Lesamnta: A Family of Hash Functions

First SHA-3 Candidate Conference

25 Feb 2009

Shoichi HIROSE

University of Fukui

Hidenori KUWAKADO

Kobe University

Hirotaka YOSHIDA

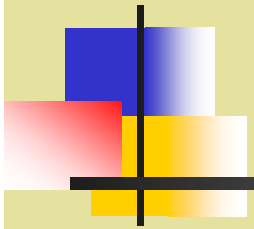
Systems Development Laboratory., Hitachi, Ltd.

Overview

- Design principle
- Specification
- Preliminary analysis
- Performance figures
- Conclusion
  - What's special about Lesamnta

Design principle of Lesamnta

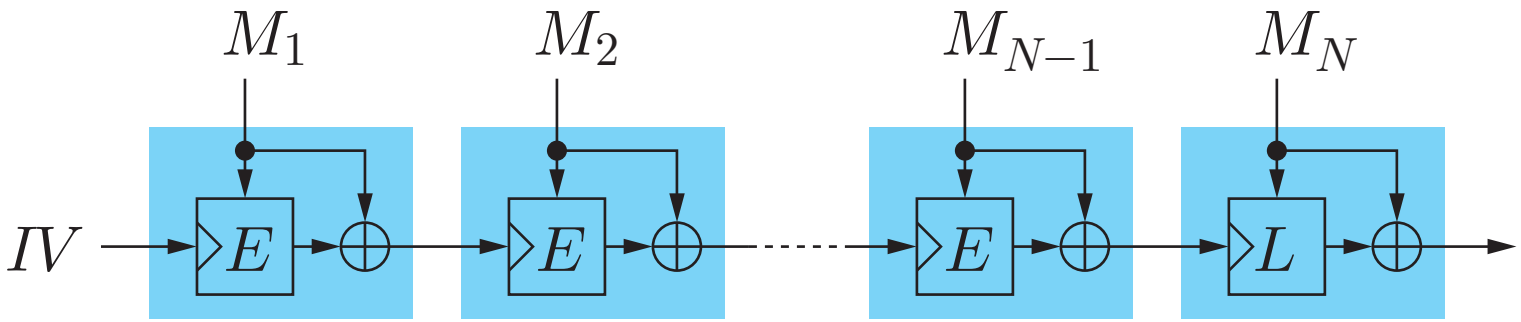
- Support 224/256/384/512-bit hash length
  - Security
    - Provable security
      - Collision resistance, Preimage resistance
      - Resistance of length-extension attacks
      - HMAC Resistance
      - Indifferentiability from random oracle
    - Evaluate resistance against major known attacks
      - Resistance against Wang *et al*'s attacks on SHA-1
  - Performance
    - In software, efficiently implemented on 8/16/32/64-bit CPU's
    - In hardware, implementation with small number of gate count or fast implementation is possible



Specifications of Lesamnta-256/512

Block-cipher-based construction

- Domain extension
  - Strengthened MD with an output function (MDO)
  - The output function prevents length extension attacks
- Compression function and output function
  - Matyas-Meyer-Oseas mode
  - Enables to reduce the security of the hash function to the security of the underlying block cipher

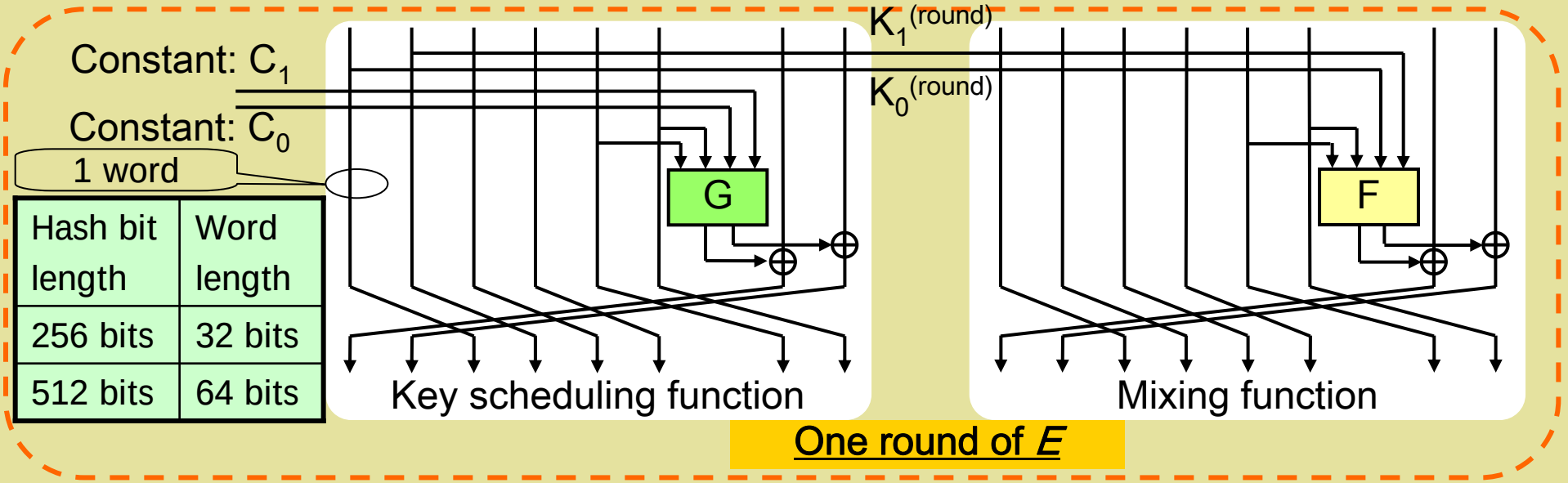


The construction of Lesmanta

- *n*-bit message block and *n*-bit chaining variable for Lesamnta-*n* (*n*= 256 or 512)

Block ciphers: *E* and *L*

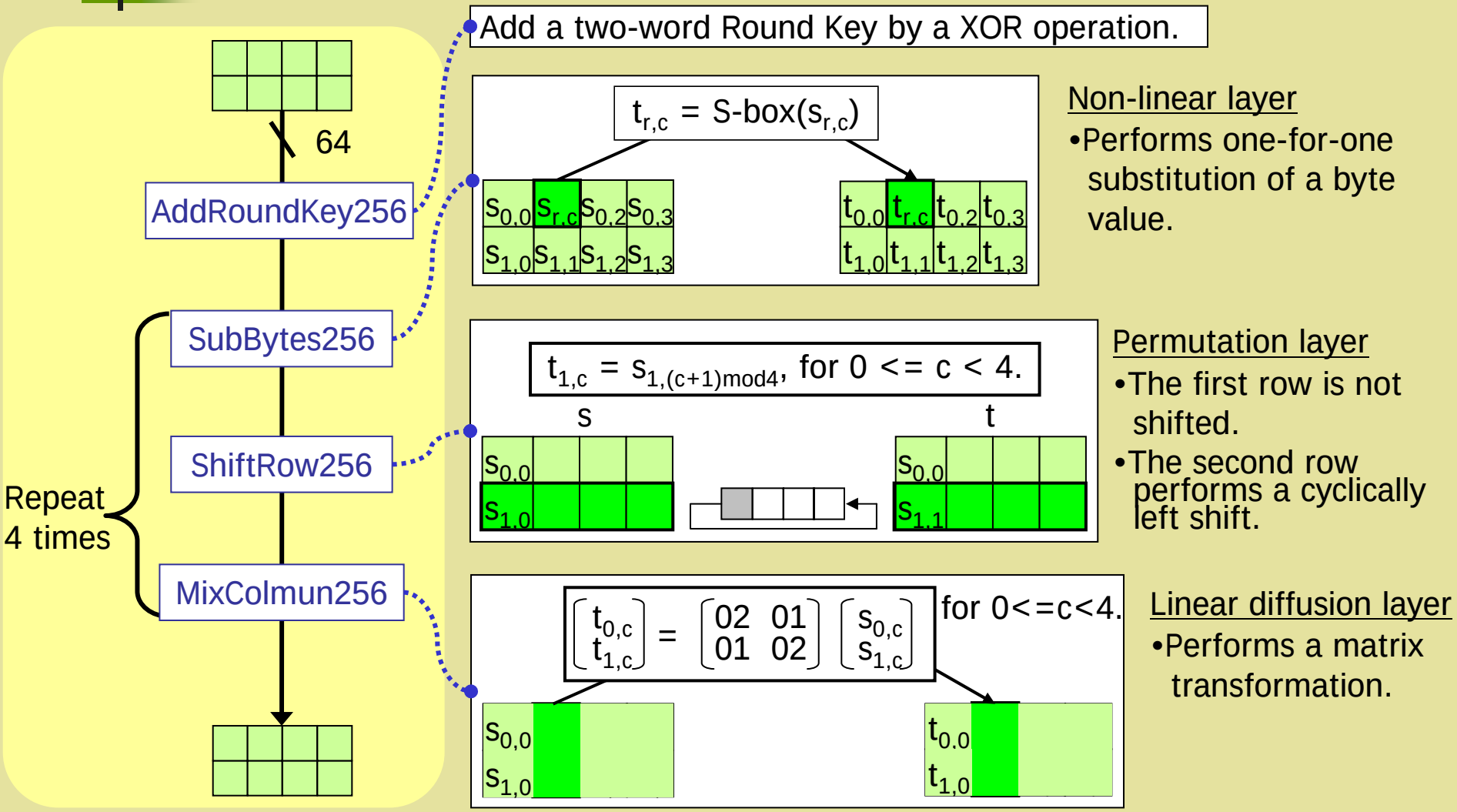
- 256-bit plaintext and 256-bit key for Lesamnta-256
- 512-bit plaintext and 512-bit key for Lesamnta-512
- Block ciphers *E* and *L* have 32 rounds



Hash bit length	Word length
256 bits	32 bits
512 bits	64 bits

- One round of *L* is almost the same as that of *E*
  - The only difference is that the non-linear function *G* in the key scheduling function is replaced by *F* in *L*.

The F function for Lesamnta-256



Non-linear layer

- Performs one-for-one substitution of a byte value.

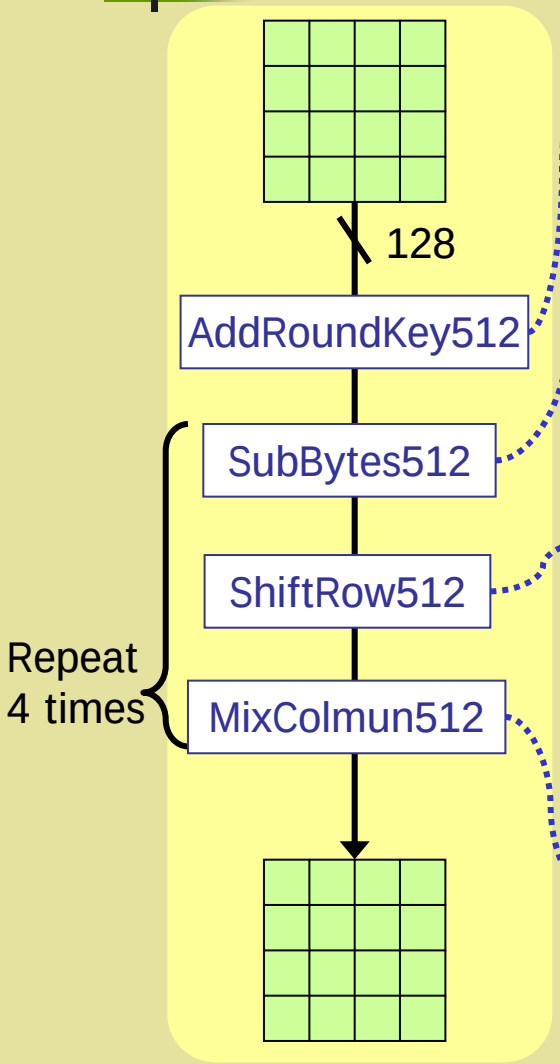
Permutation layer

- The first row is not shifted.
- The second row performs a cyclically left shift.

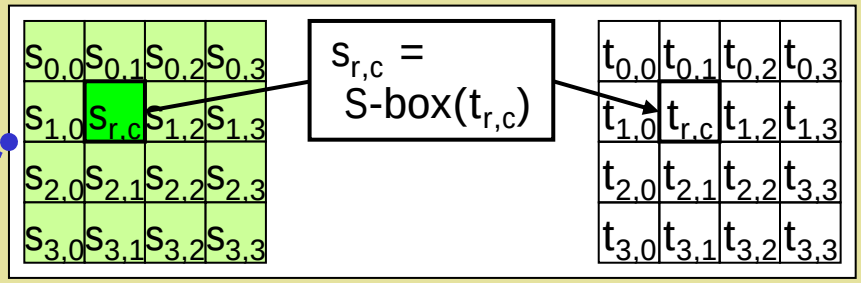
Linear diffusion layer

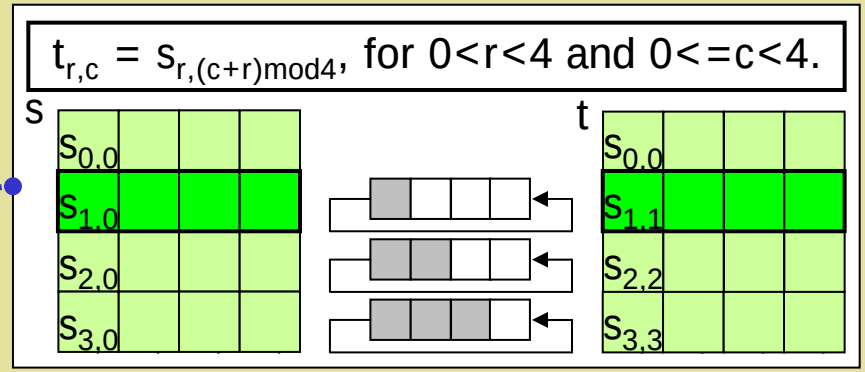
- Performs a matrix transformation.

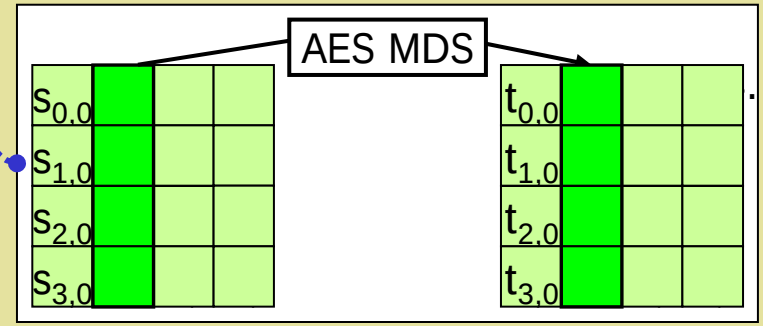
The F function for Lesamnta-512



Add a two-word Round Key by a XOR operation.







Non-linear layer

- Performs one-for-one substitution of a byte value.

Permutation layer

- The first row is not shifted.
- The last three rows perform a cyclically left shift.

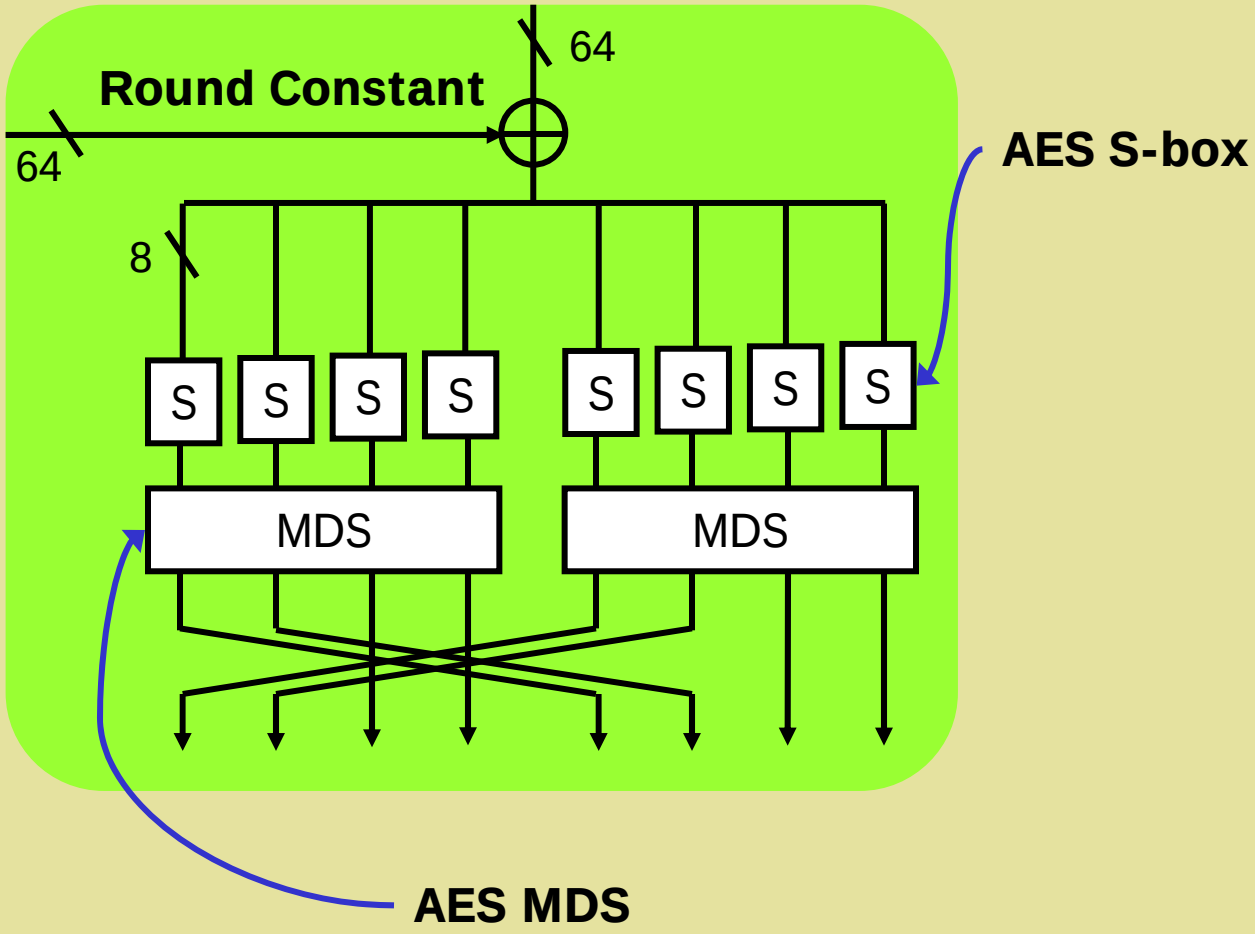
Linear diffusion layer

- Performs a transformation with AES MDS matrix.

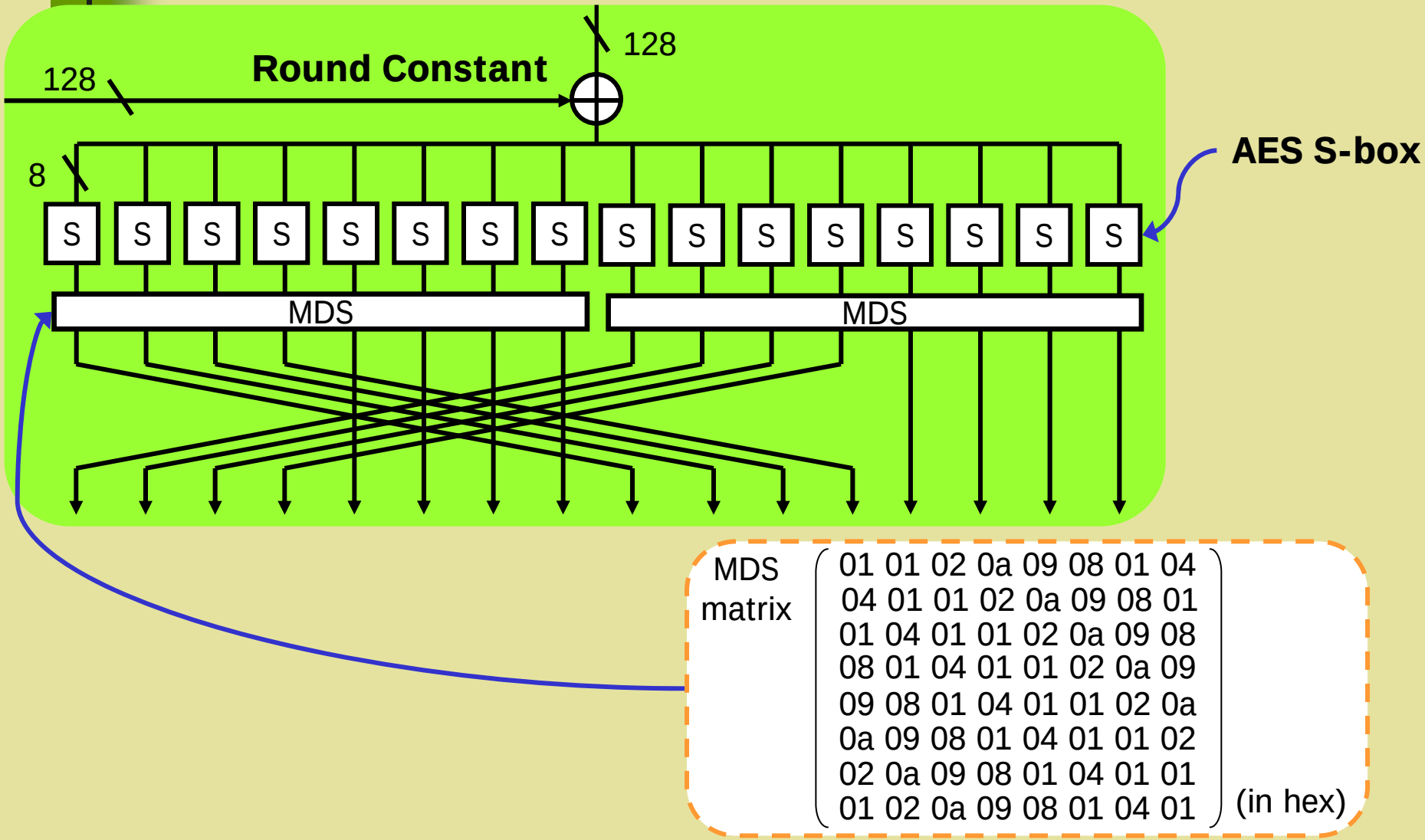
AES MDS matrix

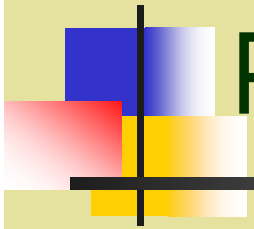
$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

The G function for Lesamnta-256



The G function for Lesamnta-512





Preliminary analysis

Provable security

The security of Lesamnta is reduced to the security of the underlying block ciphers.

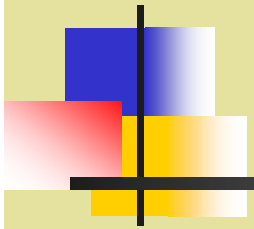
- Collision resistant if the compression & output functions are CR.
- Preimage resistant in the ideal cipher model
- Indifferentiable from random oracle in the ideal cipher model
  - Resistant against length-extension attacks.
- HMAC is PRF if the underlying block ciphers are independent PRPs.

Attack-based security analysis

- The best results on attacks are due to the known-key distinguisher.

Algorithm	Attack	Target Function	Number of Rounds	Attack complexity
Lesamnta-256	Collision finding	Hash function	16	2^{97}
	Pre-image finding	Compression function	16	2^{193}
	Second pre-image Finding	Hash function	16	2^{193}
Lesamnta-512	Collision finding	Hash function	16	2^{193}
	Pre-image finding	Compression function	16	2^{385}
	Second pre-image Finding	Hash function	16	2^{385}

- Lesamnta block ciphers are secure against a variety of known attacks.
- Difficult to apply differential style attacks to Lesamnta
  - Provable property on differential characteristic probabitliy
  - Limited degree of freedom due to small size of message block (256(512) bits)



Performance figures

Software Implementation

- Lesamnta was implemented in the **assembly** language.

CPU	Implementation method	Message digest size	Execution time		Memory requirements		
			Bulk Speed (cycles/byte)	One-block message (cycles/message)	Constant data (bytes)	Code length (bytes)	RAM (bytes)
8-bit(*1)	Speed opt.	256	**631**	**47312**	**256**	**1118**	**66**
	Area opt.	256	**901**	**69678**	**256**	**456**	**68**
32-bit(*2)	Speed opt.	256	**59.2**	**4750**	**-**	**-**	**-**
		512	**54.5**	**8827**	**-**	**-**	**-**
64-bit(*2)	Speed opt.	256	**52.7**	**4318**	**-**	**-**	**-**
		512	**51.2**	**8373**	**-**	**-**	**-**

*1: Atmel AVR ATmega8515 Processor (8-bit mode) with AVR Studio(*3) 4 simulator.
*2: Intel Core2 Duo E6600 processor (32/64-bit mode).
*3: AVR Studio is a registered trademark of Atmel Corporation

Hardware implementation

- We made estimations for speed and gate count of several different hardware architectures of Lesamnta-256/512.

Hash bit length	Architecture	Gate count (kgates)	Max. frequency (MHz)	Throughput (Mbps)
256	Speed opt.	190.1	282.5	6026.4
	Balance opt.	68.0	636.9	3623.5
	Area opt.	20.7	169.8	336.9
512	Speed opt.	393.0	234.2	9992.2
	Balance opt.	144.9	571.4	6501.6
	Area opt.	44.3	144.1	571.9

90 nm standard CMOS Cell library

Conclusion (What's special about Lesamnta?)

- Security
  - Based on the security of the underlying block ciphers
  - Large security margin against known attacks
- Performance
  - Efficient in a wide range of environments including ubiquitous systems
    - Efficient on 8-bit platforms
    - Efficient on short messages
  - Fast on future processors with instructions of AES round function
- Additional PRF modes
  - Key-prefix mode:
    - Simply feeds $K||M$ to Lesmanta as an input (K: key, M: message).
    - More efficient than HMAC
  - Keyed-via-IV mode