"Ss. Cyril and Methodius" University in Skopje
FACULTY OF COMPUTER
SCIENCE AND ENGINEERING

NTNU
Norwegian University of
Science and Technology

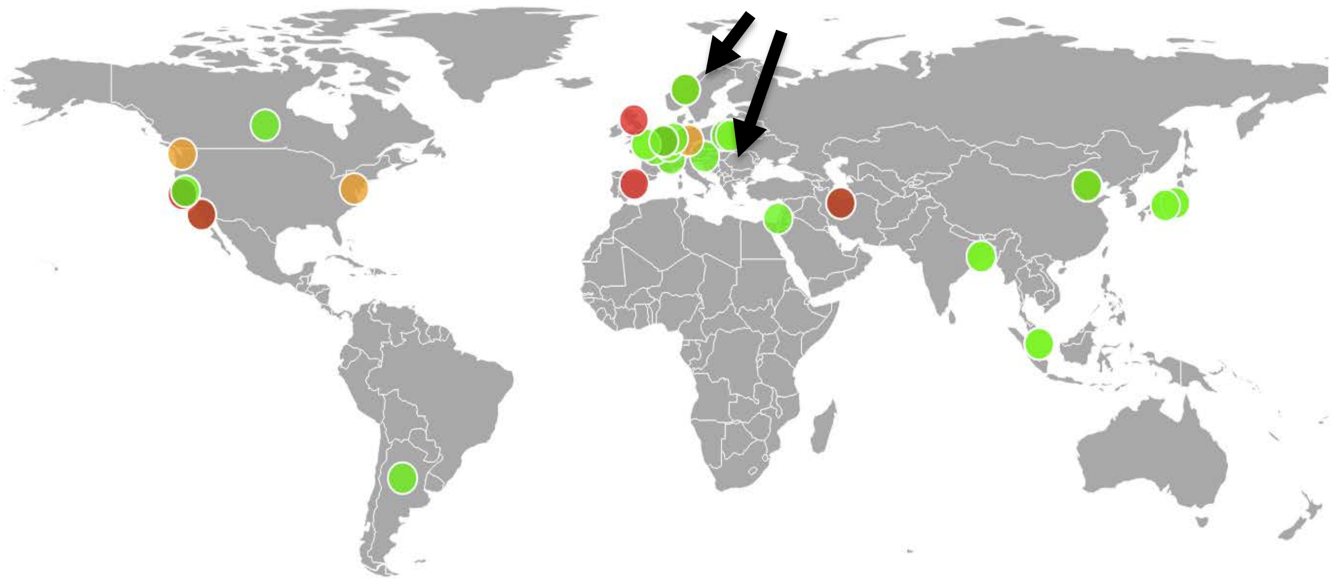
THE ARX STRUCTURE OF π-CIPHER

Hristina Mihajloska FCSE, UKIM, Macedonia
Danilo Gligoroski ITEM, NTNU, Norway
Simona Samardjiska FCSE, UKIM, Macedonia

simona.samardjiska@finki.ukim.mk

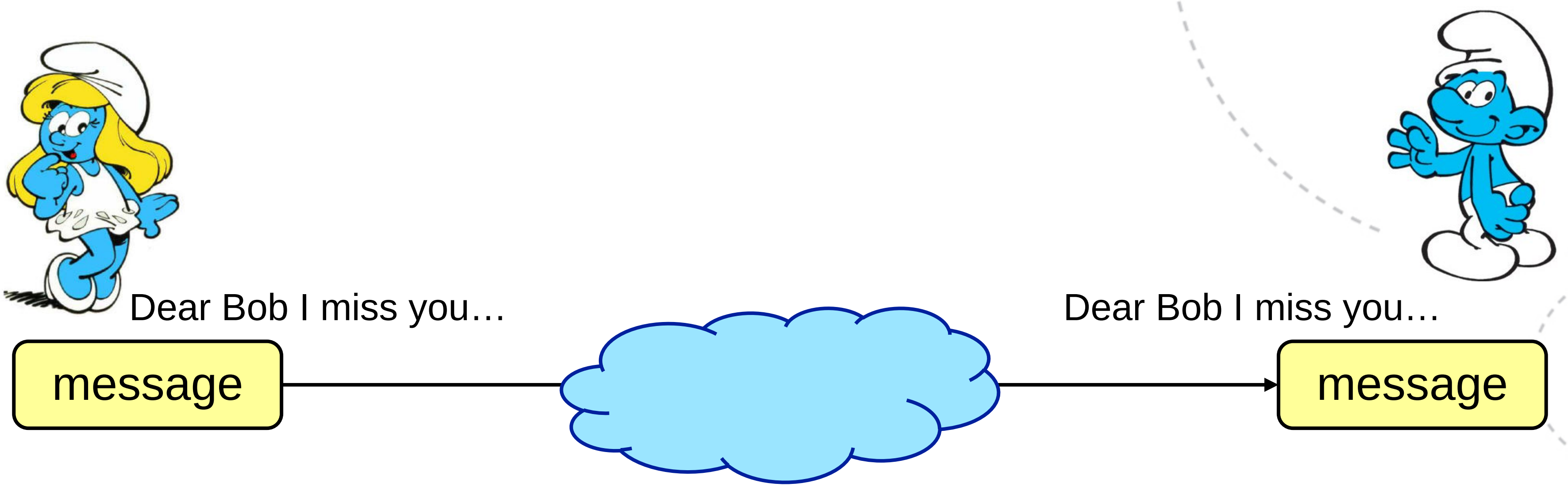
CAESAR = Competition for Authenticated Encryption: *Security Applicability* and *Robustness*

- Will identify a portfolio of authenticated ciphers that
  - offer advantages over AES-GCM
  - are suitable for widespread adoption
- Follows a long tradition of focused competitions in symmetric-key cryptography
- Currently 2 round
  - 29 candidates remaining



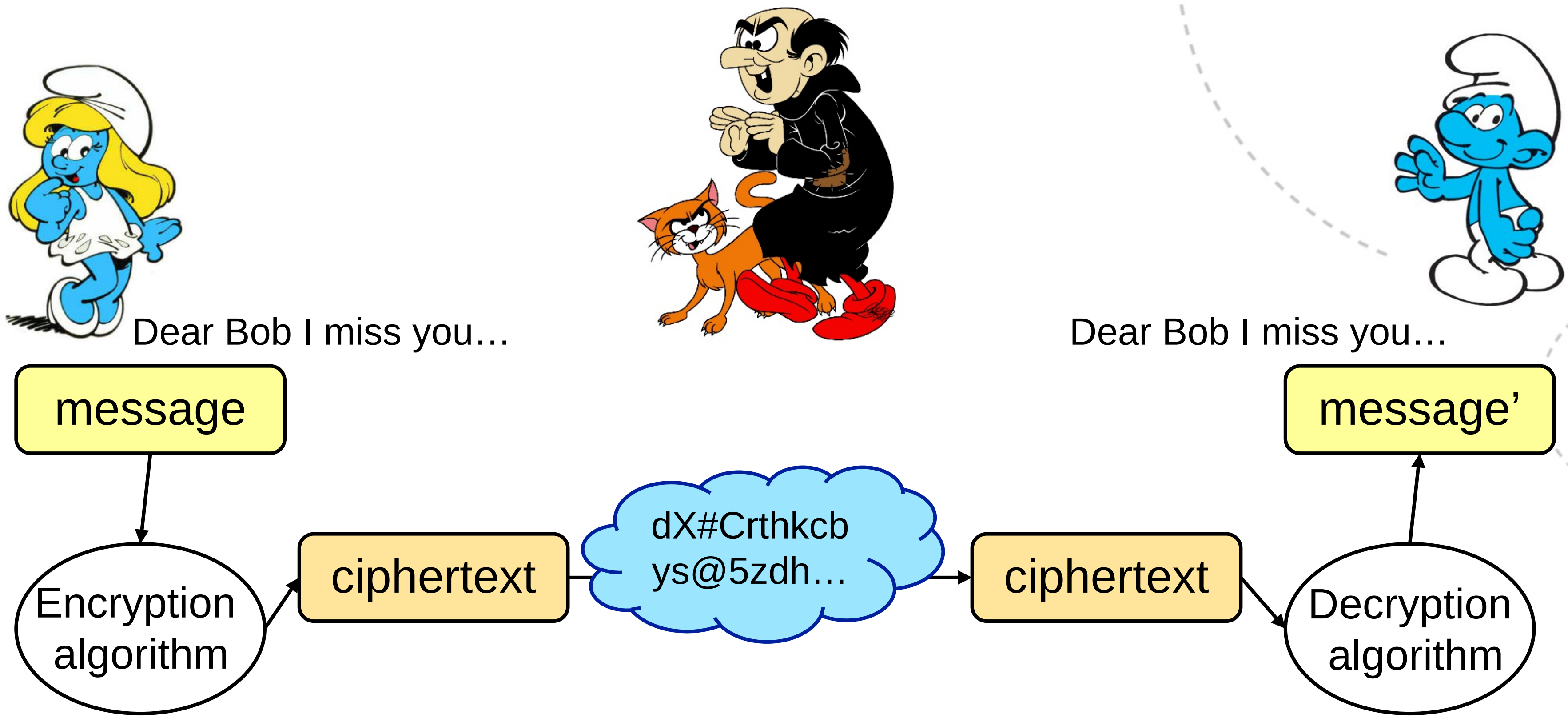
Authenticated Encryption Zoo: https://aezoo.compute.dtu.dk

What is Authenticated Encryption (AE)?

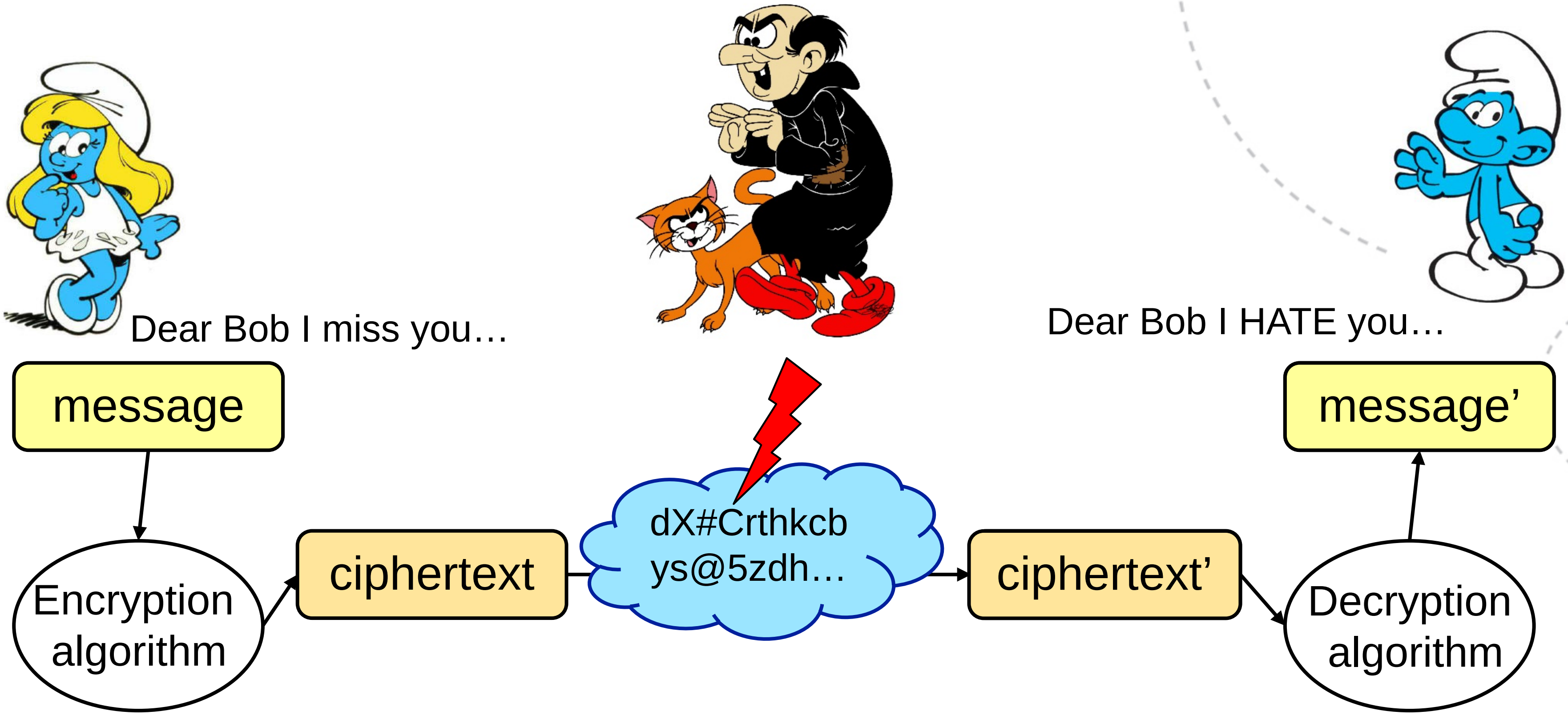


What is Authenticated Encryption (AE)?

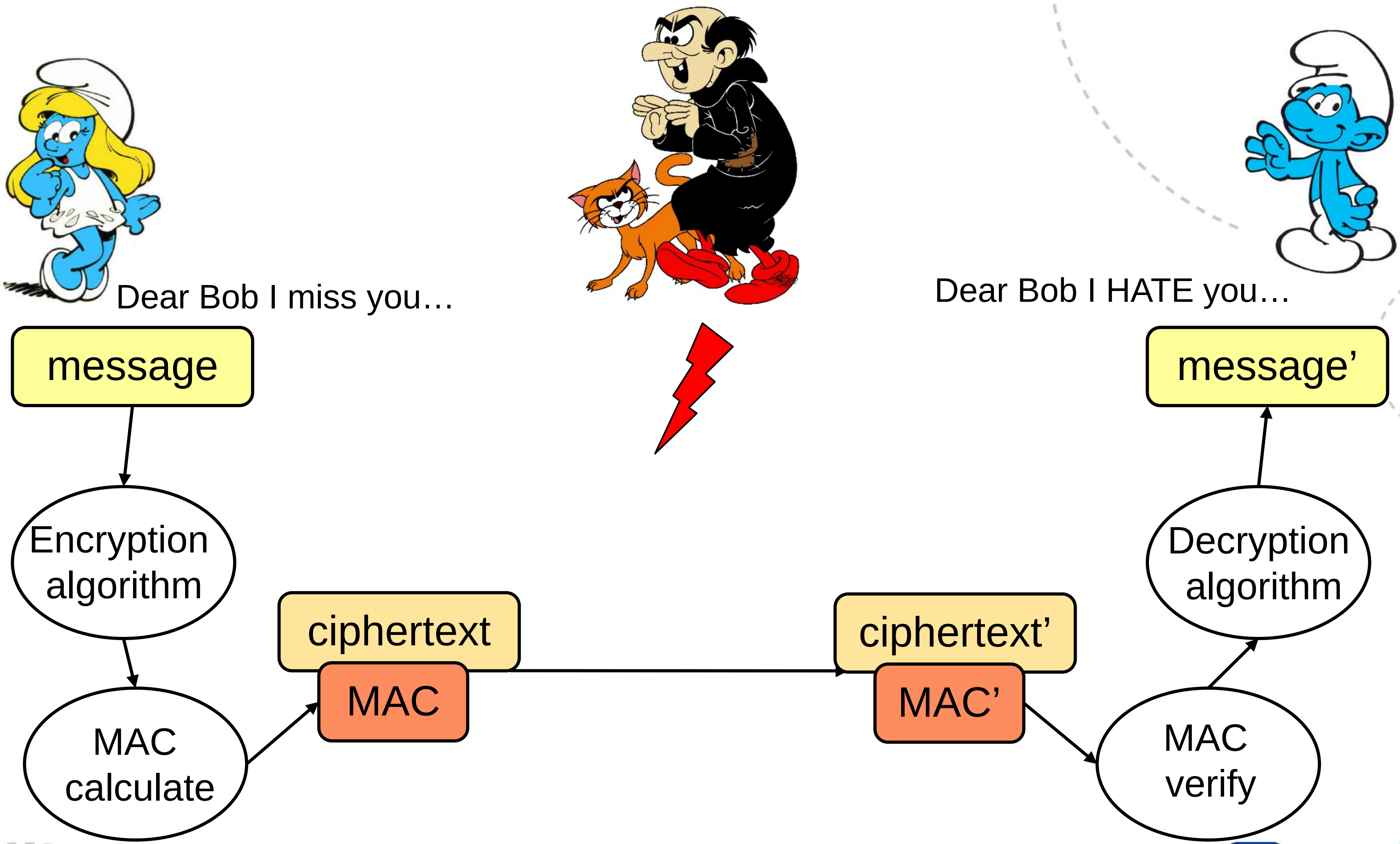
What is Authenticated Encryption (AE)?



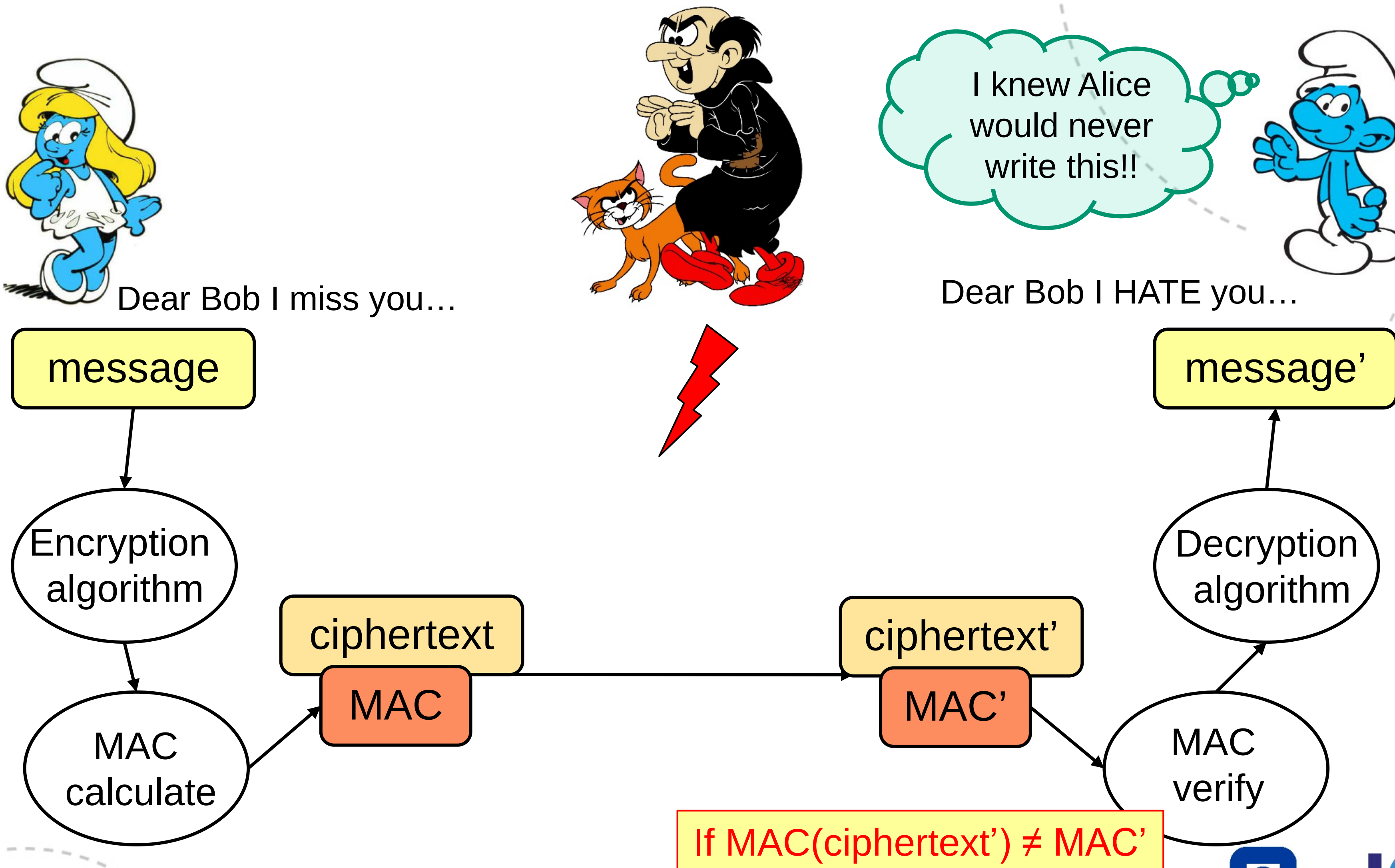
What is Authenticated Encryption (AE)?



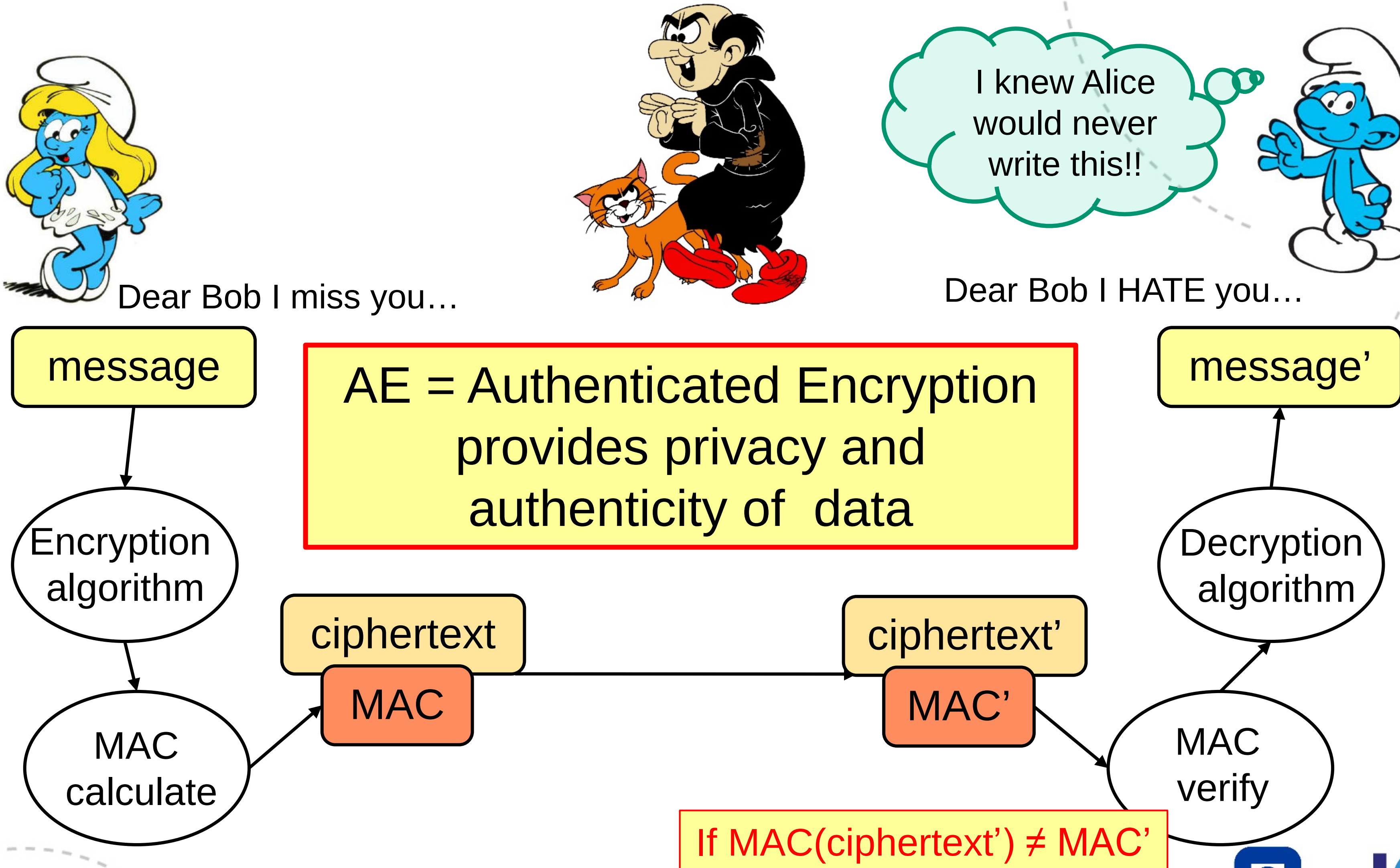
What is Authenticated Encryption (AE)?



What is Authenticated Encryption (AE)?



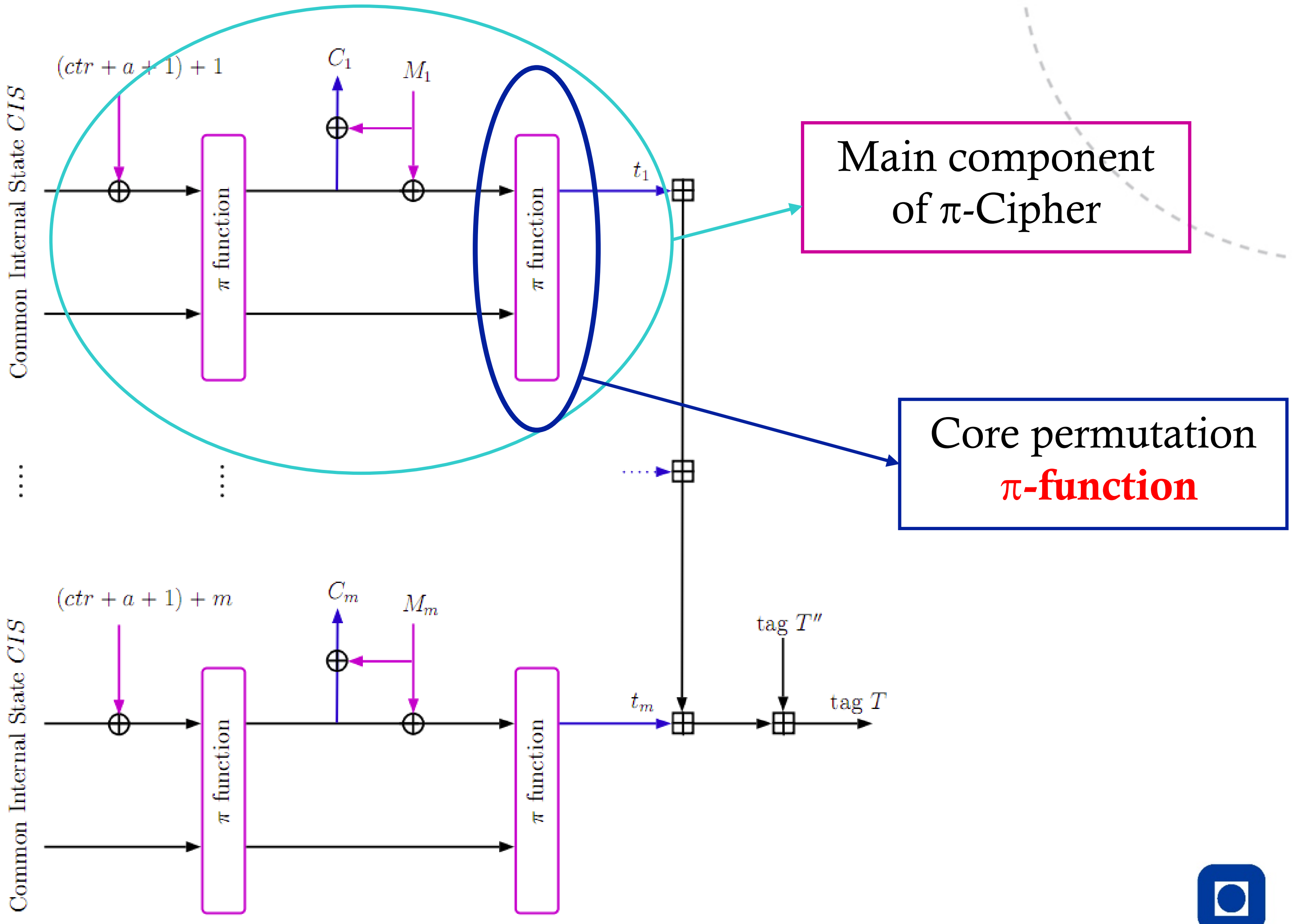
What is Authenticated Encryption (AE)?



π-Cipher: one of the candidates of the CAESAR competition

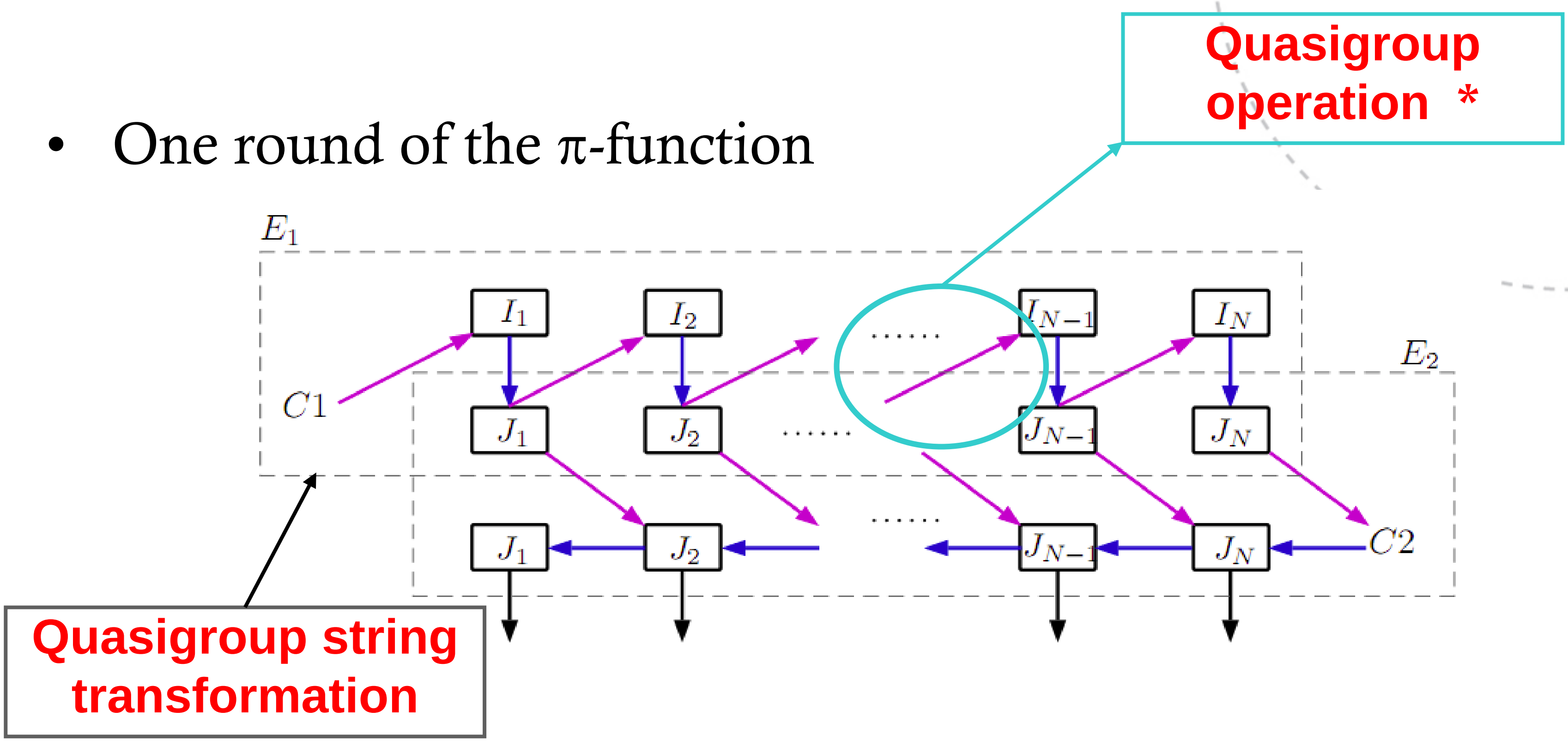
- An authenticated encryption cipher with associated data
- Second round candidate
- Norwegian-Macedonian-German collaboration
  - Danilo Gligoroski, NTNU
  - Hristina Mihajloska, FINKI
  - Simona Samardjiska, FINKI
  - Håkon Jacobsen, NTNU
  - Mohamed El-Hadedy, NTNU
  - Rune Erlend Jensen, NTNU
  - Daniel Otte, RUB

Inside π-Cipher: Processing the message



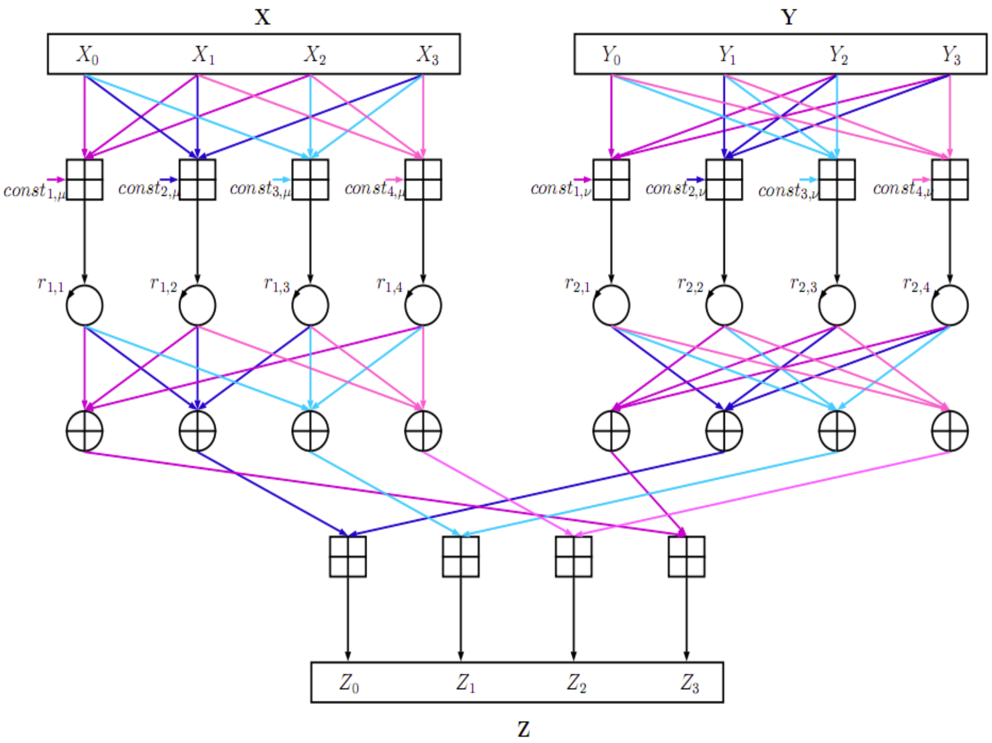
Inside the π-function

- One round of the π-function



- The number of rounds R is a tweakable parameter
- V.2 recommendation R = 3

Inside the quasigroup operation *

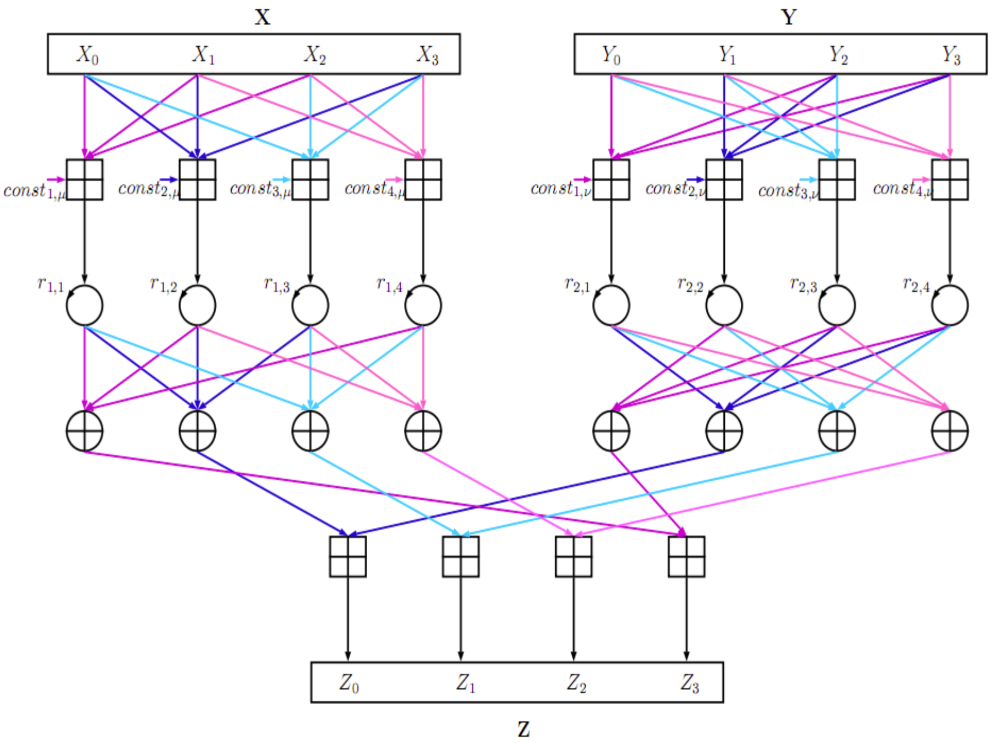


X, Y and Z - 4-tuples of ω-bit words (ω = 16, 32, 64)

ARX design

- Addition ⊞ modulo 2^{ω}
- Rotation to the left $ROTL^{r}(X)$
- XOR ⊕ on ω–bit words

Inside the quasigroup operation *



The quasigroup operation *:

$$Z = X * Y \equiv \partial(\mu(X) \boxplus_{\omega} \nu(Y))$$

Isotopic

Algorithmic view of *

μ–transformation for X:

$$
1.\quad \begin{array}{lllllllll}
T_0 & \leftarrow & ROTL^1(\texttt{0xF0E8} & + & X_0 & + & X_1 & + & X_2); \\
T_1 & \leftarrow & ROTL^4(\texttt{0xE4E2} & + & X_0 & + & X_1 & + & X_3); \\
T_2 & \leftarrow & ROTL^9(\texttt{0xE1D8} & + & X_0 & + & X_2 & + & X_3); \\
T_3 & \leftarrow & ROTL^{11}(\texttt{0xD4D2} & + & X_1 & + & X_2 & + & X_3);
\end{array}
$$

$$
2.\quad \begin{array}{lllllll}
T_4 & \leftarrow & T_0 & \oplus & T_1 & \oplus & T_3; \\
T_5 & \leftarrow & T_0 & \oplus & T_1 & \oplus & T_2; \\
T_6 & \leftarrow & T_1 & \oplus & T_2 & \oplus & T_3; \\
T_7 & \leftarrow & T_0 & \oplus & T_2 & \oplus & T_3;
\end{array}
$$

ν–transformation for Y:

$$
1.\quad \begin{array}{lllllllll}
T_0 & \leftarrow & ROTL^2(\texttt{0xD1CC} & + & Y_0 & + & Y_2 & + & Y_3); \\
T_1 & \leftarrow & ROTL^5(\texttt{0xCAC9} & + & Y_1 & + & Y_2 & + & Y_3); \\
T_2 & \leftarrow & ROTL^7(\texttt{0xC6C5} & + & Y_0 & + & Y_1 & + & Y_2); \\
T_3 & \leftarrow & ROTL^{13}(\texttt{0xC3B8} & + & Y_0 & + & Y_1 & + & Y_3);
\end{array}
$$

$$
2.\quad \begin{array}{lllllll}
T_8 & \leftarrow & T_1 & \oplus & T_2 & \oplus & T_3; \\
T_9 & \leftarrow & T_0 & \oplus & T_2 & \oplus & T_3; \\
T_{10} & \leftarrow & T_0 & \oplus & T_1 & \oplus & T_3; \\
T_{11} & \leftarrow & T_0 & \oplus & T_1 & \oplus & T_2;
\end{array}
$$

σ–transformation

$$
1.\quad \begin{array}{lllll}
Z_3 & \leftarrow & T_4 & + & T_8; \\
Z_0 & \leftarrow & T_5 & + & T_9; \\
Z_1 & \leftarrow & T_6 & + & T_{10}; \\
Z_2 & \leftarrow & T_7 & + & T_{11};
\end{array}
$$

The isotopy

Algorithmic view of *

μ–transformation for X:

1.
$$
\begin{aligned}
T_0 &\leftarrow ROTL^{1}(\texttt{0xF0E8} + X_0 + X_1 + X_2);\\
T_1 &\leftarrow ROTL^{4}(\texttt{0xE4E2} + X_0 + X_1 + X_3);\\
T_2 &\leftarrow ROTL^{9}(\texttt{0xE1D8} + X_0 + X_2 + X_3);\\
T_3 &\leftarrow ROTL^{11}(\texttt{0xD4D2} + X_1 + X_2 + X_3);
\end{aligned}
$$

2.
$$
\begin{aligned}
T_4 &\leftarrow T_0 \oplus T_1 \oplus T_3;\\
T_5 &\leftarrow T_0 \oplus T_1 \oplus T_2;\\
T_6 &\leftarrow T_1 \oplus T_2 \oplus T_3;\\
T_7 &\leftarrow T_0 \oplus T_2 \oplus T_3;
\end{aligned}
$$

ν–transformation for Y:

1.
$$
\begin{aligned}
T_0 &\leftarrow ROTL^{2}(\texttt{0xD1CC} + Y_0 + Y_2 + Y_3);\\
T_1 &\leftarrow ROTL^{5}(\texttt{0xCAC9} + Y_1 + Y_2 + Y_3);\\
T_2 &\leftarrow ROTL^{7}(\texttt{0xC6C5} + Y_0 + Y_1 + Y_2);\\
T_3 &\leftarrow ROTL^{13}(\texttt{0xC3B8} + Y_0 + Y_1 + Y_3);
\end{aligned}
$$

2.
$$
\begin{aligned}
T_8 &\leftarrow T_1 \oplus T_2 \oplus T_3;\\
T_9 &\leftarrow T_0 \oplus T_2 \oplus T_3;\\
T_{10} &\leftarrow T_0 \oplus T_1 \oplus T_3;\\
T_{11} &\leftarrow T_0 \oplus T_1 \oplus T_2;
\end{aligned}
$$

σ–transformation

1.
$$
\begin{aligned}
Z_3 &\leftarrow T_4 + T_8;\\
Z_0 &\leftarrow T_5 + T_9;\\
Z_1 &\leftarrow T_6 + T_{10};\\
Z_2 &\leftarrow T_7 + T_{11};
\end{aligned}
$$

Two orthogonal Latin squares

$$
L_1 = \begin{matrix} 0 & 1 & 2 & 3\\ 1 & 0 & 3 & 2\\ 2 & 3 & 0 & 1\\ 3 & 2 & 1 & 0 \end{matrix}
$$

$$
L_2 = \begin{matrix} 0 & 1 & 2 & 3\\ 3 & 2 & 1 & 0\\ 1 & 0 & 3 & 2\\ 2 & 3 & 0 & 1 \end{matrix}
$$

Algorithmic view of *

μ–transformation for X:

$$
\begin{array}{llcl}
 & T_0 & \leftarrow & ROTL^{1}(\texttt{0xF0E8} + X_0 + X_1 + X_2); \\
1. & T_1 & \leftarrow & ROTL^{4}(\texttt{0xE4E2} + X_0 + X_1 + X_3); \\
 & T_2 & \leftarrow & ROTL^{9}(\texttt{0xE1D8} + X_0 + X_2 + X_3); \\
 & T_3 & \leftarrow & ROTL^{11}(\texttt{0xD4D2} + X_1 + X_2 + X_3); \\
 & T_4 & \leftarrow & T_0 \oplus T_1 \oplus T_3; \\
2. & T_5 & \leftarrow & T_0 \oplus T_1 \oplus T_2; \\
 & T_6 & \leftarrow & T_1 \oplus T_2 \oplus T_3; \\
 & T_7 & \leftarrow & T_0 \oplus T_2 \oplus T_3;
\end{array}
$$

ν–transformation for Y:

$$
\begin{array}{llcl}
 & T_0 & \leftarrow & ROTL^{2}(\texttt{0xD1CC} + Y_0 + Y_2 + Y_3); \\
1. & T_1 & \leftarrow & ROTL^{5}(\texttt{0xCAC9} + Y_1 + Y_2 + Y_3); \\
 & T_2 & \leftarrow & ROTL^{7}(\texttt{0xC6C5} + Y_0 + Y_1 + Y_2); \\
 & T_3 & \leftarrow & ROTL^{13}(\texttt{0xC3B8} + Y_0 + Y_1 + Y_3); \\
 & T_8 & \leftarrow & T_1 \oplus T_2 \oplus T_3; \\
2. & T_9 & \leftarrow & T_0 \oplus T_2 \oplus T_3; \\
 & T_{10} & \leftarrow & T_0 \oplus T_1 \oplus T_3; \\
 & T_{11} & \leftarrow & T_0 \oplus T_1 \oplus T_2;
\end{array}
$$

σ–transformation

$$
\begin{array}{llcl}
 & Z_3 & \leftarrow & T_4 + T_8; \\
1. & Z_0 & \leftarrow & T_5 + T_9; \\
 & Z_1 & \leftarrow & T_6 + T_{10}; \\
 & Z_2 & \leftarrow & T_7 + T_{11};
\end{array}
$$

Two orthogonal Latin squares

$$
L_1 = L_2 = \begin{array}{cccc}
00 & 11 & 22 & 33 \\
13 & 02 & 31 & 20 \\
21 & 30 & 03 & 12 \\
32 & 23 & 10 & 01
\end{array}
$$

Algorithmic view of *

μ–transformation for X:

1.
$$\begin{aligned}
T_0 &\leftarrow ROTL^1(\mathtt{0xF0E8} + X_0 + X_1 + X_2);\\
T_1 &\leftarrow ROTL^4(\mathtt{0xE4E2} + X_0 + X_1 + X_3);\\
T_2 &\leftarrow ROTL^9(\mathtt{0xE1D8} + X_0 + X_2 + X_3);\\
T_3 &\leftarrow ROTL^{11}(\mathtt{0xD4D2} + X_1 + X_2 + X_3);
\end{aligned}$$

2.
$$\begin{aligned}
T_4 &\leftarrow T_0 \oplus T_1 \oplus T_3;\\
T_5 &\leftarrow T_0 \oplus T_1 \oplus T_2;\\
T_6 &\leftarrow T_1 \oplus T_2 \oplus T_3;\\
T_7 &\leftarrow T_0 \oplus T_2 \oplus T_3;
\end{aligned}$$

ν–transformation for Y:

1.
$$\begin{aligned}
T_0 &\leftarrow ROTL^2(\mathtt{0xD1CC} + Y_0 + Y_2 + Y_3);\\
T_1 &\leftarrow ROTL^5(\mathtt{0xCAC9} + Y_1 + Y_2 + Y_3);\\
T_2 &\leftarrow ROTL^7(\mathtt{0xC6C5} + Y_0 + Y_1 + Y_2);\\
T_3 &\leftarrow ROTL^{13}(\mathtt{0xC3B8} + Y_0 + Y_1 + Y_3);
\end{aligned}$$

2.
$$\begin{aligned}
T_8 &\leftarrow T_1 \oplus T_2 \oplus T_3;\\
T_9 &\leftarrow T_0 \oplus T_2 \oplus T_3;\\
T_{10} &\leftarrow T_0 \oplus T_1 \oplus T_3;\\
T_{11} &\leftarrow T_0 \oplus T_1 \oplus T_2;
\end{aligned}$$

σ–transformation

1.
$$\begin{aligned}
Z_3 &\leftarrow T_4 + T_8;\\
Z_0 &\leftarrow T_5 + T_9;\\
Z_1 &\leftarrow T_6 + T_{10};\\
Z_2 &\leftarrow T_7 + T_{11};
\end{aligned}$$

Two orthogonal Latin squares

$$L_1 = \begin{array}{cccc}
0 & 1 & 2 & 3\\
1 & 0 & 3 & 2\\
2 & 3 & 0 & 1\\
\hdashline
3 & 2 & 1 & 0
\end{array}$$

$$L_2 = \begin{array}{cccc}
0 & 1 & 2 & 3\\
3 & 2 & 1 & 0\\
1 & 0 & 3 & 2\\
2 & 3 & 0 & 1
\end{array}$$

Algorithmic view of *

μ–transformation for X:

1.
$$\begin{array}{llllllll}
T_0 & \leftarrow & ROTL^1(\texttt{0xF0E8} & + & X_0 & + & X_1 & + \; X_2); \\
T_1 & \leftarrow & ROTL^4(\texttt{0xE4E2} & + & X_0 & + & X_1 & + \; X_3); \\
T_2 & \leftarrow & ROTL^9(\texttt{0xE1D8} & + & X_0 & + & X_2 & + \; X_3); \\
T_3 & \leftarrow & ROTL^{11}(\texttt{0xD4D2} & + & X_1 & + & X_2 & + \; X_3);
\end{array}$$

2.
$$\begin{array}{llllll}
T_4 & \leftarrow & T_0 & \oplus & T_1 & \oplus \; T_3; \\
T_5 & \leftarrow & T_0 & \oplus & T_1 & \oplus \; T_2; \\
T_6 & \leftarrow & T_1 & \oplus & T_2 & \oplus \; T_3; \\
T_7 & \leftarrow & T_0 & \oplus & T_2 & \oplus \; T_3;
\end{array}$$

ν–transformation for Y:

1.
$$\begin{array}{llllllll}
T_0 & \leftarrow & ROTL^2(\texttt{0xD1CC} & + & Y_0 & + & Y_2 & + \; Y_3); \\
T_1 & \leftarrow & ROTL^5(\texttt{0xCAC9} & + & Y_1 & + & Y_2 & + \; Y_3); \\
T_2 & \leftarrow & ROTL^7(\texttt{0xC6C5} & + & Y_0 & + & Y_1 & + \; Y_2); \\
T_3 & \leftarrow & ROTL^{13}(\texttt{0xC3B8} & + & Y_0 & + & Y_1 & + \; Y_3);
\end{array}$$

2.
$$\begin{array}{llllll}
T_8 & \leftarrow & T_1 & \oplus & T_2 & \oplus \; T_3; \\
T_9 & \leftarrow & T_0 & \oplus & T_2 & \oplus \; T_3; \\
T_{10} & \leftarrow & T_0 & \oplus & T_1 & \oplus \; T_3; \\
T_{11} & \leftarrow & T_0 & \oplus & T_1 & \oplus \; T_2;
\end{array}$$

σ–transformation

1.
$$\begin{array}{llll}
Z_3 & \leftarrow & T_4 & + \; T_8; \\
Z_0 & \leftarrow & T_5 & + \; T_9; \\
Z_1 & \leftarrow & T_6 & + \; T_{10}; \\
Z_2 & \leftarrow & T_7 & + \; T_{11};
\end{array}$$

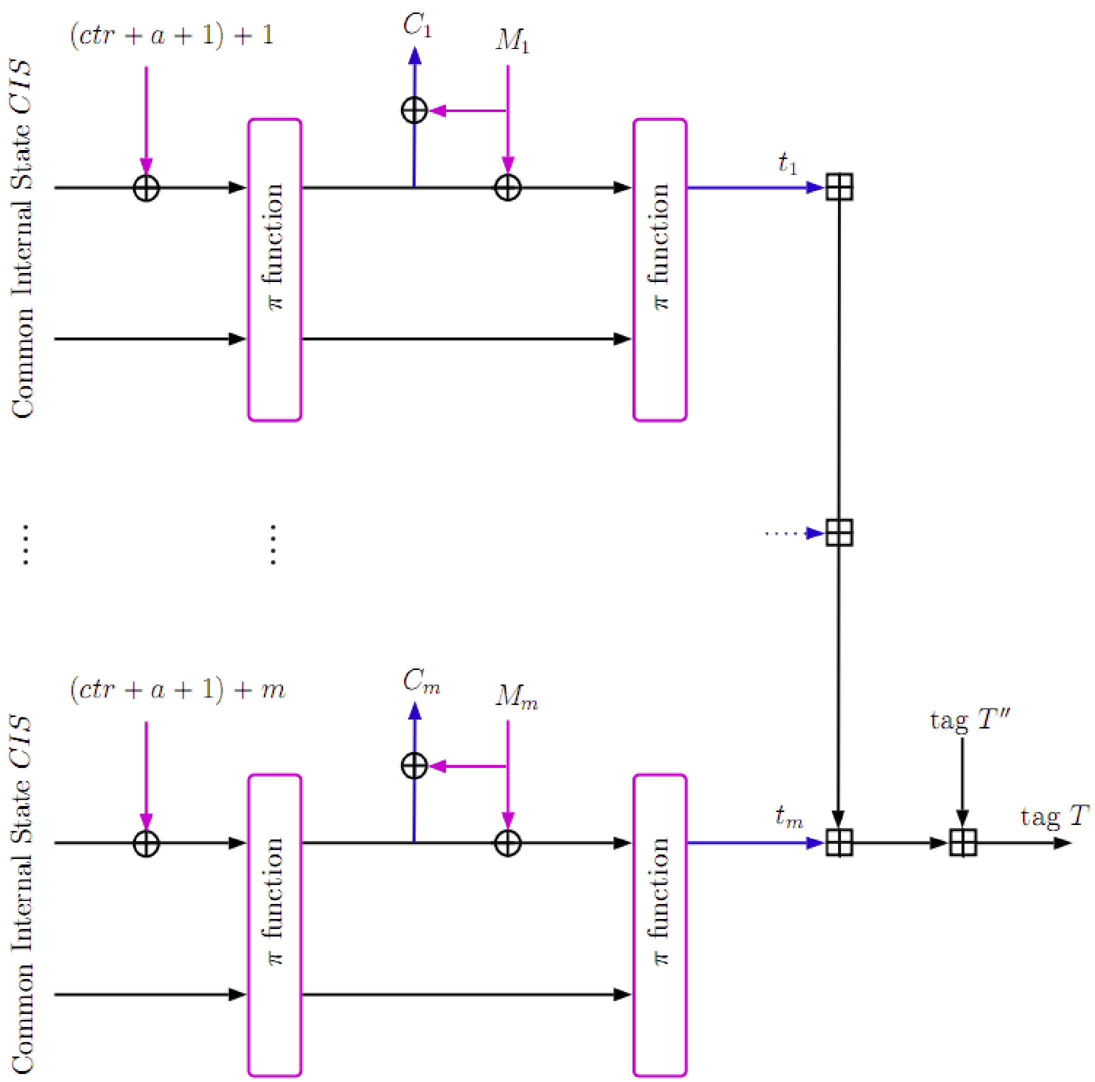
Two orthogonal Latin squares

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

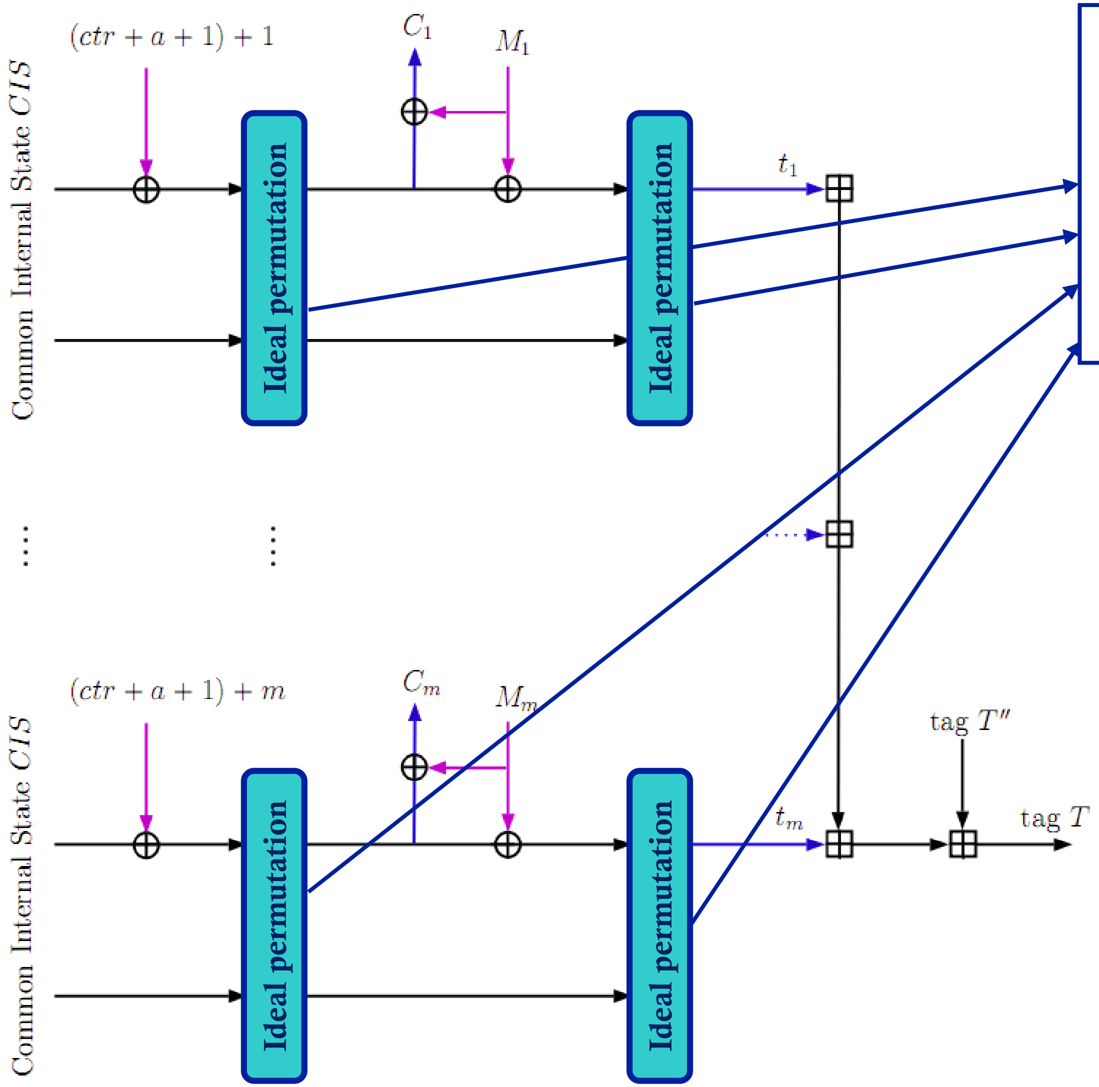
L_2 =

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

Security of π-Cipher

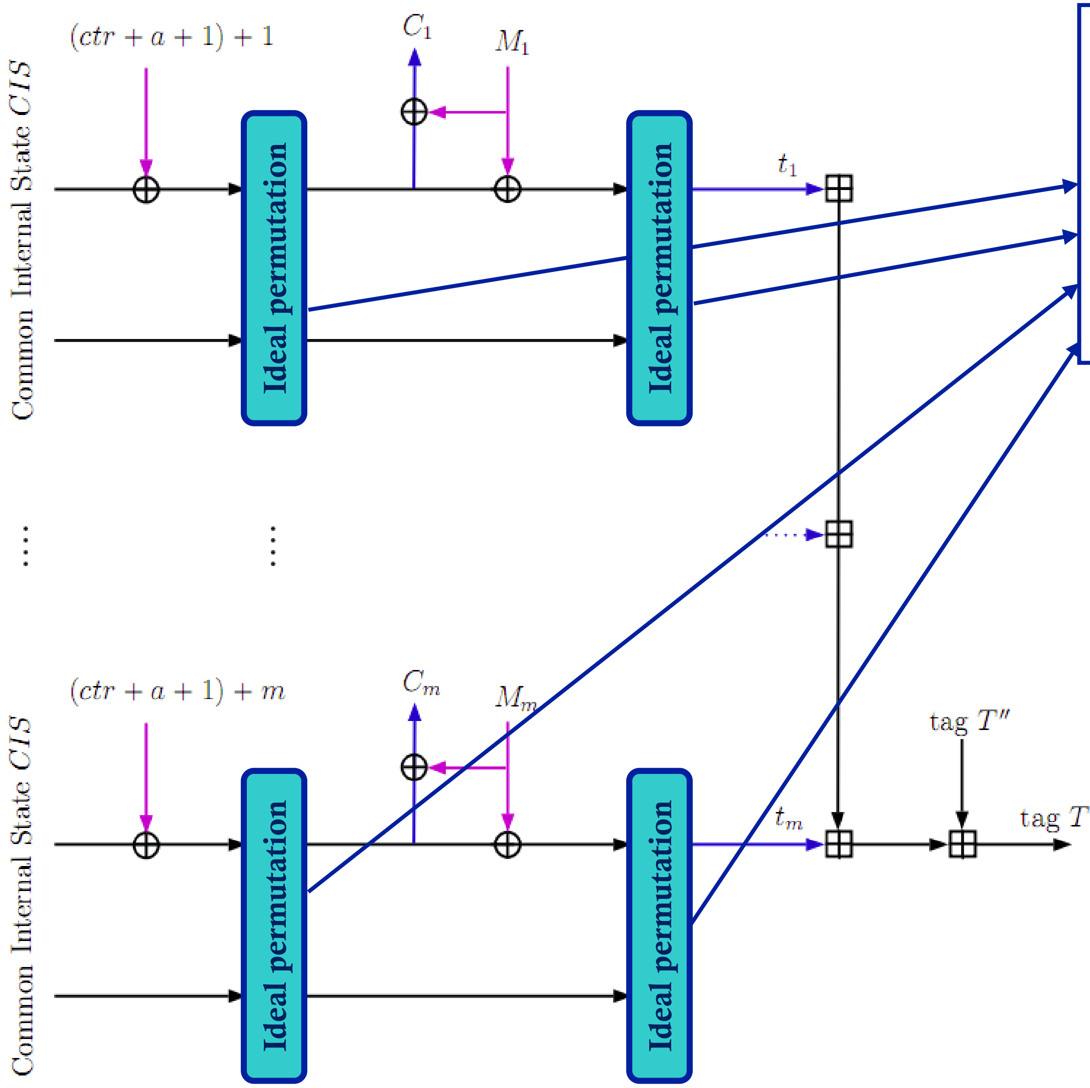


Security of π-Cipher



Assuming
π is drawn uniformly at random from the set of permutations on 16ω elements

Security of π-Cipher

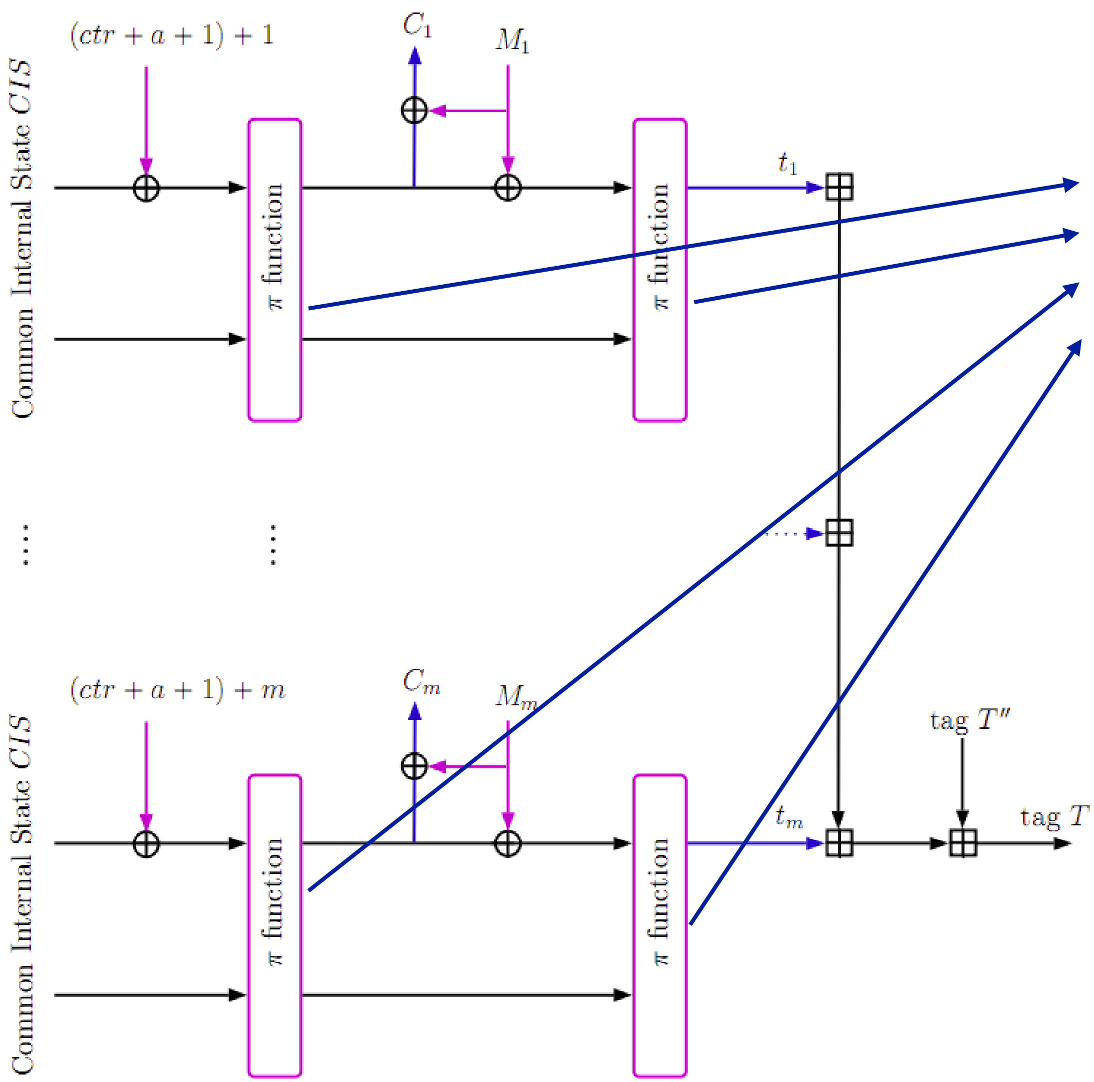


Assuming
π is drawn uniformly at random from the set of permutations on 16ω elements

π – cipher is provably secure:

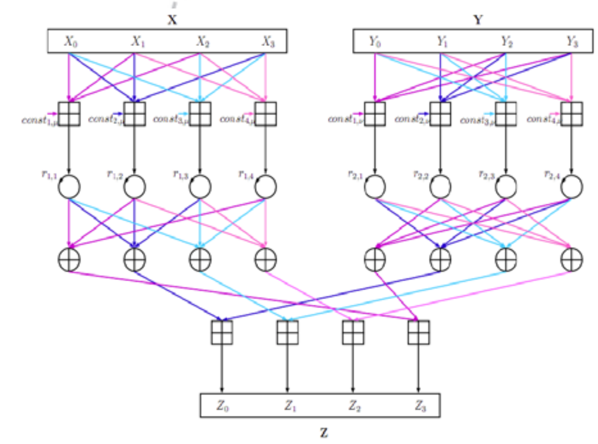
- Data privacy
- Ciphertext integrity

Security of π-Cipher



The security relies on the π – function

The structure of π – function



ARX design

Addition ⊞ modulo 2^{ω}
Rotation to the left $ROTL^{r}(X)$
XOR ⊕ on ω–bit words

Advantages

- Excellent performance
- Easy algorithm and implementation
- Functionally complete (with constant included)

Disadvantages

- Extremely hard to analyze:
  - Security against linear and differential cryptanalysis
  - Security estimate

ARX designs

Block ciphers

- FEAL, Threefish

Stream ciphers

- Salsa20, ChaCha, HC-128

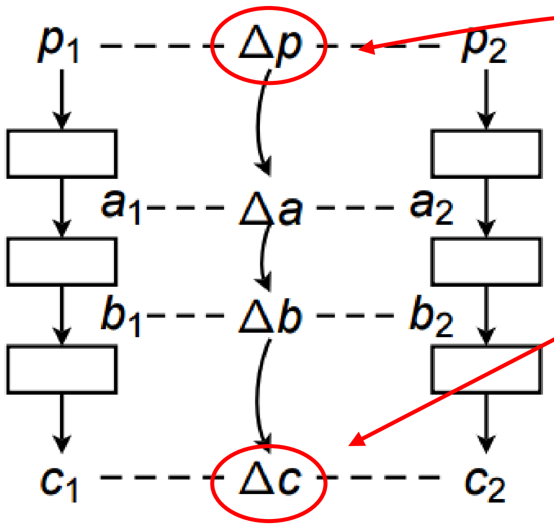
Hash functions

- SHA-3 Finalists: BLAKE, Skein
- SHA-3 Second Round: Blue Midnight Wish, Cubehash
- SHA-3 First Round: EDON-R

Authenticated ciphers

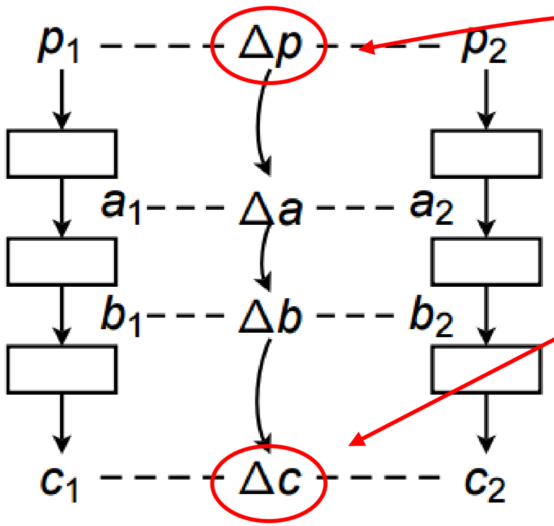
- π –cipher, NORX (LRX), MORUS (LRX)

ARX designs – Differential cryptanalysis



1. Observe the difference between two ciphertexts as a function of the difference between the plaintexts
2. Find the **highest probability differential input** (**characteristic**) which can be traced through several rounds

ARX designs – Differential cryptanalysis



1. Observe the difference between two ciphertexts as a function of the difference between the plaintexts
2. Find the **highest probability differential input** (**characteristic**) which can be traced through several rounds

S-box

- Typical size up to 8 × 8 bit
- Difference distribution table:

  up to $2^{16} = 65536$ elements
- Easy to calculate: differential probability, number of output differences, output difference with highest probability,...

ARX operations

- Typically, n = 32 or n = 64
- Difference distribution table:

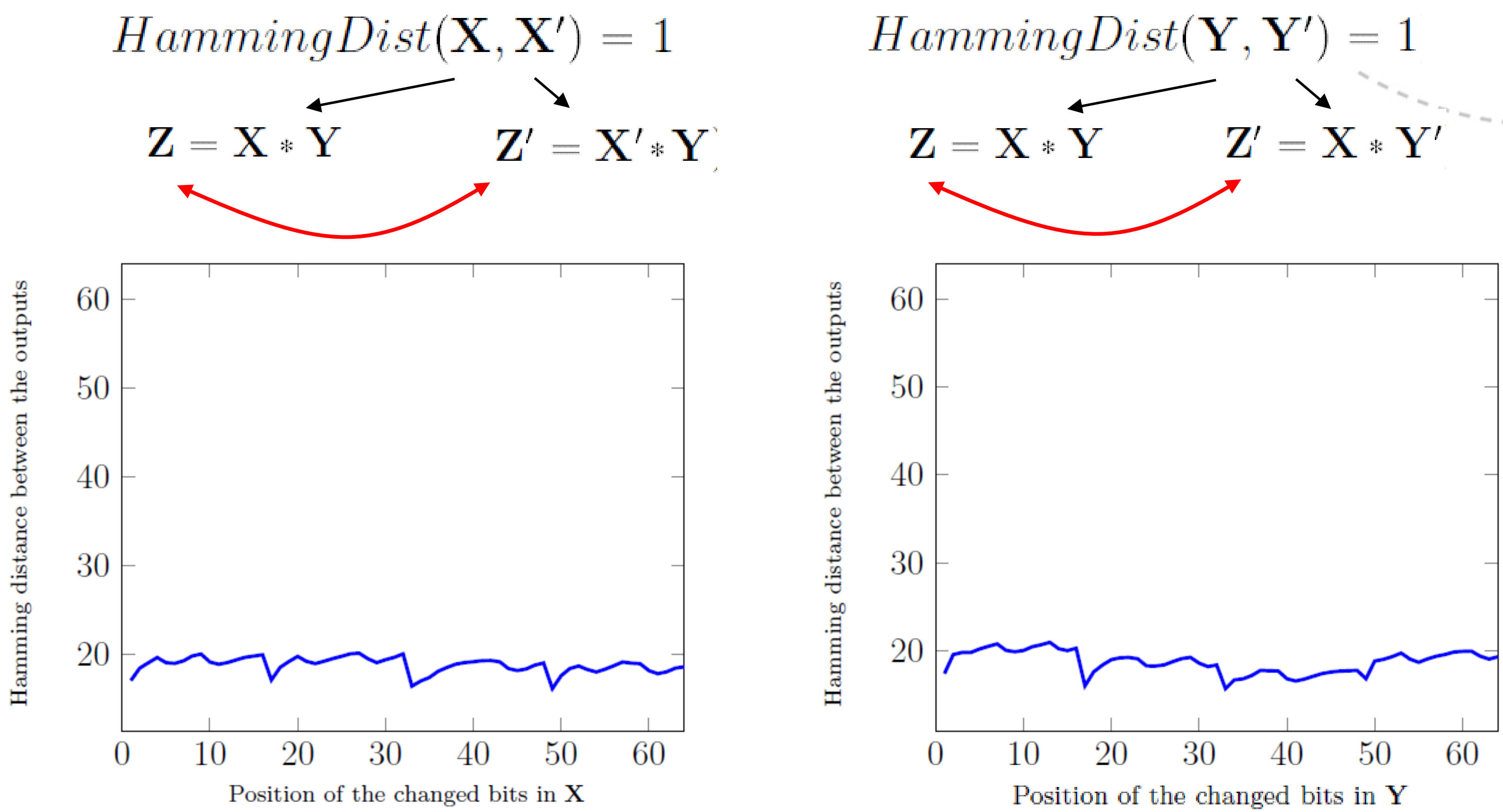
  2^{64} or 2^{128} elements, too large!

In π – cipher:

- Quasigroup operation $2^{8\omega*4\omega}$

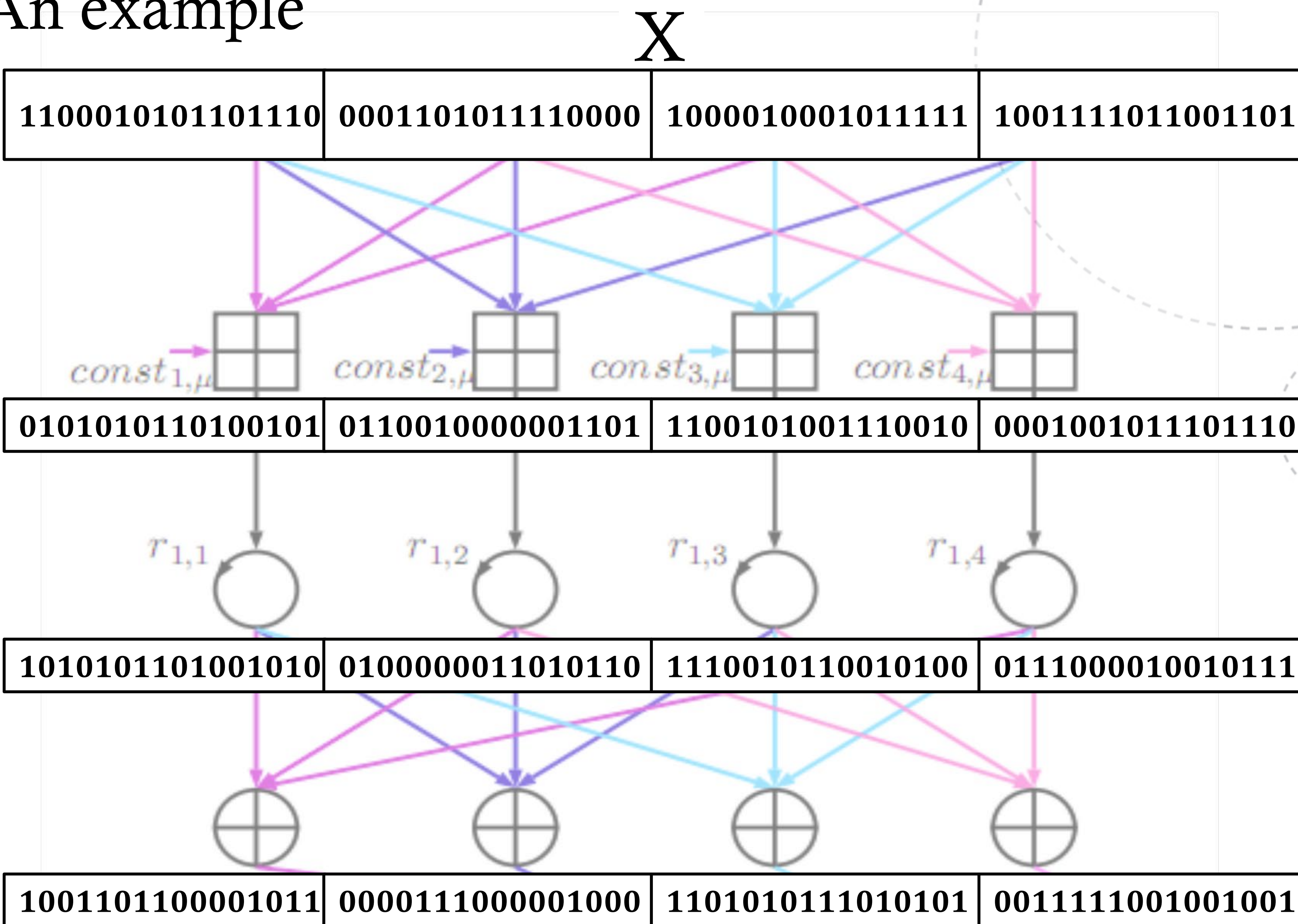
π-Cipher Security

- Bit diffusion of the used ARX permutation



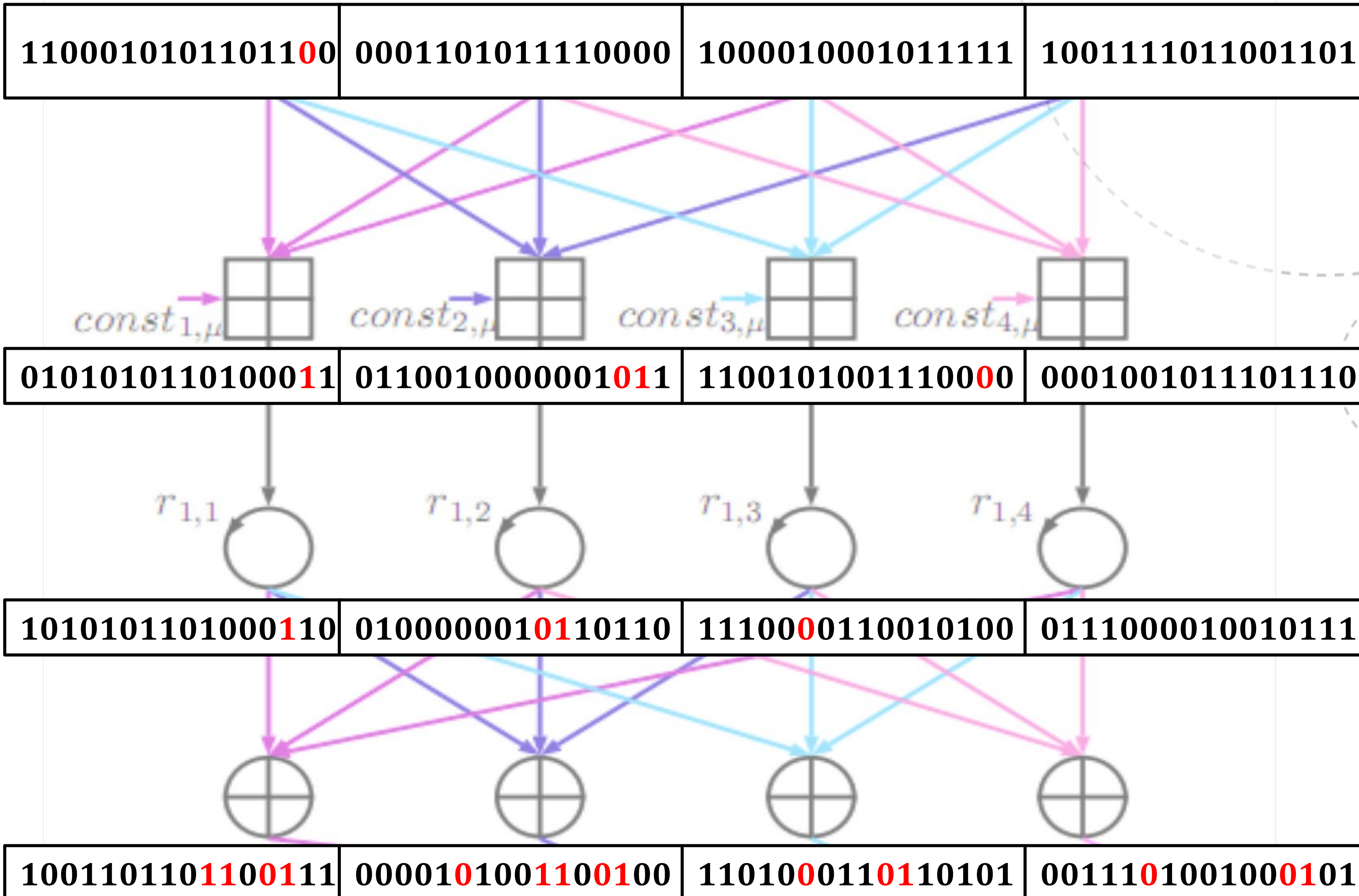
Avalanche effect of the $*$ operation for $\omega = 16$

An example

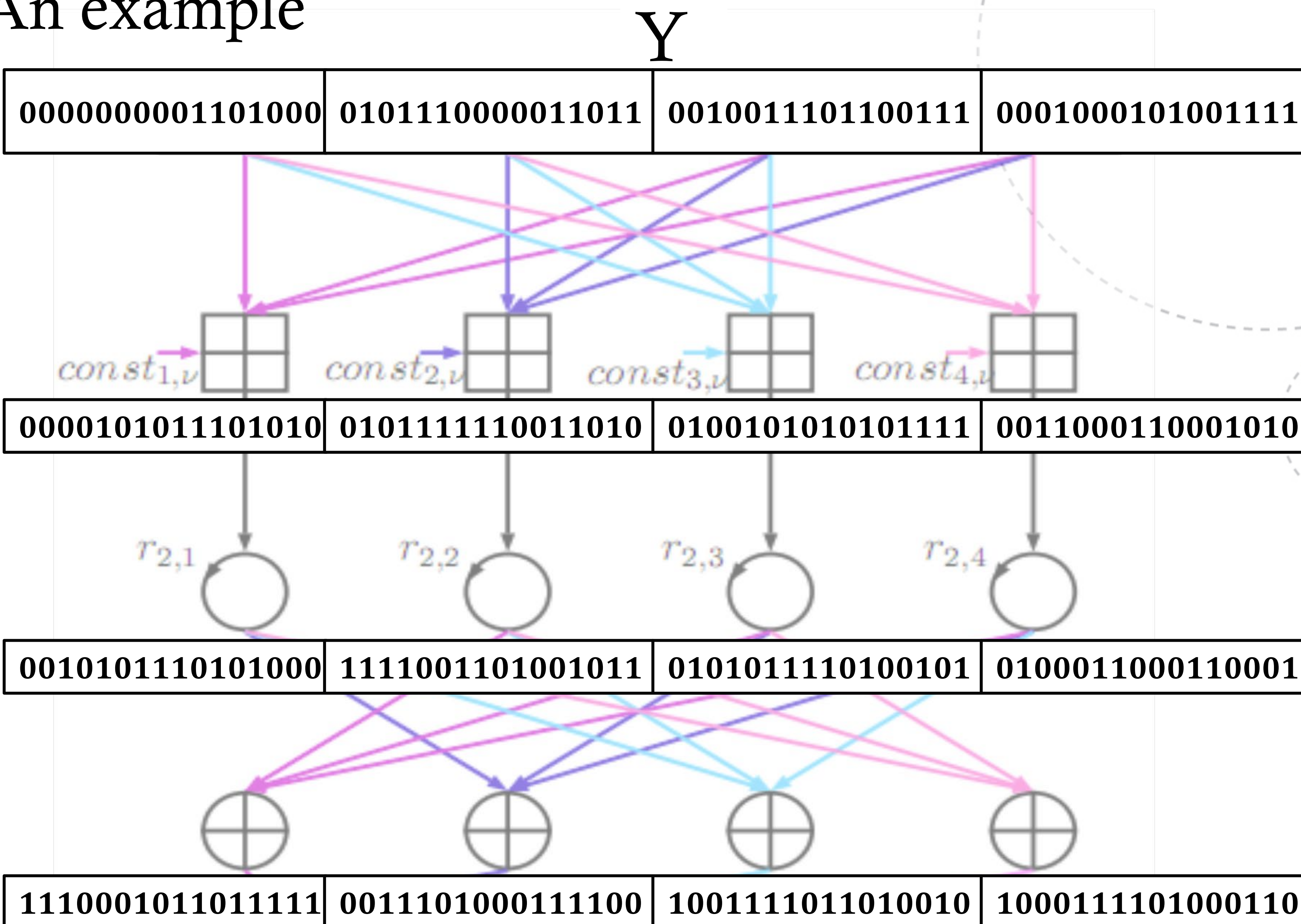

X
1100010101101110
0001101011110000
1000010001011111
1001111011001101
$const_{1,\mu}$
$const_{2,\mu}$
$const_{3,\mu}$
$const_{4,\mu}$
0101010110100101
0110010000001101
1100101001110010
0001001011101110
$r_{1,1}$
$r_{1,2}$
$r_{1,3}$
$r_{1,4}$
1010101101001010
0100000011010110
1110010110010100
0111000010010111
1001101100001011
0000111000001000
1101010111010101
0011111001001001

An example

X'

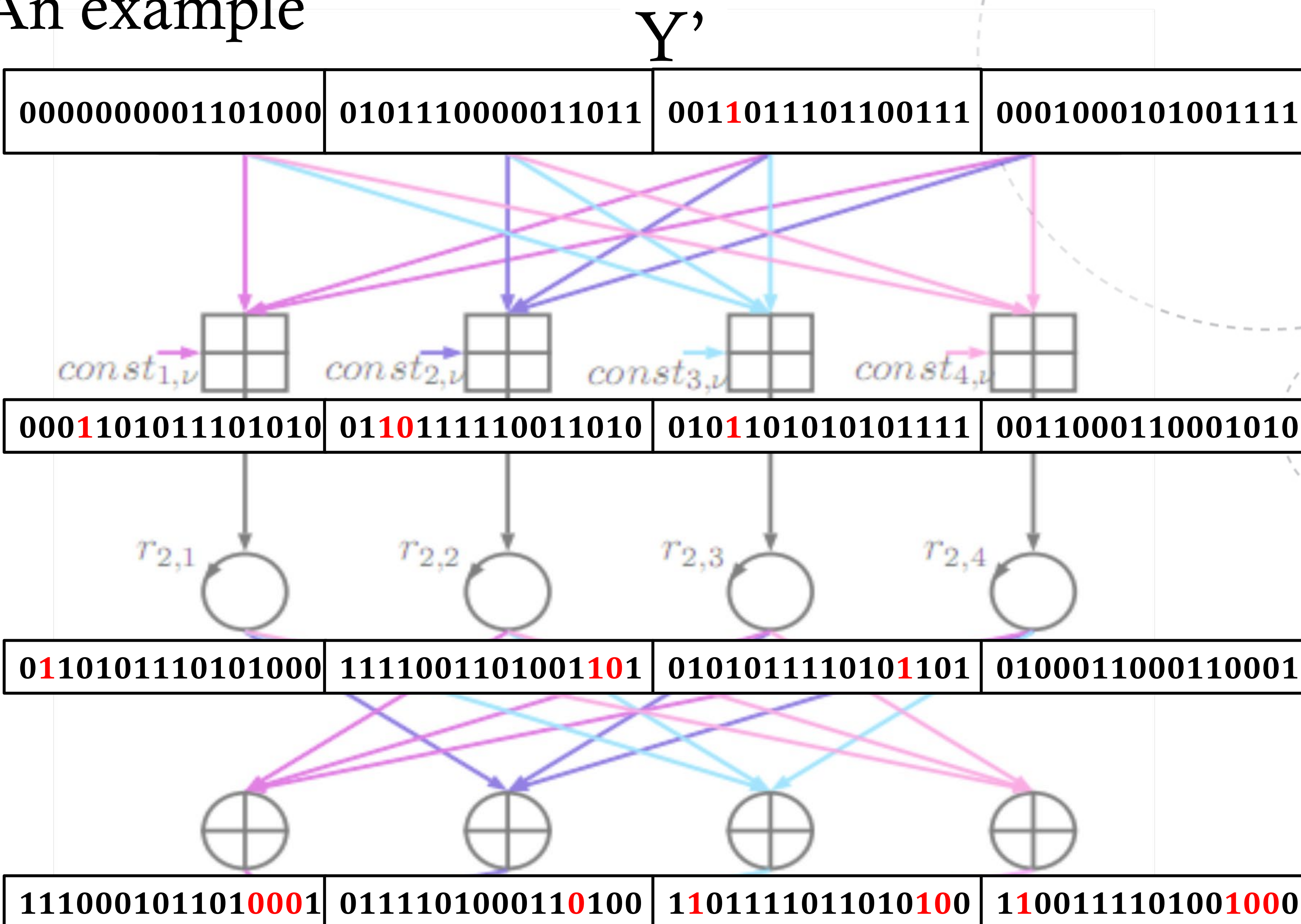

1100010101101100 0001101011110000 1000010001011111 1001111011001101
$const_{1,\mu}$
$const_{2,\mu}$
$const_{3,\mu}$
$const_{4,\mu}$
0101010110100011 0110010000001011 1100101001110000 0001001011101110
$r_{1,1}$
$r_{1,2}$
$r_{1,3}$
$r_{1,4}$
1010101101000110 0100000010110110 1110000110010100 0111000010010111
1001101101100111 0000101001100100 1101000110110101 0011101001000101

An example

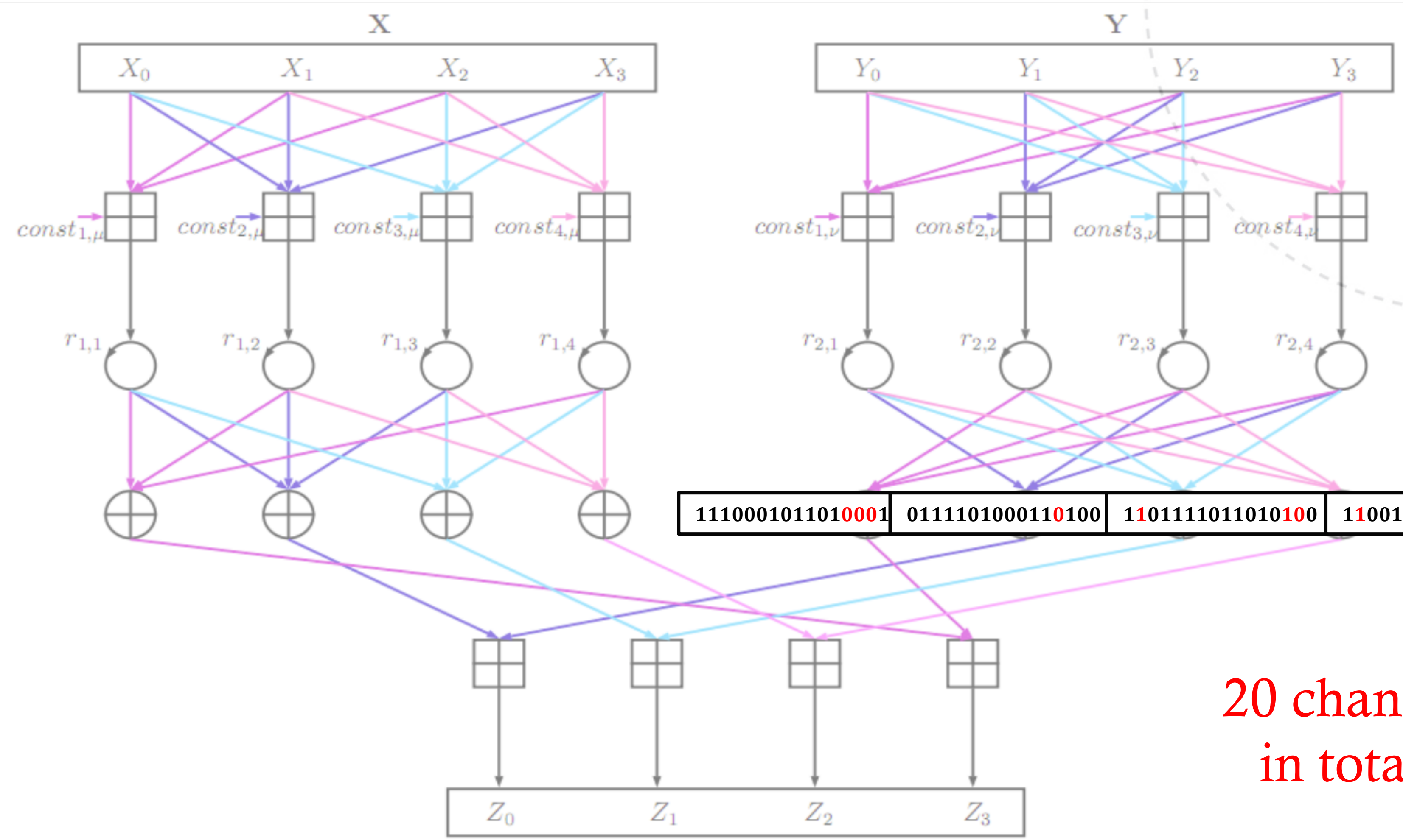


Y
0000000001101000 | 0101110000011011 | 0010011101100111 | 0001000101001111
$const_{1,\nu}$ $const_{2,\nu}$ $const_{3,\nu}$ $const_{4,\nu}$
0000101011101010 | 0101111110011010 | 0100101010101111 | 0011000110001010
$r_{2,1}$ $r_{2,2}$ $r_{2,3}$ $r_{2,4}$
0010101110101000 | 1111001101001011 | 0101011110100101 | 0100011000110001
1110001011011111 | 0011101000111100 | 1001111011010010 | 1000111101000110

An example


Y'
0000000001101000
0101110000011011
0011011101100111
0001000101001111
const1,ν
const2,ν
const3,ν
const4,ν
0001101011101010
0110111110011010
0101101010101111
0011000110001010
r2,1
r2,2
r2,3
r2,4
0110101110101000
1111001101001101
0101011110101101
0100011000110001
1110001011010001
0111101000110100
1101111011010100
1100111101001000

An example

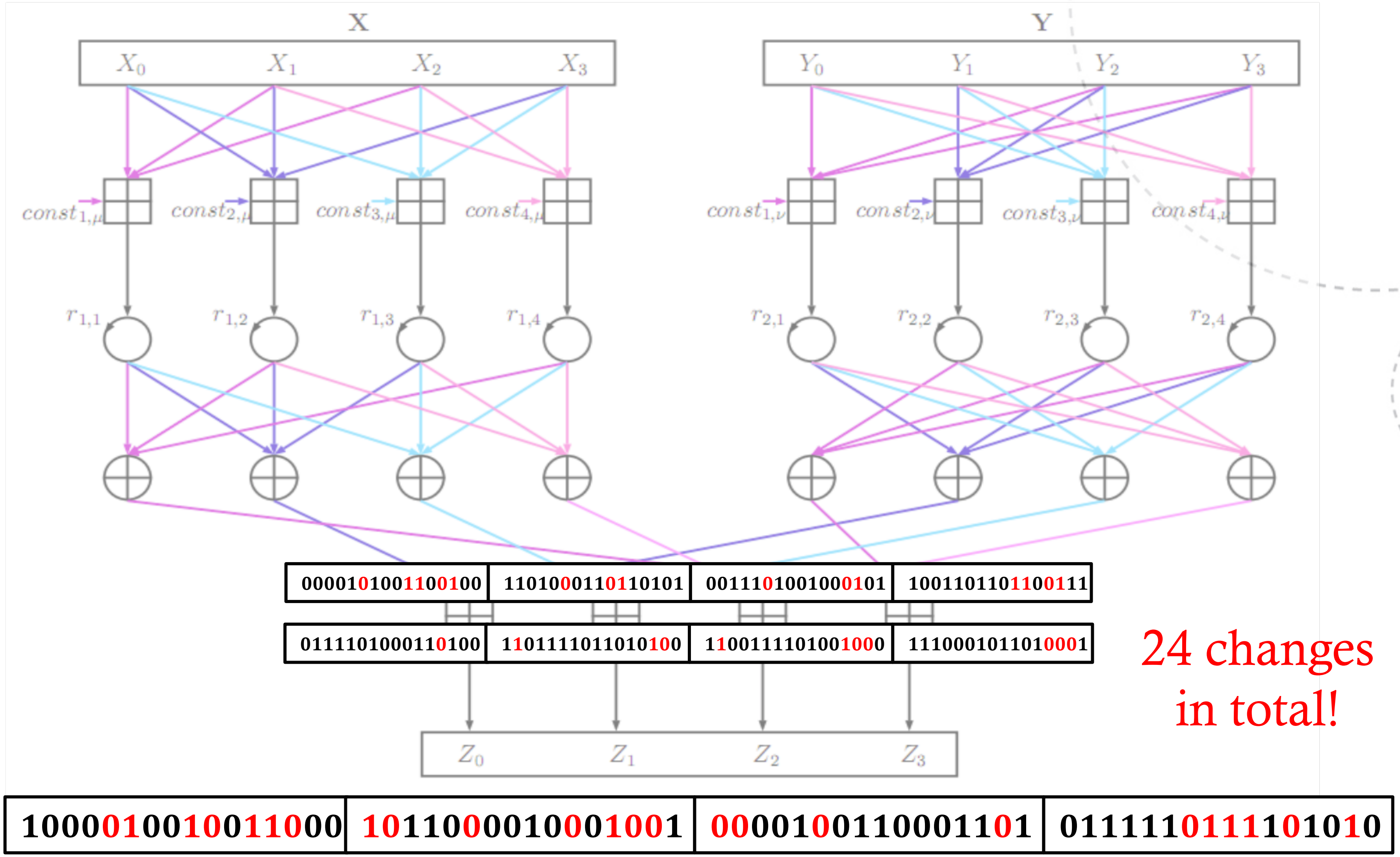


1110001011010001	0111101000110100	1101111011010100	1100111101001000

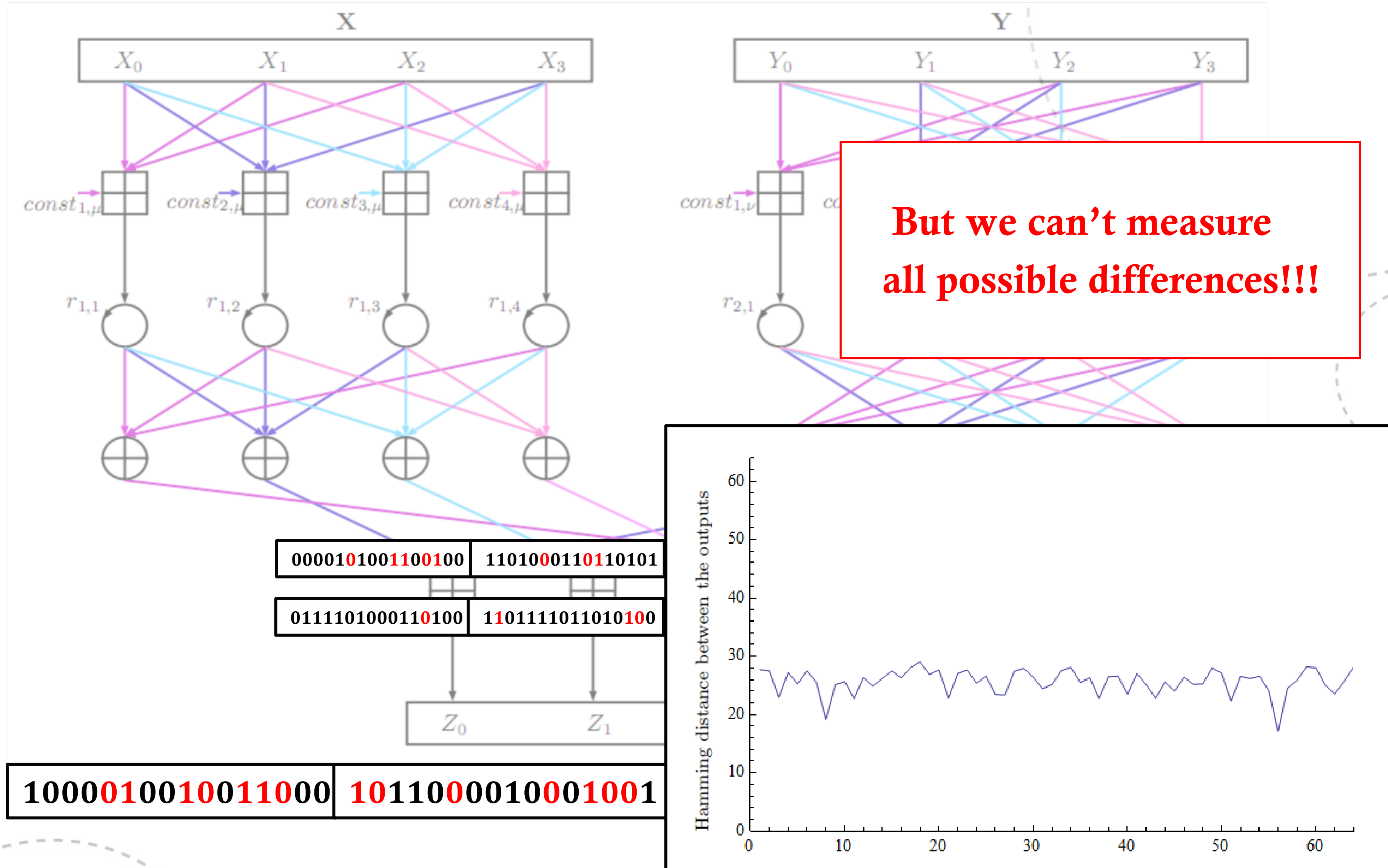
20 changes in total!

1100011011111101	1010000101000100	0101011101010001	1110100101011101

An example


X
Y
0000101001100100
1101000110110101
0011101001000101
1001101101100111
0111101000110100
1101111011010100
1100111101001000
1110001011010001
24 changes in total!
1000010010011000
1011000010001001
0000100110001101
0111110111101010

An example



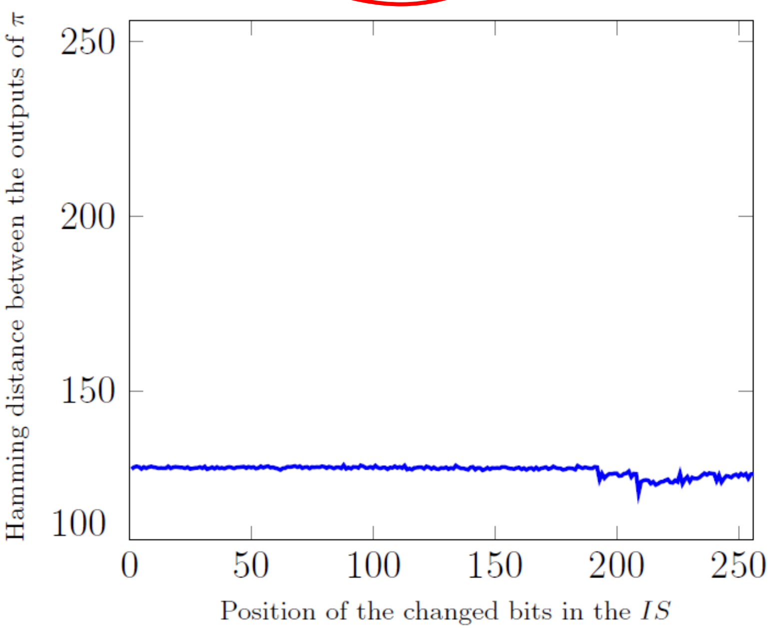
But we can't measure all possible differences!!!

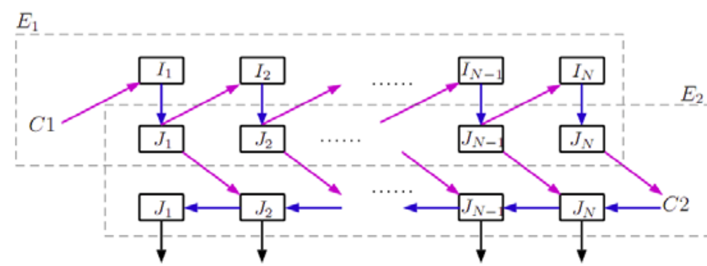
π-Cipher Security

- Bit diffusion of the one round of the permutation

$$HammingDistance(IS, IS') = 1$$

$$\pi(IS) \qquad \pi(IS')$$



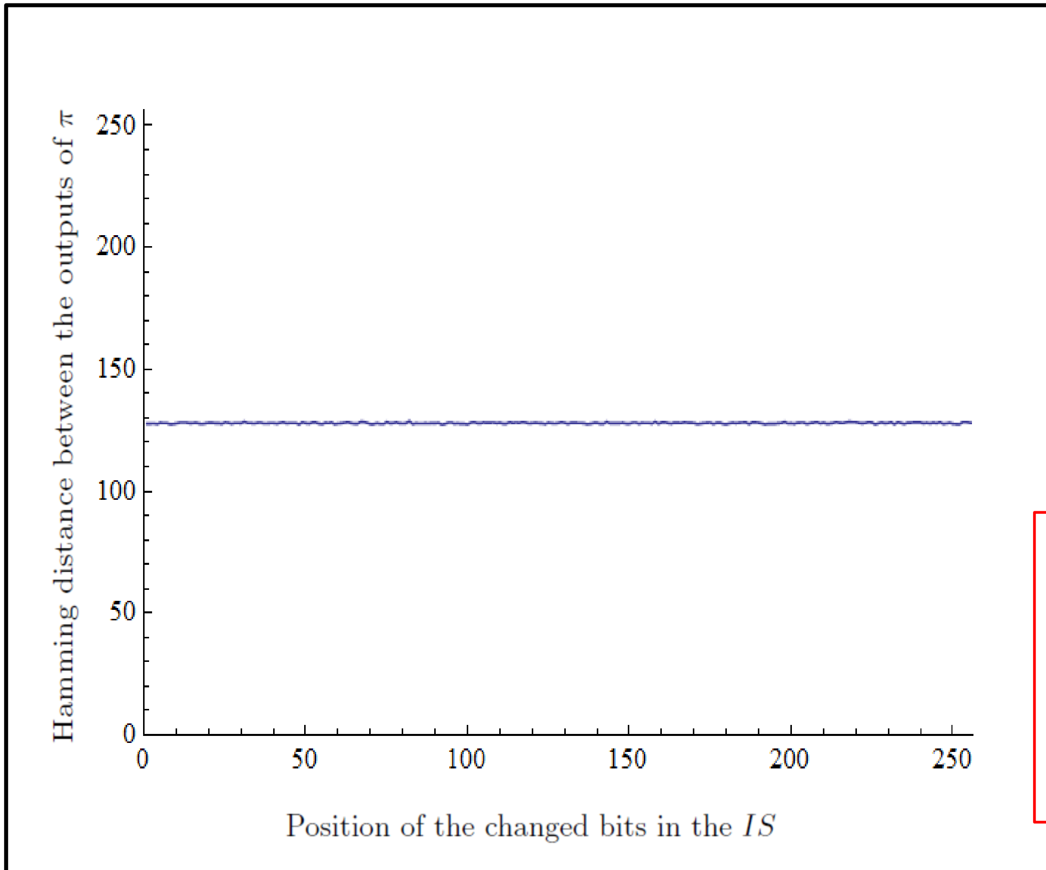


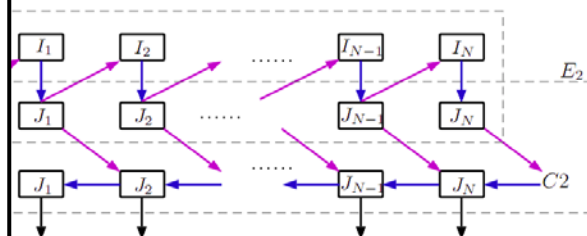
Even after ONLY one round one bit difference propagates in 1/2 of the bits

Avalanche effect of one round of the π function where $\omega = 16$

π-Cipher Security

- Bit diffusion of the one round of the permutation





After 3 rounds

Mean value 127.281

Avalanche effect of one round of the π function where $\omega = 16$

π-Cipher Security

- Similar construction as SHA-3 candidate Edon-R [Gligoroski et al. ’09] indicates solid differential properties

- New popular approach for ARX designs
  - **Automated tools**

    [Mouha et al. ’10], [Laurent ’12]

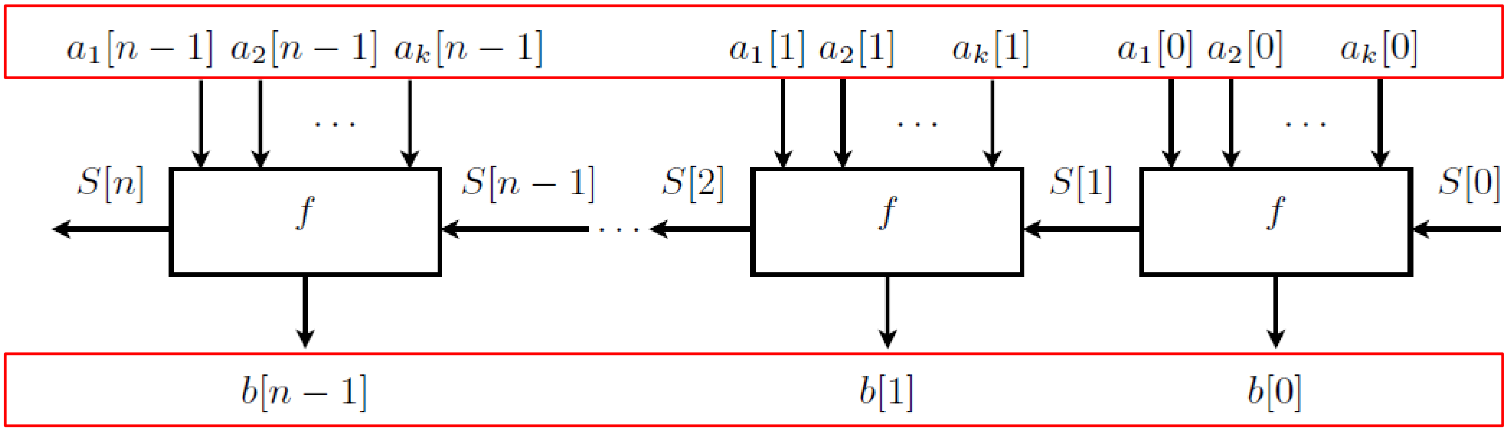
- **Ongoing work**

  – create a dedicated automated engine for π-Cipher for search of differential characteristics of a predefined weight

A taste of ARX automated tools (credit to N. Mouha)

Analysis of S-functions

Input: n-bit words $a_1, a_2, \ldots, a_k$



Output: word b

$$(b[i], S[i+1]) = f(a_1[i], a_2[i], \ldots, a_k[i], S[i]), \quad 0 \leq i < n$$

XOR Differential probability of modular addition

$$((x_1 \oplus \Delta x) + (y_1 \oplus \Delta y)) \oplus (x_1 + y_1) = \Delta z$$

$$\begin{cases} x_2 & \leftarrow x_1 \oplus \Delta x \\ y_2 & \leftarrow y_1 \oplus \Delta y \\ z_1 & \leftarrow x_1 + y_1 \\ z_2 & \leftarrow x_2 + y_2 \\ \Delta z & \leftarrow z_2 \oplus z_1 \end{cases} \Longrightarrow \begin{cases} x_2[i] & \leftarrow x_1[i] \oplus \Delta x[i] \\ y_2[i] & \leftarrow y_1[i] \oplus \Delta y[i] \\ z_1[i] & \leftarrow x_1[i] \oplus y_1[i] \oplus c_1[i] \\ c_1[i+1] & \leftarrow (x_1[i] + y_1[i] + c_1[i]) \gg 1 \\ z_2[i] & \leftarrow x_2[i] \oplus y_2[i] \oplus c_2[i] \\ c_2[i+1] & \leftarrow (x_2[i] + y_2[i] + c_2[i]) \gg 1 \\ \Delta z[i] & \leftarrow z_2[i] \oplus z_1[i] \end{cases}$$

S-function:

$$(\Delta z[i], S[i+1]) = f(x_1[i], y_1[i], \Delta x[i], \Delta y[i], S[i]), \quad 0 \leq i < n$$

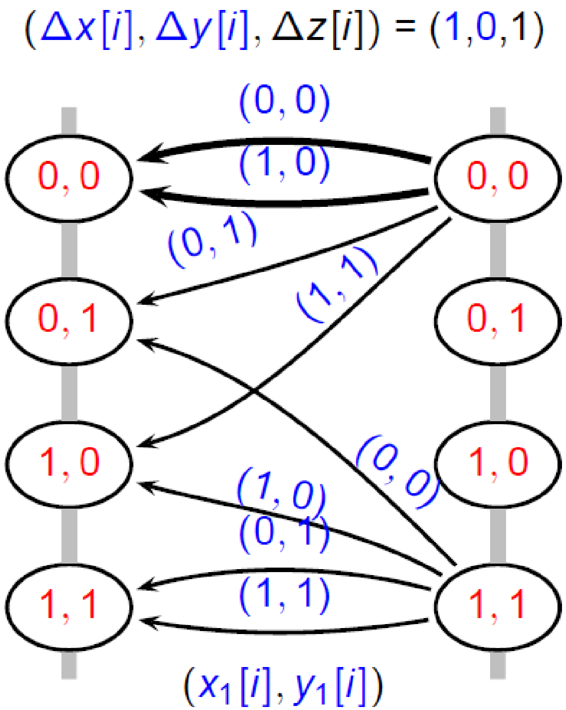
$$S[i] \leftarrow (c_1[i], c_2[i]),$$

$$S[i+1] \leftarrow (c_1[i+1], c_2[i+1]).$$

(credit to N. Mouha)

XOR Differential probability of modular addition

Represent as graphs:

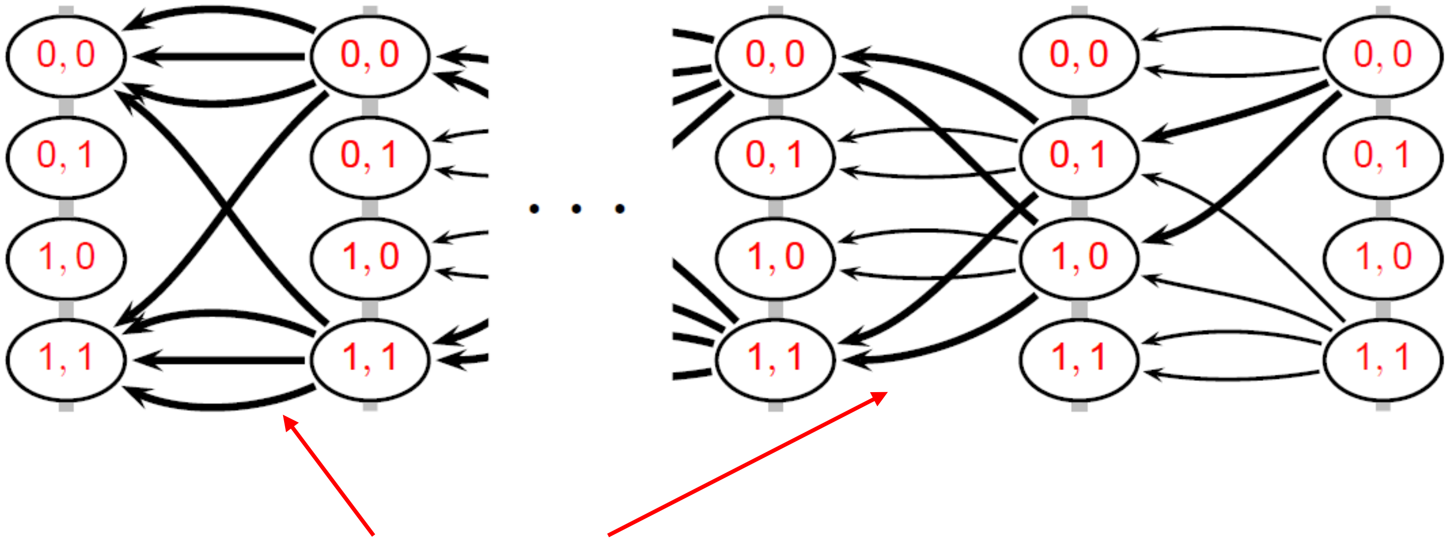


$$\begin{cases} x_2[i] & \leftarrow x_1[i] \oplus \Delta x[i] \\ y_2[i] & \leftarrow y_1[i] \oplus \Delta y[i] \\ z_1[i] & \leftarrow x_1[i] \oplus y_1[i] \oplus c_1[i] \\ c_1[i+1] & \leftarrow (x_1[i] + y_1[i] + c_1[i]) \gg 1 \\ z_2[i] & \leftarrow x_2[i] \oplus y_2[i] \oplus c_2[i] \\ c_2[i+1] & \leftarrow (x_2[i] + y_2[i] + c_2[i]) \gg 1 \\ \Delta z[i] & \leftarrow z_2[i] \oplus z_1[i] \end{cases}$$

(credit to N. Mouha)

XOR Differential probability of modular addition

Represent as graphs:

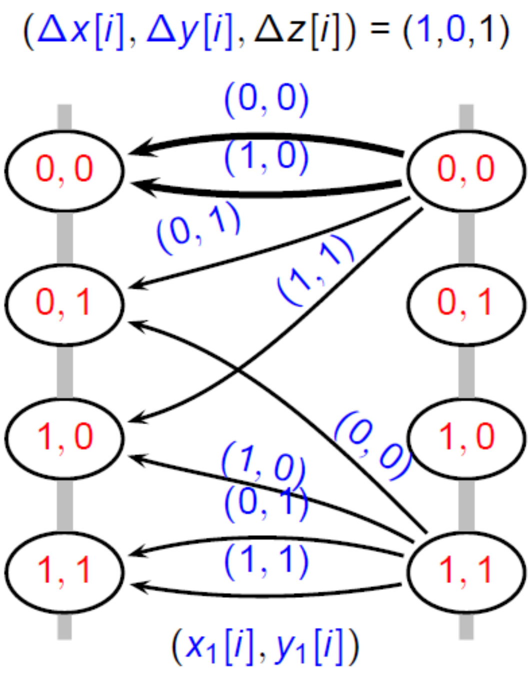


Valid paths with desired differential

Count the paths using adjacency matrices!

(credit to N. Mouha)

XOR Differential probability of modular addition



$$S[i]$$

$$\begin{array}{cc} & (0,0),(0,1),(1,0),(1,1) \\ S[i+1]\ \begin{array}{c}(0,0)\\(0,1)\\(1,0)\\(1,1)\end{array} & \frac{1}{4}\begin{bmatrix} \mathbf{2} & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix} = A_{101} \end{array}$$

Probability: $\mathrm{xdp}^{+}(\Delta x, \Delta y \rightarrow \Delta z) = L A_{w[n-1]} \cdots A_{w[1]} A_{w[0]} C$

$$w[i] = \Delta x[i] \parallel \Delta y[i] \parallel \Delta z[i], \ \ 0 \leq i < n,$$
$$L = [\ 1 \quad 1 \quad \cdots \quad 1\ ],$$
$$C = [\ 1 \quad 0 \quad \cdots \quad 0\ ]^T.$$

(credit to N. Mouha)

Thank you for listening!