بنام خدا

آشنایی با مشخصه های تفاضلی ناممکن و همبستگی صفر

صادق صادقی

دانشگاه خوارزمی

پاییز ۹۸

s.sadeghi.khu@gmail.com

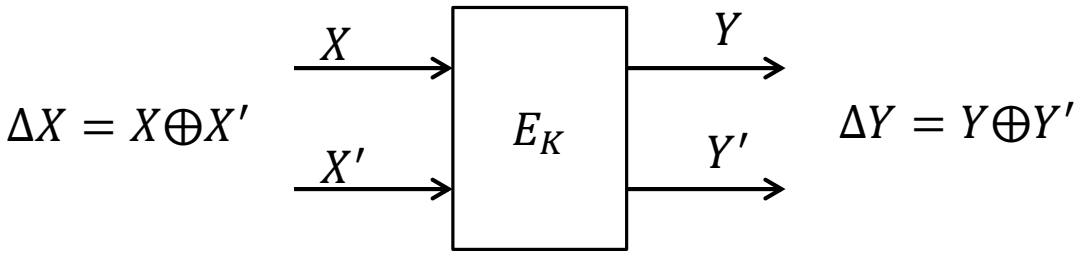
حمله تفاضلی

E. Biham and A. Shamir
Differential cryptanalysis of DES-like cryptosystems.
CRYPTOLOGY, 1991. 4(1): p. 3-72

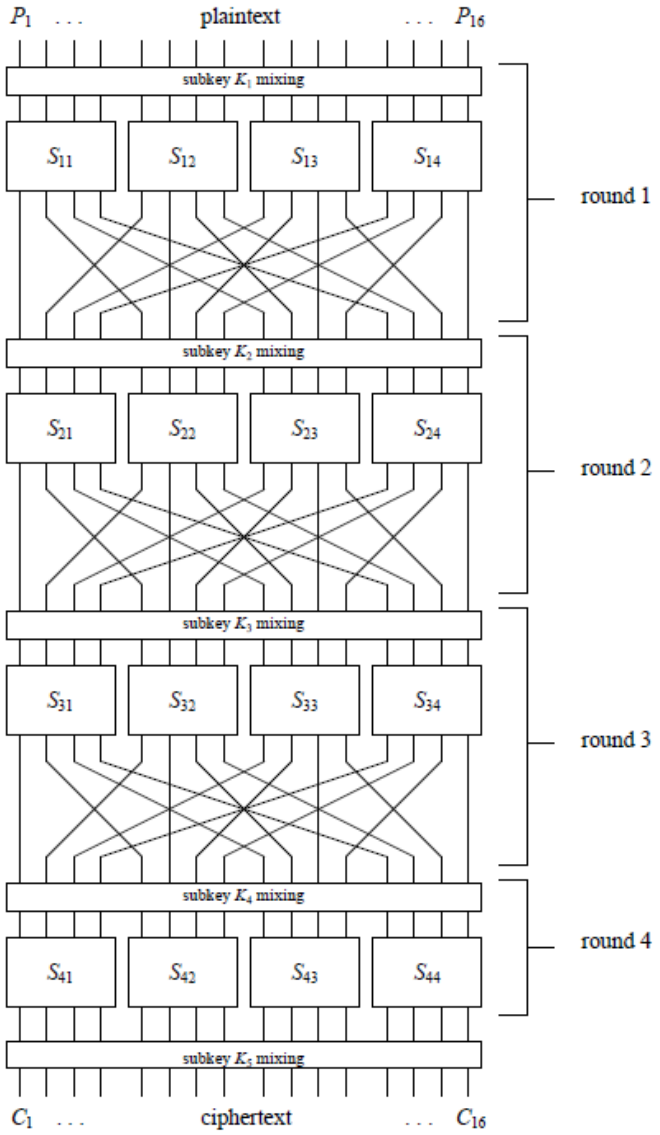
E. Biham and A. Shamir
Differential cryptanalysis of the data *encryption standard.*.
Springer, Berlin, 1993.

تغییرات بین دو ورودی از متن اصلی (حتی به اندازه یک بیت) چگونه بر روی خروجی رمز شده تـاثیر مـی-گذارد و نتیجه رمز شده این دو متن به چه اندازه با یکدیگر اختلاف دارند.

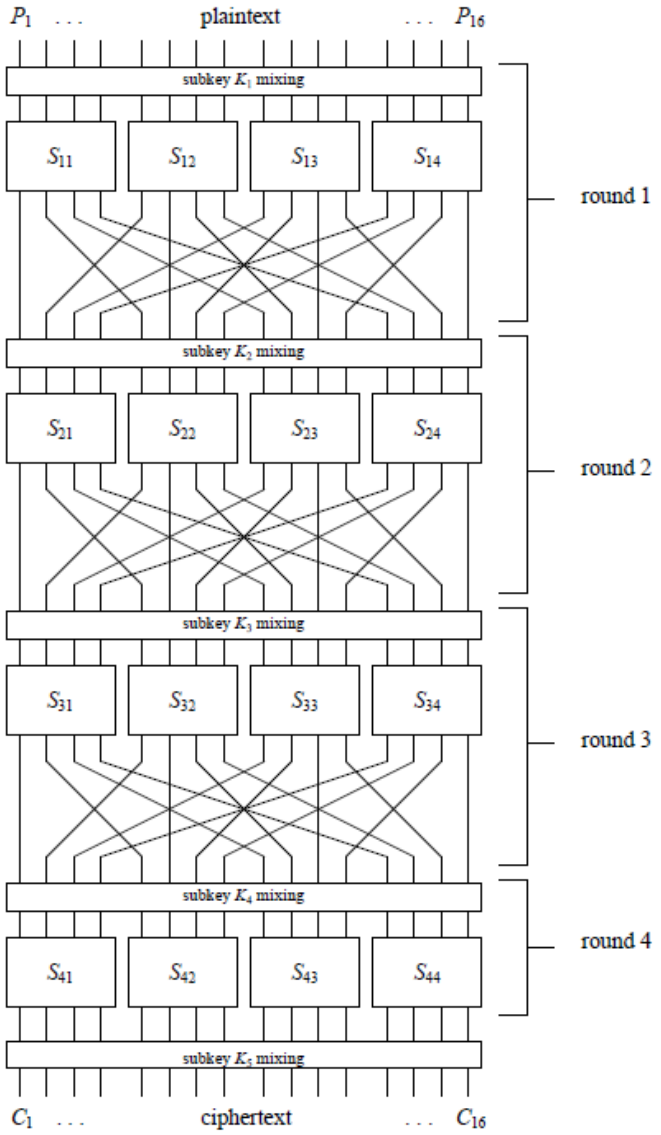
$$E_K: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$$



$$\Delta X \xrightarrow{p} \Delta Y \longrightarrow N_D \approx \frac{c}{p}$$



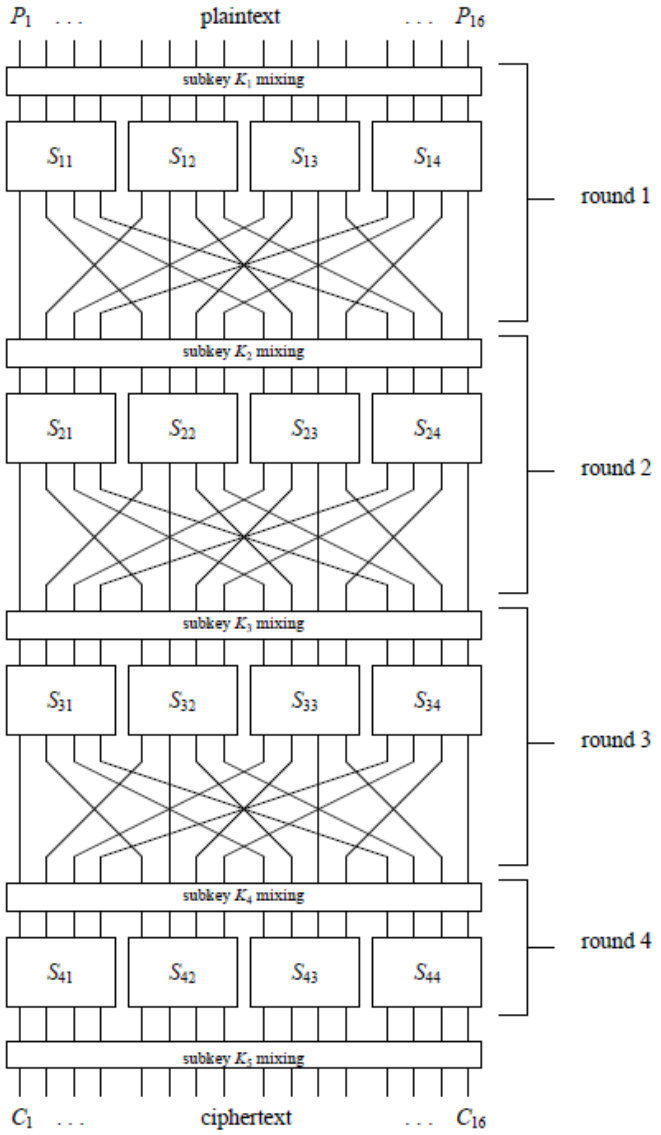
Heys, Howard M. "A tutorial on linear and differential cryptanalysis." *Cryptologia* 26.3 (2002): 189-221.



X	Y
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Sbox →

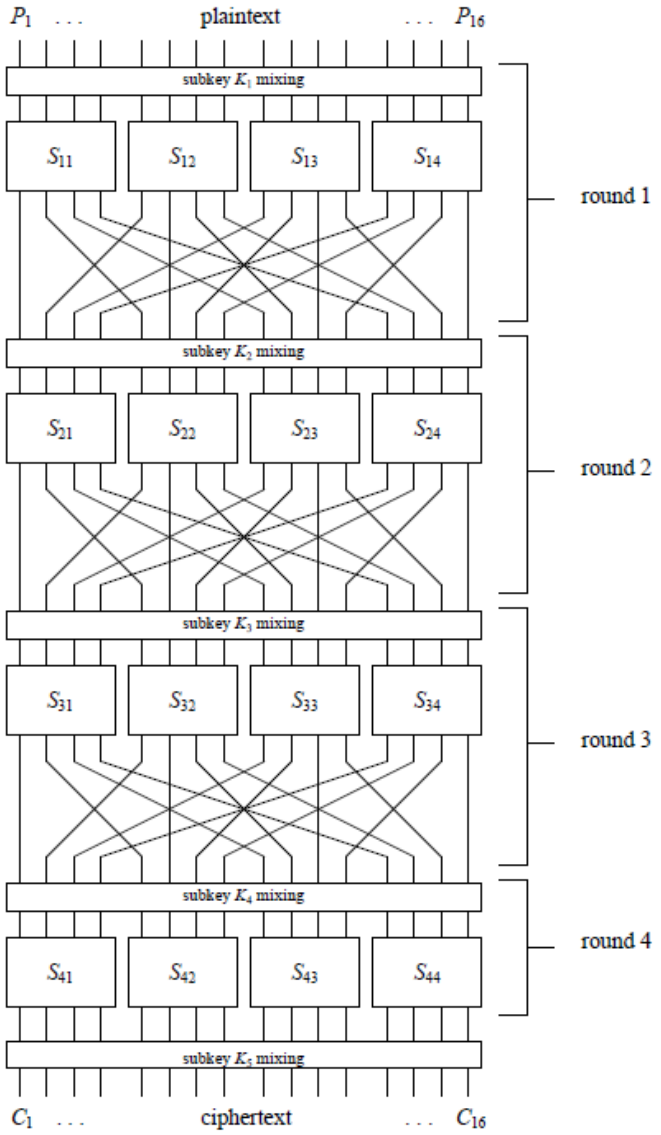
Heys, Howard M. "A tutorial on linear and differential cryptanalysis." *Cryptologia* 26.3 (2002): 189-221.



$$\Delta X = 1000 \longrightarrow \Delta Y = 1011$$

X	Y
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

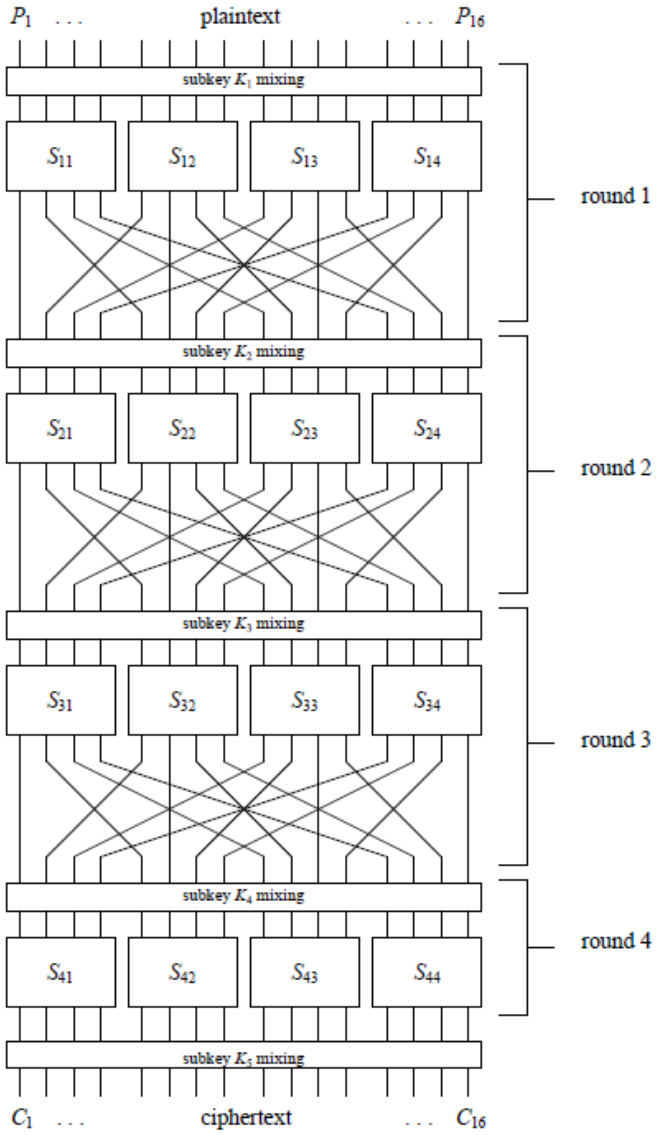
Sbox →



$$\Delta X = 1000 \longrightarrow \Delta Y = 1011$$

X	Y	X'
0000	1110	1000
0001	0100	1001
0010	1101	1010
0011	0001	1011
0100	0010	1100
0101	1111	1101
0110	1011	1110
0111	1000	1111
1000	0011	0000
1001	1010	0001
1010	0110	0010
1011	1100	0011
1100	0101	0100
1101	1001	0101
1110	0000	0110
1111	0111	0111

Sbox →



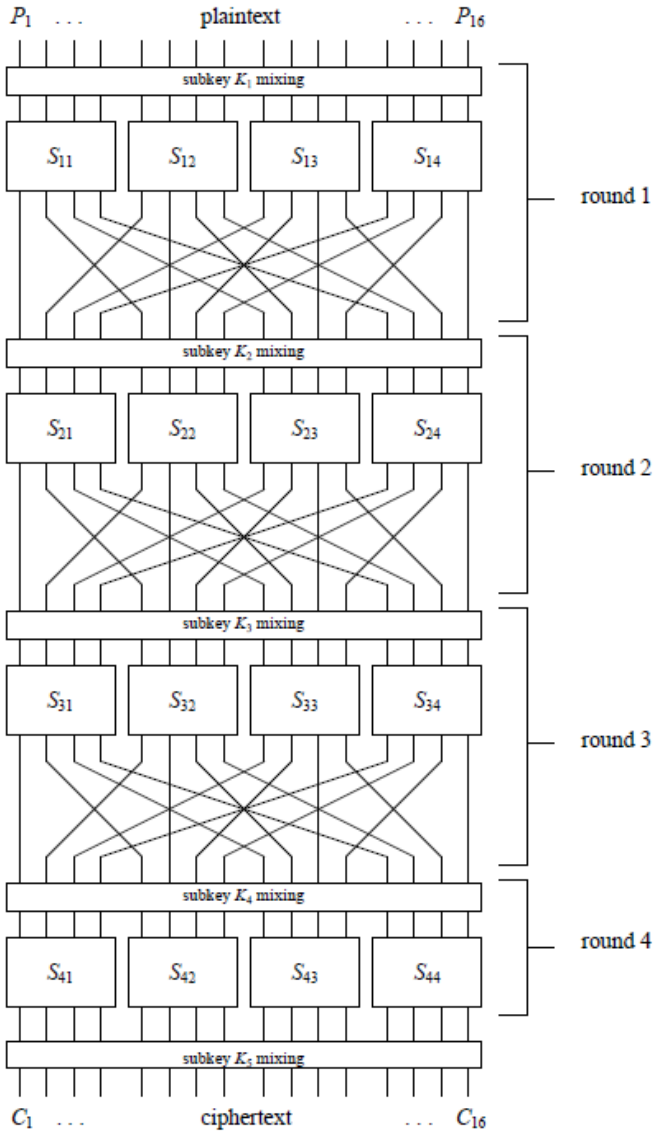
$$\Delta X = 1000 \longrightarrow \Delta Y = 1011$$

X	Y
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Sbox →

X'	Y'
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000

Sbox →

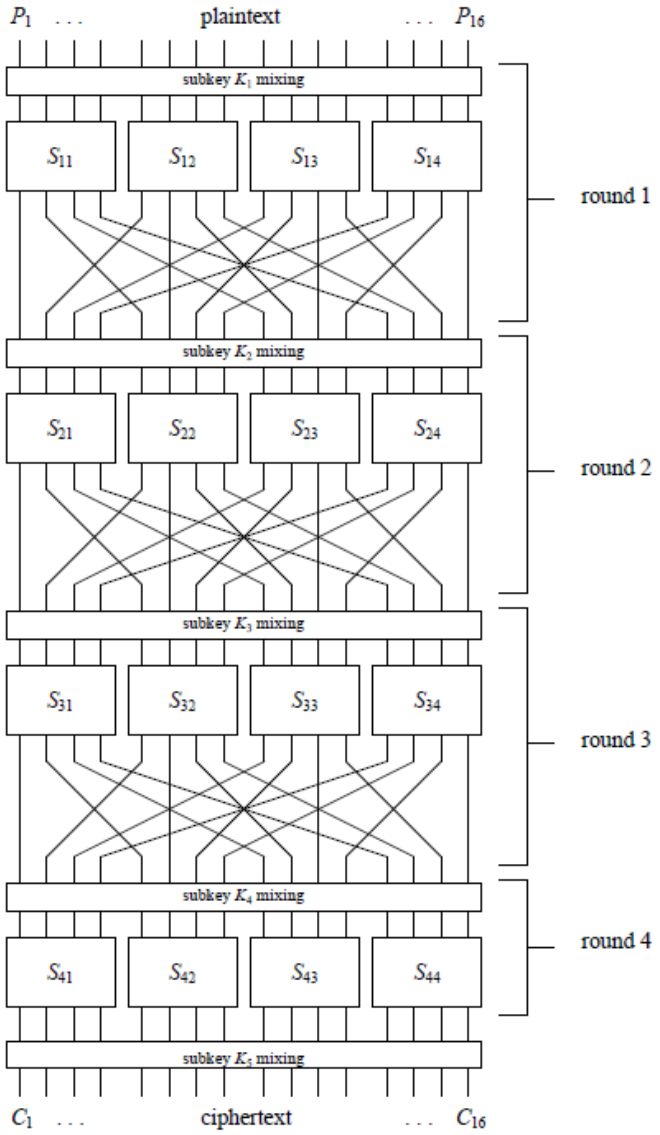


$$\Delta X = 1000 \longrightarrow \Delta Y = 1011$$

X	Y	X'	Y'	ΔY
0000	1110	1000	0011	1101
0001	0100	1001	1010	1110
0010	1101	1010	0110	0101
0011	0001	1011	1100	1011
0100	0010	1100	0101	0111
0101	1111	1101	1001	0110
0110	1011	1110	0000	1011
0111	1000	1111	0111	1111
1000	0011	0000	1110	1101
1001	1010	0001	0100	1110
1010	0110	0010	1101	0101
1011	1100	0011	0001	1011
1100	0101	0100	0010	0111
1101	1001	0101	1111	0110
1110	0000	0110	1011	1011
1111	0111	0111	1000	1111

Sbox → **Sbox** →

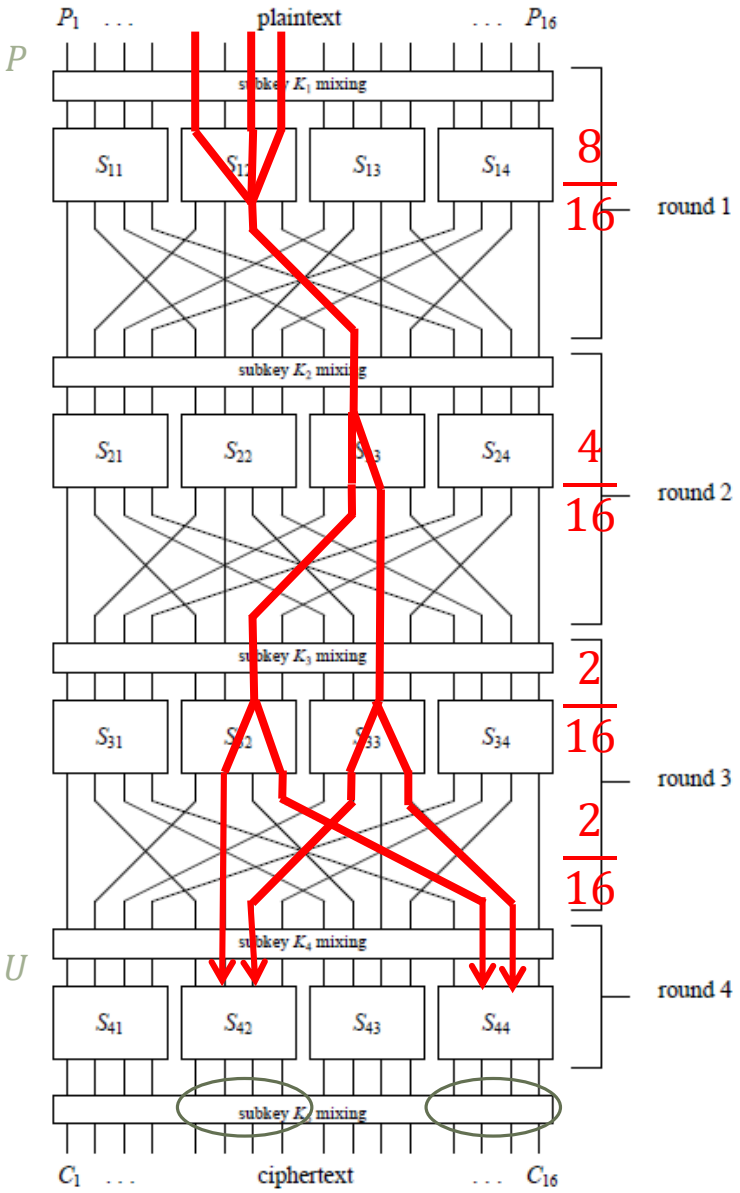
Heys, Howard M. "A tutorial on linear and differential cryptanalysis." *Cryptologia* 26.3 (2002): 189-221.



$$\Delta X = 1000 \xrightarrow{P_r = \frac{1}{4}} \Delta Y = 1011$$

X	Y	X'	Y'	ΔY
0000	1110	1000	0011	1101
0001	0100	1001	1010	1110
0010	1101	1010	0110	0101
0011	0001	1011	1100	~~1011~~
0100	0010	1100	0101	0111
0101	1111	1101	1001	0110
0110	1011	1110	0000	~~1011~~
0111	1000	1111	0111	1111
1000	0011	0000	1110	1101
1001	1010	0001	0100	1110
1010	0110	0010	1101	0101
1011	1100	0011	0001	~~1011~~
1100	0101	0100	0010	0111
1101	1001	0101	1111	0110
1110	0000	0110	1011	~~1011~~
1111	0111	0111	1000	1111

Sbox → **Sbox** →



$$\Delta P = [0000\ 1011\ 0000\ 0000]$$

$$\downarrow P_r = 2^{-9}$$

$$\Delta U = [0000\ 0110\ 0000\ 0110]$$

Heys, Howard M. "A tutorial on linear and differential cryptanalysis." *Cryptologia* 26.3 (2002): 189-221.

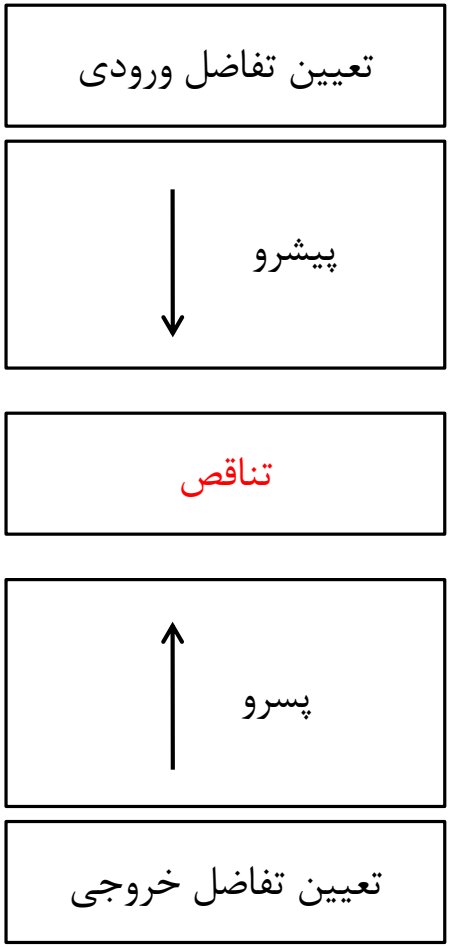
حمله تفاضلی ناممکن

Biham, Eli, Alex Biryukov, and Adi Shamir.
Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials.
International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1999.

Knudsen, Lars.
DEAL-a 128-bit block cipher.
Complexity 258.2 (1998): 216.

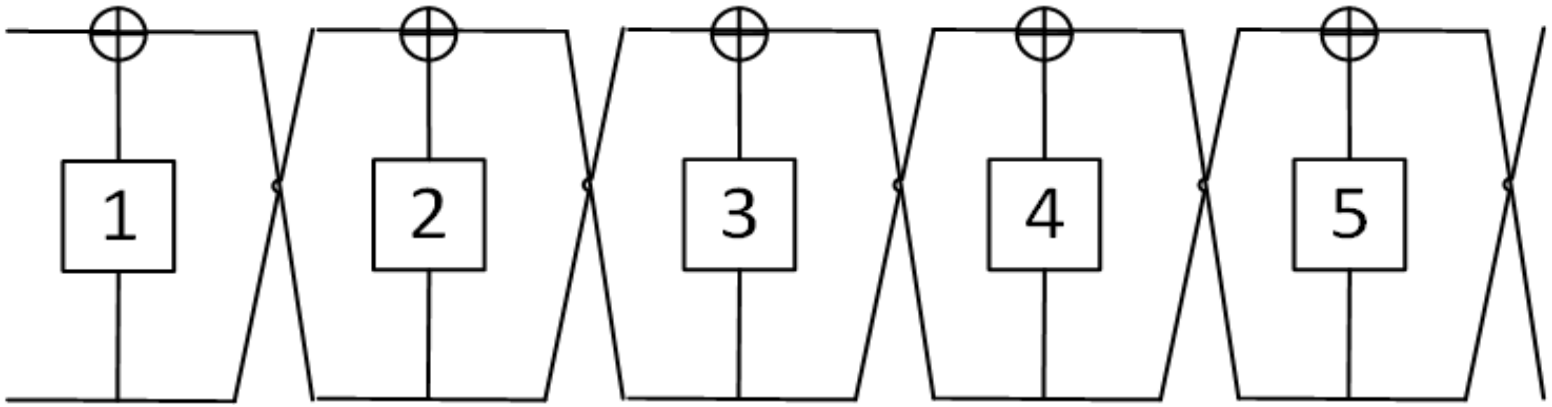
هدف جستجو برای طولانی‌ترین مشخصه تفاضلی با احتمال صفر

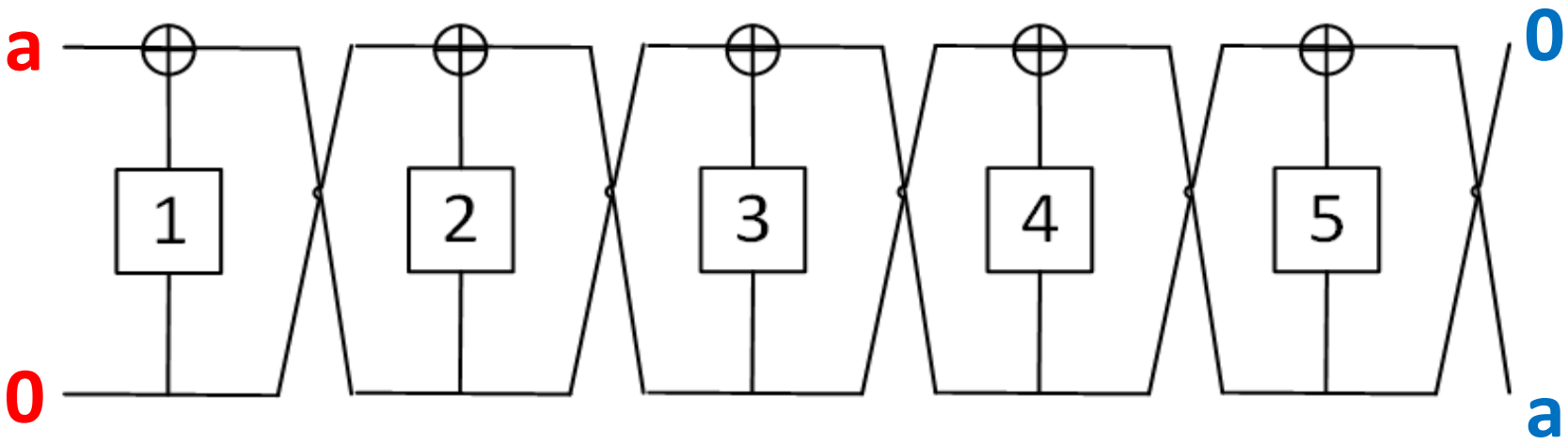
هدف جستجو برای طولانی‌ترین مشخصه تفاضلی با احتمال صفر

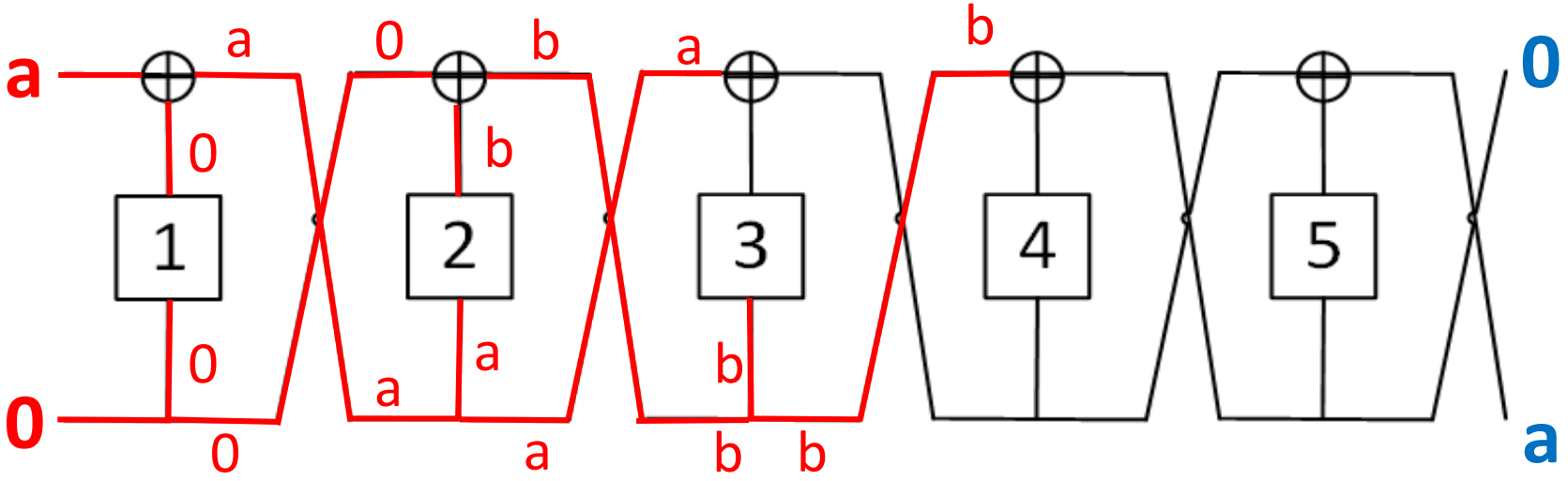


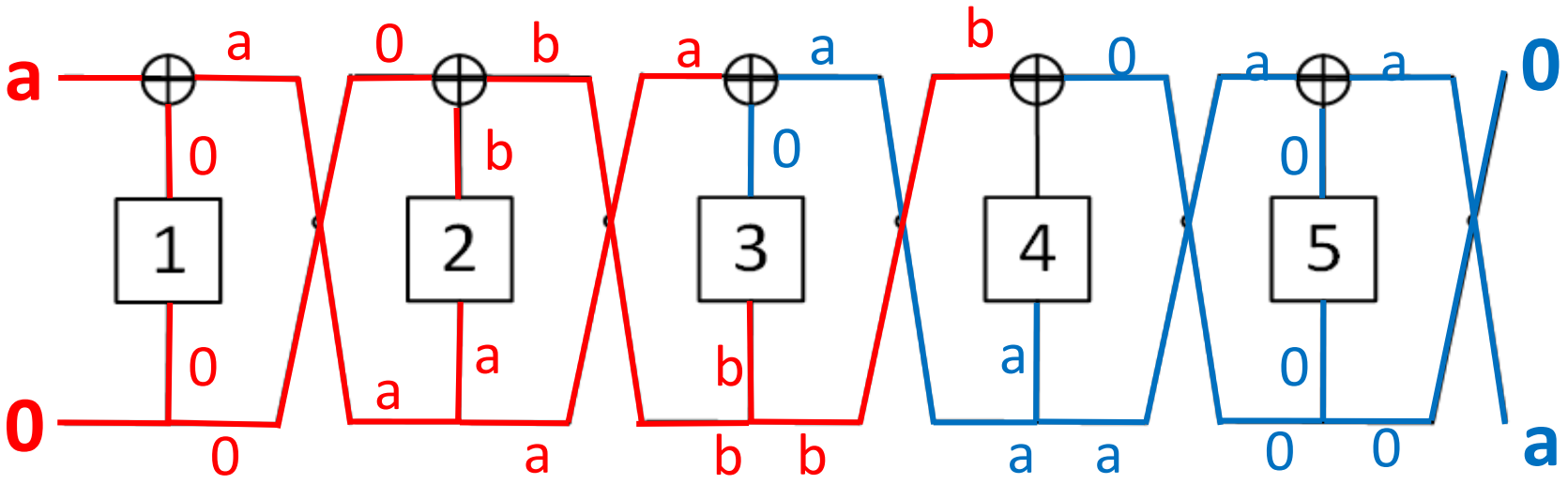
روش فقدان در میانه

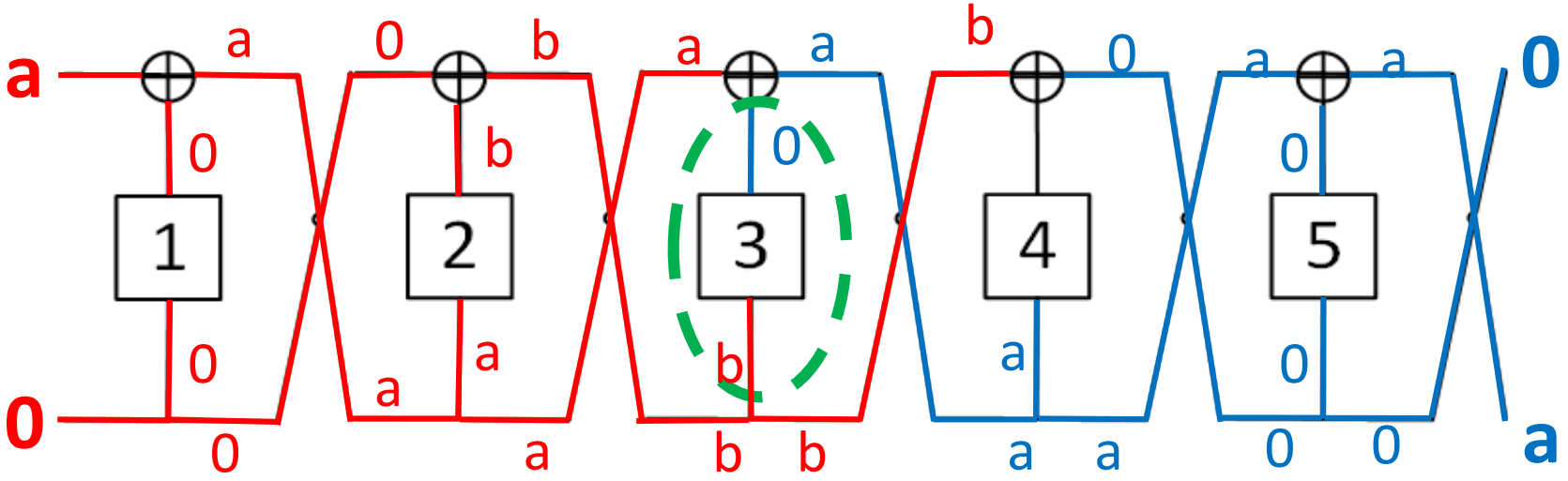
Biham, et al., *Miss in the Middle Attacks on IDEA and Khufu.* International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 1999.


1
2
3
4
5

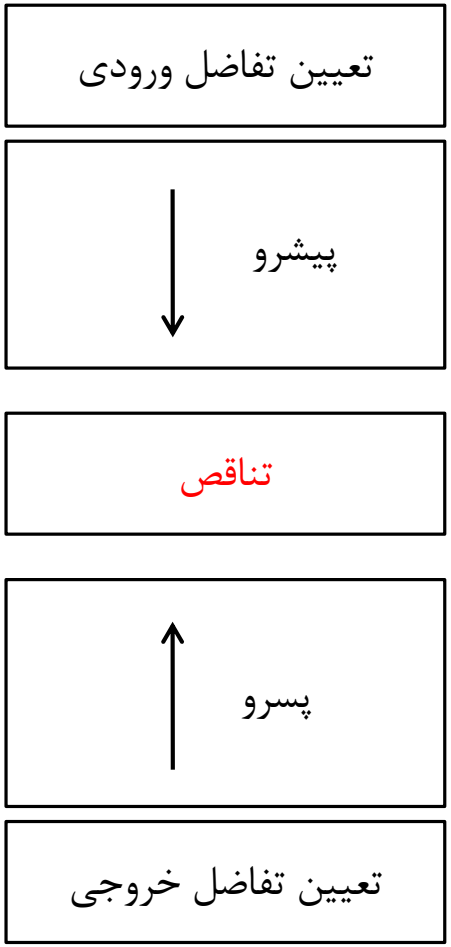

a
0
1
2
3
4
5
0
a


a
0
a
0
b
a
b
0
a
0
1
2
3
4
5
0
a
0
a
a
b
b
b


a
0
1
2
3
4
5
0
a


a
0
a
0
b
a
a
b
0
a
a
0
0
1
2
3
4
5
0
b
0
0
0
a
a
b
a
a
0
0
a
a
b
b
a
a
0
0
a

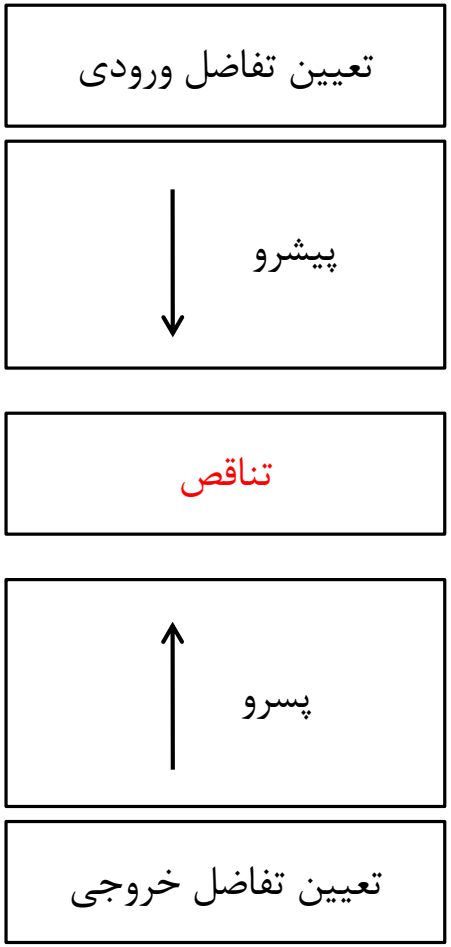
هدف جستجو برای طولانی‌ترین مشخصه تفاضلی با احتمال صفر



روش فقدان در میانه

Biham, et al., *Miss in the Middle Attacks on IDEA and Khufu.* International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 1999.

هدف جستجو برای طولانی‌ترین مشخصه تفاضلی با احتمال صفر



روش فقدان در میانه

Biham, et al., *Miss in the Middle Attacks on IDEA and Khufu.* International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 1999.

روش ماتریسی

Kim, J., S. Hong, and J. Lim, *Impossible differential cryptanalysis using matrix method.* Discrete Mathematics, 2010. **310**(5): p. 988-1002

روش UID

Luo, Y., et al., A unified method for finding impossible differentials of block cipher structures. Information Sciences, 2014. 263: p. 211-220

روش وو-وانگ

Wu, S. and M. Wang. Automatic search of truncated impossible differentials for word-oriented block ciphers. in International Conference on Cryptology in India. 2012. Springe

تعریف انواع تفاضل	
تفاضل صفر	$\mathbf{0}$
تفاضل ثابت و غیر صفر	$\boldsymbol{l_i}$
تفاضل دلخواه و غیر صفر	$\boldsymbol{m_i}$
تفاضل دلخواه	$\boldsymbol{r_i}$

فرض کنید ساختار رمز قالبی S دارای n زیرقالب باشد و بردار $U = (u_1, \cdots, u_n)$ بردار تفاضل ورودی باشد

تعریف: دو بردار تفاضلی $U = (u_1, \cdots, u_n)$ و $V = (v_1, \cdots, v_n)$ ناسازگار هستند اگر یک زیرمجموعه $I \subseteq \{1,2, \cdots, n\}$ وجود داشته باشد به طوری که

$$\oplus_{i \in I} u_i \neq \oplus_{i \in I} v_i$$

فرض کنید ساختار رمز قالبی S دارای n زیرقالب باشد و بردار $U = (u_1, \cdots, u_n)$ بردار تفاضل ورودی باشد

تعریف: دو بردار تفاضلی $U = (u_1, \cdots, u_n)$ و $V = (v_1, \cdots, v_n)$ ناسازگار هستند اگر یک زیرمجموعه $I \subseteq \{1,2, \cdots, n\}$ وجود داشته باشد به طوری که

$$\oplus_{i \in I} u_i \neq \oplus_{i \in I} v_i$$

مثال(بردارهای تفاضلی ناسازگار)

$U = (l_1 \oplus m_1, 0)$

$V = (l_1, 0)$

$\Rightarrow$ $l_1 \oplus m_1 \neq l_1$

فرض کنید ساختار رمز قالبی S دارای n زیرقالب باشد و بردار $U = (u_1, \cdots, u_n)$ بردار تفاضل ورودی باشد

تعریف: دو بردار تفاضلی $U = (u_1, \cdots, u_n)$ و $V = (v_1, \cdots, v_n)$ ناسازگار هستند اگر یک زیرمجموعه $I \subseteq \{1,2, \cdots, n\}$ وجود داشته باشد به طوری که

$$\oplus_{i \in I} u_i \neq \oplus_{i \in I} v_i$$

مثال(بردارهای تفاضلی ناسازگار)

$U = (l_1 \oplus m_1, 0)$

$V = (l_1, 0)$

$l_1 \oplus m_1 \neq l_1$

$U = (u_1, u_2) = (l_1, l_1 \oplus m_1)$

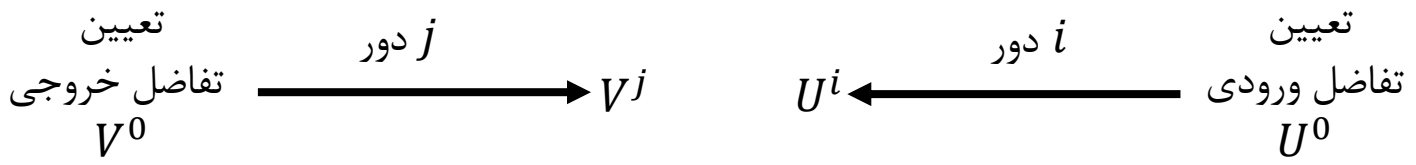
$V = (v_1, v_2) = (m_2, m_2)$

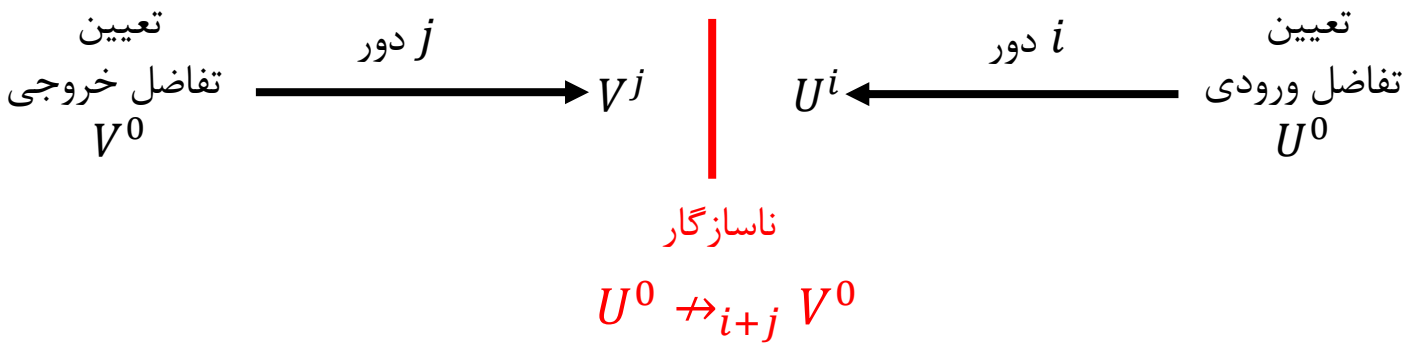
$u_1 \oplus u_2 = m_1$

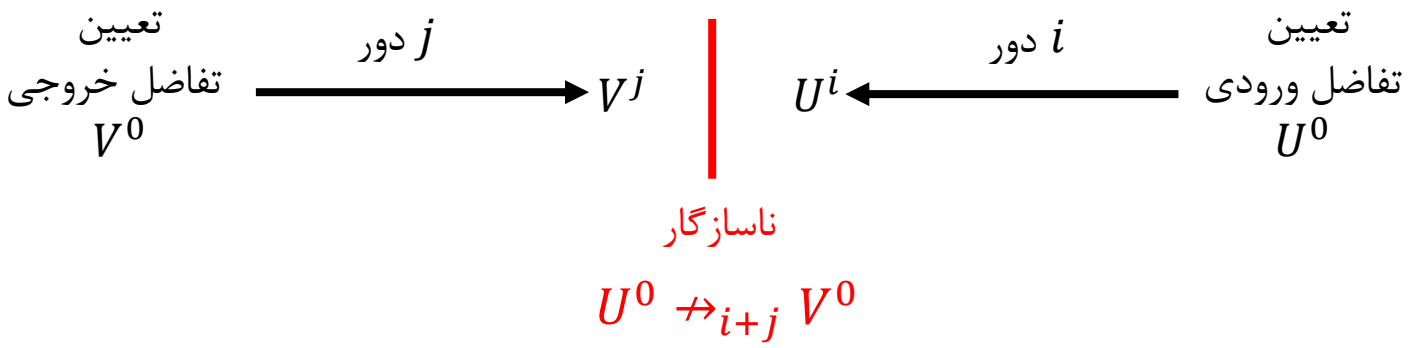
$v_1 \oplus v_2 = 0$

تعیین
تفاضل ورودی
U^0

تعیین
تفاضل خروجی
V^0


تعیین
تفاضل ورودی
U^0
i دور
U^i
تعیین
تفاضل خروجی
V^0
j دور
V^j

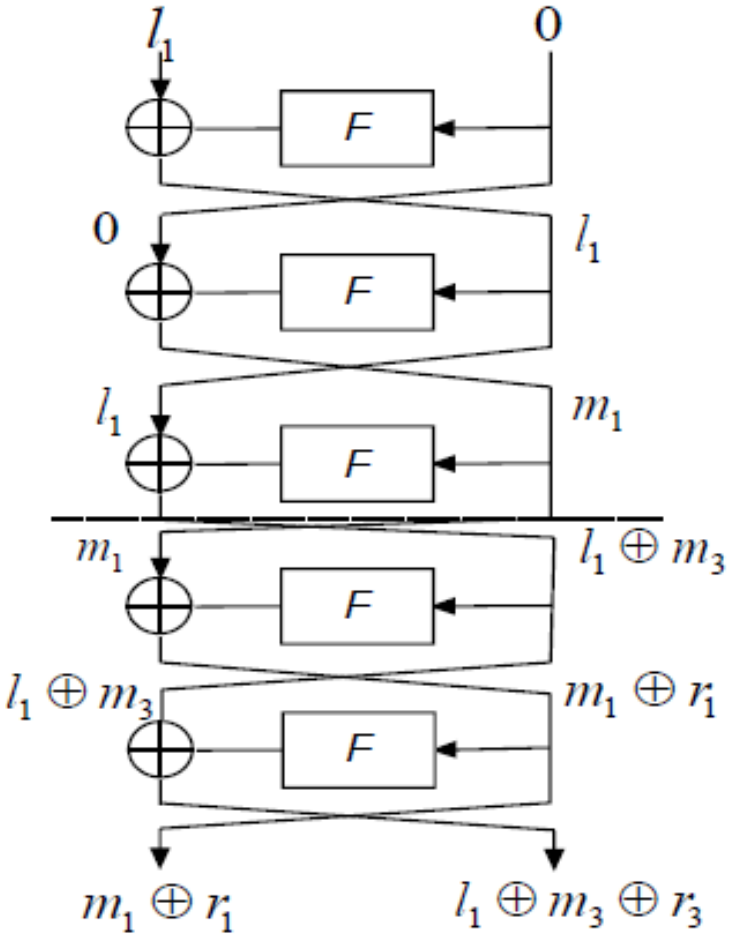

تعیین
تفاضل ورودی
U^0
i دور
U^i
V^j
j دور
تعیین
تفاضل خروجی
V^0
ناسازگار
$U^0 \nrightarrow_{i+j} V^0$

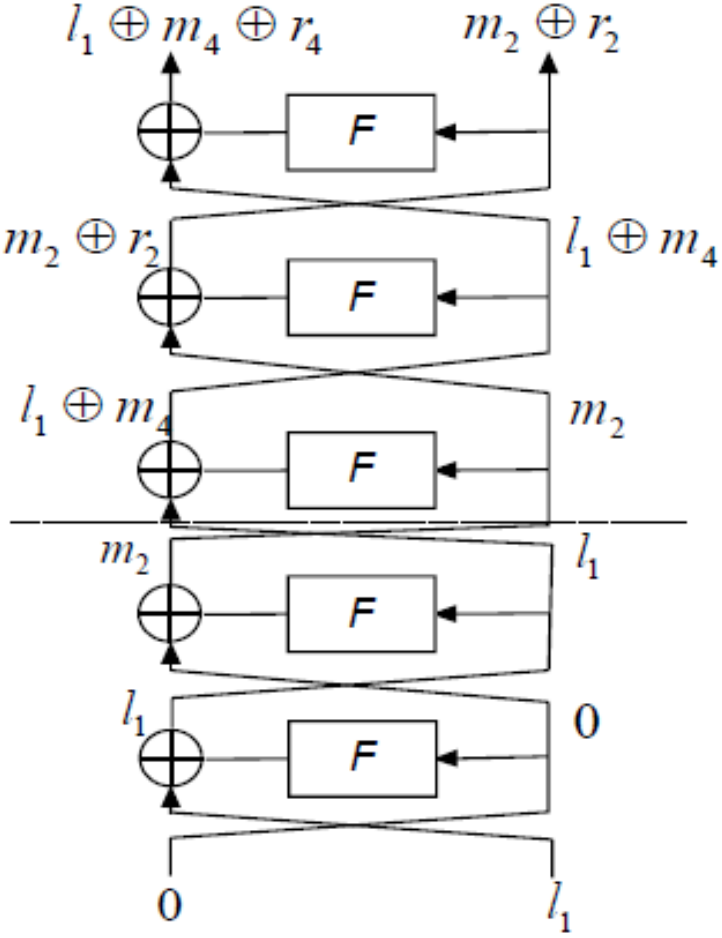


انتقال	ورودی	خروجی
$\mathbf{0}$	$x \in \{0, l_i, m_i, r_i\}$	$\mathbf{0}$
$\mathbf{1}$	$x \in \{0, l_i, m_i, r_i\}$	x
$\mathbb{F}$	$\mathbf{0}$	$\mathbf{0}$
	l_i	m_j
	m_i	m_j
	در غیر اینصورت	r_j

یک مشخصه تفاضلی ناممکن ۵ دوری از ساختارهای فیستلی

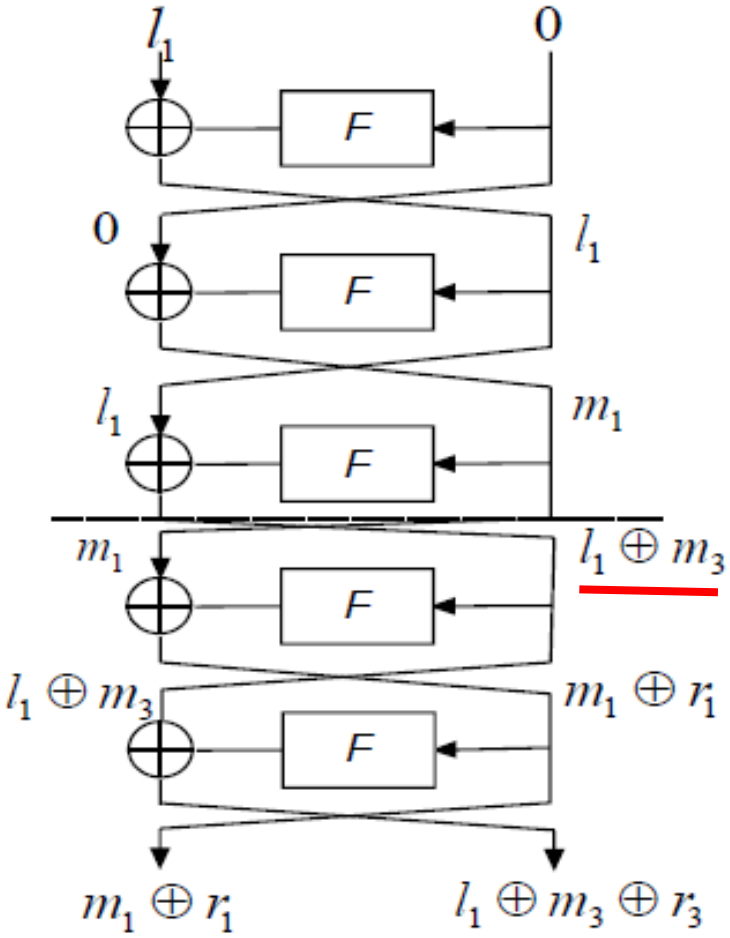
$$U^0 = (l_1, 0) \nrightarrow_5 V^0 = (0, l_1)$$

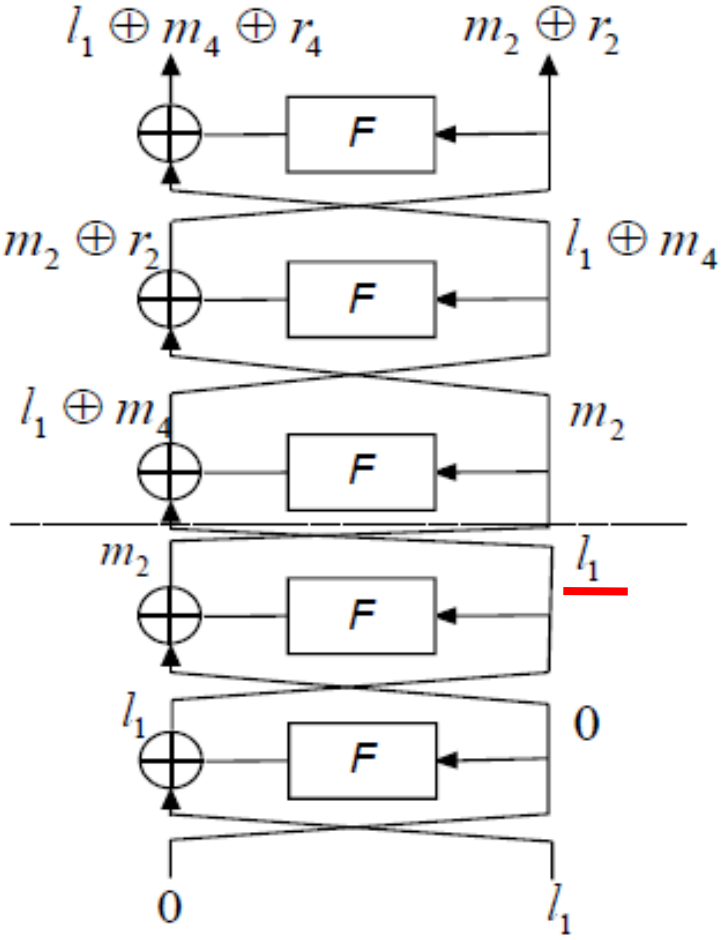


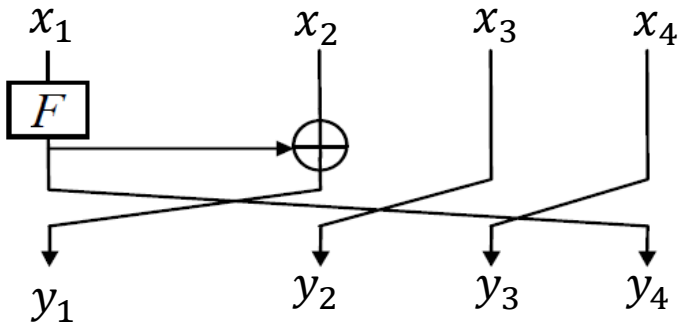


یک مشخصه تفاضلی ناممکن ۵ دوری از ساختارهای فیستلی

$$U^0 = (l_1, 0) \nrightarrow_5 V^0 = (0, l_1)$$

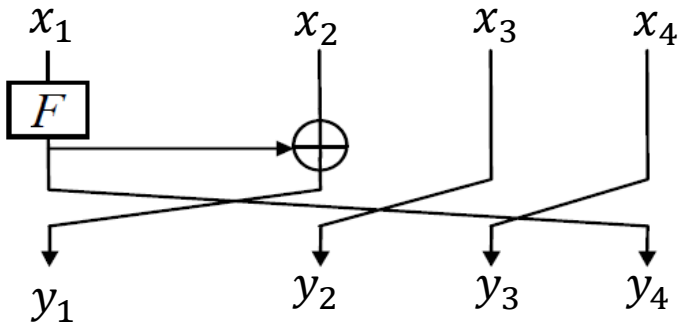






Gen-Skipjack

$$(y_1, y_2, y_3, y_4) = \left(F(x_1) \oplus x_2\ , x_3, x_4, F(x_1)\right)$$

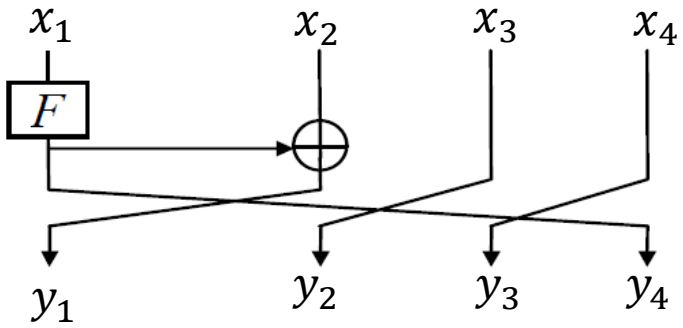


Gen-Skipjack

$$(y_1, y_2, y_3, y_4) = \left(F(x_1) \oplus x_2\ , x_3, x_4, F(x_1)\right)$$

$$\mathcal{E} = \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{array} \begin{array}{c} \begin{array}{cccc} y_1 & y_2 & y_3 & y_4 \end{array} \\ \begin{pmatrix} \mathbb{F} & 0 & 0 & \mathbb{F} \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

$$\mathcal{D} = \begin{array}{c} \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{array} \begin{array}{c} \begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \end{array} \\ \begin{pmatrix} \mathbf{0} & 1 & 0 & \mathbf{0} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \mathbb{F} & 1 & 0 & 0 \end{pmatrix} \end{array}$$



Gen-Skipjack

$$(y_1, y_2, y_3, y_4) = \left(F(x_1) \oplus x_2\ , x_3, x_4, F(x_1)\right)$$

$$\mathcal{E} = \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{array} \begin{array}{c} \begin{array}{cccc} y_1 & y_2 & y_3 & y_4 \end{array} \\ \begin{pmatrix} \mathbb{F} & 0 & 0 & \mathbb{F} \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

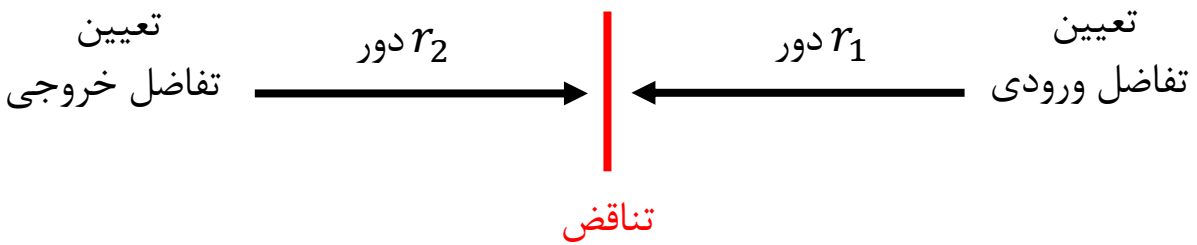
$$\mathcal{D} = \begin{array}{c} \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{array} \begin{array}{c} \begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \end{array} \\ \begin{pmatrix} \mathbf{0} & 1 & 0 & \mathbf{0} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \mathbb{F} & 1 & 0 & 0 \end{pmatrix} \end{array}$$

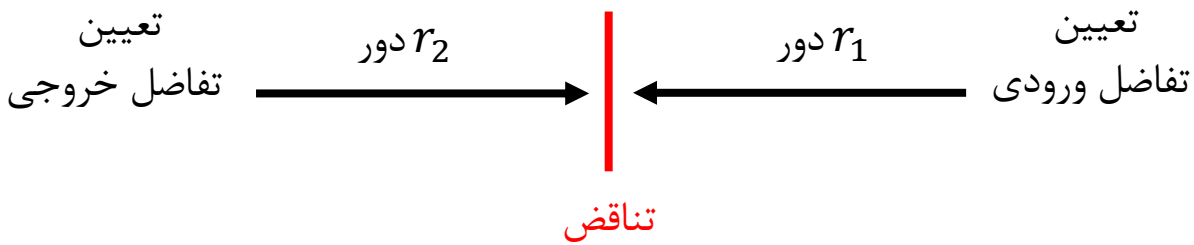
$U^0 = (0,0,0,l_1)$ $\xrightarrow{\quad U^2 = ((U^0.\underbrace{\mathcal{E}).\cdots.\mathcal{E}}_{2\ times})\quad}$ ناسازگار $\xleftarrow{\quad V^{14} = ((V^0.\underbrace{\mathcal{D}).\cdots.\mathcal{D}}_{14\ times})\quad}$ $V^0 = (l_2,0,0,l_2)$

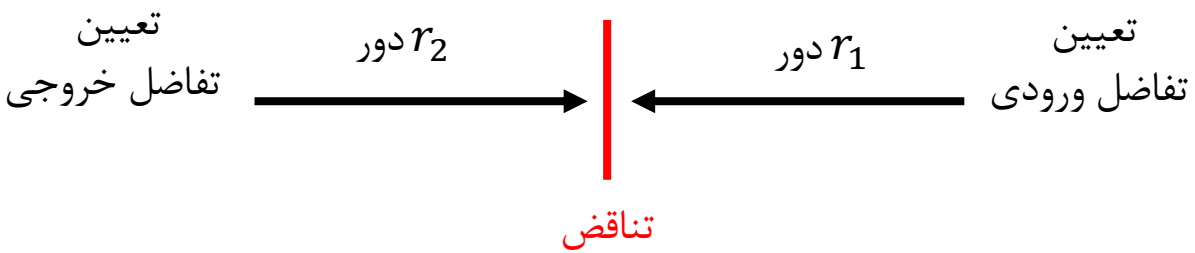
Luo, Y., et al., A unified method for finding impossible differentials of block cipher structures. Information Sciences, 2014

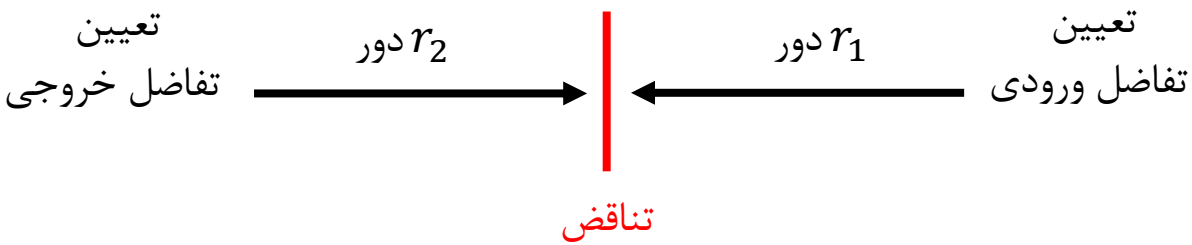
R	X_1	X_2	X_3	X_4
0 ↓	0	0	0	l_1
1	0	0	l_1	0
2	0	l_1	0	0
14	m_7	$m_1 \oplus m_6$	$m_4 \oplus r_1$	$m_2 \oplus m_3 \oplus m_5$
13	m_6	$m_4 \oplus r_1$	$m_2 \oplus m_3 \oplus m_5$	m_1
12	r_1	$m_2 \oplus m_3 \oplus m_5$	m_1	m_4
11	m_5	m_1	m_4	$m_2 \oplus m_3$
10	0	m_4	$m_2 \oplus m_3$	m_1
9	m_4	$m_2 \oplus m_3$	m_1	0
8	m_3	m_1	0	m_2
7	0	0	m_2	m_1
6	0	m_2	m_1	0
5	m_2	m_1	0	0
4	0	0	0	m_1
3	0	0	m_1	0
2	0	m_1	0	0
1	m_1	0	0	0
0 ↑	l_2	0	0	l_2

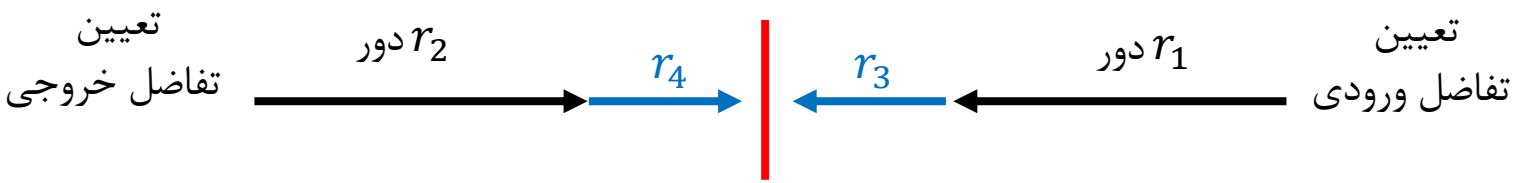
R	X_1	X_2	X_3	X_4
$0\downarrow$	0	0	0	l_1
1	0	0	l_1	0
2	0	l_1	0	0
14	m_7	$m_1 \oplus m_6$	$m_4 \oplus r_1$	$m_2 \oplus m_3 \oplus m_5$
13	m_6	$m_4 \oplus r_1$	$m_2 \oplus m_3 \oplus m_5$	m_1
12	r_1	$m_2 \oplus m_3 \oplus m_5$	m_1	m_4
11	m_5	m_1	m_4	$m_2 \oplus m_3$
10	0	m_4	$m_2 \oplus m_3$	m_1
9	m_4	$m_2 \oplus m_3$	m_1	0
8	m_3	m_1	0	m_2
7	0	0	m_2	m_1
6	0	m_2	m_1	0
5	m_2	m_1	0	0
4	0	0	0	m_1
3	0	0	m_1	0
2	0	m_1	0	0
1	m_1	0	0	0
$0\uparrow$	l_2	0	0	l_2

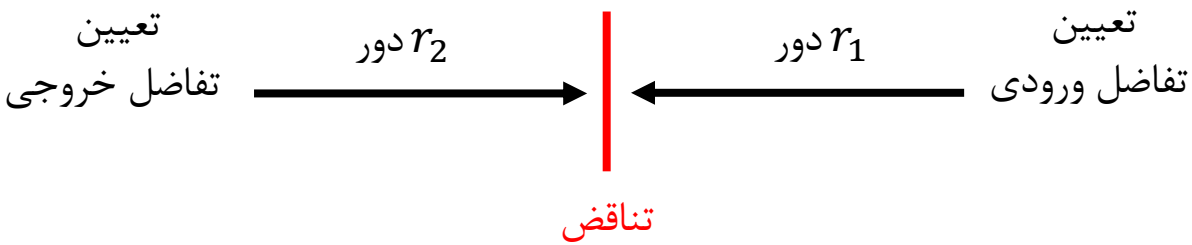

تعیین
تفاضل ورودی
دور r_1
دور r_2
تعیین
تفاضل خروجی
تناقض

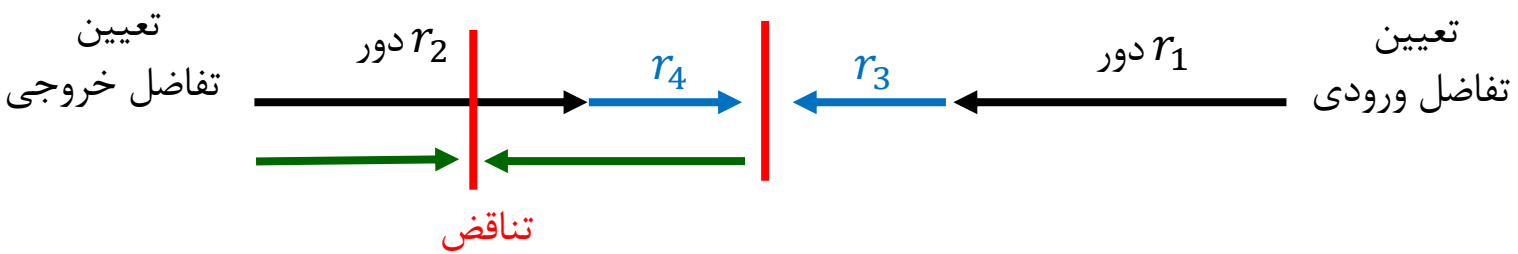

تعیین
تفاضل ورودی
دور r_1
دور r_2
تعیین
تفاضل خروجی
تناقض


تعیین
تفاضل ورودی
دور r_1
دور r_2
تعیین
تفاضل خروجی
تناقض


تعیین
تفاضل ورودی
دور r_1
دور r_2
تعیین
تفاضل خروجی
تناقض

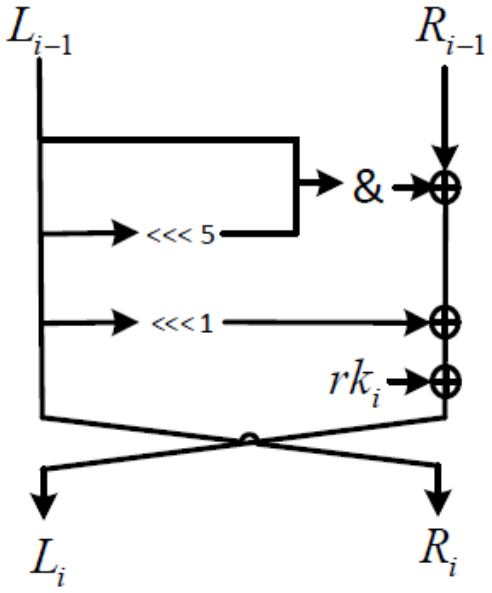

تعیین
تفاضل ورودی
دور r_1
r_3
r_4
دور r_2
تعیین
تفاضل خروجی


تعیین
تفاضل ورودی
دور r_1
دور r_2
تعیین
تفاضل خروجی
تناقض

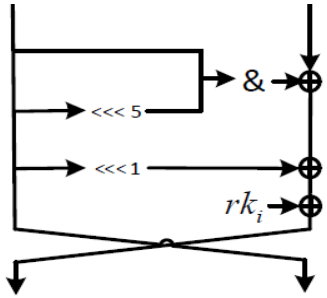

تعیین
تفاضل ورودی
دور r_1
r_3
r_4
دور r_2
تعیین
تفاضل خروجی
تناقض

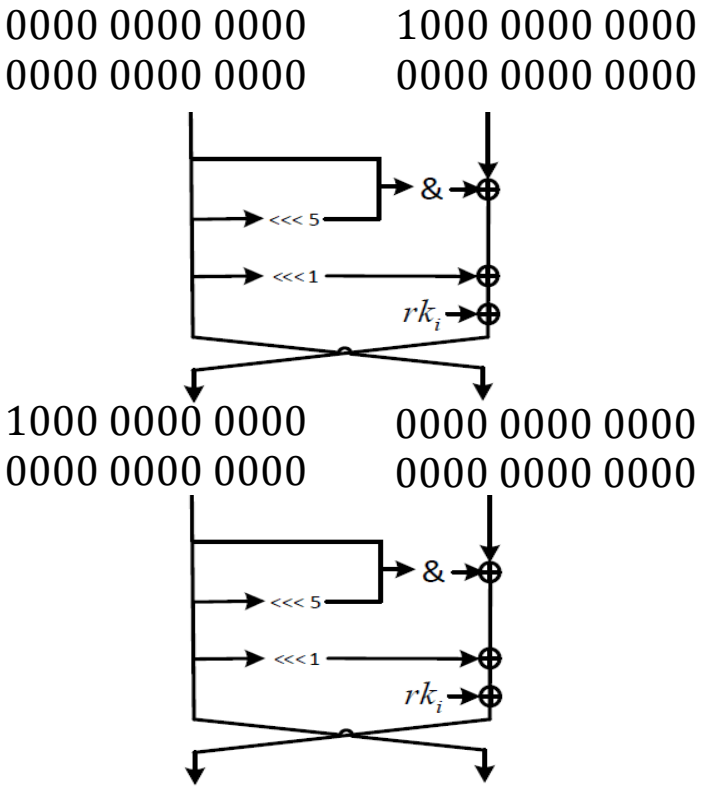
SIMECK

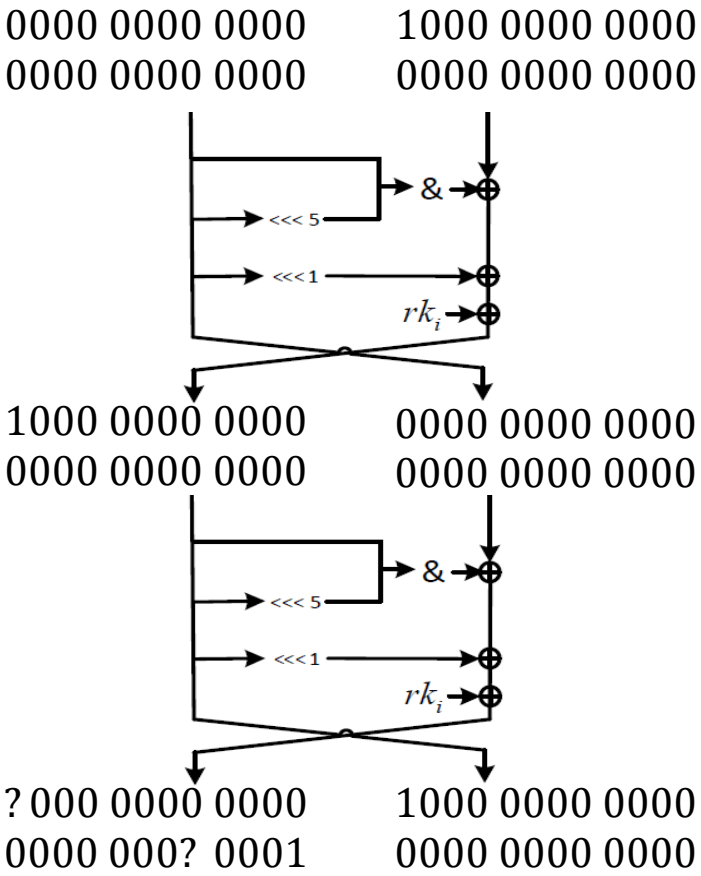
الگوریتم سایمک

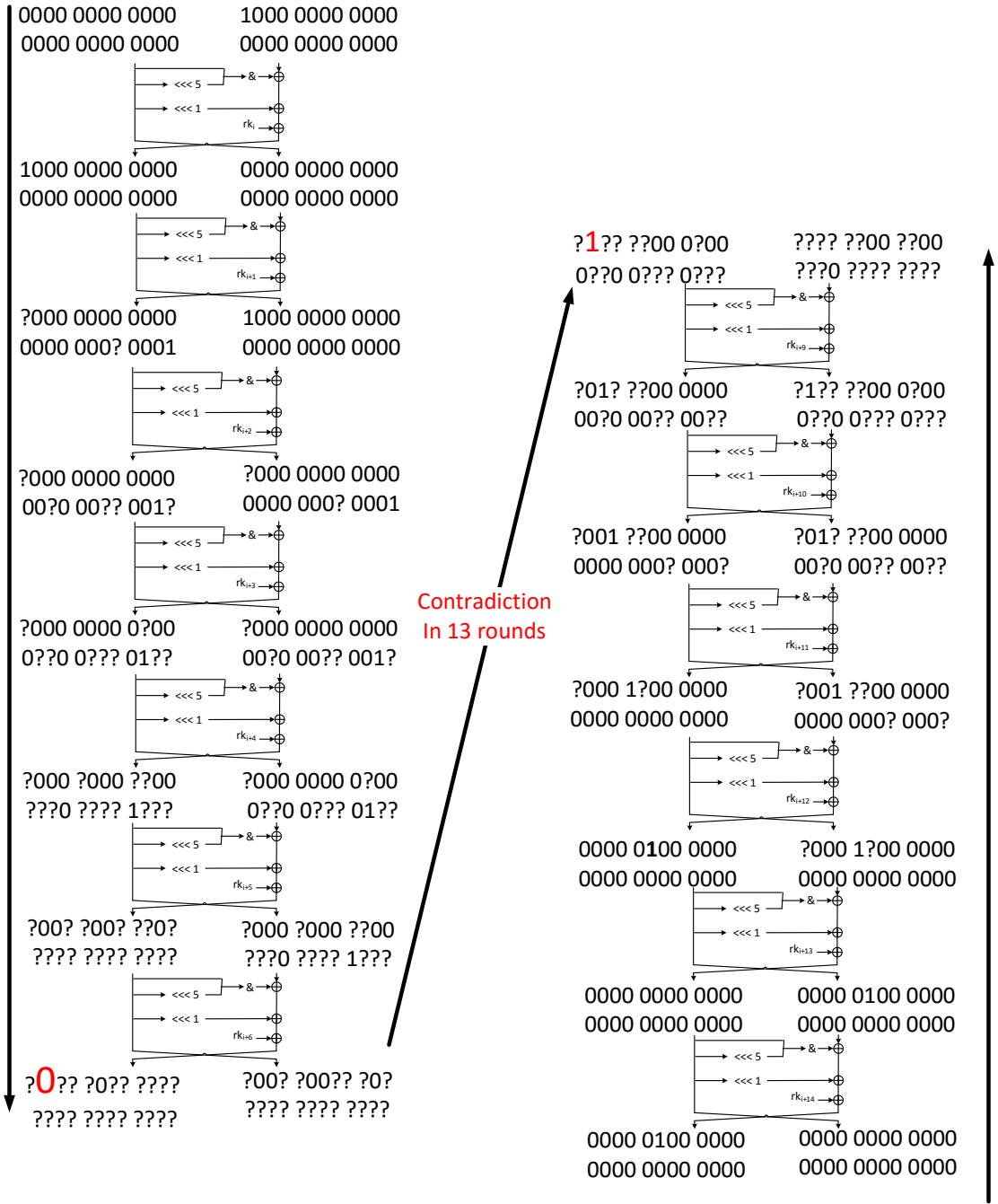


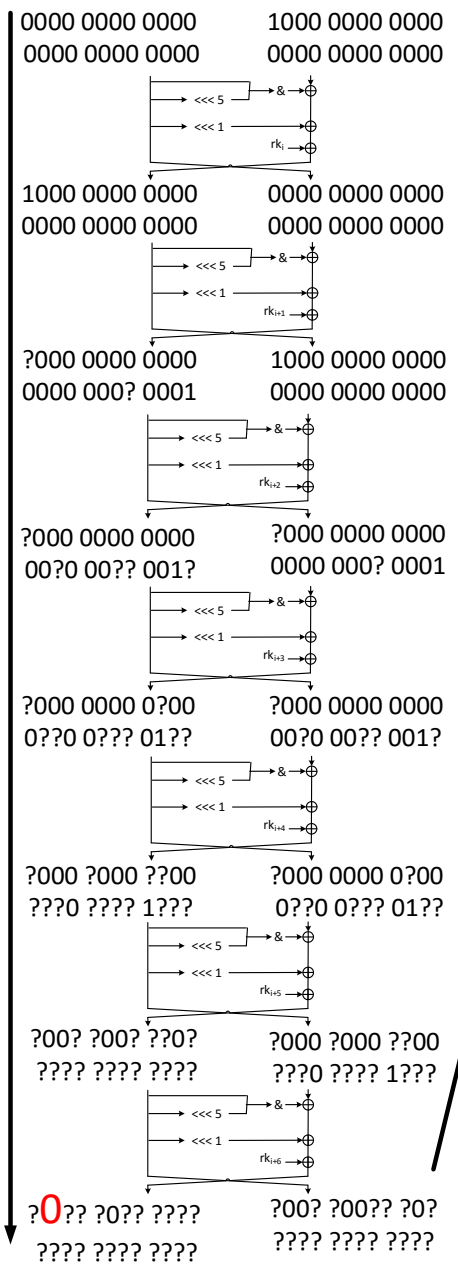
0000 0000 0000 1000 0000 0000
0000 0000 0000 0000 0000 0000



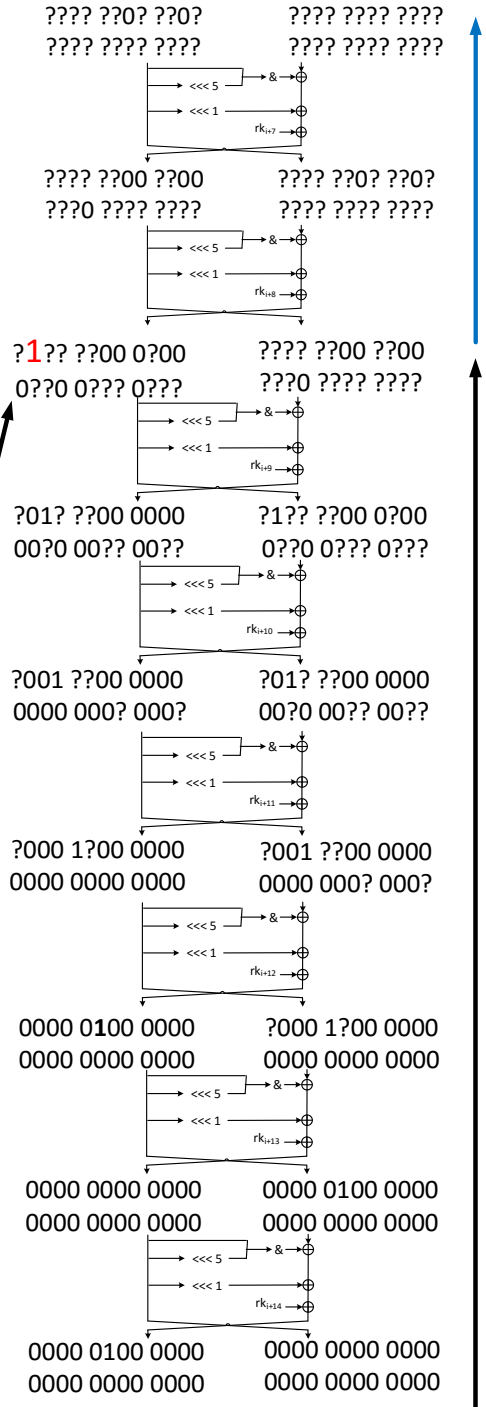

0000 0000 0000
0000 0000 0000
1000 0000 0000
0000 0000 0000
&
<<< 5
<<< 1
rk_i
1000 0000 0000
0000 0000 0000
0000 0000 0000
0000 0000 0000
&
<<< 5
<<< 1
rk_i

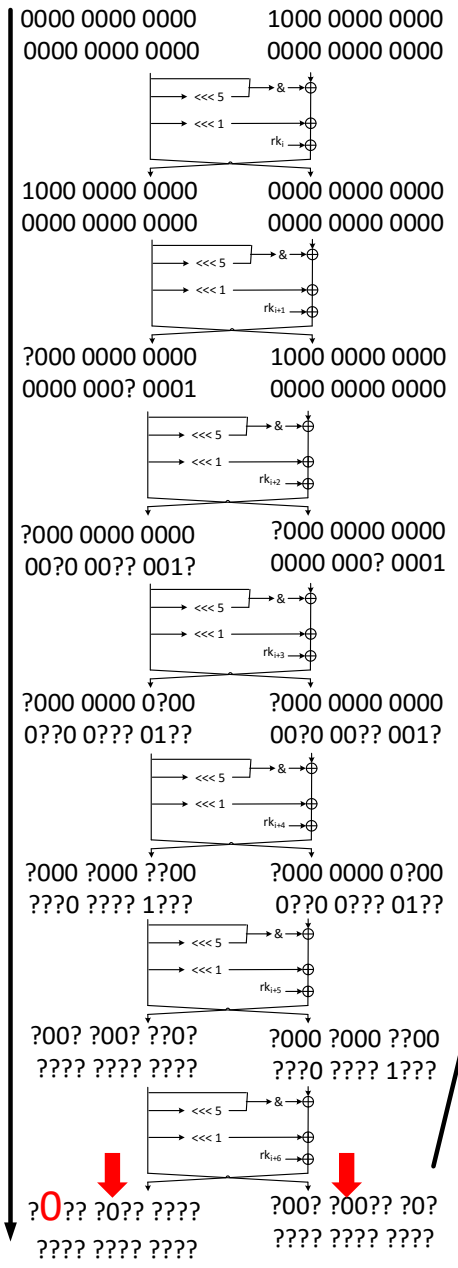

0000 0000 0000
0000 0000 0000
1000 0000 0000
0000 0000 0000
&
<<< 5
<<< 1
rk_i
1000 0000 0000
0000 0000 0000
0000 0000 0000
0000 0000 0000
&
<<< 5
<<< 1
rk_i
? 000 0000 0000
0000 000? 0001
1000 0000 0000
0000 0000 0000


0000 0000 0000
0000 0000 0000
1000 0000 0000
0000 0000 0000
1000 0000 0000
0000 0000 0000
0000 0000 0000
0000 0000 0000
?000 0000 0000
0000 000? 0001
1000 0000 0000
0000 0000 0000
?000 0000 0000
00?0 00?? 001?
?000 0000 0000
0000 000? 0001
?000 0000 0?00
0??0 0??? 01??
?000 0000 0000
00?0 00?? 001?
?000 ?000 ??00
???0 ???? 1???
?000 0000 0?00
0??0 0??? 01??
?00? ?00? ??0?
???? ???? ????
?000 ?000 ??00
???0 ???? 1???
?0?? ?0?? ????
???? ???? ????
?00? ?00?? ?0?
???? ???? ????
Contradiction
In 13 rounds
?1?? ??00 0?00
0??0 0??? 0???
???? ??00 ??00
???0 ???? ????
?01? ??00 0000
00?0 00?? 00??
?1?? ??00 0?00
0??0 0??? 0???
?001 ??00 0000
0000 000? 000?
?01? ??00 0000
00?0 00?? 00??
?000 1?00 0000
0000 0000 0000
?001 ??00 0000
0000 000? 000?
0000 0100 0000
0000 0000 0000
?000 1?00 0000
0000 0000 0000
0000 0000 0000
0000 0000 0000
0000 0100 0000
0000 0000 0000
0000 0100 0000
0000 0000 0000
0000 0000 0000
0000 0000 0000

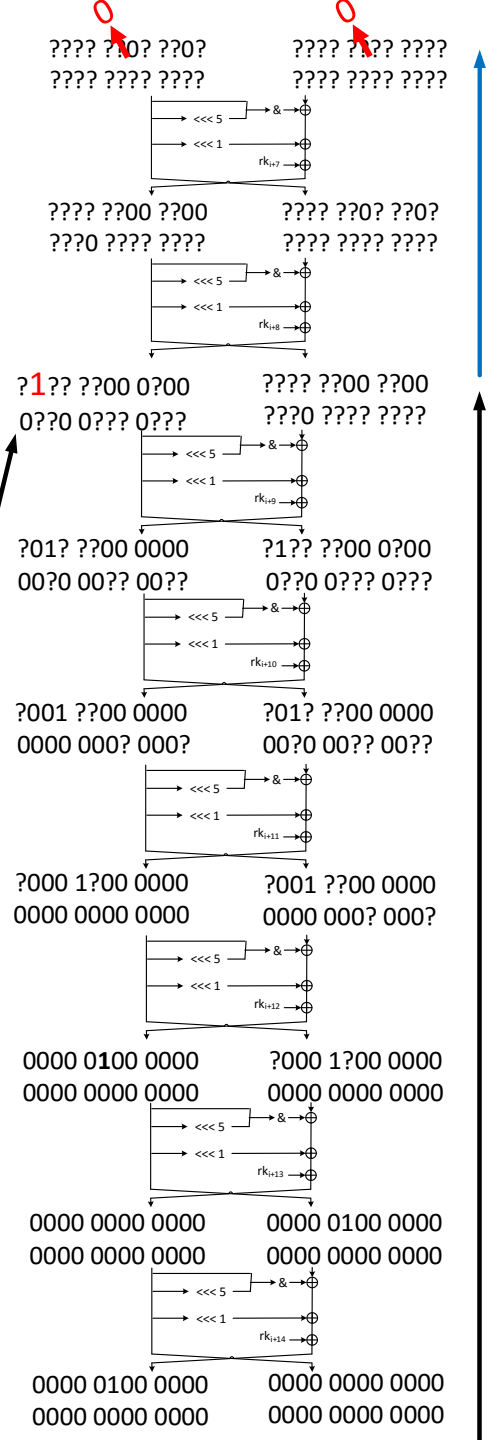


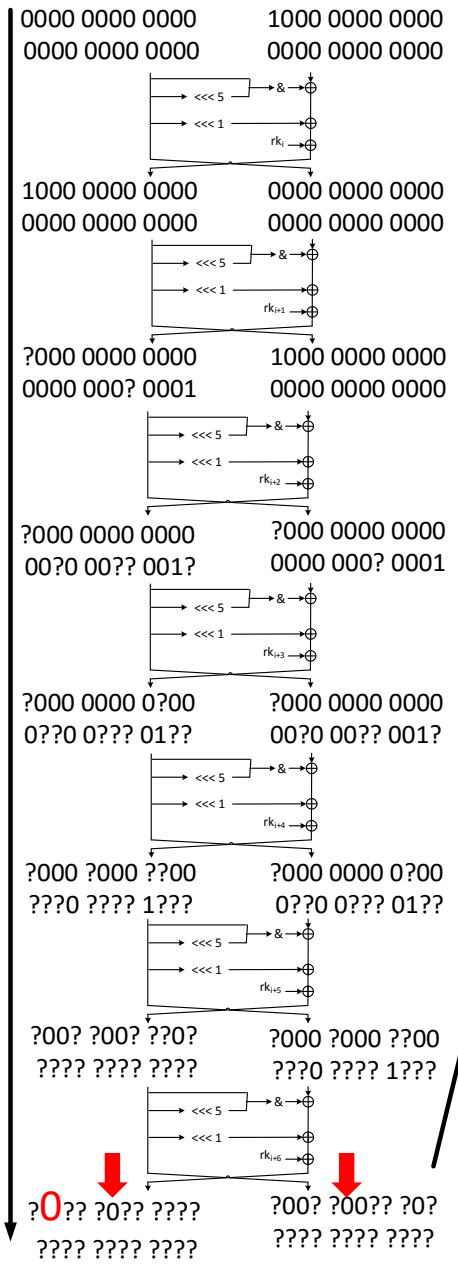
Contradiction
In 13 rounds



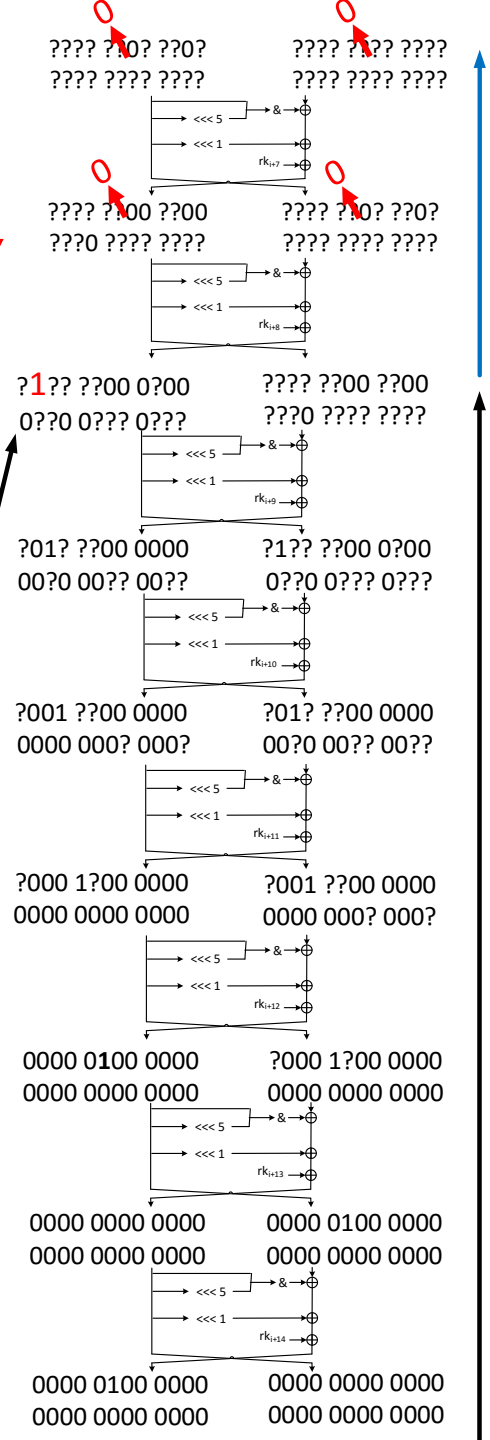


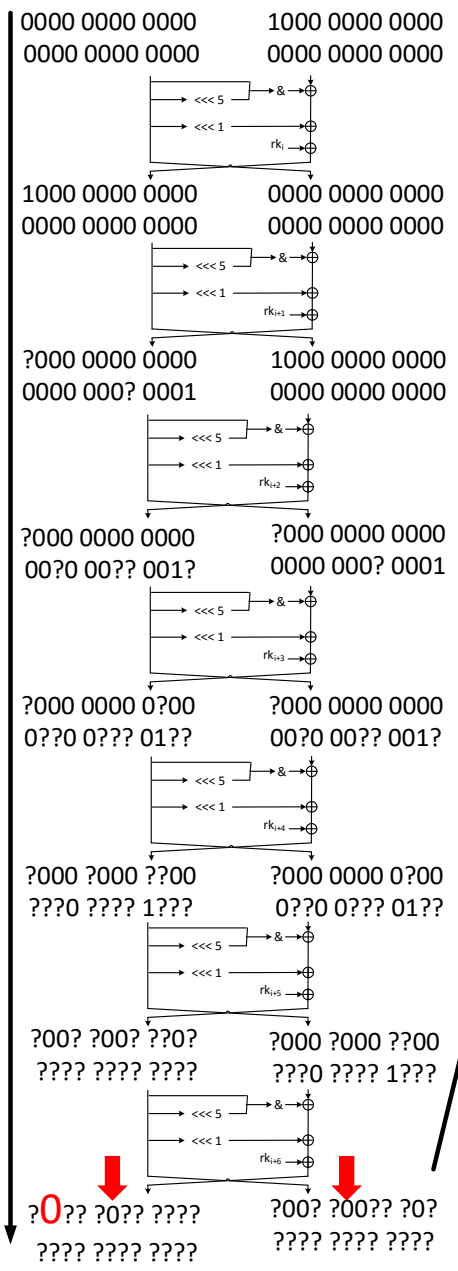
Contradiction
In 13 rounds



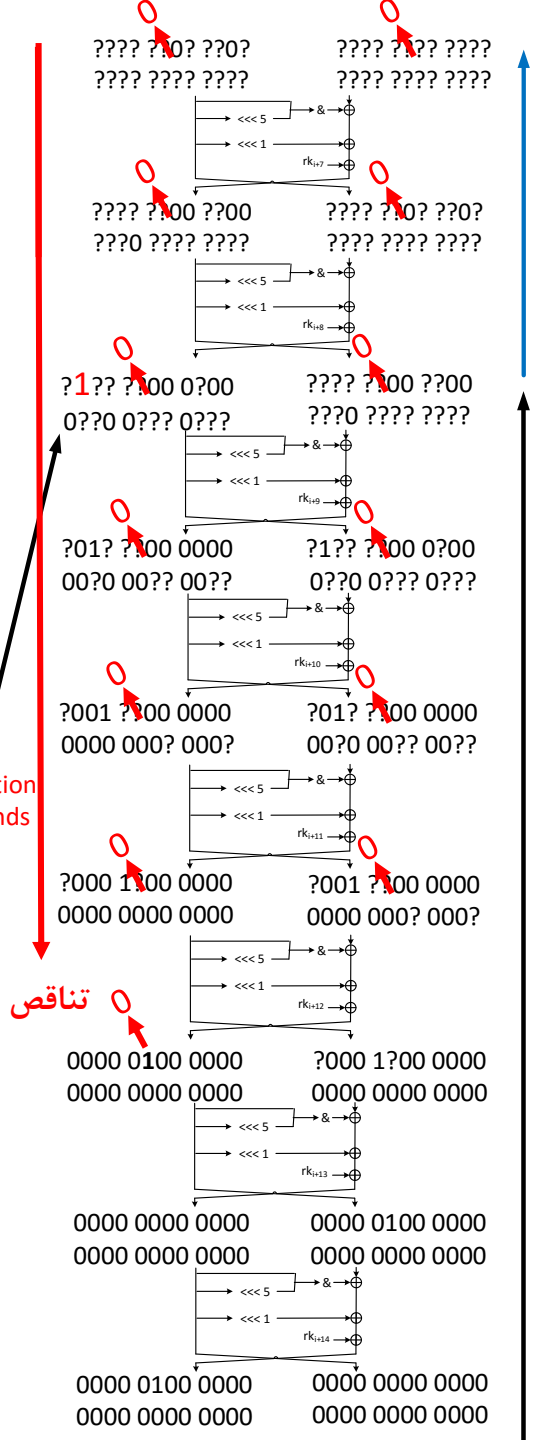


Contradiction
In 13 rounds





Contradiction
In 13 rounds



حمله خطی

M. Matsui.

Linear cryptanalysis method for DES cipher.

in Advances in Cryptology EUROCRYPT’93. 1993. Springer

هدف یافتن یک رابطه خطی بین بعضی از بیت های متن اصلی، کلید و بیت های دور آخر با احتمالی مشخص

$E_K: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$

$$\alpha.x \oplus \beta.\mathrm{E}_K(x) = \gamma.K$$

$$p = Pr_x\{\alpha.x = \beta.E_K(x)\} \neq \frac{1}{2}$$

هدف یافتن یک رابطه خطی بین بعضی از بیت های متن اصلی، کلید و بیت های دور آخر با احتمالی مشخص

$E_K: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$

$$\alpha.x \oplus \beta.\mathrm{E}_K(x) = \gamma.K$$

$$p = Pr_x\{\alpha.x = \beta.E_K(x)\} \neq \frac{1}{2} \longrightarrow \varepsilon = |p - \frac{1}{2}|$$

هدف یافتن یک رابطه خطی بین بعضی از بیت های متن اصلی، کلید و بیت های دور آخر با احتمالی مشخص

$E_K: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$

$$\alpha.x \oplus \beta.\mathrm{E}_K(x) = \gamma.K$$

$$p = Pr_x\{\alpha.x = \beta.E_K(x)\} \neq \frac{1}{2} \longrightarrow \varepsilon = |p - \frac{1}{2}|$$

لم piling-up:

فرض کنید x_i متغیرهایی مستقل و تصادفی با اریبی ε_i باشد سپس احتمال این که مقدار $x_1 \oplus x_2 \oplus \ldots \oplus x_n = 0$ باشد برابر است با

$$\frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \varepsilon_i$$

چطور با داشتن یک تقریب خطی، حمله خطی را انجام دهیم؟

$$\alpha.x \oplus \beta.\mathrm{E}_K(x) = \gamma.K \qquad \varepsilon \neq 0$$

چطور با داشتن یک تقریب خطی، حمله خطی را انجام دهیم؟

$$\alpha.x \oplus \beta.\mathrm{E}_K(x) = \gamma.K \qquad \varepsilon \neq 0$$

الگوریتم ۱ ماتسویی

الگوریتم ۲ ماتسویی

چطور با داشتن یک تقریب خطی، حمله خطی را انجام دهیم؟

$$\alpha.x \oplus \beta.\mathrm{E}_K(x) = \gamma.K \qquad \varepsilon \neq 0$$

الگوریتم ۱ ماتسویی

به ما یک بیت اطلاع از کلید می دهد ($\gamma.K = 0$ یا $\gamma.K = 1$)

پیچیدگی داده ای (تعداد متن متن و رمزشده آن مورد نیاز برای تحلیل):

$$N = \frac{1}{\varepsilon^2}$$

الگوریتم ۲ ماتسویی

چطور با داشتن یک تقریب خطی، حمله خطی را انجام دهیم؟

$$\alpha.x \oplus \beta.\mathrm{E}_K(x) = \gamma.K \qquad \varepsilon \neq 0$$

الگوریتم ۱ ماتسویی

به ما یک بیت اطلاع از کلید می دهد ($\gamma.K = 0$ یا $\gamma.K = 1$)

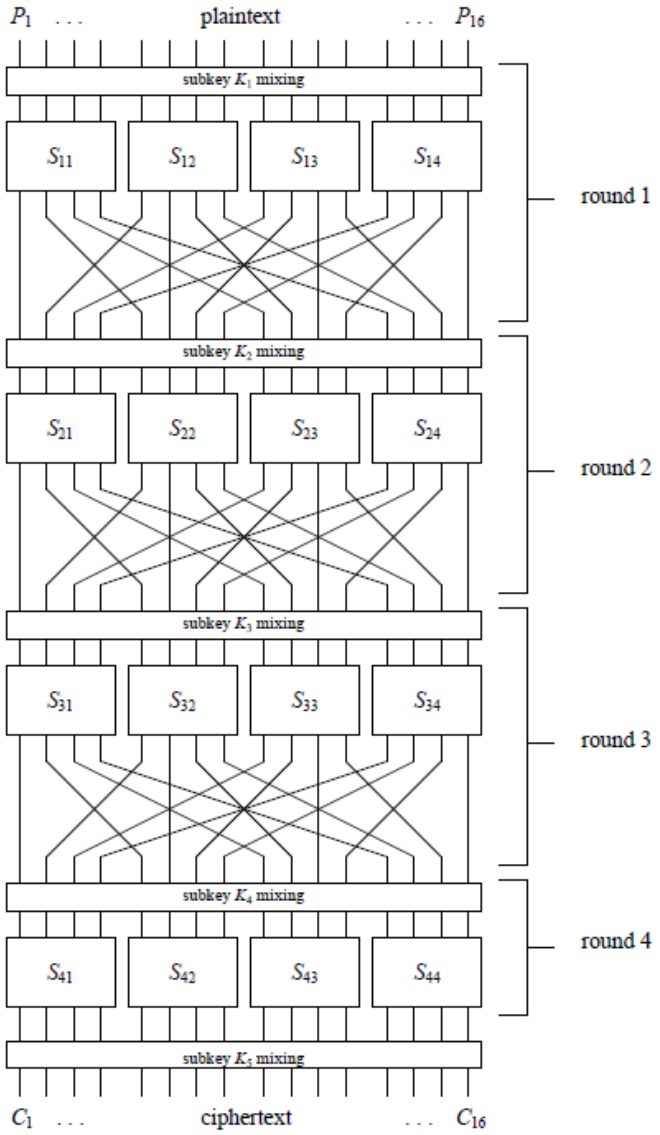
پیچیدگی داده ای (تعداد متن متن و رمزشده آن مورد نیاز برای تحلیل):

$$N = \frac{1}{\varepsilon^2}$$

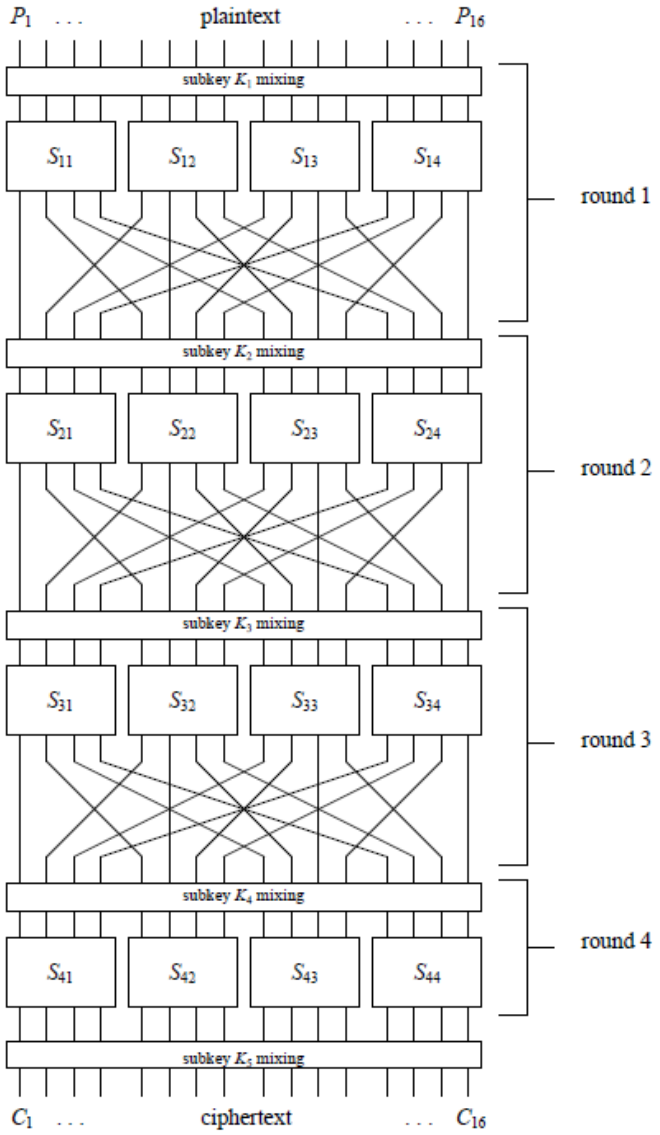
الگوریتم ۲ ماتسویی

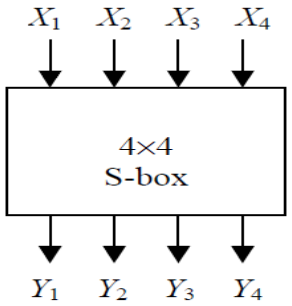
یک روش تحلیل آماری برای بازیابی بعضی از بیت های کلید

N	$2\varepsilon^{-2}$	$4\varepsilon^{-2}$	$8\varepsilon^{-2}$	$16\varepsilon^{-2}$
درصد موفقیت در الگوریتم ۲	48.6 %	78.5 %	96.7 %	**99.9 %**

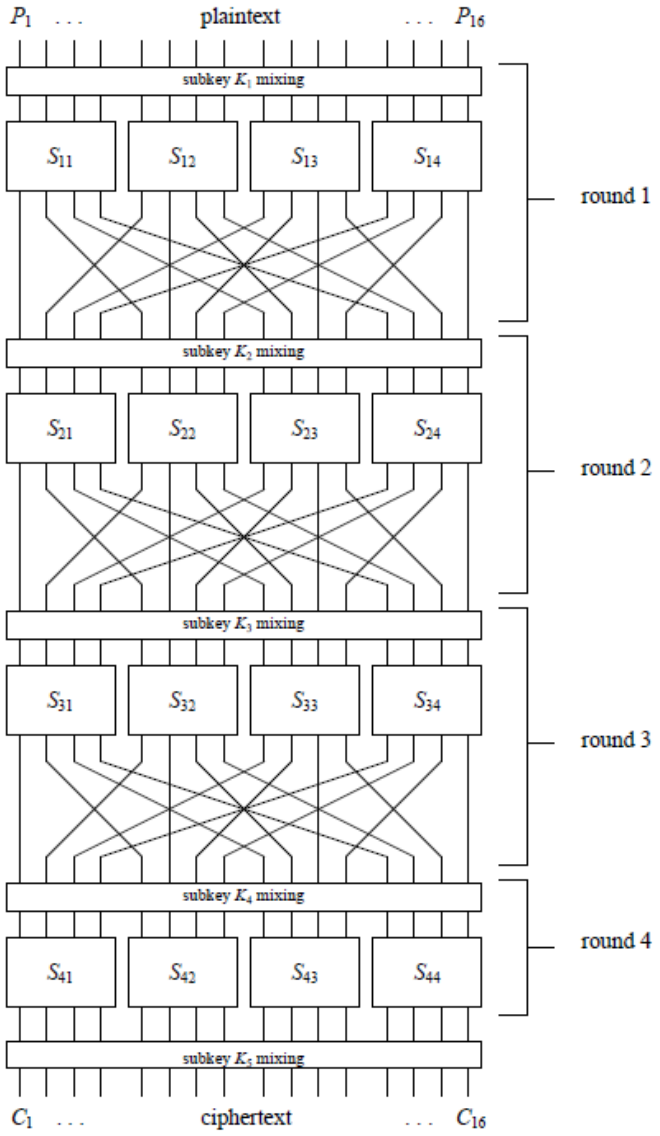


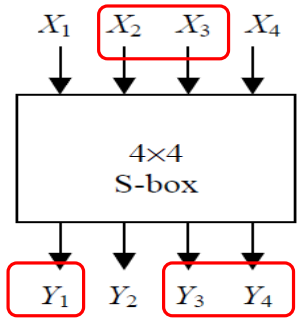
Heys, Howard M. "A tutorial on linear and differential cryptanalysis." *Cryptologia* 26.3 (2002): 189-221.





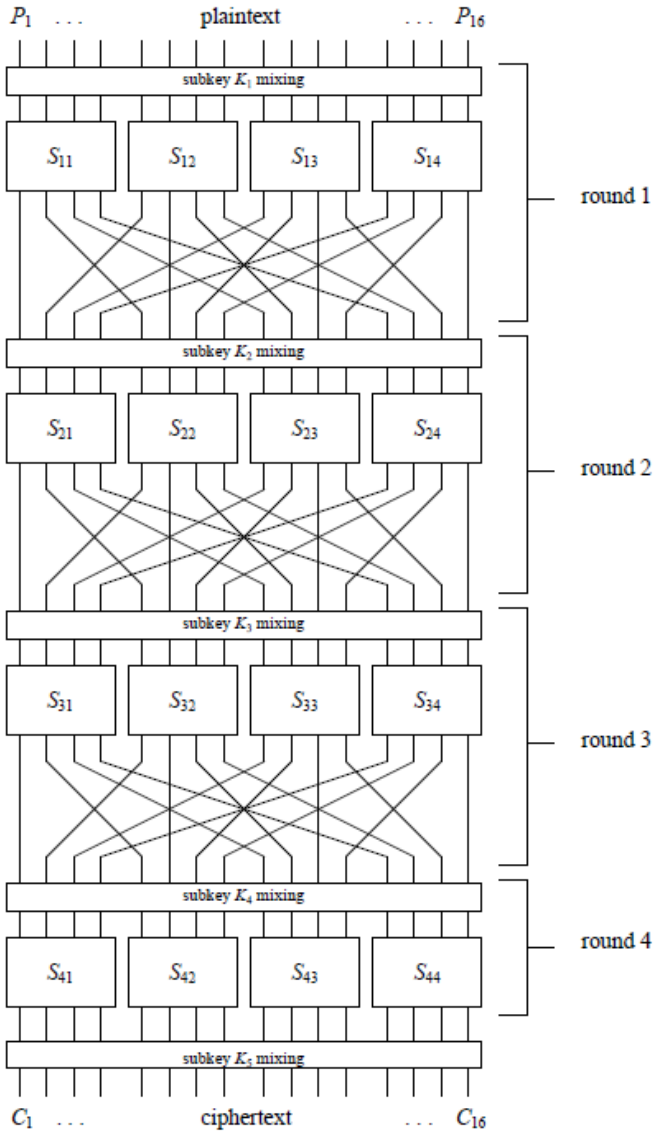
X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4
0	0	0	0	1	1	1	0
0	0	0	1	0	1	0	0
0	0	1	0	1	1	0	1
0	0	1	1	0	0	0	1
0	1	0	0	0	0	1	0
0	1	0	1	1	1	1	1
0	1	1	0	1	0	1	1
0	1	1	1	1	0	0	0
1	0	0	0	0	0	1	1
1	0	0	1	1	0	1	0
1	0	1	0	0	1	1	0
1	0	1	1	1	1	0	0
1	1	0	0	0	1	0	1
1	1	0	1	1	0	0	1
1	1	1	0	0	0	0	0
1	1	1	1	0	1	1	1

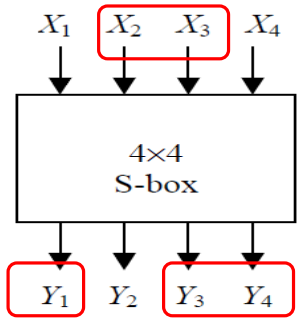




$$X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4$$

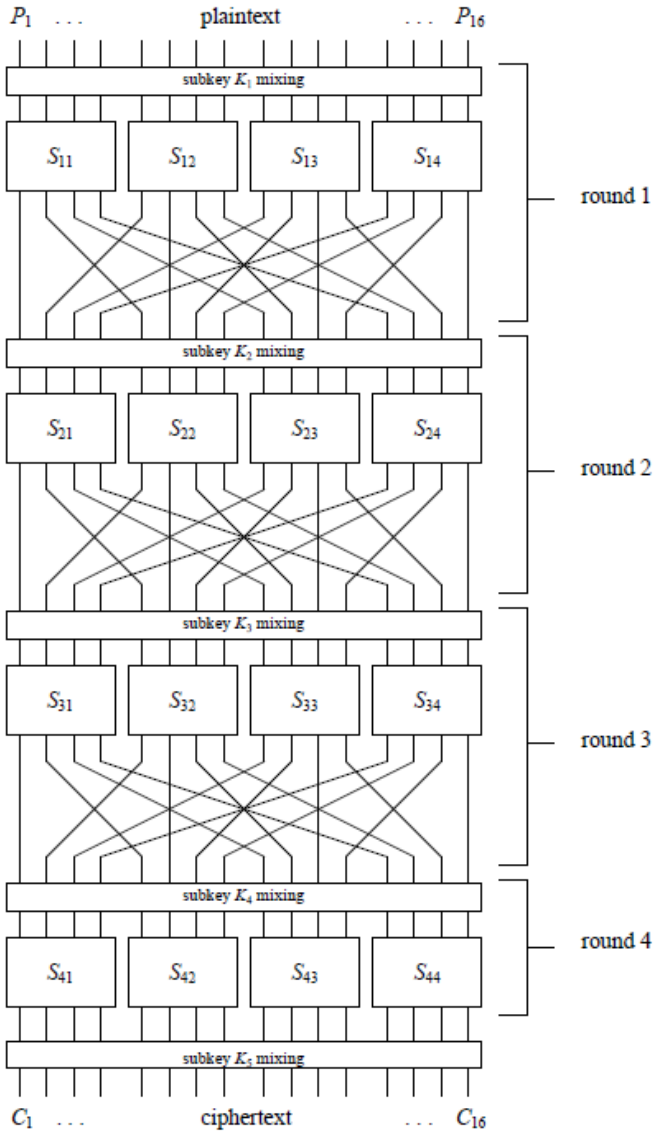
X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4
0	0	0	0	1	1	1	0
0	0	0	1	0	1	0	0
0	0	1	0	1	1	0	1
0	0	1	1	0	0	0	1
0	1	0	0	0	0	1	0
0	1	0	1	1	1	1	1
0	1	1	0	1	0	1	1
0	1	1	1	1	0	0	0
1	0	0	0	0	0	1	1
1	0	0	1	1	0	1	0
1	0	1	0	0	1	1	0
1	0	1	1	1	1	0	0
1	1	0	0	0	1	0	1
1	1	0	1	1	0	0	1
1	1	1	0	0	0	0	0
1	1	1	1	0	1	1	1

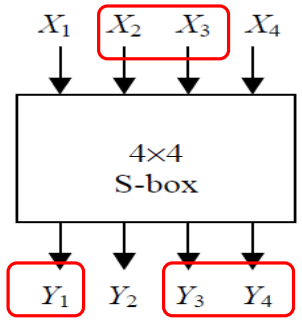




$$X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4$$

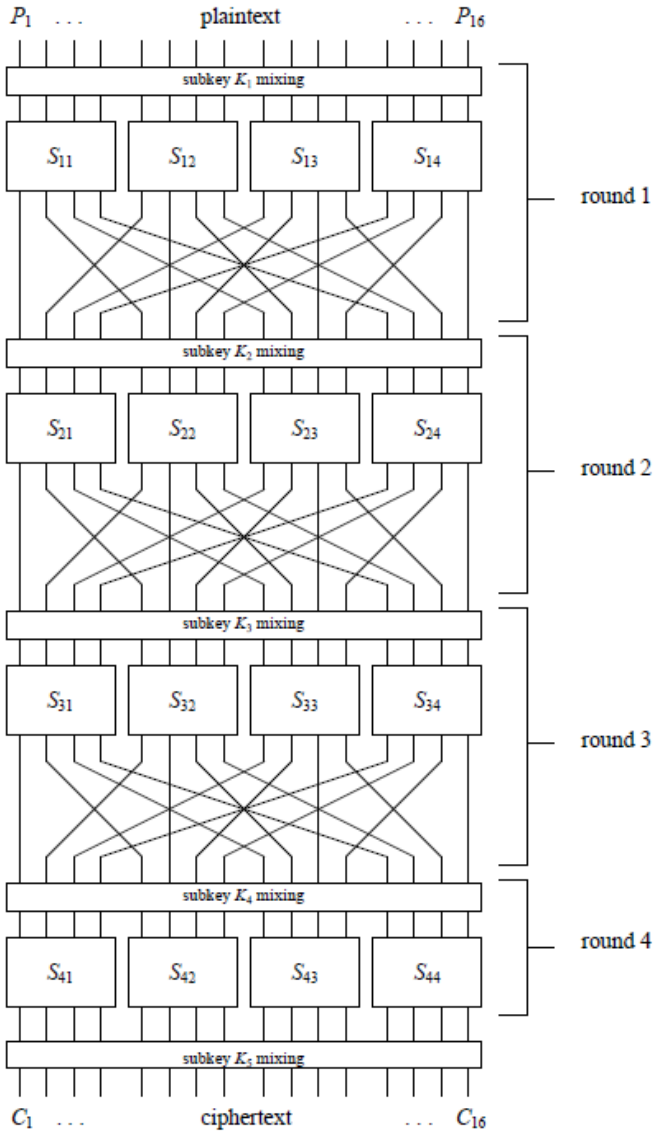
X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0
0	0	0	1	0	1	0	0	0	0
0	0	1	0	1	1	0	1	1	0
0	0	1	1	0	0	0	1	1	1
0	1	0	0	0	0	1	0	1	1
0	1	0	1	1	1	1	1	1	1
0	1	1	0	1	0	1	1	0	1
0	1	1	1	1	0	0	0	0	1
1	0	0	0	0	0	1	1	0	0
1	0	0	1	1	0	1	0	0	0
1	0	1	0	0	1	1	0	1	1
1	0	1	1	1	1	0	0	1	1
1	1	0	0	0	1	0	1	1	1
1	1	0	1	1	0	0	1	1	0
1	1	1	0	0	0	0	0	0	0
1	1	1	1	0	1	1	1	0	0

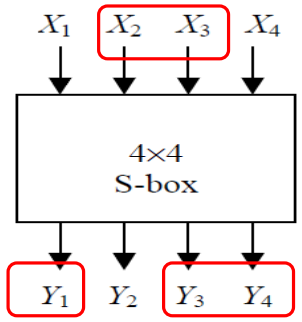




$$X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4 \longrightarrow \frac{12}{16} = \frac{3}{4}$$

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$
0	0	0	0	1	1	1	0	~~0~~	~~0~~
0	0	0	1	0	1	0	0	~~0~~	~~0~~
0	0	1	0	1	1	0	1	1	0
0	0	1	1	0	0	0	1	~~1~~	~~1~~
0	1	0	0	0	0	1	0	~~1~~	~~1~~
0	1	0	1	1	1	1	1	~~1~~	~~1~~
0	1	1	0	1	0	1	1	0	1
0	1	1	1	1	0	0	0	0	1
1	0	0	0	0	0	1	1	~~0~~	~~0~~
1	0	0	1	1	0	1	0	~~0~~	~~0~~
1	0	1	0	0	1	1	0	~~1~~	~~1~~
1	0	1	1	1	1	0	0	~~1~~	~~1~~
1	1	0	0	0	1	0	1	~~1~~	~~1~~
1	1	0	1	1	0	0	1	1	0
1	1	1	0	0	0	0	0	~~0~~	~~0~~
1	1	1	1	0	1	1	1	~~0~~	~~0~~



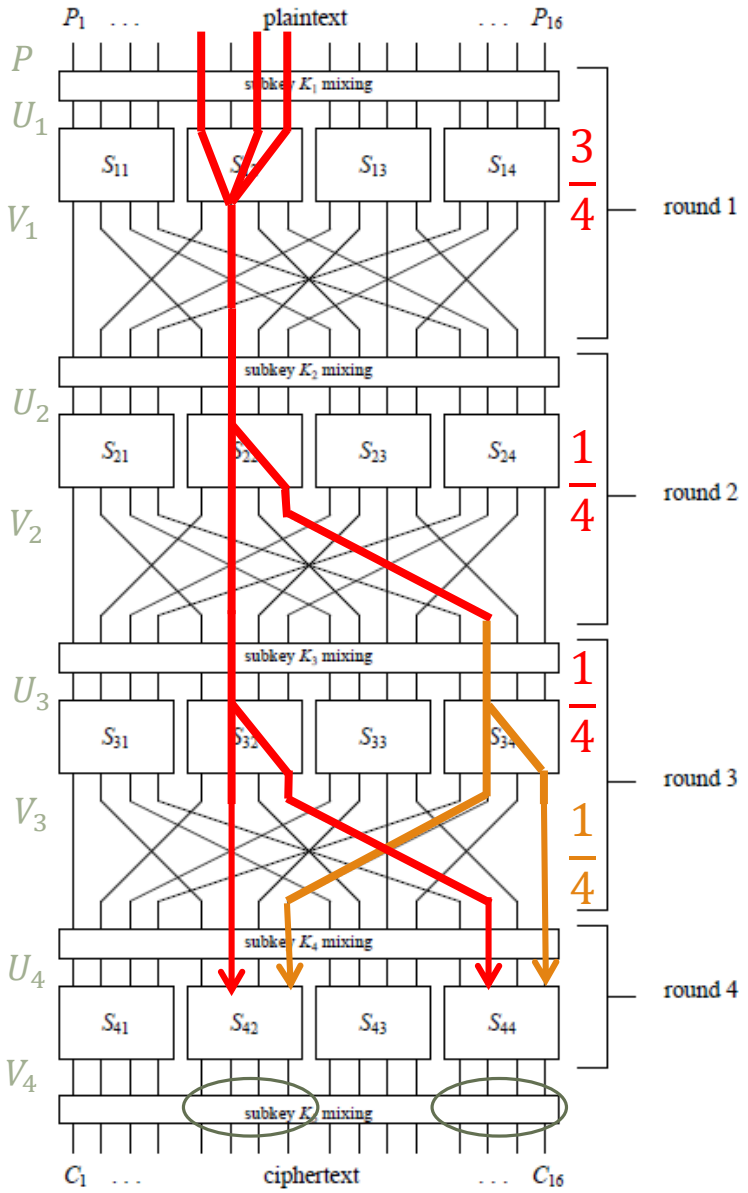


$$X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4 \longrightarrow \frac{12}{16} = \frac{3}{4}$$

$$\frac{3}{4}$$

$$\alpha = (0110) \rightarrow \beta = (1011)$$

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$
0	0	0	0	1	1	1	0	~~0~~	~~0~~
0	0	0	1	0	1	0	0	~~0~~	~~0~~
0	0	1	0	1	1	0	1	1	0
0	0	1	1	0	0	0	1	~~1~~	~~1~~
0	1	0	0	0	0	1	0	~~1~~	~~1~~
0	1	0	1	1	1	1	1	~~1~~	~~1~~
0	1	1	0	1	0	1	1	0	1
0	1	1	1	1	0	0	0	0	1
1	0	0	0	0	0	1	1	~~0~~	~~0~~
1	0	0	1	1	0	1	0	~~0~~	~~0~~
1	0	1	0	0	1	1	0	~~1~~	~~1~~
1	0	1	1	1	1	0	0	~~1~~	~~1~~
1	1	0	0	0	1	0	1	~~1~~	~~1~~
1	1	0	1	1	0	0	1	1	0
1	1	1	0	0	0	0	0	~~0~~	~~0~~
1	1	1	1	0	1	1	1	~~0~~	~~0~~



$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} = 0$$

$$\frac{1}{2} + 2^3 \left(\frac{3}{4} - \frac{1}{2}\right)\left(\frac{1}{4} - \frac{1}{2}\right)^3 = \frac{15}{32}$$

Heys, Howard M. "A tutorial on linear and differential cryptanalysis." *Cryptologia* 26.3 (2002): 189-221.

حمله همبستگی صفر

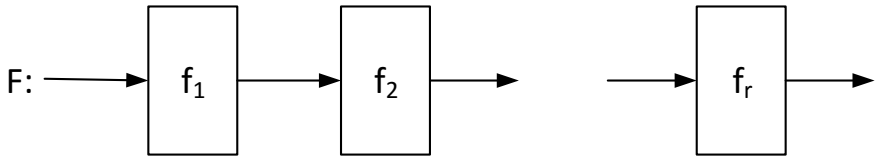
A. Bogdanov and V. Rijmen,
Linear hulls with correlation zero and linear cryptanalysis of block ciphers.
Designs, codes and cryptography, 2014. 70(3): p. 369-383

هدف پیدا کردن یک پوشش خطی با احتمال دقیقا $\frac{1}{2}$ می‌باشد

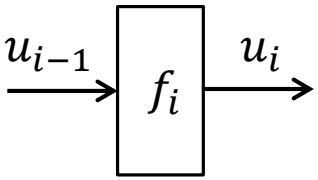
هدف پیدا کردن یک پوشش خطی با احتمال دقیقا $\frac{1}{2}$ می‌باشد

$F: \mathbb{F}_2^n \to \mathbb{F}_2^n$

$F = f_r \circ \cdots \circ f_1$



تقریب خطی $u_{i-1} \to u_i$ با نقاب ورودی u_{i-1} و نقاب خروجی u_i را برای نگاشت f_i در نظر بگیرید.

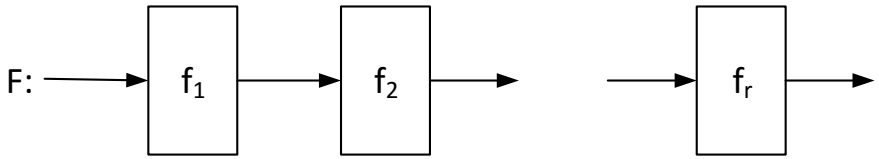


$u_{i-1}.x \oplus u_i.f_i(x) = 0$

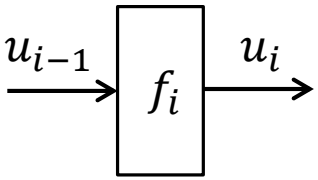
$Pr_x\{u_{i-1} \oplus x = u_i \oplus f_i(x)\}$

هدف پیدا کردن یک پوشش خطی با احتمال دقیقا $\frac{1}{2}$ می‌باشد

$$F: \mathbb{F}_2^n \to \mathbb{F}_2^n$$
$$F = f_r \circ \cdots \circ f_1$$



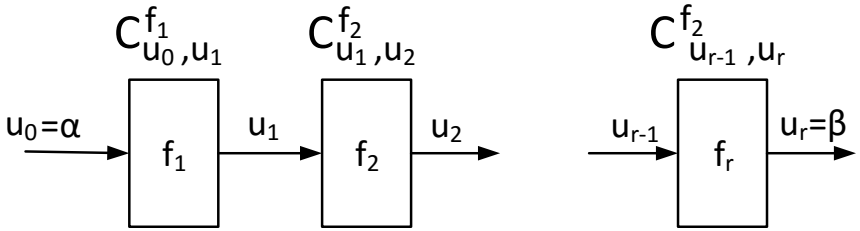
تقریب خطی $u_{i-1} \to u_i$ با نقاب ورودی u_{i-1} و نقاب خروجی u_i را برای نگاشت f_i در نظر بگیرید.

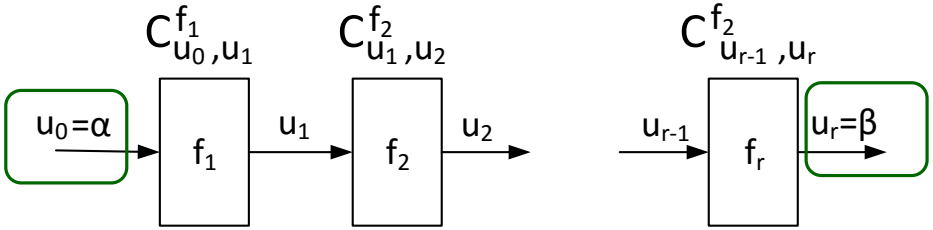


$$u_{i-1}.x \oplus u_i.f_i(x) = 0 \qquad Pr_x\{u_{i-1} \oplus x = u_i \oplus f_i(x)\}$$

همبستگی این تقریب خطی به صورت زیر تعریف می شود:

$$C^{f_i}_{u_{i-1},u_i} = 2Pr_x\{u_{i-1} \oplus x = u_i \oplus f_i(x)\} - 1$$

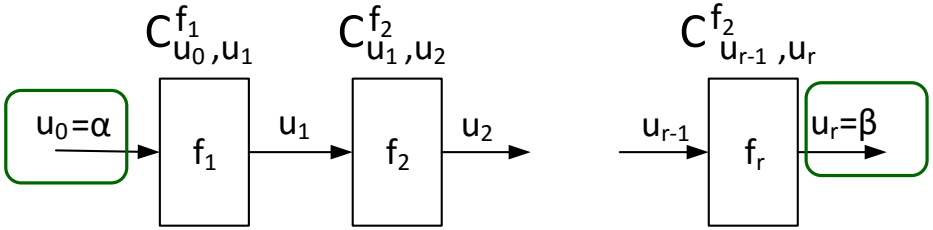




$$U = (u_0 = \boldsymbol{\alpha}, u_1, \dots, u_{r-1}, u_r = \boldsymbol{\beta})$$

همبستگی خطی نسبت به دنباله خطی $U = (u_0, u_1, \dots, u_{r-1}, u_r)$ را با C_u نشان می‌دهیم و به صورت زیر تعریف می‌شود:

$$C_u = \prod_{i=1}^{r} C^{f_i}_{u_{i-1},u_i}$$



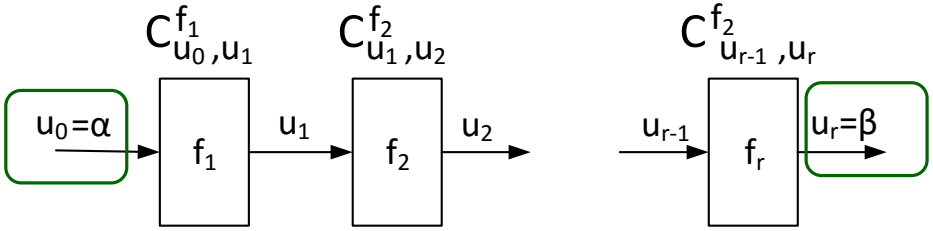
$$U = (u_0 = \boldsymbol{\alpha}, u_1, \dots, u_{r-1}, u_r = \boldsymbol{\beta})$$

همبستگی خطی نسبت به دنباله خطی $U = (u_0, u_1, \dots, u_{r-1}, u_r)$ را با C_u نشان می‌دهیم و به صورت زیر تعریف می‌شود:

$$C_u = \prod_{i=1}^{r} C^{f_i}_{u_{i-1},u_i}$$

همبستگی C برابر با مجموع همبستگی دنباله خطی U یعنی C_U با نقاب ورودی α و نقاب خروجی β می‌باشد. بنابراین داریم:

$$C = \sum_{U:u_0=\alpha,u_{r=\beta}} C_U$$



$$U = (u_0 = \boldsymbol{\alpha}, u_1, \dots, u_{r-1}, u_r = \boldsymbol{\beta})$$

همبستگی خطی نسبت به دنباله خطی $U = (u_0, u_1, \dots, u_{r-1}, u_r)$ را با C_u نشان می‌دهیم و به صورت زیر تعریف می‌شود:

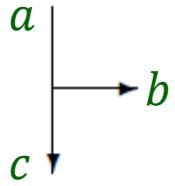
$$C_u = \prod_{i=1}^{r} C^{f_i}_{u_{i-1},u_i}$$

همبستگی C برابر با مجموع همبستگی دنباله خطی U یعنی C_U با نقاب ورودی α و نقاب خروجی β می‌باشد. بنابراین داریم:

$$C = \sum_{U:u_0=\alpha,u_r=\beta} C_U$$

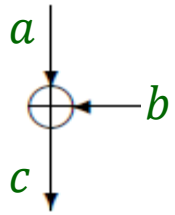
یک تقریب خطی روی رمزهای قالبی با نقاب ورودی α و نقاب خروجی β دارای همبستگی صفر می‌باشد اگر $C = 0$ شود و به صورت $\alpha \nrightarrow \beta$ نشان داده می‌شود

ویژگی ۱ (تقریب مربوط به عملگر سه شاخه‌ای): مجموع XOR نقاب های ورودی و خروجی عملگر سه شاخه‌ای برابر با صفر می‌باشد در غیر اینصورت همبستگی روی این عملگر برابر با صفر می‌باشد.



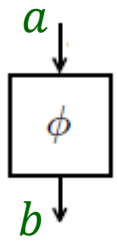
$$a \oplus b \oplus c = 0$$

ویژگی ۲ (تقریب مربوط به عملگر XOR): نقاب‌های مربوط به ورودی و خروجی این عملگر باهم برابر می‌باشند در غیر اینصورت همبستگی روی عملگر XOR برابر با صفر می‌باشد.

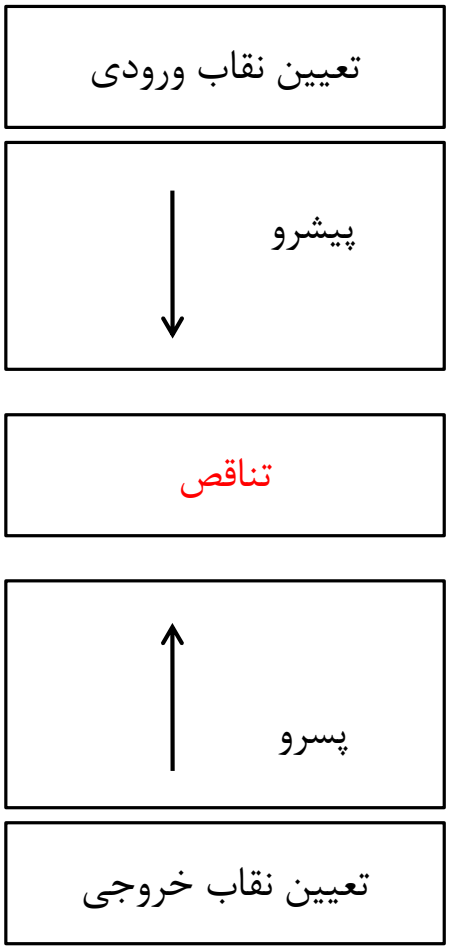


$$a = b = c$$

ویژگی ۲ (تقریب مربوط به جایگشتها): نقاب‌های مربوط به ورودی و خروجی یا هردو صفر هستند یا هردو غیر صفر در غیر اینصورت همبستگی صفر داریم.



$$\begin{cases} a = b = 0 \\ a \neq 0, b \neq 0 \end{cases}$$



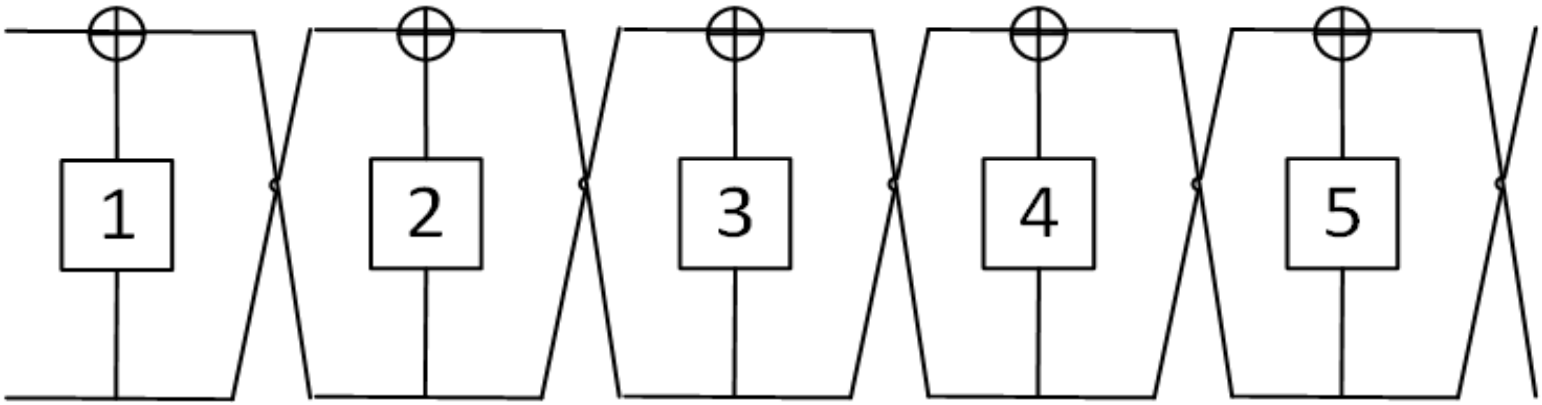
روش حمله فقدان در میانه

Biham, et al., *Miss in the Middle Attacks on IDEA and Khufu.* International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 1999.

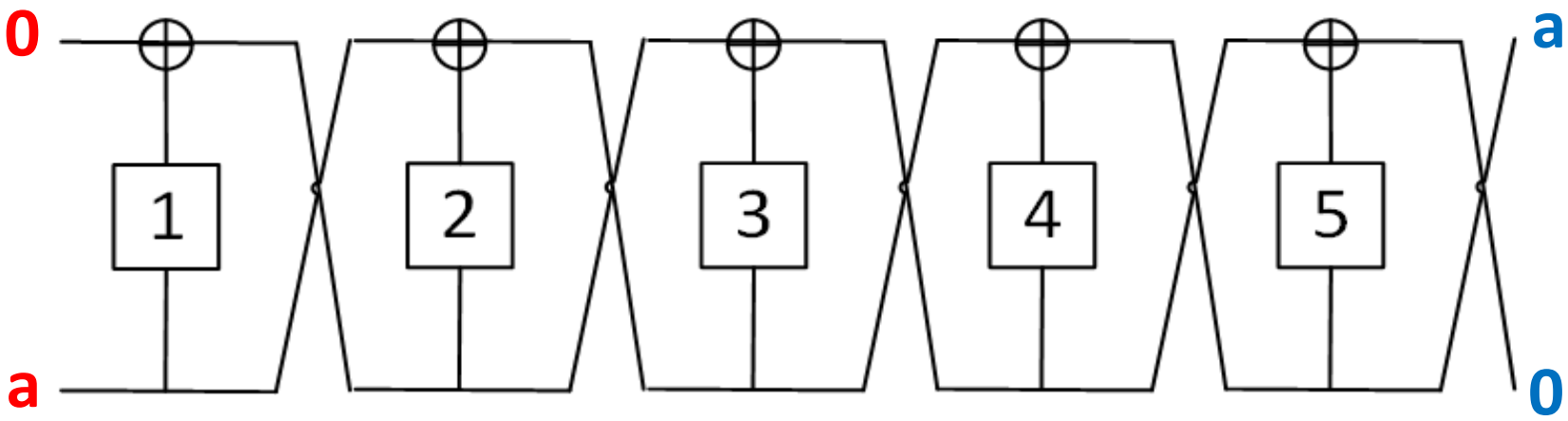
روش ماتریسی

Soleimany, Hadi, and Kaisa Nyberg. "Zero-correlation linear cryptanalysis of reduced-round LBlock." *Designs, codes and cryptography* 73.2 (2014): 683-698.

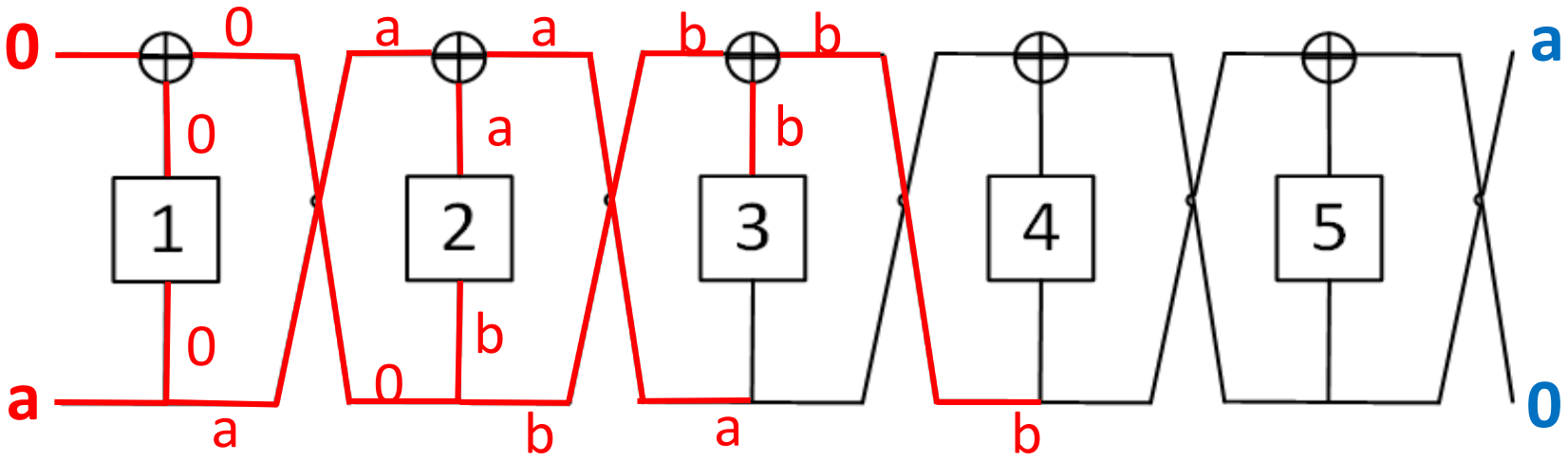
پنج دور مشخصه همبستگی صفر برای ساختارهای فیستلی



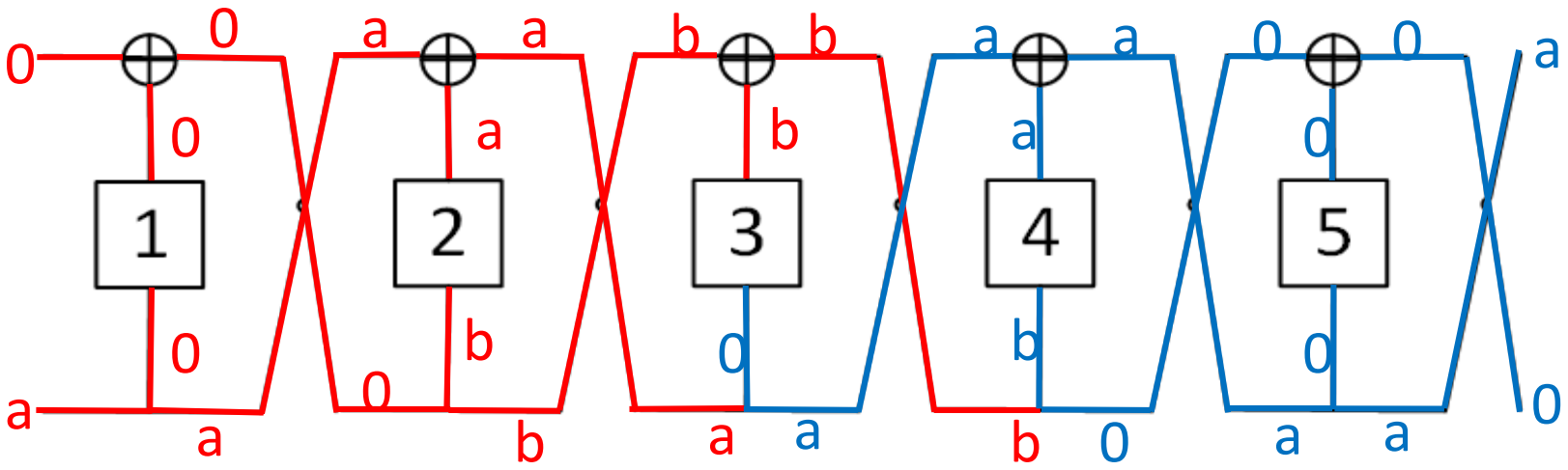
پنج دور مشخصه همبستگی صفر برای ساختارهای فیستلی



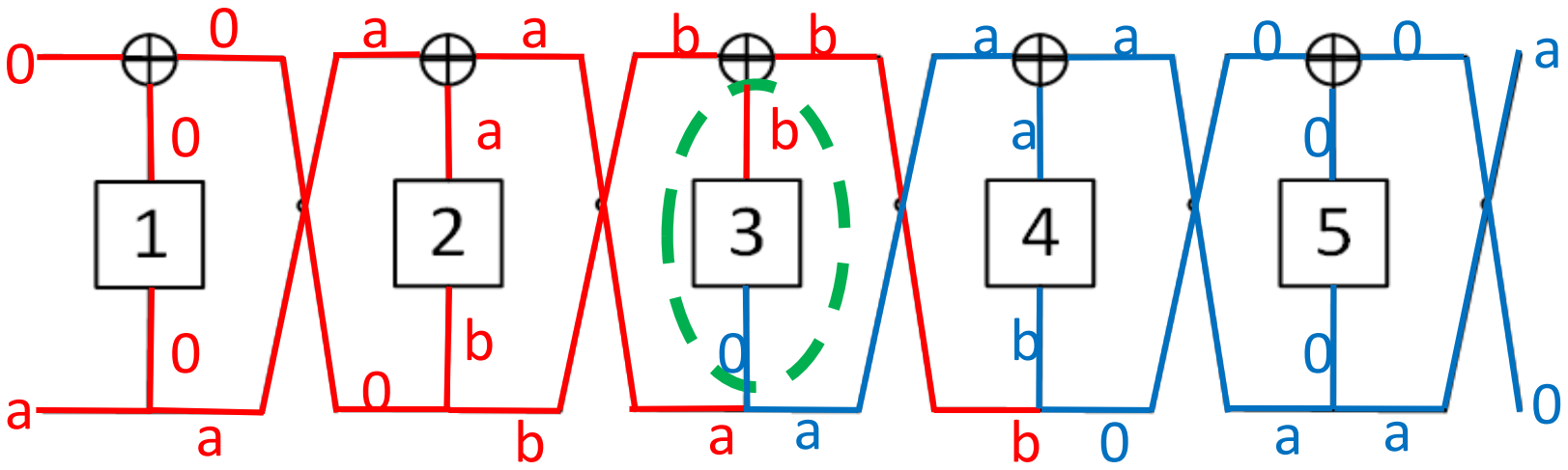
پنج دور مشخصه همبستگی صفر برای ساختارهای فیستلی



پنج دور مشخصه همبستگی صفر برای ساختارهای فیستلی

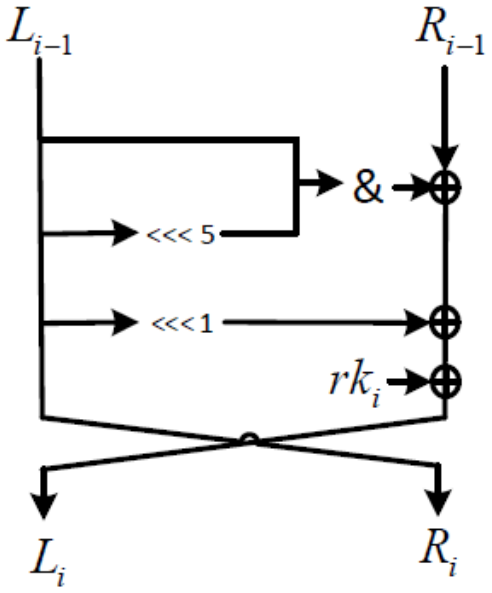


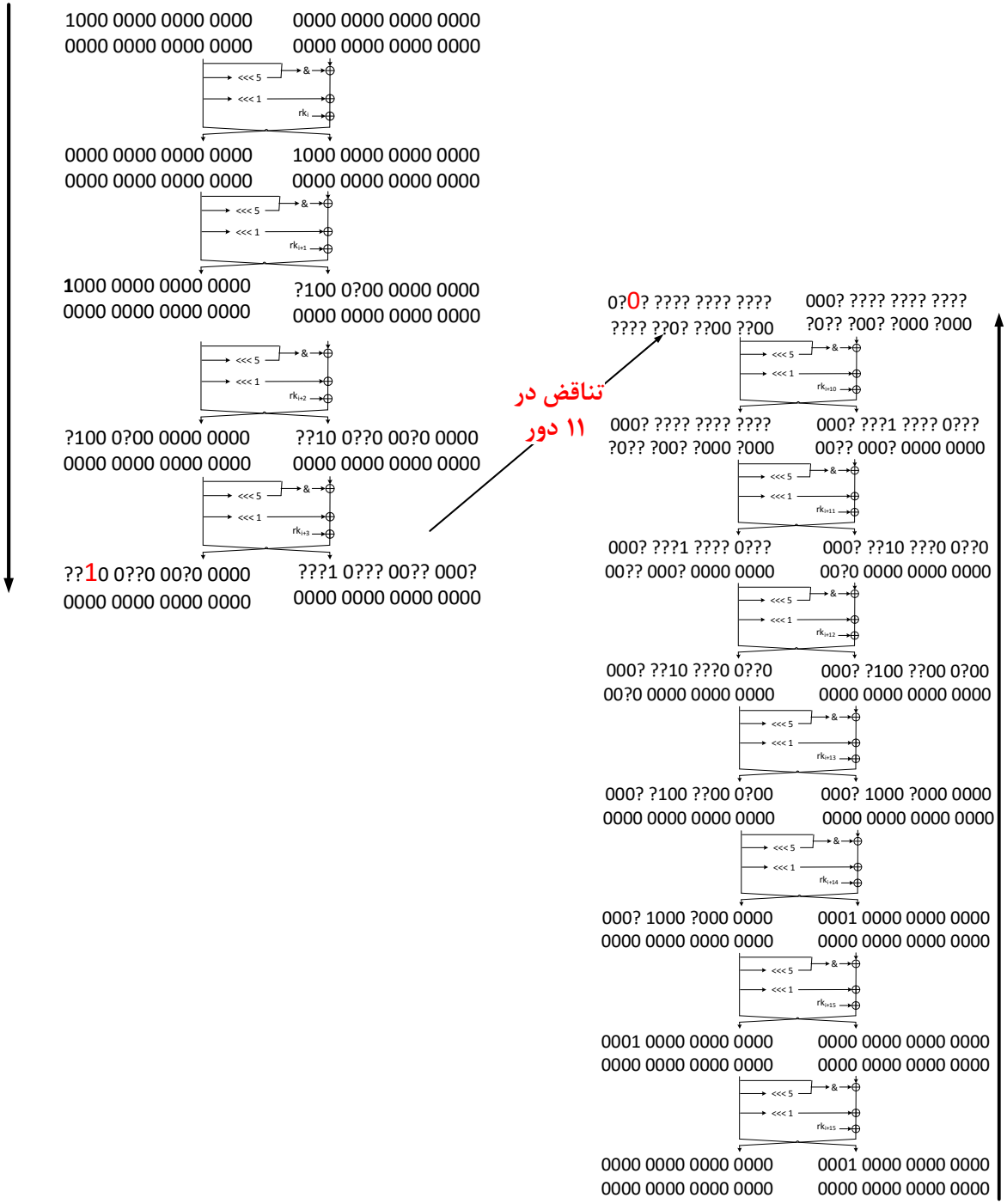
پنج دور مشخصه همبستگی صفر برای ساختارهای فیستلی

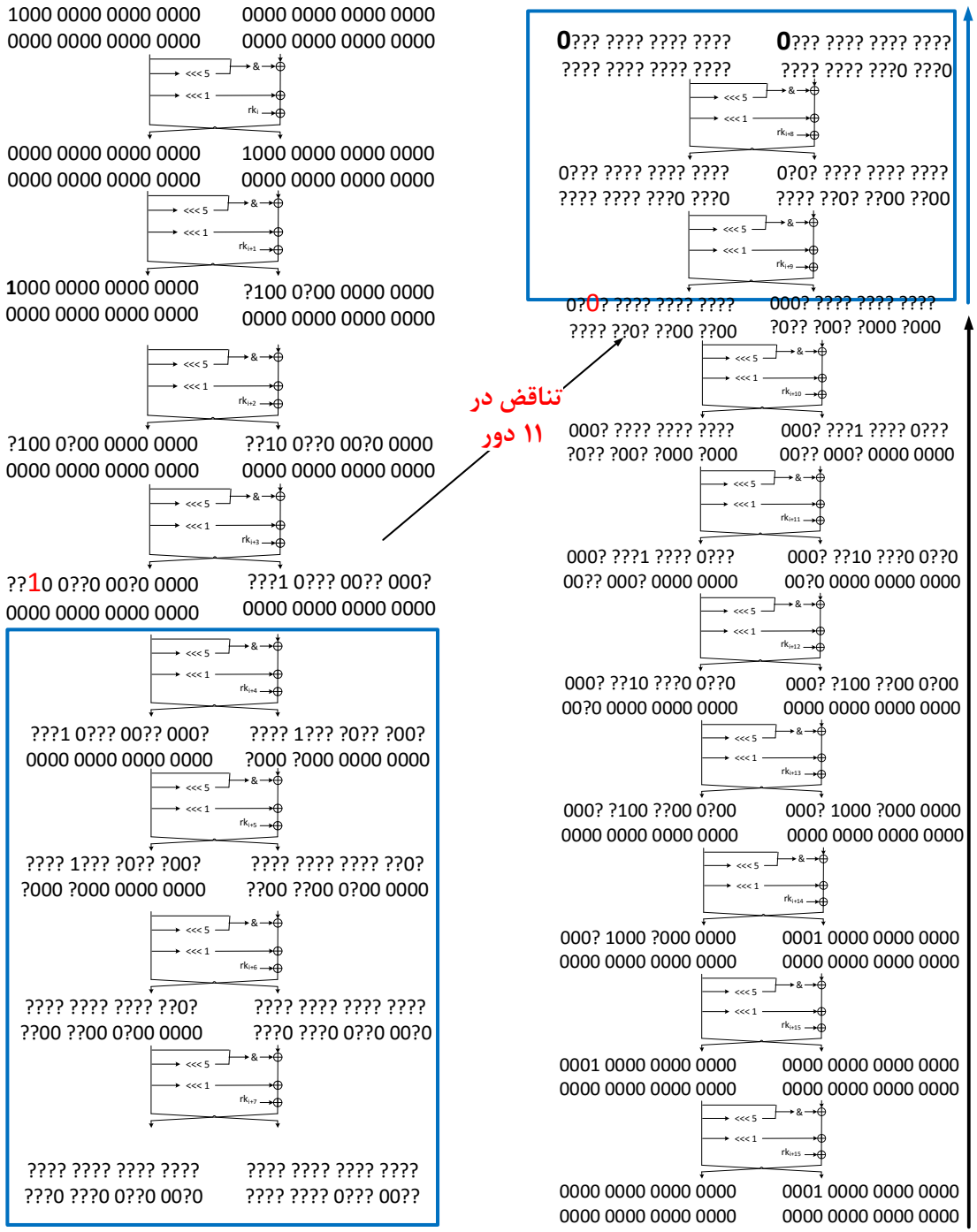


SIMECK

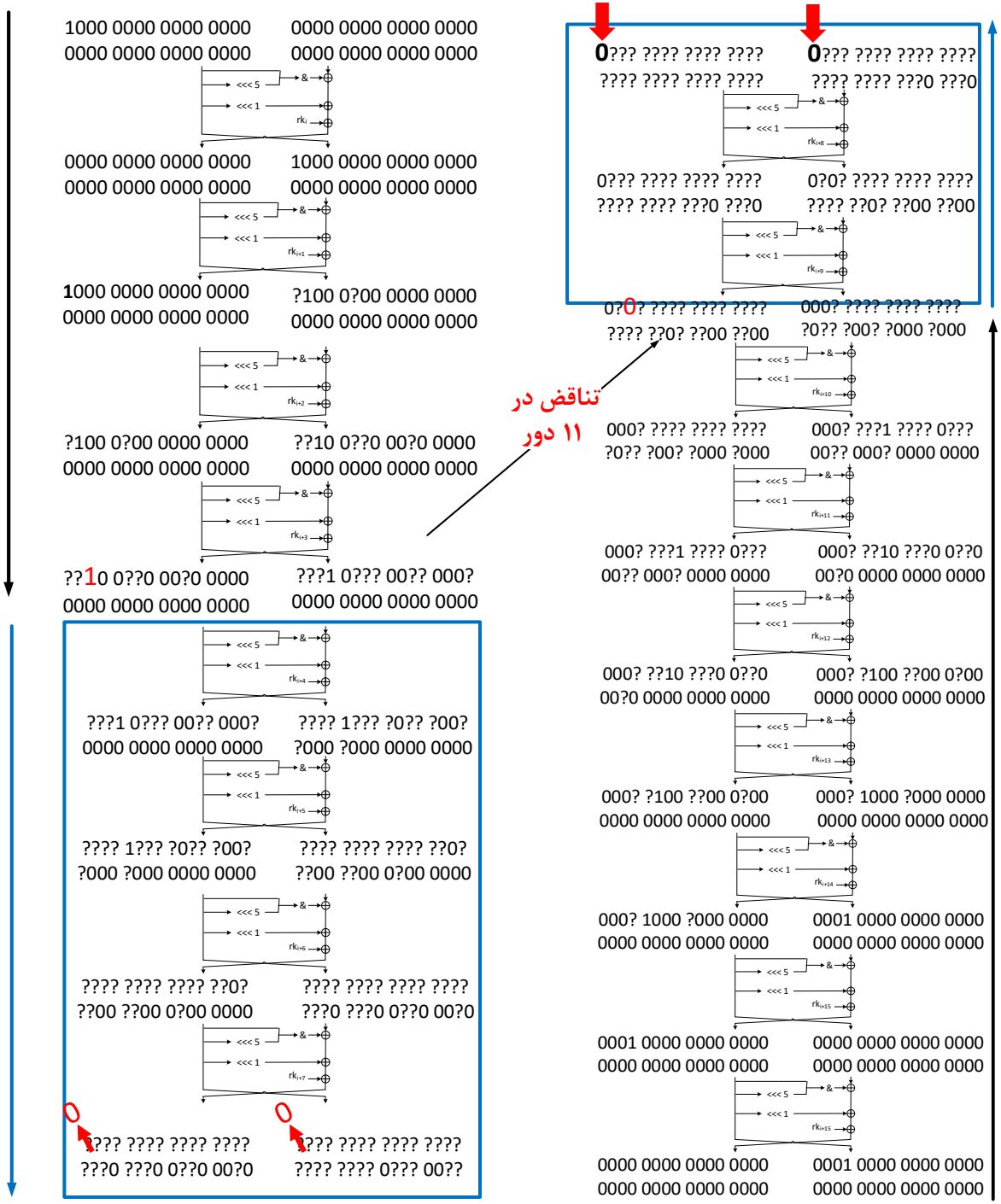
الگوریتم سایمک



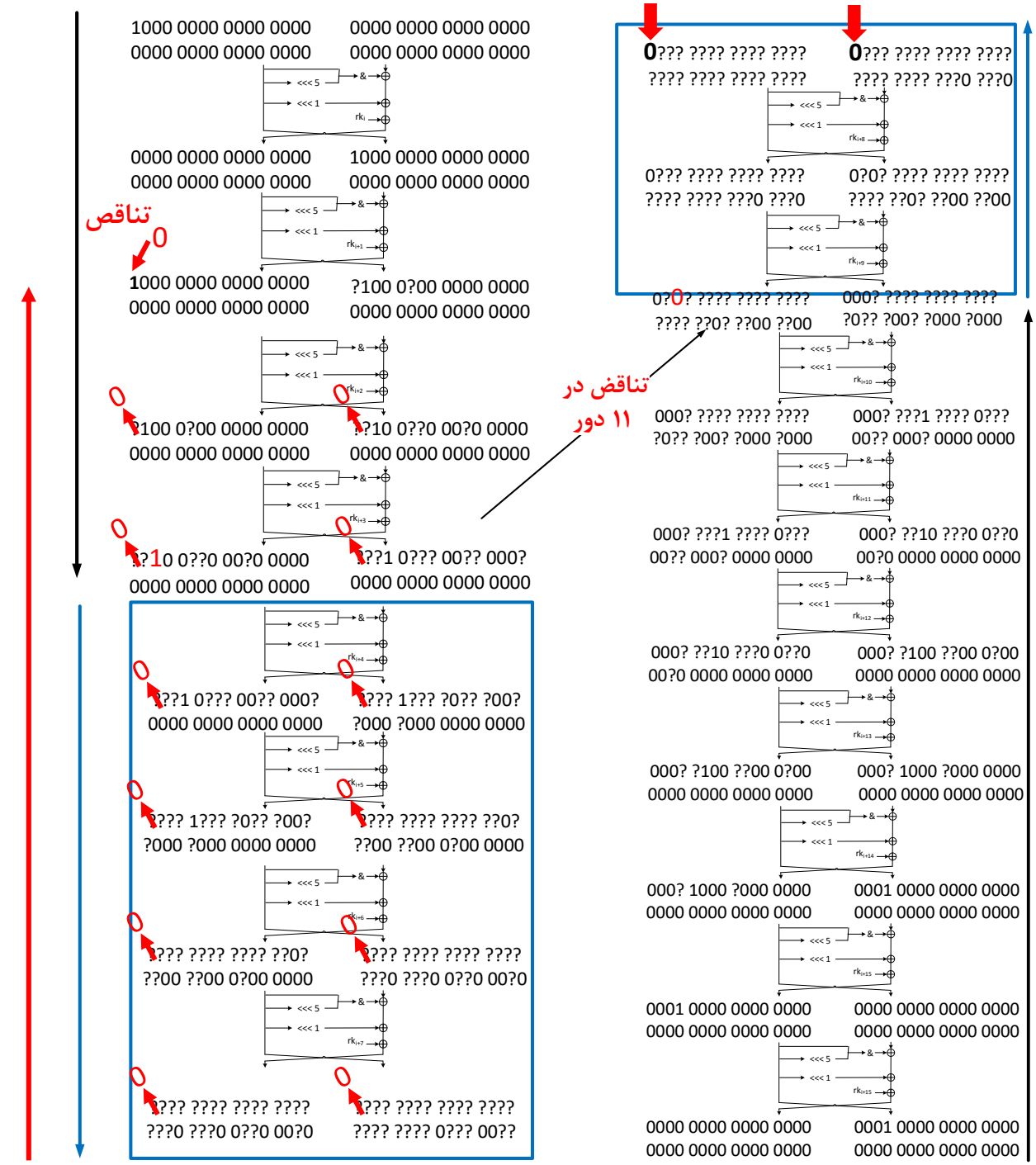

1000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
1000 0000 0000 0000
0000 0000 0000 0000
1000 0000 0000 0000
0000 0000 0000 0000
?100 0?00 0000 0000
0000 0000 0000 0000
?100 0?00 0000 0000
0000 0000 0000 0000
??10 0??0 00?0 0000
0000 0000 0000 0000
??10 0??0 00?0 0000
0000 0000 0000 0000
???1 0??? 00?? 000?
0000 0000 0000 0000
0?0? ???? ???? ????
???? ??0? ??00 ??00
000? ???? ???? ????
?0?? ?00? ?000 ?000
000? ???? ???? ????
?0?? ?00? ?000 ?000
000? ???1 ???? 0???
00?? 000? 0000 0000
000? ???1 ???? 0???
00?? 000? 0000 0000
000? ??10 ???0 0??0
00?0 0000 0000 0000
000? ??10 ???0 0??0
00?0 0000 0000 0000
000? ?100 ??00 0?00
0000 0000 0000 0000
000? ?100 ??00 0?00
0000 0000 0000 0000
000? 1000 ?000 0000
0000 0000 0000 0000
000? 1000 ?000 0000
0000 0000 0000 0000
0001 0000 0000 0000
0000 0000 0000 0000
0001 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0001 0000 0000 0000
0000 0000 0000 0000
<<< 5
<<< 1
&
تناقض در
۱۱ دور



Sadeghi, et al.
IET Information Security
2018



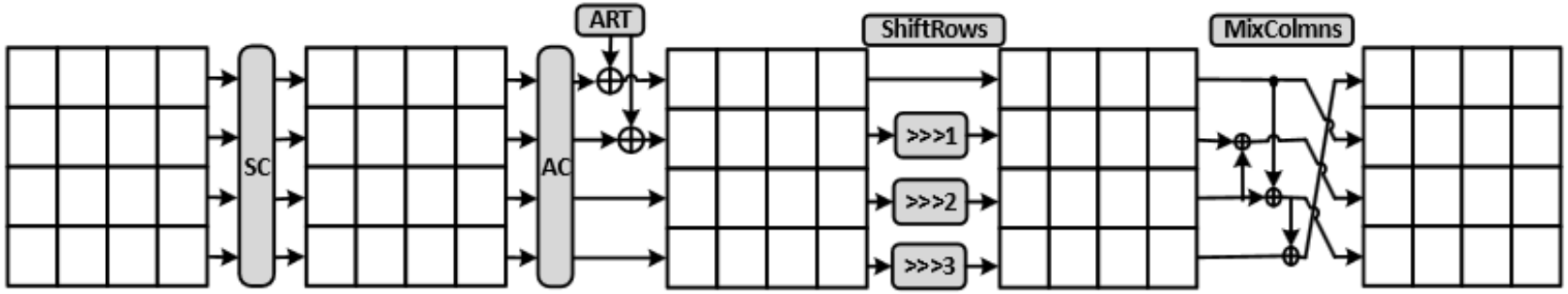
Sadeghi, et al.
IET Information Security
2018



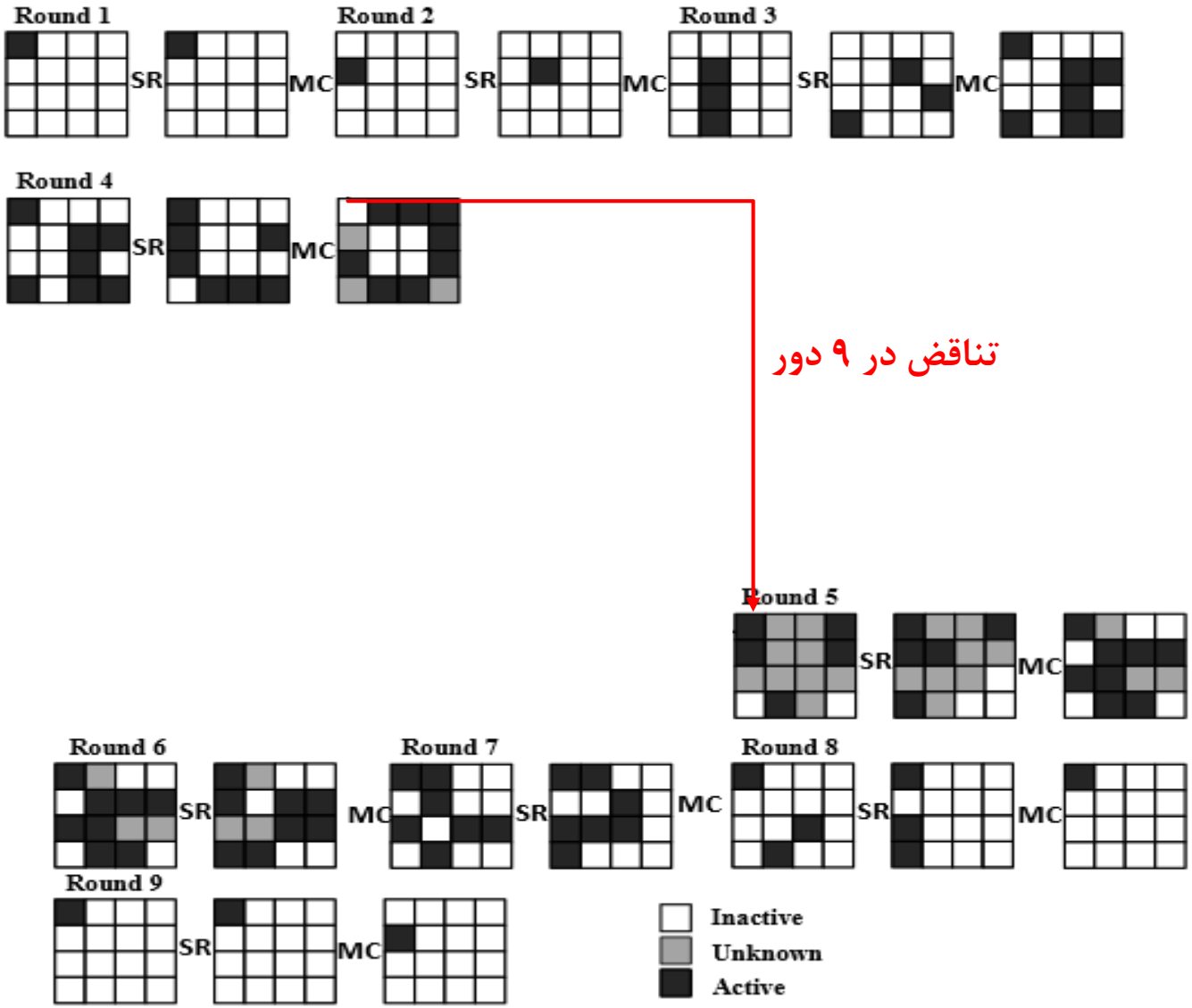
Sadeghi, et al.
IET Information Security
2018

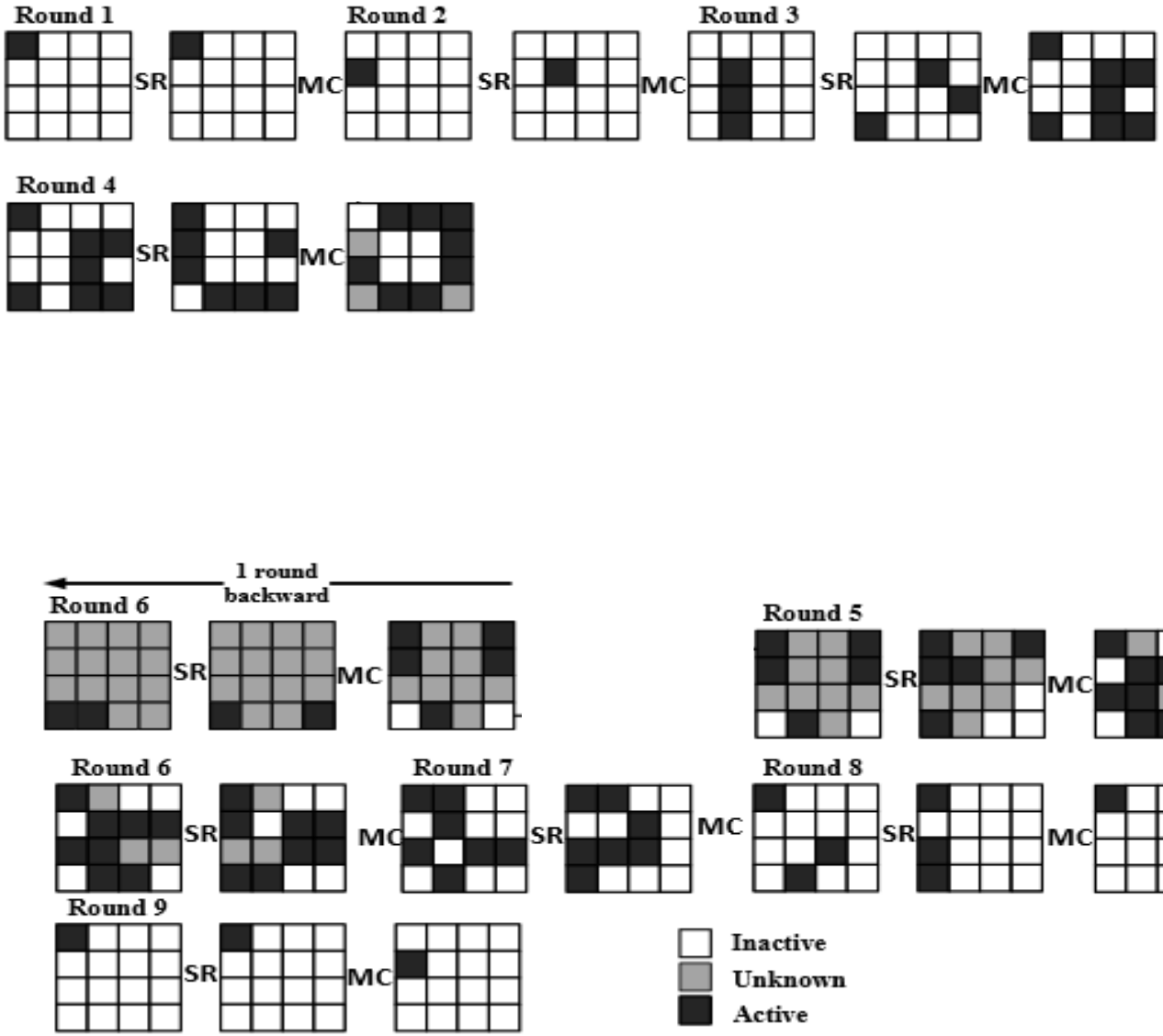
SKINNY

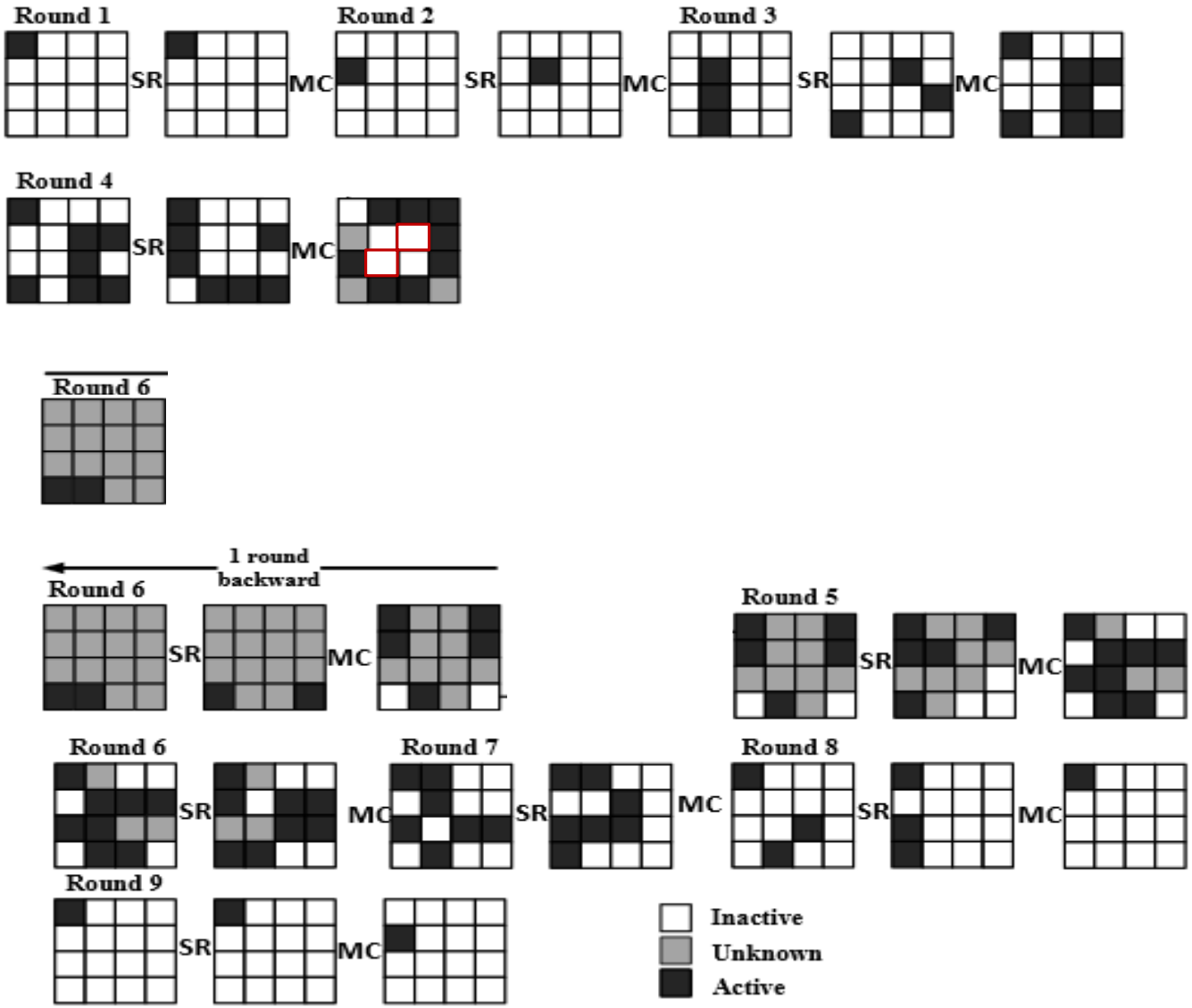
الگوریتم اسکینی



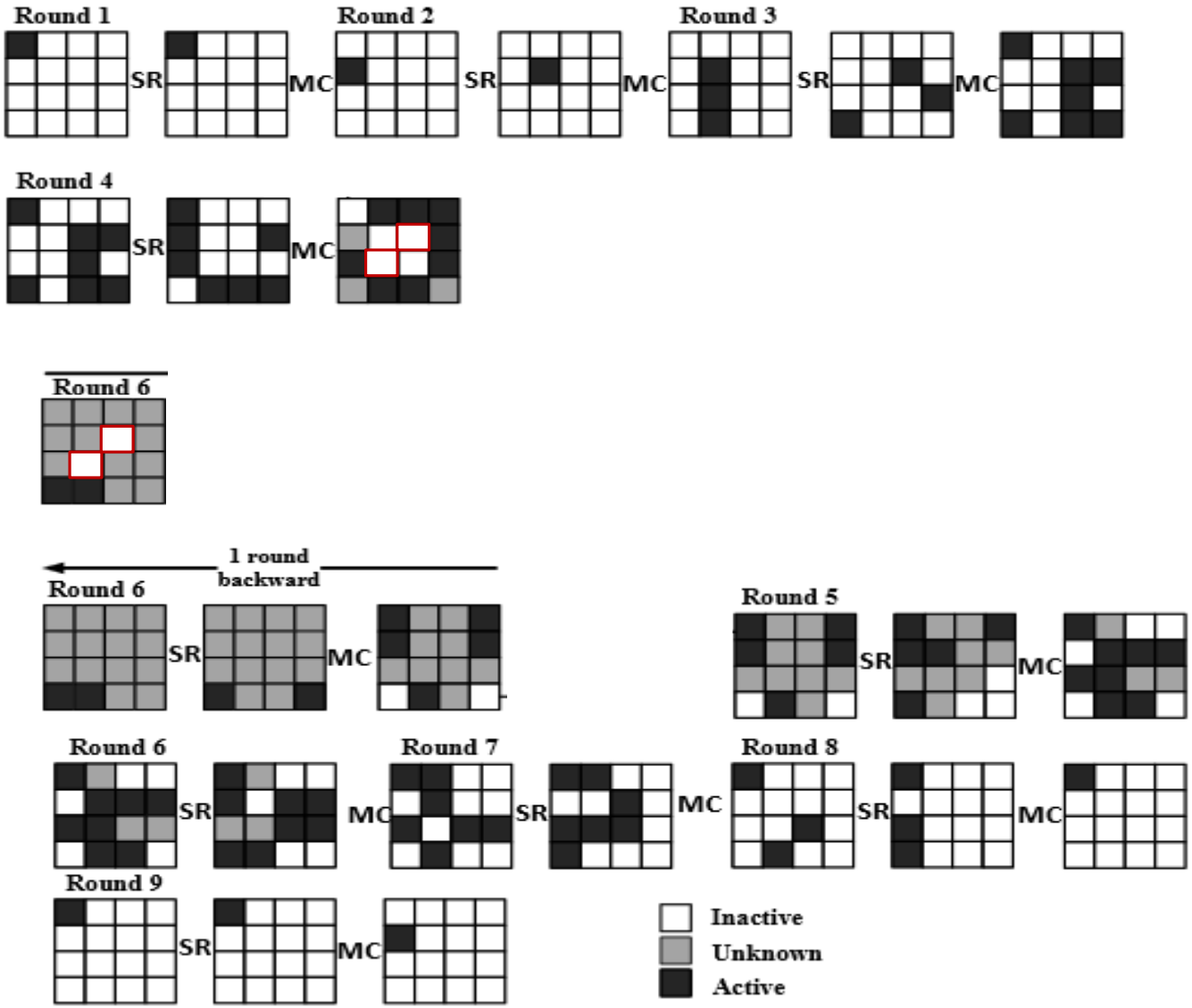
Beierle, Christof, et al. "The SKINNY family of block ciphers and its low-latency variant MANTIS." Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2016.

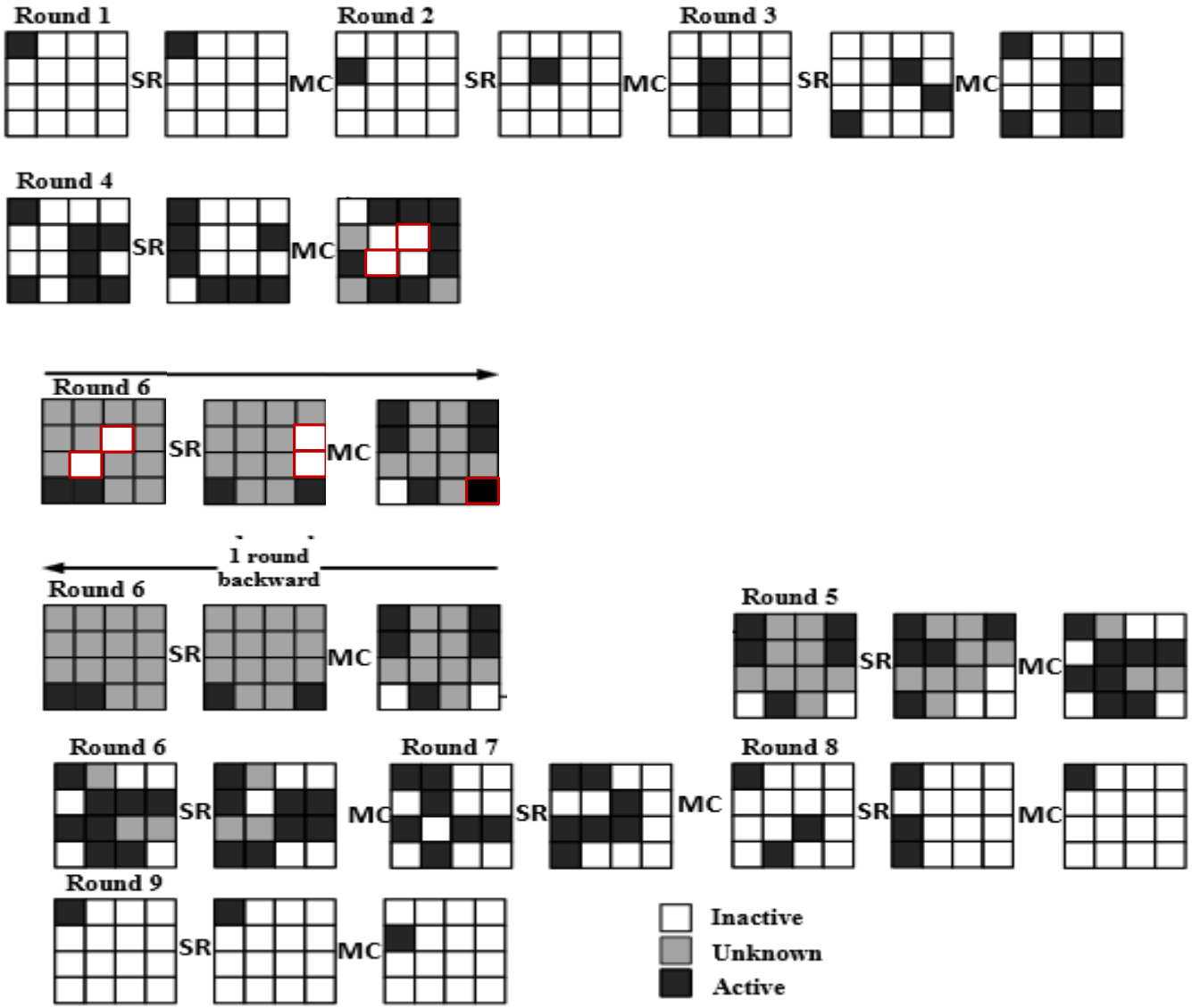

Round 1
SR
MC
Round 2
SR
MC
Round 3
SR
MC
Round 4
SR
MC
تناقض در ۹ دور
Round 5
SR
MC
Round 6
SR
MC
Round 7
SR
MC
Round 8
SR
MC
Round 9
SR
MC
Inactive
Unknown
Active

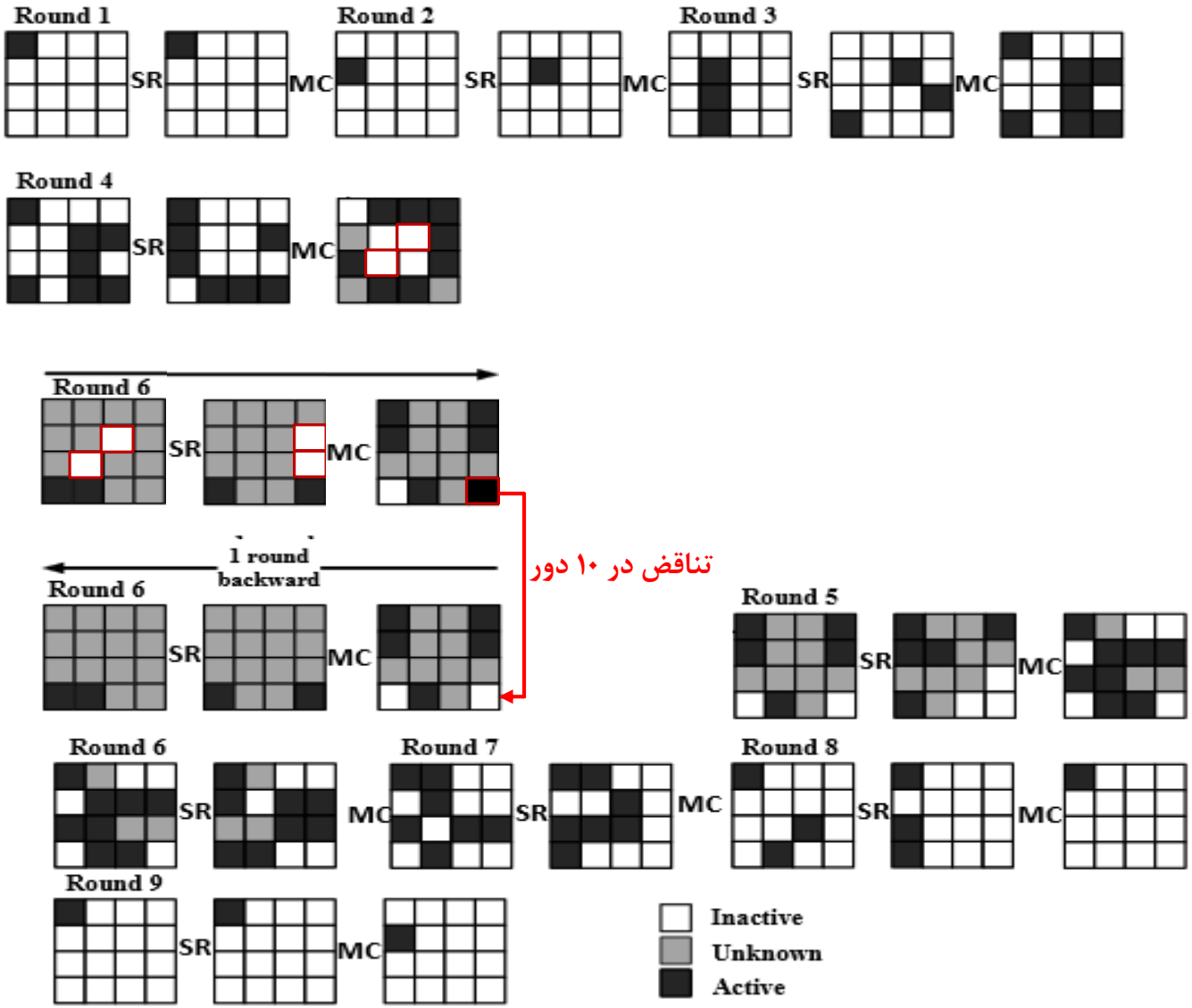

Round 1
SR
MC
Round 2
SR
MC
Round 3
SR
MC
Round 4
SR
MC
1 round backward
Round 6
SR
MC
Round 5
SR
MC
Round 6
SR
MC
Round 7
SR
MC
Round 8
SR
MC
Round 9
SR
MC
Inactive
Unknown
Active



Sadeghi, Sadegh, Tahereh Mohammadi, and Nasour Bagheri. "Cryptanalysis of reduced round SKINNY block cipher." IACR Transactions on Symmetric Cryptology (2018): 124-162.


Round 1
SR
MC
Round 2
SR
MC
Round 3
SR
MC
Round 4
SR
MC
Round 6
1 round backward
Round 6
SR
MC
Round 5
SR
MC
Round 6
SR
MC
Round 7
SR
MC
Round 8
SR
MC
Round 9
SR
MC
Inactive
Unknown
Active


Round 1
Round 2
Round 3
Round 4
Round 5
Round 6
Round 7
Round 8
Round 9
SR
MC
1 round backward
Inactive
Unknown
Active

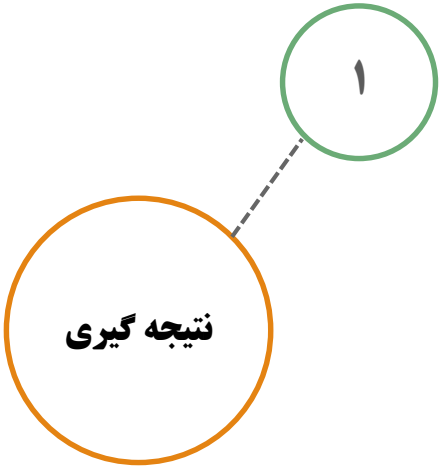


Sadeghi, Sadegh, Tahereh Mohammadi, and Nasour Bagheri. "Cryptanalysis of reduced round SKINNY block cipher." IACR Transactions on Symmetric Cryptology (2018): 124-162.

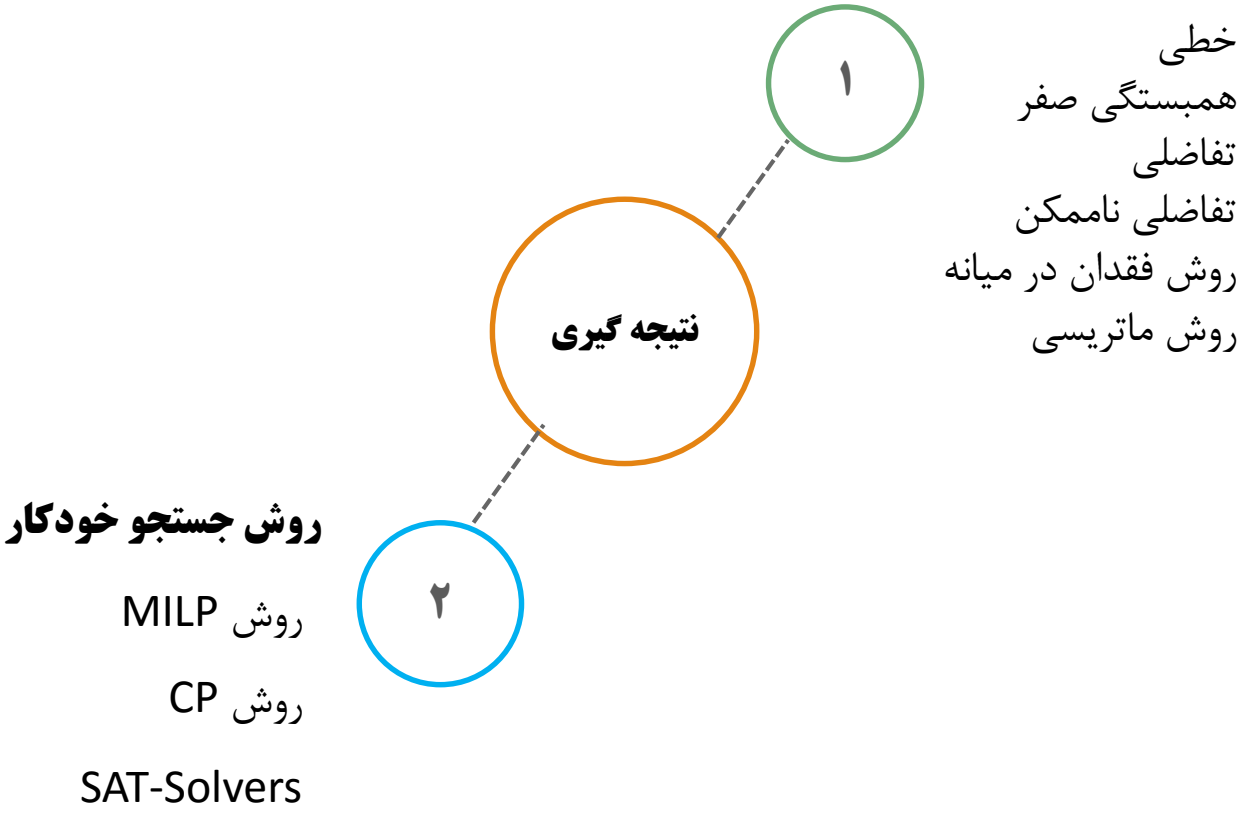
روش ماتریسی

Soleimany Hadi, and Kaisa Nyberg,
Zero-correlation linear cryptanalysis of reduced-round LBlock.
Designs, codes and cryptography, 2014. 73(2): p. 683-698

نتیجه گیری



خطی
همبستگی صفر
تفاضلی
تفاضلی ناممکن
روش فقدان در میانه
روش ماتریسی


۱
خطی
همبستگی صفر
تفاضلی
تفاضلی ناممکن
روش فقدان در میانه
روش ماتریسی
نتیجه گیری
۲
روش جستجو خودکار
روش MILP
روش CP
SAT-Solvers

باتشکر
از حضورتان