Truncated Differential Analysis of Round-Reduced RoadRunneR Block Cipher

Qianqian Yang[1,2,3], Lei Hu[1,2,**], Siwei Sun[1,2], Ling Song[1,2]

[1]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
[3]University of Chinese Academy of Sciences, Beijing 100049, China
{qqyang13,hu,swsun,lsong}@is.ac.cn

Abstract. RoadRunneR is a small and fast bitslice lightweight block cipher for low cost 8-bit processors proposed by Adnan Baysal and Sähap Şahin in the LightSec 2015 conference. While most software efficient lightweight block ciphers lacking a security proof, RoadRunneR's security is provable against differential and linear attacks. RoadRunneR is a Feistel structure block cipher with 64-bit block size. RoadRunneR-80 is a vision with 80-bit key and 10 rounds, and RoadRunneR-128 is a vision with 128-bit key and 12 rounds. In this paper, we obtain 5-round truncated differentials of RoadRunneR-80 and RoadRunneR-128 with probability 2^{-56}. Using the truncated differentials, we give a truncated differential attack on 7-round RoadRunneR-128 without whitening keys with data complexity of 2^{55} chosen plaintexts, time complexity of 2^{121} encryptions and memory complexity of 2^{68}. This is first known attack on RoadRunneR block cipher.

Keywords: Lightweight, Block Cipher, RoadRunneR, Truncated Differential Cryptanalysis

1 Introduction

Recently, lightweight block ciphers, which could be widely used in small embedded devices such as RFIDs and sensor networks, are becoming more and more popular. Due to the strong demand from industry, a lot of lightweight block ciphers are proposed in recent years, such as PRESENT[4], LED[6], LBlock[8], PRINCE[5], and two lightweight block ciphers SIMON and SPECK[2], designed by the U.S. National Security Agency.

RoadRunneR[1] is a new lightweight block cipher which was recently proposed by Adnan Baysal and Sähap Şahin in the LightSec 2015 conference. It is a small and fast bitslice block cipher for low cost 8-bit processors. While there are many lightweight block ciphers with software efficient, most of them lack a security proof. The security of RoadRunneR is provable against differential

** The corresponding author.

and linear attacks. It is a Feistel-type block cipher with 64-bit block size and 80-bit or 128-bit key size. The vision of RoadRunneR-80 has 10 rounds and RoadRunneR-128 has 12 rounds.

Our Contribution. We get 5-round truncated differentials of RoadRunneR by the method proposed by Li *et al.* that they adopted the meet-in-the-meet technique to find the truncated differential of block ciphers. By adding two rounds after the truncated differential path, we launch a truncated differential attack on 7-round RoadRunneR-128 without whitening keys with data complexity of 2^{55} chosen plaintexts, time complexity of 2^{121} encryptions and memory complexity of 2^{68}.

Organization of this paper. In section 2, we give a brief description of the RoadRunneR block cipher. In section 3, we give the security margin of RoadRunneR against differential attack. In section 4, we obtain the 5-round truncated differentials of RoadRunneR and give a truncated differential attack on 7-round RoadRunneR-128. At last, we conclude this study.

2 Description of Block Cipher Khudra

2.1 Description of RoadRunneR Block Cipher

In this section, we briefly recall the design of the block cipher RoadRunneR and we refer the readers to [1] for more details.

Recently, there are many lightweight ciphers designed for better performance in hardware. But most software efficient lightweight ciphers either lack a security proof or have a low security margin. RoadRunneR is a small and fast bitslice block cipher for low cost 8-bit processors proposed by Adnan Baysal and Sühap Şahin. The designers of RoadRunneR have shown that the block cipher, which has a very low code size, is an efficient lightweight block cipher in 8-bit software and its security is provable against differential and linear attacks.

RoadRunneR is a block cipher based on the recursive Feistel structure, with 64-bit block size and 80-bit or 128-bit key sizes. The version of 80-bit key size needs 10 rounds and the other needs 12 rounds.

The F-function. The F-function is a 4-round SPN structure, and the detail is shown in Figure 1. The first three rounds have the same function called SLK, which is the consecutive application of S-box layer, diffusion layer and key addition, and the last round only has S-box layer. After the second SLK function, round constant is XORed to the least significant byte of the state. For round $i = 0, 1, ..., NR - 1$, the round constant is $C_i = NR - i$, where NR is the number of rounds. The 4-round SPN-like structure ensures high number of active S-boxes for an active F-function.

The S-box Layer. Recently, using bit-slice techniques becomes more and more popular. Block ciphers such as NOEKEON, SEA, PRIDE, and RECTANGLE all use bit-slice S-boxes with different S-box layer design strategies. There are advantages in both hardware and software implementations about the bit-slice S-box structure.

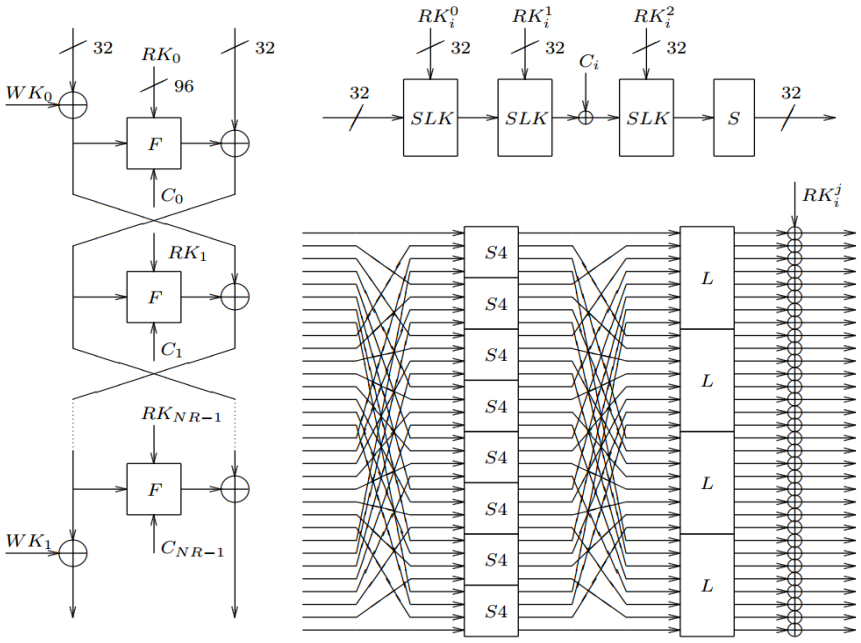

Fig. 1: Feistel Structure on left, F function on top right, and SLK function on bottom right.

In RoadRunneR, the designers adopted an efficient bit-slice S-box. The S-box is given in Table 1.

Table 1: S-box of RoadRunneR

x	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
S(x)	0x0	0x8	0x6	0xd	0x5	0xf	0x7	0xc	0x4	0xe	0x2	0x3	0x9	0x1	0xb	0xa

The Diffusion Layer. In RoadRunneR block cipher, the linear layer L is the form

$$L(x) = (x \lll i) \oplus (x \lll j) \oplus (x \lll k),$$

where $x \lll i$ represents $i-$bit left rotation of the word x. This form of L guarantees linear layers are invertible and all have branch number 4. In Table 2 showed the best linear functions . Since L_1 provides good diffusion and performance, the designers chose L_1 as the diffusion layer matrix.

Table 2: Best L Matrices

Matrix	i, j, k	# Instrctions (for two matrix mult)	# Minimum Active S-boxes in F
L_1	0,1,2	13	10
L_2	0,1,4	11	8
L_3	0,1,5	11	8
L_4	0,4,5	11	8
L_5	1,4,5	11	8

The Key Schedules. RoadRunneR has RoadRunneR-80 and RoadRunneR-128 two vision which take 80-bit and 128-bit keys respectively. For two vision, the key scheduling part generates 96-bit round keys with the same method. The initial whitening key starts from the beginning of the master key. Then for the round keys, when a new 32-bit of key material is required, the key schedule generates a 32-bit from the master key in a circular way. At last, the final whitening key is generated by the same way. The detail round keys used in RoadRunneR-80 and RoadRunneR-128 are given in Table 3.

3 Security Analysis of RoadRuuneR against Differential Attack

In this section we implement the technique proposed by Sun *et al.* to find the differential characteristic with the maximal probability. We have computed the minimum number of active S-boxes in differential characteristics, which give

Table 3: Key Schedules of RoadRunneR

80-bit Key Schedule Master Key:$A\|B\|C\|D\|E$		**128-bit Key Schedule** Master Key=$A\|B\|C\|D$	
Initial Whitening=$A\|B$		Initial Whitening:A	
Rounds	Key Words	Rounds	Key Words
0,5	$(C\|D)-(E\|A)-(B\|C)$	0,4,8	$B-C-D$
1,6	$(D\|E)-(A\|B)-(C\|D)$	1,5,9	$A-B-C$
2,7	$(E\|A)-(B\|C)-(D\|E)$	2,6,10	$D-A-B$
3,8	$(A\|B)-(C\|D)-(E\|A)$	3,7,11	$C-D-A$
4,9	$(B\|C)-(D\|E)-(A\|B)$		
Final Whitening:$C\|D$		Final Whitening:B	

Table 4: Minimum number of active S-boxes

No. of Rounds	4	5	6
Min.# Act. S-boxes	26	36	48

the same accurate measurement for the resistance of RoadRunneR block cipher against differential cryptanalysis.

Table 4 shows that the block cipher RoadRunneR is as secure as the designers claimed in. Because the highest probability is at most 2^{-72} which is smaller than 2^{-64}, there is no useful differential characteristic in 5 or more rounds of RoadRunneR.

4 Truncated Differential Attack on RoadRunneR Block Cipher

In this section, we describe our truncated differential attack on the 7-round RoadRunneR-128 without whitening key. At first, we obtain the the high probabilities truncated differential characteristics by using the method proposed by Li *et al.*[7]. Then we give the truncated differential attack on RoadRunneR-128 in detail.

Notations. We denote the round function of RoadRunneR as F and use ΔF^I and ΔF^O to denote the input difference and the output difference of the function F. The input of the round i is denoted by L_{i-1} and R_{i-1}. Similarly, the input difference of round i is denoted by ΔL_{i-1} and ΔR_{i-1}. With two branches, each of these blocks has $n/2 = 32$ bits.

4.1 Meet-in-the-Middle Technique for Truncated Differential

In[7], Li *et al.* implemented the meet-in-the-middle technique to propose a method to find the truncated differential of block ciphers.

Definition 1 *[3] For the block cipher E with a parameter key K, the truncated differential characteristic $(\Gamma_{in} \xrightarrow{E} \Gamma_{out})$ is a set of differential trails, where Γ_{in} is a set of input differences, and Γ_{out} is a set of output differences. The expected probability of such truncated differential $(\Gamma_{in} \xrightarrow{E} \Gamma_{out})$ is defined by*

$$\begin{aligned} Pr(\Gamma_{in} \xrightarrow{E} \Gamma_{out}) =& \frac{1}{\Gamma_{in}} \sum_{a \in \Gamma_{in}} Pr((E_K(X) \oplus E_K(X \oplus a)) \in \Gamma_{out}) \\ =& \frac{1}{\Gamma_{in}} \sum_{a \in \Gamma_{in}} Pr(a \to \Gamma_{out}). \end{aligned} \tag{1}$$

Propositon 1 *[7] For the block cipher $E = E_1 \circ E_0$, there are two truncated differential characteristics with high probability, i.e., $Pr(\Gamma_0 \xrightarrow{E_0} \Gamma_1) = p$, and $Pr(\Gamma_2 \xrightarrow{E_1^{-1}} \Gamma_1) = 1$, where Γ_0 is the input difference set of E, and Γ_1 and Γ_2 are the output difference sets of E_0 and E, respectively. Then the probability of the truncated differential $\Gamma_0 \xrightarrow{E} \Gamma_2$ is $p \times \frac{|\Gamma_2|}{|\Gamma_1|}$, where $|\Gamma_2| \leq |\Gamma_1|$.*

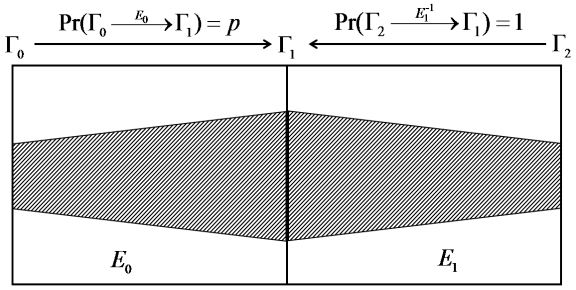

Fig. 2: Meet-in-the-Middle Technique for Truncated Differential

4.2 Truncated Differentials of RoadRunneR

Propositon 2 *Let the input difference of the F-function is $\Delta F^I = (0\cdots0*, 0\cdots0*, 0\cdots0*, 0\cdots0*)$, then after the F-function, the output difference is $\Delta F^O = (0*\cdots*, 0*\cdots*, 0*\cdots*, 0*\cdots*)$ with probability 1.*

Proof. The F-function is a 4-round SPN structure. We call the three SLK function as f_1, f_2, and f_3. With the input difference of the F-function is $\Delta F^I = (0\cdots0*, 0\cdots\ 0*, 0\cdots0*, 0\cdots0*)$, there is one active S-box in f_1. Since the linear layer is $L(x) = (x \lll 0) \oplus (x \lll 1) \oplus (x \lll 2)$, after f_1 the output difference is $f_1^O = (0\cdots0**, 0\cdots\ 0**, 0\cdots0**, 0\cdots0**)$ with probability 1.

Similarly, after f_2 the output difference is $f_2^O = (000****, 000****, 000****, 000****)$ and after f_3 the output difference is $f_3^O = (0*$

$\cdots *, 0*\cdots *, 0*\cdots *, 0*\cdots *)$. Because of the property of S-layer, there is no diffusion of active S-boxes. Thus after the F-function, the output difference is $\Delta F^O = (0*\cdots *, 0*\cdots *, 0*\cdots *, 0*\cdots *)$ with probability 1.

From Proposition 2, we obtain the following proposition.

Propositon 3 *Let the input difference be* $\Delta L_0 = (\Delta L_{00}, \Delta L_{01}, \Delta L_{02}, \Delta L_{03}) = (\boldsymbol{0}, \boldsymbol{0}, \boldsymbol{0}, \boldsymbol{0}), \Delta R_0 = (\Delta R_{00}, \Delta R_{01}, \Delta R_{02}, \Delta R_{03}), \Delta R_{00} = \Delta R_{01} = \Delta R_{02} = \Delta R_{03} = (0\cdots 0*)$*, then after a 5-round encryption of RoadRunneR, the probability of the output difference satisfying* $\Delta L_4 = (\Delta L_{40}, \Delta L_{41}, \Delta L_{42}, \Delta L_{43}) = (\boldsymbol{0}, \boldsymbol{0}, \boldsymbol{0}, \boldsymbol{0}), \Delta R_4 = (\Delta R_{40}, \Delta R_{41}, \Delta R_{42}, \Delta R_{43}), \Delta R_{40} = \Delta R_{41} = \Delta R_{42} = \Delta R_{43} = (0\cdots 0*)$ *is about* 2^{-56}.

Proof. We define the 5-round RoadRunneR as E with the first three rounds defined as E_0 and the last two rounds defined as E_1. Since the input differences

$$\begin{aligned}\Gamma_0 =&(\Delta L_0, \Delta R_0)\\ =&((\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}), (0\cdots 0*, 0\cdots 0*, 0\cdots 0*, 0\cdots 0*))\end{aligned}$$

the output differences after 3-round encryption satisfy

$$\begin{aligned}\Gamma_1 =&(\Delta L_3, \Delta R_3)\\ =&((0\cdots 0*, 0\cdots 0*, 0\cdots 0*, 0\cdots 0*), (0*\cdots *, 0*\cdots *, 0*\cdots *, 0*\cdots *))\end{aligned}$$

with probability 2^{-28}.

Similarly, for the differences

$$\begin{aligned}\Gamma_2 =&(\Delta L_5, \Delta R_5)\\ =&((0\cdots 0*, 0\cdots 0*, 0\cdots 0*, 0\cdots 0*), (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}))\end{aligned}$$

the corresponding output differences after two rounds decryption coincide to

$$\begin{aligned}\Gamma_1 =&(\Delta L_3, \Delta R_3)\\ =&((0\cdots 0*, 0\cdots 0*, 0\cdots 0*, 0\cdots 0*), (0*\cdots *, 0*\cdots *, 0*\cdots *, 0*\cdots *))\end{aligned}$$

with probability 1. By the Proposition 2, the probability of 5-round truncated differential is

$$Pr(\Gamma_0 \xrightarrow{E} \Gamma_2) = 2^{-28} \times 2^4/2^{32} = 2^{-56}.$$

By the Definition 1, we know that the uniform probability of the truncated differential characteristic is $Pr(\Gamma_0 \xrightarrow{E} \Gamma_2) = \frac{|\Gamma_2|}{2^{64}-1} = \frac{2^4}{2^{64}-1} = 2^{-60}$.

For both RoadRunneR-80 and RoadRunneR-128, there are truncated differentials with probability 2^{-56}.

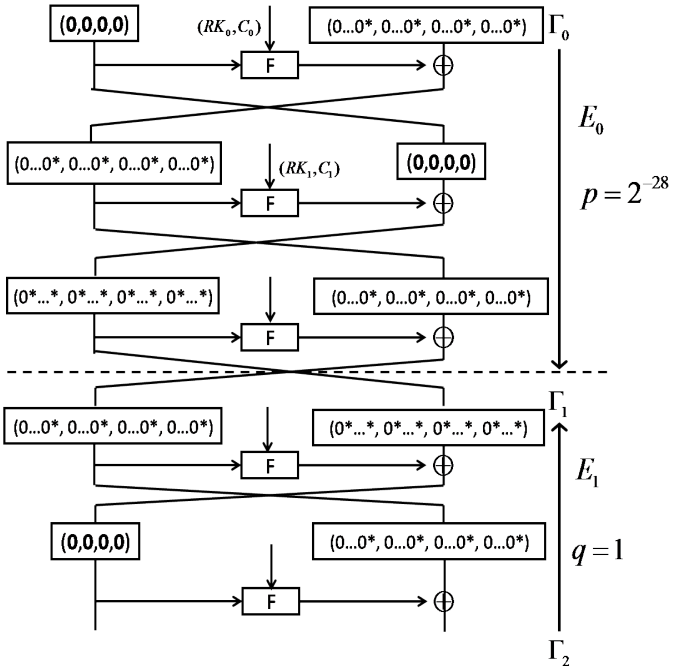

Fig. 3: The Truncated Differential of 5-round RoadRunneR

4.3 The Truncated Differential Attack on 7-Round RoadRunneR-128

With the 5-round truncated differentials on 1-5 round, we are able to extend this truncated differentials path by adding two rounds to the output and attack 7-round RoadRunneR-128.

Data Collection Phase. By expanding two rounds after the 5-round truncated differential path, we deduce the input difference is

$$\Delta P = (\Delta L_0, \Delta R_0) = ((\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}), (0 \cdots 0*, 0 \cdots 0*, 0 \cdots 0*, 0 \cdots 0*))$$

and the ciphertexts difference is

$$\begin{aligned}\Delta C =&(\Delta L_7, \Delta R_7)\\ =&((0 * \cdots *, 0 * \cdots *, 0 * \cdots *, 0 * \cdots *), (* \cdots *, * \cdots *, * \cdots *, * \cdots *)).\end{aligned}$$

We construct N_s structures of plaintexts with 4 bits fixed, which are active, and other bits traversed. For one structure, there are 2^7 plaintexts satisfying the input difference. Satisfying the output difference $\Delta C = ((0 * \cdots *, 0 * \cdots *, 0 * \cdots *, 0 * \cdots *), (* \cdots *, * \cdots *, * \cdots *, * \cdots *))$, there are $2^{N_s} \times 2^7 \times 2^{-4} = 2^{N_s+3}$ pairs left.

Key Recovery Phase.

-Step 1. Guess 68-bit subkey of $D||A$ and 4 bits of B, do the following steps for every pair.

- **(a)** In the 7-th round, by knowing the values of C_L and $D||A$, we calculate the input differences of S-boxes. Then we get 28-bit subkey of B by the input and output differences of S-boxes.
- **(b)** In the 6-th round, knowing the value of $A||B$ and the input values of F-function we calculate the input difference of the last S-box layer. Knowing the input difference and output difference of the last S-box layer, get 28-bit subkey of C.
- **(c)** Choose the subkey whose count is the largest as the candidate of right key.

-Step 2. Ultimately, for each survived candidate in Step 1, we compute the seed key by doing an exhaustive search for other 4 bits.

Complexity Analysis.

-*Data Complexity.* In our work, we choose $N_s = 51$, the expected count of the right key is $2^{-56} \times 2^{51} \times 2^7 = 4$. The data complexity is $2^{51} \times 2^4 = 2^{55}$.

-*Time Complexity.* We analyze the time complexity in each step to get the time complexity. In the data collection phase, the time complexity is 2^{55} 7-round encryptions. In step 1, we need $2^{N_s+3} = 2^{54}$ pairs chosen plaintexts, which cost $2^{54} \times 2 \times 2/7 \times 2^{68} = 2^{121}$ encryptions. In step 2 for the exhaustive searching, the time complexity is $2^{68} \times 2^4 \times 1 = 2^{72}$ encryptions. Therefore, the total time complexity is 2^{121} encryptions.

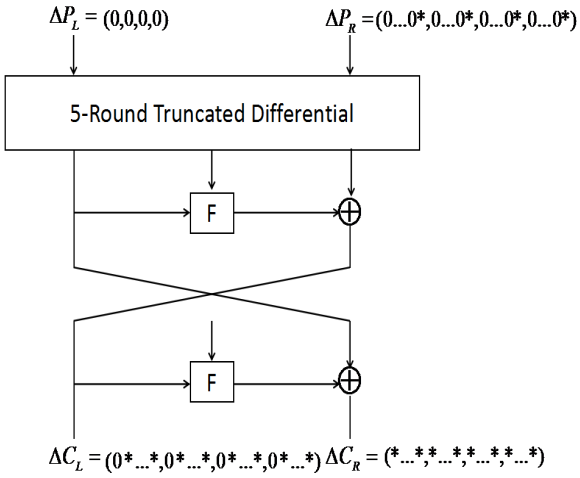

Fig. 4: The Truncated Differential Attack on 7-round RoadRunneR-128

-*Memory Complexity.* For storing the counter of 58-bit subkey, the memory complexity is 2^{58}. For storing the right keys with high probability, the memory complexity is 2^{68}. Thus the memory complexity is 2^{68}.

In summary, we propose an attack on 7-round RoadRunneR-128 with the data, time and memory complexities are $2^{55}, 2^{121}$ and 2^{68}, respectively.

5 Conclusion

In this paper, we obtain 5-round truncated differentials of RoadRunneR-80 and RoadRunneR-128 by using the meet-in-the-middle like technique. Using the truncated differentials, we propose a truncated differential attack on 7-round RoadRunneR-128 without whitening keys by extending 2 rounds backward, with a data complexity of 2^{55} chosen plaintexts, a time complexity of 2^{121} encryptions and a memory complexity of 2^{68}.

References

1. Baysal, A., Sahin, S.: Roadrunner: A small and fast bitslice block cipher for low cost 8-bit processors. Tech. rep., IACR Cryptology ePrint Archive, 2015: 906 (2015)
2. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive (2013), `https://eprint.iacr.org/2013/404`
3. Blondeau, C.: Improbable differential from impossible differential: On the validity of the model. In: Progress in Cryptology–INDOCRYPT 2013, pp. 149–160. Springer (2013)

4. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Cryptographic Hardware and Embedded Systems - CHES 2007. pp. 450–466. Springer (2007)
5. Borghoff, J., Canteaut, A., Gneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., n, T.Y.: PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications. In: Advances in Cryptology - ASIACRYPT 2012. pp. 208–225. Springer (2012)
6. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED Block Cipher. In: Cryptographic Hardware and Embedded Systems - CHES 2011. pp. 326–341. Springer (2011)
7. Li, L., Jia, K., Wang, X., Dong, X.: Meet-in-the-middle technique for truncated differential and its applications to clefia and camellia. In: Fast Software Encryption. pp. 48–70. Springer (2015)
8. Wu, W., Zhang, L.: LBlock: A Lightweight Block Cipher. In: Applied Cryptography and Network Security - ACNS 2011. pp. 327–344. Springer (2011)