[2]=60be6c78  D[2]=23e0e82a
A[3]=69f2d6b6  B[3]=cc5dd15d  C[3]=f17db732  D[3]=1ab38eac
A[4]=aa23b702  B[4]=f3c22c8c  C[4]=6e7939b0  D[4]=95ddf9e3
A[5]=b7547132  B[5]=d8e84ebe  C[5]=a93e26d7  D[5]=c7b1d38c
A[6]=9ce88f28  B[6]=4ec65b7d  C[6]=e644d338  D[6]=17d48984
A[7]=2be26331  B[7]=53a23546  C[7]=2a8ca28a  D[7]=220febd7

Step 11: (r= 7, s=28)
A[0]=1aaea868  B[0]=a7a7acf0  C[0]=cba5a3dc  D[0]=5861c3a1
A[1]=914b0856  B[1]=80ae7a08  C[1]=7ebbbab1  D[1]=d756f6bf
A[2]=fb8dc7d3  B[2]=78264b15  C[2]=76c3f2d4  D[2]=60be6c78
A[3]=4eaf1774  B[3]=f96b5b34  C[3]=cc5dd15d  D[3]=f17db732
A[4]=643eba68  B[4]=11db8155  C[4]=f3c22c8c  D[4]=6e7939b0
A[5]=2cc230a0  B[5]=aa38995b  C[5]=d8e84ebe  D[5]=a93e26d7
A[6]=4e88e47c  B[6]=7447944e  C[6]=4ec65b7d  D[6]=e644d338
A[7]=fac79835  B[7]=f1319895  C[7]=53a23546  D[7]=2a8ca28a

Step 12: (r=28, s=19)
A[0]=93ac8ca4  B[0]=81aaea86  C[0]=a7a7acf0  D[0]=cba5a3dc
A[1]=79a29bf0  B[1]=6914b085  C[1]=80ae7a08  D[1]=7ebbbab1
A[2]=8f2a8f64  B[2]=3fb8dc7d  C[2]=78264b15  D[2]=76c3f2d4
A[3]=ca1fd88e  B[3]=44eaf177  C[3]=f96b5b34  D[3]=cc5dd15d
A[4]=3983152c  B[4]=8643eba6  C[4]=11db8155  D[4]=f3c22c8c
A[5]=f459ea5c  B[5]=02cc230a  C[5]=aa38995b  D[5]=d8e84ebe
A[6]=0b89371c  B[6]=c4e88e47  C[6]=7447944e  D[6]=4ec65b7d
A[7]=1b335710  B[7]=5fac7983  C[7]=f1319895  D[7]=53a23546

Step 13: (r=19, s=22)
A[0]=deea9bed  B[0]=65249d64  C[0]=81aaea86  D[0]=a7a7acf0
A[1]=036a95d9  B[1]=df83cd14  C[1]=6914b085  D[1]=80ae7a08
A[2]=ff07856f  B[2]=7b247954  C[2]=3fb8dc7d  D[2]=78264b15
A[3]=0ea7ac58  B[3]=c47650fe  C[3]=44eaf177  D[3]=f96b5b34
A[4]=53910a06  B[4]=a961cc18  C[4]=8643eba6  D[4]=11db8155
A[5]=a74d1dc6  B[5]=52e7a2cf  C[5]=02cc230a  D[5]=aa38995b
A[6]=6017a311  B[6]=b8e05c49  C[6]=c4e88e47  D[6]=7447944e
A[7]=12dacbf6  B[7]=b880d99a  C[7]=5fac7983  D[7]=f1319895

Step 14: (r=22, s= 7)
A[0]=fefdd6ef  B[0]=fb77baa6  C[0]=65249d64  D[0]=81aaea86
A[1]=551c1512  B[1]=7640daa5  C[1]=df83cd14  D[1]=6914b085
A[2]=d8196538  B[2]=5bffc1e1  C[2]=7b247954  D[2]=3fb8dc7d
A[3]=d0b8c16e  B[3]=1603a9eb  C[3]=c47650fe  D[3]=44eaf177
A[4]=97340b19  B[4]=8194e442  C[4]=a961cc18  D[4]=8643eba6
```

```
A[5]=60d5d7c3  B[5]=71a9d347  C[5]=52e7a2cf  D[5]=02cc230a
A[6]=b39f0700  B[6]=c45805e8  C[6]=b8e05c49  D[6]=c4e88e47
A[7]=16799d51  B[7]=fd84b6b2  C[7]=b880d99a  D[7]=5fac7983

Step 15: (r= 7, s=28)
A[0]=dd5d8c02  B[0]=7eeb77ff  C[0]=fb77baa6  D[0]=65249d64
A[1]=4d0ef108  B[1]=8e0a892a  C[1]=7640daa5  D[1]=df83cd14
A[2]=450fd30e  B[2]=0cb29c6c  C[2]=5bffc1e1  D[2]=7b247954
A[3]=ef3f0e1e  B[3]=5c60b768  C[3]=1603a9eb  D[3]=c47650fe
A[4]=37a78a41  B[4]=9a058ccb  C[4]=8194e442  D[4]=a961cc18
A[5]=11938b9e  B[5]=6aebe1b0  C[5]=71a9d347  D[5]=52e7a2cf
A[6]=d56bd461  B[6]=cf838059  C[6]=c45805e8  D[6]=b8e05c49
A[7]=cc8cdbf6  B[7]=3ccea88b  C[7]=fd84b6b2  D[7]=b880d99a

Step 16: (r=29, s= 9)
A[0]=56faa177  B[0]=5babb180  C[0]=7eeb77ff  D[0]=fb77baa6
A[1]=0c8ad40d  B[1]=09a1de21  C[1]=8e0a892a  D[1]=7640daa5
A[2]=476c7907  B[2]=c8a1fa61  C[2]=0cb29c6c  D[2]=5bffc1e1
A[3]=c199225c  B[3]=dde7e1c3  C[3]=5c60b768  D[3]=1603a9eb
A[4]=f87762a9  B[4]=26f4f148  C[4]=9a058ccb  D[4]=8194e442
A[5]=2732b62d  B[5]=c2327173  C[5]=6aebe1b0  D[5]=71a9d347
A[6]=03f02304  B[6]=3aad7a8c  C[6]=cf838059  D[6]=c45805e8
A[7]=c300c59d  B[7]=d9919b7e  C[7]=3ccea88b  D[7]=fd84b6b2

Step 17: (r= 9, s=15)
A[0]=6c6a1387  B[0]=f542eead  C[0]=5babb180  D[0]=7eeb77ff
A[1]=90e2b2e2  B[1]=15a81a19  C[1]=09a1de21  D[1]=8e0a892a
A[2]=f2fb6e44  B[2]=d8f20e8e  C[2]=c8a1fa61  D[2]=0cb29c6c
A[3]=8cca00be  B[3]=3244b983  C[3]=dde7e1c3  D[3]=5c60b768
A[4]=0c676af5  B[4]=eec553f0  C[4]=26f4f148  D[4]=9a058ccb
A[5]=a8134108  B[5]=656c5a4e  C[5]=c2327173  D[5]=6aebe1b0
A[6]=2e2eaf2c  B[6]=e0460807  C[6]=3aad7a8c  D[6]=cf838059
A[7]=3c423405  B[7]=018b3b86  C[7]=d9919b7e  D[7]=3ccea88b

Step 18: (r=15, s= 5)
A[0]=99c68168  B[0]=09c3b635  C[0]=f542eead  D[0]=5babb180
A[1]=0a240c7b  B[1]=59714871  C[1]=15a81a19  D[1]=09a1de21
A[2]=1e5ca0ab  B[2]=b722797d  C[2]=d8f20e8e  D[2]=c8a1fa61
A[3]=61a9eb4c  B[3]=005f4665  C[3]=3244b983  D[3]=dde7e1c3
A[4]=b2462381  B[4]=b57a8633  C[4]=eec553f0  D[4]=26f4f148
A[5]=880f1eed  B[5]=a0845409  C[5]=656c5a4e  D[5]=c2327173
A[6]=9e1cc5c2  B[6]=57961717  C[6]=e0460807  D[6]=3aad7a8c
A[7]=cd02b129  B[7]=1a029e21  C[7]=018b3b86  D[7]=d9919b7e

Step 19: (r= 5, s=29)
A[0]=5983f93d  B[0]=38d02d13  C[0]=09c3b635  D[0]=f542eead
A[1]=56d7c90f  B[1]=44818f61  C[1]=59714871  D[1]=15a81a19
A[2]=43e7f4a7  B[2]=cb941563  C[2]=b722797d  D[2]=d8f20e8e
A[3]=b9f003a2  B[3]=353d698c  C[3]=005f4665  D[3]=3244b983
```

```
A[4]=77c553f2  B[4]=48c47036  C[4]=b57a8633  D[4]=eec553f0
A[5]=bcc5d1d3  B[5]=01e3ddb1  C[5]=a0845409  D[5]=656c5a4e
A[6]=394481b0  B[6]=c398b853  C[6]=57961717  D[6]=e0460807
A[7]=c8730078  B[7]=a0562539  C[7]=1a029e21  D[7]=018b3b86

Step 20: (r=29, s= 9)
A[0]=25d4a717  B[0]=ab307f27  C[0]=38d02d13  D[0]=09c3b635
A[1]=db6e3f00  B[1]=eadaf921  C[1]=44818f61  D[1]=59714871
A[2]=b3d001cf  B[2]=e87cfe94  C[2]=cb941563  D[2]=b722797d
A[3]=c4d78907  B[3]=573e0074  C[3]=353d698c  D[3]=005f4665
A[4]=681e1c4e  B[4]=4ef8aa7e  C[4]=48c47036  D[4]=b57a8633
A[5]=4479c3ee  B[5]=7798ba3a  C[5]=01e3ddb1  D[5]=a0845409
A[6]=0b2fc77b  B[6]=07289036  C[6]=c398b853  D[6]=57961717
A[7]=af86e3be  B[7]=190e600f  C[7]=a0562539  D[7]=1a029e21

Step 21: (r= 9, s=15)
A[0]=4c691e3b  B[0]=a94e2e4b  C[0]=ab307f27  D[0]=38d02d13
A[1]=5bf71189  B[1]=dc7e01b6  C[1]=eadaf921  D[1]=44818f61
A[2]=90a4c713  B[2]=a0039f67  C[2]=e87cfe94  D[2]=cb941563
A[3]=961dfbd0  B[3]=af120f89  C[3]=573e0074  D[3]=353d698c
A[4]=e844464f  B[4]=3c389cd0  C[4]=4ef8aa7e  D[4]=48c47036
A[5]=f1aef27a  B[5]=f387dc88  C[5]=7798ba3a  D[5]=01e3ddb1
A[6]=dde8ae62  B[6]=5f8ef616  C[6]=07289036  D[6]=c398b853
A[7]=2b5e0b7b  B[7]=0dc77d5f  C[7]=190e600f  D[7]=a0562539

Step 22: (r=15, s= 5)
A[0]=63ff1110  B[0]=8f1da634  C[0]=a94e2e4b  D[0]=ab307f27
A[1]=7366385e  B[1]=88c4adfb  C[1]=dc7e01b6  D[1]=eadaf921
A[2]=2d93f022  B[2]=6389c852  C[2]=a0039f67  D[2]=e87cfe94
A[3]=d85850c4  B[3]=fde84b0e  C[3]=af120f89  D[3]=573e0074
A[4]=ec8eb983  B[4]=2327f422  C[4]=3c389cd0  D[4]=4ef8aa7e
A[5]=cafe29d1  B[5]=793d78d7  C[5]=f387dc88  D[5]=7798ba3a
A[6]=5678184b  B[6]=57316ef4  C[6]=5f8ef616  D[6]=07289036
A[7]=8c4bb21b  B[7]=05bd95af  C[7]=0dc77d5f  D[7]=190e600f

Step 23: (r= 5, s=29)
A[0]=b26403d7  B[0]=7fe2220c  C[0]=8f1da634  D[0]=a94e2e4b
A[1]=cca973c7  B[1]=6cc70bce  C[1]=88c4adfb  D[1]=dc7e01b6
A[2]=4c0e51fe  B[2]=b27e0445  C[2]=6389c852  D[2]=a0039f67
A[3]=5200faa6  B[3]=0b0a189b  C[3]=fde84b0e  D[3]=af120f89
A[4]=66248e8d  B[4]=91d7307d  C[4]=2327f422  D[4]=3c389cd0
A[5]=90f0b0c3  B[5]=5fc53a39  C[5]=793d78d7  D[5]=f387dc88
A[6]=fea99148  B[6]=cf03096a  C[6]=57316ef4  D[6]=5f8ef616
A[7]=9874a90b  B[7]=89764371  C[7]=05bd95af  D[7]=0dc77d5f

Step 24: (r= 4, s=13)
A[0]=2c0d960e  B[0]=26403d7b  C[0]=7fe2220c  D[0]=8f1da634
A[1]=0869efbe  B[1]=ca973c7c  C[1]=6cc70bce  D[1]=88c4adfb
A[2]=0c22f858  B[2]=c0e51fe4  C[2]=b27e0445  D[2]=6389c852
```

```
A[3]=2472104a  B[3]=200faa65  C[3]=0b0a189b  D[3]=fde84b0e
A[4]=56cbca7f  B[4]=6248e8d6  C[4]=91d7307d  D[4]=2327f422
A[5]=fa4b5d1b  B[5]=0f0b0c39  C[5]=5fc53a39  D[5]=793d78d7
A[6]=bdf6afe3  B[6]=ea99148f  C[6]=cf03096a  D[6]=57316ef4
A[7]=fcda741d  B[7]=874a90b9  C[7]=89764371  D[7]=05bd95af

Step 25: (r=13, s=10)
A[0]=0647e029  B[0]=b2c1c581  C[0]=26403d7b  D[0]=7fe2220c
A[1]=8d64e603  B[1]=3df7c10d  C[1]=ca973c7c  D[1]=6cc70bce
A[2]=f579908f  B[2]=5f0b0184  C[2]=c0e51fe4  D[2]=b27e0445
A[3]=b8cddedf  B[3]=4209448e  C[3]=200faa65  D[3]=0b0a189b
A[4]=befc3754  B[4]=794fead9  C[4]=6248e8d6  D[4]=91d7307d
A[5]=15a6d75b  B[5]=6ba37f49  C[5]=0f0b0c39  D[5]=5fc53a39
A[6]=88e1088b  B[6]=d5fc77be  C[6]=ea99148f  D[6]=cf03096a
A[7]=e999cbc6  B[7]=4e83bf9b  C[7]=874a90b9  D[7]=89764371

Step 26: (r=10, s=25)
A[0]=b2bfd958  B[0]=1f80a419  C[0]=b2c1c581  D[0]=26403d7b
A[1]=953b324c  B[1]=93980e35  C[1]=3df7c10d  D[1]=ca973c7c
A[2]=854aeca0  B[2]=e6423fd5  C[2]=5f0b0184  D[2]=c0e51fe4
A[3]=86517c97  B[3]=377b7ee3  C[3]=4209448e  D[3]=200faa65
A[4]=d1eaccbe  B[4]=f0dd52fb  C[4]=794fead9  D[4]=6248e8d6
A[5]=209f2b82  B[5]=9b5d6c56  C[5]=6ba37f49  D[5]=0f0b0c39
A[6]=55e33389  B[6]=84222e23  C[6]=d5fc77be  D[6]=ea99148f
A[7]=57073a01  B[7]=672f1ba6  C[7]=4e83bf9b  D[7]=874a90b9

Step 27: (r=25, s= 4)
A[0]=f1671335  B[0]=b1657fb2  C[0]=1f80a419  D[0]=b2c1c581
A[1]=69781878  B[1]=992a7664  C[1]=93980e35  D[1]=3df7c10d
A[2]=200e8223  B[2]=410a95d9  C[2]=e6423fd5  D[2]=5f0b0184
A[3]=531693a4  B[3]=2f0ca2f9  C[3]=377b7ee3  D[3]=4209448e
A[4]=75fe2993  B[4]=7da3d599  C[4]=f0dd52fb  D[4]=794fead9
A[5]=7ee8bd83  B[5]=04413e57  C[5]=9b5d6c56  D[5]=6ba37f49
A[6]=7bf5f4cc  B[6]=12abc667  C[6]=84222e23  D[6]=d5fc77be
A[7]=809ac3cb  B[7]=02ae0e74  C[7]=672f1ba6  D[7]=4e83bf9b

Step 28: (r= 4, s=13)
A[0]=8c2bdef6  B[0]=1671335f  C[0]=b1657fb2  D[0]=1f80a419
A[1]=03ee7cb7  B[1]=97818786  C[1]=992a7664  D[1]=93980e35
A[2]=27fdaebd  B[2]=00e82232  C[2]=410a95d9  D[2]=e6423fd5
A[3]=e0dc3050  B[3]=31693a45  C[3]=2f0ca2f9  D[3]=377b7ee3
A[4]=34f73744  B[4]=5fe29937  C[4]=7da3d599  D[4]=f0dd52fb
A[5]=f3cfcdfb  B[5]=ee8bd837  C[5]=04413e57  D[5]=9b5d6c56
A[6]=dfae2f8e  B[6]=bf5f4cc7  C[6]=12abc667  D[6]=84222e23
A[7]=00176fa5  B[7]=09ac3cb8  C[7]=02ae0e74  D[7]=672f1ba6

Step 29: (r=13, s=10)
A[0]=3b602de6  B[0]=7bded185  C[0]=1671335f  D[0]=b1657fb2
A[1]=5f55a951  B[1]=cf96e07d  C[1]=97818786  D[1]=992a7664
```

```
A[2]=27022dbf  B[2]=b5d7a4ff  C[2]=00e82232  D[2]=410a95d9
A[3]=e0638bfc  B[3]=860a1c1b  C[3]=31693a45  D[3]=2f0ca2f9
A[4]=6b1e3513  B[4]=e6e8869e  C[4]=5fe29937  D[4]=7da3d599
A[5]=f0de8c72  B[5]=f9bf7e79  C[5]=ee8bd837  D[5]=04413e57
A[6]=60b2df33  B[6]=c5f1dbf5  C[6]=bf5f4cc7  D[6]=12abc667
A[7]=a551e98a  B[7]=edf4a002  C[7]=09ac3cb8  D[7]=02ae0e74

Step 30: (r=10, s=25)
A[0]=2bf0789f  B[0]=80b798ed  C[0]=7bded185  D[0]=1671335f
A[1]=853af196  B[1]=56a5457d  C[1]=cf96e07d  D[1]=97818786
A[2]=1719cccd  B[2]=08b6fc9c  C[2]=b5d7a4ff  D[2]=00e82232
A[3]=5972dfc9  B[3]=8e2ff381  C[3]=860a1c1b  D[3]=31693a45
A[4]=f17e2631  B[4]=78d44dac  C[4]=e6e8869e  D[4]=5fe29937
A[5]=c3f0067a  B[5]=7a31cbc3  C[5]=f9bf7e79  D[5]=ee8bd837
A[6]=113db280  B[6]=cb7ccd82  C[6]=c5f1dbf5  D[6]=bf5f4cc7
A[7]=0d707b53  B[7]=47a62a95  C[7]=edf4a002  D[7]=09ac3cb8

Step 31: (r=25, s= 4)
A[0]=da308396  B[0]=3e57e0f1  C[0]=80b798ed  D[0]=7bded185
A[1]=93e3bdaf  B[1]=2d0a75e3  C[1]=56a5457d  D[1]=cf96e07d
A[2]=5ba2a04d  B[2]=9a2e3399  C[2]=08b6fc9c  D[2]=b5d7a4ff
A[3]=6e0c476a  B[3]=92b2e5bf  C[3]=8e2ff381  D[3]=860a1c1b
A[4]=e5e3ae5c  B[4]=63e2fc4c  C[4]=78d44dac  D[4]=e6e8869e
A[5]=777e130a  B[5]=f587e00c  C[5]=7a31cbc3  D[5]=f9bf7e79
A[6]=b3a4b449  B[6]=00227b65  C[6]=cb7ccd82  D[6]=c5f1dbf5
A[7]=5f7de76c  B[7]=a61ae0f6  C[7]=47a62a95  D[7]=edf4a002

Feed-Forward Step 32: (r= 4, s=13)
A[0]=72a3a4e9  B[0]=a308396d  C[0]=3e57e0f1  D[0]=80b798ed
A[1]=3c3e96c0  B[1]=3e3bdaf9  C[1]=2d0a75e3  D[1]=56a5457d
A[2]=546744c4  B[2]=ba2a04d5  C[2]=9a2e3399  D[2]=08b6fc9c
A[3]=49239ce7  B[3]=e0c476a6  C[3]=92b2e5bf  D[3]=8e2ff381
A[4]=55f252e6  B[4]=5e3ae5ce  C[4]=63e2fc4c  D[4]=78d44dac
A[5]=720d1a19  B[5]=77e130a7  C[5]=f587e00c  D[5]=7a31cbc3
A[6]=e0c25e56  B[6]=3a4b449b  C[6]=00227b65  D[6]=cb7ccd82
A[7]=03f40185  B[7]=f7de76c5  C[7]=a61ae0f6  D[7]=47a62a95

Feed-Forward Step 33: (r=13, s=10)
A[0]=f1af45eb  B[0]=749d2e54  C[0]=a308396d  D[0]=3e57e0f1
A[1]=e586f10b  B[1]=d2d80787  C[1]=3e3bdaf9  D[1]=2d0a75e3
A[2]=96334055  B[2]=e8988a8c  C[2]=ba2a04d5  D[2]=9a2e3399
A[3]=2a2002eb  B[3]=739ce924  C[3]=e0c476a6  D[3]=92b2e5bf
A[4]=9684bb02  B[4]=4a5ccabe  C[4]=5e3ae5ce  D[4]=63e2fc4c
A[5]=c9ac587a  B[5]=a3432e41  C[5]=77e130a7  D[5]=f587e00c
A[6]=b9781c8c  B[6]=4bcadc18  C[6]=3a4b449b  D[6]=00227b65
A[7]=c6615778  B[7]=8030a07e  C[7]=f7de76c5  D[7]=a61ae0f6

Feed-Forward Step 34: (r=10, s=25)
A[0]=bf4bb355  B[0]=bd17afc6  C[0]=749d2e54  D[0]=a308396d
```

```
A[1]=2e4853f1  B[1]=1bc42f96  C[1]=d2d80787  D[1]=3e3bdaf9
A[2]=be2eed7e  B[2]=cd015658  C[2]=e8988a8c  D[2]=ba2a04d5
A[3]=9bbb8392  B[3]=800baca8  C[3]=739ce924  D[3]=e0c476a6
A[4]=adc9f82a  B[4]=12ec0a5a  C[4]=4a5ccabe  D[4]=5e3ae5ce
A[5]=5cf7f9aa  B[5]=b161eb26  C[5]=a3432e41  D[5]=77e130a7
A[6]=44b34cd2  B[6]=e07232e5  C[6]=4bcadc18  D[6]=3a4b449b
A[7]=14b6cdf0  B[7]=855de319  C[7]=8030a07e  D[7]=f7de76c5

Feed-Forward Step 35: (r=25, s= 4)
A[0]=7eafa551  B[0]=ab7e9766  C[0]=bd17afc6  D[0]=749d2e54
A[1]=a5d93c24  B[1]=e25c90a7  C[1]=1bc42f96  D[1]=d2d80787
A[2]=92779f98  B[2]=fd7c5dda  C[2]=cd015658  D[2]=e8988a8c
A[3]=c3c480c8  B[3]=25377707  C[3]=800baca8  D[3]=739ce924
A[4]=603d8c16  B[4]=555b93f0  C[4]=12ec0a5a  D[4]=4a5ccabe
A[5]=258751c4  B[5]=54b9eff3  C[5]=b161eb26  D[5]=a3432e41
A[6]=d15757fe  B[6]=a4896699  C[6]=e07232e5  D[6]=4bcadc18
A[7]=639ca6f7  B[7]=e0296d9b  C[7]=855de319  D[7]=8030a07e
```

Compression Function Output

```
A[0]=7eafa551  B[0]=ab7e9766  C[0]=bd17afc6  D[0]=749d2e54
A[1]=a5d93c24  B[1]=e25c90a7  C[1]=1bc42f96  D[1]=d2d80787
A[2]=92779f98  B[2]=fd7c5dda  C[2]=cd015658  D[2]=e8988a8c
A[3]=c3c480c8  B[3]=25377707  C[3]=800baca8  D[3]=739ce924
A[4]=603d8c16  B[4]=555b93f0  C[4]=12ec0a5a  D[4]=4a5ccabe
A[5]=258751c4  B[5]=54b9eff3  C[5]=b161eb26  D[5]=a3432e41
A[6]=d15757fe  B[6]=a4896699  C[6]=e07232e5  D[6]=4bcadc18
A[7]=639ca6f7  B[7]=e0296d9b  C[7]=855de319  D[7]=8030a07e
```

Hash Function Output

```
51a5af7e243cd9a5989f7792c880c4c3168c3d60c4518725fe5757d1f7a69c6366977eaba7905ce2da5d7cfd07773725f
```

A.4.2 One-block Message

We use the message block `0x00 0x01 0x02` ... as an example.

First block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
M[ 64.. 71] = 40 41 42 43 44 45 46 47
M[ 72.. 79] = 48 49 4a 4b 4c 4d 4e 4f
M[ 80.. 87] = 50 51 52 53 54 55 56 57
```

```
M[ 88.. 95] = 58 59 5a 5b 5c 5d 5e 5f
M[ 96..103] = 60 61 62 63 64 65 66 67
M[104..111] = 68 69 6a 6b 6c 6d 6e 6f
M[112..119] = 70 71 72 73 74 75 76 77
M[120..127] = 78 79 7a 7b 7c 7d 7e 7f
```

NTT Output

```
y[  0..  7] =  162   85  125  159   75  219   54   22
y[  8.. 15] =  128  171   94  185    6   71   55   63
y[ 16.. 23] =    0  203    4  152  200   45   80  133
y[ 24.. 31] =  245  117  101  152   61   77  169  230
y[ 32.. 39] =  150  100  200  254  121   31  253   22
y[ 40.. 47] =  186  171   27   59  145   41  103  177
y[ 48.. 55] =   23   10  157    5  176   84  216   88
y[ 56.. 63] =   57   20  253    9  130  255   53   84
y[ 64.. 71] =  181  160  241   61   47  252  168   18
y[ 72.. 79] =  237   26   30   19  166   18  110  113
y[ 80.. 87] =   21  240   15  103  230   72   61  142
y[ 88.. 95] =  138  119   66   45   86   29   84  243
y[ 96..103] =  202   33  131  121  206  189   63   26
y[104..111] =  129  171   92   61  218   92  254   87
y[112..119] =   84  189  205  152  233    8  203  182
y[120..127] =  168  207  190  143  124  129   57   30
y[128..135] =  192  141   92  168  121  110  169   28
y[136..143] =  128  161  211  146  197   45   44  249
y[144..151] =  171  249   62   82  157  156   70   32
y[152..159] =  122  202  163   42  174   32   21  256
y[160..167] =  244   93  107    0   28  137   44  134
y[168..175] =  129  255  154   17   97  197  180   68
y[176..183] =  132  107  244   30   65  163  147  190
y[184..191] =  115  193   79   65   69  180   30   67
y[192..199] =  205    3  191  238   12   69   15  256
y[200..207] =  106   66  122   90  108  168    4   39
y[208..215] =   82  251  217  159   43   47   16  138
y[216..223] =   62   41  152   21   23  239  124  246
y[224..231] =  176   51  194   43   74   68  188  100
y[232..239] =   19  207   16  134  197   67  195   38
y[240..247] =    3  145  211  141   79   12    7  226
y[248..255] =   91   41  102  109  195  181  241   46
```

Intermediate Expanded Message

```
Z[ 0] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
Z[ 1] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
Z[ 2] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
Z[ 3] = 073a109f  039db7bc  3cb4c577  3f98e25f
```

```
         0e742931  0681fd1c  fe8ea439  3cb4264d
Z[ 4] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
         12caf18c  0dbb15ae  0d02be3d  51a94f7e
Z[ 5] = f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
         55ffaa01  20852fb2  14f53e26  f5e23cb4
Z[ 6] = 17d9d841  5771a4f2  cedcdb25  12ca2d87
         c1daa380  2c15427c  427ce3d1  3edffdd5
Z[ 7] = cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
         dbdebfaf  ad9ecf95  a380599c  15ae2931
Z[ 8] = ac2cd107  bfaf427c  4f7e5771  143cc068
         baa05c80  afc9dec2  2085d4a4  fa381fcc
Z[ 9] = fa38c1da  3b422cce  b703b7bc  17203296
         d841582a  1e5abc12  1720c405  ff470f2d
Z[10] = 4335f69b  00004d53  a948143c  a71d1fcc
         fe8ea380  0c49b591  d4a44619  3124c85b
Z[11] = 4d53a5ab  15aef69b  bc122ef9  cf95b082
         d1c0531b  2ef93917  c85b31dd  306b15ae
Z[12] = 022bda6c  f245d04e  31dd08ac  ff470ad7
         2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
Z[13] = fbaa3b42  b92ee318  21f71f13  aa010b90
         1da12cce  0f2db41f  f2fe109f  f80d599c
Z[14] = 24dbc577  1f13d279  3124357a  4844ce23
         dbde0dbb  a71d0b90  306bd4a4  1b76d332
Z[15] = af10022b  ac2cdec2  08ac3917  e999050f
         1da141c3  4ec549b6  c914d332  213ef470
Z[16] = c4d7a989  53bc71c5  6e214443  afe83126
         74807480  d622558e  c9640576  280c320f
Z[17] = b1ba0000  386e03a4  a4fccc1f  3fb648d0
         6f0af514  aa725bed  b4753785  131dafe8
Z[18] = f42b9e9d  6163cc1f  197c6e21  280cfc5c
         8b80bf61  a2411893  58499a10  b9eb5dbf
Z[19] = 8e3b14ef  f42ba4fc  3b29b647  9be2daaf
         68ab33e1  47e7fc5c  3ecd8c69  1b4e303d
Z[20] = d0acbad4  c3eef170  0aec2ac7  0da7aeff
         607aedcc  6f0a1b4e  624cad2d  03a4641e
Z[21] = 4aa2131d  db980da7  2723e76d  0e903785
         386e93b1  a06f3c12  14ef4e46  70dc4c74
Z[22] = b647cdf1  c6a98d52  435ad195  c1333957
         114b8b80  0e9053bc  c964dc81  c792fd45
Z[23] = 02bb4c74  d622d0ac  47e7ea28  065fceda
         52d3aeff  5cd6c305  c79270dc  f17033e1
Z[24] = 966c4d5d  aeffa6ce  641edd6a  197c1406
         a8a0b1ba  9af9be78  28f5409f  f8b83957
Z[25] = f8b8ceda  4aa2a06f  a41328f5  1d208f24
         cdf16a7d  263aa06f  1d204615  ff17e76d
Z[26] = 54a55b04  0000fd45  92c81c37  900d1406
         fe2eb1ba  0f7935b3  c9642551  3de4b730
Z[27] = 6163091a  1b4e048d  aa724c74  c3055018
         c5c01234  3b290831  b9ebfe2e  3cfb4c74
```

```
Z[28] = 02bba7b7  eeb53785  3ecdfb73  ff171062
        3c1217aa  51ea114b  aeff1062  237f66d9
Z[29] = fa8af087  a6ce5dbf  2ac74188  93b19755
        25516c4f  131d28f5  ef9e1a65  f5fdf342
Z[30] = 2e6b1e09  27236e21  3de4c21c  5b0417aa
        d27eb1ba  900d3785  3cfb53bc  22964f2f
Z[31] = 9a10c21c  966ca06f  0aec0748  e3c9bbbd
        2551d27e  6335983e  bad48b80  29de1b4e
```

Expanded Message

```
W[ 0] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
        12caf18c  0dbb15ae  0d02be3d  51a94f7e
W[ 1] = 17d9d841  5771a4f2  cedcdb25  12ca2d87
        c1daa380  2c15427c  427ce3d1  3edffdd5
W[ 2] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
W[ 3] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
W[ 4] = cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
        dbdebfaf  ad9ecf95  a380599c  15ae2931
W[ 5] = f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
        55ffaa01  20852fb2  14f53e26  f5e23cb4
W[ 6] = 073a109f  039db7bc  3cb4c577  3f98e25f
        0e742931  0681fd1c  fe8ea439  3cb4264d
W[ 7] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
W[ 8] = af10022b  ac2cdec2  08ac3917  e999050f
        1da141c3  4ec549b6  c914d332  213ef470
W[ 9] = 4d53a5ab  15aef69b  bc122ef9  cf95b082
        d1c0531b  2ef93917  c85b31dd  306b15ae
W[10] = 022bda6c  f245d04e  31dd08ac  ff470ad7
        2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
W[11] = ac2cd107  bfaf427c  4f7e5771  143cc068
        baa05c80  afc9dec2  2085d4a4  fa381fcc
W[12] = fa38c1da  3b422cce  b703b7bc  17203296
        d841582a  1e5abc12  1720c405  ff470f2d
W[13] = fbaa3b42  b92ee318  21f71f13  aa010b90
        1da12cce  0f2db41f  f2fe109f  f80d599c
W[14] = 4335f69b  00004d53  a948143c  a71d1fcc
        fe8ea380  0c49b591  d4a44619  3124c85b
W[15] = 24dbc577  1f13d279  3124357a  4844ce23
        dbde0dbb  a71d0b90  306bd4a4  1b76d332
W[16] = b1ba0000  386e03a4  a4fccc1f  3fb648d0
        6f0af514  aa725bed  b4753785  131dafe8
W[17] = f42b9e9d  6163cc1f  197c6e21  280cfc5c
        8b80bf61  a2411893  58499a10  b9eb5dbf
W[18] = 02bb4c74  d622d0ac  47e7ea28  065fceda
        52d3aeff  5cd6c305  c79270dc  f17033e1
```

```
W[19] = d0acbad4  c3eef170  0aec2ac7  0da7aeff
        607aedcc  6f0a1b4e  624cad2d  03a4641e
W[20] = b647cdf1  c6a98d52  435ad195  c1333957
        114b8b80  0e9053bc  c964dc81  c792fd45
W[21] = 4aa2131d  db980da7  2723e76d  0e903785
        386e93b1  a06f3c12  14ef4e46  70dc4c74
W[22] = c4d7a989  53bc71c5  6e214443  afe83126
        74807480  d622558e  c9640576  280c320f
W[23] = 8e3b14ef  f42ba4fc  3b29b647  9be2daaf
        68ab33e1  47e7fc5c  3ecd8c69  1b4e303d
W[24] = 2e6b1e09  27236e21  3de4c21c  5b0417aa
        d27eb1ba  900d3785  3cfb53bc  22964f2f
W[25] = 966c4d5d  aeffa6ce  641edd6a  197c1406
        a8a0b1ba  9af9be78  28f5409f  f8b83957
W[26] = f8b8ceda  4aa2a06f  a41328f5  1d208f24
        cdf16a7d  263aa06f  1d204615  ff17e76d
W[27] = 9a10c21c  966ca06f  0aec0748  e3c9bbbd
        2551d27e  6335983e  bad48b80  29de1b4e
W[28] = 6163091a  1b4e048d  aa724c74  c3055018
        c5c01234  3b290831  b9ebfe2e  3cfb4c74
W[29] = fa8af087  a6ce5dbf  2ac74188  93b19755
        25516c4f  131d28f5  ef9e1a65  f5fdf342
W[30] = 02bba7b7  eeb53785  3ecdfb73  ff171062
        3c1217aa  51ea114b  aeff1062  237f66d9
W[31] = 54a55b04  0000fd45  92c81c37  900d1406
        fe2eb1ba  0f7935b3  c9642551  3de4b730
```

Feistel Steps

```
IV :
A[0]=0ba16b95  B[0]=ac506643  C[0]=7eef60a1  D[0]=09254899
A[1]=72f999ad  B[1]=a90635a5  C[1]=6b70e3e8  D[1]=d699c7bc
A[2]=9fecc2ae  B[2]=e25b878b  C[2]=9c1714d1  D[2]=9019b6dc
A[3]=ba3264fc  B[3]=aab7878f  C[3]=b958e2a8  D[3]=2b9022e4
A[4]=5e894929  B[4]=88817f7a  C[4]=ab02675e  D[4]=8fa14956
A[5]=8e9f30e5  B[5]=0a02892b  C[5]=ed1c014f  D[5]=21bf9bd3
A[6]=2f1daa37  B[6]=559a7550  C[6]=cd8d65bb  D[6]=b94d0943
A[7]=f0f2c558  B[7]=598f657e  C[7]=fdb7a257  D[7]=6ffddc22

IV XOR M :
A[0]=08a36a95  B[0]=8f724763  C[0]=3dad21e1  D[0]=6a4729f9
A[1]=75ff9ca9  B[1]=8e201081  C[1]=2c36a6ac  D[1]=b1ffa2d8
A[2]=94e6cba6  B[2]=c971aea3  C[2]=d75d5d99  D[2]=fb73dfb4
A[3]=b53c69f0  B[3]=8599aaa3  C[3]=f616afe4  D[3]=44fe4f88
A[4]=4d9b5839  B[4]=bbb34e4a  C[4]=f850360e  D[4]=fcd33826
A[5]=998925f1  B[5]=3d34bc1f  C[5]=ba4a541b  D[5]=56c9eea7
A[6]=3407b32f  B[6]=6ea04c68  C[6]=96d73ce3  D[6]=c237703b
A[7]=efecd844  B[7]=66b15842  C[7]=a2e9ff0b  D[7]=1083a15e
```

```
Step  0: (r= 3, s=23)
A[0]=e72d93e6  B[0]=451b54a8  C[0]=8f724763  D[0]=3dad21e1
A[1]=2c106f8c  B[1]=affce54b  C[1]=8e201081  D[1]=2c36a6ac
A[2]=dd40f7d5  B[2]=a7365d34  C[2]=c971aea3  D[2]=d75d5d99
A[3]=94c2eb12  B[3]=a9e34f85  C[3]=8599aaa3  D[3]=f616afe4
A[4]=acade857  B[4]=6cdac1ca  C[4]=bbb34e4a  D[4]=f850360e
A[5]=a52aa586  B[5]=cc492f8c  C[5]=3d34bc1f  D[5]=ba4a541b
A[6]=2fa1c744  B[6]=a03d9979  C[6]=6ea04c68  D[6]=96d73ce3
A[7]=b42200b1  B[7]=7f66c227  C[7]=66b15842  D[7]=a2e9ff0b

Step  1: (r=23, s=17)
A[0]=3f9f16a7  B[0]=f37396c9  C[0]=451b54a8  D[0]=8f724763
A[1]=da2874b1  B[1]=c6160837  C[1]=affce54b  D[1]=8e201081
A[2]=57beadcb  B[2]=eaeea07b  C[2]=a7365d34  D[2]=c971aea3
A[3]=156baaca  B[3]=894a6175  C[3]=a9e34f85  D[3]=8599aaa3
A[4]=2aa09406  B[4]=2bd656f4  C[4]=6cdac1ca  D[4]=bbb34e4a
A[5]=31b3666c  B[5]=c3529552  C[5]=cc492f8c  D[5]=3d34bc1f
A[6]=47ac09b4  B[6]=a217d0e3  C[6]=a03d9979  D[6]=6ea04c68
A[7]=709cb931  B[7]=58da1100  C[7]=7f66c227  D[7]=66b15842

Step  2: (r=17, s=27)
A[0]=85964a47  B[0]=2d4e7f3e  C[0]=f37396c9  D[0]=451b54a8
A[1]=df0d4239  B[1]=e963b450  C[1]=c6160837  D[1]=affce54b
A[2]=d9d3d5e8  B[2]=5b96af7d  C[2]=eaeea07b  D[2]=a7365d34
A[3]=5b5e0607  B[3]=55942ad7  C[3]=894a6175  D[3]=a9e34f85
A[4]=cacbcf5c  B[4]=280c5541  C[4]=2bd656f4  D[4]=6cdac1ca
A[5]=e11719a7  B[5]=ccd86366  C[5]=c3529552  D[5]=cc492f8c
A[6]=622c7c4e  B[6]=13688f58  C[6]=a217d0e3  D[6]=a03d9979
A[7]=0c79f9fe  B[7]=7262e139  C[7]=58da1100  D[7]=7f66c227

Step  3: (r=27, s= 3)
A[0]=611a1f48  B[0]=3c2cb252  C[0]=2d4e7f3e  D[0]=f37396c9
A[1]=fdfcc032  B[1]=cef86a11  C[1]=e963b450  D[1]=c6160837
A[2]=99db3b12  B[2]=46ce9eaf  C[2]=5b96af7d  D[2]=eaeea07b
A[3]=93223316  B[3]=3adaf030  C[3]=55942ad7  D[3]=894a6175
A[4]=aef2f2a9  B[4]=e6565e7a  C[4]=280c5541  D[4]=2bd656f4
A[5]=3cf7a80f  B[5]=3f08b8cd  C[5]=ccd86366  D[5]=c3529552
A[6]=3fdf645f  B[6]=731163e2  C[6]=13688f58  D[6]=a217d0e3
A[7]=9a25ccee  B[7]=f063cfcf  C[7]=7262e139  D[7]=58da1100

Step  4: (r= 3, s=23)
A[0]=53b4ef82  B[0]=08d0fa43  C[0]=3c2cb252  D[0]=2d4e7f3e
A[1]=d14bacae  B[1]=efe60197  C[1]=cef86a11  D[1]=e963b450
A[2]=0254b29b  B[2]=ced9d894  C[2]=46ce9eaf  D[2]=5b96af7d
A[3]=41ae782f  B[3]=991198b4  C[3]=3adaf030  D[3]=55942ad7
A[4]=7641074d  B[4]=7797954d  C[4]=e6565e7a  D[4]=280c5541
A[5]=a427df49  B[5]=e7bd4079  C[5]=3f08b8cd  D[5]=ccd86366
A[6]=85ce117c  B[6]=fefb22f9  C[6]=731163e2  D[6]=13688f58
A[7]=df0a4e98  B[7]=d12e6774  C[7]=f063cfcf  D[7]=7262e139
```

```
Step  5: (r=23, s=17)
A[0]=5dc9f89c  B[0]=c129da77  C[0]=08d0fa43  D[0]=3c2cb252
A[1]=8dbeee81  B[1]=5768a5d6  C[1]=efe60197  D[1]=cef86a11
A[2]=1205c0e7  B[2]=4d812a59  C[2]=ced9d894  D[2]=46ce9eaf
A[3]=44fb58ab  B[3]=17a0d73c  C[3]=991198b4  D[3]=3adaf030
A[4]=44c0c002  B[4]=a6bb2083  C[4]=7797954d  D[4]=e6565e7a
A[5]=2444536f  B[5]=a4d213ef  C[5]=e7bd4079  D[5]=3f08b8cd
A[6]=3a54e647  B[6]=be42e708  C[6]=fefb22f9  D[6]=731163e2
A[7]=9cbc4d55  B[7]=4c6f8527  C[7]=d12e6774  D[7]=f063cfcf

Step  6: (r=17, s=27)
A[0]=c46e0f6b  B[0]=f138bb93  C[0]=c129da77  D[0]=08d0fa43
A[1]=cbf26ec3  B[1]=dd031b7d  C[1]=5768a5d6  D[1]=efe60197
A[2]=ab1e9e10  B[2]=81ce240b  C[2]=4d812a59  D[2]=ced9d894
A[3]=f72c66d2  B[3]=b15689f6  C[3]=17a0d73c  D[3]=991198b4
A[4]=6413abd0  B[4]=80048981  C[4]=a6bb2083  D[4]=7797954d
A[5]=a45613c7  B[5]=a6de4888  C[5]=a4d213ef  D[5]=e7bd4079
A[6]=a34dbb7e  B[6]=cc8e74a9  C[6]=be42e708  D[6]=fefb22f9
A[7]=39a0bbd2  B[7]=9aab3978  C[7]=4c6f8527  D[7]=d12e6774

Step  7: (r=27, s= 3)
A[0]=35fc412b  B[0]=5e23707b  C[0]=f138bb93  D[0]=c129da77
A[1]=795d130f  B[1]=1e5f9376  C[1]=dd031b7d  D[1]=5768a5d6
A[2]=5f284f19  B[2]=8558f4f0  C[2]=81ce240b  D[2]=4d812a59
A[3]=3a2dc8c7  B[3]=97b96336  C[3]=b15689f6  D[3]=17a0d73c
A[4]=beec61b1  B[4]=83209d5e  C[4]=80048981  D[4]=a6bb2083
A[5]=88b58788  B[5]=3d22b09e  C[5]=a6de4888  D[5]=a4d213ef
A[6]=b9473795  B[6]=f51a6ddb  C[6]=cc8e74a9  D[6]=be42e708
A[7]=a7d97851  B[7]=91cd05de  C[7]=9aab3978  D[7]=4c6f8527

Step  8: (r=28, s=19)
A[0]=167e964f  B[0]=b35fc412  C[0]=5e23707b  D[0]=f138bb93
A[1]=1af2972a  B[1]=f795d130  C[1]=1e5f9376  D[1]=dd031b7d
A[2]=5805a5f9  B[2]=95f284f1  C[2]=8558f4f0  D[2]=81ce240b
A[3]=7497fe20  B[3]=73a2dc8c  C[3]=97b96336  D[3]=b15689f6
A[4]=f0a4b8d8  B[4]=1beec61b  C[4]=83209d5e  D[4]=80048981
A[5]=a50bec9d  B[5]=888b5878  C[5]=3d22b09e  D[5]=a6de4888
A[6]=b2fbab22  B[6]=5b947379  C[6]=f51a6ddb  D[6]=cc8e74a9
A[7]=d00e0dfb  B[7]=1a7d9785  C[7]=91cd05de  D[7]=9aab3978

Step  9: (r=19, s=22)
A[0]=8bf0fb3e  B[0]=b278b3f4  C[0]=b35fc412  D[0]=5e23707b
A[1]=d405f8a7  B[1]=b950d794  C[1]=f795d130  D[1]=1e5f9376
A[2]=afed823d  B[2]=2fcac02d  C[2]=95f284f1  D[2]=8558f4f0
A[3]=9cedfd59  B[3]=f103a4bf  C[3]=73a2dc8c  D[3]=97b96336
A[4]=c7aef235  B[4]=c6c78525  C[4]=1beec61b  D[4]=83209d5e
A[5]=de3a0126  B[5]=64ed285f  C[5]=888b5878  D[5]=3d22b09e
A[6]=66c2a3a8  B[6]=591597dd  C[6]=5b947379  D[6]=f51a6ddb
```

```
A[7]=8fe46134  B[7]=6fde8070  C[7]=1a7d9785  D[7]=91cd05de

Step 10: (r=22, s= 7)
A[0]=bde84908  B[0]=cfa2fc3e  C[0]=b278b3f4  D[0]=b35fc412
A[1]=aa86a7c2  B[1]=29f5017e  C[1]=b950d794  D[1]=f795d130
A[2]=b2364679  B[2]=8f6bfb60  C[2]=2fcac02d  D[2]=95f284f1
A[3]=d1ac5183  B[3]=56673b7f  C[3]=f103a4bf  D[3]=73a2dc8c
A[4]=19db0ce0  B[4]=8d71ebbc  C[4]=c6c78525  D[4]=1beec61b
A[5]=554a4409  B[5]=49b78e80  C[5]=64ed285f  D[5]=888b5878
A[6]=38ff6e86  B[6]=ea19b0a8  C[6]=591597dd  D[6]=5b947379
A[7]=7a41a5a2  B[7]=4d23f918  C[7]=6fde8070  D[7]=1a7d9785

Step 11: (r= 7, s=28)
A[0]=0415ddab  B[0]=f424845e  C[0]=cfa2fc3e  D[0]=b278b3f4
A[1]=1c98065c  B[1]=4353e155  C[1]=29f5017e  D[1]=b950d794
A[2]=88288b29  B[2]=1b233cd9  C[2]=8f6bfb60  D[2]=2fcac02d
A[3]=bf37b83f  B[3]=d628c1e8  C[3]=56673b7f  D[3]=f103a4bf
A[4]=4db22c19  B[4]=ed86700c  C[4]=8d71ebbc  D[4]=c6c78525
A[5]=fdc44a97  B[5]=a52204aa  C[5]=49b78e80  D[5]=64ed285f
A[6]=447c0187  B[6]=7fb7431c  C[6]=ea19b0a8  D[6]=591597dd
A[7]=31489263  B[7]=20d2d13d  C[7]=4d23f918  D[7]=6fde8070

Step 12: (r=28, s=19)
A[0]=c3780fd8  B[0]=b0415dda  C[0]=f424845e  D[0]=cfa2fc3e
A[1]=a23fb338  B[1]=c1c98065  C[1]=4353e155  D[1]=29f5017e
A[2]=1a6fd47a  B[2]=988288b2  C[2]=1b233cd9  D[2]=8f6bfb60
A[3]=1b82151d  B[3]=fbf37b83  C[3]=d628c1e8  D[3]=56673b7f
A[4]=274ee15d  B[4]=94db22c1  C[4]=ed86700c  D[4]=8d71ebbc
A[5]=301e1021  B[5]=7fdc44a9  C[5]=a52204aa  D[5]=49b78e80
A[6]=ad4073ff  B[6]=7447c018  C[6]=7fb7431c  D[6]=ea19b0a8
A[7]=b6f5e11d  B[7]=33148926  C[7]=20d2d13d  D[7]=4d23f918

Step 13: (r=19, s=22)
A[0]=619825c8  B[0]=7ec61bc0  C[0]=b0415dda  D[0]=f424845e
A[1]=03f320d1  B[1]=99c511fd  C[1]=c1c98065  D[1]=4353e155
A[2]=7b704bb0  B[2]=a3d0d37e  C[2]=988288b2  D[2]=1b233cd9
A[3]=2f24ba55  B[3]=a8e8dc10  C[3]=fbf37b83  D[3]=d628c1e8
A[4]=b49a541e  B[4]=0ae93a77  C[4]=94db22c1  D[4]=ed86700c
A[5]=6be892ce  B[5]=810980f0  C[5]=7fdc44a9  D[5]=a52204aa
A[6]=bca76b3f  B[6]=9ffd6a03  C[6]=7447c018  D[6]=7fb7431c
A[7]=a546dd94  B[7]=08edb7af  C[7]=33148926  D[7]=20d2d13d

Step 14: (r=22, s= 7)
A[0]=418d5d9c  B[0]=72186609  C[0]=7ec61bc0  D[0]=b0415dda
A[1]=fcb034eb  B[1]=3440fcc8  C[1]=99c511fd  D[1]=c1c98065
A[2]=b35a2cee  B[2]=ec1edc12  C[2]=a3d0d37e  D[2]=988288b2
A[3]=7f8cbea6  B[3]=954bc92e  C[3]=a8e8dc10  D[3]=fbf37b83
A[4]=2bbdebe4  B[4]=07ad2695  C[4]=0ae93a77  D[4]=94db22c1
A[5]=a1cab823  B[5]=b39afa24  C[5]=810980f0  D[5]=7fdc44a9
```

```
A[6]=06a2f9bf  B[6]=cfef29da  C[6]=9ffd6a03  D[6]=7447c018
A[7]=6e0ac913  B[7]=652951b7  C[7]=08edb7af  D[7]=33148926

Step 15: (r= 7, s=28)
A[0]=e5f777b0  B[0]=c6aece20  C[0]=72186609  D[0]=7ec61bc0
A[1]=7f3e6233  B[1]=581a75fe  C[1]=3440fcc8  D[1]=99c511fd
A[2]=85c60bbf  B[2]=ad167759  C[2]=ec1edc12  D[2]=a3d0d37e
A[3]=a57c242c  B[3]=c65f533f  C[3]=954bc92e  D[3]=a8e8dc10
A[4]=c4dcdd10  B[4]=def5f215  C[4]=07ad2695  D[4]=0ae93a77
A[5]=62e793c4  B[5]=e55c11d0  C[5]=b39afa24  D[5]=810980f0
A[6]=39f8fe05  B[6]=517cdf83  C[6]=cfef29da  D[6]=9ffd6a03
A[7]=53c5c8de  B[7]=056489b7  C[7]=652951b7  D[7]=08edb7af

Step 16: (r=29, s= 9)
A[0]=4d7c9385  B[0]=1cbeeef6  C[0]=c6aece20  D[0]=72186609
A[1]=b0d4bada  B[1]=6fe7cc46  C[1]=581a75fe  D[1]=3440fcc8
A[2]=f5ac5b61  B[2]=f0b8c177  C[2]=ad167759  D[2]=ec1edc12
A[3]=6dc3e93f  B[3]=94af8485  C[3]=c65f533f  D[3]=954bc92e
A[4]=7b836043  B[4]=189b9ba2  C[4]=def5f215  D[4]=07ad2695
A[5]=7b263354  B[5]=8c5cf278  C[5]=e55c11d0  D[5]=b39afa24
A[6]=fd9e61f9  B[6]=a73f1fc0  C[6]=517cdf83  D[6]=cfef29da
A[7]=7c5f8efa  B[7]=ca78b91b  C[7]=056489b7  D[7]=652951b7

Step 17: (r= 9, s=15)
A[0]=f177f95c  B[0]=f9270a9a  C[0]=1cbeeef6  D[0]=c6aece20
A[1]=23ddc324  B[1]=a975b561  C[1]=6fe7cc46  D[1]=581a75fe
A[2]=814c348b  B[2]=58b6c3eb  C[2]=f0b8c177  D[2]=ad167759
A[3]=24eeac96  B[3]=87d27edb  C[3]=94af8485  D[3]=c65f533f
A[4]=7b240d0a  B[4]=06c086f7  C[4]=189b9ba2  D[4]=def5f215
A[5]=5f87e517  B[5]=4c66a8f6  C[5]=8c5cf278  D[5]=e55c11d0
A[6]=fe3d0fd1  B[6]=3cc3f3fb  C[6]=a73f1fc0  D[6]=517cdf83
A[7]=a30b3b3d  B[7]=bf1df4f8  C[7]=ca78b91b  D[7]=056489b7

Step 18: (r=15, s= 5)
A[0]=d5b0d99b  B[0]=fcae78bb  C[0]=f9270a9a  D[0]=1cbeeef6
A[1]=7d1fbf25  B[1]=e19211ee  C[1]=a975b561  D[1]=6fe7cc46
A[2]=54034191  B[2]=1a45c0a6  C[2]=58b6c3eb  D[2]=f0b8c177
A[3]=b832d4aa  B[3]=564b1277  C[3]=87d27edb  D[3]=94af8485
A[4]=6e3908b4  B[4]=06853d92  C[4]=06c086f7  D[4]=189b9ba2
A[5]=cedf631c  B[5]=f28bafc3  C[5]=4c66a8f6  D[5]=8c5cf278
A[6]=18979881  B[6]=87e8ff1e  C[6]=3cc3f3fb  D[6]=a73f1fc0
A[7]=64137b02  B[7]=9d9ed185  C[7]=bf1df4f8  D[7]=ca78b91b

Step 19: (r= 5, s=29)
A[0]=3fb1c0d8  B[0]=b61b337a  C[0]=fcae78bb  D[0]=f9270a9a
A[1]=559c2a06  B[1]=a3f7e4af  C[1]=e19211ee  D[1]=a975b561
A[2]=de77b97e  B[2]=8068322a  C[2]=1a45c0a6  D[2]=58b6c3eb
A[3]=be64444b  B[3]=065a9557  C[3]=564b1277  D[3]=87d27edb
A[4]=3655985f  B[4]=c721168d  C[4]=06853d92  D[4]=06c086f7
```

```
A[5]=982a895f  B[5]=dbec6399  C[5]=f28bafc3  D[5]=4c66a8f6
A[6]=89c17dbb  B[6]=12f31023  C[6]=87e8ff1e  D[6]=3cc3f3fb
A[7]=e3c2b1e0  B[7]=826f604c  C[7]=9d9ed185  D[7]=bf1df4f8

Step 20: (r=29, s= 9)
A[0]=3b5dbde7  B[0]=07f6381b  C[0]=b61b337a  D[0]=fcae78bb
A[1]=5dcc13ce  B[1]=cab38540  C[1]=a3f7e4af  D[1]=e19211ee
A[2]=5fc38c23  B[2]=dbcef72f  C[2]=8068322a  D[2]=1a45c0a6
A[3]=bc1168fa  B[3]=77cc8889  C[3]=065a9557  D[3]=564b1277
A[4]=2a546457  B[4]=e6cab30b  C[4]=c721168d  D[4]=06853d92
A[5]=0e049fab  B[5]=f305512b  C[5]=dbec6399  D[5]=f28bafc3
A[6]=f06a6643  B[6]=71382fb7  C[6]=12f31023  D[6]=87e8ff1e
A[7]=77948a9d  B[7]=1c78563c  C[7]=826f604c  D[7]=9d9ed185

Step 21: (r= 9, s=15)
A[0]=7ad15c12  B[0]=bb7bce76  C[0]=07f6381b  D[0]=b61b337a
A[1]=8e2d9306  B[1]=98279cbb  C[1]=cab38540  D[1]=a3f7e4af
A[2]=51f10412  B[2]=871846bf  C[2]=dbcef72f  D[2]=8068322a
A[3]=70841458  B[3]=22d1f578  C[3]=77cc8889  D[3]=065a9557
A[4]=0ce868b6  B[4]=a8c8ae54  C[4]=e6cab30b  D[4]=c721168d
A[5]=4888e553  B[5]=093f561c  C[5]=f305512b  D[5]=dbec6399
A[6]=62d8c198  B[6]=d4cc87e0  C[6]=71382fb7  D[6]=12f31023
A[7]=84d71a5b  B[7]=29153aef  C[7]=1c78563c  D[7]=826f604c

Step 22: (r=15, s= 5)
A[0]=3d935422  B[0]=ae093d68  C[0]=bb7bce76  D[0]=07f6381b
A[1]=c8ab313b  B[1]=c9834716  C[1]=98279cbb  D[1]=cab38540
A[2]=80929c0c  B[2]=820928f8  C[2]=871846bf  D[2]=dbcef72f
A[3]=9394fee9  B[3]=0a2c3842  C[3]=22d1f578  D[3]=77cc8889
A[4]=8f4fcd75  B[4]=345b0674  C[4]=a8c8ae54  D[4]=e6cab30b
A[5]=6dae00a1  B[5]=72a9a444  C[5]=093f561c  D[5]=f305512b
A[6]=53fce691  B[6]=60cc316c  C[6]=d4cc87e0  D[6]=71382fb7
A[7]=a398e26c  B[7]=8d2dc26b  C[7]=29153aef  D[7]=1c78563c

Step 23: (r= 5, s=29)
A[0]=9cfd16bd  B[0]=b26a8447  C[0]=ae093d68  D[0]=bb7bce76
A[1]=63902520  B[1]=15662779  C[1]=c9834716  D[1]=98279cbb
A[2]=058c9b8d  B[2]=12538190  C[2]=820928f8  D[2]=871846bf
A[3]=182eb36d  B[3]=729fdd32  C[3]=0a2c3842  D[3]=22d1f578
A[4]=9f1500d6  B[4]=e9f9aeb1  C[4]=345b0674  D[4]=a8c8ae54
A[5]=e7afd7c5  B[5]=b5c0142d  C[5]=72a9a444  D[5]=093f561c
A[6]=ea13fb31  B[6]=7f9cd22a  C[6]=60cc316c  D[6]=d4cc87e0
A[7]=d1dca14a  B[7]=731c4d94  C[7]=8d2dc26b  D[7]=29153aef

Step 24: (r= 4, s=13)
A[0]=6623ca5a  B[0]=cfd16bd9  C[0]=b26a8447  D[0]=ae093d68
A[1]=270c01d9  B[1]=39025206  C[1]=15662779  D[1]=c9834716
A[2]=0e5bbae5  B[2]=58c9b8d0  C[2]=12538190  D[2]=820928f8
A[3]=6499fdd5  B[3]=82eb36d1  C[3]=729fdd32  D[3]=0a2c3842
```

```
A[4]=6aa1d941  B[4]=f1500d69  C[4]=e9f9aeb1  D[4]=345b0674
A[5]=39747cf7  B[5]=7afd7c5e  C[5]=b5c0142d  D[5]=72a9a444
A[6]=10be8bf2  B[6]=a13fb31e  C[6]=7f9cd22a  D[6]=60cc316c
A[7]=0af80286  B[7]=1dca14ad  C[7]=731c4d94  D[7]=8d2dc26b

Step 25: (r=13, s=10)
A[0]=8b036f98  B[0]=794b4cc4  C[0]=cfd16bd9  D[0]=b26a8447
A[1]=cf783ffb  B[1]=803b24e1  C[1]=39025206  D[1]=15662779
A[2]=c7518d58  B[2]=775ca1cb  C[2]=58c9b8d0  D[2]=12538190
A[3]=af832eef  B[3]=3fbaac93  C[3]=82eb36d1  D[3]=729fdd32
A[4]=cfdba3da  B[4]=3b282d54  C[4]=f1500d69  D[4]=e9f9aeb1
A[5]=d8c7b7ee  B[5]=8f9ee72e  C[5]=7afd7c5e  D[5]=b5c0142d
A[6]=40cf4477  B[6]=d17e4217  C[6]=a13fb31e  D[6]=7f9cd22a
A[7]=4081fdc9  B[7]=0050c15f  C[7]=1dca14ad  D[7]=731c4d94

Step 26: (r=10, s=25)
A[0]=cde91241  B[0]=0dbe622c  C[0]=794b4cc4  D[0]=cfd16bd9
A[1]=d732635c  B[1]=e0ffef3d  C[1]=803b24e1  D[1]=39025206
A[2]=b90c3a1b  B[2]=4635631d  C[2]=775ca1cb  D[2]=58c9b8d0
A[3]=420ec090  B[3]=0cbbbebe  C[3]=3fbaac93  D[3]=82eb36d1
A[4]=4ca1a54b  B[4]=6e8f6b3f  C[4]=3b282d54  D[4]=f1500d69
A[5]=fb42d664  B[5]=1edfbb63  C[5]=8f9ee72e  D[5]=7afd7c5e
A[6]=9dfc6753  B[6]=3d11dd03  C[6]=d17e4217  D[6]=a13fb31e
A[7]=eadd6018  B[7]=07f72502  C[7]=0050c15f  D[7]=1dca14ad

Step 27: (r=25, s= 4)
A[0]=0f610ae4  B[0]=839bd224  C[0]=0dbe622c  D[0]=794b4cc4
A[1]=c49c28d4  B[1]=b9ae64c6  C[1]=e0ffef3d  D[1]=803b24e1
A[2]=47e237e8  B[2]=37721874  C[2]=4635631d  D[2]=775ca1cb
A[3]=78cfacda  B[3]=20841d81  C[3]=0cbbbebe  D[3]=3fbaac93
A[4]=e64c628d  B[4]=9699434a  C[4]=6e8f6b3f  D[4]=3b282d54
A[5]=8acae535  B[5]=c9f685ac  C[5]=1edfbb63  D[5]=8f9ee72e
A[6]=c9da52cf  B[6]=a73bf8ce  C[6]=3d11dd03  D[6]=d17e4217
A[7]=c86131a5  B[7]=31d5bac0  C[7]=07f72502  D[7]=0050c15f

Step 28: (r= 4, s=13)
A[0]=7cc2ea99  B[0]=f610ae40  C[0]=839bd224  D[0]=0dbe622c
A[1]=e8d8fdc8  B[1]=49c28d4c  C[1]=b9ae64c6  D[1]=e0ffef3d
A[2]=b1323acf  B[2]=7e237e84  C[2]=37721874  D[2]=4635631d
A[3]=754c23ed  B[3]=8cfacda7  C[3]=20841d81  D[3]=0cbbbebe
A[4]=61015046  B[4]=64c628de  C[4]=9699434a  D[4]=6e8f6b3f
A[5]=3756b392  B[5]=acae5358  C[5]=c9f685ac  D[5]=1edfbb63
A[6]=4935a16c  B[6]=9da52cfc  C[6]=a73bf8ce  D[6]=3d11dd03
A[7]=c58f94e4  B[7]=86131a5c  C[7]=31d5bac0  D[7]=07f72502

Step 29: (r=13, s=10)
A[0]=25205921  B[0]=5d532f98  C[0]=f610ae40  D[0]=839bd224
A[1]=5787ba77  B[1]=1fb91d1b  C[1]=49c28d4c  D[1]=b9ae64c6
A[2]=e58672c0  B[2]=4759f626  C[2]=7e237e84  D[2]=37721874
```

```
A[3]=bc0129fe  B[3]=847daea9  C[3]=8cfacda7  D[3]=20841d81
A[4]=cfb96a07  B[4]=2a08cc20  C[4]=64c628de  D[4]=9699434a
A[5]=525d7228  B[5]=d67246ea  C[5]=acae5358  D[5]=c9f685ac
A[6]=f3d4827f  B[6]=b42d8926  C[6]=9da52cfc  D[6]=a73bf8ce
A[7]=52853f29  B[7]=f29c98b1  C[7]=86131a5c  D[7]=31d5bac0

Step 30: (r=10, s=25)
A[0]=d1c1d2e7  B[0]=81648494  C[0]=5d532f98  D[0]=f610ae40
A[1]=58b7c963  B[1]=1ee9dd5e  C[1]=1fb91d1b  D[1]=49c28d4c
A[2]=591f0ba8  B[2]=19cb0396  C[2]=4759f626  D[2]=7e237e84
A[3]=44420715  B[3]=04a7faf0  C[3]=847daea9  D[3]=8cfacda7
A[4]=468c6754  B[4]=e5a81f3e  C[4]=2a08cc20  D[4]=64c628de
A[5]=d4e1631c  B[5]=75c8a149  C[5]=d67246ea  D[5]=acae5358
A[6]=41bfe061  B[6]=5209ffcf  C[6]=b42d8926  D[6]=9da52cfc
A[7]=1a1875c0  B[7]=14fca54a  C[7]=f29c98b1  D[7]=86131a5c

Step 31: (r=25, s= 4)
A[0]=ea01818f  B[0]=cfa383a5  C[0]=81648494  D[0]=5d532f98
A[1]=d888bcdd  B[1]=c6b16f92  C[1]=1ee9dd5e  D[1]=1fb91d1b
A[2]=6b1b55a8  B[2]=50b23e17  C[2]=19cb0396  D[2]=4759f626
A[3]=e69c8987  B[3]=2a88840e  C[3]=04a7faf0  D[3]=847daea9
A[4]=1806cdb7  B[4]=a88d18ce  C[4]=e5a81f3e  D[4]=2a08cc20
A[5]=d30244f9  B[5]=39a9c2c6  C[5]=75c8a149  D[5]=d67246ea
A[6]=ad1d7e11  B[6]=c2837fc0  C[6]=5209ffcf  D[6]=b42d8926
A[7]=11d58d9b  B[7]=803430eb  C[7]=14fca54a  D[7]=f29c98b1

Feed-Forward Step 32: (r= 4, s=13)
A[0]=743c9628  B[0]=a01818fe  C[0]=cfa383a5  D[0]=81648494
A[1]=04f826a3  B[1]=888bcddd  C[1]=c6b16f92  D[1]=1ee9dd5e
A[2]=373620b4  B[2]=b1b55a86  C[2]=50b23e17  D[2]=19cb0396
A[3]=529b4d45  B[3]=69c8987e  C[3]=2a88840e  D[3]=04a7faf0
A[4]=4e86bca4  B[4]=806cdb71  C[4]=a88d18ce  D[4]=e5a81f3e
A[5]=eb4a0c59  B[5]=30244f9d  C[5]=39a9c2c6  D[5]=75c8a149
A[6]=102e0f27  B[6]=d1d7e11a  C[6]=c2837fc0  D[6]=5209ffcf
A[7]=218ff77f  B[7]=1d58d9b1  C[7]=803430eb  D[7]=14fca54a

Feed-Forward Step 33: (r=13, s=10)
A[0]=3ee1f796  B[0]=92c50e87  C[0]=a01818fe  D[0]=cfa383a5
A[1]=a767342e  B[1]=04d4609f  C[1]=888bcddd  D[1]=c6b16f92
A[2]=ac31df20  B[2]=c41686e6  C[2]=b1b55a86  D[2]=50b23e17
A[3]=77bfbe2f  B[3]=69a8aa53  C[3]=69c8987e  D[3]=2a88840e
A[4]=4685328b  B[4]=d79489d0  C[4]=806cdb71  D[4]=a88d18ce
A[5]=77fad5a7  B[5]=418b3d69  C[5]=30244f9d  D[5]=39a9c2c6
A[6]=b46fe687  B[6]=c1e4e205  C[6]=d1d7e11a  D[6]=c2837fc0
A[7]=a636f646  B[7]=feefe431  C[7]=1d58d9b1  D[7]=803430eb

Feed-Forward Step 34: (r=10, s=25)
A[0]=7e8d0500  B[0]=87de58fb  C[0]=92c50e87  D[0]=a01818fe
A[1]=9dd47c59  B[1]=9cd0ba9d  C[1]=04d4609f  D[1]=888bcddd
```

```
A[2]=dc9eda84  B[2]=c77c82b0  C[2]=c41686e6  D[2]=b1b55a86
A[3]=ee74aeba  B[3]=fef8bdde  C[3]=69a8aa53  D[3]=69c8987e
A[4]=c013518f  B[4]=14ca2d1a  C[4]=d79489d0  D[4]=806cdb71
A[5]=39a16263  B[5]=eb569ddf  C[5]=418b3d69  D[5]=30244f9d
A[6]=f8208e41  B[6]=bf9a1ed1  C[6]=c1e4e205  D[6]=d1d7e11a
A[7]=e573735f  B[7]=dbd91a98  C[7]=feefe431  D[7]=1d58d9b1

Feed-Forward Step 35: (r=25, s= 4)
A[0]=b3d26adb  B[0]=00fd1a0a  C[0]=87de58fb  D[0]=92c50e87
A[1]=c059fd99  B[1]=b33ba8f8  C[1]=9cd0ba9d  D[1]=04d4609f
A[2]=d4966d9d  B[2]=09b93db5  C[2]=c77c82b0  D[2]=c41686e6
A[3]=5ecfc18d  B[3]=75dce95d  C[3]=fef8bdde  D[3]=69a8aa53
A[4]=3fbe24d6  B[4]=1f8026a3  C[4]=14ca2d1a  D[4]=d79489d0
A[5]=ce60b25e  B[5]=c67342c4  C[5]=eb569ddf  D[5]=418b3d69
A[6]=0e60710a  B[6]=83f0411c  C[6]=bf9a1ed1  D[6]=c1e4e205
A[7]=173501d2  B[7]=bfcae6e6  C[7]=dbd91a98  D[7]=feefe431
```

Compression Function Output

```
A[0]=b3d26adb  B[0]=00fd1a0a  C[0]=87de58fb  D[0]=92c50e87
A[1]=c059fd99  B[1]=b33ba8f8  C[1]=9cd0ba9d  D[1]=04d4609f
A[2]=d4966d9d  B[2]=09b93db5  C[2]=c77c82b0  D[2]=c41686e6
A[3]=5ecfc18d  B[3]=75dce95d  C[3]=fef8bdde  D[3]=69a8aa53
A[4]=3fbe24d6  B[4]=1f8026a3  C[4]=14ca2d1a  D[4]=d79489d0
A[5]=ce60b25e  B[5]=c67342c4  C[5]=eb569ddf  D[5]=418b3d69
A[6]=0e60710a  B[6]=83f0411c  C[6]=bf9a1ed1  D[6]=c1e4e205
A[7]=173501d2  B[7]=bfcae6e6  C[7]=dbd91a98  D[7]=feefe431
```

Final block

```
M[  0..  7] = 00 04 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    6  110  198  227   45   48  240  162
```

```
y[  8.. 15] =   28  167  162   26  100  136  175   13
y[ 16.. 23] =  105   29   76  156   65  201   12  201
y[ 24.. 31] =   15   98    1   79  129  256  249   61
y[ 32.. 39] =  205   87   89  188  218  234  222   16
y[ 40.. 47] =    8   18  139  161  188  152  117  155
y[ 48.. 55] =  128  188  255   28   91  244   83  200
y[ 56.. 63] =   53   68  175   17  160   80  211  216
y[ 64.. 71] =   64  142   32   39  250  230  185  240
y[ 72.. 79] =    2  135    4   52   93  171   62   66
y[ 80.. 87] =  122  169  162   57   34  120   35  241
y[ 88.. 95] =   17  171    7   54  154  138   45  134
y[ 96..103] =  188   88  126  118  158  140    4  182
y[104..111] =  145  232   35  172  254  196   31    3
y[112..119] =  245   43   90   31   48   46   68   79
y[120..127] =  214   32   35   98  155  162   14   33
y[128..135] =  251  147   59   30  212  209   17   95
y[136..143] =  229   90   95  231  157  121   82  244
y[144..151] =  152  228  181  101  192   56  245   56
y[152..159] =  242  159  256  178  128    1    8  196
y[160..167] =   52  170  168   69   39   23   35  241
y[168..175] =  249  239  118   96   69  105  140  102
y[176..183] =  129   69    2  229  166   13  174   57
y[184..191] =  204  189   82  240   97  177   46   41
y[192..199] =  193  115  225  218    7   27   72   17
y[200..207] =  255  122  253  205  164   86  195  191
y[208..215] =  135   88   95  200  223  137  222   16
y[216..223] =  240   86  250  203  103  119  212  123
y[224..231] =   69  169  131  139   99  117  253   75
y[232..239] =  112   25  222   85    3   61  226  254
y[240..247] =   12  214  167  226  209  211  189  178
y[248..255] =   43  225  222  159  102   95  243  224
```

Intermediate Expanded Message

```
Z[ 0] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
Z[ 1] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
Z[ 2] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
Z[ 3] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
Z[ 4] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
        a7d60172  259402e4  c1da4335  2fb22cce
Z[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
Z[ 6] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
Z[ 7] = 1f13f754  1667410a  213e22b0  39173124
```

```
          1720e0ed  46d2194b  bb59b64a  17d90a1e
Z[ 8] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
          410aebc4  ed3644a7  5771b7bc  f69b3b42
Z[ 9] = eb0bb41f  48fdc914  2878d107  2878f754
          b92ef529  c6e9ff47  00b95c80  d3eb05c8
Z[10] = c1212594  31ddbfaf  109f1c2f  f470194b
          f2fefa38  45605546  4be131dd  49b6ab73
Z[11] = 31dda380  ebc40172  0965be3d  2931c405
          cedcd9b3  f3b73b42  c6304619  1da1213e
Z[12] = 531bd1c0  e3d1e8e0  1383050f  0c493408
          582afe8e  da6cfd1c  3e26bccb  d04ed332
Z[13] = 3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
          3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
Z[14] = c06831dd  aabaa4f2  548d478b  3633fd1c
          121150f0  3d6de6b5  2c15022b  fdd5e999
Z[15] = e0ed08ac  e999bef6  dec2dd50  c6e9cedc
          e8e01f13  b92ee6b5  44a749b6  e827f5e2
Z[16] = fa8a0576  35b3ca4d  d70b28f5  0f79f087
          e684197c  5677a989  a4fc5b04  4aa2b55e
Z[17] = a06f5f91  bad4452c  c4d73b29  f5140aec
          f2590da7  ff1700e9  74808b80  0748f8b8
Z[18] = 2f54d0ac  aeff5101  237fdc81  1fdbe025
          f8b80748  6b66949a  3ecdc133  95836a7d
Z[19] = 8b807480  01d2fe2e  ad2d52d3  b4754b8b
          cfc3303d  4aa2b55e  5849a7b7  29ded622
Z[20] = c5c03a40  e2e01d20  065ff9a1  4188be78
          fe2e01d2  fc5c03a4  ab5b54a5  c792386e
Z[21] = 90f66f0a  5677a989  e10e1ef2  e0251fdb
          f0870f79  f9a1065f  5dbfa241  d70b28f5
Z[22] = 3ecdc133  8d5272ae  5a1ba5e5  fc5c03a4
          65f09a10  e0251fdb  02bbfd45  e3c91c37
Z[23] = 0aecf514  ae1651ea  d4502bb0  c21c3de4
          2723d8dd  e0251fdb  5cd6a32a  f3420cbe
Z[24] = 9be2641e  1b4ee4b2  d4502bb0  5677a989
          51eaae16  e85617aa  6e2191df  f42b0bd5
Z[25] = e59b1a65  5beda413  32f8cd08  32f8cd08
          a6ce5932  b81947e7  00e9ff17  c87b3785
Z[26] = b0d14f2f  3ecdc133  14efeb11  f1700e90
          ef9e1062  5760a8a0  5f91a06f  5cd6a32a
Z[27] = 3ecdc133  e684197c  0bd5f42b  33e1cc1f
          c21c3de4  f0870f79  b73048d0  2551daaf
Z[28] = 68ab9755  dc81237f  1893e76d  0f79f087
          6f0a90f6  d0ac2f54  4e46b1ba  c3ee3c12
Z[29] = 5018afe8  cc1f33e1  92c86d38  0e90f170
          4e46b1ba  ceda3126  6c4f93b1  6ff3900d
Z[30] = afe85018  949a6b66  6a7d9583  4443bbbd
          16c1e93f  4d5db2a3  3785c87b  fd4502bb
Z[31] = d8dd2723  e3c91c37  d62229de  b81947e7
          e2e01d20  a6ce5932  5677a989  e1f71e09
```

Expanded Message

```
W[ 0] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
        a7d60172  259402e4  c1da4335  2fb22cce
W[ 1] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
W[ 2] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
W[ 3] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
W[ 4] = 1f13f754  1667410a  213e22b0  39173124
        1720e0ed  46d2194b  bb59b64a  17d90a1e
W[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
W[ 6] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
W[ 7] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
W[ 8] = e0ed08ac  e999bef6  dec2dd50  c6e9cedc
        e8e01f13  b92ee6b5  44a749b6  e827f5e2
W[ 9] = 31dda380  ebc40172  0965be3d  2931c405
        cedcd9b3  f3b73b42  c6304619  1da1213e
W[10] = 531bd1c0  e3d1e8e0  1383050f  0c493408
        582afe8e  da6cfd1c  3e26bccb  d04ed332
W[11] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
        410aebc4  ed3644a7  5771b7bc  f69b3b42
W[12] = eb0bb41f  48fdc914  2878d107  2878f754
        b92ef529  c6e9ff47  00b95c80  d3eb05c8
W[13] = 3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
        3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
W[14] = c1212594  31ddbfaf  109f1c2f  f470194b
        f2fefa38  45605546  4be131dd  49b6ab73
W[15] = c06831dd  aabaa4f2  548d478b  3633fd1c
        121150f0  3d6de6b5  2c15022b  fdd5e999
W[16] = a06f5f91  bad4452c  c4d73b29  f5140aec
        f2590da7  ff1700e9  74808b80  0748f8b8
W[17] = 2f54d0ac  aeff5101  237fdc81  1fdbe025
        f8b80748  6b66949a  3ecdc133  95836a7d
W[18] = 0aecf514  ae1651ea  d4502bb0  c21c3de4
        2723d8dd  e0251fdb  5cd6a32a  f3420cbe
W[19] = c5c03a40  e2e01d20  065ff9a1  4188be78
        fe2e01d2  fc5c03a4  ab5b54a5  c792386e
W[20] = 3ecdc133  8d5272ae  5a1ba5e5  fc5c03a4
        65f09a10  e0251fdb  02bbfd45  e3c91c37
W[21] = 90f66f0a  5677a989  e10e1ef2  e0251fdb
        f0870f79  f9a1065f  5dbfa241  d70b28f5
W[22] = fa8a0576  35b3ca4d  d70b28f5  0f79f087
        e684197c  5677a989  a4fc5b04  4aa2b55e
W[23] = 8b807480  01d2fe2e  ad2d52d3  b4754b8b
        cfc3303d  4aa2b55e  5849a7b7  29ded622
```

```
W[24] = afe85018  949a6b66  6a7d9583  4443bbbd
        16c1e93f  4d5db2a3  3785c87b  fd4502bb
W[25] = 9be2641e  1b4ee4b2  d4502bb0  5677a989
        51eaae16  e85617aa  6e2191df  f42b0bd5
W[26] = e59b1a65  5beda413  32f8cd08  32f8cd08
        a6ce5932  b81947e7  00e9ff17  c87b3785
W[27] = d8dd2723  e3c91c37  d62229de  b81947e7
        e2e01d20  a6ce5932  5677a989  e1f71e09
W[28] = 3ecdc133  e684197c  0bd5f42b  33e1cc1f
        c21c3de4  f0870f79  b73048d0  2551daaf
W[29] = 5018afe8  cc1f33e1  92c86d38  0e90f170
        4e46b1ba  ceda3126  6c4f93b1  6ff3900d
W[30] = 68ab9755  dc81237f  1893e76d  0f79f087
        6f0a90f6  d0ac2f54  4e46b1ba  c3ee3c12
W[31] = b0d14f2f  3ecdc133  14efeb11  f1700e90
        ef9e1062  5760a8a0  5f91a06f  5cd6a32a
```

Feistel Steps

```
IV :
A[0]=b3d26adb  B[0]=00fd1a0a  C[0]=87de58fb  D[0]=92c50e87
A[1]=c059fd99  B[1]=b33ba8f8  C[1]=9cd0ba9d  D[1]=04d4609f
A[2]=d4966d9d  B[2]=09b93db5  C[2]=c77c82b0  D[2]=c41686e6
A[3]=5ecfc18d  B[3]=75dce95d  C[3]=fef8bdde  D[3]=69a8aa53
A[4]=3fbe24d6  B[4]=1f8026a3  C[4]=14ca2d1a  D[4]=d79489d0
A[5]=ce60b25e  B[5]=c67342c4  C[5]=eb569ddf  D[5]=418b3d69
A[6]=0e60710a  B[6]=83f0411c  C[6]=bf9a1ed1  D[6]=c1e4e205
A[7]=173501d2  B[7]=bfcae6e6  C[7]=dbd91a98  D[7]=feefe431

IV XOR M :
A[0]=b3d26edb  B[0]=00fd1a0a  C[0]=87de58fb  D[0]=92c50e87
A[1]=c059fd99  B[1]=b33ba8f8  C[1]=9cd0ba9d  D[1]=04d4609f
A[2]=d4966d9d  B[2]=09b93db5  C[2]=c77c82b0  D[2]=c41686e6
A[3]=5ecfc18d  B[3]=75dce95d  C[3]=fef8bdde  D[3]=69a8aa53
A[4]=3fbe24d6  B[4]=1f8026a3  C[4]=14ca2d1a  D[4]=d79489d0
A[5]=ce60b25e  B[5]=c67342c4  C[5]=eb569ddf  D[5]=418b3d69
A[6]=0e60710a  B[6]=83f0411c  C[6]=bf9a1ed1  D[6]=c1e4e205
A[7]=173501d2  B[7]=bfcae6e6  C[7]=dbd91a98  D[7]=feefe431

Step  0: (r= 3, s=23)
A[0]=7b722ff9  B[0]=9e9376dd  C[0]=00fd1a0a  D[0]=87de58fb
A[1]=cc72456e  B[1]=02cfecce  C[1]=b33ba8f8  D[1]=9cd0ba9d
A[2]=bcd85302  B[2]=a4b36cee  C[2]=09b93db5  D[2]=c77c82b0
A[3]=79dc9ba7  B[3]=f67e0c6a  C[3]=75dce95d  D[3]=fef8bdde
A[4]=d9552852  B[4]=fdf126b1  C[4]=1f8026a3  D[4]=14ca2d1a
A[5]=07187159  B[5]=730592f6  C[5]=c67342c4  D[5]=eb569ddf
A[6]=4343eb4a  B[6]=73038850  C[6]=83f0411c  D[6]=bf9a1ed1
A[7]=578abd65  B[7]=b9a80e90  C[7]=bfcae6e6  D[7]=dbd91a98
```

```
Step  1: (r=23, s=17)
A[0]=61156621  B[0]=fcbdb917  C[0]=9e9376dd  D[0]=00fd1a0a
A[1]=b7be1024  B[1]=b7663922  C[1]=02cfecce  D[1]=b33ba8f8
A[2]=7924dbd7  B[2]=815e6c29  C[2]=a4b36cee  D[2]=09b93db5
A[3]=fefc067c  B[3]=d3bcee4d  C[3]=f67e0c6a  D[3]=75dce95d
A[4]=8716313f  B[4]=296caa94  C[4]=fdf126b1  D[4]=1f8026a3
A[5]=67b9d0e6  B[5]=ac838c38  C[5]=730592f6  D[5]=c67342c4
A[6]=46b2678a  B[6]=a521a1f5  C[6]=73038850  D[6]=83f0411c
A[7]=b66968ba  B[7]=b2abc55e  C[7]=b9a80e90  D[7]=bfcae6e6

Step  2: (r=17, s=27)
A[0]=a22784c2  B[0]=cc42c22a  C[0]=fcbdb917  D[0]=9e9376dd
A[1]=07a1b1d1  B[1]=20496f7c  C[1]=b7663922  D[1]=02cfecce
A[2]=e9d2c87d  B[2]=b7aef249  C[2]=815e6c29  D[2]=a4b36cee
A[3]=306916d7  B[3]=0cf9fdf8  C[3]=d3bcee4d  D[3]=f67e0c6a
A[4]=69d7686f  B[4]=627f0e2c  C[4]=296caa94  D[4]=fdf126b1
A[5]=39e388d4  B[5]=a1cccf73  C[5]=ac838c38  D[5]=730592f6
A[6]=e58c17c5  B[6]=cf148d64  C[6]=a521a1f5  D[6]=73038850
A[7]=95f39f00  B[7]=d1756cd2  C[7]=b2abc55e  D[7]=b9a80e90

Step  3: (r=27, s= 3)
A[0]=89f39bbb  B[0]=15113c26  C[0]=cc42c22a  D[0]=fcbdb917
A[1]=f9214acf  B[1]=883d0d8e  C[1]=20496f7c  D[1]=b7663922
A[2]=355eb5cf  B[2]=ef4e9643  C[2]=b7aef249  D[2]=815e6c29
A[3]=4578bbe4  B[3]=b98348b6  C[3]=0cf9fdf8  D[3]=d3bcee4d
A[4]=604556a3  B[4]=7b4ebb43  C[4]=627f0e2c  D[4]=296caa94
A[5]=ca62b204  B[5]=a1cf1c46  C[5]=a1cccf73  D[5]=ac838c38
A[6]=0416fb85  B[6]=2f2c60be  C[6]=cf148d64  D[6]=a521a1f5
A[7]=96ac371c  B[7]=04af9cf8  C[7]=d1756cd2  D[7]=b2abc55e

Step  4: (r= 3, s=23)
A[0]=9dea22cb  B[0]=4f9cdddc  C[0]=15113c26  D[0]=cc42c22a
A[1]=ff65b07f  B[1]=c90a567f  C[1]=883d0d8e  D[1]=20496f7c
A[2]=478eae86  B[2]=aaf5ae79  C[2]=ef4e9643  D[2]=b7aef249
A[3]=d3454334  B[3]=2bc5df22  C[3]=b98348b6  D[3]=0cf9fdf8
A[4]=9b5bc4d3  B[4]=022ab51b  C[4]=7b4ebb43  D[4]=627f0e2c
A[5]=34676ffd  B[5]=53159026  C[5]=a1cf1c46  D[5]=a1cccf73
A[6]=1d7da742  B[6]=20b7dc28  C[6]=2f2c60be  D[6]=cf148d64
A[7]=d525477f  B[7]=b561b8e4  C[7]=04af9cf8  D[7]=d1756cd2

Step  5: (r=23, s=17)
A[0]=6e2fe729  B[0]=65cef511  C[0]=4f9cdddc  D[0]=15113c26
A[1]=1fb6e423  B[1]=3fffb2d8  C[1]=c90a567f  D[1]=883d0d8e
A[2]=70d83022  B[2]=4323c757  C[2]=aaf5ae79  D[2]=ef4e9643
A[3]=2ec12840  B[3]=9a69a2a1  C[3]=2bc5df22  D[3]=b98348b6
A[4]=39fa21e8  B[4]=69cdade2  C[4]=022ab51b  D[4]=7b4ebb43
A[5]=24f5bb8a  B[5]=fe9a33b7  C[5]=53159026  D[5]=a1cf1c46
A[6]=8e3eff80  B[6]=a10ebed3  C[6]=20b7dc28  D[6]=2f2c60be
A[7]=ba751081  B[7]=bfea92a3  C[7]=b561b8e4  D[7]=04af9cf8
```

```
Step  6: (r=17, s=27)
A[0]=3e669061  B[0]=ce52dc5f  C[0]=65cef511  D[0]=4f9cdddc
A[1]=34f611ff  B[1]=c8463f6d  C[1]=3fffb2d8  D[1]=c90a567f
A[2]=c947f870  B[2]=6044e1b0  C[2]=4323c757  D[2]=aaf5ae79
A[3]=aedc1660  B[3]=50805d82  C[3]=9a69a2a1  D[3]=2bc5df22
A[4]=a505c89a  B[4]=43d073f4  C[4]=69cdade2  D[4]=022ab51b
A[5]=196bb412  B[5]=771449eb  C[5]=fe9a33b7  D[5]=53159026
A[6]=888ec279  B[6]=ff011c7d  C[6]=a10ebed3  D[6]=20b7dc28
A[7]=2db3e5e4  B[7]=210374ea  C[7]=bfea92a3  D[7]=b561b8e4

Step  7: (r=27, s= 3)
A[0]=906fa105  B[0]=09f33483  C[0]=ce52dc5f  D[0]=65cef511
A[1]=f2113fc8  B[1]=f9a7b08f  C[1]=c8463f6d  D[1]=3fffb2d8
A[2]=23a4d7c9  B[2]=864a3fc3  C[2]=6044e1b0  D[2]=4323c757
A[3]=76fa3337  B[3]=0576e0b3  C[3]=50805d82  D[3]=9a69a2a1
A[4]=e6e0acc5  B[4]=d5282e44  C[4]=43d073f4  D[4]=69cdade2
A[5]=2f5e42d4  B[5]=90cb5da0  C[5]=771449eb  D[5]=fe9a33b7
A[6]=69de903d  B[6]=cc447613  C[6]=ff011c7d  D[6]=a10ebed3
A[7]=4521b603  B[7]=216d9f2f  C[7]=210374ea  D[7]=bfea92a3

Step  8: (r=28, s=19)
A[0]=a762927e  B[0]=5906fa10  C[0]=09f33483  D[0]=ce52dc5f
A[1]=482b2a65  B[1]=8f2113fc  C[1]=f9a7b08f  D[1]=c8463f6d
A[2]=43312c02  B[2]=923a4d7c  C[2]=864a3fc3  D[2]=6044e1b0
A[3]=3479125b  B[3]=776fa333  C[3]=0576e0b3  D[3]=50805d82
A[4]=f5830c6e  B[4]=5e6e0acc  C[4]=d5282e44  D[4]=43d073f4
A[5]=9827e3ce  B[5]=42f5e42d  C[5]=90cb5da0  D[5]=771449eb
A[6]=7fdd19e9  B[6]=d69de903  C[6]=cc447613  D[6]=ff011c7d
A[7]=8aa75dae  B[7]=34521b60  C[7]=216d9f2f  D[7]=210374ea

Step  9: (r=19, s=22)
A[0]=fc148a96  B[0]=93f53b14  C[0]=5906fa10  D[0]=09f33483
A[1]=86350fbc  B[1]=532a4159  C[1]=8f2113fc  D[1]=f9a7b08f
A[2]=7fb14443  B[2]=60121989  C[2]=923a4d7c  D[2]=864a3fc3
A[3]=61d609da  B[3]=92d9a3c8  C[3]=776fa333  D[3]=0576e0b3
A[4]=cc25b4c5  B[4]=6377ac18  C[4]=5e6e0acc  D[4]=d5282e44
A[5]=43cf439a  B[5]=1e74c13f  C[5]=42f5e42d  D[5]=90cb5da0
A[6]=cdde9fcc  B[6]=cf4bfee8  C[6]=d69de903  D[6]=cc447613
A[7]=70ccbd0b  B[7]=ed74553a  C[7]=34521b60  D[7]=216d9f2f

Step 10: (r=22, s= 7)
A[0]=8958a179  B[0]=a5bf0522  C[0]=93f53b14  D[0]=5906fa10
A[1]=5db55045  B[1]=ef218d43  C[1]=532a4159  D[1]=8f2113fc
A[2]=e2c894ff  B[2]=10dfec51  C[2]=60121989  D[2]=923a4d7c
A[3]=029b5736  B[3]=76987582  C[3]=92d9a3c8  D[3]=776fa333
A[4]=2449a06e  B[4]=3173096d  C[4]=6377ac18  D[4]=5e6e0acc
A[5]=c9d3755d  B[5]=e690f3d0  C[5]=1e74c13f  D[5]=42f5e42d
A[6]=c229c8c4  B[6]=f33377a7  C[6]=cf4bfee8  D[6]=d69de903
```

```
A[7]=3ab7ef18  B[7]=42dc332f  C[7]=ed74553a  D[7]=34521b60

Step 11: (r= 7, s=28)
A[0]=d38f1ff1  B[0]=ac50bcc4  C[0]=a5bf0522  D[0]=93f53b14
A[1]=b40fdb11  B[1]=daa822ae  C[1]=ef218d43  D[1]=532a4159
A[2]=e2fde7c1  B[2]=644a7ff1  C[2]=10dfec51  D[2]=60121989
A[3]=79d35cb5  B[3]=4dab9b01  C[3]=76987582  D[3]=92d9a3c8
A[4]=9ad722de  B[4]=24d03712  C[4]=3173096d  D[4]=6377ac18
A[5]=0cbece68  B[5]=e9baaee4  C[5]=e690f3d0  D[5]=1e74c13f
A[6]=0d82cc77  B[6]=14e46261  C[6]=f33377a7  D[6]=cf4bfee8
A[7]=3376988d  B[7]=5bf78c1d  C[7]=42dc332f  D[7]=ed74553a

Step 12: (r=28, s=19)
A[0]=3bd08e88  B[0]=1d38f1ff  C[0]=ac50bcc4  D[0]=a5bf0522
A[1]=1c5cff53  B[1]=1b40fdb1  C[1]=daa822ae  D[1]=ef218d43
A[2]=53db383c  B[2]=1e2fde7c  C[2]=644a7ff1  D[2]=10dfec51
A[3]=ae97399c  B[3]=579d35cb  C[3]=4dab9b01  D[3]=76987582
A[4]=7c97a199  B[4]=e9ad722d  C[4]=24d03712  D[4]=3173096d
A[5]=99666f49  B[5]=80cbece6  C[5]=e9baaee4  D[5]=e690f3d0
A[6]=29c02aef  B[6]=70d82cc7  C[6]=14e46261  D[6]=f33377a7
A[7]=b5b19cae  B[7]=d3376988  C[7]=5bf78c1d  D[7]=42dc332f

Step 13: (r=19, s=22)
A[0]=7dd48ed7  B[0]=7441de84  C[0]=1d38f1ff  D[0]=ac50bcc4
A[1]=e1c4d9a7  B[1]=fa98e2e7  C[1]=1b40fdb1  D[1]=daa822ae
A[2]=e63d6b15  B[2]=c1e29ed9  C[2]=1e2fde7c  D[2]=644a7ff1
A[3]=55aa1fb1  B[3]=cce574b9  C[3]=579d35cb  D[3]=4dab9b01
A[4]=83b8ea50  B[4]=0ccbe4bd  C[4]=e9ad722d  D[4]=24d03712
A[5]=63eb409e  B[5]=7a4ccb33  C[5]=80cbece6  D[5]=e9baaee4
A[6]=01411b94  B[6]=57794e01  C[6]=70d82cc7  D[6]=14e46261
A[7]=9a8152a0  B[7]=e575ad8c  C[7]=d3376988  D[7]=5bf78c1d

Step 14: (r=22, s= 7)
A[0]=cb59092b  B[0]=b5df7523  C[0]=7441de84  D[0]=1d38f1ff
A[1]=d94d7727  B[1]=69f87136  C[1]=fa98e2e7  D[1]=1b40fdb1
A[2]=7912a924  B[2]=c5798f5a  C[2]=c1e29ed9  D[2]=1e2fde7c
A[3]=a9ee9225  B[3]=ec556a87  C[3]=cce574b9  D[3]=579d35cb
A[4]=e422bea0  B[4]=9420ee3a  C[4]=0ccbe4bd  D[4]=e9ad722d
A[5]=87875e82  B[5]=2798fad0  C[5]=7a4ccb33  D[5]=80cbece6
A[6]=b778022d  B[6]=e5005046  C[6]=57794e01  D[6]=70d82cc7
A[7]=56d0dc82  B[7]=a826a054  C[7]=e575ad8c  D[7]=d3376988

Step 15: (r= 7, s=28)
A[0]=b930beea  B[0]=ac8495e5  C[0]=b5df7523  D[0]=7441de84
A[1]=146b8287  B[1]=a6bb93ec  C[1]=69f87136  D[1]=fa98e2e7
A[2]=04a24bc7  B[2]=8954923c  C[2]=c5798f5a  D[2]=c1e29ed9
A[3]=8b5aab9b  B[3]=f74912d4  C[3]=ec556a87  D[3]=cce574b9
A[4]=e152ad59  B[4]=115f5072  C[4]=9420ee3a  D[4]=0ccbe4bd
A[5]=d5a57db6  B[5]=c3af4143  C[5]=2798fad0  D[5]=7a4ccb33
```

```
A[6]=25caecf4  B[6]=bc0116db  C[6]=e5005046  D[6]=57794e01
A[7]=0213b3e6  B[7]=686e412b  C[7]=a826a054  D[7]=e575ad8c

Step 16: (r=29, s= 9)
A[0]=e2bc36fb  B[0]=572617dd  C[0]=ac8495e5  D[0]=b5df7523
A[1]=c3a2e3b9  B[1]=e28d7050  C[1]=a6bb93ec  D[1]=69f87136
A[2]=7de6546d  B[2]=e0944978  C[2]=8954923c  D[2]=c5798f5a
A[3]=7011e3a2  B[3]=716b5573  C[3]=f74912d4  D[3]=ec556a87
A[4]=b32309c7  B[4]=3c2a55ab  C[4]=115f5072  D[4]=9420ee3a
A[5]=03613336  B[5]=dab4afb6  C[5]=c3af4143  D[5]=2798fad0
A[6]=3006fd0a  B[6]=84b95d9e  C[6]=bc0116db  D[6]=e5005046
A[7]=a4039cdf  B[7]=c042767c  C[7]=686e412b  D[7]=a826a054

Step 17: (r= 9, s=15)
A[0]=929d5e8c  B[0]=786df7c5  C[0]=572617dd  D[0]=ac8495e5
A[1]=65eedac3  B[1]=45c77387  C[1]=e28d7050  D[1]=a6bb93ec
A[2]=5cf1584e  B[2]=cca8dafb  C[2]=e0944978  D[2]=8954923c
A[3]=c67ef982  B[3]=23c744e0  C[3]=716b5573  D[3]=f74912d4
A[4]=aad49df3  B[4]=46138f66  C[4]=3c2a55ab  D[4]=115f5072
A[5]=076abf36  B[5]=c2666c06  C[5]=dab4afb6  D[5]=c3af4143
A[6]=7b10c3ed  B[6]=0dfa1460  C[6]=84b95d9e  D[6]=bc0116db
A[7]=763a1272  B[7]=0739bf48  C[7]=c042767c  D[7]=686e412b

Step 18: (r=15, s= 5)
A[0]=f3b75d76  B[0]=af46494e  C[0]=786df7c5  D[0]=572617dd
A[1]=e224e28d  B[1]=6d61b2f7  C[1]=45c77387  D[1]=e28d7050
A[2]=525c27e6  B[2]=ac272e78  C[2]=cca8dafb  D[2]=e0944978
A[3]=f78972c5  B[3]=7cc1633f  C[3]=23c744e0  D[3]=716b5573
A[4]=45208a20  B[4]=4ef9d56a  C[4]=46138f66  D[4]=3c2a55ab
A[5]=8897fddd  B[5]=5f9b03b5  C[5]=c2666c06  D[5]=dab4afb6
A[6]=4edc3233  B[6]=61f6bd88  C[6]=0dfa1460  D[6]=84b95d9e
A[7]=f13fb534  B[7]=09393b1d  C[7]=0739bf48  D[7]=c042767c

Step 19: (r= 5, s=29)
A[0]=c0fd4e5a  B[0]=76ebaede  C[0]=af46494e  D[0]=786df7c5
A[1]=c0f06e87  B[1]=449c51bc  C[1]=6d61b2f7  D[1]=45c77387
A[2]=6172e3e3  B[2]=4b84fcca  C[2]=ac272e78  D[2]=cca8dafb
A[3]=a908b34a  B[3]=f12e58be  C[3]=7cc1633f  D[3]=23c744e0
A[4]=613fd45a  B[4]=a4114408  C[4]=4ef9d56a  D[4]=46138f66
A[5]=6fc57368  B[5]=12ffbbb1  C[5]=5f9b03b5  D[5]=c2666c06
A[6]=b2ddae8c  B[6]=db864669  C[6]=61f6bd88  D[6]=0dfa1460
A[7]=48cd6c26  B[7]=27f6a69e  C[7]=09393b1d  D[7]=0739bf48

Step 20: (r=29, s= 9)
A[0]=a236a7c7  B[0]=581fa9cb  C[0]=76ebaede  D[0]=af46494e
A[1]=22aa869d  B[1]=f81e0dd0  C[1]=449c51bc  D[1]=6d61b2f7
A[2]=6d3b4af0  B[2]=6c2e5c7c  C[2]=4b84fcca  D[2]=ac272e78
A[3]=209131b6  B[3]=55211669  C[3]=f12e58be  D[3]=7cc1633f
A[4]=d41b29eb  B[4]=4c27fa8b  C[4]=a4114408  D[4]=4ef9d56a
```

```
A[5]=cd9d31d4  B[5]=0df8ae6d  C[5]=12ffbbb1  D[5]=5f9b03b5
A[6]=85aeb685  B[6]=965bb5d1  C[6]=db864669  D[6]=61f6bd88
A[7]=55345253  B[7]=c919ad84  C[7]=27f6a69e  D[7]=09393b1d

Step 21: (r= 9, s=15)
A[0]=89211383  B[0]=6d4f8f44  C[0]=581fa9cb  D[0]=76ebaede
A[1]=1e5da17f  B[1]=550d3a45  C[1]=f81e0dd0  D[1]=449c51bc
A[2]=f794e972  B[2]=7695e0da  C[2]=6c2e5c7c  D[2]=4b84fcca
A[3]=408247dd  B[3]=22636c41  C[3]=55211669  D[3]=f12e58be
A[4]=611aab65  B[4]=3653d7a8  C[4]=4c27fa8b  D[4]=a4114408
A[5]=19588b44  B[5]=3a63a99b  C[5]=0df8ae6d  D[5]=12ffbbb1
A[6]=f3e9d24c  B[6]=5d6d0b0b  C[6]=965bb5d1  D[6]=db864669
A[7]=e2c11dc7  B[7]=68a4a6aa  C[7]=c919ad84  D[7]=27f6a69e

Step 22: (r=15, s= 5)
A[0]=39ce7ceb  B[0]=89c1c490  C[0]=6d4f8f44  D[0]=581fa9cb
A[1]=5c8c9d3a  B[1]=d0bf8f2e  C[1]=550d3a45  D[1]=f81e0dd0
A[2]=7a5477c0  B[2]=74b97bca  C[2]=7695e0da  D[2]=6c2e5c7c
A[3]=5f13fe74  B[3]=23eea041  C[3]=22636c41  D[3]=55211669
A[4]=49e4a187  B[4]=55b2b08d  C[4]=3653d7a8  D[4]=4c27fa8b
A[5]=81f0b131  B[5]=45a20cac  C[5]=3a63a99b  D[5]=0df8ae6d
A[6]=87485b5a  B[6]=e92679f4  C[6]=5d6d0b0b  D[6]=965bb5d1
A[7]=3420bf79  B[7]=8ee3f160  C[7]=68a4a6aa  D[7]=c919ad84

Step 23: (r= 5, s=29)
A[0]=ac3cf570  B[0]=39cf9d67  C[0]=89c1c490  D[0]=6d4f8f44
A[1]=6c4fa3f0  B[1]=9193a74b  C[1]=d0bf8f2e  D[1]=550d3a45
A[2]=6bcdc1ca  B[2]=4a8ef80f  C[2]=74b97bca  D[2]=7695e0da
A[3]=3732f111  B[3]=e27fce8b  C[3]=23eea041  D[3]=22636c41
A[4]=974726da  B[4]=3c9430e9  C[4]=55b2b08d  D[4]=3653d7a8
A[5]=0f67b0d6  B[5]=3e162630  C[5]=45a20cac  D[5]=3a63a99b
A[6]=94166805  B[6]=e90b6b50  C[6]=e92679f4  D[6]=5d6d0b0b
A[7]=02094d91  B[7]=8417ef26  C[7]=8ee3f160  D[7]=68a4a6aa

Step 24: (r= 4, s=13)
A[0]=21d699f3  B[0]=c3cf570a  C[0]=39cf9d67  D[0]=89c1c490
A[1]=277b4bf1  B[1]=c4fa3f06  C[1]=9193a74b  D[1]=d0bf8f2e
A[2]=d3072700  B[2]=bcdc1ca6  C[2]=4a8ef80f  D[2]=74b97bca
A[3]=80d7483e  B[3]=732f1113  C[3]=e27fce8b  D[3]=23eea041
A[4]=6ecb6d49  B[4]=74726da9  C[4]=3c9430e9  D[4]=55b2b08d
A[5]=32755b21  B[5]=f67b0d60  C[5]=3e162630  D[5]=45a20cac
A[6]=a029dd22  B[6]=41668059  C[6]=e90b6b50  D[6]=e92679f4
A[7]=294b2c02  B[7]=2094d910  C[7]=8417ef26  D[7]=8ee3f160

Step 25: (r=13, s=10)
A[0]=785af74b  B[0]=d33e643a  C[0]=c3cf570a  D[0]=39cf9d67
A[1]=9234d7dd  B[1]=697e24ef  C[1]=c4fa3f06  D[1]=9193a74b
A[2]=bf8e6caf  B[2]=e4e01a60  C[2]=bcdc1ca6  D[2]=4a8ef80f
A[3]=92e5cb77  B[3]=e907d01a  C[3]=732f1113  D[3]=e27fce8b
```

```
A[4]=38ef555e  B[4]=6da92dd9  C[4]=74726da9  D[4]=3c9430e9
A[5]=80847deb  B[5]=ab64264e  C[5]=f67b0d60  D[5]=3e162630
A[6]=93c05e9b  B[6]=3ba45405  C[6]=41668059  D[6]=e90b6b50
A[7]=74017efc  B[7]=65804529  C[7]=2094d910  D[7]=8417ef26

Step 26: (r=10, s=25)
A[0]=b3e20607  B[0]=6bdd2de1  C[0]=d33e643a  D[0]=c3cf570a
A[1]=5bdf6d3f  B[1]=d35f7648  C[1]=697e24ef  D[1]=c4fa3f06
A[2]=803c5dbc  B[2]=39b2befe  C[2]=e4e01a60  D[2]=bcdc1ca6
A[3]=094289ba  B[3]=972dde4b  C[3]=e907d01a  D[3]=732f1113
A[4]=bfce15bb  B[4]=bd5578e3  C[4]=6da92dd9  D[4]=74726da9
A[5]=fd8c1c22  B[5]=11f7ae02  C[5]=ab64264e  D[5]=f67b0d60
A[6]=23daaec5  B[6]=017a6e4f  C[6]=3ba45405  D[6]=41668059
A[7]=133f7db8  B[7]=05fbf1d0  C[7]=65804529  D[7]=2094d910

Step 27: (r=25, s= 4)
A[0]=800dc28b  B[0]=0f67c40c  C[0]=6bdd2de1  D[0]=d33e643a
A[1]=0a271889  B[1]=7eb7beda  C[1]=d35f7648  D[1]=697e24ef
A[2]=092e0d6c  B[2]=790078bb  C[2]=39b2befe  D[2]=e4e01a60
A[3]=35098f3b  B[3]=74128513  C[3]=972dde4b  D[3]=e907d01a
A[4]=5ae3fed1  B[4]=777f9c2b  C[4]=bd5578e3  D[4]=6da92dd9
A[5]=91910ce5  B[5]=45fb1838  C[5]=11f7ae02  D[5]=ab64264e
A[6]=8ecafb36  B[6]=8a47b55d  C[6]=017a6e4f  D[6]=3ba45405
A[7]=f8890fb9  B[7]=70267efb  C[7]=05fbf1d0  D[7]=65804529

Step 28: (r= 4, s=13)
A[0]=dfb04c3b  B[0]=00dc28b8  C[0]=0f67c40c  D[0]=6bdd2de1
A[1]=30829dff  B[1]=a2718890  C[1]=7eb7beda  D[1]=d35f7648
A[2]=5a0a18ee  B[2]=92e0d6c0  C[2]=790078bb  D[2]=39b2befe
A[3]=f84b60fe  B[3]=5098f3b3  C[3]=74128513  D[3]=972dde4b
A[4]=c624e440  B[4]=ae3fed15  C[4]=777f9c2b  D[4]=bd5578e3
A[5]=767ce2d0  B[5]=1910ce59  C[5]=45fb1838  D[5]=11f7ae02
A[6]=7c178b42  B[6]=ecafb368  C[6]=8a47b55d  D[6]=017a6e4f
A[7]=a0a9f2d7  B[7]=8890fb9f  C[7]=70267efb  D[7]=05fbf1d0

Step 29: (r=13, s=10)
A[0]=9a1056b1  B[0]=09877bf6  C[0]=00dc28b8  D[0]=0f67c40c
A[1]=0777035d  B[1]=53bfe610  C[1]=a2718890  D[1]=7eb7beda
A[2]=8a9c995d  B[2]=431dcb41  C[2]=92e0d6c0  D[2]=790078bb
A[3]=031fc726  B[3]=6c1fdf09  C[3]=5098f3b3  D[3]=74128513
A[4]=b3784708  B[4]=9c8818c4  C[4]=ae3fed15  D[4]=777f9c2b
A[5]=96c5dfe2  B[5]=9c5a0ecf  C[5]=1910ce59  D[5]=45fb1838
A[6]=505c9d5d  B[6]=f1684f82  C[6]=ecafb368  D[6]=8a47b55d
A[7]=95b2d66a  B[7]=3e5af415  C[7]=8890fb9f  D[7]=70267efb

Step 30: (r=10, s=25)
A[0]=9566c5d6  B[0]=415ac668  C[0]=09877bf6  D[0]=00dc28b8
A[1]=51d9f8d4  B[1]=dc0d741d  C[1]=53bfe610  D[1]=a2718890
A[2]=138328de  B[2]=7265762a  C[2]=431dcb41  D[2]=92e0d6c0
```

```
A[3]=5794ccb6  B[3]=7f1c980c  C[3]=6c1fdf09  D[3]=5098f3b3
A[4]=bdbefa35  B[4]=e11c22cd  C[4]=9c8818c4  D[4]=ae3fed15
A[5]=7abf9a82  B[5]=177f8a5b  C[5]=9c5a0ecf  D[5]=1910ce59
A[6]=a0ae18d9  B[6]=72757541  C[6]=f1684f82  D[6]=ecafb368
A[7]=7120d9bd  B[7]=cb59aa56  C[7]=3e5af415  D[7]=8890fb9f

Step 31: (r=25, s= 4)
A[0]=9bf32774  B[0]=ad2acd8b  C[0]=415ac668  D[0]=09877bf6
A[1]=e9fae3c4  B[1]=a8a3b3f1  C[1]=dc0d741d  D[1]=53bfe610
A[2]=560675b0  B[2]=bc270651  C[2]=7265762a  D[2]=431dcb41
A[3]=bf88b287  B[3]=6caf2999  C[3]=7f1c980c  D[3]=6c1fdf09
A[4]=3285c578  B[4]=6b7b7df4  C[4]=e11c22cd  D[4]=9c8818c4
A[5]=a2517879  B[5]=04f57f35  C[5]=177f8a5b  D[5]=9c5a0ecf
A[6]=cfd098b8  B[6]=b3415c31  C[6]=72757541  D[6]=f1684f82
A[7]=7784ebda  B[7]=7ae241b3  C[7]=cb59aa56  D[7]=3e5af415

Feed-Forward Step 32: (r= 4, s=13)
A[0]=ba92b86a  B[0]=bf327749  C[0]=ad2acd8b  D[0]=415ac668
A[1]=5bccb19b  B[1]=9fae3c4e  C[1]=a8a3b3f1  D[1]=dc0d741d
A[2]=e02dc72a  B[2]=60675b05  C[2]=bc270651  D[2]=7265762a
A[3]=762d727d  B[3]=f88b287b  C[3]=6caf2999  D[3]=7f1c980c
A[4]=94603439  B[4]=285c5783  C[4]=6b7b7df4  D[4]=e11c22cd
A[5]=169e8750  B[5]=2517879a  C[5]=04f57f35  D[5]=177f8a5b
A[6]=c04adee0  B[6]=fd098b8c  C[6]=b3415c31  D[6]=72757541
A[7]=87570512  B[7]=784ebda7  C[7]=7ae241b3  D[7]=cb59aa56

Feed-Forward Step 33: (r=13, s=10)
A[0]=29fb3cf0  B[0]=570d5752  C[0]=bf327749  D[0]=ad2acd8b
A[1]=3d1a1534  B[1]=96336b79  C[1]=9fae3c4e  D[1]=a8a3b3f1
A[2]=e8c6c6b4  B[2]=b8e55c05  C[2]=60675b05  D[2]=bc270651
A[3]=1934bc42  B[3]=ae4faec5  C[3]=f88b287b  D[3]=6caf2999
A[4]=8cec8474  B[4]=0687328c  C[4]=285c5783  D[4]=6b7b7df4
A[5]=6416af8e  B[5]=d0ea02d3  C[5]=2517879a  D[5]=04f57f35
A[6]=5337271e  B[6]=5bdc1809  C[6]=fd098b8c  D[6]=b3415c31
A[7]=8268d362  B[7]=e0a250ea  C[7]=784ebda7  D[7]=7ae241b3

Feed-Forward Step 34: (r=10, s=25)
A[0]=71a9f72e  B[0]=ecf3c0a7  C[0]=570d5752  D[0]=bf327749
A[1]=6c768ec0  B[1]=6854d0f4  C[1]=96336b79  D[1]=9fae3c4e
A[2]=e8f58b18  B[2]=1b1ad3a3  C[2]=b8e55c05  D[2]=60675b05
A[3]=83f5f930  B[3]=d2f10864  C[3]=ae4faec5  D[3]=f88b287b
A[4]=183d74a4  B[4]=b211d233  C[4]=0687328c  D[4]=285c5783
A[5]=b4b76f33  B[5]=5abe3990  C[5]=d0ea02d3  D[5]=2517879a
A[6]=2ffec3aa  B[6]=dc9c794c  C[6]=5bdc1809  D[6]=fd098b8c
A[7]=378ecc16  B[7]=a34d8a09  C[7]=e0a250ea  D[7]=784ebda7

Feed-Forward Step 35: (r=25, s= 4)
A[0]=0aad5188  B[0]=5ce353ee  C[0]=ecf3c0a7  D[0]=570d5752
A[1]=4a6b4257  B[1]=80d8ed1d  C[1]=6854d0f4  D[1]=96336b79
```

```
A[2]=29f37af5  B[2]=31d1eb16  C[2]=1b1ad3a3  D[2]=b8e55c05
A[3]=44c00647  B[3]=6107ebf2  C[3]=d2f10864  D[3]=ae4faec5
A[4]=cfaca68f  B[4]=48307ae9  C[4]=b211d233  D[4]=0687328c
A[5]=c23f6824  B[5]=67696ede  C[5]=5abe3990  D[5]=d0ea02d3
A[6]=e51b8739  B[6]=545ffd87  C[6]=dc9c794c  D[6]=5bdc1809
A[7]=fb13a98c  B[7]=2c6f1d98  C[7]=a34d8a09  D[7]=e0a250ea
```

Compression Function Output

```
A[0]=0aad5188  B[0]=5ce353ee  C[0]=ecf3c0a7  D[0]=570d5752
A[1]=4a6b4257  B[1]=80d8ed1d  C[1]=6854d0f4  D[1]=96336b79
A[2]=29f37af5  B[2]=31d1eb16  C[2]=1b1ad3a3  D[2]=b8e55c05
A[3]=44c00647  B[3]=6107ebf2  C[3]=d2f10864  D[3]=ae4faec5
A[4]=cfaca68f  B[4]=48307ae9  C[4]=b211d233  D[4]=0687328c
A[5]=c23f6824  B[5]=67696ede  C[5]=5abe3990  D[5]=d0ea02d3
A[6]=e51b8739  B[6]=545ffd87  C[6]=dc9c794c  D[6]=5bdc1809
A[7]=fb13a98c  B[7]=2c6f1d98  C[7]=a34d8a09  D[7]=e0a250ea
```

Hash Function Output

```
8851ad0a57426b4af57af3294706c0448fa6accf24683fc239871be58ca913fbee53e35c1dedd88016ebd131f2eb0761e
```

A.4.3 Two-block Message

We use the message made of 1079 `1` bits.

First block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
M[ 64.. 71] = ff ff ff ff ff ff ff ff
M[ 72.. 79] = ff ff ff ff ff ff ff ff
M[ 80.. 87] = ff ff ff ff ff ff ff ff
M[ 88.. 95] = ff ff ff ff ff ff ff ff
M[ 96..103] = ff ff ff ff ff ff ff ff
M[104..111] = ff ff ff ff ff ff ff ff
M[112..119] = ff ff ff ff ff ff ff ff
M[120..127] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =    2   86   98  227   95   77   58  143
y[  8.. 15] =   30   88  113  180   23   99  198   13
y[ 16.. 23] =  129   99   49  124  176  112   29   25
```

```
y[ 24.. 31] =   15   75  185   88  140  162   99  143
y[ 32.. 39] =  193   12  153  234   88   32  143  123
y[ 40.. 47] =  136  228  221  198   70  243  178  116
y[ 48.. 55] =  225  137  205    0   44    3  200  137
y[ 56.. 63] =   68   61  239  127   35  160   89  129
y[ 64.. 71] =  241   24  231  210   22  182  100  124
y[ 72.. 79] =   34   91  248   64  146  239  173   25
y[ 80.. 87] =  249   80  244  174   11   64   50   18
y[ 88.. 95] =   17  161  124   95   73  100  215  156
y[ 96..103] =  253  250  122   18  134  251   25  162
y[104..111] =  137  234   62   10  165  228  236   41
y[112..119] =  255  140   61   62   67  176  141  238
y[120..127] =  197  205   31  131  211   74  118   53
y[128..135] =  256  253  159   94  162  227  199   89
y[136..143] =  227  118  144   32  234  217   59  152
y[144..151] =  128  177  208  172   81  165  228  147
y[152..159] =  242  179   72  170  117  128  158  176
y[160..167] =   64   85  104  220  169  115  114  114
y[168..175] =  121   95   36  140  187  171   79  181
y[176..183] =   32  233   52  163  213   31   57   89
y[184..191] =  189  205   18  166  222  123  168   76
y[192..199] =   16   20   26   13  235   31  157  116
y[200..207] =  223  189    9  151  111  104   84  111
y[208..215] =    8  129   13  175  246  104  207  165
y[216..223] =  240  108  133    7  184  209   42  253
y[224..231] =    4  194  135  198  123  254  232   90
y[232..239] =  120  100  195  219   92  239   21  189
y[240..247] =    2  201  196  128  190  118  116   62
y[248..255] =   60   69  226   71   46  111  139  114
```

Intermediate Expanded Message

```
Z[ 0] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
Z[ 1] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
Z[ 2] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
Z[ 3] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
Z[ 4] = 1158f470  de09ed36  c9cd0fe6  599c4844
        41c31892  2e40f97f  f2feafc9  1211c34c
Z[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
        baa00c49  44a7599c  484434c1  b703e1a6
Z[ 6] = faf1fd1c  0d02582a  fbaaa71d  bb591211
        ef61a948  073a2cce  eb0bbd84  1da1f0d3
Z[ 7] = ab73fe8e  2cce2c15  c577306b  f245ac2c
        da6cd4a4  a4f21667  357adec2  264d5546
Z[ 8] = fd1cff47  43eeb92e  ea52bb59  4051d616
```

```
        5546ea52  1720ae57  e318ef61  b41f2aa3
Z[ 9] = c6305c80  c293dc97  bd843a89  b082eb0b
        c7a2f529  c1213408  5c80548d  c577b875
Z[10] = 3d6d2e40  e5434b28  531bc068  52625262
        44a75771  ab731a04  c1dacd6a  c9143917
Z[11] = eea81720  bc122594  1667e034  40512931
        da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
Z[12] = 0e740b90  096512ca  1667f01a  53d4b7bc
        cedce76e  b3660681  4b285037  50373cb4
Z[13] = a38005c8  c4be0965  4b28f80d  bd84dbde
        4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
Z[14] = d27902e4  d55da7d6  fdd558e3  410aedef
        484456b8  e48ad332  f2fe427c  cedc0f2d
Z[15] = d7880172  5c80d3eb  5546cf95  2cce53d4
        31dd2b5c  334fe999  5037213e  5262aaba
Z[16] = ff1701d2  a6ce5932  a9895677  cb3634ca
        e4b21b4e  992766d9  eb1114ef  35b3ca4d
Z[17] = 74808b80  d3672c99  49b9b647  e59b1a65
        f2590da7  4188be78  6a7d9583  a5e55a1b
Z[18] = 3a40c5c0  5ea8a158  afe85018  67c2983e
        6e2191df  20c4df3c  c04a3fb6  47e7b819
Z[19] = 1d20e2e0  2f54d0ac  d7f4280c  33e1cc1f
        c21c3de4  1062ef9e  e0251fdb  aeff5101
Z[20] = 0e90f170  17aae856  ebfa1406  a4fc5b04
        e10e1ef2  0831f7cf  65079af9  4c74b38c
Z[21] = 0748f8b8  0bd5f42b  f5fd0a03  d27e2d82
        f0870f79  8f2470dc  bd8f4271  263ad9c6
Z[22] = 03a4fc5c  90f66f0a  6ff3900d  e93f16c1
        6d3892c8  c792386e  53bcac44  131dece3
Z[23] = 01d2fe2e  c87b3785  c3053cfb  6994966c
        369cc964  e3c91c37  29ded622  949a6b66
Z[24] = fc5c4e46  558ee4b2  e4b24615  5101983e
        6b665018  1d20b9eb  db985a1b  a06f0bd5
Z[25] = b7305a1b  b2a370dc  ac4465f0  9be216c1
        b9024443  b0d15018  7480a989  b647983e
Z[26] = 4d5d0aec  de53eb11  68ab1d20  67c26ff3
        5677e59b  9583ca4d  b1baf342  bad46994
Z[27] = ea2892c8  aa720000  1c3702bb  510192c8
        d0ac3785  ad2d7397  6ff3a7b7  452c8b80
Z[28] = 123415d8  0bd5d539  1c37bbbd  699470dc
        c21c52d3  9f863a40  5ea8ef9e  650716c1
Z[29] = 8b8048d0  b55eb475  5ea83a40  ac441062
        624ca8a0  065f5677  d4505b04  fc5ca413
Z[30] = c6a9f9a1  ca4d1062  fd45fa8a  51eaa989
        5b04eb11  dd6a091a  ef9ee59b  c21c2551
Z[31] = cd089583  7480386e  6b66b647  386eeeb5
        3ecdd0ac  409f8d52  6507435a  67c2303d
```

Expanded Message

```
W[ 0] = 1158f470  de09ed36  c9cd0fe6  599c4844
        41c31892  2e40f97f  f2feafc9  1211c34c
W[ 1] = faf1fd1c  0d02582a  fbaaa71d  bb591211
        ef61a948  073a2cce  eb0bbd84  1da1f0d3
W[ 2] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
W[ 3] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
W[ 4] = ab73fe8e  2cce2c15  c577306b  f245ac2c
        da6cd4a4  a4f21667  357adec2  264d5546
W[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
        baa00c49  44a7599c  484434c1  b703e1a6
W[ 6] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
W[ 7] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
W[ 8] = d7880172  5c80d3eb  5546cf95  2cce53d4
        31dd2b5c  334fe999  5037213e  5262aaba
W[ 9] = eea81720  bc122594  1667e034  40512931
        da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
W[10] = 0e740b90  096512ca  1667f01a  53d4b7bc
        cedce76e  b3660681  4b285037  50373cb4
W[11] = fd1cff47  43eeb92e  ea52bb59  4051d616
        5546ea52  1720ae57  e318ef61  b41f2aa3
W[12] = c6305c80  c293dc97  bd843a89  b082eb0b
        c7a2f529  c1213408  5c80548d  c577b875
W[13] = a38005c8  c4be0965  4b28f80d  bd84dbde
        4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
W[14] = 3d6d2e40  e5434b28  531bc068  52625262
        44a75771  ab731a04  c1dacd6a  c9143917
W[15] = d27902e4  d55da7d6  fdd558e3  410aedef
        484456b8  e48ad332  f2fe427c  cedc0f2d
W[16] = 74808b80  d3672c99  49b9b647  e59b1a65
        f2590da7  4188be78  6a7d9583  a5e55a1b
W[17] = 3a40c5c0  5ea8a158  afe85018  67c2983e
        6e2191df  20c4df3c  c04a3fb6  47e7b819
W[18] = 01d2fe2e  c87b3785  c3053cfb  6994966c
        369cc964  e3c91c37  29ded622  949a6b66
W[19] = 0e90f170  17aae856  ebfa1406  a4fc5b04
        e10e1ef2  0831f7cf  65079af9  4c74b38c
W[20] = 03a4fc5c  90f66f0a  6ff3900d  e93f16c1
        6d3892c8  c792386e  53bcac44  131dece3
W[21] = 0748f8b8  0bd5f42b  f5fd0a03  d27e2d82
        f0870f79  8f2470dc  bd8f4271  263ad9c6
W[22] = ff1701d2  a6ce5932  a9895677  cb3634ca
        e4b21b4e  992766d9  eb1114ef  35b3ca4d
W[23] = 1d20e2e0  2f54d0ac  d7f4280c  33e1cc1f
        c21c3de4  1062ef9e  e0251fdb  aeff5101
W[24] = c6a9f9a1  ca4d1062  fd45fa8a  51eaa989
```

```
        5b04eb11  dd6a091a  ef9ee59b  c21c2551
W[25] = fc5c4e46  558ee4b2  e4b24615  5101983e
        6b665018  1d20b9eb  db985a1b  a06f0bd5
W[26] = b7305a1b  b2a370dc  ac4465f0  9be216c1
        b9024443  b0d15018  7480a989  b647983e
W[27] = cd089583  7480386e  6b66b647  386eeeb5
        3ecdd0ac  409f8d52  6507435a  67c2303d
W[28] = ea2892c8  aa720000  1c3702bb  510192c8
        d0ac3785  ad2d7397  6ff3a7b7  452c8b80
W[29] = 8b8048d0  b55eb475  5ea83a40  ac441062
        624ca8a0  065f5677  d4505b04  fc5ca413
W[30] = 123415d8  0bd5d539  1c37bbbd  699470dc
        c21c52d3  9f863a40  5ea8ef9e  650716c1
W[31] = 4d5d0aec  de53eb11  68ab1d20  67c26ff3
        5677e59b  9583ca4d  b1baf342  bad46994
```

Feistel Steps

```
IV :
A[0]=0ba16b95  B[0]=ac506643  C[0]=7eef60a1  D[0]=09254899
A[1]=72f999ad  B[1]=a90635a5  C[1]=6b70e3e8  D[1]=d699c7bc
A[2]=9fecc2ae  B[2]=e25b878b  C[2]=9c1714d1  D[2]=9019b6dc
A[3]=ba3264fc  B[3]=aab7878f  C[3]=b958e2a8  D[3]=2b9022e4
A[4]=5e894929  B[4]=88817f7a  C[4]=ab02675e  D[4]=8fa14956
A[5]=8e9f30e5  B[5]=0a02892b  C[5]=ed1c014f  D[5]=21bf9bd3
A[6]=2f1daa37  B[6]=559a7550  C[6]=cd8d65bb  D[6]=b94d0943
A[7]=f0f2c558  B[7]=598f657e  C[7]=fdb7a257  D[7]=6ffddc22

IV XOR M :
A[0]=f45e946a  B[0]=53af99bc  C[0]=81109f5e  D[0]=f6dab766
A[1]=8d066652  B[1]=56f9ca5a  C[1]=948f1c17  D[1]=29663843
A[2]=60133d51  B[2]=1da47874  C[2]=63e8eb2e  D[2]=6fe64923
A[3]=45cd9b03  B[3]=55487870  C[3]=46a71d57  D[3]=d46fdd1b
A[4]=a176b6d6  B[4]=777e8085  C[4]=54fd98a1  D[4]=705eb6a9
A[5]=7160cf1a  B[5]=f5fd76d4  C[5]=12e3feb0  D[5]=de40642c
A[6]=d0e255c8  B[6]=aa658aaf  C[6]=32729a44  D[6]=46b2f6bc
A[7]=0f0d3aa7  B[7]=a6709a81  C[7]=02485da8  D[7]=900223dd

Step  0: (r= 3, s=23)
A[0]=f15fd3b7  B[0]=a2f4a357  C[0]=53af99bc  D[0]=81109f5e
A[1]=8b02a016  B[1]=68333294  C[1]=56f9ca5a  D[1]=948f1c17
A[2]=f20ba643  B[2]=0099ea8b  C[2]=1da47874  D[2]=63e8eb2e
A[3]=da54a5ab  B[3]=2e6cd81a  C[3]=55487870  D[3]=46a71d57
A[4]=7b1a897e  B[4]=0bb5b6b5  C[4]=777e8085  D[4]=54fd98a1
A[5]=3975e91f  B[5]=8b0678d3  C[5]=f5fd76d4  D[5]=12e3feb0
A[6]=0157e650  B[6]=8712ae46  C[6]=aa658aaf  D[6]=32729a44
A[7]=e066d869  B[7]=7869d538  C[7]=a6709a81  D[7]=02485da8

Step  1: (r=23, s=17)
```

```
A[0]=7732e9e1  B[0]=dbf8afe9  C[0]=a2f4a357  D[0]=53af99bc
A[1]=f22c3085  B[1]=0b458150  C[1]=68333294  D[1]=56f9ca5a
A[2]=d84267c7  B[2]=21f905d3  C[2]=0099ea8b  D[2]=1da47874
A[3]=9f20dd8e  B[3]=d5ed2a52  C[3]=2e6cd81a  D[3]=55487870
A[4]=a735ad7a  B[4]=bf3d8d44  C[4]=0bb5b6b5  D[4]=777e8085
A[5]=2a90f9a7  B[5]=8f9cbaf4  C[5]=8b0678d3  D[5]=f5fd76d4
A[6]=e968414b  B[6]=2800abf3  C[6]=8712ae46  D[6]=aa658aaf
A[7]=4d8c8e06  B[7]=34f0336c  C[7]=7869d538  D[7]=a6709a81

Step  2: (r=17, s=27)
A[0]=fabe02bd  B[0]=d3c2ee65  C[0]=dbf8afe9  D[0]=a2f4a357
A[1]=9d7856da  B[1]=610be458  C[1]=0b458150  D[1]=68333294
A[2]=067408bc  B[2]=cf8fb084  C[2]=21f905d3  D[2]=0099ea8b
A[3]=c6ce79ab  B[3]=bb1d3e41  C[3]=d5ed2a52  D[3]=2e6cd81a
A[4]=45ce347f  B[4]=5af54e6b  C[4]=bf3d8d44  D[4]=0bb5b6b5
A[5]=a65c1724  B[5]=f34e5521  C[5]=8f9cbaf4  D[5]=8b0678d3
A[6]=03f568bf  B[6]=8297d2d0  C[6]=2800abf3  D[6]=8712ae46
A[7]=ca741339  B[7]=1c0c9b19  C[7]=34f0336c  D[7]=7869d538

Step  3: (r=27, s= 3)
A[0]=595797b0  B[0]=efd5f015  C[0]=d3c2ee65  D[0]=dbf8afe9
A[1]=b5490667  B[1]=d4ebc2b6  C[1]=610be458  D[1]=0b458150
A[2]=cf254207  B[2]=e033a045  C[2]=cf8fb084  D[2]=21f905d3
A[3]=c3c3f05d  B[3]=5e3673cd  C[3]=bb1d3e41  D[3]=d5ed2a52
A[4]=5c0b0618  B[4]=fa2e71a3  C[4]=5af54e6b  D[4]=bf3d8d44
A[5]=59a8913d  B[5]=2532e0b9  C[5]=f34e5521  D[5]=8f9cbaf4
A[6]=6188061e  B[6]=f81fab45  C[6]=8297d2d0  D[6]=2800abf3
A[7]=4044ed93  B[7]=ce53a099  C[7]=1c0c9b19  D[7]=34f0336c

Step  4: (r= 3, s=23)
A[0]=23762c3c  B[0]=cabcbd82  C[0]=efd5f015  D[0]=d3c2ee65
A[1]=cdeee07b  B[1]=aa48333d  C[1]=d4ebc2b6  D[1]=610be458
A[2]=2402b885  B[2]=792a103e  C[2]=e033a045  D[2]=cf8fb084
A[3]=7211d617  B[3]=1e1f82ee  C[3]=5e3673cd  D[3]=bb1d3e41
A[4]=b4422011  B[4]=e05830c2  C[4]=fa2e71a3  D[4]=5af54e6b
A[5]=150f9a53  B[5]=cd4489ea  C[5]=2532e0b9  D[5]=f34e5521
A[6]=a2be9074  B[6]=0c4030f3  C[6]=f81fab45  D[6]=8297d2d0
A[7]=9efdd157  B[7]=02276c9a  C[7]=ce53a099  D[7]=1c0c9b19

Step  5: (r=23, s=17)
A[0]=f53371f9  B[0]=1e11bb16  C[0]=cabcbd82  D[0]=efd5f015
A[1]=b4b74341  B[1]=3de6f770  C[1]=aa48333d  D[1]=d4ebc2b6
A[2]=fa8343b1  B[2]=4292015c  C[2]=792a103e  D[2]=e033a045
A[3]=733e6d7e  B[3]=0bb908eb  C[3]=1e1f82ee  D[3]=5e3673cd
A[4]=222714aa  B[4]=08da2110  C[4]=e05830c2  D[4]=fa2e71a3
A[5]=b2027b54  B[5]=298a87cd  C[5]=cd4489ea  D[5]=2532e0b9
A[6]=adf3dd65  B[6]=3a515f48  C[6]=0c4030f3  D[6]=f81fab45
A[7]=d8c67e26  B[7]=abcf7ee8  C[7]=02276c9a  D[7]=ce53a099
```

```
Step  6: (r=17, s=27)
A[0]=650ec8e2  B[0]=e3f3ea66  C[0]=1e11bb16  D[0]=cabcbd82
A[1]=9337fc88  B[1]=8683696e  C[1]=3de6f770  D[1]=aa48333d
A[2]=25b261f1  B[2]=8763f506  C[2]=4292015c  D[2]=792a103e
A[3]=4d63a428  B[3]=dafce67c  C[3]=0bb908eb  D[3]=1e1f82ee
A[4]=2e28d900  B[4]=2954444e  C[4]=08da2110  D[4]=e05830c2
A[5]=9fd3546a  B[5]=f6a96404  C[5]=298a87cd  D[5]=cd4489ea
A[6]=1656b615  B[6]=bacb5be7  C[6]=3a515f48  D[6]=0c4030f3
A[7]=82e1c178  B[7]=fc4db18c  C[7]=abcf7ee8  D[7]=02276c9a

Step  7: (r=27, s= 3)
A[0]=0f7c1b27  B[0]=13287647  C[0]=e3f3ea66  D[0]=1e11bb16
A[1]=ef8b16bb  B[1]=4499bfe4  C[1]=8683696e  D[1]=3de6f770
A[2]=d0d4d56f  B[2]=892d930f  C[2]=8763f506  D[2]=4292015c
A[3]=6a7f756a  B[3]=426b1d21  C[3]=dafce67c  D[3]=0bb908eb
A[4]=4c1a7f6c  B[4]=017146c8  C[4]=2954444e  D[4]=08da2110
A[5]=64b6183e  B[5]=54fe9aa3  C[5]=f6a96404  D[5]=298a87cd
A[6]=d380eb63  B[6]=a8b2b5b0  C[6]=bacb5be7  D[6]=3a515f48
A[7]=7d4fe61a  B[7]=c4170e0b  C[7]=fc4db18c  D[7]=abcf7ee8

Step  8: (r=28, s=19)
A[0]=b3b6d8e3  B[0]=70f7c1b2  C[0]=13287647  D[0]=e3f3ea66
A[1]=01d3f5eb  B[1]=bef8b16b  C[1]=4499bfe4  D[1]=8683696e
A[2]=d4c29ffa  B[2]=fd0d4d56  C[2]=892d930f  D[2]=8763f506
A[3]=85e3bd1a  B[3]=a6a7f756  C[3]=426b1d21  D[3]=dafce67c
A[4]=92c02db2  B[4]=c4c1a7f6  C[4]=017146c8  D[4]=2954444e
A[5]=12e99425  B[5]=e64b6183  C[5]=54fe9aa3  D[5]=f6a96404
A[6]=02495c53  B[6]=3d380eb6  C[6]=a8b2b5b0  D[6]=bacb5be7
A[7]=c87ec335  B[7]=a7d4fe61  C[7]=c4170e0b  D[7]=fc4db18c

Step  9: (r=19, s=22)
A[0]=0ad77cce  B[0]=c71d9db6  C[0]=70f7c1b2  D[0]=13287647
A[1]=85360aaf  B[1]=af580e9f  C[1]=bef8b16b  D[1]=4499bfe4
A[2]=6b7c5bee  B[2]=ffd6a614  C[2]=fd0d4d56  D[2]=892d930f
A[3]=e7908d10  B[3]=e8d42f1d  C[3]=a6a7f756  D[3]=426b1d21
A[4]=abb97ee8  B[4]=6d949601  C[4]=c4c1a7f6  D[4]=017146c8
A[5]=fc2d1554  B[5]=a128974c  C[5]=e64b6183  D[5]=54fe9aa3
A[6]=8143b07d  B[6]=e298124a  C[6]=3d380eb6  D[6]=a8b2b5b0
A[7]=7ad67b5b  B[7]=19ae43f6  C[7]=a7d4fe61  D[7]=c4170e0b

Step 10: (r=22, s= 7)
A[0]=2d49aaec  B[0]=3382b5df  C[0]=c71d9db6  D[0]=70f7c1b2
A[1]=e7621d9c  B[1]=abe14d82  C[1]=af580e9f  D[1]=bef8b16b
A[2]=2125ec51  B[2]=fb9adf16  C[2]=ffd6a614  D[2]=fd0d4d56
A[3]=af2ccf9a  B[3]=4439e423  C[3]=e8d42f1d  D[3]=a6a7f756
A[4]=e6415bbd  B[4]=ba2aee5f  C[4]=6d949601  D[4]=c4c1a7f6
A[5]=86ebc6c1  B[5]=553f0b45  C[5]=a128974c  D[5]=e64b6183
A[6]=5ed1641d  B[6]=1f6050ec  C[6]=e298124a  D[6]=3d380eb6
A[7]=a4b40737  B[7]=d6deb59e  C[7]=19ae43f6  D[7]=a7d4fe61
```

```
Step 11: (r= 7, s=28)
A[0]=eaf5f830  B[0]=a4d57616  C[0]=3382b5df  D[0]=c71d9db6
A[1]=eb93d694  B[1]=b10ece73  C[1]=abe14d82  D[1]=af580e9f
A[2]=9876c93e  B[2]=92f62890  C[2]=fb9adf16  D[2]=ffd6a614
A[3]=9b7139c6  B[3]=9667cd57  C[3]=4439e423  D[3]=e8d42f1d
A[4]=0d68a479  B[4]=20addef3  C[4]=ba2aee5f  D[4]=6d949601
A[5]=16fee848  B[5]=75e360c3  C[5]=553f0b45  D[5]=a128974c
A[6]=f451625d  B[6]=68b20eaf  C[6]=1f6050ec  D[6]=e298124a
A[7]=428f4f7d  B[7]=5a039bd2  C[7]=d6deb59e  D[7]=19ae43f6

Step 12: (r=28, s=19)
A[0]=468a7616  B[0]=0eaf5f83  C[0]=a4d57616  D[0]=3382b5df
A[1]=ad8601a2  B[1]=4eb93d69  C[1]=b10ece73  D[1]=abe14d82
A[2]=cf0ab111  B[2]=e9876c93  C[2]=92f62890  D[2]=fb9adf16
A[3]=cc50088f  B[3]=69b7139c  C[3]=9667cd57  D[3]=4439e423
A[4]=36e1fe9f  B[4]=90d68a47  C[4]=20addef3  D[4]=ba2aee5f
A[5]=86352edc  B[5]=816fee84  C[5]=75e360c3  D[5]=553f0b45
A[6]=9cdf19ae  B[6]=df451625  C[6]=68b20eaf  D[6]=1f6050ec
A[7]=f0f8ed2f  B[7]=d428f4f7  C[7]=5a039bd2  D[7]=d6deb59e

Step 13: (r=19, s=22)
A[0]=64711b9b  B[0]=b0b23453  C[0]=0eaf5f83  D[0]=a4d57616
A[1]=896bbd02  B[1]=0d156c30  C[1]=4eb93d69  D[1]=b10ece73
A[2]=ba797977  B[2]=888e7855  C[2]=e9876c93  D[2]=92f62890
A[3]=d1b31539  B[3]=447e6280  C[3]=69b7139c  D[3]=9667cd57
A[4]=ec007bc3  B[4]=f4f9b70f  C[4]=90d68a47  D[4]=20addef3
A[5]=288d59b8  B[5]=76e431a9  C[5]=816fee84  D[5]=75e360c3
A[6]=3f44da63  B[6]=cd74e6f8  C[6]=df451625  D[6]=68b20eaf
A[7]=c0676b74  B[7]=697f87c7  C[7]=d428f4f7  D[7]=5a039bd2

Step 14: (r=22, s= 7)
A[0]=bb844f72  B[0]=e6d91c46  C[0]=b0b23453  D[0]=0eaf5f83
A[1]=ac847a17  B[1]=40a25aef  C[1]=0d156c30  D[1]=4eb93d69
A[2]=9f25148c  B[2]=5dee9e5e  C[2]=888e7855  D[2]=e9876c93
A[3]=9e8846f3  B[3]=4e746cc5  C[3]=447e6280  D[3]=69b7139c
A[4]=8102f903  B[4]=f0fb001e  C[4]=f4f9b70f  D[4]=90d68a47
A[5]=12f537bf  B[5]=6e0a2356  C[5]=76e431a9  D[5]=816fee84
A[6]=c60956de  B[6]=98cfd136  C[6]=cd74e6f8  D[6]=df451625
A[7]=5cae41a7  B[7]=dd3019da  C[7]=697f87c7  D[7]=d428f4f7

Step 15: (r= 7, s=28)
A[0]=9de6f74e  B[0]=c227b95d  C[0]=e6d91c46  D[0]=b0b23453
A[1]=ba2a89a5  B[1]=423d0bd6  C[1]=40a25aef  D[1]=0d156c30
A[2]=a9cd2fdd  B[2]=928a464f  C[2]=5dee9e5e  D[2]=888e7855
A[3]=4a2fc60d  B[3]=442379cf  C[3]=4e746cc5  D[3]=447e6280
A[4]=7f2baf6f  B[4]=817c81c0  C[4]=f0fb001e  D[4]=f4f9b70f
A[5]=a1f16926  B[5]=7a9bdf89  C[5]=6e0a2356  D[5]=76e431a9
A[6]=bc10cc56  B[6]=04ab6f63  C[6]=98cfd136  D[6]=cd74e6f8
```

```
A[7]=f2413c34  B[7]=5720d3ae  C[7]=dd3019da  D[7]=697f87c7

Step 16: (r=29, s= 9)
A[0]=9a2be409  B[0]=d3bcdee9  C[0]=c227b95d  D[0]=e6d91c46
A[1]=f32f2707  B[1]=b7455134  C[1]=423d0bd6  D[1]=40a25aef
A[2]=b946b636  B[2]=b539a5fb  C[2]=928a464f  D[2]=5dee9e5e
A[3]=d110b611  B[3]=a945f8c1  C[3]=442379cf  D[3]=4e746cc5
A[4]=6e0e265c  B[4]=efe575ed  C[4]=817c81c0  D[4]=f0fb001e
A[5]=aebf09d4  B[5]=d43e2d24  C[5]=7a9bdf89  D[5]=6e0a2356
A[6]=73993066  B[6]=d782198a  C[6]=04ab6f63  D[6]=98cfd136
A[7]=fe25ce01  B[7]=9e482786  C[7]=5720d3ae  D[7]=dd3019da

Step 17: (r= 9, s=15)
A[0]=811e1d45  B[0]=57c81334  C[0]=d3bcdee9  D[0]=c227b95d
A[1]=907a16a2  B[1]=5e4e0fe6  C[1]=b7455134  D[1]=423d0bd6
A[2]=47c6f095  B[2]=8d6c6d72  C[2]=b539a5fb  D[2]=928a464f
A[3]=d73130e1  B[3]=216c23a2  C[3]=a945f8c1  D[3]=442379cf
A[4]=e780ab44  B[4]=1c4cb8dc  C[4]=efe575ed  D[4]=817c81c0
A[5]=23307e6d  B[5]=7e13a95d  C[5]=d43e2d24  D[5]=7a9bdf89
A[6]=b60b81bb  B[6]=3260cce7  C[6]=d782198a  D[6]=04ab6f63
A[7]=111d9ae7  B[7]=4b9c03fc  C[7]=9e482786  D[7]=5720d3ae

Step 18: (r=15, s= 5)
A[0]=33a7f87a  B[0]=0ea2c08f  C[0]=57c81334  D[0]=d3bcdee9
A[1]=9693d5e8  B[1]=0b51483d  C[1]=5e4e0fe6  D[1]=b7455134
A[2]=2f10a10f  B[2]=784aa3e3  C[2]=8d6c6d72  D[2]=b539a5fb
A[3]=a47cf67f  B[3]=9870eb98  C[3]=216c23a2  D[3]=a945f8c1
A[4]=9b3a4a75  B[4]=55a273c0  C[4]=1c4cb8dc  D[4]=efe575ed
A[5]=9f076239  B[5]=3f369198  C[5]=7e13a95d  D[5]=d43e2d24
A[6]=d9ccb0ac  B[6]=c0dddb05  C[6]=3260cce7  D[6]=d782198a
A[7]=db3782f2  B[7]=cd73888e  C[7]=4b9c03fc  D[7]=9e482786

Step 19: (r= 5, s=29)
A[0]=4c1770c7  B[0]=74ff0f46  C[0]=0ea2c08f  D[0]=57c81334
A[1]=3cbfc612  B[1]=d27abd12  C[1]=0b51483d  D[1]=5e4e0fe6
A[2]=6a205c21  B[2]=e21421e5  C[2]=784aa3e3  D[2]=8d6c6d72
A[3]=213fb59e  B[3]=8f9ecff4  C[3]=9870eb98  D[3]=216c23a2
A[4]=8c6a20e8  B[4]=67494eb3  C[4]=55a273c0  D[4]=1c4cb8dc
A[5]=cd84f7ae  B[5]=e0ec4733  C[5]=3f369198  D[5]=7e13a95d
A[6]=16698f2b  B[6]=3996159b  C[6]=c0dddb05  D[6]=3260cce7
A[7]=8b8e1ada  B[7]=66f05e5b  C[7]=cd73888e  D[7]=4b9c03fc

Step 20: (r=29, s= 9)
A[0]=5a2df36d  B[0]=e982ee18  C[0]=74ff0f46  D[0]=0ea2c08f
A[1]=5a46a308  B[1]=4797f8c2  C[1]=d27abd12  D[1]=0b51483d
A[2]=230bf2b3  B[2]=2d440b84  C[2]=e21421e5  D[2]=784aa3e3
A[3]=25c5c282  B[3]=c427f6b3  C[3]=8f9ecff4  D[3]=9870eb98
A[4]=c8dff7b5  B[4]=118d441d  C[4]=67494eb3  D[4]=55a273c0
A[5]=dd0b0328  B[5]=d9b09ef5  C[5]=e0ec4733  D[5]=3f369198
```

```
A[6]=237478b1  B[6]=62cd31e5  C[6]=3996159b  D[6]=c0dddb05
A[7]=1c3f6910  B[7]=5171c35b  C[7]=66f05e5b  D[7]=cd73888e

Step 21: (r= 9, s=15)
A[0]=618fd801  B[0]=5be6dab4  C[0]=e982ee18  D[0]=74ff0f46
A[1]=569c0f72  B[1]=8d4610b4  C[1]=4797f8c2  D[1]=d27abd12
A[2]=744accf0  B[2]=17e56646  C[2]=2d440b84  D[2]=e21421e5
A[3]=87cbde81  B[3]=8b85044b  C[3]=c427f6b3  D[3]=8f9ecff4
A[4]=7afd95b5  B[4]=bfef6b91  C[4]=118d441d  D[4]=67494eb3
A[5]=44c23f92  B[5]=160651ba  C[5]=d9b09ef5  D[5]=e0ec4733
A[6]=2665f158  B[6]=e8f16246  C[6]=62cd31e5  D[6]=3996159b
A[7]=bfc90655  B[7]=7ed22038  C[7]=5171c35b  D[7]=66f05e5b

Step 22: (r=15, s= 5)
A[0]=ac49784d  B[0]=ec00b0c7  C[0]=5be6dab4  D[0]=e982ee18
A[1]=9f10c6bc  B[1]=07b92b4e  C[1]=8d4610b4  D[1]=4797f8c2
A[2]=e713a196  B[2]=66783a25  C[2]=17e56646  D[2]=2d440b84
A[3]=6b648a9d  B[3]=ef40c3e5  C[3]=8b85044b  D[3]=c427f6b3
A[4]=638e2cf5  B[4]=cadabd7e  C[4]=bfef6b91  D[4]=118d441d
A[5]=c1fa7bbe  B[5]=1fc92261  C[5]=160651ba  D[5]=d9b09ef5
A[6]=dd942a97  B[6]=f8ac1332  C[6]=e8f16246  D[6]=62cd31e5
A[7]=965e8b71  B[7]=832adfe4  C[7]=7ed22038  D[7]=5171c35b

Step 23: (r= 5, s=29)
A[0]=a0d0cc13  B[0]=892f09b5  C[0]=ec00b0c7  D[0]=5be6dab4
A[1]=ad50ed32  B[1]=e218d793  C[1]=07b92b4e  D[1]=8d4610b4
A[2]=56c43467  B[2]=e27432dc  C[2]=66783a25  D[2]=17e56646
A[3]=de82a046  B[3]=6c9153ad  C[3]=ef40c3e5  D[3]=8b85044b
A[4]=8a7448f9  B[4]=71c59eac  C[4]=cadabd7e  D[4]=bfef6b91
A[5]=6c0d2e7b  B[5]=3f4f77d8  C[5]=1fc92261  D[5]=160651ba
A[6]=393a6d26  B[6]=b28552fb  C[6]=f8ac1332  D[6]=e8f16246
A[7]=d228ebd1  B[7]=cbd16e32  C[7]=832adfe4  D[7]=7ed22038

Step 24: (r= 4, s=13)
A[0]=09cf623f  B[0]=0d0cc13a  C[0]=892f09b5  D[0]=ec00b0c7
A[1]=0951e5be  B[1]=d50ed32a  C[1]=e218d793  D[1]=07b92b4e
A[2]=c871621e  B[2]=6c434675  C[2]=e27432dc  D[2]=66783a25
A[3]=0b3bea9f  B[3]=e82a046d  C[3]=6c9153ad  D[3]=ef40c3e5
A[4]=8518c895  B[4]=a7448f98  C[4]=71c59eac  D[4]=cadabd7e
A[5]=43cc58ca  B[5]=c0d2e7b6  C[5]=3f4f77d8  D[5]=1fc92261
A[6]=541560d8  B[6]=93a6d263  C[6]=b28552fb  D[6]=f8ac1332
A[7]=bfbc3016  B[7]=228ebd1d  C[7]=cbd16e32  D[7]=832adfe4

Step 25: (r=13, s=10)
A[0]=b03c663f  B[0]=ec47e139  C[0]=0d0cc13a  D[0]=892f09b5
A[1]=5c9f5da4  B[1]=3cb7c12a  C[1]=d50ed32a  D[1]=e218d793
A[2]=454f12cc  B[2]=2c43d90e  C[2]=6c434675  D[2]=e27432dc
A[3]=5dd04d35  B[3]=7d53e167  C[3]=e82a046d  D[3]=6c9153ad
A[4]=5768f9da  B[4]=1912b0a3  C[4]=a7448f98  D[4]=71c59eac
```

```
A[5]=a1575c1f  B[5]=8b194879  C[5]=c0d2e7b6  D[5]=3f4f77d8
A[6]=a052a382  B[6]=ac1b0a82  C[6]=93a6d263  D[6]=b28552fb
A[7]=c9eb8f27  B[7]=8602d7f7  C[7]=228ebd1d  D[7]=cbd16e32

Step 26: (r=10, s=25)
A[0]=c21767b1  B[0]=f198fec0  C[0]=ec47e139  D[0]=0d0cc13a
A[1]=7cf2b298  B[1]=7d769172  C[1]=3cb7c12a  D[1]=d50ed32a
A[2]=70e6765f  B[2]=3c4b3115  C[2]=2c43d90e  D[2]=6c434675
A[3]=59f344b4  B[3]=4134d577  C[3]=7d53e167  D[3]=e82a046d
A[4]=24ec6ea9  B[4]=a3e7695d  C[4]=1912b0a3  D[4]=a7448f98
A[5]=8fae967c  B[5]=5d707e85  C[5]=8b194879  D[5]=c0d2e7b6
A[6]=4d2c0a10  B[6]=4a8e0a81  C[6]=ac1b0a82  D[6]=93a6d263
A[7]=4fe13e3b  B[7]=ae3c9f27  C[7]=8602d7f7  D[7]=228ebd1d

Step 27: (r=25, s= 4)
A[0]=b8adad39  B[0]=63842ecf  C[0]=f198fec0  D[0]=ec47e139
A[1]=598d29d8  B[1]=30f9e565  C[1]=7d769172  D[1]=3cb7c12a
A[2]=5f75b525  B[2]=bee1ccec  C[2]=3c4b3115  D[2]=2c43d90e
A[3]=d33d4c14  B[3]=68b3e689  C[3]=4134d577  D[3]=7d53e167
A[4]=6419b3c1  B[4]=5249d8dd  C[4]=a3e7695d  D[4]=1912b0a3
A[5]=1b371635  B[5]=f91f5d2c  C[5]=5d707e85  D[5]=8b194879
A[6]=cbb3d0ea  B[6]=209a5814  C[6]=4a8e0a81  D[6]=ac1b0a82
A[7]=eff0ba9a  B[7]=769fc27c  C[7]=ae3c9f27  D[7]=8602d7f7

Step 28: (r= 4, s=13)
A[0]=3d2bf684  B[0]=8adad39b  C[0]=63842ecf  D[0]=f198fec0
A[1]=772e1fbf  B[1]=98d29d85  C[1]=30f9e565  D[1]=7d769172
A[2]=c5f29228  B[2]=f75b5255  C[2]=bee1ccec  D[2]=3c4b3115
A[3]=5e63d446  B[3]=33d4c14d  C[3]=68b3e689  D[3]=4134d577
A[4]=cfb20cd2  B[4]=419b3c16  C[4]=5249d8dd  D[4]=a3e7695d
A[5]=04e1ee45  B[5]=b3716351  C[5]=f91f5d2c  D[5]=5d707e85
A[6]=2062d683  B[6]=bb3d0eac  C[6]=209a5814  D[6]=4a8e0a81
A[7]=3af3c5e9  B[7]=ff0ba9ae  C[7]=769fc27c  D[7]=ae3c9f27

Step 29: (r=13, s=10)
A[0]=ebc8e2ae  B[0]=7ed087a5  C[0]=8adad39b  D[0]=63842ecf
A[1]=b84b58ed  B[1]=c3f7eee5  C[1]=98d29d85  D[1]=30f9e565
A[2]=de916041  B[2]=524518be  C[2]=f75b5255  D[2]=bee1ccec
A[3]=f0713a3d  B[3]=7a88cbcc  C[3]=33d4c14d  D[3]=68b3e689
A[4]=8f0065e5  B[4]=419a59f6  C[4]=419b3c16  D[4]=5249d8dd
A[5]=7f99d021  B[5]=3dc8a09c  C[5]=b3716351  D[5]=f91f5d2c
A[6]=e1e0aca1  B[6]=5ad0640c  C[6]=bb3d0eac  D[6]=209a5814
A[7]=980c8789  B[7]=78bd275e  C[7]=ff0ba9ae  D[7]=769fc27c

Step 30: (r=10, s=25)
A[0]=f242298a  B[0]=238abbaf  C[0]=7ed087a5  D[0]=8adad39b
A[1]=cc943ef0  B[1]=2d63b6e1  C[1]=c3f7eee5  D[1]=98d29d85
A[2]=20ed9160  B[2]=4581077a  C[2]=524518be  D[2]=f75b5255
A[3]=91ede926  B[3]=c4e8f7c1  C[3]=7a88cbcc  D[3]=33d4c14d
```

```
A[4]=cf5e88da  B[4]=0197963c  C[4]=419a59f6  D[4]=419b3c16
A[5]=2dcf254e  B[5]=674085fe  C[5]=3dc8a09c  D[5]=b3716351
A[6]=be8dfd24  B[6]=82b28787  C[6]=5ad0640c  D[6]=bb3d0eac
A[7]=fee7eeff  B[7]=321e2660  C[7]=78bd275e  D[7]=ff0ba9ae

Step 31: (r=25, s= 4)
A[0]=fccc7f36  B[0]=15e48453  C[0]=238abbaf  D[0]=7ed087a5
A[1]=12265296  B[1]=e199287d  C[1]=2d63b6e1  D[1]=c3f7eee5
A[2]=ee513777  B[2]=c041db22  C[2]=4581077a  D[2]=524518be
A[3]=dde65499  B[3]=4d23dbd2  C[3]=c4e8f7c1  D[3]=7a88cbcc
A[4]=9b197ada  B[4]=b59ebd11  C[4]=0197963c  D[4]=419a59f6
A[5]=b55a53c1  B[5]=9c5b9e4a  C[5]=674085fe  D[5]=3dc8a09c
A[6]=14ea0d6a  B[6]=497d1bfa  C[6]=82b28787  D[6]=5ad0640c
A[7]=ff925914  B[7]=fffdcfdd  C[7]=321e2660  D[7]=78bd275e

Feed-Forward Step 32: (r= 4, s=13)
A[0]=649ff062  B[0]=ccc7f36f  C[0]=15e48453  D[0]=238abbaf
A[1]=17389a2f  B[1]=22652961  C[1]=e199287d  D[1]=2d63b6e1
A[2]=56f867cd  B[2]=e513777e  C[2]=c041db22  D[2]=4581077a
A[3]=1333e6dd  B[3]=de65499d  C[3]=4d23dbd2  D[3]=c4e8f7c1
A[4]=6e4f8f99  B[4]=b197ada9  C[4]=b59ebd11  D[4]=0197963c
A[5]=19c7e7c7  B[5]=55a53c1b  C[5]=9c5b9e4a  D[5]=674085fe
A[6]=b1ab8b29  B[6]=4ea0d6a1  C[6]=497d1bfa  D[6]=82b28787
A[7]=7098c4a7  B[7]=f925914f  C[7]=fffdcfdd  D[7]=321e2660

Feed-Forward Step 33: (r=13, s=10)
A[0]=24ee82aa  B[0]=fe0c4c93  C[0]=ccc7f36f  D[0]=15e48453
A[1]=9db91519  B[1]=1345e2e7  C[1]=22652961  D[1]=e199287d
A[2]=b732b2e7  B[2]=0cf9aadf  C[2]=e513777e  D[2]=c041db22
A[3]=f956ed00  B[3]=7cdba266  C[3]=de65499d  D[3]=4d23dbd2
A[4]=40289f54  B[4]=f1f32dc9  C[4]=b197ada9  D[4]=b59ebd11
A[5]=8e267afa  B[5]=fcf8e338  C[5]=55a53c1b  D[5]=9c5b9e4a
A[6]=19850b6c  B[6]=71653635  C[6]=4ea0d6a1  D[6]=497d1bfa
A[7]=4a6942bf  B[7]=1894ee13  C[7]=f925914f  D[7]=fffdcfdd

Feed-Forward Step 34: (r=10, s=25)
A[0]=197f13ad  B[0]=ba0aa893  C[0]=fe0c4c93  D[0]=ccc7f36f
A[1]=26ec88a1  B[1]=e4546676  C[1]=1345e2e7  D[1]=22652961
A[2]=b96ec615  B[2]=cacb9edc  C[2]=0cf9aadf  D[2]=e513777e
A[3]=d414dde7  B[3]=5bb403e5  C[3]=7cdba266  D[3]=de65499d
A[4]=6aaf5937  B[4]=a27d5100  C[4]=f1f32dc9  D[4]=b197ada9
A[5]=89229881  B[5]=99ebea38  C[5]=fcf8e338  D[5]=55a53c1b
A[6]=7fa7ff8c  B[6]=142db066  C[6]=71653635  D[6]=4ea0d6a1
A[7]=6b217870  B[7]=a50afd29  C[7]=1894ee13  D[7]=f925914f

Feed-Forward Step 35: (r=25, s= 4)
A[0]=81c662ce  B[0]=5a32fe27  C[0]=ba0aa893  D[0]=fe0c4c93
A[1]=3e783659  B[1]=424dd911  C[1]=e4546676  D[1]=1345e2e7
A[2]=f035fd3b  B[2]=2b72dd8c  C[2]=cacb9edc  D[2]=0cf9aadf
```

```
A[3]=58bbe3f4  B[3]=cfa829bb  C[3]=5bb403e5  D[3]=7cdba266
A[4]=4e7911b0  B[4]=6ed55eb2  C[4]=a27d5100  D[4]=f1f32dc9
A[5]=c4d19119  B[5]=03124531  C[5]=99ebea38  D[5]=fcf8e338
A[6]=a60f4481  B[6]=18ff4fff  C[6]=142db066  D[6]=71653635
A[7]=c4860948  B[7]=e0d642f0  C[7]=a50afd29  D[7]=1894ee13
```

Compression Function Output

```
A[0]=81c662ce  B[0]=5a32fe27  C[0]=ba0aa893  D[0]=fe0c4c93
A[1]=3e783659  B[1]=424dd911  C[1]=e4546676  D[1]=1345e2e7
A[2]=f035fd3b  B[2]=2b72dd8c  C[2]=cacb9edc  D[2]=0cf9aadf
A[3]=58bbe3f4  B[3]=cfa829bb  C[3]=5bb403e5  D[3]=7cdba266
A[4]=4e7911b0  B[4]=6ed55eb2  C[4]=a27d5100  D[4]=f1f32dc9
A[5]=c4d19119  B[5]=03124531  C[5]=99ebea38  D[5]=fcf8e338
A[6]=a60f4481  B[6]=18ff4fff  C[6]=142db066  D[6]=71653635
A[7]=c4860948  B[7]=e0d642f0  C[7]=a50afd29  D[7]=1894ee13
```

Second block

```
M[  0..  7] = ff ff ff ff ff ff fe 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  243   52  151  163  238  141  176    4
y[  8.. 15] =  180  170  128   28   36   36  157   38
y[ 16.. 23] =   68  208   55  168  117  214   88  115
y[ 24.. 31] =   88   14   70  255  173  206  169   46
y[ 32.. 39] =   81  175  138  212   24   95  231  105
y[ 40.. 47] =  163  164  237  239  114   30  101  108
y[ 48.. 55] =  102  116  229   89  170  203   57    2
y[ 56.. 63] =  150  206  145   68  168   96   16  188
y[ 64.. 71] =  210  224  100   35  104  221  190  234
y[ 72.. 79] =  203  159  117   35  162  121   51  137
y[ 80.. 87] =   97   84   41   28  139  160   93  199
y[ 88.. 95] =  238  155  235   82  216  157   67  105
```

```
y[ 96..103] =  229  108  176  114  150  225   87  208
y[104..111] =   58   82  135   16    6  210  241  166
y[112..119] =   89  198  134   39   32  224  244  138
y[120..127] =    9  162  101  242  177   36   78  190
y[128..135] =  253  161   80   99   75   12   46   44
y[136..143] =    1  237  214   23  113   75  160  107
y[144..151] =  235   99   19  146  256   79    1  106
y[152..159] =  146   91   23  147  116  103  187  140
y[160..167] =  208  212  231  175  207  151   95    1
y[168..175] =  232   88  172   20   98   63   73   48
y[176..183] =  192  109  121  224  218  244   52   10
y[184..191] =  169   63  154   13   36   77  121  168
y[192..199] =   49  215  209  231   73  167  162   11
y[200..207] =   90   10  183  251  131  157  153  143
y[208..215] =  235  138  164    2  252   99  127   19
y[216..223] =   36   81   41  145    5  224   66  204
y[224..231] =  253  122  184  240  141    0   25  148
y[232..239] =   85  102   83  143   95   63   76    8
y[240..247] =  251   60  249   59   85   46   93  166
y[248..255] =  176  240  243   60  121  113   51  228
```

Intermediate Expanded Message

```
Z[ 0] = 2594f5e2  bc12b366  ac2cf245  02e4c577
        c121c85b  143c5c80  1a041a04  1b76b7bc
Z[ 1] = dc973124  bfaf27bf  e0ed548d  531b3f98
        0a1e3f98  fe8e3296  db25c34c  213ec068
Z[ 2] = c4be3a89  df7baa01  44a71158  4be1ed36
        bccbbc12  f2fef18c  15ae5262  4e0c48fd
Z[ 3] = 53d449b6  4051ebc4  d8fac121  01722931
        db25b2ad  3124af10  4560bfaf  ce230b90
Z[ 4] = e827de09  194b4844  e5fc4b28  ef61cf95
        b92ed8fa  194b548d  5771bb59  a94824db
Z[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
        b64af245  3b42f01a  b7bce25f  4be1306b
Z[ 6] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
        3b4229ea  0b90a7d6  de090456  be3df470
Z[ 7] = d55d4051  1c2fa71d  e8271720  aa01f69b
        bb590681  f52948fd  1a04c630  cf95385e
Z[ 8] = baa0fd1c  478b39d0  08ac3633  1fcc213e
        f18c00b9  109fe0ed  363351a9  4d53b9e7
Z[ 9] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
        41c3afc9  b082109f  4a6f53d4  ab73cd6a
Z[10] = df7bdc97  c4beed36  b366dbde  00b944a7
        3f98edef  0e74c293  2d8746d2  22b034c1
Z[11] = 4ec5d107  e8275771  f69be3d1  073a2594
        2d87c068  0965b591  37a51a04  bfaf5771
Z[12] = e1a62369  ed36dd50  bef634c1  07f3bb59
        073a410a  fbaaca86  b7bca4f2  ad9eb4d8
```

```
Z[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
        3a891a04  af101da1  e827039d  d9b32fb2
Z[14] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
        49b63d6d  ad9e3bfb  2d8744a7  05c836ec
Z[15] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
        f3b7c577  2b5cf5e2  51a95771  eb0b24db
Z[16] = fc5cf342  48d09f86  4443eeb5  29deb647
        00e9b9eb  d8dd7480  66d920c4  a7b7a4fc
Z[17] = ebfa3de4  114b320f  ff176a7d  00e95018
        9af95018  14ef3fb6  6994b38c  c04aafe8
Z[18] = d36749b9  e85693b1  d27e15d8  5677e856
        e93faa72  b2a3edcc  593267c2  42715bed
Z[19] = c4d75cd6  6e21e684  dc81b0d1  2f5433e1
        afe89e9d  a2419a10  20c4aeff  6e210e90
Z[20] = 2c99d539  d4505b04  42715ea8  a989c305
        51eaceda  bca66a7d  8d52a989  a1582e6b
Z[21] = ebfa5849  ab5b2551  fb73949a  739754a5
        20c4eeb5  2551ebfa  048ddaaf  3c123cfb
Z[22] = fc5ce684  bd8fb647  966c9e9d  16c14f2f
        4d5d34ca  4b8b90f6  56770576  452cf170
Z[23] = fa8a5101  f8b8900d  4d5d1d20  54a5f42b
        b6470831  f3425bed  6e21b730  2e6b46fe
Z[24] = a8a02f54  5a1baa72  0aec966c  280c03a4
        edccb0d1  14ef197c  444320c4  61632296
Z[25] = 5a1bd367  9af9aeff  47e7d8dd  607a68ab
        52d30cbe  9be2fe2e  5dbfd195  958329de
Z[26] = d70bb55e  b55ed70b  9f865677  00e95f91
        5018ab5b  1234ef9e  39571b4e  2bb0624c
Z[27] = 63356994  e1f75101  f42bceda  091a01d2
        3957d195  0bd53de4  46155760  aeffc133
Z[28] = d9c6e1f7  e8561fdb  ae16df3c  0a03eb11
        091aa6ce  fa8a1fdb  a4fc6e21  983e92c8
Z[29] = 93b14c74  01d2197c  5a1ba7b7  114bcb36
        49b9a32a  9a104aa2  e1f7a4fc  cfc35f91
Z[30] = 6f0a624c  f08767c2  0000e2e0  9ccbd367
        5cd64aa2  983e0e90  3957d539  0748ad2d
Z[31] = 369cca4d  35b3237f  29dee1f7  ad2d93b1
        f087a989  369cf259  66d920c4  e59bc305
```

Expanded Message

```
W[ 0] = e827de09  194b4844  e5fc4b28  ef61cf95
        b92ed8fa  194b548d  5771bb59  a94824db
W[ 1] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
        3b4229ea  0b90a7d6  de090456  be3df470
W[ 2] = 2594f5e2  bc12b366  ac2cf245  02e4c577
        c121c85b  143c5c80  1a041a04  1b76b7bc
W[ 3] = c4be3a89  df7baa01  44a71158  4be1ed36
        bccbbc12  f2fef18c  15ae5262  4e0c48fd
```

```
W[ 4] = d55d4051  1c2fa71d  e8271720  aa01f69b
        bb590681  f52948fd  1a04c630  cf95385e
W[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
        b64af245  3b42f01a  b7bce25f  4be1306b
W[ 6] = 53d449b6  4051ebc4  d8fac121  01722931
        db25b2ad  3124af10  4560bfaf  ce230b90
W[ 7] = dc973124  bfaf27bf  e0ed548d  531b3f98
        0a1e3f98  fe8e3296  db25c34c  213ec068
W[ 8] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
        f3b7c577  2b5cf5e2  51a95771  eb0b24db
W[ 9] = 4ec5d107  e8275771  f69be3d1  073a2594
        2d87c068  0965b591  37a51a04  bfaf5771
W[10] = e1a62369  ed36dd50  bef634c1  07f3bb59
        073a410a  fbaaca86  b7bca4f2  ad9eb4d8
W[11] = baa0fd1c  478b39d0  08ac3633  1fcc213e
        f18c00b9  109fe0ed  363351a9  4d53b9e7
W[12] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
        41c3afc9  b082109f  4a6f53d4  ab73cd6a
W[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
        3a891a04  af101da1  e827039d  d9b32fb2
W[14] = df7bdc97  c4beed36  b366dbde  00b944a7
        3f98edef  0e74c293  2d8746d2  22b034c1
W[15] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
        49b63d6d  ad9e3bfb  2d8744a7  05c836ec
W[16] = ebfa3de4  114b320f  ff176a7d  00e95018
        9af95018  14ef3fb6  6994b38c  c04aafe8
W[17] = d36749b9  e85693b1  d27e15d8  5677e856
        e93faa72  b2a3edcc  593267c2  42715bed
W[18] = fa8a5101  f8b8900d  4d5d1d20  54a5f42b
        b6470831  f3425bed  6e21b730  2e6b46fe
W[19] = 2c99d539  d4505b04  42715ea8  a989c305
        51eaceda  bca66a7d  8d52a989  a1582e6b
W[20] = fc5ce684  bd8fb647  966c9e9d  16c14f2f
        4d5d34ca  4b8b90f6  56770576  452cf170
W[21] = ebfa5849  ab5b2551  fb73949a  739754a5
        20c4eeb5  2551ebfa  048ddaaf  3c123cfb
W[22] = fc5cf342  48d09f86  4443eeb5  29deb647
        00e9b9eb  d8dd7480  66d920c4  a7b7a4fc
W[23] = c4d75cd6  6e21e684  dc81b0d1  2f5433e1
        afe89e9d  a2419a10  20c4aeff  6e210e90
W[24] = 6f0a624c  f08767c2  0000e2e0  9ccbd367
        5cd64aa2  983e0e90  3957d539  0748ad2d
W[25] = a8a02f54  5a1baa72  0aec966c  280c03a4
        edccb0d1  14ef197c  444320c4  61632296
W[26] = 5a1bd367  9af9aeff  47e7d8dd  607a68ab
        52d30cbe  9be2fe2e  5dbfd195  958329de
W[27] = 369cca4d  35b3237f  29dee1f7  ad2d93b1
        f087a989  369cf259  66d920c4  e59bc305
W[28] = 63356994  e1f75101  f42bceda  091a01d2
```

```
        3957d195  0bd53de4  46155760  aeffc133
W[29] = 93b14c74  01d2197c  5a1ba7b7  114bcb36
        49b9a32a  9a104aa2  e1f7a4fc  cfc35f91
W[30] = d9c6e1f7  e8561fdb  ae16df3c  0a03eb11
        091aa6ce  fa8a1fdb  a4fc6e21  983e92c8
W[31] = d70bb55e  b55ed70b  9f865677  00e95f91
        5018ab5b  1234ef9e  39571b4e  2bb0624c
```

Feistel Steps

```
IV :
A[0]=81c662ce  B[0]=5a32fe27  C[0]=ba0aa893  D[0]=fe0c4c93
A[1]=3e783659  B[1]=424dd911  C[1]=e4546676  D[1]=1345e2e7
A[2]=f035fd3b  B[2]=2b72dd8c  C[2]=cacb9edc  D[2]=0cf9aadf
A[3]=58bbe3f4  B[3]=cfa829bb  C[3]=5bb403e5  D[3]=7cdba266
A[4]=4e7911b0  B[4]=6ed55eb2  C[4]=a27d5100  D[4]=f1f32dc9
A[5]=c4d19119  B[5]=03124531  C[5]=99ebea38  D[5]=fcf8e338
A[6]=a60f4481  B[6]=18ff4fff  C[6]=142db066  D[6]=71653635
A[7]=c4860948  B[7]=e0d642f0  C[7]=a50afd29  D[7]=1894ee13

IV XOR M :
A[0]=7e399d31  B[0]=5a32fe27  C[0]=ba0aa893  D[0]=fe0c4c93
A[1]=3e86c9a6  B[1]=424dd911  C[1]=e4546676  D[1]=1345e2e7
A[2]=f035fd3b  B[2]=2b72dd8c  C[2]=cacb9edc  D[2]=0cf9aadf
A[3]=58bbe3f4  B[3]=cfa829bb  C[3]=5bb403e5  D[3]=7cdba266
A[4]=4e7911b0  B[4]=6ed55eb2  C[4]=a27d5100  D[4]=f1f32dc9
A[5]=c4d19119  B[5]=03124531  C[5]=99ebea38  D[5]=fcf8e338
A[6]=a60f4481  B[6]=18ff4fff  C[6]=142db066  D[6]=71653635
A[7]=c4860948  B[7]=e0d642f0  C[7]=a50afd29  D[7]=1894ee13

Step  0: (r= 3, s=23)
A[0]=941680a4  B[0]=f1cce98b  C[0]=5a32fe27  D[0]=ba0aa893
A[1]=2fc45c98  B[1]=f4364d31  C[1]=424dd911  D[1]=e4546676
A[2]=af6e180c  B[2]=81afe9df  C[2]=2b72dd8c  D[2]=cacb9edc
A[3]=580bdea8  B[3]=c5df1fa2  C[3]=cfa829bb  D[3]=5bb403e5
A[4]=e0594479  B[4]=73c88d82  C[4]=6ed55eb2  D[4]=a27d5100
A[5]=eee04cd3  B[5]=268c88ce  C[5]=03124531  D[5]=99ebea38
A[6]=5f1ccdb9  B[6]=307a240d  C[6]=18ff4fff  D[6]=142db066
A[7]=d84bda10  B[7]=24304a46  C[7]=e0d642f0  D[7]=a50afd29

Step  1: (r=23, s=17)
A[0]=026552df  B[0]=524a0b40  C[0]=f1cce98b  D[0]=5a32fe27
A[1]=fa695b76  B[1]=4c17e22e  C[1]=f4364d31  D[1]=424dd911
A[2]=7b1a9678  B[2]=0657b70c  C[2]=81afe9df  D[2]=2b72dd8c
A[3]=6ee77013  B[3]=542c05ef  C[3]=c5df1fa2  D[3]=cfa829bb
A[4]=39305023  B[4]=3cf02ca2  C[4]=73c88d82  D[4]=6ed55eb2
A[5]=8c0da00c  B[5]=69f77026  C[5]=268c88ce  D[5]=03124531
A[6]=c86011a3  B[6]=dcaf8e66  C[6]=307a240d  D[6]=18ff4fff
A[7]=c50ae9e8  B[7]=086c25ed  C[7]=24304a46  D[7]=e0d642f0
```

```
Step  2: (r=17, s=27)
A[0]=788d7b2f  B[0]=a5be04ca  C[0]=524a0b40  D[0]=f1cce98b
A[1]=d27a9c62  B[1]=b6edf4d2  C[1]=4c17e22e  D[1]=f4364d31
A[2]=a890c345  B[2]=2cf0f635  C[2]=0657b70c  D[2]=81afe9df
A[3]=63ac3cc8  B[3]=e026ddce  C[3]=542c05ef  D[3]=c5df1fa2
A[4]=a09f0e65  B[4]=a0467260  C[4]=3cf02ca2  D[4]=73c88d82
A[5]=8de02868  B[5]=4019181b  C[5]=69f77026  D[5]=268c88ce
A[6]=29a05ed1  B[6]=234790c0  C[6]=dcaf8e66  D[6]=307a240d
A[7]=10fd410f  B[7]=d3d18a15  C[7]=086c25ed  D[7]=24304a46

Step  3: (r=27, s= 3)
A[0]=0de684dc  B[0]=7bc46bd9  C[0]=a5be04ca  D[0]=524a0b40
A[1]=be43f21d  B[1]=1693d4e3  C[1]=b6edf4d2  D[1]=4c17e22e
A[2]=c00b5f0a  B[2]=2d44861a  C[2]=2cf0f635  D[2]=0657b70c
A[3]=aaedc215  B[3]=431d61e6  C[3]=e026ddce  D[3]=542c05ef
A[4]=e05b4dbf  B[4]=2d04f873  C[4]=a0467260  D[4]=3cf02ca2
A[5]=56639639  B[5]=446f0143  C[5]=4019181b  D[5]=69f77026
A[6]=1e2f3bec  B[6]=894d02f6  C[6]=234790c0  D[6]=dcaf8e66
A[7]=8572b9b7  B[7]=7887ea08  C[7]=d3d18a15  D[7]=086c25ed

Step  4: (r= 3, s=23)
A[0]=e7c77872  B[0]=6f3426e0  C[0]=7bc46bd9  D[0]=a5be04ca
A[1]=11e9f3be  B[1]=f21f90ed  C[1]=1693d4e3  D[1]=b6edf4d2
A[2]=4ea32d8e  B[2]=005af856  C[2]=2d44861a  D[2]=2cf0f635
A[3]=19ea0d3f  B[3]=576e10ad  C[3]=431d61e6  D[3]=e026ddce
A[4]=bd6bd8c2  B[4]=02da6dff  C[4]=2d04f873  D[4]=a0467260
A[5]=0e85ecc4  B[5]=b31cb1ca  C[5]=446f0143  D[5]=4019181b
A[6]=146f1260  B[6]=f179df60  C[6]=894d02f6  D[6]=234790c0
A[7]=30afe2da  B[7]=2b95cdbc  C[7]=7887ea08  D[7]=d3d18a15

Step  5: (r=23, s=17)
A[0]=d8befc5e  B[0]=3973e3bc  C[0]=6f3426e0  D[0]=7bc46bd9
A[1]=f6cff314  B[1]=df08f4f9  C[1]=f21f90ed  D[1]=1693d4e3
A[2]=fc23292c  B[2]=c7275196  C[2]=005af856  D[2]=2d44861a
A[3]=a6c2c942  B[3]=9f8cf506  C[3]=576e10ad  D[3]=431d61e6
A[4]=5abdfcbe  B[4]=615eb5ec  C[4]=02da6dff  D[4]=2d04f873
A[5]=1b165469  B[5]=620742f6  C[5]=b31cb1ca  D[5]=446f0143
A[6]=ea07cddc  B[6]=300a3789  C[6]=f179df60  D[6]=894d02f6
A[7]=83a49431  B[7]=6d1857f1  C[7]=2b95cdbc  D[7]=7887ea08

Step  6: (r=17, s=27)
A[0]=53c3325f  B[0]=f8bdb17d  C[0]=3973e3bc  D[0]=6f3426e0
A[1]=cb39e3b9  B[1]=e629ed9f  C[1]=df08f4f9  D[1]=f21f90ed
A[2]=2a0cea11  B[2]=5259f846  C[2]=c7275196  D[2]=005af856
A[3]=1745fa29  B[3]=92854d85  C[3]=9f8cf506  D[3]=576e10ad
A[4]=eb15fec5  B[4]=f97cb57b  C[4]=615eb5ec  D[4]=02da6dff
A[5]=d36f3da8  B[5]=a8d2362c  C[5]=620742f6  D[5]=b31cb1ca
A[6]=c04fc559  B[6]=9bb9d40f  C[6]=300a3789  D[6]=f179df60
```

```
A[7]=de174bdf  B[7]=28630749  C[7]=6d1857f1  D[7]=2b95cdbc

Step  7: (r=27, s= 3)
A[0]=fc522b2b  B[0]=fa9e1992  C[0]=f8bdb17d  D[0]=3973e3bc
A[1]=02630cbe  B[1]=ce59cf1d  C[1]=e629ed9f  D[1]=df08f4f9
A[2]=636c579a  B[2]=89506750  C[2]=5259f846  D[2]=c7275196
A[3]=99cad1a2  B[3]=48ba2fd1  C[3]=92854d85  D[3]=9f8cf506
A[4]=f9469614  B[4]=2f58aff6  C[4]=f97cb57b  D[4]=615eb5ec
A[5]=cee9885a  B[5]=469b79ed  C[5]=a8d2362c  D[5]=620742f6
A[6]=e44c7808  B[6]=ce027e2a  C[6]=9bb9d40f  D[6]=300a3789
A[7]=95412e17  B[7]=fef0ba5e  C[7]=28630749  D[7]=6d1857f1

Step  8: (r=28, s=19)
A[0]=5427b403  B[0]=bfc522b2  C[0]=fa9e1992  D[0]=f8bdb17d
A[1]=5bcb9297  B[1]=e02630cb  C[1]=ce59cf1d  D[1]=e629ed9f
A[2]=4254371c  B[2]=a636c579  C[2]=89506750  D[2]=5259f846
A[3]=daf1db4f  B[3]=299cad1a  C[3]=48ba2fd1  D[3]=92854d85
A[4]=bd4ab9f2  B[4]=4f946961  C[4]=2f58aff6  D[4]=f97cb57b
A[5]=e3c44d15  B[5]=acee9885  C[5]=469b79ed  D[5]=a8d2362c
A[6]=18102dde  B[6]=8e44c780  C[6]=ce027e2a  D[6]=9bb9d40f
A[7]=2176d4f8  B[7]=795412e1  C[7]=fef0ba5e  D[7]=28630749

Step  9: (r=19, s=22)
A[0]=be639acc  B[0]=a01aa13d  C[0]=bfc522b2  D[0]=fa9e1992
A[1]=81637076  B[1]=94bade5c  C[1]=e02630cb  D[1]=ce59cf1d
A[2]=fc0fa3c5  B[2]=b8e212a1  C[2]=a636c579  D[2]=89506750
A[3]=c1a374e4  B[3]=da7ed78e  C[3]=299cad1a  D[3]=48ba2fd1
A[4]=c0be45aa  B[4]=cf95ea55  C[4]=4f946961  D[4]=2f58aff6
A[5]=d256d17f  B[5]=68af1e22  C[5]=acee9885  D[5]=469b79ed
A[6]=3c7e42a6  B[6]=6ef0c081  C[6]=8e44c780  D[6]=ce027e2a
A[7]=d0e917c8  B[7]=a7c10bb6  C[7]=795412e1  D[7]=fef0ba5e

Step 10: (r=22, s= 7)
A[0]=1e9f059b  B[0]=b32f98e6  C[0]=a01aa13d  D[0]=bfc522b2
A[1]=ccfda935  B[1]=1da058dc  C[1]=94bade5c  D[1]=e02630cb
A[2]=5a11bddd  B[2]=f17f03e8  C[2]=b8e212a1  D[2]=a636c579
A[3]=2993fd02  B[3]=393068dd  C[3]=da7ed78e  D[3]=299cad1a
A[4]=05e0dac8  B[4]=6ab02f91  C[4]=cf95ea55  D[4]=4f946961
A[5]=23bdaa67  B[5]=5ff495b4  C[5]=68af1e22  D[5]=acee9885
A[6]=77e8e3ce  B[6]=a98f1f90  C[6]=6ef0c081  D[6]=8e44c780
A[7]=9ce99b3c  B[7]=f2343a45  C[7]=a7c10bb6  D[7]=795412e1

Step 11: (r= 7, s=28)
A[0]=219c8f98  B[0]=4f82cd8f  C[0]=b32f98e6  D[0]=a01aa13d
A[1]=64b2a091  B[1]=7ed49ae6  C[1]=1da058dc  D[1]=94bade5c
A[2]=becafe47  B[2]=08deeead  C[2]=f17f03e8  D[2]=b8e212a1
A[3]=38c03ac9  B[3]=c9fe8114  C[3]=393068dd  D[3]=da7ed78e
A[4]=6f91f430  B[4]=f06d6402  C[4]=6ab02f91  D[4]=cf95ea55
A[5]=b0171e68  B[5]=ded53391  C[5]=5ff495b4  D[5]=68af1e22
```

```
A[6]=78df82de  B[6]=f471e73b  C[6]=a98f1f90  D[6]=6ef0c081
A[7]=f07b6d21  B[7]=74cd9e4e  C[7]=f2343a45  D[7]=a7c10bb6

Step 12: (r=28, s=19)
A[0]=1630107a  B[0]=8219c8f9  C[0]=4f82cd8f  D[0]=b32f98e6
A[1]=0eec01d1  B[1]=164b2a09  C[1]=7ed49ae6  D[1]=1da058dc
A[2]=91aec8ae  B[2]=7becafe4  C[2]=08deeead  D[2]=f17f03e8
A[3]=101c278b  B[3]=938c03ac  C[3]=c9fe8114  D[3]=393068dd
A[4]=84ffe403  B[4]=06f91f43  C[4]=f06d6402  D[4]=6ab02f91
A[5]=af7c7016  B[5]=8b0171e6  C[5]=ded53391  D[5]=5ff495b4
A[6]=f5c8bc05  B[6]=e78df82d  C[6]=f471e73b  D[6]=a98f1f90
A[7]=3d43e689  B[7]=1f07b6d2  C[7]=74cd9e4e  D[7]=f2343a45

Step 13: (r=19, s=22)
A[0]=9ef4f893  B[0]=83d0b180  C[0]=8219c8f9  D[0]=4f82cd8f
A[1]=9ac4f3ab  B[1]=0e887760  C[1]=164b2a09  D[1]=7ed49ae6
A[2]=9e046cc0  B[2]=45748d76  C[2]=7becafe4  D[2]=08deeead
A[3]=40800c11  B[3]=3c5880e1  C[3]=938c03ac  D[3]=c9fe8114
A[4]=e9db3f2b  B[4]=201c27ff  C[4]=06f91f43  D[4]=f06d6402
A[5]=49700de9  B[5]=80b57be3  C[5]=8b0171e6  D[5]=ded53391
A[6]=1c166d7d  B[6]=e02fae45  C[6]=e78df82d  D[6]=f471e73b
A[7]=6c9acca9  B[7]=3449ea1f  C[7]=1f07b6d2  D[7]=74cd9e4e

Step 14: (r=22, s= 7)
A[0]=d2b80d14  B[0]=24e7bd3e  C[0]=83d0b180  D[0]=8219c8f9
A[1]=52e55fef  B[1]=eae6b13c  C[1]=0e887760  D[1]=164b2a09
A[2]=d98c5790  B[2]=3027811b  C[2]=45748d76  D[2]=7becafe4
A[3]=d00aaf88  B[3]=04502003  C[3]=3c5880e1  D[3]=938c03ac
A[4]=ea1b0a2b  B[4]=cafa76cf  C[4]=201c27ff  D[4]=06f91f43
A[5]=08b27a8a  B[5]=7a525c03  C[5]=80b57be3  D[5]=8b0171e6
A[6]=2ee863b6  B[6]=5f47059b  C[6]=e02fae45  D[6]=e78df82d
A[7]=2427db04  B[7]=2a5b26b3  C[7]=3449ea1f  D[7]=1f07b6d2

Step 15: (r= 7, s=28)
A[0]=0a053349  B[0]=5c068a69  C[0]=24e7bd3e  D[0]=83d0b180
A[1]=593bf8dd  B[1]=72aff7a9  C[1]=eae6b13c  D[1]=0e887760
A[2]=3a563407  B[2]=c62bc86c  C[2]=3027811b  D[2]=45748d76
A[3]=3ecf4067  B[3]=0557c468  C[3]=04502003  D[3]=3c5880e1
A[4]=b9d860a5  B[4]=0d8515f5  C[4]=cafa76cf  D[4]=201c27ff
A[5]=496ce6ee  B[5]=593d4504  C[5]=7a525c03  D[5]=80b57be3
A[6]=143ed0af  B[6]=7431db17  C[6]=5f47059b  D[6]=e02fae45
A[7]=c741b526  B[7]=13ed8212  C[7]=2a5b26b3  D[7]=3449ea1f

Step 16: (r=29, s= 9)
A[0]=4a468db9  B[0]=2140a669  C[0]=5c068a69  D[0]=24e7bd3e
A[1]=6f101831  B[1]=ab277f1b  C[1]=72aff7a9  D[1]=eae6b13c
A[2]=8032c4f6  B[2]=e74ac680  C[2]=c62bc86c  D[2]=3027811b
A[3]=dd8a319e  B[3]=e7d9e80c  C[3]=0557c468  D[3]=04502003
A[4]=51a5e622  B[4]=b73b0c14  C[4]=0d8515f5  D[4]=cafa76cf
```

```
A[5]=9f1772c5  B[5]=c92d9cdd  C[5]=593d4504  D[5]=7a525c03
A[6]=23a8dd66  B[6]=e287da15  C[6]=7431db17  D[6]=5f47059b
A[7]=a966d11c  B[7]=d8e836a4  C[7]=13ed8212  D[7]=2a5b26b3

Step 17: (r= 9, s=15)
A[0]=db134402  B[0]=8d1b7294  C[0]=2140a669  D[0]=5c068a69
A[1]=07ccf476  B[1]=203062de  C[1]=ab277f1b  D[1]=72aff7a9
A[2]=d1ee4736  B[2]=6589ed00  C[2]=e74ac680  D[2]=c62bc86c
A[3]=837e02e6  B[3]=14633dbb  C[3]=e7d9e80c  D[3]=0557c468
A[4]=692da1ff  B[4]=4bcc44a3  C[4]=b73b0c14  D[4]=0d8515f5
A[5]=01854758  B[5]=2ee58b3e  C[5]=c92d9cdd  D[5]=593d4504
A[6]=d29ea2c3  B[6]=51bacc47  C[6]=e287da15  D[6]=7431db17
A[7]=161f487d  B[7]=cda23952  C[7]=d8e836a4  D[7]=13ed8212

Step 18: (r=15, s= 5)
A[0]=a043bb41  B[0]=a2016d89  C[0]=8d1b7294  D[0]=2140a669
A[1]=427e1738  B[1]=7a3b03e6  C[1]=203062de  D[1]=ab277f1b
A[2]=0673ec9e  B[2]=239b68f7  C[2]=6589ed00  D[2]=e74ac680
A[3]=2d961106  B[3]=017341bf  C[3]=14633dbb  D[3]=e7d9e80c
A[4]=d7805d1a  B[4]=d0ffb496  C[4]=4bcc44a3  D[4]=b73b0c14
A[5]=47a8ff4b  B[5]=a3ac00c2  C[5]=2ee58b3e  D[5]=c92d9cdd
A[6]=5f609589  B[6]=5161e94f  C[6]=51bacc47  D[6]=e287da15
A[7]=0afc64f8  B[7]=a43e8b0f  C[7]=cda23952  D[7]=d8e836a4

Step 19: (r= 5, s=29)
A[0]=5eeb1ba7  B[0]=08776834  C[0]=a2016d89  D[0]=8d1b7294
A[1]=a848f8eb  B[1]=4fc2e708  C[1]=7a3b03e6  D[1]=203062de
A[2]=c6cadb3f  B[2]=ce7d93c0  C[2]=239b68f7  D[2]=6589ed00
A[3]=04667e74  B[3]=b2c220c5  C[3]=017341bf  D[3]=14633dbb
A[4]=ef005eb9  B[4]=f00ba35a  C[4]=d0ffb496  D[4]=4bcc44a3
A[5]=e4b5b4ba  B[5]=f51fe968  C[5]=a3ac00c2  D[5]=2ee58b3e
A[6]=07fd90a5  B[6]=ec12b12b  C[6]=5161e94f  D[6]=51bacc47
A[7]=306737f7  B[7]=5f8c9f01  C[7]=a43e8b0f  D[7]=cda23952

Step 20: (r=29, s= 9)
A[0]=f56586fe  B[0]=ebdd6374  C[0]=08776834  D[0]=a2016d89
A[1]=7290d527  B[1]=75091f1d  C[1]=4fc2e708  D[1]=7a3b03e6
A[2]=45cedb99  B[2]=f8d95b67  C[2]=ce7d93c0  D[2]=239b68f7
A[3]=f3e8a555  B[3]=808ccfce  C[3]=b2c220c5  D[3]=017341bf
A[4]=563d7286  B[4]=3de00bd7  C[4]=f00ba35a  D[4]=d0ffb496
A[5]=d2835bdd  B[5]=5c96b697  C[5]=f51fe968  D[5]=a3ac00c2
A[6]=3fdf3542  B[6]=a0ffb214  C[6]=ec12b12b  D[6]=5161e94f
A[7]=7c20625b  B[7]=e60ce6fe  C[7]=5f8c9f01  D[7]=a43e8b0f

Step 21: (r= 9, s=15)
A[0]=b5cd8a9d  B[0]=cb0dfdea  C[0]=ebdd6374  D[0]=08776834
A[1]=4b304c75  B[1]=21aa4ee5  C[1]=75091f1d  D[1]=4fc2e708
A[2]=3df421dd  B[2]=9db7328b  C[2]=f8d95b67  D[2]=ce7d93c0
A[3]=3bcbc674  B[3]=d14aabe7  C[3]=808ccfce  D[3]=b2c220c5
```

```
A[4]=ea486e9b  B[4]=7ae50cac  C[4]=3de00bd7  D[4]=f00ba35a
A[5]=6f31db76  B[5]=06b7bba5  C[5]=5c96b697  D[5]=f51fe968
A[6]=fb44b85f  B[6]=be6a847f  C[6]=a0ffb214  D[6]=ec12b12b
A[7]=959d33ad  B[7]=40c4b6f8  C[7]=e60ce6fe  D[7]=5f8c9f01

Step 22: (r=15, s= 5)
A[0]=7078ec00  B[0]=c54edae6  C[0]=cb0dfdea  D[0]=ebdd6374
A[1]=d1516b4d  B[1]=263aa598  C[1]=21aa4ee5  D[1]=75091f1d
A[2]=4e24bdbe  B[2]=10ee9efa  C[2]=9db7328b  D[2]=f8d95b67
A[3]=bb3015e5  B[3]=e33a1de5  C[3]=d14aabe7  D[3]=808ccfce
A[4]=8b9c1b87  B[4]=374df524  C[4]=7ae50cac  D[4]=3de00bd7
A[5]=79dd51c8  B[5]=edbb3798  C[5]=06b7bba5  D[5]=5c96b697
A[6]=709f24a7  B[6]=5c2ffda2  C[6]=be6a847f  D[6]=a0ffb214
A[7]=a05a04d1  B[7]=99d6cace  C[7]=40c4b6f8  D[7]=e60ce6fe

Step 23: (r= 5, s=29)
A[0]=52d7ef6e  B[0]=0f1d800e  C[0]=c54edae6  D[0]=cb0dfdea
A[1]=268f6b64  B[1]=2a2d69ba  C[1]=263aa598  D[1]=21aa4ee5
A[2]=6d5db96c  B[2]=c497b7c9  C[2]=10ee9efa  D[2]=9db7328b
A[3]=be90cdec  B[3]=6602bcb7  C[3]=e33a1de5  D[3]=d14aabe7
A[4]=19174df1  B[4]=738370f1  C[4]=374df524  D[4]=7ae50cac
A[5]=f8d38ab9  B[5]=3baa390f  C[5]=edbb3798  D[5]=06b7bba5
A[6]=bb41f1a8  B[6]=13e494ee  C[6]=5c2ffda2  D[6]=be6a847f
A[7]=164ac89b  B[7]=0b409a34  C[7]=99d6cace  D[7]=40c4b6f8

Step 24: (r= 4, s=13)
A[0]=a72576f1  B[0]=2d7ef6e5  C[0]=0f1d800e  D[0]=c54edae6
A[1]=ca677d53  B[1]=68f6b642  C[1]=2a2d69ba  D[1]=263aa598
A[2]=629f748f  B[2]=d5db96c6  C[2]=c497b7c9  D[2]=10ee9efa
A[3]=50fd718d  B[3]=e90cdecb  C[3]=6602bcb7  D[3]=e33a1de5
A[4]=4db4eb91  B[4]=9174df11  C[4]=738370f1  D[4]=374df524
A[5]=b506f61f  B[5]=8d38ab9f  C[5]=3baa390f  D[5]=edbb3798
A[6]=ac04f585  B[6]=b41f1a8b  C[6]=13e494ee  D[6]=5c2ffda2
A[7]=cf44198d  B[7]=64ac89b1  C[7]=0b409a34  D[7]=99d6cace

Step 25: (r=13, s=10)
A[0]=8ec89d0c  B[0]=aede34e4  C[0]=2d7ef6e5  D[0]=0f1d800e
A[1]=af85fd59  B[1]=efaa794c  C[1]=68f6b642  D[1]=2a2d69ba
A[2]=5e666d69  B[2]=ee91ec53  C[2]=d5db96c6  D[2]=c497b7c9
A[3]=f2a9c745  B[3]=ae31aa1f  C[3]=e90cdecb  D[3]=6602bcb7
A[4]=39b012ad  B[4]=9d7229b6  C[4]=9174df11  D[4]=738370f1
A[5]=facf032d  B[5]=dec3f6a0  C[5]=8d38ab9f  D[5]=3baa390f
A[6]=0aeeef80  B[6]=9eb0b580  C[6]=b41f1a8b  D[6]=13e494ee
A[7]=e876414f  B[7]=8331b9e8  C[7]=64ac89b1  D[7]=0b409a34

Step 26: (r=10, s=25)
A[0]=8d37af35  B[0]=2274323b  C[0]=aede34e4  D[0]=2d7ef6e5
A[1]=c3283353  B[1]=17f566be  C[1]=efaa794c  D[1]=68f6b642
A[2]=17c4eb09  B[2]=99b5a579  C[2]=ee91ec53  D[2]=d5db96c6
```

```
A[3]=a32dfa65  B[3]=a71d17ca  C[3]=ae31aa1f  D[3]=e90cdecb
A[4]=6ddcae60  B[4]=c04ab4e6  C[4]=9d7229b6  D[4]=9174df11
A[5]=7924a73c  B[5]=3c0cb7eb  C[5]=dec3f6a0  D[5]=8d38ab9f
A[6]=345612f6  B[6]=bbbe002b  C[6]=9eb0b580  D[6]=b41f1a8b
A[7]=36bf2ad7  B[7]=d9053fa1  C[7]=8331b9e8  D[7]=64ac89b1

Step 27: (r=25, s= 4)
A[0]=325afb94  B[0]=6b1a6f5e  C[0]=2274323b  D[0]=aede34e4
A[1]=5db6874a  B[1]=a7865066  C[1]=17f566be  D[1]=efaa794c
A[2]=816a8db4  B[2]=122f89d6  C[2]=99b5a579  D[2]=ee91ec53
A[3]=03e5cbb9  B[3]=cb465bf4  C[3]=a71d17ca  D[3]=ae31aa1f
A[4]=918d5863  B[4]=c0dbb95c  C[4]=c04ab4e6  D[4]=9d7229b6
A[5]=d15faa6e  B[5]=78f2494e  C[5]=3c0cb7eb  D[5]=dec3f6a0
A[6]=6d1d90f3  B[6]=ec68ac25  C[6]=bbbe002b  D[6]=9eb0b580
A[7]=8026e1f1  B[7]=ae6d7e55  C[7]=d9053fa1  D[7]=8331b9e8

Step 28: (r= 4, s=13)
A[0]=9e9b3b32  B[0]=25afb943  C[0]=6b1a6f5e  D[0]=2274323b
A[1]=27c7366e  B[1]=db6874a5  C[1]=a7865066  D[1]=17f566be
A[2]=e780ea0d  B[2]=16a8db48  C[2]=122f89d6  D[2]=99b5a579
A[3]=37a6029a  B[3]=3e5cbb90  C[3]=cb465bf4  D[3]=a71d17ca
A[4]=cc70d9df  B[4]=18d58639  C[4]=c0dbb95c  D[4]=c04ab4e6
A[5]=14d3d297  B[5]=15faa6ed  C[5]=78f2494e  D[5]=3c0cb7eb
A[6]=540e9958  B[6]=d1d90f36  C[6]=ec68ac25  D[6]=bbbe002b
A[7]=b13aa680  B[7]=026e1f18  C[7]=ae6d7e55  D[7]=d9053fa1

Step 29: (r=13, s=10)
A[0]=d6131218  B[0]=676653d3  C[0]=25afb943  D[0]=6b1a6f5e
A[1]=8ca2992d  B[1]=e6cdc4f8  C[1]=db6874a5  D[1]=a7865066
A[2]=039de9b7  B[2]=1d41bcf0  C[2]=16a8db48  D[2]=122f89d6
A[3]=364d2678  B[3]=c05346f4  C[3]=3e5cbb90  D[3]=cb465bf4
A[4]=7507743b  B[4]=1b3bf98e  C[4]=18d58639  D[4]=c0dbb95c
A[5]=ff68baa0  B[5]=7a52e29a  C[5]=15faa6ed  D[5]=78f2494e
A[6]=602fc19a  B[6]=d32b0a81  C[6]=d1d90f36  D[6]=ec68ac25
A[7]=c242ce24  B[7]=54d01627  C[7]=026e1f18  D[7]=ae6d7e55

Step 30: (r=10, s=25)
A[0]=c8feecd7  B[0]=4c486358  C[0]=676653d3  D[0]=25afb943
A[1]=11576b62  B[1]=8a64b632  C[1]=e6cdc4f8  D[1]=db6874a5
A[2]=51f8041e  B[2]=77a6dc0e  C[2]=1d41bcf0  D[2]=16a8db48
A[3]=747c050d  B[3]=3499e0d9  C[3]=c05346f4  D[3]=3e5cbb90
A[4]=8acc8628  B[4]=1dd0edd4  C[4]=1b3bf98e  D[4]=18d58639
A[5]=af1e8120  B[5]=a2ea83fd  C[5]=7a52e29a  D[5]=15faa6ed
A[6]=ce960e1f  B[6]=bf066980  C[6]=d32b0a81  D[6]=d1d90f36
A[7]=25fc605b  B[7]=0b389309  C[7]=54d01627  D[7]=026e1f18

Step 31: (r=25, s= 4)
A[0]=ad861f4e  B[0]=af91fdd9  C[0]=4c486358  D[0]=676653d3
A[1]=6d771229  B[1]=c422aed6  C[1]=8a64b632  D[1]=e6cdc4f8
```

```
A[2]=851f8ca6  B[2]=3ca3f008  C[2]=77a6dc0e  D[2]=1d41bcf0
A[3]=e987fdc4  B[3]=1ae8f80a  C[3]=3499e0d9  D[3]=c05346f4
A[4]=02bdeac8  B[4]=5115990c  C[4]=1dd0edd4  D[4]=1b3bf98e
A[5]=683ed059  B[5]=415e3d02  C[5]=a2ea83fd  D[5]=7a52e29a
A[6]=e4c18d60  B[6]=3f9d2c1c  C[6]=bf066980  D[6]=d32b0a81
A[7]=927ecfff  B[7]=b64bf8c0  C[7]=0b389309  D[7]=54d01627

Feed-Forward Step 32: (r= 4, s=13)
A[0]=2a6c4074  B[0]=d861f4ea  C[0]=af91fdd9  D[0]=4c486358
A[1]=400b29ed  B[1]=d7712296  C[1]=c422aed6  D[1]=8a64b632
A[2]=9933707c  B[2]=51f8ca68  C[2]=3ca3f008  D[2]=77a6dc0e
A[3]=5078fcc3  B[3]=987fdc4e  C[3]=1ae8f80a  D[3]=3499e0d9
A[4]=2a7c7377  B[4]=2bdeac80  C[4]=5115990c  D[4]=1dd0edd4
A[5]=294cd52a  B[5]=83ed0596  C[5]=415e3d02  D[5]=a2ea83fd
A[6]=cff03366  B[6]=4c18d60e  C[6]=3f9d2c1c  D[6]=bf066980
A[7]=70fec0fc  B[7]=27ecfff9  C[7]=b64bf8c0  D[7]=0b389309

Feed-Forward Step 33: (r=13, s=10)
A[0]=8d9d2ef0  B[0]=880e854d  C[0]=d861f4ea  D[0]=af91fdd9
A[1]=57444041  B[1]=653da801  C[1]=d7712296  D[1]=c422aed6
A[2]=c48d508c  B[2]=6e0f9326  C[2]=51f8ca68  D[2]=3ca3f008
A[3]=7a0a5dcb  B[3]=1f986a0f  C[3]=987fdc4e  D[3]=1ae8f80a
A[4]=2f6aa22f  B[4]=8e6ee54f  C[4]=2bdeac80  D[4]=5115990c
A[5]=d9e856c3  B[5]=9aa54529  C[5]=83ed0596  D[5]=415e3d02
A[6]=f09c1d51  B[6]=066cd9fe  C[6]=4c18d60e  D[6]=3f9d2c1c
A[7]=7b4a4b98  B[7]=d81f8e1f  C[7]=27ecfff9  D[7]=b64bf8c0

Feed-Forward Step 34: (r=10, s=25)
A[0]=170ccfb2  B[0]=74bbc236  C[0]=880e854d  D[0]=d861f4ea
A[1]=683667d6  B[1]=1101055d  C[1]=653da801  D[1]=d7712296
A[2]=012f2214  B[2]=35423312  C[2]=6e0f9326  D[2]=51f8ca68
A[3]=25509774  B[3]=29772de8  C[3]=1f986a0f  D[3]=987fdc4e
A[4]=aac0e563  B[4]=aa88bcbd  C[4]=8e6ee54f  D[4]=2bdeac80
A[5]=afece435  B[5]=a15b0f67  C[5]=9aa54529  D[5]=83ed0596
A[6]=f601e281  B[6]=707547c2  C[6]=066cd9fe  D[6]=4c18d60e
A[7]=eee73950  B[7]=292e61ed  C[7]=d81f8e1f  D[7]=27ecfff9

Feed-Forward Step 35: (r=25, s= 4)
A[0]=d460ac96  B[0]=642e199f  C[0]=74bbc236  D[0]=880e854d
A[1]=603746cd  B[1]=acd06ccf  C[1]=1101055d  D[1]=653da801
A[2]=c79d28ca  B[2]=28025e44  C[2]=35423312  D[2]=6e0f9326
A[3]=3b412039  B[3]=e84aa12e  C[3]=29772de8  D[3]=1f986a0f
A[4]=3367c134  B[4]=c75581ca  C[4]=aa88bcbd  D[4]=8e6ee54f
A[5]=ea44617d  B[5]=6b5fd9c8  C[5]=a15b0f67  D[5]=9aa54529
A[6]=80945284  B[6]=03ec03c5  C[6]=707547c2  D[6]=066cd9fe
A[7]=8ff5597c  B[7]=a1ddce72  C[7]=292e61ed  D[7]=d81f8e1f
```

Compression Function Output

```
A[0]=d460ac96  B[0]=642e199f  C[0]=74bbc236  D[0]=880e854d
```

```
A[1]=603746cd  B[1]=acd06ccf  C[1]=1101055d  D[1]=653da801
A[2]=c79d28ca  B[2]=28025e44  C[2]=35423312  D[2]=6e0f9326
A[3]=3b412039  B[3]=e84aa12e  C[3]=29772de8  D[3]=1f986a0f
A[4]=3367c134  B[4]=c75581ca  C[4]=aa88bcbd  D[4]=8e6ee54f
A[5]=ea44617d  B[5]=6b5fd9c8  C[5]=a15b0f67  D[5]=9aa54529
A[6]=80945284  B[6]=03ec03c5  C[6]=707547c2  D[6]=066cd9fe
A[7]=8ff5597c  B[7]=a1ddce72  C[7]=292e61ed  D[7]=d81f8e1f
```

Final block

```
M[  0..  7] = 37 04 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =   61  165  253   25  100  103   38  217
y[  8.. 15] =   83  222  217   81  155  191  230   68
y[ 16.. 23] =  160   84  131  211  120  256   67  256
y[ 24.. 31] =   70  153   56  134  184   54   47  116
y[ 32.. 39] =    3  142  144  243   16   32   20   71
y[ 40.. 47] =   63   73  194  216  243  207  172  210
y[ 48.. 55] =  183  243   53   83  146   42  138  255
y[ 56.. 63] =  108  123  230   72  215  135    9   14
y[ 64.. 71] =  119  197   87   94   48   28  240   38
y[ 72.. 79] =   57  190   59  107  148  226  117  121
y[ 80.. 87] =  177  224  217  112   89  175   90   39
y[ 88.. 95] =   72  226   62  109  209  193  100  189
y[ 96..103] =  243  143  181  173  213  195   59  237
y[104..111] =  200   30   90  227   52  251   86   58
y[112..119] =   43   98  145   86  103  101  123  134
y[120..127] =   12   87   90  153  210  217   69   88
y[128..135] =   49  202  114   85   10    7   72  150
y[136..143] =   27  145  150   29  212  176  137   42
y[144..151] =  207   26  236  156  247  111   43  111
y[152..159] =   40  214   54  233  183   56   63  251
y[160..167] =  107  225  223  124   94   78   90   39
```

```
y[168..175] =  47  37 173 151 124 160 195 157
y[176..183] = 184 124  57  27 221  68 229 112
y[184..191] =   2 244 137  38 152 232 101  96
y[192..199] = 248 170  23  16  62  82 127  72
y[200..207] =  53 177  51   3 219 141 250 246
y[208..215] = 190 143 150 255  21 192  20  71
y[216..223] =  38 141  48   1 158 174  10 178
y[224..231] = 124 224 186 194 154 172  51 130
y[232..239] = 167  80  20 140  58 116  24  52
y[240..247] =  67  12 222  24   7   9 244 233
y[248..255] =  98  23  20 214 157 150  41  22
```

Intermediate Expanded Message

```
Z[ 0] = bd842c15  1211fd1c  4a6f4844  e3181b76
        e6b53bfb  3a89e318  d04eb64a  3124ec7d
Z[ 1] = 3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
        b4d83296  a71d2878  2706cb3f  53d421f7
Z[ 2] = ace5022b  f5e2ae57  17200b90  334f0e74
        34c12d87  e25fd279  dbdef5e2  de09c293
Z[ 3] = f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
        58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
Z[ 4] = d4a455ff  43ee3edf  143c22b0  1b76f3b7
        cf952931  4d532aa3  e999b13b  5771548d
Z[ 5] = e827c630  50f0e318  c4be4051  1c2f410a
        e9993408  4ec52cce  d1c0dd50  cedc4844
Z[ 6] = ad9ef5e2  c34cc914  d332e034  f18c2aa3
        15aed6cf  ea52410a  fbaa2594  29ea3e26
Z[ 7] = 46d21f13  3e26af10  48fd4a6f  a71d58e3
        3edf08ac  b4d8410a  e318de09  3f9831dd
Z[ 8] = d8412369  3d6d5262  050f073a  b2ad3408
        af101383  14f5b2ad  c577df7b  1e5aa948
Z[ 9] = 12cadbde  b703f0d3  5037f8c6  50371f13
        e0ed1ce8  eea82706  2878ca86  fbaa2d87
Z[10] = e8e04d53  599ce76e  385e43ee  1c2f410a
        1abd21f7  b366c34c  b9e7599c  b7bcd332
Z[11] = 599ccb3f  13832931  3124e5fc  50f0ebc4
        f69b0172  1b76a948  edefb41f  456048fd
Z[12] = c121f97f  0b90109f  3b422cce  34085bc7
        c630264d  022b24db  ac2ce48a  f80dfaf1
Z[13] = ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
        ac2c1b76  00b922b0  c405b875  c6e9073a
Z[14] = e827599c  d279ccb1  c293b591  a43924db
        39d0bef6  ab730e74  53d429ea  25941158
Z[15] = 08ac306b  1158e6b5  0681050f  eea8f69b
        109f46d2  e0ed0e74  b2adb7bc  0fe61da1
Z[16] = 2c993785  67c2fc5c  091a5b04  41882296
        18934b8b  9e9ddb98  d70ba32a  92c8e76d
Z[17] = d27ea7b7  ece38d52  f6e66d38  27233cfb
```

```
         24683fb6  312632f8  bca6bd8f  39572ac7
Z[18] =  616302bb  e10e9927  558e0e90  51ea1234
         2ac73957  b38cc6a9  70dcf342  c792b2a3
Z[19] =  bd8fbca6  33e1303d  df3c9af9  e68493b1
         01d2624c  92c8e76d  a06fd9c6  5bed0831
Z[20] =  f7cf6c4f  14ef4f2f  386e2bb0  7397f087
         303d33e1  2e6b35b3  dd6a9ccb  f9a16a7d
Z[21] =  c305b730  9e9ddb98  131d5101  123451ea
         22964188  2bb0386e  a5e5d450  091a5b04
Z[22] =  70dcf342  bf61bad4  a241d7f4  2e6b35b3
         ae16cc1f  123451ea  34ca2f54  15d84e46
Z[23] =  3cfb2723  e0259a10  065f5dbf  f42b6ff3
         59320aec  123451ea  a4fcd539  25513ecd
Z[24] =  cdf1ac44  4d5d16c1  065f5dbf  9e9ddb98
         9a10e025  1a6549b9  b647c3ee  263a3de4
Z[25] =  17aa4c74  a413d622  6507ff17  6507ff17
         d8dda158  ea28900d  32f83126  fa8a6994
Z[26] =  e2e09755  70dcf342  46fe1d20  237f409f
         21ad4271  9f86daaf  a7b7d27e  a4fcd539
Z[27] =  70dcf342  18934b8b  3de4263a  65f0fe2e
         f42b6ff3  22964188  e93f90f6  57600cbe
Z[28] =  b0d1c964  0e90558e  4aa2197c  41882296
         b730c305  02bb6163  966ce3c9  f5fd6e21
Z[29] =  983ee1f7  fe2e65f0  c4d7b55e  409f237f
         966ce3c9  00e96335  b475c5c0  b819c21c
Z[30] =  e1f7983e  c6a9b38c  b2a3c792  8c69edcc
         48d01b4e  9583e4b2  6994fa8a  2f5434ca
Z[31] =  0aec5932  15d84e46  08315bed  ea28900d
         14ef4f2f  d8dda158  9e9ddb98  14065018
```

Expanded Message

```
W[ 0] =  d4a455ff  43ee3edf  143c22b0  1b76f3b7
         cf952931  4d532aa3  e999b13b  5771548d
W[ 1] =  ad9ef5e2  c34cc914  d332e034  f18c2aa3
         15aed6cf  ea52410a  fbaa2594  29ea3e26
W[ 2] =  bd842c15  1211fd1c  4a6f4844  e3181b76
         e6b53bfb  3a89e318  d04eb64a  3124ec7d
W[ 3] =  ace5022b  f5e2ae57  17200b90  334f0e74
         34c12d87  e25fd279  dbdef5e2  de09c293
W[ 4] =  46d21f13  3e26af10  48fd4a6f  a71d58e3
         3edf08ac  b4d8410a  e318de09  3f9831dd
W[ 5] =  e827c630  50f0e318  c4be4051  1c2f410a
         e9993408  4ec52cce  d1c0dd50  cedc4844
W[ 6] =  f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
         58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
W[ 7] =  3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
         b4d83296  a71d2878  2706cb3f  53d421f7
W[ 8] =  08ac306b  1158e6b5  0681050f  eea8f69b
```

```
         109f46d2  e0ed0e74  b2adb7bc  0fe61da1
W[ 9] =  599ccb3f  13832931  3124e5fc  50f0ebc4
         f69b0172  1b76a948  edefb41f  456048fd
W[10] =  c121f97f  0b90109f  3b422cce  34085bc7
         c630264d  022b24db  ac2ce48a  f80dfaf1
W[11] =  d8412369  3d6d5262  050f073a  b2ad3408
         af101383  14f5b2ad  c577df7b  1e5aa948
W[12] =  12cadbde  b703f0d3  5037f8c6  50371f13
         e0ed1ce8  eea82706  2878ca86  fbaa2d87
W[13] =  ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
         ac2c1b76  00b922b0  c405b875  c6e9073a
W[14] =  e8e04d53  599ce76e  385e43ee  1c2f410a
         1abd21f7  b366c34c  b9e7599c  b7bcd332
W[15] =  e827599c  d279ccb1  c293b591  a43924db
         39d0bef6  ab730e74  53d429ea  25941158
W[16] =  d27ea7b7  ece38d52  f6e66d38  27233cfb
         24683fb6  312632f8  bca6bd8f  39572ac7
W[17] =  616302bb  e10e9927  558e0e90  51ea1234
         2ac73957  b38cc6a9  70dcf342  c792b2a3
W[18] =  3cfb2723  e0259a10  065f5dbf  f42b6ff3
         59320aec  123451ea  a4fcd539  25513ecd
W[19] =  f7cf6c4f  14ef4f2f  386e2bb0  7397f087
         303d33e1  2e6b35b3  dd6a9ccb  f9a16a7d
W[20] =  70dcf342  bf61bad4  a241d7f4  2e6b35b3
         ae16cc1f  123451ea  34ca2f54  15d84e46
W[21] =  c305b730  9e9ddb98  131d5101  123451ea
         22964188  2bb0386e  a5e5d450  091a5b04
W[22] =  2c993785  67c2fc5c  091a5b04  41882296
         18934b8b  9e9ddb98  d70ba32a  92c8e76d
W[23] =  bd8fbca6  33e1303d  df3c9af9  e68493b1
         01d2624c  92c8e76d  a06fd9c6  5bed0831
W[24] =  e1f7983e  c6a9b38c  b2a3c792  8c69edcc
         48d01b4e  9583e4b2  6994fa8a  2f5434ca
W[25] =  cdf1ac44  4d5d16c1  065f5dbf  9e9ddb98
         9a10e025  1a6549b9  b647c3ee  263a3de4
W[26] =  17aa4c74  a413d622  6507ff17  6507ff17
         d8dda158  ea28900d  32f83126  fa8a6994
W[27] =  0aec5932  15d84e46  08315bed  ea28900d
         14ef4f2f  d8dda158  9e9ddb98  14065018
W[28] =  70dcf342  18934b8b  3de4263a  65f0fe2e
         f42b6ff3  22964188  e93f90f6  57600cbe
W[29] =  983ee1f7  fe2e65f0  c4d7b55e  409f237f
         966ce3c9  00e96335  b475c5c0  b819c21c
W[30] =  b0d1c964  0e90558e  4aa2197c  41882296
         b730c305  02bb6163  966ce3c9  f5fd6e21
W[31] =  e2e09755  70dcf342  46fe1d20  237f409f
         21ad4271  9f86daaf  a7b7d27e  a4fcd539
```

Feistel Steps

```
IV :
A[0]=d460ac96  B[0]=642e199f  C[0]=74bbc236  D[0]=880e854d
A[1]=603746cd  B[1]=acd06ccf  C[1]=1101055d  D[1]=653da801
A[2]=c79d28ca  B[2]=28025e44  C[2]=35423312  D[2]=6e0f9326
A[3]=3b412039  B[3]=e84aa12e  C[3]=29772de8  D[3]=1f986a0f
A[4]=3367c134  B[4]=c75581ca  C[4]=aa88bcbd  D[4]=8e6ee54f
A[5]=ea44617d  B[5]=6b5fd9c8  C[5]=a15b0f67  D[5]=9aa54529
A[6]=80945284  B[6]=03ec03c5  C[6]=707547c2  D[6]=066cd9fe
A[7]=8ff5597c  B[7]=a1ddce72  C[7]=292e61ed  D[7]=d81f8e1f

IV XOR M :
A[0]=d460a8a1  B[0]=642e199f  C[0]=74bbc236  D[0]=880e854d
A[1]=603746cd  B[1]=acd06ccf  C[1]=1101055d  D[1]=653da801
A[2]=c79d28ca  B[2]=28025e44  C[2]=35423312  D[2]=6e0f9326
A[3]=3b412039  B[3]=e84aa12e  C[3]=29772de8  D[3]=1f986a0f
A[4]=3367c134  B[4]=c75581ca  C[4]=aa88bcbd  D[4]=8e6ee54f
A[5]=ea44617d  B[5]=6b5fd9c8  C[5]=a15b0f67  D[5]=9aa54529
A[6]=80945284  B[6]=03ec03c5  C[6]=707547c2  D[6]=066cd9fe
A[7]=8ff5597c  B[7]=a1ddce72  C[7]=292e61ed  D[7]=d81f8e1f

Step  0: (r= 3, s=23)
A[0]=f39aed7d  B[0]=a305450e  C[0]=642e199f  D[0]=74bbc236
A[1]=01f26324  B[1]=01ba366b  C[1]=acd06ccf  D[1]=1101055d
A[2]=6d6248b1  B[2]=3ce94656  C[2]=28025e44  D[2]=35423312
A[3]=141b091b  B[3]=da0901c9  C[3]=e84aa12e  D[3]=29772de8
A[4]=5717f4d5  B[4]=9b3e09a1  C[4]=c75581ca  D[4]=aa88bcbd
A[5]=2667b580  B[5]=52230bef  C[5]=6b5fd9c8  D[5]=a15b0f67
A[6]=ff5b41ad  B[6]=04a29424  C[6]=03ec03c5  D[6]=707547c2
A[7]=d38b4c49  B[7]=7faacbe4  C[7]=a1ddce72  D[7]=292e61ed

Step  1: (r=23, s=17)
A[0]=f24d409e  B[0]=bef9cd76  C[0]=a305450e  D[0]=642e199f
A[1]=1fa2c9a5  B[1]=9200f931  C[1]=01ba366b  D[1]=acd06ccf
A[2]=3ddff5a4  B[2]=58b6b124  C[2]=3ce94656  D[2]=28025e44
A[3]=b3835a73  B[3]=8d8a0d84  C[3]=da0901c9  D[3]=e84aa12e
A[4]=82e5583f  B[4]=6aab8bfa  C[4]=9b3e09a1  D[4]=c75581ca
A[5]=c1fdbb55  B[5]=c01333da  C[5]=52230bef  D[5]=6b5fd9c8
A[6]=9e6eaf00  B[6]=d6ffada0  C[6]=04a29424  D[6]=03ec03c5
A[7]=670c871f  B[7]=24e9c5a6  C[7]=7faacbe4  D[7]=a1ddce72

Step  2: (r=17, s=27)
A[0]=41f05815  B[0]=813de49a  C[0]=bef9cd76  D[0]=a305450e
A[1]=6b6f4250  B[1]=934a3f45  C[1]=9200f931  D[1]=01ba366b
A[2]=75972769  B[2]=eb487bbf  C[2]=58b6b124  D[2]=3ce94656
A[3]=f7f1a576  B[3]=b4e76706  C[3]=8d8a0d84  D[3]=da0901c9
A[4]=5c4f6b18  B[4]=b07f05ca  C[4]=6aab8bfa  D[4]=9b3e09a1
A[5]=e1feb59f  B[5]=76ab83fb  C[5]=c01333da  D[5]=52230bef
A[6]=4bd85183  B[6]=5e013cdd  C[6]=d6ffada0  D[6]=04a29424
A[7]=1f28f041  B[7]=0e3ece19  C[7]=24e9c5a6  D[7]=7faacbe4
```

```
Step  3: (r=27, s= 3)
A[0]=30dff283  B[0]=aa0f82c0  C[0]=813de49a  D[0]=bef9cd76
A[1]=a2e9ba57  B[1]=835b7a12  C[1]=934a3f45  D[1]=9200f931
A[2]=6caba2af  B[2]=4bacb93b  C[2]=eb487bbf  D[2]=58b6b124
A[3]=fc2970de  B[3]=b7bf8d2b  C[3]=b4e76706  D[3]=8d8a0d84
A[4]=206f1012  B[4]=c2e27b58  C[4]=b07f05ca  D[4]=6aab8bfa
A[5]=c3d1d4a8  B[5]=ff0ff5ac  C[5]=76ab83fb  D[5]=c01333da
A[6]=f45a2ae9  B[6]=1a5ec28c  C[6]=5e013cdd  D[6]=d6ffada0
A[7]=27d51c4c  B[7]=08f94782  C[7]=0e3ece19  D[7]=24e9c5a6

Step  4: (r= 3, s=23)
A[0]=a4619b2d  B[0]=86ff9419  C[0]=aa0f82c0  D[0]=813de49a
A[1]=4fa23a02  B[1]=174dd2bd  C[1]=835b7a12  D[1]=934a3f45
A[2]=e7af90bc  B[2]=655d157b  C[2]=4bacb93b  D[2]=eb487bbf
A[3]=5dc602b4  B[3]=e14b86f7  C[3]=b7bf8d2b  D[3]=b4e76706
A[4]=1772cf90  B[4]=03788091  C[4]=c2e27b58  D[4]=b07f05ca
A[5]=cd35cfbe  B[5]=1e8ea546  C[5]=ff0ff5ac  D[5]=76ab83fb
A[6]=1c57c052  B[6]=a2d1574f  C[6]=1a5ec28c  D[6]=5e013cdd
A[7]=2b16d51d  B[7]=3ea8e261  C[7]=08f94782  D[7]=0e3ece19

Step  5: (r=23, s=17)
A[0]=083bab14  B[0]=96d230cd  C[0]=86ff9419  D[0]=aa0f82c0
A[1]=61ee02ed  B[1]=0127d11d  C[1]=174dd2bd  D[1]=835b7a12
A[2]=79fcca4f  B[2]=5e73d7c8  C[2]=655d157b  D[2]=4bacb93b
A[3]=259b4733  B[3]=5a2ee301  C[3]=e14b86f7  D[3]=b7bf8d2b
A[4]=64f41e17  B[4]=c80bb967  C[4]=03788091  D[4]=c2e27b58
A[5]=8b6320c9  B[5]=df669ae7  C[5]=1e8ea546  D[5]=ff0ff5ac
A[6]=ba1e6550  B[6]=290e2be0  C[6]=a2d1574f  D[6]=1a5ec28c
A[7]=518e4074  B[7]=8e958b6a  C[7]=3ea8e261  D[7]=08f94782

Step  6: (r=17, s=27)
A[0]=556639d3  B[0]=56281077  C[0]=96d230cd  D[0]=86ff9419
A[1]=27994a5e  B[1]=05dac3dc  C[1]=0127d11d  D[1]=174dd2bd
A[2]=49dd9e3e  B[2]=949ef3f9  C[2]=5e73d7c8  D[2]=655d157b
A[3]=79a3730e  B[3]=8e664b36  C[3]=5a2ee301  D[3]=e14b86f7
A[4]=310a0382  B[4]=3c2ec9e8  C[4]=c80bb967  D[4]=03788091
A[5]=8c6ebff3  B[5]=419316c6  C[5]=df669ae7  D[5]=1e8ea546
A[6]=28019454  B[6]=caa1743c  C[6]=290e2be0  D[6]=a2d1574f
A[7]=a7f36bb9  B[7]=80e8a31c  C[7]=8e958b6a  D[7]=3ea8e261

Step  7: (r=27, s= 3)
A[0]=c1f0c10a  B[0]=9aab31ce  C[0]=56281077  D[0]=96d230cd
A[1]=780d0a2d  B[1]=f13cca52  C[1]=05dac3dc  D[1]=0127d11d
A[2]=7fef3cf6  B[2]=f24eecf1  C[2]=949ef3f9  D[2]=5e73d7c8
A[3]=c817c032  B[3]=73cd1b98  C[3]=8e664b36  D[3]=5a2ee301
A[4]=1f3d5e4e  B[4]=1188501c  C[4]=3c2ec9e8  D[4]=c80bb967
A[5]=aa1bb548  B[5]=9c6375ff  C[5]=419316c6  D[5]=df669ae7
A[6]=5c0a5374  B[6]=a1400ca2  C[6]=caa1743c  D[6]=290e2be0
```

```
A[7]=6cb58922  B[7]=cd3f9b5d  C[7]=80e8a31c  D[7]=8e958b6a

Step  8: (r=28, s=19)
A[0]=db7a566a  B[0]=ac1f0c10  C[0]=9aab31ce  D[0]=56281077
A[1]=43df9b8e  B[1]=d780d0a2  C[1]=f13cca52  D[1]=05dac3dc
A[2]=48769082  B[2]=67fef3cf  C[2]=f24eecf1  D[2]=949ef3f9
A[3]=b026353b  B[3]=2c817c03  C[3]=73cd1b98  D[3]=8e664b36
A[4]=f727417d  B[4]=e1f3d5e4  C[4]=1188501c  D[4]=3c2ec9e8
A[5]=35cdcaba  B[5]=8aa1bb54  C[5]=9c6375ff  D[5]=419316c6
A[6]=ea41fef8  B[6]=45c0a537  C[6]=a1400ca2  D[6]=caa1743c
A[7]=78bc286c  B[7]=26cb5892  C[7]=cd3f9b5d  D[7]=80e8a31c

Step  9: (r=19, s=22)
A[0]=d2a05bb4  B[0]=b356dbd2  C[0]=ac1f0c10  D[0]=9aab31ce
A[1]=21a0c0e0  B[1]=dc721efc  C[1]=d780d0a2  D[1]=f13cca52
A[2]=6d84ec87  B[2]=841243b4  C[2]=67fef3cf  D[2]=f24eecf1
A[3]=3bc2e719  B[3]=a9dd8131  C[3]=2c817c03  D[3]=73cd1b98
A[4]=274c6f56  B[4]=0befb93a  C[4]=e1f3d5e4  D[4]=1188501c
A[5]=1c5d3140  B[5]=55d1ae6e  C[5]=8aa1bb54  D[5]=9c6375ff
A[6]=2f6e2dad  B[6]=f7c7520f  C[6]=45c0a537  D[6]=a1400ca2
A[7]=206ca38f  B[7]=4363c5e1  C[7]=26cb5892  D[7]=cd3f9b5d

Step 10: (r=22, s= 7)
A[0]=bc945f45  B[0]=ed34a816  C[0]=b356dbd2  D[0]=ac1f0c10
A[1]=98514b24  B[1]=38086830  C[1]=dc721efc  D[1]=d780d0a2
A[2]=3dbf2dca  B[2]=21db613b  C[2]=841243b4  D[2]=67fef3cf
A[3]=b8bce180  B[3]=c64ef0b9  C[3]=a9dd8131  D[3]=2c817c03
A[4]=bfe028f5  B[4]=d589d31b  C[4]=0befb93a  D[4]=e1f3d5e4
A[5]=2b6e72a5  B[5]=5007174c  C[5]=55d1ae6e  D[5]=8aa1bb54
A[6]=e9bfbd26  B[6]=6b4bdb8b  C[6]=f7c7520f  D[6]=45c0a537
A[7]=ee41c301  B[7]=e3c81b28  C[7]=4363c5e1  D[7]=26cb5892

Step 11: (r= 7, s=28)
A[0]=aa74be15  B[0]=4a2fa2de  C[0]=ed34a816  D[0]=b356dbd2
A[1]=b72582de  B[1]=28a5924c  C[1]=38086830  D[1]=dc721efc
A[2]=91cc16db  B[2]=df96e51e  C[2]=21db613b  D[2]=841243b4
A[3]=a5e65c7f  B[3]=5e70c05c  C[3]=c64ef0b9  D[3]=a9dd8131
A[4]=4b0ec9f4  B[4]=f0147adf  C[4]=d589d31b  D[4]=0befb93a
A[5]=497293a2  B[5]=b7395295  C[5]=5007174c  D[5]=55d1ae6e
A[6]=37190657  B[6]=dfde9374  C[6]=6b4bdb8b  D[6]=f7c7520f
A[7]=821f65b9  B[7]=20e180f7  C[7]=e3c81b28  D[7]=4363c5e1

Step 12: (r=28, s=19)
A[0]=a657790e  B[0]=5aa74be1  C[0]=4a2fa2de  D[0]=ed34a816
A[1]=04cfed41  B[1]=eb72582d  C[1]=28a5924c  D[1]=38086830
A[2]=31425a7f  B[2]=b91cc16d  C[2]=df96e51e  D[2]=21db613b
A[3]=cabef07a  B[3]=fa5e65c7  C[3]=5e70c05c  D[3]=c64ef0b9
A[4]=8a6c5514  B[4]=44b0ec9f  C[4]=f0147adf  D[4]=d589d31b
A[5]=00e16ed4  B[5]=2497293a  C[5]=b7395295  D[5]=5007174c
```

```
A[6]=6ad7550a  B[6]=73719065  C[6]=dfde9374  D[6]=6b4bdb8b
A[7]=03b65a98  B[7]=9821f65b  C[7]=20e180f7  D[7]=e3c81b28

Step 13: (r=19, s=22)
A[0]=871d921a  B[0]=c87532bb  C[0]=5aa74be1  D[0]=4a2fa2de
A[1]=4137e6c7  B[1]=6a08267f  C[1]=eb72582d  D[1]=28a5924c
A[2]=223e5506  B[2]=d3f98a12  C[2]=b91cc16d  D[2]=df96e51e
A[3]=b7b524e9  B[3]=83d655f7  C[3]=fa5e65c7  D[3]=5e70c05c
A[4]=9485ad55  B[4]=a8a45362  C[4]=44b0ec9f  D[4]=f0147adf
A[5]=8e2582e8  B[5]=76a0070b  C[5]=2497293a  D[5]=b7395295
A[6]=2d24545b  B[6]=a85356ba  C[6]=73719065  D[6]=dfde9374
A[7]=d3412ab4  B[7]=d4c01db2  C[7]=9821f65b  D[7]=20e180f7

Step 14: (r=22, s= 7)
A[0]=5451c477  B[0]=86a1c764  C[0]=c87532bb  D[0]=5aa74be1
A[1]=4111dc5a  B[1]=b1d04df9  C[1]=6a08267f  D[1]=eb72582d
A[2]=d362f6ae  B[2]=41888f95  C[2]=d3f98a12  D[2]=b91cc16d
A[3]=7cbc362c  B[3]=3a6ded49  C[3]=83d655f7  D[3]=fa5e65c7
A[4]=7568a027  B[4]=5565216b  C[4]=a8a45362  D[4]=44b0ec9f
A[5]=f7f1a733  B[5]=ba238960  C[5]=76a0070b  D[5]=2497293a
A[6]=48d5962b  B[6]=16cb4915  C[6]=a85356ba  D[6]=73719065
A[7]=8694b6e9  B[7]=ad34d04a  C[7]=d4c01db2  D[7]=9821f65b

Step 15: (r= 7, s=28)
A[0]=ab3f1c63  B[0]=28e23baa  C[0]=86a1c764  D[0]=c87532bb
A[1]=dc4b3bd8  B[1]=88ee2d20  C[1]=b1d04df9  D[1]=6a08267f
A[2]=f949a413  B[2]=b17b5769  C[2]=41888f95  D[2]=d3f98a12
A[3]=f66cd9fb  B[3]=5e1b163e  C[3]=3a6ded49  D[3]=83d655f7
A[4]=40b9b438  B[4]=b45013ba  C[4]=5565216b  D[4]=a8a45362
A[5]=7a85d22b  B[5]=f8d399fb  C[5]=ba238960  D[5]=76a0070b
A[6]=d5e3ccb2  B[6]=6acb15a4  C[6]=16cb4915  D[6]=a85356ba
A[7]=5d12d6e9  B[7]=4a5b74c3  C[7]=ad34d04a  D[7]=d4c01db2

Step 16: (r=29, s= 9)
A[0]=ac946611  B[0]=7567e38c  C[0]=28e23baa  D[0]=86a1c764
A[1]=0b0f7f40  B[1]=1b89677b  C[1]=88ee2d20  D[1]=b1d04df9
A[2]=c7758285  B[2]=7f293482  C[2]=b17b5769  D[2]=41888f95
A[3]=2117bf8d  B[3]=7ecd9b3f  C[3]=5e1b163e  D[3]=3a6ded49
A[4]=1c05a15a  B[4]=08173687  C[4]=b45013ba  D[4]=5565216b
A[5]=ff49381d  B[5]=6f50ba45  C[5]=f8d399fb  D[5]=ba238960
A[6]=924b13d6  B[6]=5abc7996  C[6]=6acb15a4  D[6]=16cb4915
A[7]=0a8b3431  B[7]=2ba25add  C[7]=4a5b74c3  D[7]=ad34d04a

Step 17: (r= 9, s=15)
A[0]=d263a077  B[0]=28cc2359  C[0]=7567e38c  D[0]=28e23baa
A[1]=12451af2  B[1]=1efe8016  C[1]=1b89677b  D[1]=88ee2d20
A[2]=19050736  B[2]=eb050b8e  C[2]=7f293482  D[2]=b17b5769
A[3]=f62a288b  B[3]=2f7f1a42  C[3]=7ecd9b3f  D[3]=5e1b163e
A[4]=dd1a7655  B[4]=0b42b438  C[4]=08173687  D[4]=b45013ba
```

```
A[5]=1b201be5  B[5]=92703bfe  C[5]=6f50ba45  D[5]=f8d399fb
A[6]=bb76bd16  B[6]=9627ad24  C[6]=5abc7996  D[6]=6acb15a4
A[7]=f5231404  B[7]=16686215  C[7]=2ba25add  D[7]=4a5b74c3

Step 18: (r=15, s= 5)
A[0]=722b6261  B[0]=d03be931  C[0]=28cc2359  D[0]=7567e38c
A[1]=d73077fd  B[1]=8d790922  C[1]=1efe8016  D[1]=1b89677b
A[2]=6aff9055  B[2]=839b0c82  C[2]=eb050b8e  D[2]=7f293482
A[3]=854f8aab  B[3]=1445fb15  C[3]=2f7f1a42  D[3]=7ecd9b3f
A[4]=5ea37024  B[4]=3b2aee8d  C[4]=0b42b438  D[4]=08173687
A[5]=ff50e261  B[5]=0df28d90  C[5]=92703bfe  D[5]=6f50ba45
A[6]=63210751  B[6]=5e8b5dbb  C[6]=9627ad24  D[6]=5abc7996
A[7]=4d3ada33  B[7]=8a027a91  C[7]=16686215  D[7]=2ba25add

Step 19: (r= 5, s=29)
A[0]=40201c8b  B[0]=456c4c2e  C[0]=d03be931  D[0]=28cc2359
A[1]=fbefd125  B[1]=e60effba  C[1]=8d790922  D[1]=1efe8016
A[2]=718299b6  B[2]=5ff20aad  C[2]=839b0c82  D[2]=eb050b8e
A[3]=b889694b  B[3]=a9f15570  C[3]=1445fb15  D[3]=2f7f1a42
A[4]=34683f40  B[4]=d46e048b  C[4]=3b2aee8d  D[4]=0b42b438
A[5]=35579bdf  B[5]=ea1c4c3f  C[5]=0df28d90  D[5]=92703bfe
A[6]=a7d4d82c  B[6]=6420ea2c  C[6]=5e8b5dbb  D[6]=9627ad24
A[7]=2d5d141b  B[7]=a75b4669  C[7]=8a027a91  D[7]=16686215

Step 20: (r=29, s= 9)
A[0]=a952959b  B[0]=68040391  C[0]=456c4c2e  D[0]=d03be931
A[1]=86d30d16  B[1]=bf7dfa24  C[1]=e60effba  D[1]=8d790922
A[2]=46d2ecc6  B[2]=ce305336  C[2]=5ff20aad  D[2]=839b0c82
A[3]=bd3e2eb0  B[3]=77112d29  C[3]=a9f15570  D[3]=1445fb15
A[4]=ef61c56c  B[4]=068d07e8  C[4]=d46e048b  D[4]=3b2aee8d
A[5]=b5b509c7  B[5]=e6aaf37b  C[5]=ea1c4c3f  D[5]=0df28d90
A[6]=b3999b98  B[6]=94fa9b05  C[6]=6420ea2c  D[6]=5e8b5dbb
A[7]=af1e16e0  B[7]=65aba283  C[7]=a75b4669  D[7]=8a027a91

Step 21: (r= 9, s=15)
A[0]=7918ab4f  B[0]=a52b3752  C[0]=68040391  D[0]=456c4c2e
A[1]=1723a08d  B[1]=a61a2d0d  C[1]=bf7dfa24  D[1]=e60effba
A[2]=d072544f  B[2]=a5d98c8d  C[2]=ce305336  D[2]=5ff20aad
A[3]=62f17e62  B[3]=7c5d617a  C[3]=77112d29  D[3]=a9f15570
A[4]=85122182  B[4]=c38ad9de  C[4]=068d07e8  D[4]=d46e048b
A[5]=4b496a0d  B[5]=6a138f6b  C[5]=e6aaf37b  D[5]=ea1c4c3f
A[6]=22b99df2  B[6]=33373167  C[6]=94fa9b05  D[6]=6420ea2c
A[7]=21724e82  B[7]=3c2dc15e  C[7]=65aba283  D[7]=a75b4669

Step 22: (r=15, s= 5)
A[0]=30adf237  B[0]=55a7bc8c  C[0]=a52b3752  D[0]=68040391
A[1]=c8f59519  B[1]=d0468b91  C[1]=a61a2d0d  D[1]=bf7dfa24
A[2]=c0587a8e  B[2]=2a27e839  C[2]=a5d98c8d  D[2]=ce305336
A[3]=ee6353b0  B[3]=bf313178  C[3]=7c5d617a  D[3]=77112d29
```

```
A[4]=bb922447  B[4]=10c14289  C[4]=c38ad9de  D[4]=068d07e8
A[5]=17f399d6  B[5]=b506a5a4  C[5]=6a138f6b  D[5]=e6aaf37b
A[6]=12ac9439  B[6]=cef9115c  C[6]=33373167  D[6]=94fa9b05
A[7]=ba44969c  B[7]=274110b9  C[7]=3c2dc15e  D[7]=65aba283

Step 23: (r= 5, s=29)
A[0]=b677c0a1  B[0]=15be46e6  C[0]=55a7bc8c  D[0]=a52b3752
A[1]=22e12d0c  B[1]=1eb2a339  C[1]=d0468b91  D[1]=a61a2d0d
A[2]=9f7721bd  B[2]=0b0f51d8  C[2]=2a27e839  D[2]=a5d98c8d
A[3]=6a338983  B[3]=cc6a761d  C[3]=bf313178  D[3]=7c5d617a
A[4]=c90ebc82  B[4]=724488f7  C[4]=10c14289  D[4]=c38ad9de
A[5]=1ea3c0b0  B[5]=fe733ac2  C[5]=b506a5a4  D[5]=6a138f6b
A[6]=7b4979c0  B[6]=55928722  C[6]=cef9115c  D[6]=33373167
A[7]=1e6f022c  B[7]=4892d397  C[7]=274110b9  D[7]=3c2dc15e

Step 24: (r= 4, s=13)
A[0]=ccc033d1  B[0]=677c0a1b  C[0]=15be46e6  D[0]=55a7bc8c
A[1]=47f863c6  B[1]=2e12d0c2  C[1]=1eb2a339  D[1]=d0468b91
A[2]=d1c9c132  B[2]=f7721bd9  C[2]=0b0f51d8  D[2]=2a27e839
A[3]=977406d8  B[3]=a3389836  C[3]=cc6a761d  D[3]=bf313178
A[4]=fee70e65  B[4]=90ebc82c  C[4]=724488f7  D[4]=10c14289
A[5]=87cbd3de  B[5]=ea3c0b01  C[5]=fe733ac2  D[5]=b506a5a4
A[6]=6fddb950  B[6]=b4979c07  C[6]=55928722  D[6]=cef9115c
A[7]=12037abc  B[7]=e6f022c1  C[7]=4892d397  D[7]=274110b9

Step 25: (r=13, s=10)
A[0]=d937eedd  B[0]=067a3998  C[0]=677c0a1b  D[0]=15be46e6
A[1]=bb59f4ca  B[1]=0c78c8ff  C[1]=2e12d0c2  D[1]=1eb2a339
A[2]=a4b6c26f  B[2]=38265a39  C[2]=f7721bd9  D[2]=0b0f51d8
A[3]=dd1ea29f  B[3]=80db12ee  C[3]=a3389836  D[3]=cc6a761d
A[4]=e32659ed  B[4]=e1ccbfdc  C[4]=90ebc82c  D[4]=724488f7
A[5]=96e3b0be  B[5]=7a7bd0f9  C[5]=ea3c0b01  D[5]=fe733ac2
A[6]=e2a8c5d5  B[6]=b72a0dfb  C[6]=b4979c07  D[6]=55928722
A[7]=67eedc99  B[7]=6f578240  C[7]=e6f022c1  D[7]=4892d397

Step 26: (r=10, s=25)
A[0]=a41a2b16  B[0]=dfbb7764  C[0]=067a3998  D[0]=677c0a1b
A[1]=eeb599fe  B[1]=67d32aed  C[1]=0c78c8ff  D[1]=2e12d0c2
A[2]=e089f5b4  B[2]=db09be92  C[2]=38265a39  D[2]=f7721bd9
A[3]=5f0f10ab  B[3]=7a8a7f74  C[3]=80db12ee  D[3]=a3389836
A[4]=b1045efc  B[4]=9967b78c  C[4]=e1ccbfdc  D[4]=90ebc82c
A[5]=ebcff55f  B[5]=8ec2fa5b  C[5]=7a7bd0f9  D[5]=ea3c0b01
A[6]=9e50be99  B[6]=a317578a  C[6]=b72a0dfb  D[6]=b4979c07
A[7]=b6105f22  B[7]=bb72659f  C[7]=6f578240  D[7]=e6f022c1

Step 27: (r=25, s= 4)
A[0]=878b765c  B[0]=2d483456  C[0]=dfbb7764  D[0]=067a3998
A[1]=6c1e1f44  B[1]=fddd6b33  C[1]=67d32aed  D[1]=0c78c8ff
A[2]=b070077a  B[2]=69c113eb  C[2]=db09be92  D[2]=38265a39
```

```
A[3]=c91fcb34  B[3]=56be1e21  C[3]=7a8a7f74  D[3]=80db12ee
A[4]=a7c522cd  B[4]=f96208bd  C[4]=9967b78c  D[4]=e1ccbfdc
A[5]=dea74078  B[5]=bfd79fea  C[5]=8ec2fa5b  D[5]=7a7bd0f9
A[6]=d0ba0c8a  B[6]=333ca17d  C[6]=a317578a  D[6]=b72a0dfb
A[7]=bba19fe0  B[7]=456c20be  C[7]=bb72659f  D[7]=6f578240

Step 28: (r= 4, s=13)
A[0]=1647b522  B[0]=78b765c8  C[0]=2d483456  D[0]=dfbb7764
A[1]=e0b55825  B[1]=c1e1f446  C[1]=fddd6b33  D[1]=67d32aed
A[2]=050a6135  B[2]=070077ab  C[2]=69c113eb  D[2]=db09be92
A[3]=550a7fd8  B[3]=91fcb34c  C[3]=56be1e21  D[3]=7a8a7f74
A[4]=d4bf9978  B[4]=7c522cda  C[4]=f96208bd  D[4]=9967b78c
A[5]=b9f19455  B[5]=ea74078d  C[5]=bfd79fea  D[5]=8ec2fa5b
A[6]=aea9687f  B[6]=0ba0c8ad  C[6]=333ca17d  D[6]=a317578a
A[7]=023858ef  B[7]=ba19fe0b  C[7]=456c20be  D[7]=bb72659f

Step 29: (r=13, s=10)
A[0]=334a6ca6  B[0]=f6a442c8  C[0]=78b765c8  D[0]=2d483456
A[1]=e741f166  B[1]=ab04bc16  C[1]=c1e1f446  D[1]=fddd6b33
A[2]=7acd892a  B[2]=4c26a0a1  C[2]=070077ab  D[2]=69c113eb
A[3]=d213a381  B[3]=4ffb0aa1  C[3]=91fcb34c  D[3]=56be1e21
A[4]=66b7d552  B[4]=f32f1a97  C[4]=7c522cda  D[4]=f96208bd
A[5]=d7d07fcf  B[5]=328ab73e  C[5]=ea74078d  D[5]=bfd79fea
A[6]=cebb60d4  B[6]=2d0ff5d5  C[6]=0ba0c8ad  D[6]=333ca17d
A[7]=bd8665ed  B[7]=0b1de047  C[7]=ba19fe0b  D[7]=456c20be

Step 30: (r=10, s=25)
A[0]=3ac62ab0  B[0]=29b298cd  C[0]=f6a442c8  D[0]=78b765c8
A[1]=5e6d66b2  B[1]=07c59b9d  C[1]=ab04bc16  D[1]=c1e1f446
A[2]=4db7686b  B[2]=3624a9eb  C[2]=4c26a0a1  D[2]=070077ab
A[3]=789e1f65  B[3]=4e8e0748  C[3]=4ffb0aa1  D[3]=91fcb34c
A[4]=15d0e70b  B[4]=df55499a  C[4]=f32f1a97  D[4]=7c522cda
A[5]=d3027d67  B[5]=41ff3f5f  C[5]=328ab73e  D[5]=ea74078d
A[6]=1707f466  B[6]=ed83533a  C[6]=2d0ff5d5  D[6]=0ba0c8ad
A[7]=9fec4e45  B[7]=1997b6f6  C[7]=0b1de047  D[7]=ba19fe0b

Step 31: (r=25, s= 4)
A[0]=2ed1ba97  B[0]=60758c55  C[0]=29b298cd  D[0]=f6a442c8
A[1]=f6e5d0b4  B[1]=64bcdacd  C[1]=07c59b9d  D[1]=ab04bc16
A[2]=0710b636  B[2]=d69b6ed0  C[2]=3624a9eb  D[2]=4c26a0a1
A[3]=a215c115  B[3]=caf13c3e  C[3]=4e8e0748  D[3]=4ffb0aa1
A[4]=e08b8703  B[4]=162ba1ce  C[4]=df55499a  D[4]=f32f1a97
A[5]=a4802ba5  B[5]=cfa604fa  C[5]=41ff3f5f  D[5]=328ab73e
A[6]=d5af0f18  B[6]=cc2e0fe8  C[6]=ed83533a  D[6]=2d0ff5d5
A[7]=c1773a85  B[7]=8b3fd89c  C[7]=1997b6f6  D[7]=0b1de047

Feed-Forward Step 32: (r= 4, s=13)
A[0]=56fa37e9  B[0]=ed1ba972  C[0]=60758c55  D[0]=29b298cd
A[1]=24867e5a  B[1]=6e5d0b4f  C[1]=64bcdacd  D[1]=07c59b9d
```

```
A[2]=169c319a  B[2]=710b6360  C[2]=d69b6ed0  D[2]=3624a9eb
A[3]=4117bcc7  B[3]=215c115a  C[3]=caf13c3e  D[3]=4e8e0748
A[4]=4309b40d  B[4]=08b8703e  C[4]=162ba1ce  D[4]=df55499a
A[5]=b2d265cb  B[5]=4802ba5a  C[5]=cfa604fa  D[5]=41ff3f5f
A[6]=764c8494  B[6]=5af0f18d  C[6]=cc2e0fe8  D[6]=ed83533a
A[7]=cbe289f9  B[7]=1773a85c  C[7]=8b3fd89c  D[7]=1997b6f6

Feed-Forward Step 33: (r=13, s=10)
A[0]=52aebd44  B[0]=46fd2adf  C[0]=ed1ba972  D[0]=60758c55
A[1]=dadf7b2c  B[1]=cfcb4490  C[1]=6e5d0b4f  D[1]=64bcdacd
A[2]=16973312  B[2]=863342d3  C[2]=710b6360  D[2]=d69b6ed0
A[3]=69656b6c  B[3]=f798e822  C[3]=215c115a  D[3]=caf13c3e
A[4]=4b8db30d  B[4]=3681a861  C[4]=08b8703e  D[4]=162ba1ce
A[5]=9b19cabd  B[5]=4cb9765a  C[5]=4802ba5a  D[5]=cfa604fa
A[6]=1756f3bf  B[6]=90928ec9  C[6]=5af0f18d  D[6]=cc2e0fe8
A[7]=1c743dda  B[7]=513f397c  C[7]=1773a85c  D[7]=8b3fd89c

Feed-Forward Step 34: (r=10, s=25)
A[0]=3a56121c  B[0]=baf5114a  C[0]=46fd2adf  D[0]=ed1ba972
A[1]=41f408ac  B[1]=7decb36b  C[1]=cfcb4490  D[1]=6e5d0b4f
A[2]=04b4ee25  B[2]=5ccc485a  C[2]=863342d3  D[2]=710b6360
A[3]=81a26a35  B[3]=95adb1a5  C[3]=f798e822  D[3]=215c115a
A[4]=387bddc7  B[4]=36cc352e  C[4]=3681a861  D[4]=08b8703e
A[5]=f55eec78  B[5]=672af66c  C[5]=4cb9765a  D[5]=4802ba5a
A[6]=c3f6f40e  B[6]=5bcefc5d  C[6]=90928ec9  D[6]=5af0f18d
A[7]=613cfd8c  B[7]=d0f76871  C[7]=513f397c  D[7]=1773a85c

Feed-Forward Step 35: (r=25, s= 4)
A[0]=9afa60c0  B[0]=3874ac24  C[0]=baf5114a  D[0]=46fd2adf
A[1]=711424ae  B[1]=5883e811  C[1]=7decb36b  D[1]=cfcb4490
A[2]=c5273a5a  B[2]=4a0969dc  C[2]=5ccc485a  D[2]=863342d3
A[3]=d4db22df  B[3]=6b0344d4  C[3]=95adb1a5  D[3]=f798e822
A[4]=d0e36914  B[4]=8e70f7bb  C[4]=36cc352e  D[4]=3681a861
A[5]=93b05690  B[5]=f1eabdd8  C[5]=672af66c  D[5]=4cb9765a
A[6]=6b0f1f86  B[6]=1d87ede8  C[6]=5bcefc5d  D[6]=90928ec9
A[7]=1a31dc9b  B[7]=18c279fb  C[7]=d0f76871  D[7]=513f397c
```

Compression Function Output

```
A[0]=9afa60c0  B[0]=3874ac24  C[0]=baf5114a  D[0]=46fd2adf
A[1]=711424ae  B[1]=5883e811  C[1]=7decb36b  D[1]=cfcb4490
A[2]=c5273a5a  B[2]=4a0969dc  C[2]=5ccc485a  D[2]=863342d3
A[3]=d4db22df  B[3]=6b0344d4  C[3]=95adb1a5  D[3]=f798e822
A[4]=d0e36914  B[4]=8e70f7bb  C[4]=36cc352e  D[4]=3681a861
A[5]=93b05690  B[5]=f1eabdd8  C[5]=672af66c  D[5]=4cb9765a
A[6]=6b0f1f86  B[6]=1d87ede8  C[6]=5bcefc5d  D[6]=90928ec9
A[7]=1a31dc9b  B[7]=18c279fb  C[7]=d0f76871  D[7]=513f397c
```

Hash Function Output

```
c060fa9aae2414715a3a27c5df22dbd41469e3d09056b093861f0f6b9bdc311a24ac743811e88358dc69094ad444036bb
```