LBlock: A Lightweight Block Cipher

Wenling Wu, Lei Zhang

Institute of Software,
Chinese Academy of Sciences

09-Jun-2011

Outline

- **Background and Previous Works**
- **LBlock: Specification**
- **Design Rationale**
- **Security and Performance Evaluations**

Background

⌘ Application Security Requirements

- RFID applications, wireless sensor network…

⌘ Main Features

- extremely resource constrained environment
  - Weak computation ability
  - Small storage space
  - Strict power constraints
- Moderate security requirement

⌘ Solutions: Lightweight Ciphers

- mCrypton, HIGHT, PRESENT, CGEN, DESL, MIBS, KATAN, TWIS, …

Previous Works

- **PRESENT** Bogdanov, Knudsen, Leander, Paar, Poschmann, Robshaw, Seurin, Vikkelsoe CHES '07
  - SP-network, 31-round, 64-bit block, 80/128-bit key
  - Attacks:
    - linear attack on 25-round
    - differential attack on 16-round
    - statistical saturation attack on 15-round
- **HIGHT** Hong, Sung, Hong, Lim, Lee, Koo, Lee, Chang, Lee, Jeong, Kim, Kim, Chee CHES '06
  - Generalized Feistel Structure, 32-round, 64-bit block, 128-bit key
  - Attacks:
    - related-key attack on full-round
    - related-key impossible attack on 31-round
    - saturation attack on 22-round
- **mCrypton, CGEN, DESL, MIBS, KATAN/KTANTAN, TWIS …**
    - differential distinguisher on full-round TWIS
    - meet-in-the-middle attack on KTANTAN family

LBlock

Motivation

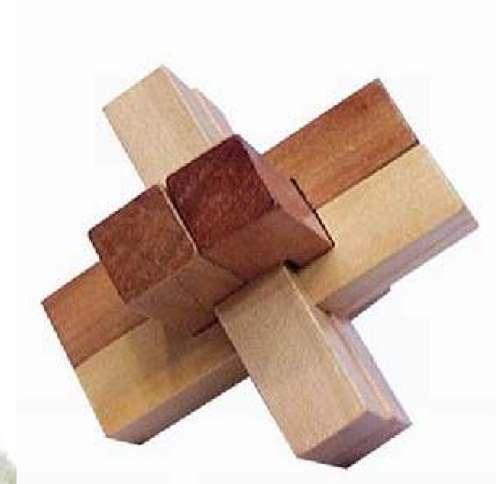
- New proposals in cipher design are always valuable attempts.
- Improve cryptanalysis and design techniques

Main Idea

- Trade-off between security and performance
- Ultra lightweight in both hardware and 8-bit platforms

The Name -- LBlock

- LuBan lock “鲁班锁”
- Lightweight Block cipher



1. Specification of LBlock

⌘ Overall Parameters

Variant Feistel structure, 32-round, 64-bit block, 80-bit key

⌘ Encryption Algorithm

1. For $i = 2, 3, \ldots, 33$, do

$$X_i = F(X_{i-1}, K_{i-1}) \oplus (X_{i-2} <<< 8)$$

2. Output $C = X_{32} || X_{33}$ as the 64-bit ciphertext

Specification of LBlock

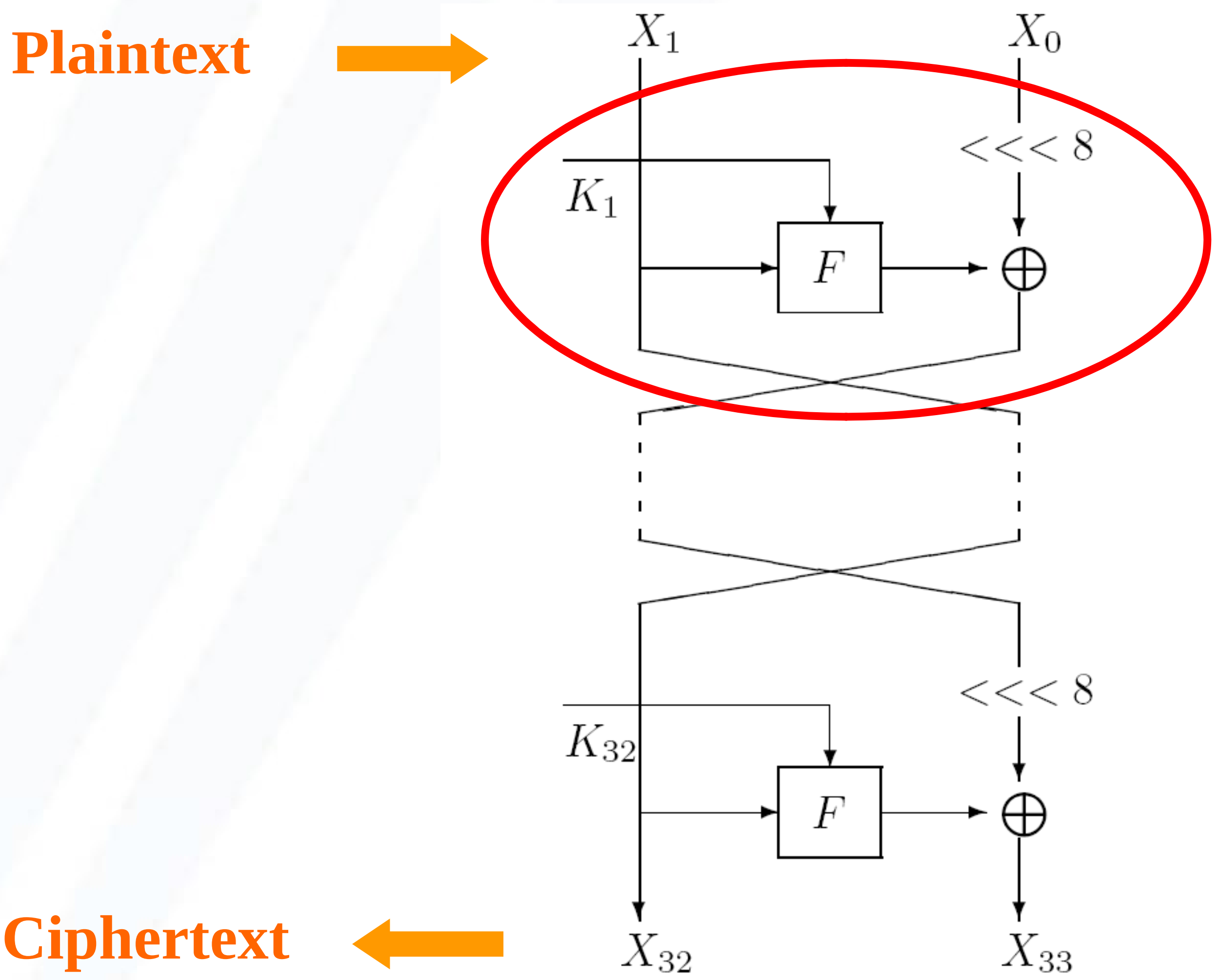
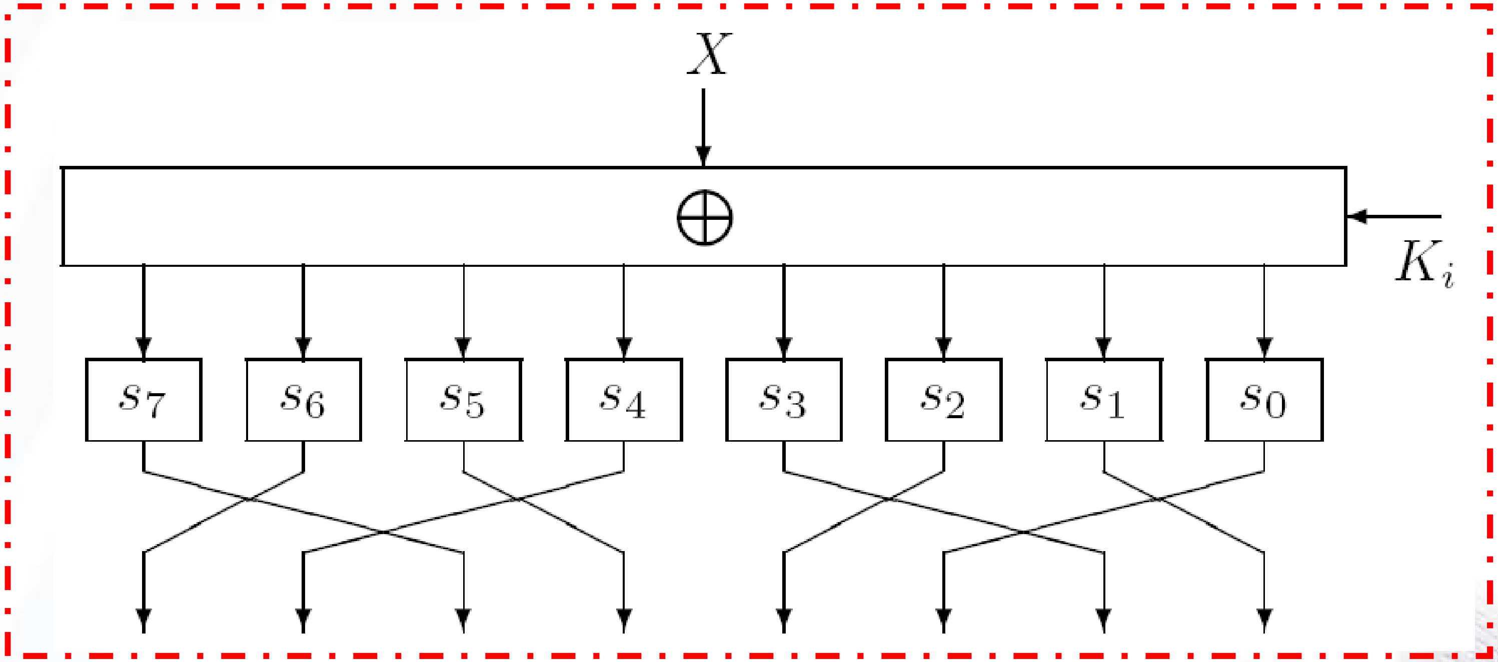


Fig. 1. Encryption procedure of LBlock

Specification of LBlock

⌘ Round function *F*

$$F: \{0,1\}^{32} \times \{0,1\}^{32} \longrightarrow \{0,1\}^{32}$$
$$(X, K_i) \longrightarrow U = P(S(X \oplus K_i))$$

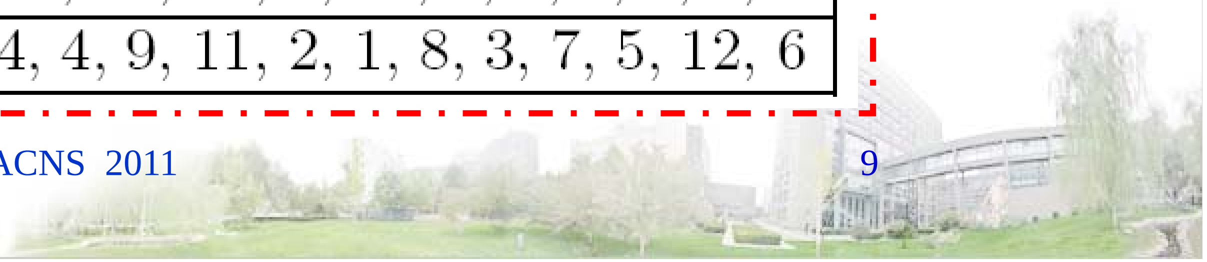


Specification of LBlock

⌘ Round function *F*

$$\begin{array}{rccc} F: & \{0,1\}^{32} \times \{0,1\}^{32} & \longrightarrow & \{0,1\}^{32} \\ & (X, K_i) & \longrightarrow & U = P(S(X \oplus K_i)) \end{array}$$

s_0	14, 9, 15, 0, 13, 4, 10, 11, 1, 2, 8, 3, 7, 6, 12, 5
s_1	4, 11, 14, 9, 15, 13, 0, 10, 7, 12, 5, 6, 2, 8, 1, 3
s_2	1, 14, 7, 12, 15, 13, 0, 6, 11, 5, 9, 3, 2, 4, 8, 10
s_3	7, 6, 8, 11, 0, 15, 3, 14, 9, 10, 12, 13, 5, 2, 4, 1
s_4	14, 5, 15, 0, 7, 2, 12, 13, 1, 8, 4, 9, 11, 10, 6, 3
s_5	2, 13, 11, 12, 15, 14, 0, 9, 7, 10, 6, 3, 1, 8, 4, 5
s_6	11, 9, 4, 14, 0, 15, 10, 13, 6, 12, 5, 7, 3, 8, 1, 2
s_7	13, 10, 15, 0, 14, 4, 9, 11, 2, 1, 8, 3, 7, 5, 12, 6



Specification of LBlock

⌘ Decryption

1. For $j = 31, 30, \ldots, 0$, do

$$X_j = (F(X_{j+1}, K_{j+1}) \oplus X_{j+2}) >>> 8$$

2. Output $M = X_1 || X_0$ as the 64-bit plaintext.

Specification of LBlock

⌘ Key Scheduling

- 80-bit master key K → 32-bit round subkey K_i (i=1,2,…,32)

k_{79}	k_{78}	k_{77}	k_{76}	…	…	k_{49}	k_{48}	k_{47}	k_{46}	…	…	k_3	k_2	k_1	k_0

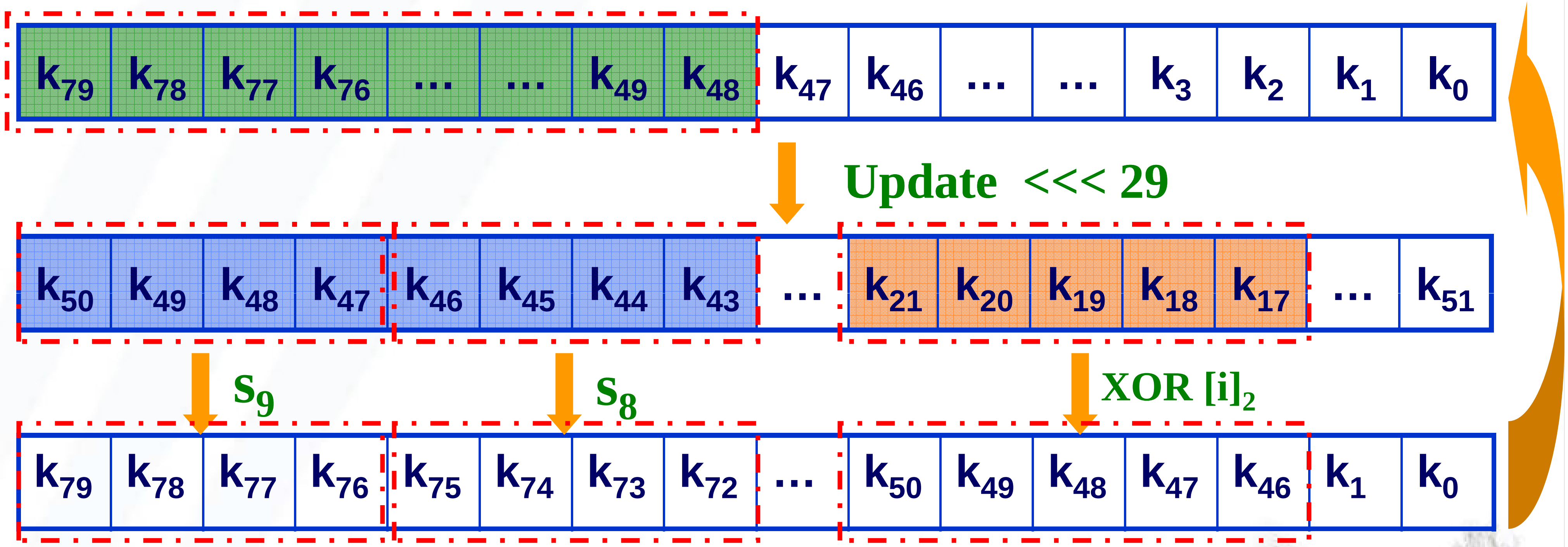
Update <<< 29

k_{50}	k_{49}	k_{48}	k_{47}	k_{46}	k_{45}	k_{44}	k_{43}	…	k_{21}	k_{20}	k_{19}	k_{18}	k_{17}	…	k_{51}

Specification of LBlock

⌘ Key Scheduling

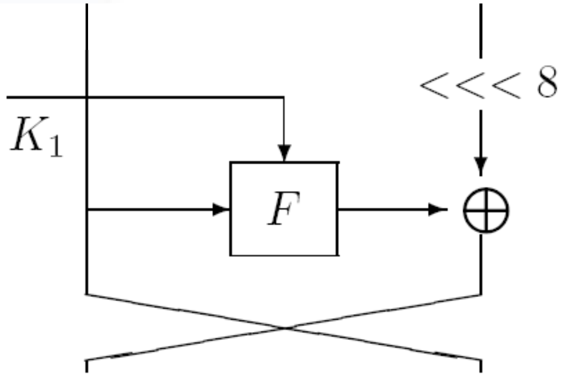
- 80-bit master key K → 32-bit round subkey K_i (i=1,2,…,32)



2. Design Rationale

⌘ Structure

- Variant Feistel Structure



- Main Features
  - Considerations about security and efficient implementation
  - Feistel-type structure suitable for lightweight environment
  - Choice of the rotation constant

Design Rationale

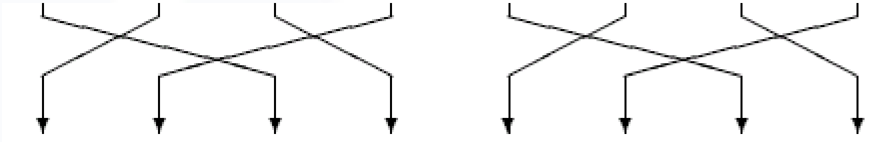
⌘ S-Box Layer

- Efficiency in hardware implementation
  - 4-bit s-boxes used, average require about 22 GE
- Security Property
  - best differential probability
  - best non linearity
  - no fix point
  - completed
  - good algebraic order
  - … …

Design Rationale

⌘ Diffusion P-Layer

- 4-bit word-wise permutation *P* in round function



- 8-bit left rotation in the right half
  - need no additional area cost in hardware implementation
  - also suitable for software environments with word-wise structure
  - their combination can guarantee both the best diffusion rounds and the number of active S-boxes

Design Rationale

⌘ Key Scheduling Part

- design in a stream cipher way
- choice of the rotation constant in update step
  - <<< 29 can break the 4-bit word structure and avoid weak relations between subkeys
- employ two 4-bit S-boxes as non-linear part
- choice of constants and position of constant addition

3. Security Evaluation

⌘ Differential/Linear Cryptanalysis

- ❖ Evaluate by counting the least number of active S-boxes

Table Guaranteed number of active S-boxes of LBlock

Rounds	DS	LS	Rounds	DS	LS
1	0	0	**11**	22	22
2	1	1	**12**	24	24
3	2	2	**13**	27	27
4	3	3	**14**	30	30
5	4	5	**15**	32	32
6	6	6	**16**	35	35
7	8	8	**17**	36	36
8	11	11	**18**	39	39
9	14	14	**19**	41	41
10	18	18	**20**	44	44

- ❖ Conclusion
  - ☞ there is no useful 15-round differential/linear characteristic for LBlock

Security Evaluation

⌘ Impossible Differential Cryptanalysis

- Best impossible differential characteristic: 14-round

1	$(00000000, 00\alpha00000) \overset{14r}{\nrightarrow} (0\beta000000, 00000000)$	9	$(00000000, 0000\alpha000) \overset{14r}{\nrightarrow} (\beta0000000, 00000000)$
2	$(00000000, 00\alpha00000) \overset{14r}{\nrightarrow} (\beta0000000, 00000000)$	10	$(00000000, 0000\alpha000) \overset{14r}{\nrightarrow} (00000\beta00, 00000000)$
3	$(00000000, 00\alpha00000) \overset{14r}{\nrightarrow} (00\beta00000, 00000000)$	11	$(00000000, 0000\alpha000) \overset{14r}{\nrightarrow} (0000000\beta, 00000000)$
4	$(00000000, 00\alpha00000) \overset{14r}{\nrightarrow} (0000\beta000, 00000000)$	12	$(00000000, 00000\alpha00) \overset{14r}{\nrightarrow} (\beta0000000, 00000000)$
5	$(00000000, 00\alpha00000) \overset{14r}{\nrightarrow} (000000\beta0, 00000000)$	13	$(00000000, 000000\alpha0) \overset{14r}{\nrightarrow} (0\beta000000, 00000000)$
6	$(00000000, 000\alpha0000) \overset{14r}{\nrightarrow} (0\beta000000, 00000000)$	14	$(00000000, 0000000\alpha) \overset{14r}{\nrightarrow} (0\beta000000, 00000000)$
7	$(00000000, 0000\alpha000) \overset{14r}{\nrightarrow} (0\beta000000, 00000000)$	15	$(00000000, \alpha0000000) \overset{14r}{\nrightarrow} (\beta0000000, 00000000)$
8	$(00000000, 0000\alpha000) \overset{14r}{\nrightarrow} (000\beta0000, 00000000)$	16	$(00000000, 0\alpha000000) \overset{14r}{\nrightarrow} (\beta0000000, 00000000)$

- Conclusion: key recovery attack can reach 20-round

Security Evaluation

⌘ Integral Attack

❖ Best integral characteristic: 15-round

Rounds	Integral characterisitcs			
0	$AAAC$	$AAAA$	$AAAA$	$AAAA$
1	$AAAC$	$ACAC$	$AAAC$	$AAAA$
2	$CCCC$	$AAAC$	$AAAC$	$ACAC$
3	$ACAC$	$CCCC$	$CCCC$	$AAAC$
4	$CCCC$	$ACCC$	$ACAC$	$CCCC$
5	$ACCC$	$CCCC$	$CCCC$	$ACCC$
6	$CCCC$	$CCCC$	$ACCC$	$CCCC$
7	$CCCC$	$CCAC$	$CCCC$	$CCCC$
8	$CCCC$	$CCCA$	$CCCC$	$CCAC$
9	$CCCC$	$AACC$	$CCCC$	$CCCA$
10	$CCCC$	$AAAC$	$CCCC$	$AACC$
11	$CCAA$	$ACAA$	$CCCC$	$AAAC$
12	$CAAB$	$AAAA$	$CCAA$	$ACAA$
13	$B?AA$	$BBAA$	$CAAB$	$AAAA$
14	$?B?B$	$?B?B$	$B?AA$	$BBAA$
15	$????$	$????$	$?B?B$	$?B?B$

❖ Conclusion: key recovery attack can reach 20-round

Security Evaluation

⌘ Related-Key Attacks

- Best related-key differential: 14-round with 32 active S-boxes

Table 14-Round related-key differential characteristic of LBlock

Rounds	ΔX_L	ΔRK	ΔI_S	ΔO_P	ΔX_R
1	01200101	00000000	01200101	20012100	01222121
2	02200001	00000000	02200001	20010100	01200101
3	00000001	02000000	02000001	20000100	02200001
4	00000002	00000000	00000002	00000100	00000001
5	00000000	00000008	00000008	00000200	00000002
6	00000000	00000000	00000000	00000000	00000000
7	00000000	00000000	00000000	00000000	00000000
8	00000000	00000400	00000400	00001000	00000000
9	00001000	00000000	00001000	00000010	00000000
10	00000010	00000000	00000010	00000002	00001000
11	00100002	00020000	00120002	01010100	00000010
12	01011100	00000000	01011100	21002010	00100002
13	31002210	00000000	31002210	20102012	01011100
14	21012013	04000000	25012013	41200212	31002210

4. Performance Evaluation

⌘ Hardware Evaluation: 1320 GE

Table Area requirement of LBlock

Module	Speed Optimized	Area Optimized
64-bit Data Register	384	192
Key Addition	87	87
S-box Layer	174.8	174.8
P Layer	0	0
32-bit XOR	87	87
80-bit Key Register	480	212
S-boxes (Key Scheule)	43.7	30
5-bit Constant XOR	13.5	13.5
Control Logic	50	70
Sum	1320 GE	866.3 GE (with RAM)

Conclusion

⌘ **LBlock**

- tries to achieve better hardware and software performance
- should achieve enough security margin against known attacks

In the end, we strongly encourage the security analysis of LBlock and various helpful comments

Contact Us

⌘ **Email:** wwl@is.iscas.ac.cn
zhanglei1015@is.iscas.ac.cn

Thank you for your attention !