Cryptographic Hash Function EDON-R

Presented by
Prof. Danilo Gligoroski

Department of Telematics
Faculty of Information Technology, Mathematics and Electrical Engineering
Norwegian University of Science and TechnologyTechnology - NTNU,
NORWAY

NTNU
Innovation and Creativity

Outline

- Short history of EDON-R
- Specific design characteristics
- Known attacks on EDON-R
- Are there any one-way bijections embedded in EDON-R?
- SW/HW performance and memory requirements

NTNU
Innovation and Creativity

Short history of EDON-R

- Theoretical principles of EDON-R were described at the Second NIST Hash Workshop – 2006 in the presentation: **Edon-R Family of Cryptographic Hash Functions**
  - No concrete realization

Short history of EDON-R

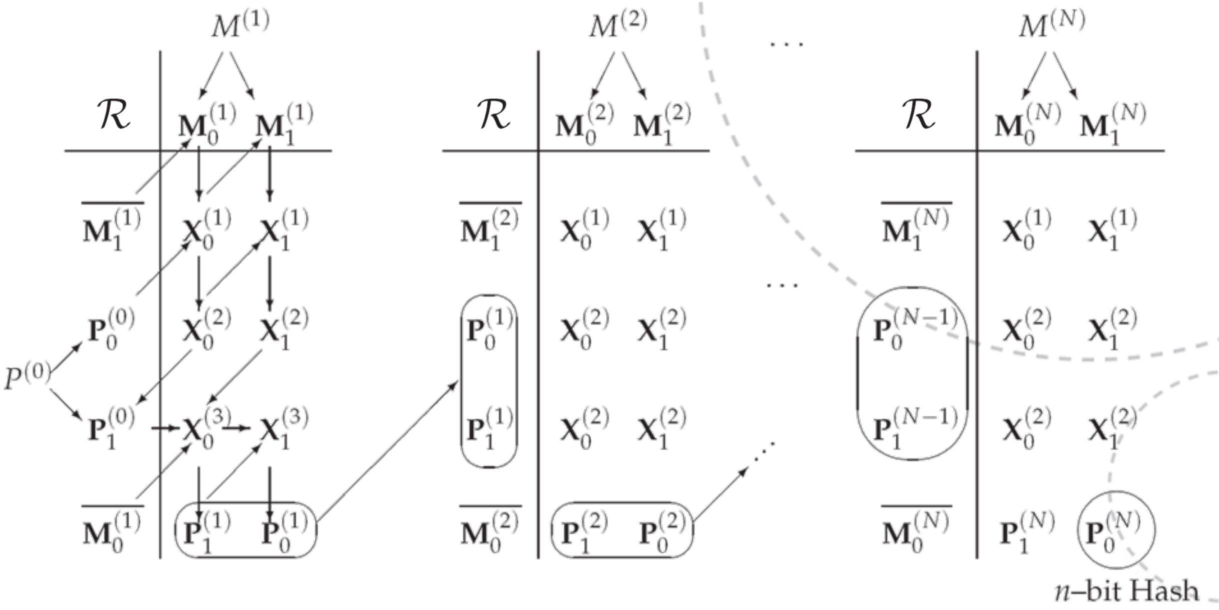
- Theoretical principles of EDON-R were described at the Second NIST Hash Workshop – 2006 in the presentation: **Edon-R Family of Cryptographic Hash Functions**
  - No concrete realization
- First implementation of Edon-*R*(256, 384, 512) published at **http://eprint.iacr.org/2007/154**
  - **Big acknowledgement** for Søren Steffen Thomsen, giving me comments about zero being a fixed point in that realization

Short history of EDON-R

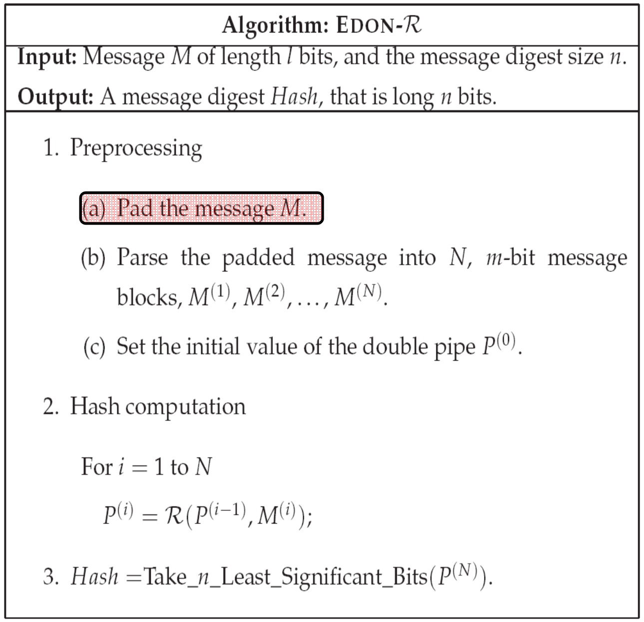
- Additionally, the following contributors joined the EDON-R (SHA-3) team:
  - **Rune Steinsmo Ødegård** – Investigating the mathematical properties of defined quasigroups
  - **Marija Mihova** – Investigating the differential properties in EDON-R operations
  - **Svein Johan Knapskog** (general comments and suggestions for improvements, proofreading)
  - **Ljupco Kocarev** (general comments and suggestions for improvements, proofreading)
  - **Aleš Drápal** (Theory of quasigroups and suggestions for improvements)
  - **Vlastimil Klima** (cryptanalysis and suggestions for improvements)

Specific design characteristics for EDON-R

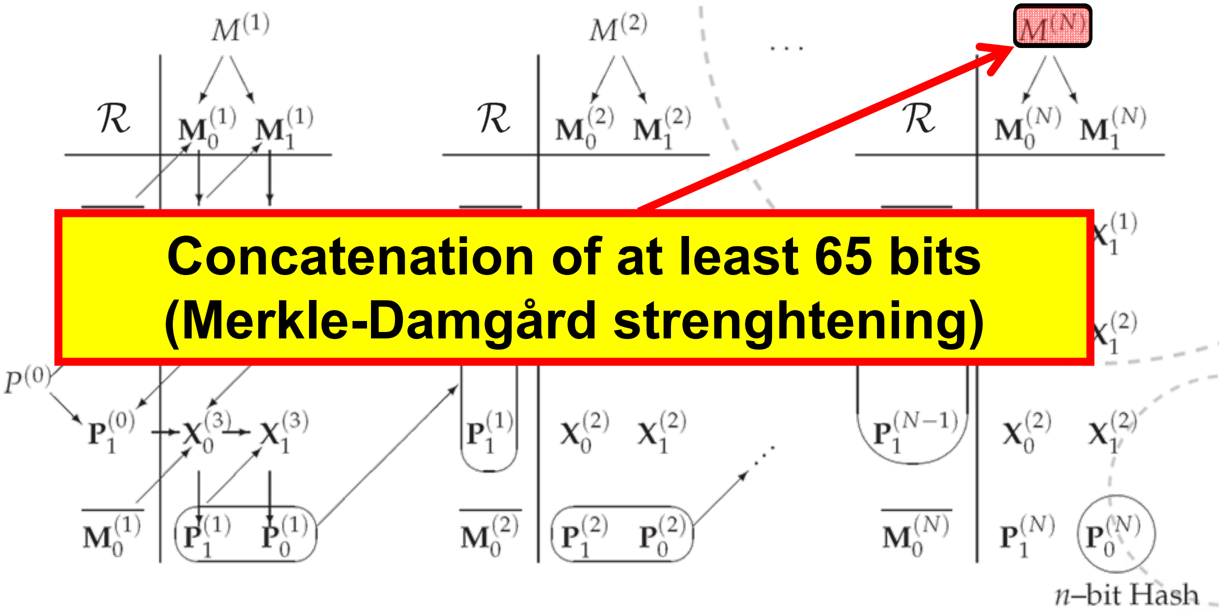
```
Algorithm: EDON-$\mathcal{R}$
Input: Message $M$ of length $l$ bits, and the message digest size $n$.
Output: A message digest $Hash$, that is long $n$ bits.

1. Preprocessing
    (a) Pad the message $M$.
    (b) Parse the padded message into $N$, $m$-bit message blocks, $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$.
    (c) Set the initial value of the double pipe $P^{(0)}$.
2. Hash computation
    For $i = 1$ to $N$
        $P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)})$;
3. $Hash$ = Take_$n$_Least_Significant_Bits$(P^{(N)})$.
```



Specific design characteristics for EDON-R

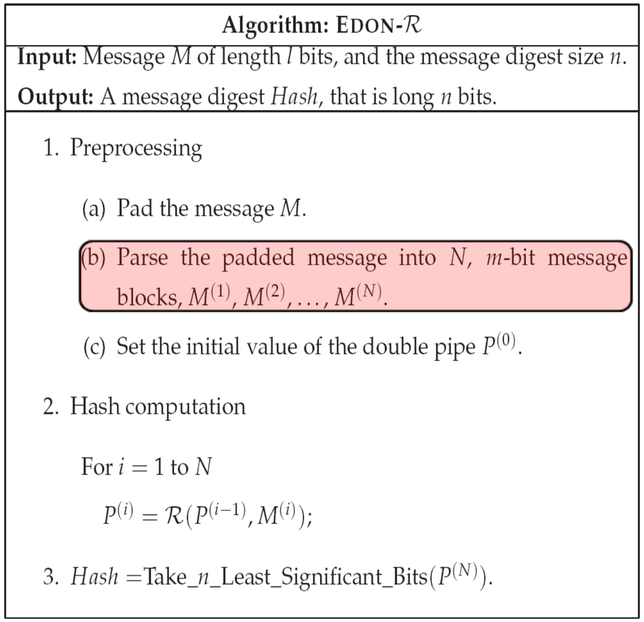


```
Algorithm: EDON-$\mathcal{R}$
Input: Message $M$ of length $l$ bits, and the message digest size $n$.
Output: A message digest $Hash$, that is long $n$ bits.
1. Preprocessing
    (a) Pad the message $M$.
    (b) Parse the padded message into $N$, $m$-bit message blocks, $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$.
    (c) Set the initial value of the double pipe $P^{(0)}$.
2. Hash computation
    For $i = 1$ to $N$
        $P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)})$;
3. $Hash$ =Take_$n$_Least_Significant_Bits($P^{(N)}$).
```



Concatenation of at least 65 bits (Merkle-Damgård strenghtening)

Specific design characteristics for EDON-R

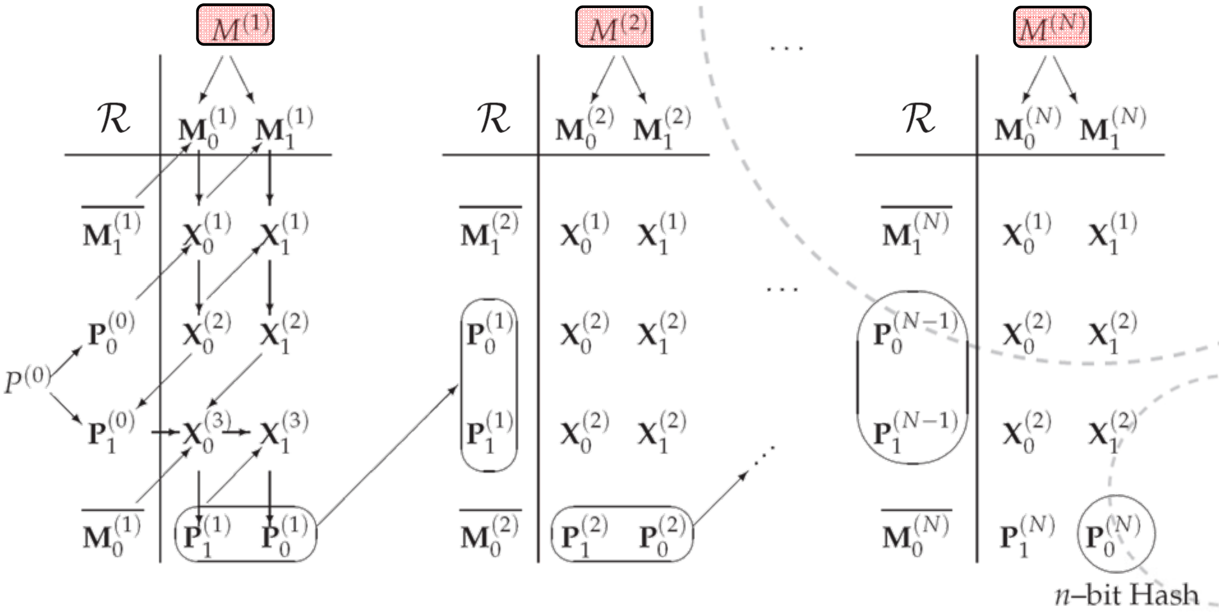


Algorithm: EDON-$\mathcal{R}$

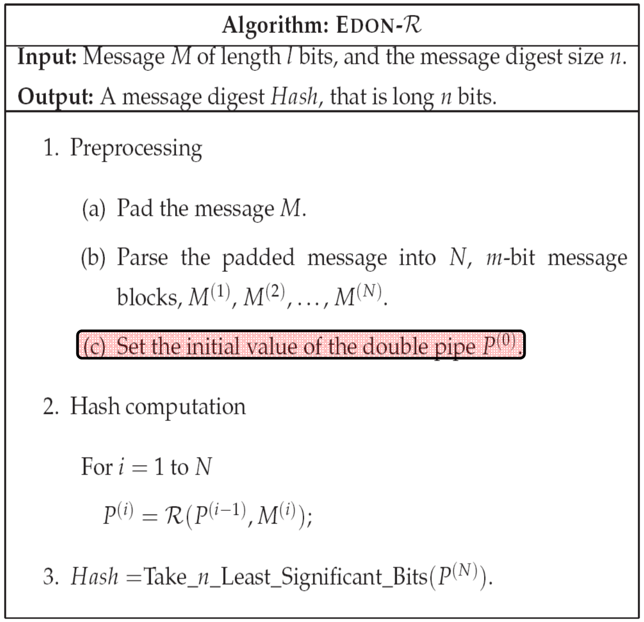
Input: Message M of length l bits, and the message digest size n.

Output: A message digest $Hash$, that is long n bits.

```
1. Preprocessing
    (a) Pad the message $M$.
    (b) Parse the padded message into $N$, $m$-bit message blocks, $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$.
    (c) Set the initial value of the double pipe $P^{(0)}$.
2. Hash computation
    For $i = 1$ to $N$
        $P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)})$;
3. $Hash$ =Take_$n$_Least_Significant_Bits($P^{(N)}$).
```



Specific design characteristics for EDON-R

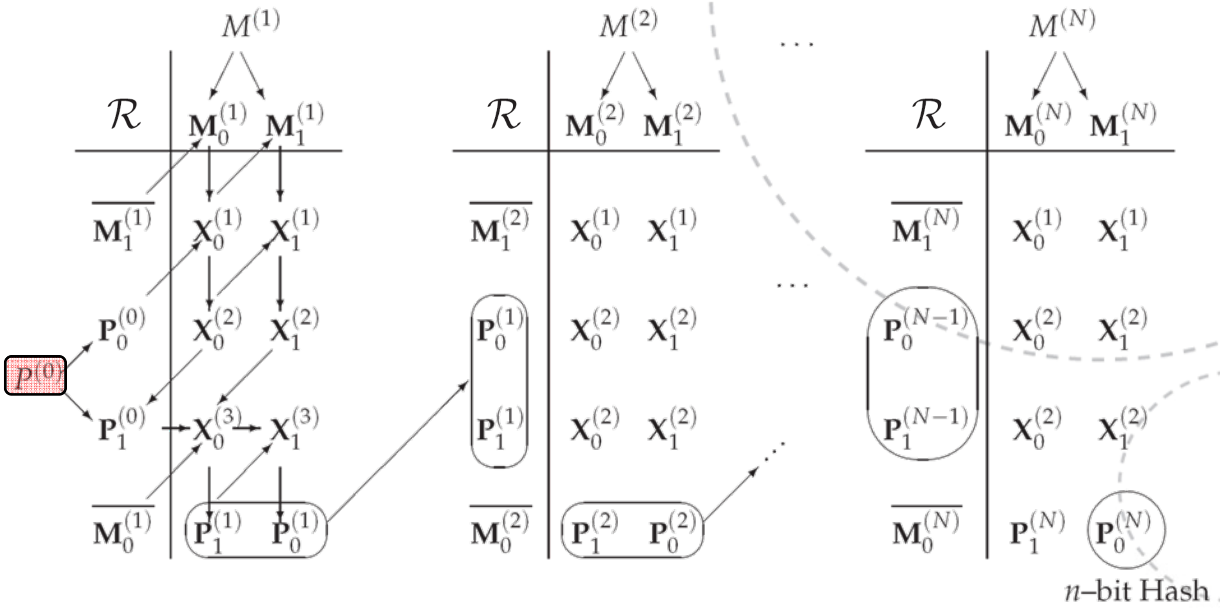


Algorithm: EDON-$\mathcal{R}$

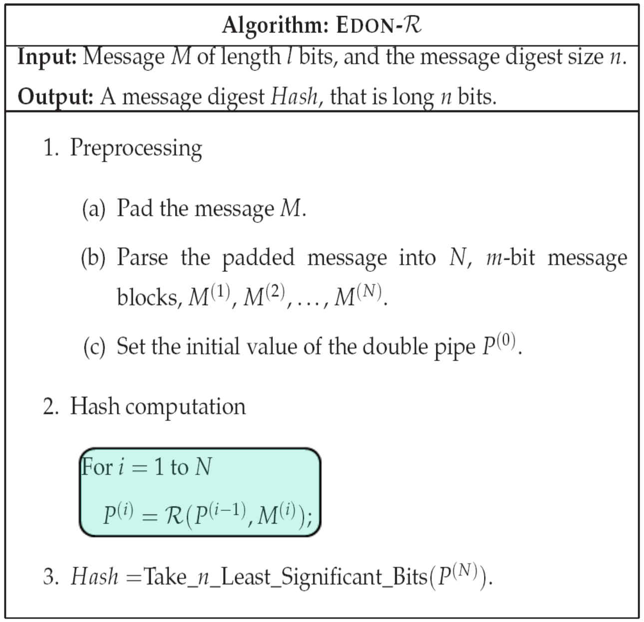
Input: Message M of length l bits, and the message digest size n.

Output: A message digest $Hash$, that is long n bits.

```
1. Preprocessing
    (a) Pad the message $M$.
    (b) Parse the padded message into $N$, $m$-bit message blocks, $M^{(1)}, M^{(2)}, \dots, M^{(N)}$.
    (c) Set the initial value of the double pipe $P^{(0)}$.
2. Hash computation
    For $i = 1$ to $N$
        $P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)})$;
3. $Hash$ =Take_n_Least_Significant_Bits($P^{(N)}$).
```



Specific design characteristics for EDON-R



Algorithm: EDON-$\mathcal{R}$

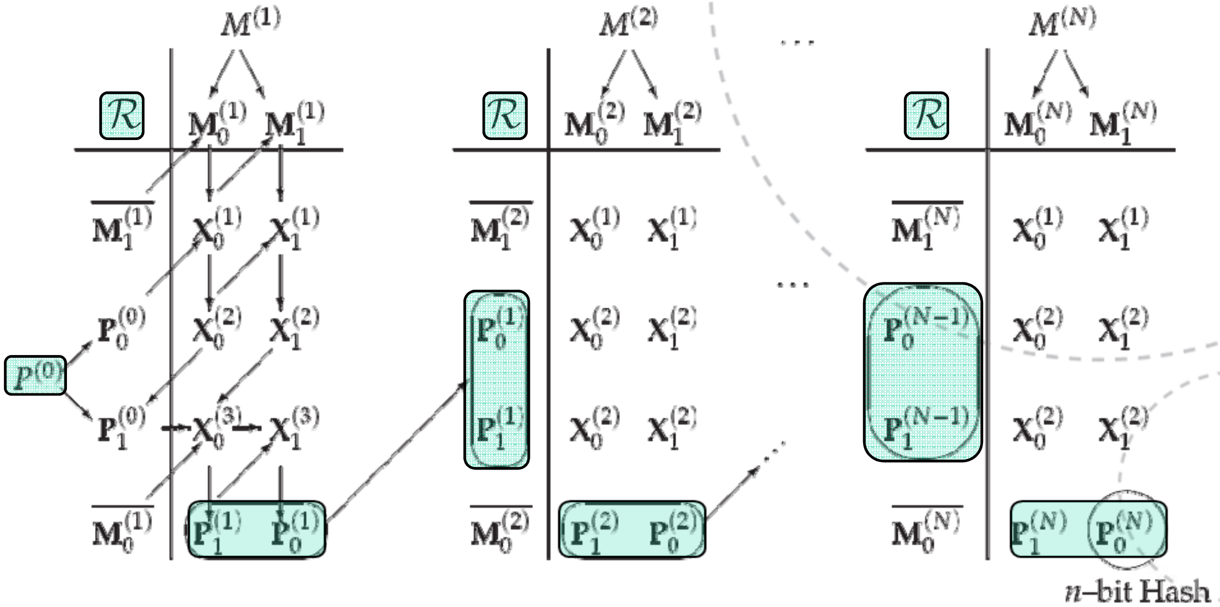
Input: Message M of length l bits, and the message digest size n.

Output: A message digest $Hash$, that is long n bits.

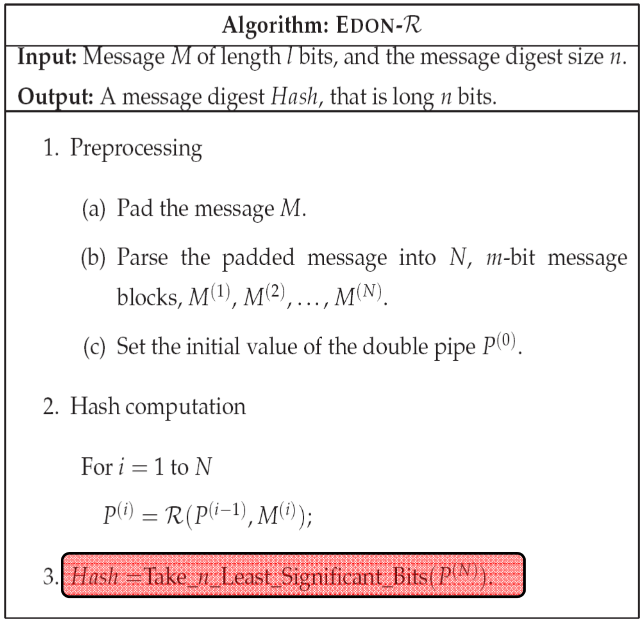
1. Preprocessing
   - (a) Pad the message M.
   - (b) Parse the padded message into N, m-bit message blocks, $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$.
   - (c) Set the initial value of the double pipe $P^{(0)}$.
2. Hash computation

```
For $i = 1$ to $N$
    $P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)})$;
```

3. $Hash$ =Take_n_Least_Significant_Bits$(P^{(N)})$.



Specific design characteristics for EDON-R

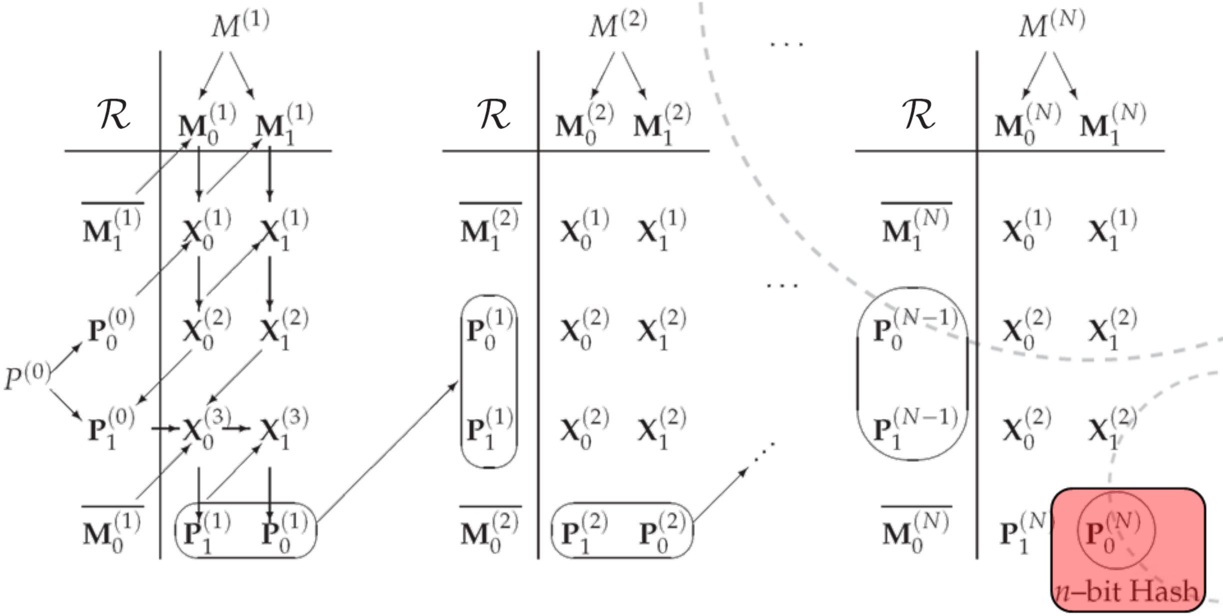


Algorithm: EDON-$\mathcal{R}$

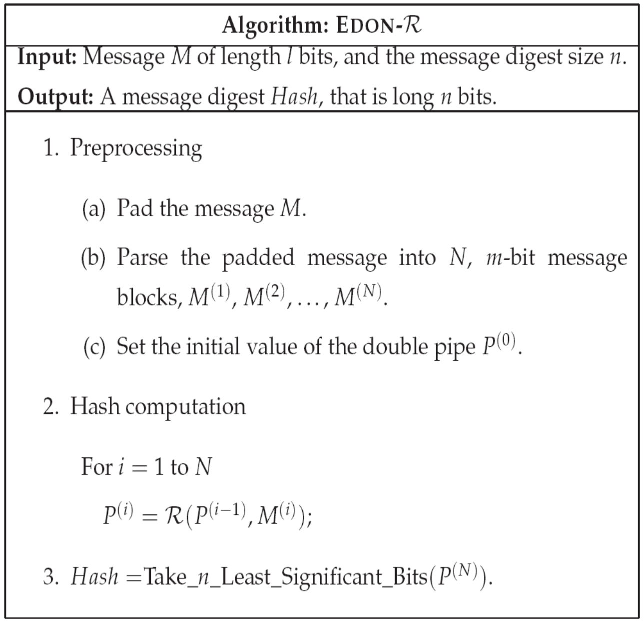
Input: Message M of length l bits, and the message digest size n.

Output: A message digest $Hash$, that is long n bits.

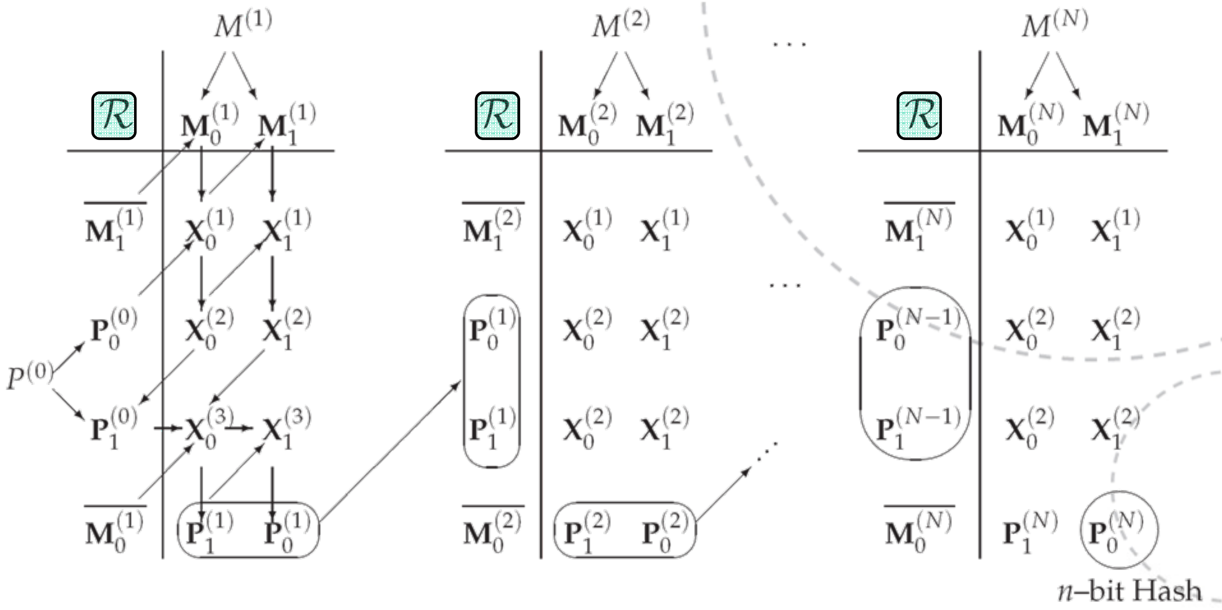
```
1. Preprocessing
    (a) Pad the message $M$.
    (b) Parse the padded message into $N$, $m$-bit message blocks, $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$.
    (c) Set the initial value of the double pipe $P^{(0)}$.
2. Hash computation
    For $i = 1$ to $N$
        $P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)})$;
3. $Hash$ = Take_$n$_Least_Significant_Bits($P^{(N)}$).
```



Specific design characteristics for EDON-R



```
Algorithm: EDON-$\mathcal{R}$
Input: Message $M$ of length $l$ bits, and the message digest size $n$.
Output: A message digest $Hash$, that is long $n$ bits.
1. Preprocessing
    (a) Pad the message $M$.
    (b) Parse the padded message into $N$, $m$-bit message blocks, $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$.
    (c) Set the initial value of the double pipe $P^{(0)}$.
2. Hash computation
    For $i = 1$ to $N$
        $P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)})$;
3. $Hash =$ Take_$n$_Least_Significant_Bits$(P^{(N)})$.
```



Function $\mathcal{R}(\mathbf{C}_0, \mathbf{C}_1, \mathbf{A}_0, \mathbf{A}_1)$ is defined by quasigroup operations

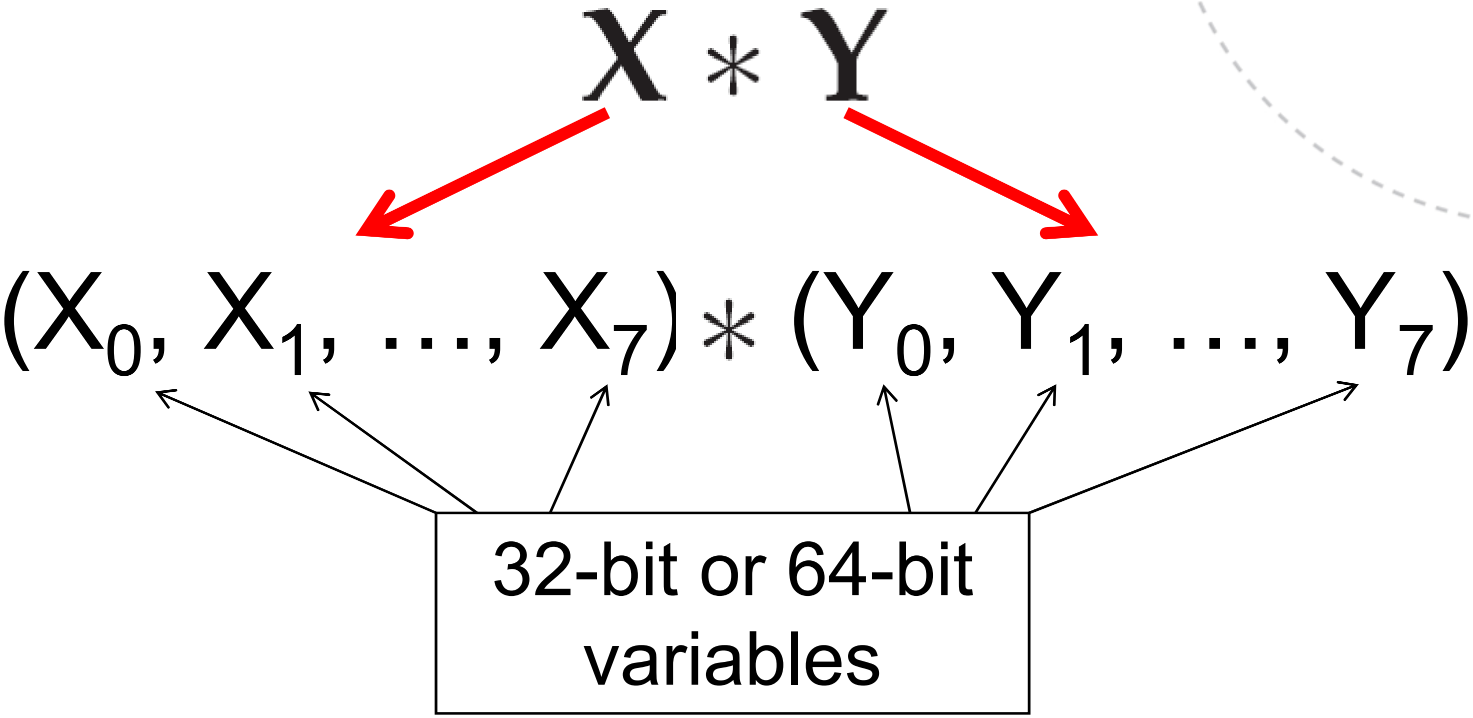
Specific design characteristics for EDON-R

Quasigroup operations are defined on 256-bit or 512-bit operands.

$$\mathbf{X} * \mathbf{Y}$$

Specific design characteristics for EDON-R

Quasigroup operations are defined on 256-bit or 512-bit operands.



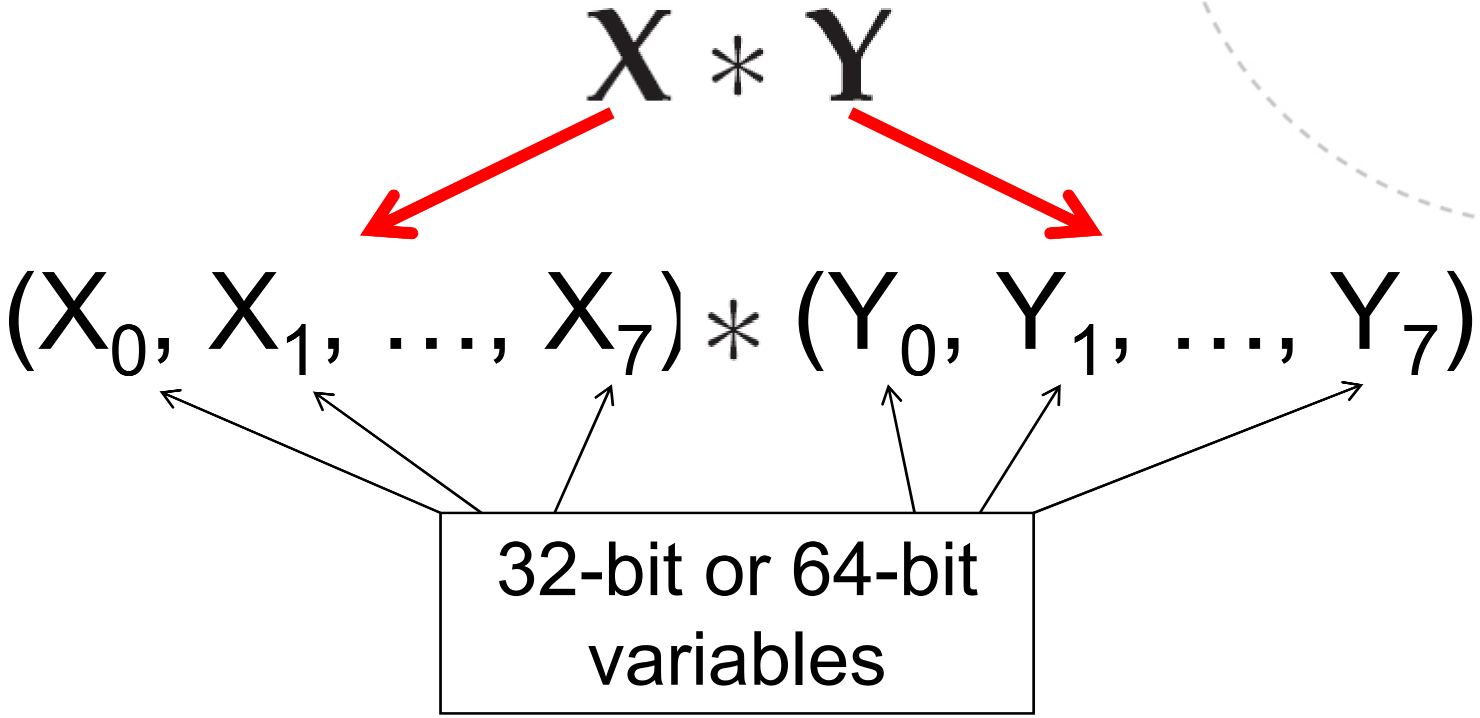
$$\mathbf{X} * \mathbf{Y}$$

$$(X_0, X_1, \ldots, X_7) * (Y_0, Y_1, \ldots, Y_7)$$

32-bit or 64-bit variables

Specific design characteristics for EDON-R

Quasigroup operations are defined on 256-bit or 512-bit operands.



$$\mathbf{X} * \mathbf{Y}$$

$$(X_0, X_1, \ldots, X_7) * (Y_0, Y_1, \ldots, Y_7)$$

32-bit or 64-bit variables

Operations:

1. **Additions modulo 2^{32} or modulo 2^{64}**
2. **Left rotations of 32-bit or 64-bit words**
3. **Bitwise XOR operations of 32-bit or 64-bit words**

Specific design characteristics for EDON-R

Quasigroup operation of order 2^{256}

Input: $\mathbf{X} = (X_0, X_1, \ldots, X_7)$ and $\mathbf{Y} = (Y_0, Y_1, \ldots, Y_7)$ where X_i and Y_i are 32–bit variables.

Output: $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_7)$ where Z_i are 32–bit variables.

Temporary 32–bit variables: $T_0, \ldots, T_{15}$.

1.
$$\begin{array}{lll}
T_0 & \leftarrow & ROTL^0(\texttt{0xAAAAAAAA} + X_0 + X_1 + X_2 + X_4 + X_7);\\
T_1 & \leftarrow & ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7);\\
T_2 & \leftarrow & ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7);\\
T_3 & \leftarrow & ROTL^{13}(X_2 + X_3 + X_5 + X_6 + X_7);\\
T_4 & \leftarrow & ROTL^{17}(X_1 + X_2 + X_3 + X_5 + X_6);\\
T_5 & \leftarrow & ROTL^{22}(X_0 + X_2 + X_3 + X_4 + X_5);\\
T_6 & \leftarrow & ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7);\\
T_7 & \leftarrow & ROTL^{29}(X_2 + X_3 + X_4 + X_5 + X_6);
\end{array}$$

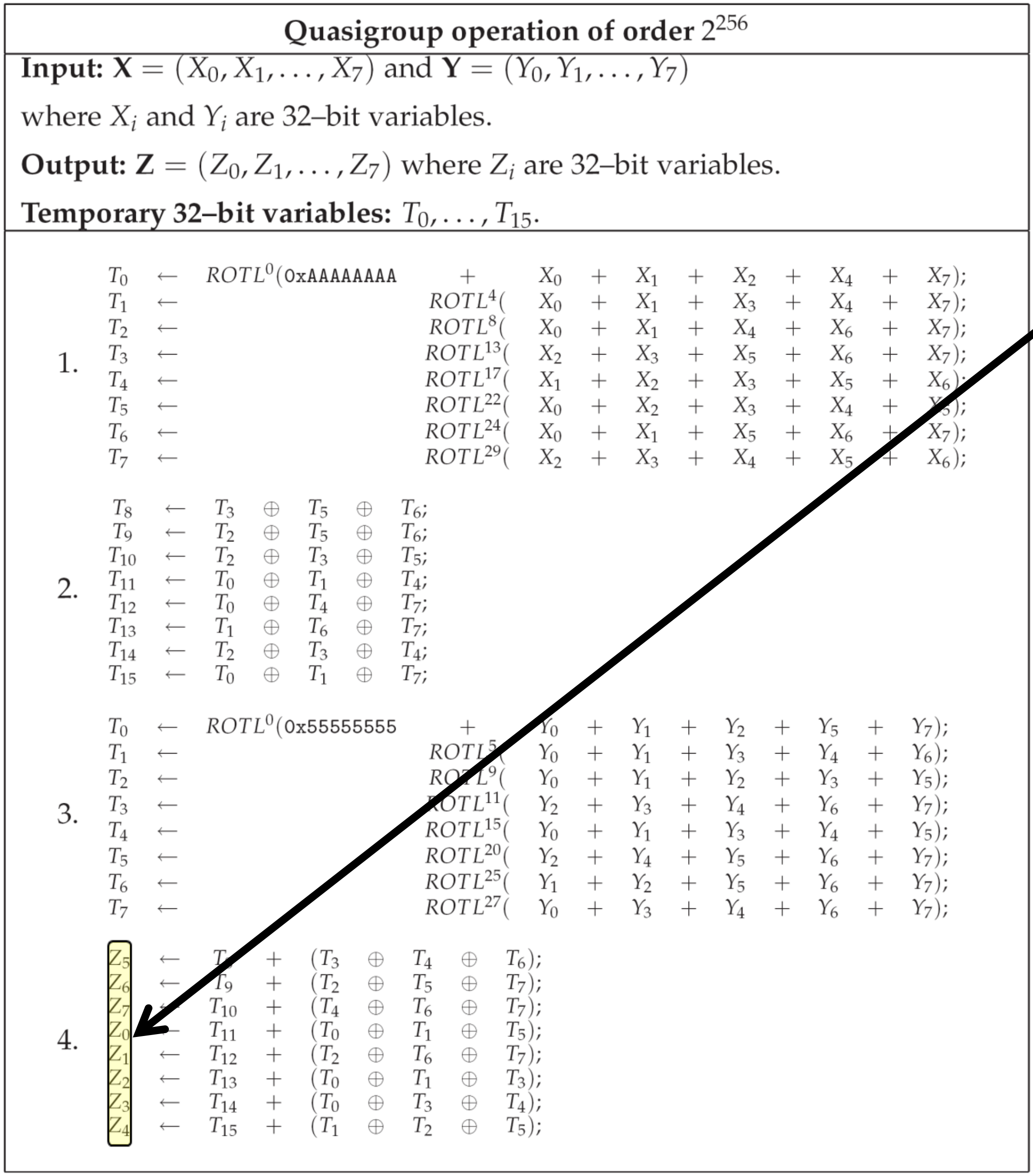
2.
$$\begin{array}{lll}
T_8 & \leftarrow & T_3 \oplus T_5 \oplus T_6;\\
T_9 & \leftarrow & T_2 \oplus T_5 \oplus T_6;\\
T_{10} & \leftarrow & T_2 \oplus T_3 \oplus T_5;\\
T_{11} & \leftarrow & T_0 \oplus T_1 \oplus T_4;\\
T_{12} & \leftarrow & T_0 \oplus T_4 \oplus T_7;\\
T_{13} & \leftarrow & T_1 \oplus T_6 \oplus T_7;\\
T_{14} & \leftarrow & T_2 \oplus T_3 \oplus T_4;\\
T_{15} & \leftarrow & T_0 \oplus T_1 \oplus T_7;
\end{array}$$

3.
$$\begin{array}{lll}
T_0 & \leftarrow & ROTL^0(\texttt{0x55555555} + Y_0 + Y_1 + Y_2 + Y_5 + Y_7);\\
T_1 & \leftarrow & ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6);\\
T_2 & \leftarrow & ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5);\\
T_3 & \leftarrow & ROTL^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7);\\
T_4 & \leftarrow & ROTL^{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_5);\\
T_5 & \leftarrow & ROTL^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);\\
T_6 & \leftarrow & ROTL^{25}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7);\\
T_7 & \leftarrow & ROTL^{27}(Y_0 + Y_3 + Y_4 + Y_6 + Y_7);
\end{array}$$

4.
$$\begin{array}{lll}
Z_5 & \leftarrow & T_8 + (T_3 \oplus T_4 \oplus T_6);\\
Z_6 & \leftarrow & T_9 + (T_2 \oplus T_5 \oplus T_7);\\
Z_7 & \leftarrow & T_{10} + (T_4 \oplus T_6 \oplus T_7);\\
Z_0 & \leftarrow & T_{11} + (T_0 \oplus T_1 \oplus T_5);\\
Z_1 & \leftarrow & T_{12} + (T_2 \oplus T_6 \oplus T_7);\\
Z_2 & \leftarrow & T_{13} + (T_0 \oplus T_1 \oplus T_3);\\
Z_3 & \leftarrow & T_{14} + (T_0 \oplus T_3 \oplus T_4);\\
Z_4 & \leftarrow & T_{15} + (T_1 \oplus T_2 \oplus T_5);
\end{array}$$

$$\mathbf{X} * \mathbf{Y} \equiv \pi_1(\pi_2(\mathbf{X}) +_8 \pi_3(\mathbf{Y}))$$

Specific design characteristics for EDON-R



Quasigroup operation of order 2^{256}

Input: $\mathbf{X} = (X_0, X_1, \ldots, X_7)$ and $\mathbf{Y} = (Y_0, Y_1, \ldots, Y_7)$ where X_i and Y_i are 32–bit variables.

Output: $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_7)$ where Z_i are 32–bit variables.

Temporary 32–bit variables: $T_0, \ldots, T_{15}$.

```
1.  $T_0 \leftarrow ROTL^0(\texttt{0xAAAAAAAA} + X_0 + X_1 + X_2 + X_4 + X_7);$
    $T_1 \leftarrow ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7);$
    $T_2 \leftarrow ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7);$
    $T_3 \leftarrow ROTL^{13}(X_2 + X_3 + X_5 + X_6 + X_7);$
    $T_4 \leftarrow ROTL^{17}(X_1 + X_2 + X_3 + X_5 + X_6);$
    $T_5 \leftarrow ROTL^{22}(X_0 + X_2 + X_3 + X_4 + X_5);$
    $T_6 \leftarrow ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7);$
    $T_7 \leftarrow ROTL^{29}(X_2 + X_3 + X_4 + X_5 + X_6);$

2.  $T_8 \leftarrow T_3 \oplus T_5 \oplus T_6;$
    $T_9 \leftarrow T_2 \oplus T_5 \oplus T_6;$
    $T_{10} \leftarrow T_2 \oplus T_3 \oplus T_5;$
    $T_{11} \leftarrow T_0 \oplus T_1 \oplus T_4;$
    $T_{12} \leftarrow T_0 \oplus T_4 \oplus T_7;$
    $T_{13} \leftarrow T_1 \oplus T_6 \oplus T_7;$
    $T_{14} \leftarrow T_2 \oplus T_3 \oplus T_4;$
    $T_{15} \leftarrow T_0 \oplus T_1 \oplus T_7;$

3.  $T_0 \leftarrow ROTL^0(\texttt{0x55555555} + Y_0 + Y_1 + Y_2 + Y_5 + Y_7);$
    $T_1 \leftarrow ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6);$
    $T_2 \leftarrow ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5);$
    $T_3 \leftarrow ROTL^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7);$
    $T_4 \leftarrow ROTL^{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_5);$
    $T_5 \leftarrow ROTL^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);$
    $T_6 \leftarrow ROTL^{25}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7);$
    $T_7 \leftarrow ROTL^{27}(Y_0 + Y_3 + Y_4 + Y_6 + Y_7);$

4.  $Z_5 \leftarrow T_8 + (T_3 \oplus T_4 \oplus T_6);$
    $Z_6 \leftarrow T_9 + (T_2 \oplus T_5 \oplus T_7);$
    $Z_7 \leftarrow T_{10} + (T_4 \oplus T_6 \oplus T_7);$
    $Z_0 \leftarrow T_{11} + (T_0 \oplus T_1 \oplus T_5);$
    $Z_1 \leftarrow T_{12} + (T_2 \oplus T_6 \oplus T_7);$
    $Z_2 \leftarrow T_{13} + (T_0 \oplus T_1 \oplus T_3);$
    $Z_3 \leftarrow T_{14} + (T_0 \oplus T_3 \oplus T_4);$
    $Z_4 \leftarrow T_{15} + (T_1 \oplus T_2 \oplus T_5);$
```

$$\mathbf{X} * \mathbf{Y} \equiv \boxed{\pi_1}(\pi_2(\mathbf{X}) +_8 \pi_3(\mathbf{Y}))$$

Simple re-indexing (no computational costs)

Specific design characteristics for EDON-R

Quasigroup operation of order 2^{256}

Input: $\mathbf{X} = (X_0, X_1, \ldots, X_7)$ and $\mathbf{Y} = (Y_0, Y_1, \ldots, Y_7)$ where X_i and Y_i are 32–bit variables.

Output: $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_7)$ where Z_i are 32–bit variables.

Temporary 32–bit variables: $T_0, \ldots, T_{15}$.

$$
1.\quad
\begin{array}{lcl}
T_0 & \leftarrow & ROTL^0(\texttt{0xAAAAAAAA} + X_0 + X_1 + X_2 + X_4 + X_7);\\
T_1 & \leftarrow & ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7);\\
T_2 & \leftarrow & ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7);\\
T_3 & \leftarrow & ROTL^{13}(X_2 + X_3 + X_5 + X_6 + X_7);\\
T_4 & \leftarrow & ROTL^{17}(X_1 + X_2 + X_3 + X_5 + X_6);\\
T_5 & \leftarrow & ROTL^{22}(X_0 + X_2 + X_3 + X_4 + X_5);\\
T_6 & \leftarrow & ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7);\\
T_7 & \leftarrow & ROTL^{29}(X_2 + X_3 + X_4 + X_5 + X_6);
\end{array}
$$

$$
2.\quad
\begin{array}{lcl}
T_8 & \leftarrow & T_3 \oplus T_5 \oplus T_6;\\
T_9 & \leftarrow & T_2 \oplus T_5 \oplus T_6;\\
T_{10} & \leftarrow & T_2 \oplus T_3 \oplus T_5;\\
T_{11} & \leftarrow & T_0 \oplus T_1 \oplus T_4;\\
T_{12} & \leftarrow & T_0 \oplus T_4 \oplus T_7;\\
T_{13} & \leftarrow & T_1 \oplus T_6 \oplus T_7;\\
T_{14} & \leftarrow & T_2 \oplus T_3 \oplus T_4;\\
T_{15} & \leftarrow & T_0 \oplus T_1 \oplus T_7;
\end{array}
$$

$$
3.\quad
\begin{array}{lcl}
T_0 & \leftarrow & ROTL^0(\texttt{0x55555555} + Y_0 + Y_1 + Y_2 + Y_5 + Y_7);\\
T_1 & \leftarrow & ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6);\\
T_2 & \leftarrow & ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5);\\
T_3 & \leftarrow & ROTL^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7);\\
T_4 & \leftarrow & ROTL^{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_5);\\
T_5 & \leftarrow & ROTL^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);\\
T_6 & \leftarrow & ROTL^{25}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7);\\
T_7 & \leftarrow & ROTL^{27}(Y_0 + Y_3 + Y_4 + Y_6 + Y_7);
\end{array}
$$

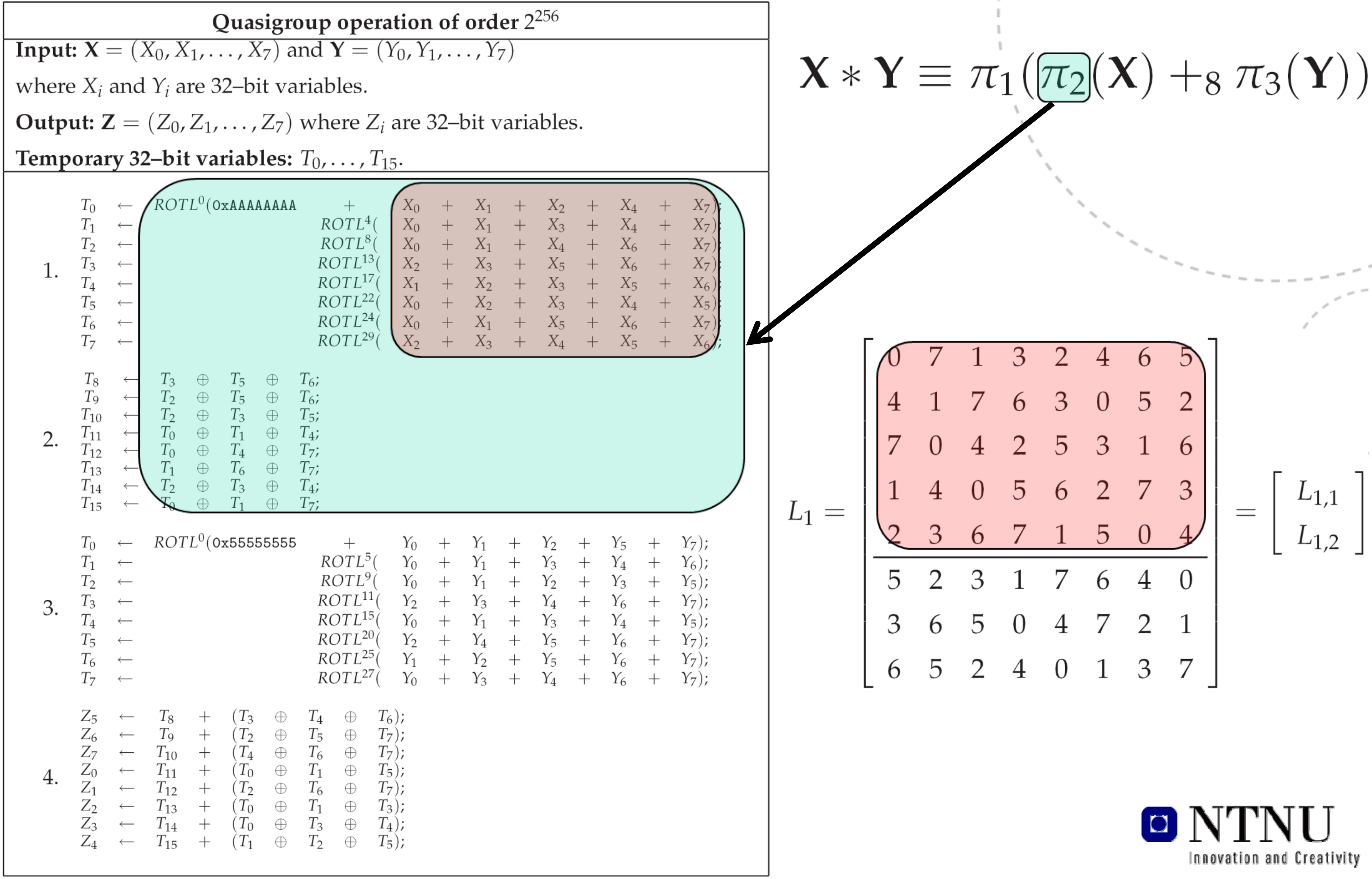
$$
4.\quad
\begin{array}{lcl}
Z_5 & \leftarrow & T_8 + (T_3 \oplus T_4 \oplus T_6);\\
Z_6 & \leftarrow & T_9 + (T_2 \oplus T_5 \oplus T_7);\\
Z_7 & \leftarrow & T_{10} + (T_4 \oplus T_6 \oplus T_7);\\
Z_0 & \leftarrow & T_{11} + (T_0 \oplus T_1 \oplus T_5);\\
Z_1 & \leftarrow & T_{12} + (T_2 \oplus T_6 \oplus T_7);\\
Z_2 & \leftarrow & T_{13} + (T_0 \oplus T_1 \oplus T_3);\\
Z_3 & \leftarrow & T_{14} + (T_0 \oplus T_3 \oplus T_4);\\
Z_4 & \leftarrow & T_{15} + (T_1 \oplus T_2 \oplus T_5);
\end{array}
$$

$$\mathbf{X} * \mathbf{Y} \equiv \pi_1(\boxed{\pi_2}(\mathbf{X}) +_8 \pi_3(\mathbf{Y}))$$

$$
L_1 = \left[\begin{array}{cccccccc}
0 & 7 & 1 & 3 & 2 & 4 & 6 & 5\\
4 & 1 & 7 & 6 & 3 & 0 & 5 & 2\\
7 & 0 & 4 & 2 & 5 & 3 & 1 & 6\\
1 & 4 & 0 & 5 & 6 & 2 & 7 & 3\\
2 & 3 & 6 & 7 & 1 & 5 & 0 & 4\\
\hline
5 & 2 & 3 & 1 & 7 & 6 & 4 & 0\\
3 & 6 & 5 & 0 & 4 & 7 & 2 & 1\\
6 & 5 & 2 & 4 & 0 & 1 & 3 & 7
\end{array}\right] = \left[\begin{array}{c} L_{1,1}\\ L_{1,2}\end{array}\right]
$$

NTNU
Innovation and Creativity

Specific design characteristics for EDON-R



Quasigroup operation of order 2^{256}

Input: $\mathbf{X} = (X_0, X_1, \ldots, X_7)$ and $\mathbf{Y} = (Y_0, Y_1, \ldots, Y_7)$ where X_i and Y_i are 32–bit variables.

Output: $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_7)$ where Z_i are 32–bit variables.

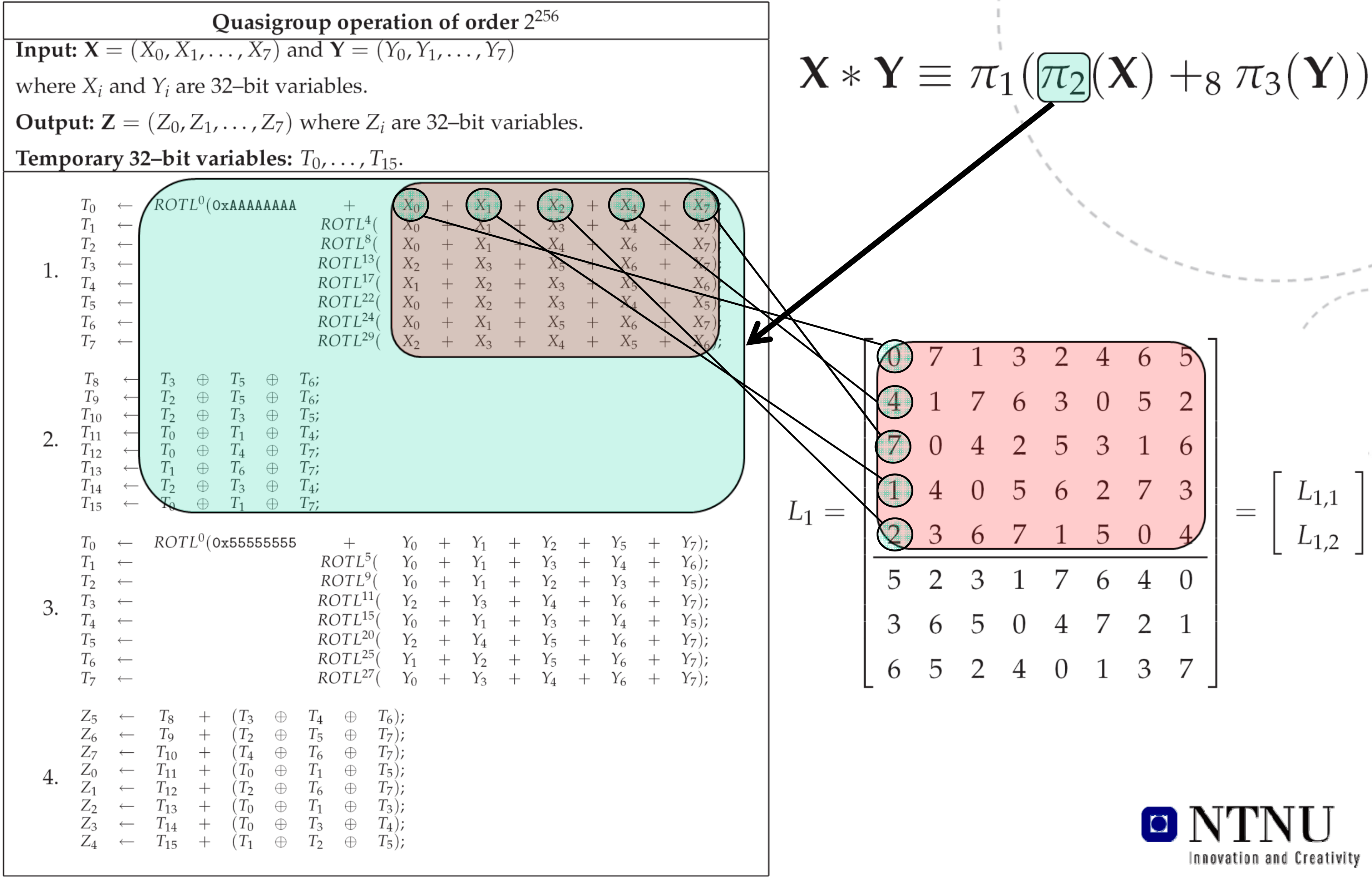
Temporary 32–bit variables: $T_0, \ldots, T_{15}$.

```
1.  $T_0 \leftarrow ROTL^0(\texttt{0xAAAAAAAA} + X_0 + X_1 + X_2 + X_4 + X_7);$
    $T_1 \leftarrow ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7);$
    $T_2 \leftarrow ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7);$
    $T_3 \leftarrow ROTL^{13}(X_2 + X_3 + X_5 + X_6 + X_7);$
    $T_4 \leftarrow ROTL^{17}(X_1 + X_2 + X_3 + X_5 + X_6);$
    $T_5 \leftarrow ROTL^{22}(X_0 + X_2 + X_3 + X_4 + X_5);$
    $T_6 \leftarrow ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7);$
    $T_7 \leftarrow ROTL^{29}(X_2 + X_3 + X_4 + X_5 + X_6);$
2.  $T_8 \leftarrow T_3 \oplus T_5 \oplus T_6;$
    $T_9 \leftarrow T_2 \oplus T_5 \oplus T_6;$
    $T_{10} \leftarrow T_2 \oplus T_3 \oplus T_5;$
    $T_{11} \leftarrow T_0 \oplus T_1 \oplus T_4;$
    $T_{12} \leftarrow T_0 \oplus T_4 \oplus T_7;$
    $T_{13} \leftarrow T_1 \oplus T_6 \oplus T_7;$
    $T_{14} \leftarrow T_2 \oplus T_3 \oplus T_4;$
    $T_{15} \leftarrow T_0 \oplus T_1 \oplus T_7;$
3.  $T_0 \leftarrow ROTL^0(\texttt{0x55555555} + Y_0 + Y_1 + Y_2 + Y_5 + Y_7);$
    $T_1 \leftarrow ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6);$
    $T_2 \leftarrow ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5);$
    $T_3 \leftarrow ROTL^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7);$
    $T_4 \leftarrow ROTL^{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_5);$
    $T_5 \leftarrow ROTL^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);$
    $T_6 \leftarrow ROTL^{25}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7);$
    $T_7 \leftarrow ROTL^{27}(Y_0 + Y_3 + Y_4 + Y_6 + Y_7);$
4.  $Z_5 \leftarrow T_8 + (T_3 \oplus T_4 \oplus T_6);$
    $Z_6 \leftarrow T_9 + (T_2 \oplus T_5 \oplus T_7);$
    $Z_7 \leftarrow T_{10} + (T_4 \oplus T_6 \oplus T_7);$
    $Z_0 \leftarrow T_{11} + (T_0 \oplus T_1 \oplus T_5);$
    $Z_1 \leftarrow T_{12} + (T_2 \oplus T_6 \oplus T_7);$
    $Z_2 \leftarrow T_{13} + (T_0 \oplus T_1 \oplus T_3);$
    $Z_3 \leftarrow T_{14} + (T_0 \oplus T_3 \oplus T_4);$
    $Z_4 \leftarrow T_{15} + (T_1 \oplus T_2 \oplus T_5);$
```

$$\mathbf{X} * \mathbf{Y} \equiv \pi_1(\boxed{\pi_2}(\mathbf{X}) +_8 \pi_3(\mathbf{Y}))$$

$$L_1 = \left[\begin{array}{cccccccc}
0 & 7 & 1 & 3 & 2 & 4 & 6 & 5 \\
4 & 1 & 7 & 6 & 3 & 0 & 5 & 2 \\
7 & 0 & 4 & 2 & 5 & 3 & 1 & 6 \\
1 & 4 & 0 & 5 & 6 & 2 & 7 & 3 \\
2 & 3 & 6 & 7 & 1 & 5 & 0 & 4 \\
\hline
5 & 2 & 3 & 1 & 7 & 6 & 4 & 0 \\
3 & 6 & 5 & 0 & 4 & 7 & 2 & 1 \\
6 & 5 & 2 & 4 & 0 & 1 & 3 & 7
\end{array}\right] = \left[\begin{array}{c} L_{1,1} \\ L_{1,2} \end{array}\right]$$

Specific design characteristics for EDON-R



Quasigroup operation of order 2^{256}

Input: $\mathbf{X} = (X_0, X_1, \ldots, X_7)$ and $\mathbf{Y} = (Y_0, Y_1, \ldots, Y_7)$ where X_i and Y_i are 32–bit variables.

Output: $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_7)$ where Z_i are 32–bit variables.

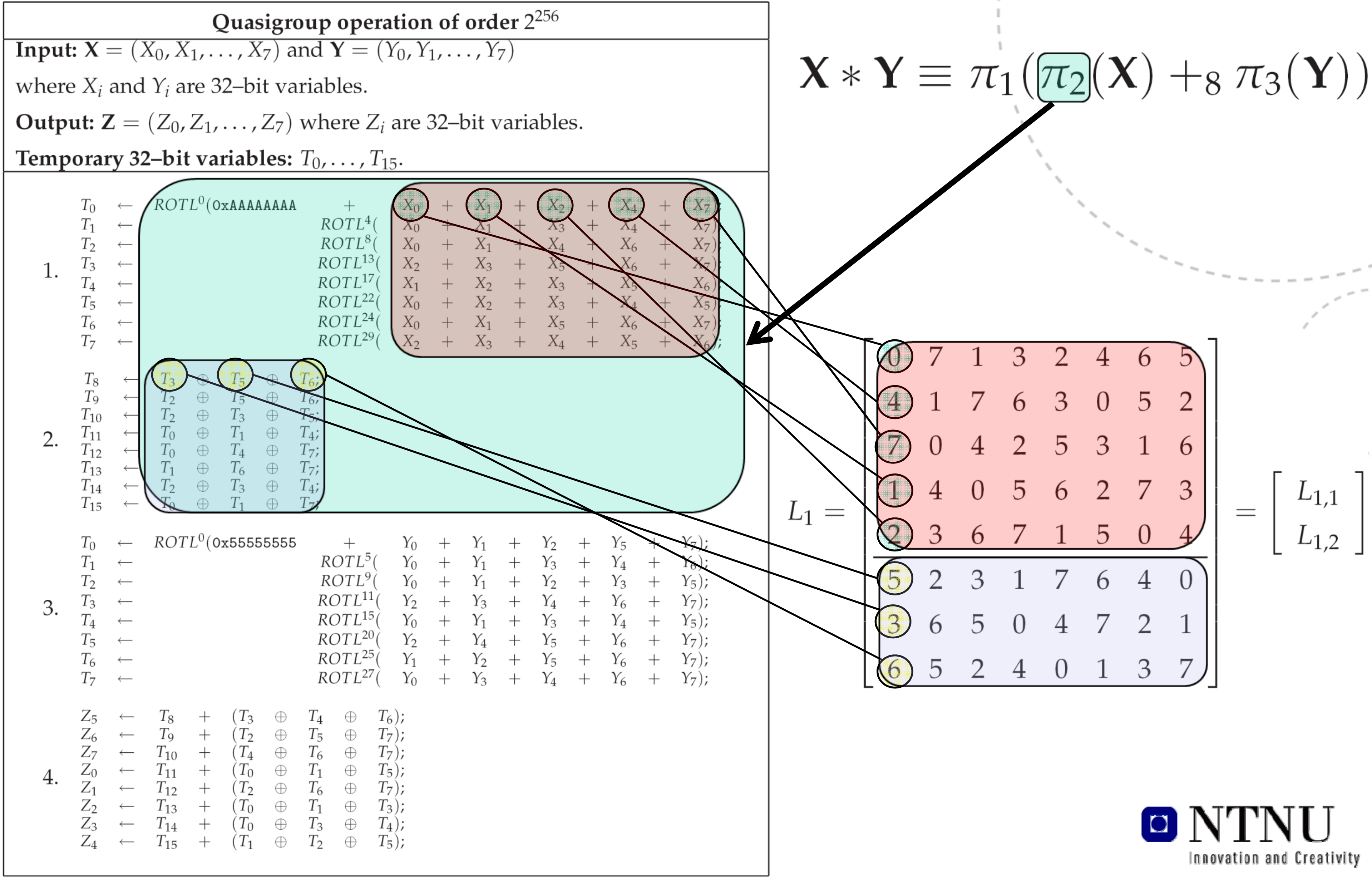
Temporary 32–bit variables: $T_0, \ldots, T_{15}$.

```
1.  $T_0 \leftarrow ROTL^0(\texttt{0xAAAAAAAA} + X_0 + X_1 + X_2 + X_4 + X_7);$
    $T_1 \leftarrow ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7);$
    $T_2 \leftarrow ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7);$
    $T_3 \leftarrow ROTL^{13}(X_2 + X_3 + X_5 + X_6 + X_7);$
    $T_4 \leftarrow ROTL^{17}(X_1 + X_2 + X_3 + X_5 + X_6);$
    $T_5 \leftarrow ROTL^{22}(X_0 + X_2 + X_3 + X_4 + X_5);$
    $T_6 \leftarrow ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7);$
    $T_7 \leftarrow ROTL^{29}(X_2 + X_3 + X_4 + X_5 + X_6);$

2.  $T_8 \leftarrow T_3 \oplus T_5 \oplus T_6;$
    $T_9 \leftarrow T_2 \oplus T_5 \oplus T_6;$
    $T_{10} \leftarrow T_2 \oplus T_3 \oplus T_5;$
    $T_{11} \leftarrow T_0 \oplus T_1 \oplus T_4;$
    $T_{12} \leftarrow T_0 \oplus T_4 \oplus T_7;$
    $T_{13} \leftarrow T_1 \oplus T_6 \oplus T_7;$
    $T_{14} \leftarrow T_2 \oplus T_3 \oplus T_4;$
    $T_{15} \leftarrow T_0 \oplus T_1 \oplus T_7;$

3.  $T_0 \leftarrow ROTL^0(\texttt{0x55555555} + Y_0 + Y_1 + Y_2 + Y_5 + Y_7);$
    $T_1 \leftarrow ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6);$
    $T_2 \leftarrow ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5);$
    $T_3 \leftarrow ROTL^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7);$
    $T_4 \leftarrow ROTL^{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_5);$
    $T_5 \leftarrow ROTL^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);$
    $T_6 \leftarrow ROTL^{25}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7);$
    $T_7 \leftarrow ROTL^{27}(Y_0 + Y_3 + Y_4 + Y_6 + Y_7);$

4.  $Z_5 \leftarrow T_8 + (T_3 \oplus T_4 \oplus T_6);$
    $Z_6 \leftarrow T_9 + (T_2 \oplus T_5 \oplus T_7);$
    $Z_7 \leftarrow T_{10} + (T_4 \oplus T_6 \oplus T_7);$
    $Z_0 \leftarrow T_{11} + (T_0 \oplus T_1 \oplus T_5);$
    $Z_1 \leftarrow T_{12} + (T_2 \oplus T_6 \oplus T_7);$
    $Z_2 \leftarrow T_{13} + (T_0 \oplus T_1 \oplus T_3);$
    $Z_3 \leftarrow T_{14} + (T_0 \oplus T_3 \oplus T_4);$
    $Z_4 \leftarrow T_{15} + (T_1 \oplus T_2 \oplus T_5);$
```

$$\mathbf{X} * \mathbf{Y} \equiv \pi_1(\boxed{\pi_2}(\mathbf{X}) +_8 \pi_3(\mathbf{Y}))$$

$$L_1 = \left[\begin{array}{cccccccc}
0 & 7 & 1 & 3 & 2 & 4 & 6 & 5 \\
4 & 1 & 7 & 6 & 3 & 0 & 5 & 2 \\
7 & 0 & 4 & 2 & 5 & 3 & 1 & 6 \\
1 & 4 & 0 & 5 & 6 & 2 & 7 & 3 \\
2 & 3 & 6 & 7 & 1 & 5 & 0 & 4 \\
\hline
5 & 2 & 3 & 1 & 7 & 6 & 4 & 0 \\
3 & 6 & 5 & 0 & 4 & 7 & 2 & 1 \\
6 & 5 & 2 & 4 & 0 & 1 & 3 & 7
\end{array}\right] = \left[\begin{array}{c} L_{1,1} \\ L_{1,2} \end{array}\right]$$

Specific design characteristics for EDON-R



Quasigroup operation of order 2^{256}

Input: $\mathbf{X} = (X_0, X_1, \ldots, X_7)$ and $\mathbf{Y} = (Y_0, Y_1, \ldots, Y_7)$ where X_i and Y_i are 32–bit variables.

Output: $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_7)$ where Z_i are 32–bit variables.

Temporary 32–bit variables: $T_0, \ldots, T_{15}$.

$$
\begin{array}{lllllllllllll}
1. & T_0 & \leftarrow & ROTL^0(\texttt{0xAAAAAAAA} & + & X_0 & + & X_1 & + & X_2 & + & X_4 & + X_7); \\
 & T_1 & \leftarrow & & ROTL^4(& X_0 & + & X_1 & + & X_3 & + & X_4 & + X_7); \\
 & T_2 & \leftarrow & & ROTL^8(& X_0 & + & X_1 & + & X_4 & + & X_6 & + X_7); \\
 & T_3 & \leftarrow & & ROTL^{13}(& X_2 & + & X_3 & + & X_5 & + & X_6 & + X_7); \\
 & T_4 & \leftarrow & & ROTL^{17}(& X_1 & + & X_2 & + & X_3 & + & X_5 & + X_6); \\
 & T_5 & \leftarrow & & ROTL^{22}(& X_0 & + & X_2 & + & X_3 & + & X_4 & + X_5); \\
 & T_6 & \leftarrow & & ROTL^{24}(& X_0 & + & X_1 & + & X_5 & + & X_6 & + X_7); \\
 & T_7 & \leftarrow & & ROTL^{29}(& X_2 & + & X_3 & + & X_4 & + & X_5 & + X_6);
\end{array}
$$

$$
\begin{array}{lllllll}
2. & T_8 & \leftarrow & T_3 & \oplus & T_5 & \oplus\ T_6; \\
 & T_9 & \leftarrow & T_2 & \oplus & T_5 & \oplus\ T_6; \\
 & T_{10} & \leftarrow & T_2 & \oplus & T_3 & \oplus\ T_5; \\
 & T_{11} & \leftarrow & T_0 & \oplus & T_1 & \oplus\ T_4; \\
 & T_{12} & \leftarrow & T_0 & \oplus & T_4 & \oplus\ T_7; \\
 & T_{13} & \leftarrow & T_1 & \oplus & T_6 & \oplus\ T_7; \\
 & T_{14} & \leftarrow & T_2 & \oplus & T_3 & \oplus\ T_4; \\
 & T_{15} & \leftarrow & T_0 & \oplus & T_1 & \oplus\ T_7;
\end{array}
$$

$$
\begin{array}{lllllllllllll}
3. & T_0 & \leftarrow & ROTL^0(\texttt{0x55555555} & + & Y_0 & + & Y_1 & + & Y_2 & + & Y_5 & + Y_7); \\
 & T_1 & \leftarrow & & ROTL^5(& Y_0 & + & Y_1 & + & Y_3 & + & Y_4 & + Y_6); \\
 & T_2 & \leftarrow & & ROTL^9(& Y_0 & + & Y_1 & + & Y_2 & + & Y_3 & + Y_5); \\
 & T_3 & \leftarrow & & ROTL^{11}(& Y_2 & + & Y_3 & + & Y_4 & + & Y_6 & + Y_7); \\
 & T_4 & \leftarrow & & ROTL^{15}(& Y_0 & + & Y_1 & + & Y_3 & + & Y_4 & + Y_5); \\
 & T_5 & \leftarrow & & ROTL^{20}(& Y_2 & + & Y_4 & + & Y_5 & + & Y_6 & + Y_7); \\
 & T_6 & \leftarrow & & ROTL^{25}(& Y_1 & + & Y_2 & + & Y_5 & + & Y_6 & + Y_7); \\
 & T_7 & \leftarrow & & ROTL^{27}(& Y_0 & + & Y_3 & + & Y_4 & + & Y_6 & + Y_7);
\end{array}
$$

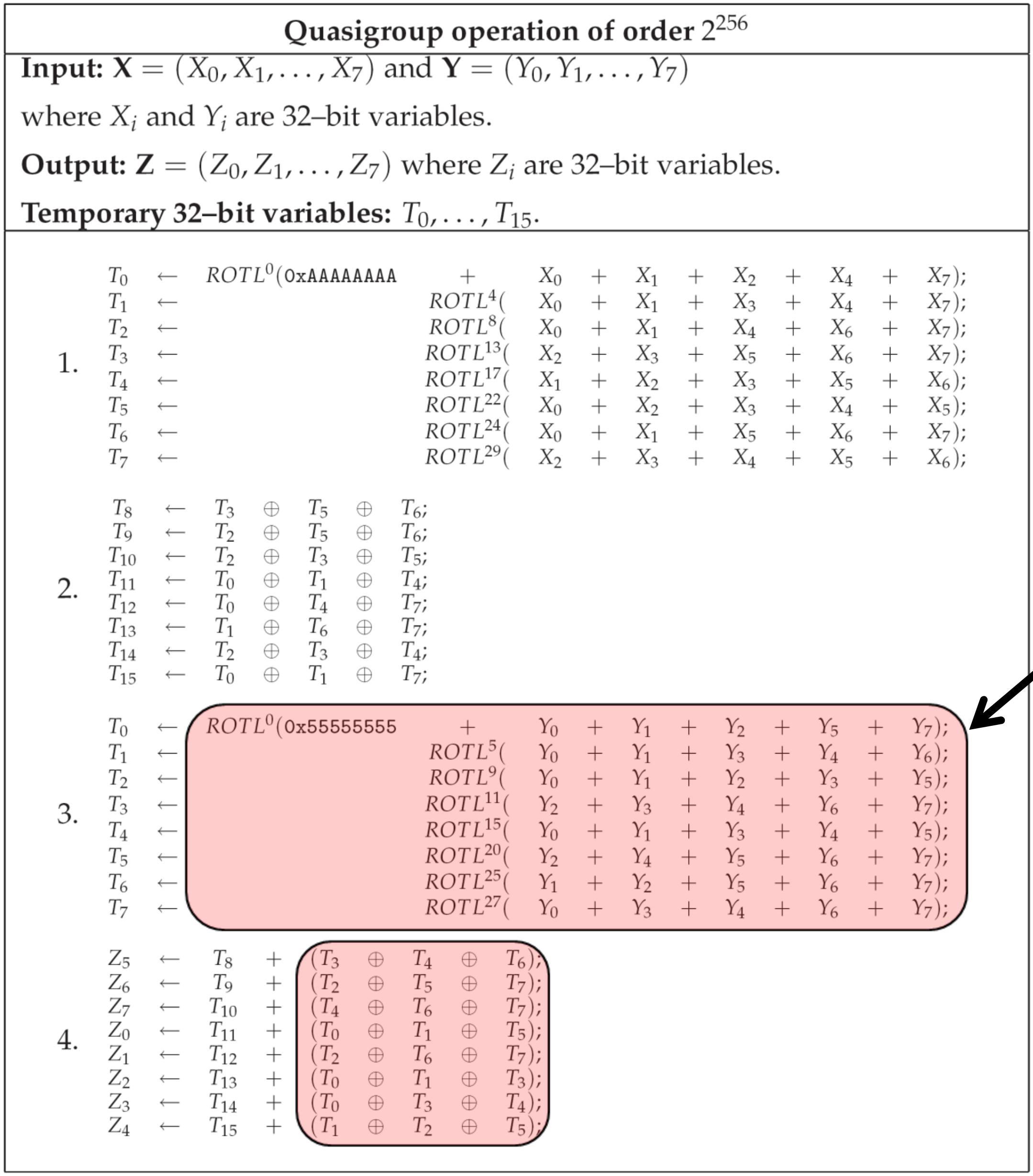
$$
\begin{array}{lllllllll}
4. & Z_5 & \leftarrow & T_8 & + & (T_3 & \oplus & T_4 & \oplus\ T_6); \\
 & Z_6 & \leftarrow & T_9 & + & (T_2 & \oplus & T_5 & \oplus\ T_7); \\
 & Z_7 & \leftarrow & T_{10} & + & (T_4 & \oplus & T_6 & \oplus\ T_7); \\
 & Z_0 & \leftarrow & T_{11} & + & (T_0 & \oplus & T_1 & \oplus\ T_5); \\
 & Z_1 & \leftarrow & T_{12} & + & (T_2 & \oplus & T_6 & \oplus\ T_7); \\
 & Z_2 & \leftarrow & T_{13} & + & (T_0 & \oplus & T_1 & \oplus\ T_3); \\
 & Z_3 & \leftarrow & T_{14} & + & (T_0 & \oplus & T_3 & \oplus\ T_4); \\
 & Z_4 & \leftarrow & T_{15} & + & (T_1 & \oplus & T_2 & \oplus\ T_5);
\end{array}
$$

$$\mathbf{X} * \mathbf{Y} \equiv \pi_1(\boxed{\pi_2}(\mathbf{X}) +_8 \pi_3(\mathbf{Y}))$$

$$
L_1 = \begin{bmatrix}
0 & 7 & 1 & 3 & 2 & 4 & 6 & 5 \\
4 & 1 & 7 & 6 & 3 & 0 & 5 & 2 \\
7 & 0 & 4 & 2 & 5 & 3 & 1 & 6 \\
1 & 4 & 0 & 5 & 6 & 2 & 7 & 3 \\
2 & 3 & 6 & 7 & 1 & 5 & 0 & 4 \\
\hline
5 & 2 & 3 & 1 & 7 & 6 & 4 & 0 \\
3 & 6 & 5 & 0 & 4 & 7 & 2 & 1 \\
6 & 5 & 2 & 4 & 0 & 1 & 3 & 7
\end{bmatrix}
= \begin{bmatrix} L_{1,1} \\ L_{1,2} \end{bmatrix}
$$

NTNU
Innovation and Creativity

Specific design characteristics for EDON-R



Quasigroup operation of order 2^{256}

Input: $\mathbf{X} = (X_0, X_1, \ldots, X_7)$ and $\mathbf{Y} = (Y_0, Y_1, \ldots, Y_7)$ where X_i and Y_i are 32–bit variables.

Output: $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_7)$ where Z_i are 32–bit variables.

Temporary 32–bit variables: $T_0, \ldots, T_{15}$.

1.
$$\begin{array}{lll}
T_0 & \leftarrow & ROTL^0(\texttt{0xAAAAAAAA} + X_0 + X_1 + X_2 + X_4 + X_7);\\
T_1 & \leftarrow & ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7);\\
T_2 & \leftarrow & ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7);\\
T_3 & \leftarrow & ROTL^{13}(X_2 + X_3 + X_5 + X_6 + X_7);\\
T_4 & \leftarrow & ROTL^{17}(X_1 + X_2 + X_3 + X_5 + X_6);\\
T_5 & \leftarrow & ROTL^{22}(X_0 + X_2 + X_3 + X_4 + X_5);\\
T_6 & \leftarrow & ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7);\\
T_7 & \leftarrow & ROTL^{29}(X_2 + X_3 + X_4 + X_5 + X_6);
\end{array}$$

2.
$$\begin{array}{lll}
T_8 & \leftarrow & T_3 \oplus T_5 \oplus T_6;\\
T_9 & \leftarrow & T_2 \oplus T_5 \oplus T_6;\\
T_{10} & \leftarrow & T_2 \oplus T_3 \oplus T_5;\\
T_{11} & \leftarrow & T_0 \oplus T_1 \oplus T_4;\\
T_{12} & \leftarrow & T_0 \oplus T_4 \oplus T_7;\\
T_{13} & \leftarrow & T_1 \oplus T_6 \oplus T_7;\\
T_{14} & \leftarrow & T_2 \oplus T_3 \oplus T_4;\\
T_{15} & \leftarrow & T_0 \oplus T_1 \oplus T_7;
\end{array}$$

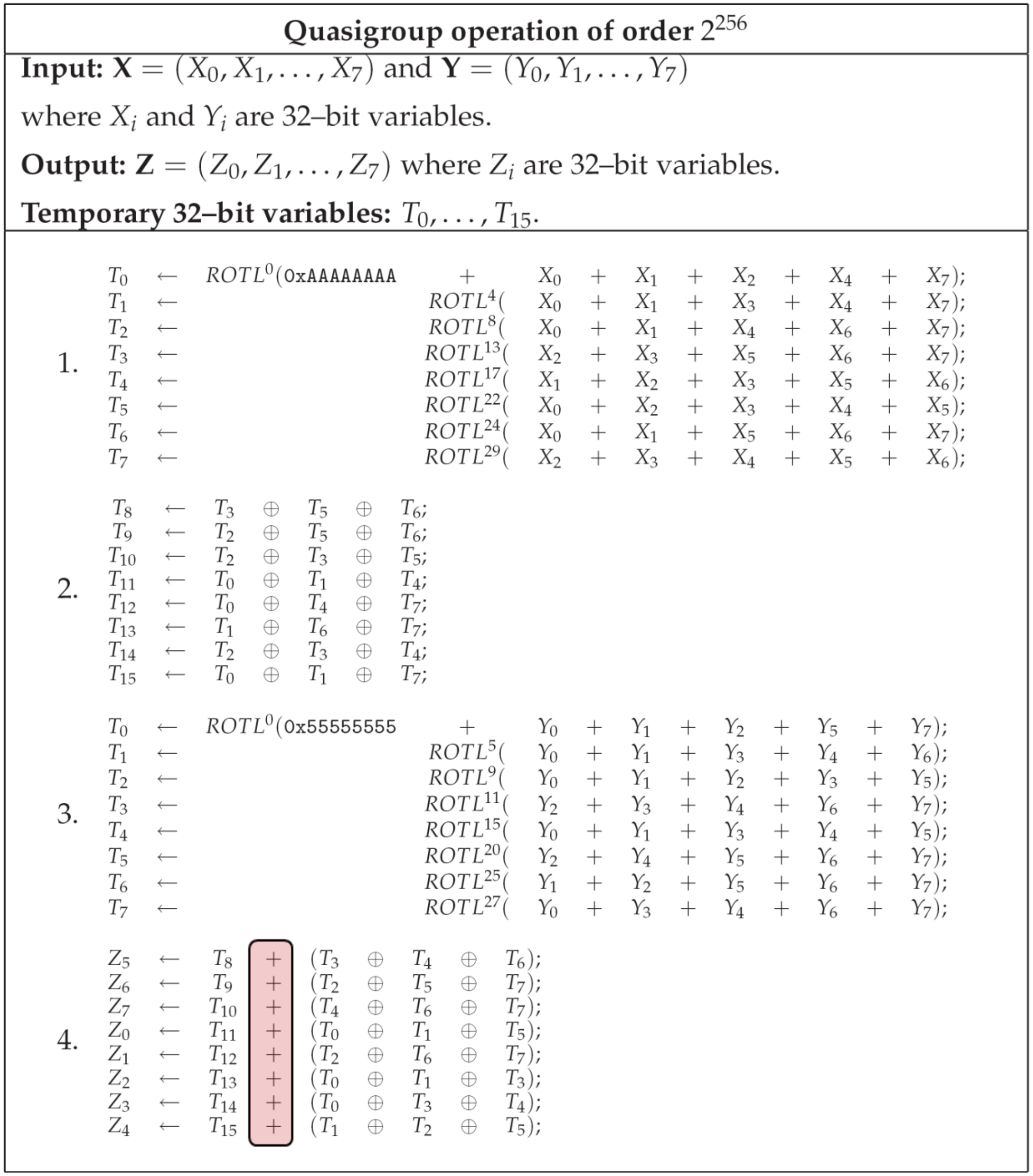
3.
$$\begin{array}{lll}
T_0 & \leftarrow & ROTL^0(\texttt{0x55555555} + Y_0 + Y_1 + Y_2 + Y_5 + Y_7);\\
T_1 & \leftarrow & ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6);\\
T_2 & \leftarrow & ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5);\\
T_3 & \leftarrow & ROTL^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7);\\
T_4 & \leftarrow & ROTL^{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_5);\\
T_5 & \leftarrow & ROTL^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);\\
T_6 & \leftarrow & ROTL^{25}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7);\\
T_7 & \leftarrow & ROTL^{27}(Y_0 + Y_3 + Y_4 + Y_6 + Y_7);
\end{array}$$

4.
$$\begin{array}{lll}
Z_5 & \leftarrow & T_8 + (T_3 \oplus T_4 \oplus T_6);\\
Z_6 & \leftarrow & T_9 + (T_2 \oplus T_5 \oplus T_7);\\
Z_7 & \leftarrow & T_{10} + (T_4 \oplus T_6 \oplus T_7);\\
Z_0 & \leftarrow & T_{11} + (T_0 \oplus T_1 \oplus T_5);\\
Z_1 & \leftarrow & T_{12} + (T_2 \oplus T_6 \oplus T_7);\\
Z_2 & \leftarrow & T_{13} + (T_0 \oplus T_1 \oplus T_3);\\
Z_3 & \leftarrow & T_{14} + (T_0 \oplus T_3 \oplus T_4);\\
Z_4 & \leftarrow & T_{15} + (T_1 \oplus T_2 \oplus T_5);
\end{array}$$

$$\mathbf{X} * \mathbf{Y} \equiv \pi_1(\pi_2(\mathbf{X}) +_8 \pi_3(\mathbf{Y}))$$

$$L_2 = \left[\begin{array}{cccccccc}
0 & 4 & 2 & 3 & 1 & 6 & 5 & 7\\
7 & 6 & 3 & 2 & 5 & 4 & 1 & 0\\
5 & 3 & 1 & 6 & 0 & 2 & 7 & 4\\
1 & 0 & 5 & 4 & 3 & 7 & 2 & 6\\
2 & 1 & 0 & 7 & 4 & 5 & 6 & 3\\
\hline
3 & 5 & 7 & 0 & 6 & 1 & 4 & 2\\
4 & 7 & 6 & 1 & 2 & 0 & 3 & 5\\
6 & 2 & 4 & 5 & 7 & 3 & 0 & 1
\end{array}\right] = \left[\begin{array}{c} L_{2,1}\\ L_{2,2}\end{array}\right]$$

Specific design characteristics for EDON-R



Quasigroup operation of order 2^{256}

Input: $\mathbf{X} = (X_0, X_1, \dots, X_7)$ and $\mathbf{Y} = (Y_0, Y_1, \dots, Y_7)$ where X_i and Y_i are 32–bit variables.

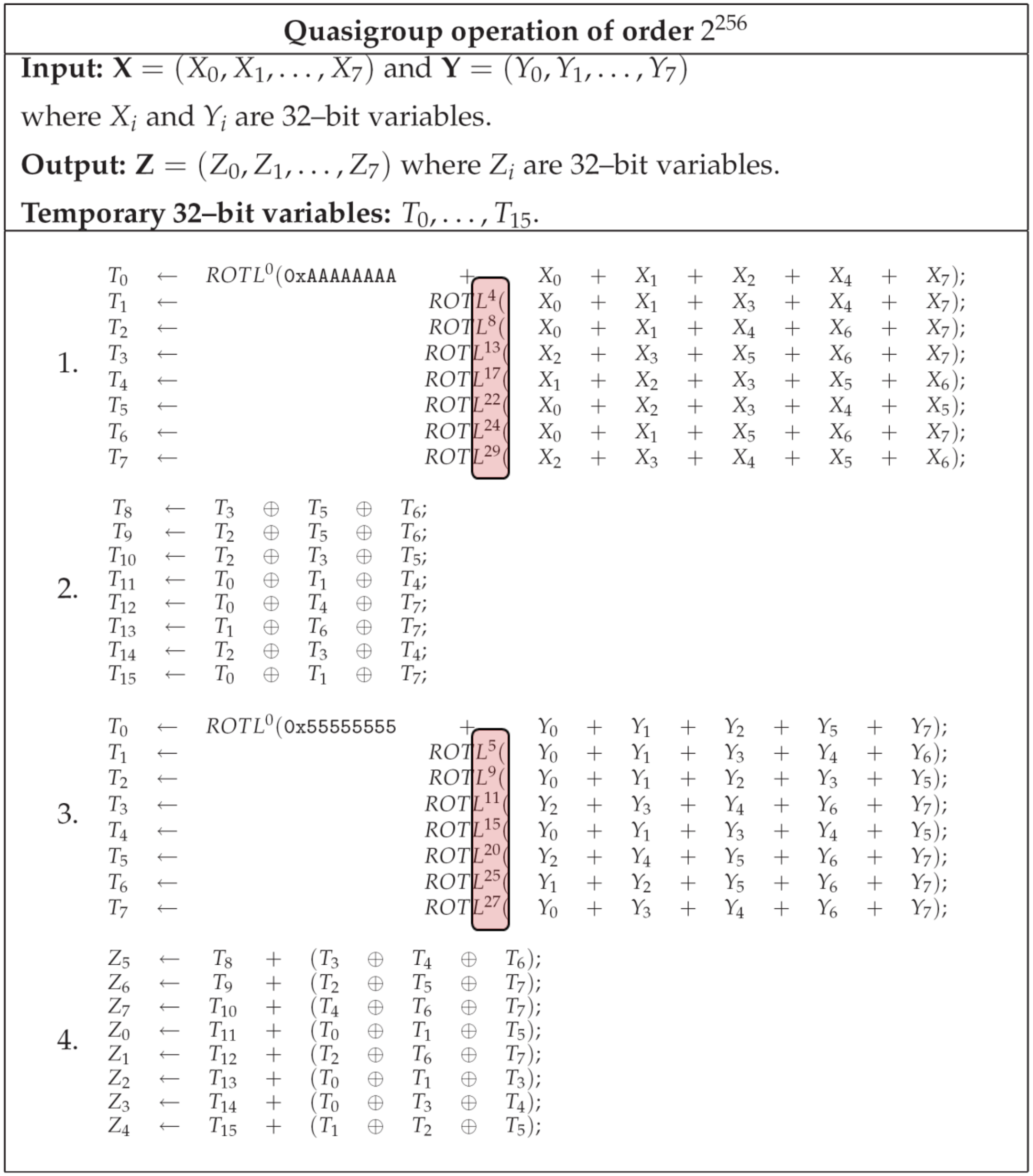
Output: $\mathbf{Z} = (Z_0, Z_1, \dots, Z_7)$ where Z_i are 32–bit variables.

Temporary 32–bit variables: $T_0, \dots, T_{15}$.

```
1.  $T_0 \leftarrow ROTL^0(\texttt{0xAAAAAAAA} + X_0 + X_1 + X_2 + X_4 + X_7);$
    $T_1 \leftarrow ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7);$
    $T_2 \leftarrow ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7);$
    $T_3 \leftarrow ROTL^{13}(X_2 + X_3 + X_5 + X_6 + X_7);$
    $T_4 \leftarrow ROTL^{17}(X_1 + X_2 + X_3 + X_5 + X_6);$
    $T_5 \leftarrow ROTL^{22}(X_0 + X_2 + X_3 + X_4 + X_5);$
    $T_6 \leftarrow ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7);$
    $T_7 \leftarrow ROTL^{29}(X_2 + X_3 + X_4 + X_5 + X_6);$

2.  $T_8 \leftarrow T_3 \oplus T_5 \oplus T_6;$
    $T_9 \leftarrow T_2 \oplus T_5 \oplus T_6;$
    $T_{10} \leftarrow T_2 \oplus T_3 \oplus T_5;$
    $T_{11} \leftarrow T_0 \oplus T_1 \oplus T_4;$
    $T_{12} \leftarrow T_0 \oplus T_4 \oplus T_7;$
    $T_{13} \leftarrow T_1 \oplus T_6 \oplus T_7;$
    $T_{14} \leftarrow T_2 \oplus T_3 \oplus T_4;$
    $T_{15} \leftarrow T_0 \oplus T_1 \oplus T_7;$

3.  $T_0 \leftarrow ROTL^0(\texttt{0x55555555} + Y_0 + Y_1 + Y_2 + Y_5 + Y_7);$
    $T_1 \leftarrow ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6);$
    $T_2 \leftarrow ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5);$
    $T_3 \leftarrow ROTL^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7);$
    $T_4 \leftarrow ROTL^{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_5);$
    $T_5 \leftarrow ROTL^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);$
    $T_6 \leftarrow ROTL^{25}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7);$
    $T_7 \leftarrow ROTL^{27}(Y_0 + Y_3 + Y_4 + Y_6 + Y_7);$

4.  $Z_5 \leftarrow T_8 \boxed{+} (T_3 \oplus T_4 \oplus T_6);$
    $Z_6 \leftarrow T_9 \boxed{+} (T_2 \oplus T_5 \oplus T_7);$
    $Z_7 \leftarrow T_{10} \boxed{+} (T_4 \oplus T_6 \oplus T_7);$
    $Z_0 \leftarrow T_{11} \boxed{+} (T_0 \oplus T_1 \oplus T_5);$
    $Z_1 \leftarrow T_{12} \boxed{+} (T_2 \oplus T_6 \oplus T_7);$
    $Z_2 \leftarrow T_{13} \boxed{+} (T_0 \oplus T_1 \oplus T_3);$
    $Z_3 \leftarrow T_{14} \boxed{+} (T_0 \oplus T_3 \oplus T_4);$
    $Z_4 \leftarrow T_{15} \boxed{+} (T_1 \oplus T_2 \oplus T_5);$
```

$$\mathbf{X} * \mathbf{Y} \equiv \pi_1(\pi_2(\mathbf{X}) \boxed{+_8} \pi_3(\mathbf{Y}))$$

Specific design characteristics for EDON-R



Quasigroup operation of order 2^{256}

Input: $\mathbf{X} = (X_0, X_1, \ldots, X_7)$ and $\mathbf{Y} = (Y_0, Y_1, \ldots, Y_7)$ where X_i and Y_i are 32–bit variables.

Output: $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_7)$ where Z_i are 32–bit variables.

Temporary 32–bit variables: $T_0, \ldots, T_{15}$.

1.
$$\begin{array}{lll}
T_0 & \leftarrow & ROTL^0(\mathtt{0xAAAAAAAA} + X_0 + X_1 + X_2 + X_4 + X_7);\\
T_1 & \leftarrow & ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7);\\
T_2 & \leftarrow & ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7);\\
T_3 & \leftarrow & ROTL^{13}(X_2 + X_3 + X_5 + X_6 + X_7);\\
T_4 & \leftarrow & ROTL^{17}(X_1 + X_2 + X_3 + X_5 + X_6);\\
T_5 & \leftarrow & ROTL^{22}(X_0 + X_2 + X_3 + X_4 + X_5);\\
T_6 & \leftarrow & ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7);\\
T_7 & \leftarrow & ROTL^{29}(X_2 + X_3 + X_4 + X_5 + X_6);
\end{array}$$

2.
$$\begin{array}{lll}
T_8 & \leftarrow & T_3 \oplus T_5 \oplus T_6;\\
T_9 & \leftarrow & T_2 \oplus T_5 \oplus T_6;\\
T_{10} & \leftarrow & T_2 \oplus T_3 \oplus T_5;\\
T_{11} & \leftarrow & T_0 \oplus T_1 \oplus T_4;\\
T_{12} & \leftarrow & T_0 \oplus T_4 \oplus T_7;\\
T_{13} & \leftarrow & T_1 \oplus T_6 \oplus T_7;\\
T_{14} & \leftarrow & T_2 \oplus T_3 \oplus T_4;\\
T_{15} & \leftarrow & T_0 \oplus T_1 \oplus T_7;
\end{array}$$

3.
$$\begin{array}{lll}
T_0 & \leftarrow & ROTL^0(\mathtt{0x55555555} + Y_0 + Y_1 + Y_2 + Y_5 + Y_7);\\
T_1 & \leftarrow & ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6);\\
T_2 & \leftarrow & ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5);\\
T_3 & \leftarrow & ROTL^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7);\\
T_4 & \leftarrow & ROTL^{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_5);\\
T_5 & \leftarrow & ROTL^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);\\
T_6 & \leftarrow & ROTL^{25}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7);\\
T_7 & \leftarrow & ROTL^{27}(Y_0 + Y_3 + Y_4 + Y_6 + Y_7);
\end{array}$$

4.
$$\begin{array}{lll}
Z_5 & \leftarrow & T_8 + (T_3 \oplus T_4 \oplus T_6);\\
Z_6 & \leftarrow & T_9 + (T_2 \oplus T_5 \oplus T_7);\\
Z_7 & \leftarrow & T_{10} + (T_4 \oplus T_6 \oplus T_7);\\
Z_0 & \leftarrow & T_{11} + (T_0 \oplus T_1 \oplus T_5);\\
Z_1 & \leftarrow & T_{12} + (T_2 \oplus T_6 \oplus T_7);\\
Z_2 & \leftarrow & T_{13} + (T_0 \oplus T_1 \oplus T_3);\\
Z_3 & \leftarrow & T_{14} + (T_0 \oplus T_3 \oplus T_4);\\
Z_4 & \leftarrow & T_{15} + (T_1 \oplus T_2 \oplus T_5);
\end{array}$$

$$\mathbf{X} * \mathbf{Y} \equiv \pi_1(\pi_2(\mathbf{X}) +_8 \pi_3(\mathbf{Y}))$$

Rotations differ from each other for at least 2 positions.

Specific design characteristics for EDON-R

$$L_1 = \left[\begin{array}{cccccccc} 0 & 7 & 1 & 3 & 2 & 4 & 6 & 5 \\ 4 & 1 & 7 & 6 & 3 & 0 & 5 & 2 \\ 7 & 0 & 4 & 2 & 5 & 3 & 1 & 6 \\ 1 & 4 & 0 & 5 & 6 & 2 & 7 & 3 \\ 2 & 3 & 6 & 7 & 1 & 5 & 0 & 4 \\ \hline 5 & 2 & 3 & 1 & 7 & 6 & 4 & 0 \\ 3 & 6 & 5 & 0 & 4 & 7 & 2 & 1 \\ 6 & 5 & 2 & 4 & 0 & 1 & 3 & 7 \end{array}\right] = \left[\begin{array}{c} L_{1,1} \\ L_{1,2} \end{array}\right] \qquad L_2 = \left[\begin{array}{cccccccc} 0 & 4 & 2 & 3 & 1 & 6 & 5 & 7 \\ 7 & 6 & 3 & 2 & 5 & 4 & 1 & 0 \\ 5 & 3 & 1 & 6 & 0 & 2 & 7 & 4 \\ 1 & 0 & 5 & 4 & 3 & 7 & 2 & 6 \\ 2 & 1 & 0 & 7 & 4 & 5 & 6 & 3 \\ \hline 3 & 5 & 7 & 0 & 6 & 1 & 4 & 2 \\ 4 & 7 & 6 & 1 & 2 & 0 & 3 & 5 \\ 6 & 2 & 4 & 5 & 7 & 3 & 0 & 1 \end{array}\right] = \left[\begin{array}{c} L_{2,1} \\ L_{2,2} \end{array}\right]$$

Two orthogonal Latin Squares of order 8

Specific design characteristics for EDON-R

$$L_1 = \left[\begin{array}{cccccccc} 0 & 7 & 1 & 3 & 2 & 4 & 6 & 5 \\ 4 & 1 & 7 & 6 & 3 & 0 & 5 & 2 \\ 7 & 0 & 4 & 2 & 5 & 3 & 1 & 6 \\ 1 & 4 & 0 & 5 & 6 & 2 & 7 & 3 \\ 2 & 3 & 6 & 7 & 1 & 5 & 0 & 4 \\ \hline 5 & 2 & 3 & 1 & 7 & 6 & 4 & 0 \\ 3 & 6 & 5 & 0 & 4 & 7 & 2 & 1 \\ 6 & 5 & 2 & 4 & 0 & 1 & 3 & 7 \end{array}\right] = \left[\begin{array}{c} L_{1,1} \\ L_{1,2} \end{array}\right] \qquad L_2 = \left[\begin{array}{cccccccc} 0 & 4 & 2 & 3 & 1 & 6 & 5 & 7 \\ 7 & 6 & 3 & 2 & 5 & 4 & 1 & 0 \\ 5 & 3 & 1 & 6 & 0 & 2 & 7 & 4 \\ 1 & 0 & 5 & 4 & 3 & 7 & 2 & 6 \\ 2 & 1 & 0 & 7 & 4 & 5 & 6 & 3 \\ \hline 3 & 5 & 7 & 0 & 6 & 1 & 4 & 2 \\ 4 & 7 & 6 & 1 & 2 & 0 & 3 & 5 \\ 6 & 2 & 4 & 5 & 7 & 3 & 0 & 1 \end{array}\right] = \left[\begin{array}{c} L_{2,1} \\ L_{2,2} \end{array}\right]$$

Two orthogonal Latin Squares of order 8

Four corresponding nonsingular in (Z_2, +, x) matrices.

$$\mathbb{A}_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \quad \mathbb{A}_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathbb{A}_3 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix} \quad \mathbb{A}_4 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

NTNU
Innovation and Creativity

Specific design characteristics for EDON-R

Four nonsingular in (Z_2, +, x) matrices.

$$\mathbb{A}_1 = \begin{pmatrix} 1&1&1&0&1&0&0&1\\ 1&1&0&1&1&0&0&1\\ 1&1&0&0&1&0&1&1\\ 0&0&1&1&0&1&1&1\\ 0&1&1&1&0&1&1&0\\ 1&0&1&1&1&1&0&0\\ 1&1&0&0&0&1&1&1\\ 0&0&1&1&1&1&1&0 \end{pmatrix} \quad \mathbb{A}_2 = \begin{pmatrix} \mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}\\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}\\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}\\ \mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\ \mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}\\ \mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}\\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\ \mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1} \end{pmatrix}$$

$$\mathbb{A}_3 = \begin{pmatrix} 1&1&1&0&0&1&0&1\\ 1&1&0&1&1&0&1&0\\ 1&1&1&1&0&1&0&0\\ 0&0&1&1&1&0&1&1\\ 1&1&0&1&1&1&0&0\\ 0&0&1&0&1&1&1&1\\ 0&1&1&0&0&1&1&1\\ 1&0&0&1&1&0&1&1 \end{pmatrix} \quad \mathbb{A}_4 = \begin{pmatrix} \mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0}\\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}\\ \mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}\\ \mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}\\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}\\ \mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\ \mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\ \mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0} \end{pmatrix}$$

Specific design characteristics for EDON-R

Four nonsingular in (Z_2, +, x) matrices.

$$\mathbb{A}_1 = \begin{pmatrix} 1&1&1&0&1&0&0&1 \\ 1&1&0&1&1&0&0&1 \\ 1&1&0&0&1&0&1&1 \\ 0&0&1&1&0&1&1&1 \\ 0&1&1&1&0&1&1&0 \\ 1&0&1&1&1&1&0&0 \\ 1&1&0&0&0&1&1&1 \\ 0&0&1&1&1&1&1&0 \end{pmatrix} \quad \mathbb{A}_2 = \begin{pmatrix} \mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0} \\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0} \\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0} \\ \mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0} \\ \mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1} \\ \mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1} \\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0} \\ \mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1} \end{pmatrix}$$

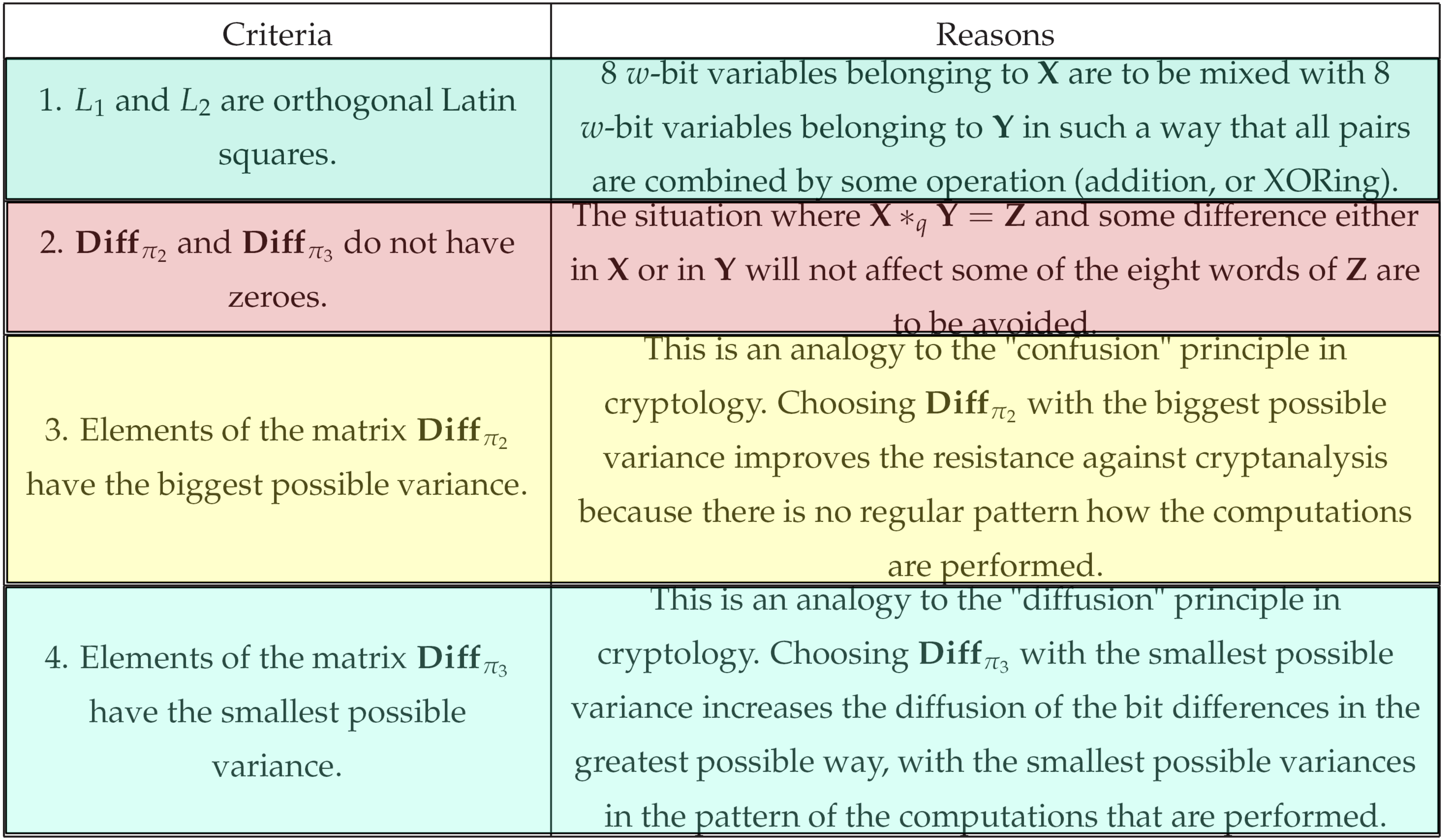
$$\mathbb{A}_3 = \begin{pmatrix} 1&1&1&0&0&1&0&1 \\ 1&1&0&1&1&0&1&0 \\ 1&1&1&1&0&1&0&0 \\ 0&0&1&1&1&0&1&1 \\ 1&1&0&1&1&1&0&0 \\ 0&0&1&0&1&1&1&1 \\ 0&1&1&0&0&1&1&1 \\ 1&0&0&1&1&0&1&1 \end{pmatrix} \quad \mathbb{A}_4 = \begin{pmatrix} \mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0} \\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1} \\ \mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1} \\ \mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0} \\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1} \\ \mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0} \\ \mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0} \\ \mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0} \end{pmatrix}$$

Two diffusion (bi-stochastic) matrices

$$\mathbf{Diff}_{\pi_2} = \left(\mathbb{A}_1 \cdot \mathbb{A}_2\right)^T = \begin{pmatrix} 2&3&2&2&1&2&1&2 \\ 1&2&1&3&2&2&2&2 \\ 2&1&2&2&3&1&2&2 \\ 2&1&2&2&2&2&2&2 \\ 1&2&2&2&2&2&1&3 \\ 3&2&2&1&2&2&2&1 \\ 2&2&2&1&2&2&3&1 \\ 2&2&2&2&1&2&2&2 \end{pmatrix}$$

$$\mathbf{Diff}_{\pi_3} = \left(\mathbb{A}_3 \cdot \mathbb{A}_4\right)^T = \begin{pmatrix} 1&2&2&2&2&2&2&2 \\ 2&1&2&2&2&2&2&2 \\ 2&2&1&2&2&2&2&2 \\ 2&2&2&1&2&2&2&2 \\ 2&2&2&2&1&2&2&2 \\ 2&2&2&2&2&1&2&2 \\ 2&2&2&2&2&2&1&2 \\ 2&2&2&2&2&2&2&1 \end{pmatrix}$$

Specific design characteristics for EDON-R



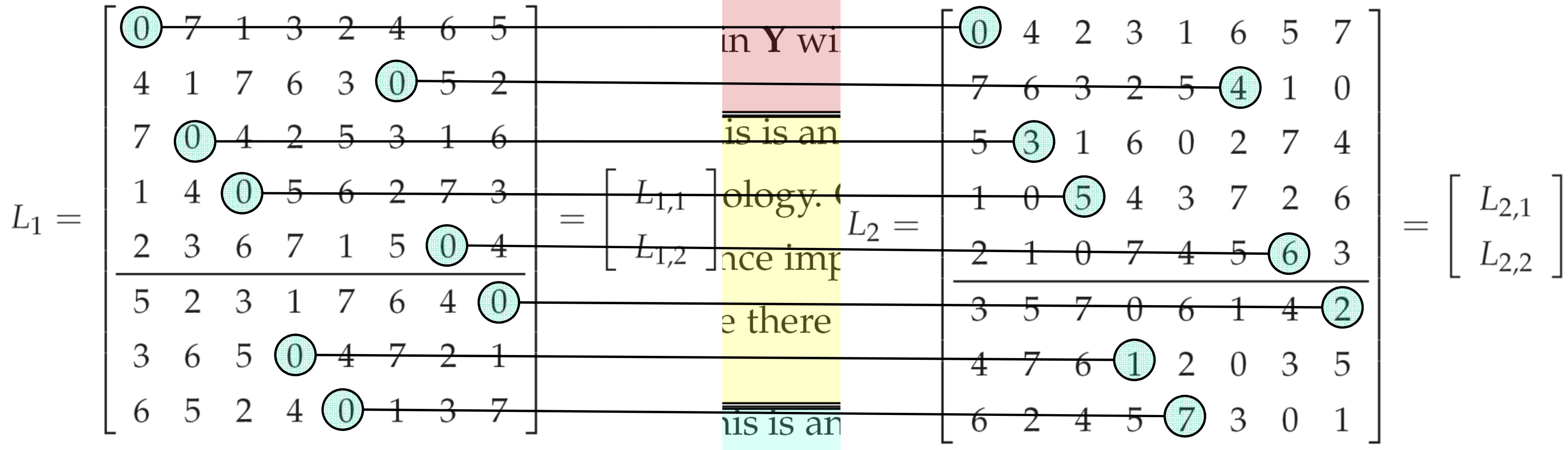
Criteria	Reasons
1. L_1 and L_2 are orthogonal Latin squares.	8 w-bit variables belonging to $\mathbf{X}$ are to be mixed with 8 w-bit variables belonging to $\mathbf{Y}$ in such a way that all pairs are combined by some operation (addition, or XORing).
2. $\mathbf{Diff}_{\pi_2}$ and $\mathbf{Diff}_{\pi_3}$ do not have zeroes.	The situation where $\mathbf{X} *_q \mathbf{Y} = \mathbf{Z}$ and some difference either in $\mathbf{X}$ or in $\mathbf{Y}$ will not affect some of the eight words of $\mathbf{Z}$ are to be avoided.
3. Elements of the matrix $\mathbf{Diff}_{\pi_2}$ have the biggest possible variance.	This is an analogy to the "confusion" principle in cryptology. Choosing $\mathbf{Diff}_{\pi_2}$ with the biggest possible variance improves the resistance against cryptanalysis because there is no regular pattern how the computations are performed.
4. Elements of the matrix $\mathbf{Diff}_{\pi_3}$ have the smallest possible variance.	This is an analogy to the "diffusion" principle in cryptology. Choosing $\mathbf{Diff}_{\pi_3}$ with the smallest possible variance increases the diffusion of the bit differences in the greatest possible way, with the smallest possible variances in the pattern of the computations that are performed.

Table 3.9: Criteria for choosing the Latin squares

Specific design characteristics for EDON-R

Criteria	Reasons
1. L_1 and L_2 are orthogonal Latin squares.	8 w-bit variables belonging to $\mathbf{X}$ are to be mixed with 8 w-bit variables belonging to $\mathbf{Y}$ in such a way that all pairs are combined by some operation (addition, or XORing).
2.	The situation where $\mathbf{X} *_q \mathbf{Y} = \mathbf{Z}$ and some difference either in $\mathbf{Y}$ wi e
3 ha	is is an ology. (nce imp e there
4. Elements of the matrix $\mathbf{Diff}_{\pi_3}$ have the smallest possible variance.	is is an cryptology. Choosing $\mathbf{Diff}_{\pi_3}$ with the smallest possible variance increases the diffusion of the bit differences in the greatest possible way, with the smallest possible variances in the pattern of the computations that are performed.

Table 3.9: Criteria for choosing the Latin squares



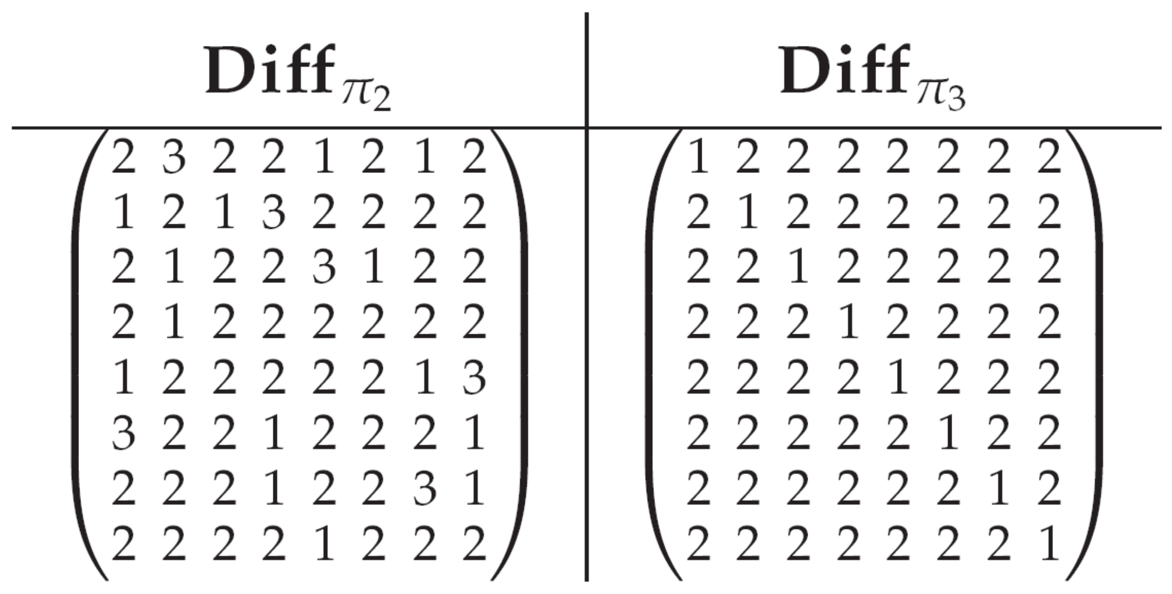
$$L_1 = \left[\begin{array}{cccccccc} \textcircled{0} & 7 & 1 & 3 & 2 & 4 & 6 & 5 \\ 4 & 1 & 7 & 6 & 3 & \textcircled{0} & 5 & 2 \\ 7 & \textcircled{0} & 4 & 2 & 5 & 3 & 1 & 6 \\ 1 & 4 & \textcircled{0} & 5 & 6 & 2 & 7 & 3 \\ 2 & 3 & 6 & 7 & 1 & 5 & \textcircled{0} & 4 \\ \hline 5 & 2 & 3 & 1 & 7 & 6 & 4 & \textcircled{0} \\ 3 & 6 & 5 & \textcircled{0} & 4 & 7 & 2 & 1 \\ 6 & 5 & 2 & 4 & \textcircled{0} & 1 & 3 & 7 \end{array}\right] = \left[\begin{array}{c} L_{1,1} \\ L_{1,2} \end{array}\right]$$

$$L_2 = \left[\begin{array}{cccccccc} \textcircled{0} & 4 & 2 & 3 & 1 & 6 & 5 & 7 \\ 7 & 6 & 3 & 2 & 5 & \textcircled{4} & 1 & 0 \\ 5 & \textcircled{3} & 1 & 6 & 0 & 2 & 7 & 4 \\ 1 & 0 & \textcircled{5} & 4 & 3 & 7 & 2 & 6 \\ 2 & 1 & 0 & 7 & 4 & 5 & \textcircled{6} & 3 \\ \hline 3 & 5 & 7 & 0 & 6 & 1 & 4 & \textcircled{2} \\ 4 & 7 & 6 & \textcircled{1} & 2 & 0 & 3 & 5 \\ 6 & 2 & 4 & 5 & \textcircled{7} & 3 & 0 & 1 \end{array}\right] = \left[\begin{array}{c} L_{2,1} \\ L_{2,2} \end{array}\right]$$

Specific design characteristics for EDON-R

Criteria	Reasons
1. L_1 and L_2 are orthogonal Latin squares.	8 w-bit variables belonging to $\mathbf{X}$ are to be mixed with 8 w-bit variables belonging to $\mathbf{Y}$ in such a way that all pairs are combined by some operation (addition, or XORing).
2. $\mathbf{Diff}_{\pi_2}$ and $\mathbf{Diff}_{\pi_3}$ do not have zeroes.	The situation where $\mathbf{X} *_q \mathbf{Y} = \mathbf{Z}$ and some difference either in $\mathbf{X}$ or in $\mathbf{Y}$ will not affect some of the eight words of $\mathbf{Z}$ are to be avoided.
3. Elements of have the bigges	n" principle in e biggest possible inst cryptanalysis v the computations
4. Elements of have the s va	n" principle in smallest possible it differences in the t possible variances in the pattern of the computations that are performed.

Table 3.9: Criteria for choosing the Latin squares



$\mathbf{Diff}_{\pi_2}$	$\mathbf{Diff}_{\pi_3}$
$\begin{pmatrix} 2&3&2&2&1&2&1&2\\ 1&2&1&3&2&2&2&2\\ 2&1&2&2&3&1&2&2\\ 2&1&2&2&2&2&2&2\\ 1&2&2&2&2&2&1&3\\ 3&2&2&1&2&2&2&1\\ 2&2&2&1&2&2&3&1\\ 2&2&2&2&1&2&2&2 \end{pmatrix}$	$\begin{pmatrix} 1&2&2&2&2&2&2&2\\ 2&1&2&2&2&2&2&2\\ 2&2&1&2&2&2&2&2\\ 2&2&2&1&2&2&2&2\\ 2&2&2&2&1&2&2&2\\ 2&2&2&2&2&1&2&2\\ 2&2&2&2&2&2&1&2\\ 2&2&2&2&2&2&2&1 \end{pmatrix}$

$$\mathbf{Diff}_{\pi_2}$$

$$\begin{pmatrix}
2 & 3 & 2 & 2 & 1 & 2 & 1 & 2 \\
1 & 2 & 1 & 3 & 2 & 2 & 2 & 2 \\
2 & 1 & 2 & 2 & 3 & 1 & 2 & 2 \\
2 & 1 & 2 & 2 & 2 & 2 & 2 & 2 \\
1 & 2 & 2 & 2 & 2 & 2 & 1 & 3 \\
3 & 2 & 2 & 1 & 2 & 2 & 2 & 1 \\
2 & 2 & 2 & 1 & 2 & 2 & 3 & 1 \\
2 & 2 & 2 & 2 & 1 & 2 & 2 & 2
\end{pmatrix}$$

sign characteristics for EDON-R

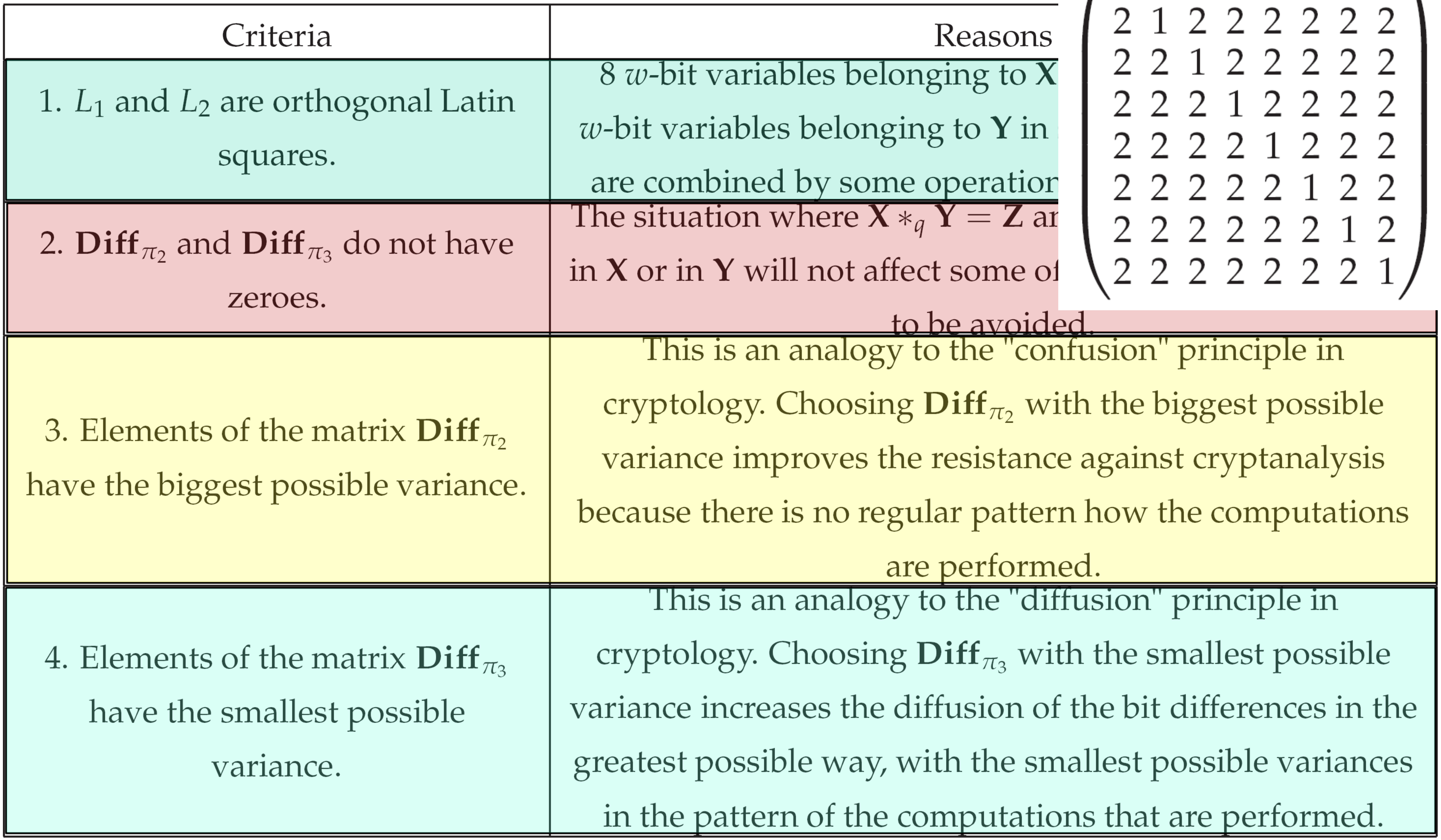
	Reasons
l Latin	8 w-bit variables belonging to $\mathbf{X}$ are to be mixed with 8 w-bit variables belonging to $\mathbf{Y}$ in such a way that all pairs are combined by some operation (addition, or XORing).
t have	The situation where $\mathbf{X} *_q \mathbf{Y} = \mathbf{Z}$ and some difference either in $\mathbf{X}$ or in $\mathbf{Y}$ will not affect some of the eight words of $\mathbf{Z}$ are to be avoided.
3. Elements of the matrix $\mathbf{Diff}_{\pi_2}$ have the biggest possible variance.	This is an analogy to the "confusion" principle in cryptology. Choosing $\mathbf{Diff}_{\pi_2}$ with the biggest possible variance improves the resistance against cryptanalysis because there is no regular pattern how the computations are performed.
4. Elements of the matrix $\mathbf{Diff}_{\pi_3}$ have the smallest possible variance.	This is an analogy to the "diffusion" principle in cryptology. Choosing $\mathbf{Diff}_{\pi_3}$ with the smallest possible variance increases the diffusion of the bit differences in the greatest possible way, with the smallest possible variances in the pattern of the computations that are performed.

Table 3.9: Criteria for choosing the Latin squares

Specific design characteristics for

$$\mathbf{Diff}_{\pi_3}$$

$$\begin{pmatrix} 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 1 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 1 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 1 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 1 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 1 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 \end{pmatrix}$$



Criteria	Reasons
1. L_1 and L_2 are orthogonal Latin squares.	8 w-bit variables belonging to $\mathbf{X}$ w-bit variables belonging to $\mathbf{Y}$ in are combined by some operation
2. $\mathbf{Diff}_{\pi_2}$ and $\mathbf{Diff}_{\pi_3}$ do not have zeroes.	The situation where $\mathbf{X} *_q \mathbf{Y} = \mathbf{Z}$ ar in $\mathbf{X}$ or in $\mathbf{Y}$ will not affect some of to be avoided.
3. Elements of the matrix $\mathbf{Diff}_{\pi_2}$ have the biggest possible variance.	This is an analogy to the "confusion" principle in cryptology. Choosing $\mathbf{Diff}_{\pi_2}$ with the biggest possible variance improves the resistance against cryptanalysis because there is no regular pattern how the computations are performed.
4. Elements of the matrix $\mathbf{Diff}_{\pi_3}$ have the smallest possible variance.	This is an analogy to the "diffusion" principle in cryptology. Choosing $\mathbf{Diff}_{\pi_3}$ with the smallest possible variance increases the diffusion of the bit differences in the greatest possible way, with the smallest possible variances in the pattern of the computations that are performed.

Table 3.9: Criteria for choosing the Latin squares

Specific design characteristics for EDON-R

Criteria	Reasons
1. L_1 and L_2 are orthogonal Latin squares.	8 w-bit variables belonging to $\mathbf{X}$ are to be mixed with 8 w-bit variables belonging to $\mathbf{Y}$ in such a way that all pairs are combined by some operation (addition, or XORing).
2. $\mathbf{Diff}_{\pi_2}$ and $\mathbf{Diff}_{\pi_3}$ do not have zeroes.	The situation where $\mathbf{X} *_q \mathbf{Y} = \mathbf{Z}$ and some difference either in $\mathbf{X}$ or in $\mathbf{Y}$ will not affect some of the eight words of $\mathbf{Z}$ are to be avoided.
3. Elements of the matrix $\mathbf{Diff}_{\pi_2}$ have the biggest possible variance.	This is an analogy to the "confusion" principle in cryptology. Choosing $\mathbf{Diff}_{\pi_2}$ with the biggest possible variance improves the resistance against cryptanalysis because there is no regular pattern how the computations are performed.
4. Elements of the matrix $\mathbf{Diff}_{\pi_3}$ have the smallest possible variance.	This is an analogy to the "diffusion" principle in cryptology. Choosing $\mathbf{Diff}_{\pi_3}$ with the smallest possible variance increases the diffusion of the bit differences in the greatest possible way, with the smallest possible variances in the pattern of the computations that are performed.

Table 3.9: Criteria for choosing the Latin squares

We took all 2165 main classes of orthogonal Latin Sauares of order 8 from Brendan McKay's web page http://cs.anu.edu.au/people/bdm/data/latin.html and searched trough $(8!)^2 \sim 2^{30.6}$ pairs of orthogonal isotopes. We found that Latin Squares that comply with all 4 criteria give diffusion matrices with maximal variance 19/63 and the minimal variance 1/9. We took the first such pair for EDON-R.

Specific design characteristics for EDON-R

Definition 12. Let $\mathbf{X}, \mathbf{X}', \mathbf{Y}, \mathbf{Y}' \in Q_q$ and let $\mathbf{\Delta_X} = \mathbf{X} \oplus \mathbf{X}'$ and $\mathbf{\Delta_Y} = \mathbf{Y} \oplus \mathbf{Y}'$ be two difference vectors. Let $\mathbf{Z} = \mathbf{X} *_q \mathbf{Y}$ and $\mathbf{Z}' = \mathbf{X}' *_q \mathbf{Y}'$. The vector $\mathcal{D}_{(\mathbf{\Delta_X}, \mathbf{\Delta_Y})} = (\delta_0, \ldots, \delta_7) \in (\mathbb{Z})^8$ is called *bit flip counter for the quasigroup operation* $*_q$, if every δ_i, $i = 0, \ldots, 7$ is a counter of the minimal number of bit flips that the quasigroup operation $*_q$ performs to transfer the value $\mathbf{Z}$ to the value $\mathbf{Z}'$.

Theorem 3: $\mathcal{D}_{(\mathbf{\Delta_X}, \mathbf{\Delta_Y})} = \mathbf{Diff}_{\pi_2} \cdot \mathbf{\Delta_X} + \mathbf{Diff}_{\pi_3} \cdot \mathbf{\Delta_Y}$

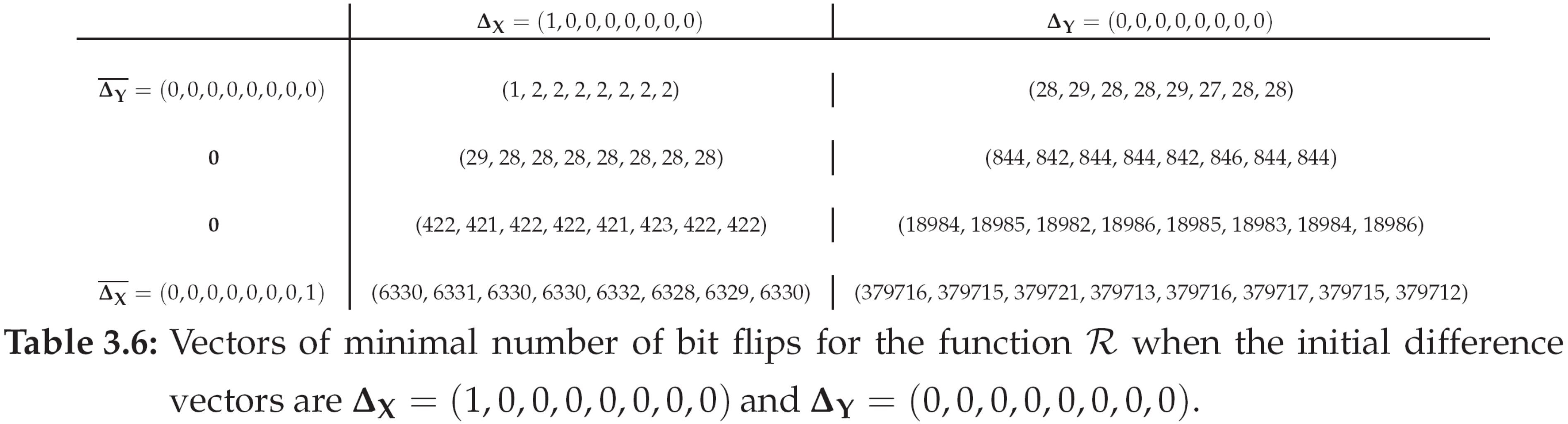
Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

	Δ_X	Δ_Y
$\overline{\Delta_Y}$	$\mathcal{D}_1 = \mathbf{Diff}_{\pi_2} \cdot \overline{\Delta_Y} + \mathbf{Diff}_{\pi_3} \cdot \Delta_X$	$\mathcal{D}_2 = \mathbf{Diff}_{\pi_2} \cdot \mathcal{D}_1 + \mathbf{Diff}_{\pi_3} \cdot \Delta_Y$
0	$\mathcal{D}_3 = \mathbf{Diff}_{\pi_2} \cdot 0 + \mathbf{Diff}_{\pi_3} \cdot \mathcal{D}_1$	$\mathcal{D}_4 = \mathbf{Diff}_{\pi_2} \cdot \mathcal{D}_3 + \mathbf{Diff}_{\pi_3} \cdot \mathcal{D}_2$
0	$\mathcal{D}_5 = \mathbf{Diff}_{\pi_2} \cdot \mathcal{D}_3 + \mathbf{Diff}_{\pi_3} \cdot 0$	$\mathcal{D}_6 = \mathbf{Diff}_{\pi_2} \cdot \mathcal{D}_4 + \mathbf{Diff}_{\pi_3} \cdot \mathcal{D}_5$
$\overline{\Delta_X}$	$\mathcal{D}_7 = \mathbf{Diff}_{\pi_2} \cdot \overline{\Delta_X} + \mathbf{Diff}_{\pi_3} \cdot \mathcal{D}_5$	$\mathcal{D}_8 = \mathbf{Diff}_{\pi_2} \cdot \mathcal{D}_7 + \mathbf{Diff}_{\pi_3} \cdot \mathcal{D}_6$

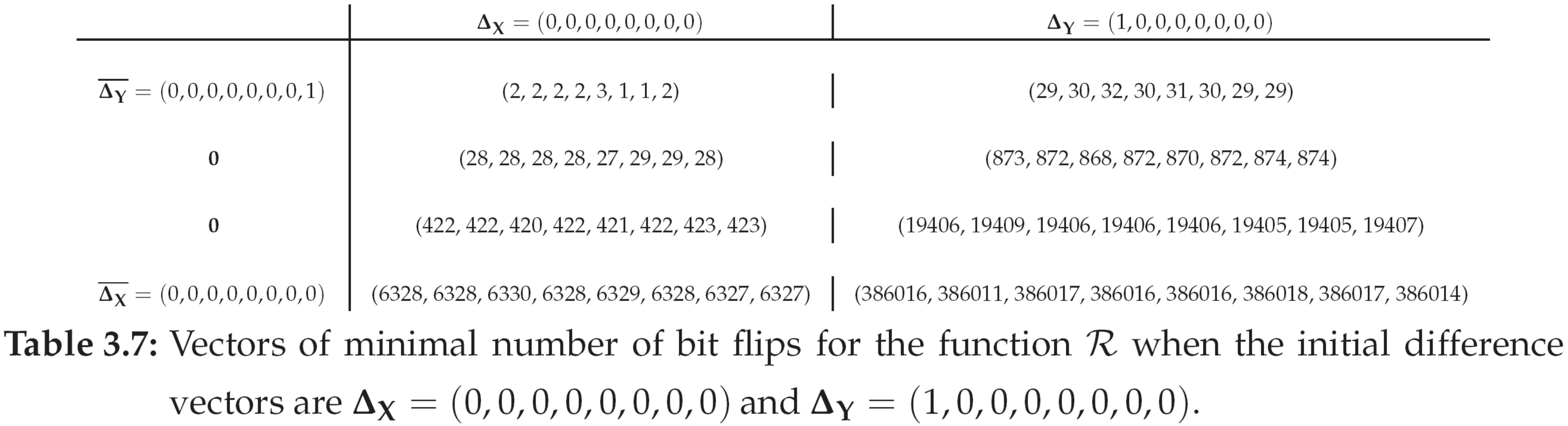
Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis



	$\Delta_X = (1,0,0,0,0,0,0,0)$	$\Delta_Y = (0,0,0,0,0,0,0,0)$
$\overline{\Delta_Y} = (0,0,0,0,0,0,0,0)$	(1, 2, 2, 2, 2, 2, 2, 2)	(28, 29, 28, 28, 29, 27, 28, 28)
$\mathbf{0}$	(29, 28, 28, 28, 28, 28, 28, 28)	(844, 842, 844, 844, 842, 846, 844, 844)
$\mathbf{0}$	(422, 421, 422, 422, 421, 423, 422, 422)	(18984, 18985, 18982, 18986, 18985, 18983, 18984, 18986)
$\overline{\Delta_X} = (0,0,0,0,0,0,0,1)$	(6330, 6331, 6330, 6330, 6332, 6328, 6329, 6330)	(379716, 379715, 379721, 379713, 379716, 379717, 379715, 379712)

Table 3.6: Vectors of minimal number of bit flips for the function $\mathcal{R}$ when the initial difference vectors are $\mathbf{\Delta_X} = (1,0,0,0,0,0,0,0)$ and $\mathbf{\Delta_Y} = (0,0,0,0,0,0,0,0)$.



	$\Delta_X = (0,0,0,0,0,0,0,0)$	$\Delta_Y = (1,0,0,0,0,0,0,0)$
$\overline{\Delta_Y} = (0,0,0,0,0,0,0,1)$	(2, 2, 2, 2, 3, 1, 1, 2)	(29, 30, 32, 30, 31, 30, 29, 29)
$\mathbf{0}$	(28, 28, 28, 28, 27, 29, 29, 28)	(873, 872, 868, 872, 870, 872, 874, 874)
$\mathbf{0}$	(422, 422, 420, 422, 421, 422, 423, 423)	(19406, 19409, 19406, 19406, 19406, 19405, 19405, 19407)
$\overline{\Delta_X} = (0,0,0,0,0,0,0,0)$	(6328, 6328, 6330, 6328, 6329, 6328, 6327, 6327)	(386016, 386011, 386017, 386016, 386016, 386018, 386017, 386014)

Table 3.7: Vectors of minimal number of bit flips for the function $\mathcal{R}$ when the initial difference vectors are $\mathbf{\Delta_X} = (0,0,0,0,0,0,0,0)$ and $\mathbf{\Delta_Y} = (1,0,0,0,0,0,0,0)$.

Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

	$\mathbf{\Delta_X} = (1,0,0,0,0,0,0,0)$	$\mathbf{\Delta_Y} = (0,0,0,0,0,0,0,0)$
$\overline{\mathbf{\Delta_Y}} = (0,0,0,0,0,0,0,0)$	(1, 2, 2, 2, 2, 2, 2, 2)	(28, 29, 28, 28, 29, 27, 28, 28)
0	(29, 28, 28, 28, 28, 28, 28, 28)	(844, 842, 844, 844, 842, 846, 844, 844)
0	(422, 421, 422, 422, 421, 423, 422, 422)	(18984, 18985, 18982, 18986, 18985, 18983, 18984, 18986)
$\overline{\mathbf{\Delta_X}} = (0,0,0,0,0,0,0,1)$	(6330, 6331, 6330, 6330, 6332, 6328, 6329, 6330)	(379716, 379715, 379721, 379713, 379716, 379717, 379715, 379712)

Table 3.

Note the variance of the elements!

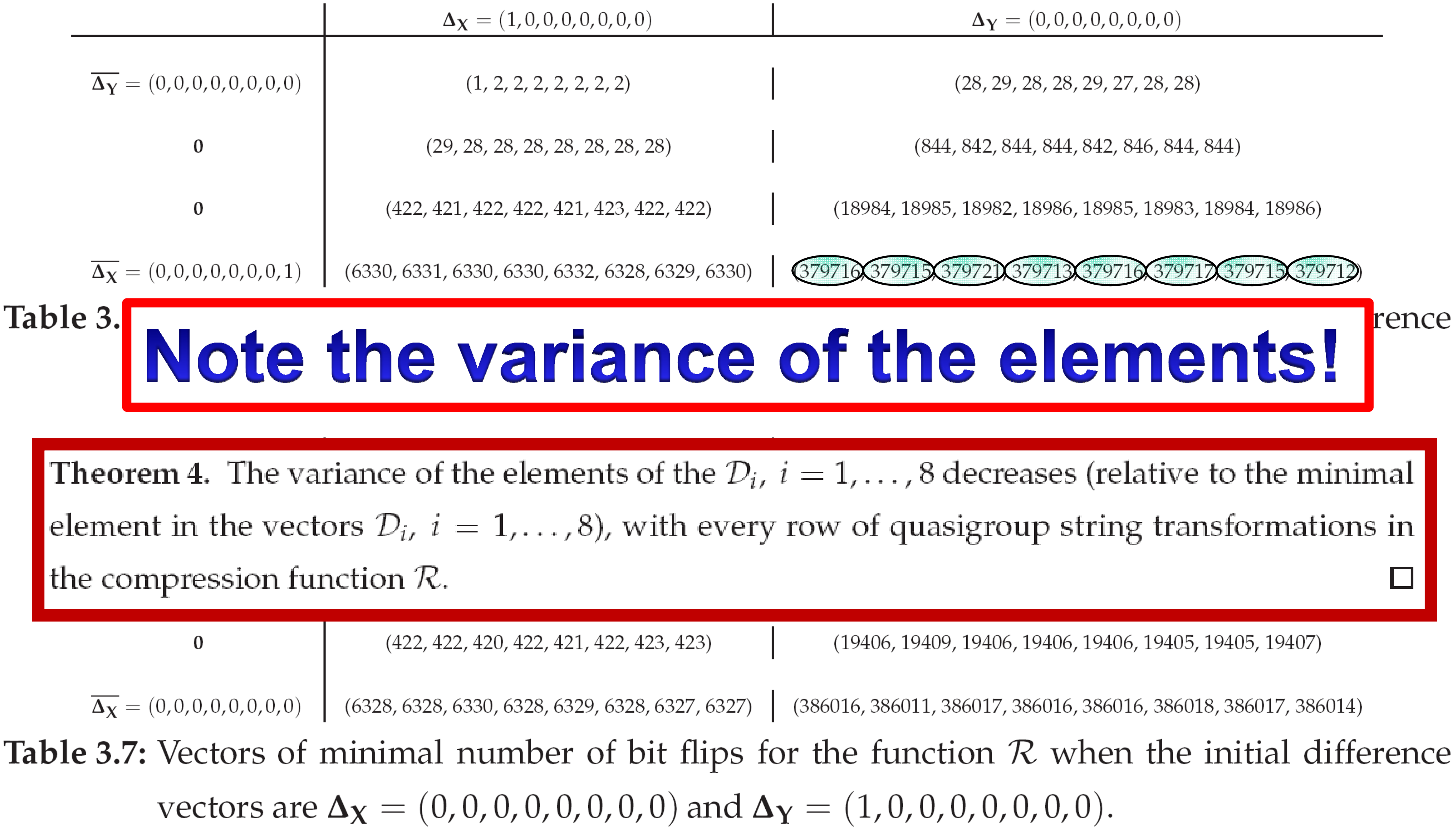
rence

	$\mathbf{\Delta_X} = (0,0,0,0,0,0,0,0)$	$\mathbf{\Delta_Y} = (1,0,0,0,0,0,0,0)$
$\overline{\mathbf{\Delta_Y}} = (0,0,0,0,0,0,0,1)$	(2, 2, 2, 2, 3, 1, 1, 2)	(29, 30, 32, 30, 31, 30, 29, 29)
0	(28, 28, 28, 28, 27, 29, 29, 28)	(873, 872, 868, 872, 870, 872, 874, 874)
0	(422, 422, 420, 422, 421, 422, 423, 423)	(19406, 19409, 19406, 19406, 19406, 19405, 19405, 19407)
$\overline{\mathbf{\Delta_X}} = (0,0,0,0,0,0,0,0)$	(6328, 6328, 6330, 6328, 6329, 6328, 6327, 6327)	(386016, 386011, 386017, 386016, 386016, 386018, 386017, 386014)

Table 3.7: Vectors of minimal number of bit flips for the function $\mathcal{R}$ when the initial difference vectors are $\mathbf{\Delta_X} = (0,0,0,0,0,0,0,0)$ and $\mathbf{\Delta_Y} = (1,0,0,0,0,0,0,0)$.

Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis



	$\Delta_X = (1,0,0,0,0,0,0,0)$	$\Delta_Y = (0,0,0,0,0,0,0,0)$
$\overline{\Delta_Y} = (0,0,0,0,0,0,0,0)$	(1, 2, 2, 2, 2, 2, 2, 2)	(28, 29, 28, 28, 29, 27, 28, 28)
0	(29, 28, 28, 28, 28, 28, 28, 28)	(844, 842, 844, 844, 842, 846, 844, 844)
0	(422, 421, 422, 422, 421, 423, 422, 422)	(18984, 18985, 18982, 18986, 18985, 18983, 18984, 18986)
$\overline{\Delta_X} = (0,0,0,0,0,0,0,1)$	(6330, 6331, 6330, 6330, 6332, 6328, 6329, 6330)	(379716, 379715, 379721, 379713, 379716, 379717, 379715, 379712)

Table 3. rence

Note the variance of the elements!

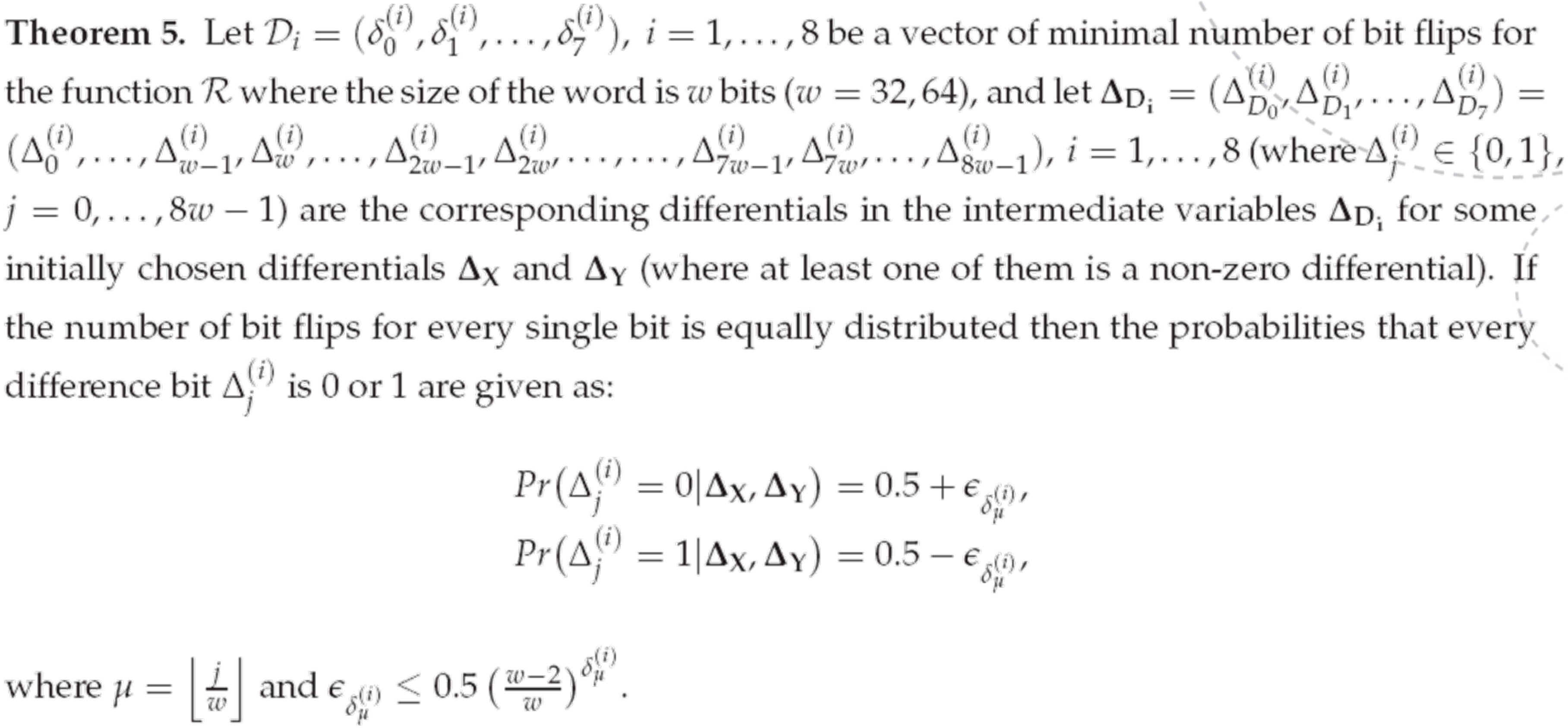
Theorem 4. The variance of the elements of the $\mathcal{D}_i$, $i = 1, \ldots, 8$ decreases (relative to the minimal element in the vectors $\mathcal{D}_i$, $i = 1, \ldots, 8$), with every row of quasigroup string transformations in the compression function $\mathcal{R}$. ☐

0	(422, 422, 420, 422, 421, 422, 423, 423)	(19406, 19409, 19406, 19406, 19406, 19405, 19405, 19407)
$\overline{\Delta_X} = (0,0,0,0,0,0,0,0)$	(6328, 6328, 6330, 6328, 6329, 6328, 6327, 6327)	(386016, 386011, 386017, 386016, 386016, 386018, 386017, 386014)

Table 3.7: Vectors of minimal number of bit flips for the function $\mathcal{R}$ when the initial difference vectors are $\mathbf{\Delta_X} = (0,0,0,0,0,0,0,0)$ and $\mathbf{\Delta_Y} = (1,0,0,0,0,0,0,0)$.

Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis



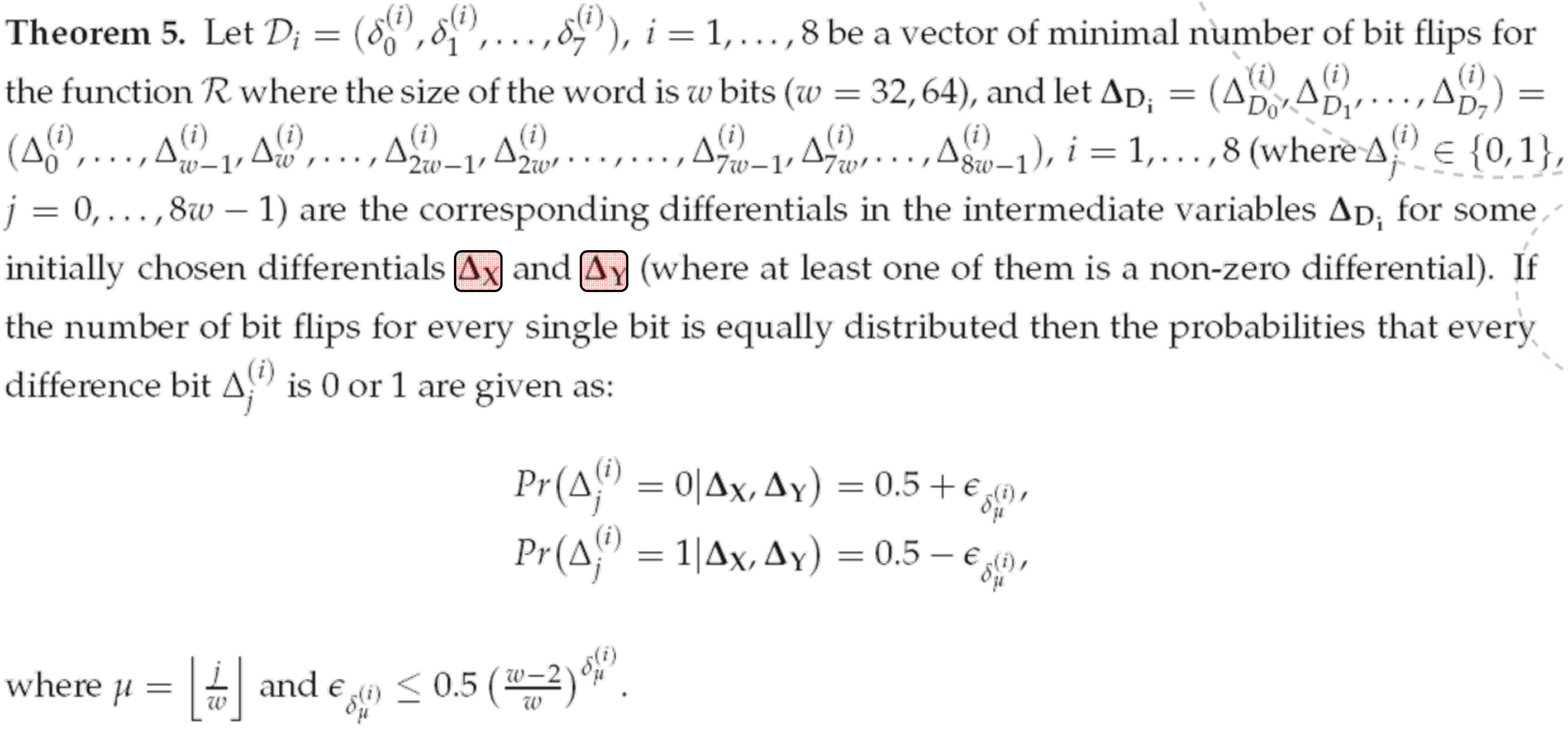
Theorem 5. Let $\mathcal{D}_i = (\delta_0^{(i)}, \delta_1^{(i)}, \ldots, \delta_7^{(i)})$, $i = 1, \ldots, 8$ be a vector of minimal number of bit flips for the function $\mathcal{R}$ where the size of the word is w bits ($w = 32, 64$), and let $\mathbf{\Delta_{D_i}} = (\Delta_{D_0}^{(i)}, \Delta_{D_1}^{(i)}, \ldots, \Delta_{D_7}^{(i)}) = (\Delta_0^{(i)}, \ldots, \Delta_{w-1}^{(i)}, \Delta_w^{(i)}, \ldots, \Delta_{2w-1}^{(i)}, \Delta_{2w}^{(i)}, \ldots, \ldots, \Delta_{7w-1}^{(i)}, \Delta_{7w}^{(i)}, \ldots, \Delta_{8w-1}^{(i)})$, $i = 1, \ldots, 8$ (where $\Delta_j^{(i)} \in \{0, 1\}$, $j = 0, \ldots, 8w-1$) are the corresponding differentials in the intermediate variables $\mathbf{\Delta_{D_i}}$ for some initially chosen differentials $\mathbf{\Delta_X}$ and $\mathbf{\Delta_Y}$ (where at least one of them is a non-zero differential). If the number of bit flips for every single bit is equally distributed then the probabilities that every difference bit $\Delta_j^{(i)}$ is 0 or 1 are given as:

$$Pr(\Delta_j^{(i)} = 0 | \mathbf{\Delta_X}, \mathbf{\Delta_Y}) = 0.5 + \epsilon_{\delta_\mu^{(i)}},$$
$$Pr(\Delta_j^{(i)} = 1 | \mathbf{\Delta_X}, \mathbf{\Delta_Y}) = 0.5 - \epsilon_{\delta_\mu^{(i)}},$$

where $\mu = \left\lfloor \frac{j}{w} \right\rfloor$ and $\epsilon_{\delta_\mu^{(i)}} \leq 0.5 \left(\frac{w-2}{w}\right)^{\delta_\mu^{(i)}}$.

Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis



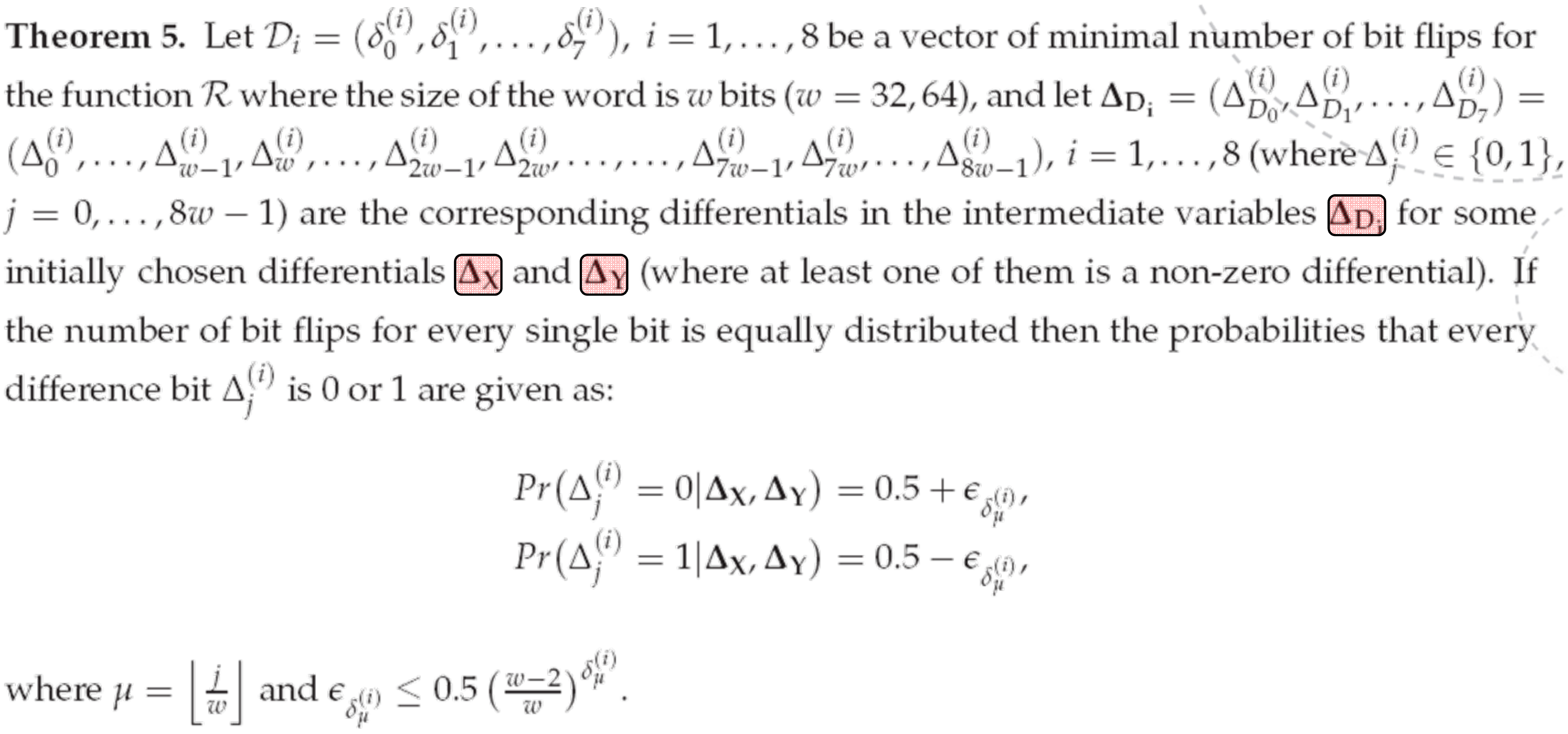
Theorem 5. Let $\mathcal{D}_i = (\delta_0^{(i)}, \delta_1^{(i)}, \ldots, \delta_7^{(i)})$, $i = 1, \ldots, 8$ be a vector of minimal number of bit flips for the function $\mathcal{R}$ where the size of the word is w bits ($w = 32, 64$), and let $\mathbf{\Delta_{D_i}} = (\Delta_{D_0}^{(i)}, \Delta_{D_1}^{(i)}, \ldots, \Delta_{D_7}^{(i)}) = (\Delta_0^{(i)}, \ldots, \Delta_{w-1}^{(i)}, \Delta_w^{(i)}, \ldots, \Delta_{2w-1}^{(i)}, \Delta_{2w}^{(i)}, \ldots, \ldots, \Delta_{7w-1}^{(i)}, \Delta_{7w}^{(i)}, \ldots, \Delta_{8w-1}^{(i)})$, $i = 1, \ldots, 8$ (where $\Delta_j^{(i)} \in \{0, 1\}$, $j = 0, \ldots, 8w - 1$) are the corresponding differentials in the intermediate variables $\mathbf{\Delta_{D_i}}$ for some initially chosen differentials $\boxed{\mathbf{\Delta_X}}$ and $\boxed{\mathbf{\Delta_Y}}$ (where at least one of them is a non-zero differential). If the number of bit flips for every single bit is equally distributed then the probabilities that every difference bit $\Delta_j^{(i)}$ is 0 or 1 are given as:

$$Pr(\Delta_j^{(i)} = 0 | \mathbf{\Delta_X}, \mathbf{\Delta_Y}) = 0.5 + \epsilon_{\delta_\mu^{(i)}},$$
$$Pr(\Delta_j^{(i)} = 1 | \mathbf{\Delta_X}, \mathbf{\Delta_Y}) = 0.5 - \epsilon_{\delta_\mu^{(i)}},$$

where $\mu = \left\lfloor \frac{j}{w} \right\rfloor$ and $\epsilon_{\delta_\mu^{(i)}} \le 0.5 \left(\frac{w-2}{w}\right)^{\delta_\mu^{(i)}}$.

Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis



Theorem 5. Let $\mathcal{D}_i = (\delta_0^{(i)}, \delta_1^{(i)}, \ldots, \delta_7^{(i)})$, $i = 1, \ldots, 8$ be a vector of minimal number of bit flips for the function $\mathcal{R}$ where the size of the word is w bits ($w = 32, 64$), and let $\mathbf{\Delta_{D_i}} = (\Delta_{D_0}^{(i)}, \Delta_{D_1}^{(i)}, \ldots, \Delta_{D_7}^{(i)}) = (\Delta_0^{(i)}, \ldots, \Delta_{w-1}^{(i)}, \Delta_w^{(i)}, \ldots, \Delta_{2w-1}^{(i)}, \Delta_{2w}^{(i)}, \ldots, \ldots, \Delta_{7w-1}^{(i)}, \Delta_{7w}^{(i)}, \ldots, \Delta_{8w-1}^{(i)})$, $i = 1, \ldots, 8$ (where $\Delta_j^{(i)} \in \{0, 1\}$, $j = 0, \ldots, 8w - 1$) are the corresponding differentials in the intermediate variables $\boxed{\mathbf{\Delta_{D_i}}}$ for some initially chosen differentials $\boxed{\mathbf{\Delta_X}}$ and $\boxed{\mathbf{\Delta_Y}}$ (where at least one of them is a non-zero differential). If the number of bit flips for every single bit is equally distributed then the probabilities that every difference bit $\Delta_j^{(i)}$ is 0 or 1 are given as:

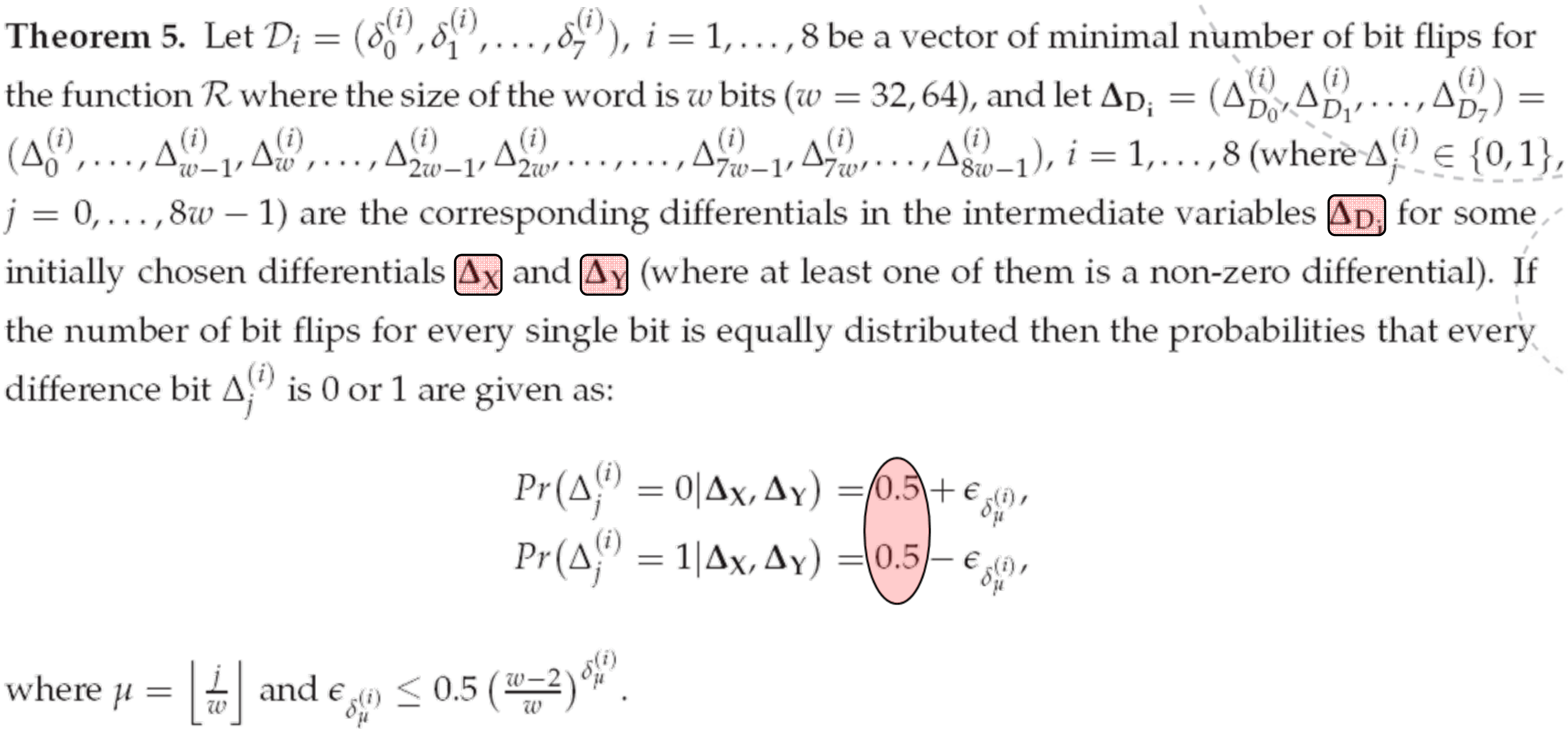
$$Pr(\Delta_j^{(i)} = 0 | \mathbf{\Delta_X}, \mathbf{\Delta_Y}) = 0.5 + \epsilon_{\delta_\mu^{(i)}},$$
$$Pr(\Delta_j^{(i)} = 1 | \mathbf{\Delta_X}, \mathbf{\Delta_Y}) = 0.5 - \epsilon_{\delta_\mu^{(i)}},$$

where $\mu = \left\lfloor \frac{j}{w} \right\rfloor$ and $\epsilon_{\delta_\mu^{(i)}} \leq 0.5 \left(\frac{w-2}{w}\right)^{\delta_\mu^{(i)}}$.

NTNU
Innovation and Creativity

Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis



Theorem 5. Let $\mathcal{D}_i = (\delta_0^{(i)}, \delta_1^{(i)}, \ldots, \delta_7^{(i)})$, $i = 1, \ldots, 8$ be a vector of minimal number of bit flips for the function $\mathcal{R}$ where the size of the word is w bits ($w = 32, 64$), and let $\mathbf{\Delta_{D_i}} = (\Delta_{D_0}^{(i)}, \Delta_{D_1}^{(i)}, \ldots, \Delta_{D_7}^{(i)}) = (\Delta_0^{(i)}, \ldots, \Delta_{w-1}^{(i)}, \Delta_w^{(i)}, \ldots, \Delta_{2w-1}^{(i)}, \Delta_{2w}^{(i)}, \ldots, \ldots, \Delta_{7w-1}^{(i)}, \Delta_{7w}^{(i)}, \ldots, \Delta_{8w-1}^{(i)})$, $i = 1, \ldots, 8$ (where $\Delta_j^{(i)} \in \{0, 1\}$, $j = 0, \ldots, 8w - 1$) are the corresponding differentials in the intermediate variables $\boxed{\mathbf{\Delta_{D_i}}}$ for some initially chosen differentials $\boxed{\mathbf{\Delta_X}}$ and $\boxed{\mathbf{\Delta_Y}}$ (where at least one of them is a non-zero differential). If the number of bit flips for every single bit is equally distributed then the probabilities that every difference bit $\Delta_j^{(i)}$ is 0 or 1 are given as:

$$Pr(\Delta_j^{(i)} = 0 | \mathbf{\Delta_X}, \mathbf{\Delta_Y}) = 0.5 + \epsilon_{\delta_\mu^{(i)}},$$

$$Pr(\Delta_j^{(i)} = 1 | \mathbf{\Delta_X}, \mathbf{\Delta_Y}) = 0.5 - \epsilon_{\delta_\mu^{(i)}},$$

where $\mu = \left\lfloor \frac{j}{w} \right\rfloor$ and $\epsilon_{\delta_\mu^{(i)}} \leq 0.5 \left(\frac{w-2}{w}\right)^{\delta_\mu^{(i)}}$.

Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis

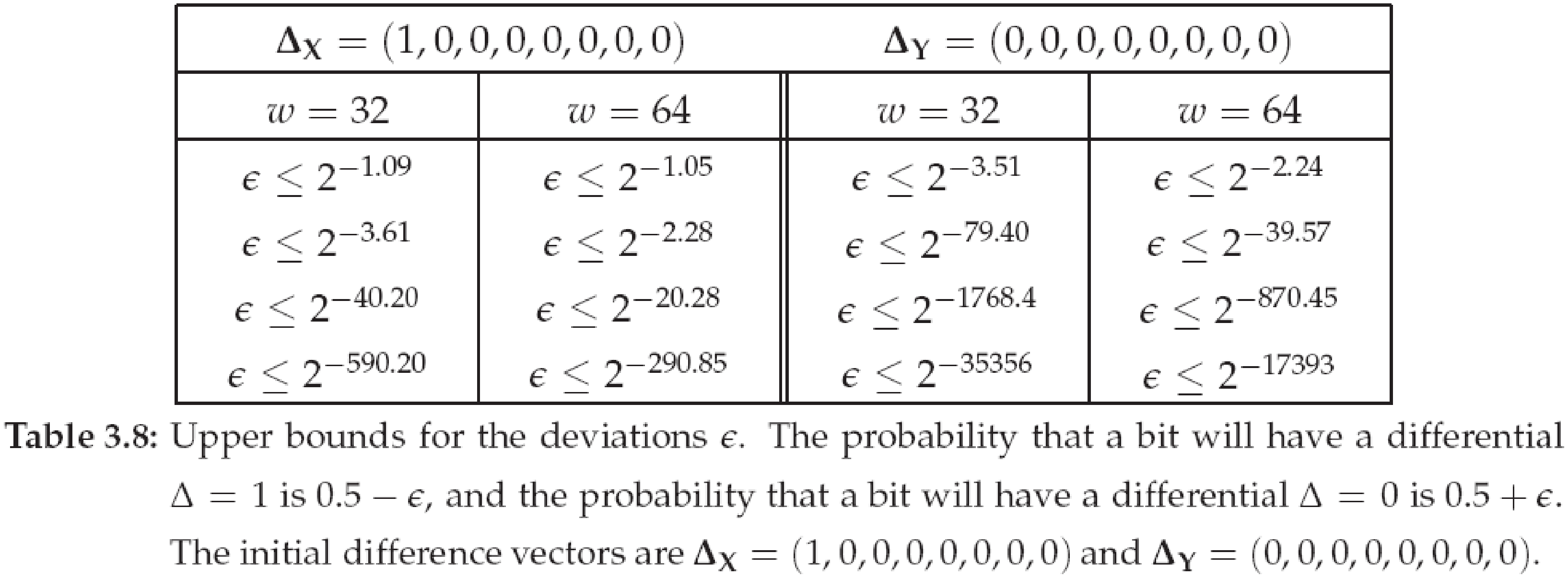
Theorem 5. Let $\mathcal{D}_i = (\delta_0^{(i)}, \delta_1^{(i)}, \ldots, \delta_7^{(i)})$, $i = 1, \ldots, 8$ be a vector of minimal number of bit flips for the function $\mathcal{R}$ where the size of the word is w bits ($w = 32, 64$), and let $\mathbf{\Delta_{D_i}} = (\Delta_{D_0}^{(i)}, \Delta_{D_1}^{(i)}, \ldots, \Delta_{D_7}^{(i)}) = (\Delta_0^{(i)}, \ldots, \Delta_{w-1}^{(i)}, \Delta_w^{(i)}, \ldots, \Delta_{2w-1}^{(i)}, \Delta_{2w}^{(i)}, \ldots, \ldots, \Delta_{7w-1}^{(i)}, \Delta_{7w}^{(i)}, \ldots, \Delta_{8w-1}^{(i)})$, $i = 1, \ldots, 8$ (where $\Delta_j^{(i)} \in \{0, 1\}$, $j = 0, \ldots, 8w-1$) are the corresponding differentials in the intermediate variables $\boxed{\mathbf{\Delta_{D_i}}}$ for some initially chosen differentials $\boxed{\mathbf{\Delta_X}}$ and $\boxed{\mathbf{\Delta_Y}}$ (where at least one of them is a non-zero differential). If the number of bit flips for every single bit is equally distributed then the probabilities that every difference bit $\Delta_j^{(i)}$ is 0 or 1 are given as:

$$Pr(\Delta_j^{(i)} = 0 | \mathbf{\Delta_X}, \mathbf{\Delta_Y}) = 0.5 + \epsilon_{\delta_\mu^{(i)}},$$
$$Pr(\Delta_j^{(i)} = 1 | \mathbf{\Delta_X}, \mathbf{\Delta_Y}) = 0.5 - \epsilon_{\delta_\mu^{(i)}},$$

where $\mu = \left\lfloor \frac{j}{w} \right\rfloor$ and $\boxed{\epsilon_{\delta_\mu^{(i)}} \leq 0.5 \left(\frac{w-2}{w}\right)^{\delta_\mu^{(i)}}.}$

Specific design characteristics for EDON-R

EDON-R is provably resistant against differential cryptanalysis



$\Delta_X = (1,0,0,0,0,0,0,0)$		$\Delta_Y = (0,0,0,0,0,0,0,0)$	
$w = 32$	$w = 64$	$w = 32$	$w = 64$
$\epsilon \leq 2^{-1.09}$	$\epsilon \leq 2^{-1.05}$	$\epsilon \leq 2^{-3.51}$	$\epsilon \leq 2^{-2.24}$
$\epsilon \leq 2^{-3.61}$	$\epsilon \leq 2^{-2.28}$	$\epsilon \leq 2^{-79.40}$	$\epsilon \leq 2^{-39.57}$
$\epsilon \leq 2^{-40.20}$	$\epsilon \leq 2^{-20.28}$	$\epsilon \leq 2^{-1768.4}$	$\epsilon \leq 2^{-870.45}$
$\epsilon \leq 2^{-590.20}$	$\epsilon \leq 2^{-290.85}$	$\epsilon \leq 2^{-35356}$	$\epsilon \leq 2^{-17393}$

Table 3.8: Upper bounds for the deviations ϵ. The probability that a bit will have a differential $\Delta = 1$ is $0.5 - \epsilon$, and the probability that a bit will have a differential $\Delta = 0$ is $0.5 + \epsilon$. The initial difference vectors are $\Delta_X = (1,0,0,0,0,0,0,0)$ and $\Delta_Y = (0,0,0,0,0,0,0,0)$.

Specific design characteristics for EDON-R

EDON-R has double size chaining (pipe) values

- For n=224, 256, chaining value has 512 bits
- For n=384, 512, chaining value has 1024 bits

- Gives resistance against length-extension attack
- Gives resistance against multi-collision attack

Known attacks on EDON-R

1. **Khovratovic and Nikolic**
   - Free-start collisions in Edon-R
   - Using free-start collisions to launch preimage attack with TIME ~ $O(2^{2n/3})$ and MEMORY ~ $O(2^{2n/3})$ i.e. the attack has this property:

$$\mathbf{TIME * MEMORY > 2^{n + n/3} >> 2^n}$$

2. **Klima:** EDON-R is **"almost"** as ordinary strengthened MD design.
   - That **"almost"** is in the small additional factor of 2^{65} to the generic multicollision attack that comes from the Merkle-Damgård strengthening.

NTNU
Innovation and Creativity

Known attacks on EDON-R

1. **Khovratovic and Nikolic**
    - Free-start collisions in Edon-R
    - Using free-start collisions to launch preimage attack with TIME ~ O($2^{2n/3}$) and MEMORY ~ O($2^{2n/3}$) i.e. the attack has this property:
    TIME * MEMORY > $2^{n + n/3}$ >> 2^n

2. **Klima:** EDON-R is **"almost"** as ordinary strengthened MD design.
    - That **"almost"** is in the small additional factor of 2^{65} to the generic multicollision attack that comes from the Merkle-Damgård strengthening.

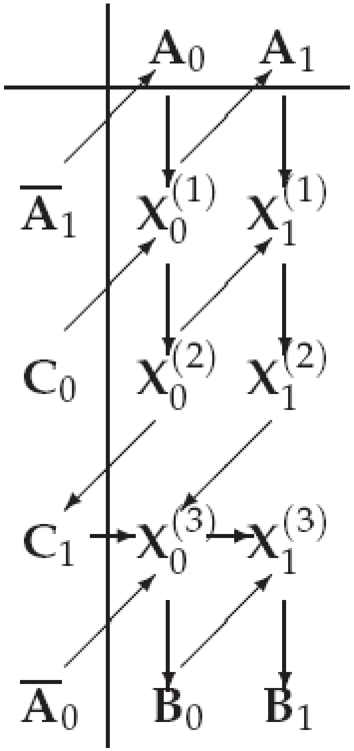
Idea to defend from both attacks without changing anything in the definition of the compression function

Make the Merkle-Damgård strengthening of EDON-R to be 129 bits (instead of the current 65 bit strengthening).

Are there one-way bijections embedded in EDON-R?

Example:

*	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

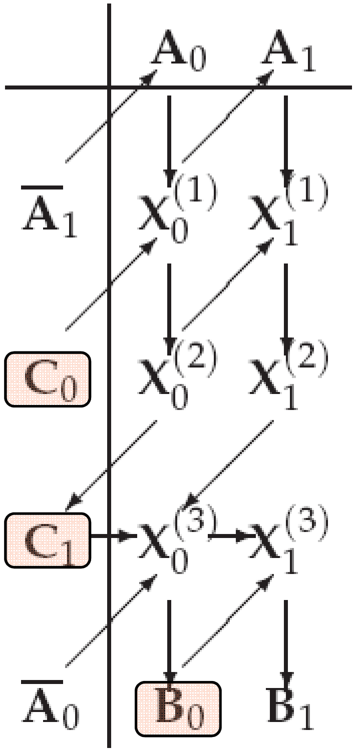


Are there one-way bijections embedded in EDON-R?

Example:

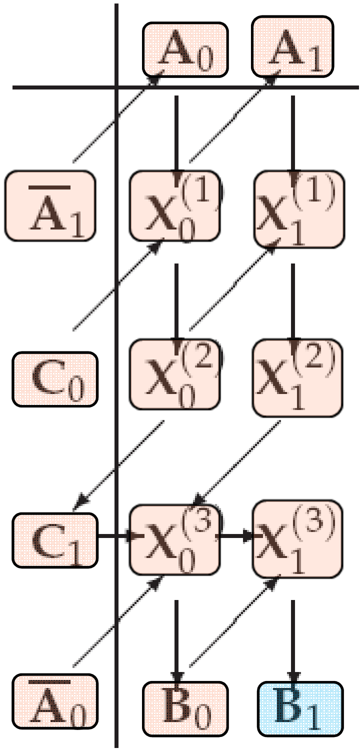
*	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

1. Fix $C_0=1$, $C_1=0$, $B_0=2$,



Are there one-way bijections embedded in EDON-R?

Example:

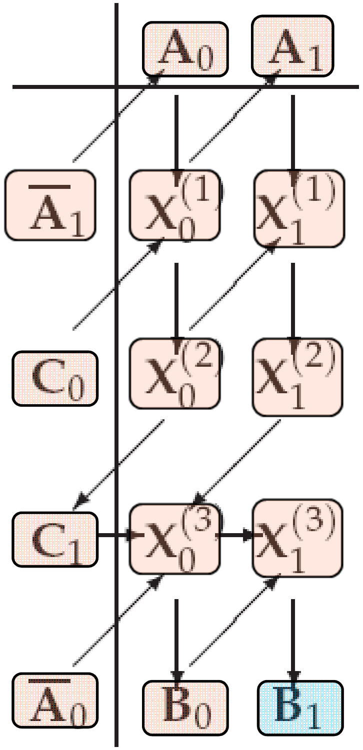


*	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

1. Fix $C_0=1$, $C_1=0$, $B_0=2$,
2. For every A_0 in {0,1,2,3}, compute:
    1. $X_0^{(3)}$,
    2. $X_0^{(2)}$,
    3. $X_0^{(1)}$,
    4. A_1,
    5. $X_1^{(1)}$,
    6. $X_1^{(2)}$,
    7. $X_1^{(3)}$,
    8. B_1,

Are there one-way bijections embedded in EDON-R?

Example:



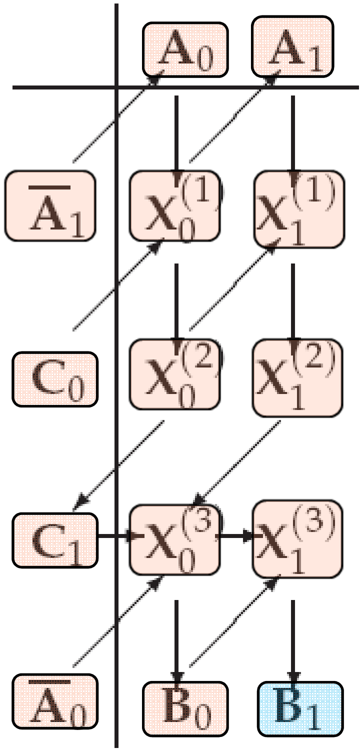
*	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

1. Fix $C_0=1$, $C_1=0$, $B_0=2$,
2. For every A_0 in {0,1,2,3}, compute:
   1. $X_0^{(3)}$,
   2. $X_0^{(2)}$,
   3. $X_0^{(1)}$,

1. **The mapping: $A_0 \rightarrow B_1$ is a bijection.**
2. **Knowing A_0, it is easy to compute B_1.**
3. **However: Knowing B_1, it is "hard" to find A_0.**
4. **For tiny quasigroups of order 4 we found that 144 quasigroups. give bijections for every value of C_0, C_1 and B_0.**

Are there one-way bijections embedded in EDON-R?

Example:



*	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

1. Fix $C_0=1$, $C_1=0$, $B_0=2$,
2. For every A_0 in {0,1,2,3}, compute:
   1. $X_0^{(3)}$,
   2. $X_0^{(2)}$,
   3. $X_0^{(1)}$

s.

Hypothesis: For certain values of C_0, C_1, B_0, one-way bijections can be defined by EDON-R compression function.

SW/HW performance and memory requirements

Software performances of the optimized C implementation on the NIST reference platform

Intel C++ v11.0.66, in 64-bit mode
EDON-R 224/256 achieves **4.54 cycles/byte**

Intel C++ v11.0.66, in 64-bit mode
EDON-R 384/512 achieves **2.29 cycles/byte**

HW – gate count

EDON-R 224/256, ~13,000 gates

EDON-R 384/512, ~25,000 gates

Memory requirements

EDON-R 224/256 needs **256 bytes**

EDON-R 384/512 needs **512 bytes**

8-bit MCU (ATmega16, ATmega406)

EDON-R 224/256, compiled C code produces ~6KB of machine instructions, speed 616 cycles/bytes

EDON-R 384/512, compiled C code produces ~38KB of machine instructions, speed 1857 cycles/bytes

NTNU
Innovation and Creativity

Thank you for your attention!

NTNU
Innovation and Creativity