Automatic Security Evaluation of Block Cipher

Liu Zhang

School of Cyber Engineering, Xidian University

October 13, 2020

Outline

Block Cipher

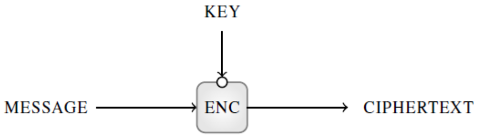

Figure: The process of encryption

A block cipher has two important parameters:

- the *blocksize*, which will be denoted by $\mathbf{b}$, and
- the *keysize*, which will be denoted by $\mathbf{k}$.

Structure of Block Cipher

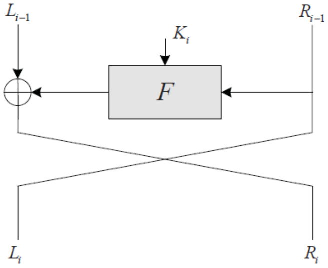

Figure: Feistel-Structure

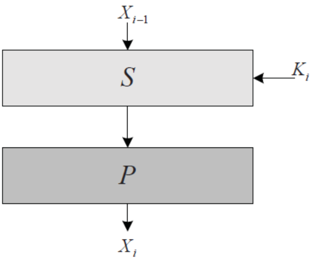

Figure: SP-Structure

Present

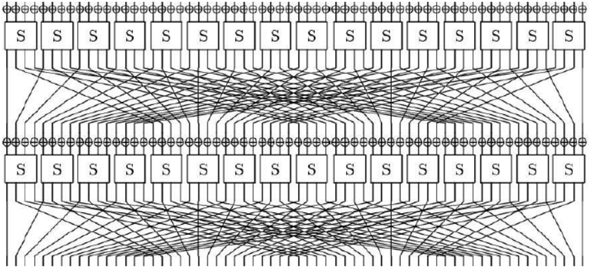

Figure: Two consecutive rounds of Present-80 encryption process

Differential Model of Sbox

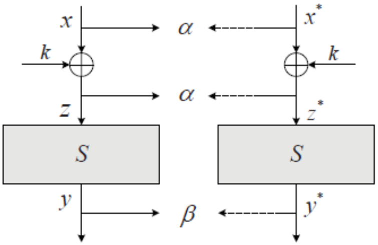

Figure: Differential Model of Sbox

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Figure: The S-box of Present

The Differential Distribution Table of Present S-box

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2_x	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3_x	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4_x	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5_x	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6_x	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7_x	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8_x	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9_x	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
A_x	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
B_x	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
C_x	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
D_x	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
E_x	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
F_x	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

Figure: The Differential Distribution Table of Present S-box

Outline

Differential Cryptanalysis of a Toy Cipher

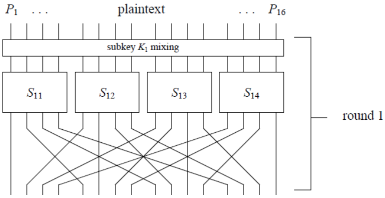

Figure: Round-1

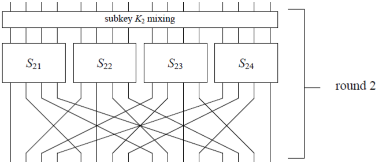

Figure: Round-2

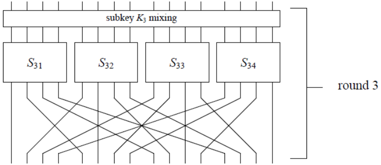

Figure: Round-3

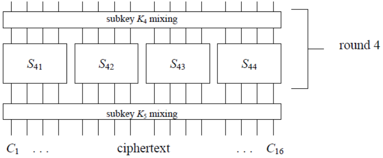

Figure: Round-4

Differential Cryptanalysis of a Toy Cipher

- S-box Representation of Toy Cipher

input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
output	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

- Permutation of Toy Cipher

input	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
output	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Differential Cryptanalysis of a Toy Cipher

Input Difference \ Output Difference	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Figure: Difference Distribution Table

Differential Cryptanalysis of a Toy Cipher

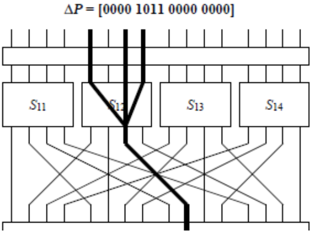

Figure: Round-1

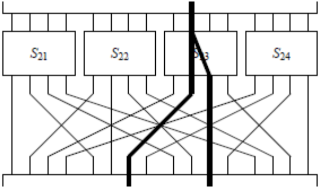

Figure: Round-2

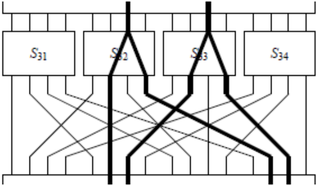

Figure: Round-3

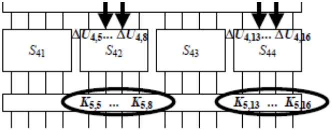

Figure: Round-4

Differential Cryptanalysis of a Toy Cipher

We use the follwing difference pairs of the S-box:

- $S_{12} : \Delta X = B \rightarrow \Delta Y = 2$ with probability 8/16
- $S_{12} : \Delta X = 4 \rightarrow \Delta Y = 6$ with probability 6/16
- $S_{12} : \Delta X = 2 \rightarrow \Delta Y = 5$ with probability 6/16
- $S_{12} : \Delta X = 2 \rightarrow \Delta Y = 5$ with probability 6/16

The input difference and output difference to the every round

- $\Delta P = \Delta U_1 = [0000\ 1011\ 0000\ 0000]$ with probability 8/16
- $\Delta V_1 = [0000\ 0010\ 0000\ 0000]$
- $\Delta U_2 = [0000\ 0000\ 0100\ 0000]$ with probability 6/16
- $\Delta V_2 = [0000\ 0000\ 0110\ 0000]$
- $\Delta U_3 = [0000\ 0010\ 0010\ 0000]$ with probability (6/16)*(6/16)
- $\Delta V_3 = [0000\ 0101\ 0101\ 0000]$
- $\Delta U_4 = [0000\ 0110\ 0000\ 0110]$

Total probability is $8/16 \times 6/16 \times (6/16)^2 = 27/1024$

Differential Cryptanalysis of a Toy Cipher

partial subkey $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	prob	*partial subkey* $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	prob
1 C	0.0000	2 A	0.0032
1 D	0.0000	2 B	0.0022
1 E	0.0000	2 C	0.0000
1 F	0.0000	2 D	0.0000
2 0	0.0000	2 E	0.0000
2 1	0.0136	2 F	0.0000
2 2	0.0068	3 0	0.0004
2 3	0.0068	3 1	0.0000
2 4	**0.0244**	3 2	0.0004
2 5	0.0000	3 3	0.0004
2 6	0.0068	3 4	0.0000
2 7	0.0068	3 5	0.0004
2 8	0.0030	3 6	0.0000
2 9	0.0024	3 7	0.0008

Figure: Experimental Results for Differential Attack

Outline

Introduction of MILP

- Counting the number of active S-boxes is a common way to evaluate the security of symmetric key cryptographic schemes against differential attack. Based on Mixed Integer Linear Programming (MILP), we can the minimal number of active S-boxes.
- MILP: Given $A \in \mathbb{R}^{m\times n}, b \in \mathbb{R}^m$ and $c_1, \cdots, c_n \in \mathbb{R}^n$, find an $x \in \mathbb{Z}^k \times \mathbb{R}^{n-k} \subseteq \mathbb{R}^n$ with $Ax \leq b$, such that the linear function $c_1x_1 + c_2x_2 + \cdots + c_nx_n$ is minimized (or maximized) with respect to the linear constraint $Ax \leq b$.

Building the Model

- For every input and output bit-level difference, a new 0-1 variable x_i is introduced obeying the following rule of variable assignment.

$$x_i = \begin{cases} 1, & \text{for nonzero difference at this bit,} \\ 0, & \text{otherwise.} \end{cases}$$

- For every S-box in the schematic diagram, including the encryption provess and the key schedule algorithm, we instroduce a new 0-1 variable A_j such that

$$A_j = \begin{cases} 1, & \text{if the input word of the Sbox is nonzero,} \\ 0, & \text{otherwise.} \end{cases}$$

- At this point, it is natural to choose the objective function f, which will be minimized, as $\sum A_j$ for the goal of determining a lower bound of the number of active S-boxes.

$$Min\, f = \sum A_j$$

Constrains Describing the S-box Operation

- Suppose $\left(x_{i_0}, \ldots, x_{i_{\omega-1}}\right)$ and $\left(y_{j_0}, \ldots, y_{j_{\nu-1}}\right)$ are the input and output bit-level differences of an $\omega \times \nu$ S-box marked by A_t. Firstly, to ensure that $A_t = 1$ holds if and only if $\left(x_{i_0}, \ldots, x_{i_{\omega-1}}\right)$ are not all zero,we require that:

$$\begin{cases} A_t - x_{i_k} \geq 0, \quad k \in \{0, \ldots, \omega - 1\} \\ x_{i_0} + x_{i_1} + \cdots + x_{i_{\omega-1}} - A_t \geq 0 \end{cases}$$

- For bijective S-boxes, nonzero input difference must result in nonzero output difference and vice versa:

$$\begin{cases} \omega y_{j0} + \omega y_{j_1} + \cdots + \omega y_{j_{\omega-1}} - \left(x_{i_0} + x_{i_1} + \cdots + x_{i_{\omega-1}}\right) \geq 0 \\ \nu x_{i_0} + \nu x_{i_1} + \cdots + \nu x_{i_{\omega-1}} - \left(y_{j_0} + y_{j_1} + \cdots + y_{j_{\nu-1}}\right) \geq 0 \end{cases}$$

Constrains Describing the S-box Operation, cont

- The Hamming weight of the $(\omega+\nu)$-bit word $x_{i_0}\cdots x_{i_{\omega-1}}, y_{j_0}\cdots y_{j_{\nu-1}}$ is lower bounded by the branch number $\mathcal{B}_{\mathcal{S}}$ of the S-box for nonzero input difference $x_{i_0}\cdots x_{i_{\omega-1}}$, where $d_{\mathcal{S}}$ is a dummy variable:

$$\begin{cases} \sum_{k=0}^{\omega-1} x_{i_k} + \sum_{k=0}^{\nu-1} y_{j_k} \geq \mathcal{B}_{\mathcal{S}} d_{\mathcal{S}} \\ d_{\mathcal{S}} \geq x_{i_k}, \quad k \in \{0,\ldots,\omega-1\} \\ d_{\mathcal{S}} \geq y_{j_k}, \quad k \in \{0,\ldots,\omega-1\} \end{cases}$$

- The branch number $\mathcal{B}_{\mathcal{S}}$ of an S-box $\mathcal{S}$ is defined as

$$\mathcal{B}_{\mathcal{S}} = \min_{a\neq b}\{\mathrm{wt}\left((a\oplus b)\|(\mathcal{S}(a)\oplus\mathcal{S}(b)\right) : a,b\in\mathbb{F}_2^{\omega}\}$$

  and $\mathrm{wt}(\cdot)$ is the standard Hamming wight of a 2ω-bit word.

Constrains Imposed by XOR Operations

- Suppose $a \oplus b = c$, where $a, b, c \in \mathbb{F}_2^\omega$ are the input and output differences of the XOR operation, the following constraints will make sure that when a, b and c are not all zero, then there are at least two of them are nonzero:

$$\begin{cases} a + b + c \geq 2d_\oplus \\ d_\oplus \geq a \\ d_\oplus \geq b \\ d_\oplus \geq c \end{cases}$$

  where $d_\oplus$ is a dummy variable taking values from $\{0, 1\}$.

- If each one of a, b and c represents one bit, we should also add the inequalitie:

$$a + b + c \leq 2$$

Result for the single-key Present differential analysis

Rounds	#Variables	#Constraints	#Active S-boxes	Timing (in seconds)
1	96 + 64	257	1	1
2	128 + 128	513	2	1
3	160 + 192	769	4	1
4	192 + 256	1025	6	1
5	224 + 320	1281	10	1
6	256 + 384	1537	12	1
7	288 + 448	1739	14	2
8	320 + 512	2049	16	5
9	352 + 576	2305	18	3
10	384 + 640	2561	20	6
11	416 + 704	2817	22	14
12	448 + 768	3073	24	13
13	480 + 832	3329	26	14
14	512 + 896	3585	28	17
15	544 + 960	3841	30	22
16	576 + 1024	4097	32	27
17	608 + 1088	4353	34	35
18	640 + 1152	4609	36	33
19	672 + 1216	4865	38	46
20	704 + 1280	5121	40	39
21	736 + 1344	5377	42	43
22	768 + 1408	5633	44	82
23	800 + 1472	5889	46	69
24	832 + 1536	6145	48	88
25	864 + 1600	6401	50	107
26	896 + 1664	6657	52	105
27	928 + 1728	6913	54	116
28	960 + 1792	7169	56	140
29	992 + 1856	7425	58	165
30	1024 + 1920	7681	60	262
31	1056 + 1984	7937	62	222

Figure: Result for the single-key Present differential analysis

Outline

Valid Cutting-off Inequalities

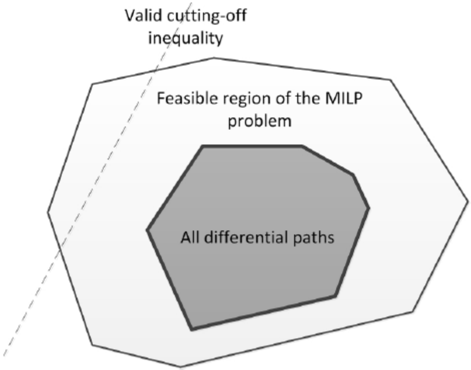

Figure: The relationship between the set of all differential paths and the feasible region of the MILP problem, and the effect of cutting-off inequality

Methods for Generating Valid Cutting-off Inequalities

Theorem (1)

The S-box of PRESENT-80 has the following properties:
(i) $1001 \rightarrow ???0$*: If the input difference of the S-box is* $0x9 = 1001$*, then the least significant bit of the output difference must be 0;*
(ii) $0001 \rightarrow ???1$*: If the input difference of the S-box is* $0x1 = 0001$ *or* $0x8 = 1000$*, then the least significant bit of the output difference must be 1;*
(iii) $???1 \rightarrow 0001$ *and* $???1 \rightarrow 0100$*: If the output difference of the S-box is* $0x1 = 0001$ *or* $0x4 = 0100$*, then the least significant bit of the input difference must be 1;*
(iiii) $???0 \rightarrow 0101$*: If the output difference of the S-box is* $0x5 = 0101$*, then the least significant bit of the input difference must be 0.*

Methods for Generating Valid Cutting-off Inequalities, cont

Theorem (2)

Let 0-1 *variables* (x_0, x_1, x_2, x_3) *and* (y_0, y_1, y_2, y_3) *represent the input and output differences of the S-box respectively, where* x_3 *and* y_3 *are the least significant bit. Then the logical conditions in Theorem 1 can be described by the following linear inequalities:*

$$-x_0 + x_1 + x_2 - x_3 - y_3 + 2 \geq 0$$

$$\begin{cases} x_0 + x_1 + x_2 - x_3 + y_3 \geq 0 \\ -x_0 + x_1 + x_2 + x_3 + y_3 \geq 0 \end{cases}$$

$$\begin{cases} x_3 + y_0 + y_1 + y_2 - y_3 \geq 0 \\ x_3 + y_0 - y_1 + y_2 + y_3 \geq 0 \end{cases}$$

$$-x_3 + y_0 - y_1 + y_2 - y_3 + 2 \geq 0$$

Convex Hull of All Possible Differentials for an S-box

- The convex hull of a set Q of discrete points in $\mathbb{R}^n$ is the smallest convex set that contains Q. A convex hull can be described as the common solutions of a set of finitely many linear euqations and inequalities as follows:

$$\begin{cases} \lambda_{0,0}x_0 + \cdots + \lambda_{0,n-1}x_{n-1} + \lambda_{0,n} \geq 0 \\ \gamma_{0,0}x_0 + \cdots + \gamma_{0,n-1}x_{n-1} + \gamma_{0,n} = 0 \end{cases}$$

  This is called the H-representation of a convex hull.

- Define the convex hull of a specfic $\omega \times \nu$ S-box to the set of all linear inequalities in the H-Representation of the convex hull $\nu_S \subseteq \mathbb{R}^{\omega+\nu}$ of all possible differential patterns of the S-box.

Convex Hull of All Possible Differentials for an S-box, cont

Constraints selected from the convex hull by the greedy algorithm	Impossible differential patterns removed
$(-2, 1, 1, 3, 1, -1, 1, 2, 0)$	(1, 0, 1, 0, 0, 1, 0, 0) (1, 0, 0, 0, 1, 1, 0, 0) (1, 0, 0, 0, 1, 0, 0, 0) (1, 0, 1, 0, 0, 1, 1, 0) (1, 0, 0, 0, 1, 1, 1, 0) (1, 1, 0, 0, 0, 1, 0, 0) (1, 1, 0, 0, 0, 1, 1, 0) (1, 0, 0, 0, 0, 1, 1, 0) (1, 0, 1, 0, 1, 1, 0, 0) (1, 0, 0, 0, 0, 1, 0, 0) (1, 0, 0, 0, 0, 1, 0, 1) (1, 0, 0, 0, 0, 0, 1, 0) (1, 1, 0, 0, 1, 1, 0, 0) (1, 1, 1, 0, 0, 1, 0, 0)
$(1, -2, -3, -2, 1, -4, 3, -3, 10)$	(0, 1, 1, 0, 1, 1, 0, 1) (1, 1, 1, 0, 0, 1, 0, 1) (0, 1, 1, 1, 0, 1, 1, 1) (1, 0, 1, 1, 0, 1, 0, 1) (0, 1, 1, 0, 0, 1, 0, 1) (0, 1, 1, 1, 0, 1, 0, 0) (0, 1, 1, 1, 0, 1, 0, 1) (1, 1, 1, 1, 1, 1, 0, 1) (0, 0, 1, 1, 0, 1, 0, 1) (0, 1, 1, 1, 1, 1, 0, 1) (1, 1, 1, 1, 0, 1, 0, 1) (0, 1, 0, 1, 0, 1, 0, 1) (0, 0, 1, 1, 1, 1, 0, 1)
$(2, -2, 3, -4, -1, -4, -4, 1, 11)$	(0, 1, 0, 1, 0, 1, 1, 0) (1, 1, 0, 1, 0, 1, 1, 0) (0, 0, 0, 1, 1, 1, 1, 0) (0, 1, 0, 1, 0, 1, 1, 1) (0, 0, 0, 1, 1, 1, 1, 1) (0, 1, 0, 1, 1, 1, 1, 1) (0, 1, 0, 1, 1, 1, 1, 0) (0, 0, 0, 1, 0, 1, 1, 0) (1, 1, 0, 1, 1, 1, 1, 0) (0, 1, 1, 1, 1, 1, 1, 0) (1, 1, 0, 1, 1, 1, 1, 1)
$(-1, -2, -2, -1, -1, 2, -1, 0, 6)$	(1, 1, 1, 0, 1, 0, 1, 1) (1, 1, 1, 0, 1, 0, 1, 0) (1, 1, 1, 1, 1, 0, 0, 1) (1, 1, 1, 1, 1, 0, 0, 0) (0, 1, 1, 1, 1, 0, 1, 1) (1, 1, 1, 1, 1, 0, 1, 0) (0, 1, 1, 1, 1, 0, 1, 0) (1, 1, 1, 1, 0, 0, 1, 1) (1, 1, 1, 1, 1, 0, 1, 1) (1, 1, 1, 1, 0, 0, 1, 0)
(-2, 1, -2, -1, 1, -1, -2, 0, 6)	(1, 1, 1, 1, 0, 1, 1, 0) (1, 1, 1, 1, 0, 1, 1, 1) (1, 0, 1, 1, 0, 0, 1, 0) (1, 0, 1, 0, 0, 1, 1, 1) (1, 0, 1, 1, 0, 0, 1, 1) (1, 0, 1, 1, 1, 1, 1, 0) (1, 0, 1, 1, 1, 1, 1, 1) (1, 0, 1, 1, 0, 1, 1, 1) (1, 0, 1, 1, 0, 1, 1, 0)
$(2, 1, 1, -3, 1, 2, 1, 2, 0)$	(0, 0, 0, 1, 1, 0, 0, 0) (0, 0, 1, 1, 0, 0, 1, 0) (0, 0, 0, 1, 0, 0, 0, 1) (0, 1, 0, 1, 1, 0, 0, 0) (0, 0, 0, 1, 0, 1, 0, 0) (0, 0, 0, 1, 0, 0, 1, 0) (0, 0, 1, 1, 1, 0, 0, 0) (0, 1, 0, 1, 0, 0, 1, 0) (0, 0, 0, 1, 1, 0, 1, 0)

Figure: Impossible differential patterns removed by the constraints selected from the convex hull of the Present S-box

Convex Hull of All Possible Differentials for an S-box, cont

Rounds	#Variables	#Constraints	#Active S-boxes	Time (in seconds)
1	$97 + 277$	632	0	1
2	$130 + 474$	1262	0	1
3	$163 + 671$	1892	1	1
4	$196 + 868$	2522	2	1
5	$229 + 1065$	3152	3	5
6	$262 + 1262$	3782	5	16
7	$295 + 1459$	4412	7	107
8	$328 + 1656$	5042	9	254
9	$361 + 1853$	5672	10	522
10	$394 + 2050$	6302	13	4158
11	$427 + 2247$	6932	15	18124
12	$460 + 2444$	7562	16	50017
13	$493 + 2641$	8192	18	137160*
14	$526 + 2838$	8822	20	1316808*
15	$559 + 3035$	9452	–	$>$ 20days

Figure: MILP related-key models for Present with CDP constraints added

Outline

NBC

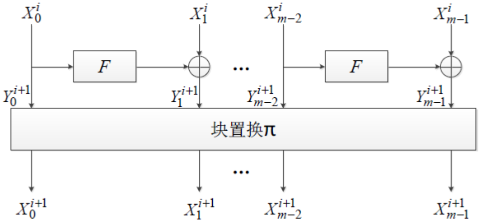

Figure: NBC Round Function

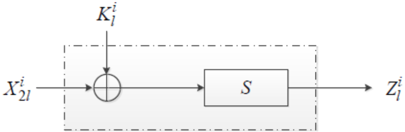

Figure: F Function

NBC-128

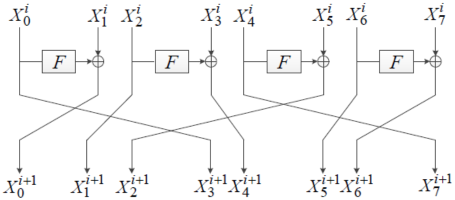

Figure: NBC-128 Round Function

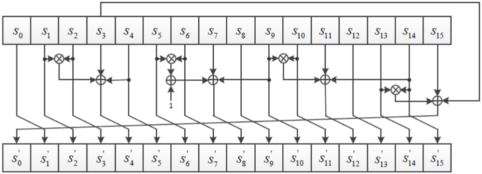

Figure: NBC-128 S-box