Related-key Impossible Boomerang Cryptanalysis on LBlock-s

Min Xie*, Qiya Zeng

State Key Laboratory of Integrated Service Networks, Xidian University

Xi'an 710071, China

[e-mail: mxie@xidian.edu.cn, m15686247918@163.com]

*Corresponding author: Min Xie

Received March 26, 2018; revised April 2, 2019; accepted May 3, 2019; published November 30, 2019

Abstract

LBlock-s is the core block cipher of authentication encryption algorithm LAC, which uses the same structure of LBlock and an improved key schedule algorithm with better diffusion property. Using the differential properties of the key schedule algorithm and the cryptanalytic technique which combines impossible boomerang attacks with related-key attacks, a 15-round related-key impossible boomerang distinguisher is constructed for the first time. Based on the distinguisher, an attack on 22-round LBlock-s is proposed by adding 4 rounds on the top and 3 rounds at the bottom. The time complexity is about only $2^{68.76}$ 22-round encryptions and the data complexity is about 2^{58} chosen plaintexts. Compared with published cryptanalysis results on LBlock-s, there has been a sharp decrease in time complexity and an ideal data complexity.

Keywords: LBlock-s, lightweight block cipher, related-key, impossible differential, boomerang cryptanalysis

This research was supported in part by the National Key Research and Development Program of China (Grant No. 2016YFB0800601) and Key Program of NSFC-Tongyong Union Foundation (Grant No. U1636209).

http://doi.org/10.3837/tiis.2019.11.024 **ISSN : 1976-7277**

1. Introduction

With the rapid development of electronic information technology and the widespread application of technologies such as RFID (Radio Frequency Identification), traditional block ciphers are not suitable for resource constrained environments. Therefore, lightweight block ciphers which are designed with a trade-off between the security and hardware performance for resource constrained environments have become a hot topic.

As the kernel block cipher of LAC submitted to CAESAR competition [1], LBlock-s is an improved version of LBlock [2] which is proposed by Wu et al. in ACNS 2011. Similar to LBlock, it uses a variant of Feistel structure and consists of 32 rounds. The block length and the key length are 64-bit and 80-bit, respectively. What LBlock-s differs from LBlock is that LBlock-s employs an improved key schedule algorithm with a faster diffusion speed and replaces 10 different S-boxes in LBlock with 10 identical S-boxes to reduce hardware and software costs. In terms of security, Shan et al. [3] showed that there were at least 32 active boxes in the 32-round related-key differential characteristic, that is, the probability must not be higher than 2^{-64}, and they gave a 10-round and an 11-round related-key differential characteristics. Xiao [4] used differential cryptanalysis to give a 16-round differential path. Li et al. [5] mounted a 23-round attack on LBlock-s with improved multidimensional zero-correlation linear cryptanalysis. Using the 14-round impossible differential characteristic of LBlock which was given by the designers of LBlock, Jia [6] carried out a 21-round attack on LBlock-s. They gave the results on 22-round and 23-round attacks without the detailed analysis. And the results showed that the time complexity of 22-round attack was $2^{78.86}$ 22-round encryptions, which is close to the one in exhaustive search and much higher than the corresponding attack result in this paper.

Related-key cryptanalysis was independently introduced by Knudsen [7] and Biham [8] respectively. The basic idea of the technique is that the attackers find weaknesses of the key schedule algorithm to choose appropriate relation between keys and then predict the encryptions under these keys. Impossible differential cryptanalysis was proposed by Knudsen [9] and further by Biham against Skipjack [10], in which the attackers try to find a differential characteristic with a probability of 0 to eliminate the wrong keys and then to recover the correct key. Related-key cryptanalysis and impossible differential cryptanalysis are both very powerful techniques for analyzing the security of a wide variety of block ciphers, and there are many satisfactory attack results on a lot of block ciphers such as Hummingbird-2, TEA, LBlock , MIBS and so on [11-17]. Boomerang cryptanalysis was presented by Wagner in 1999 [18], which is a variant of differential cryptanalysis. The basic idea of boomerang cryptanalysis is to use short differential characteristics with relatively large probabilities to form long differential characteristics with high probability. Related-key impossible boomerang cryptanalysis [19] is obtained by using these three attacks in combination. Until now, many satisfying analysis results are obtained on AES and LBlock by

using this cryptanalytic technique [19-20].

In this paper, we study the security of LBlock-s from the aspect of related-key impossible boomerang cryptanalysis for the first time. Through analyzing the property of round function and key schedule function of LBlock-s, a 15-round related-key impossible boomerang distinguisher is carried out, and we get a 22-round related-key impossible boomerang characteristic to recover 68-bit key with time complexity of $2^{68.76}$ and 2^{58} chosen plaintexts. Up to now, this is the best attack result on 22-round LBlock-s.

Outline. In Section 2, a description of LBlock-s and some notations used in this paper are given. In Section 3, we study the related-key impossible boomerang cryptanalysis. In Section 4, a 15-round related-key impossible boomerang distinguisher and attack on 22-round LBlock-s are described, followed by conclusion in Section 5.

2. Description of LBlock-s

2.1 Notations

The following notations are used in this paper.

P, C: the 64-bit plaintext and the 64-bit ciphertext;

K, ΔK: the 80-bit master key and the difference of K;

K_i, ΔK_i: the i-th round subkey and the difference of K_i;

K_i^j, ΔK_i^j: the j-th nibble of K_i and the j-th nibble of ΔK_i;

X_i, ΔX_i: the left half of the i-th round input and the difference of X_i;

X_0: the right half of the first round input;

X_i^j, ΔX_i^j: the j-th nibble of X_i and the j-th nibble of ΔX_i;

$X_i||X_j$: the concatenation of X_i and X_j;

$X<<< i$: a left rotation of X by i bits;

$X>>> i$: a right rotation of X by i bits;

$[i]_2$: the binary form of an integer i.

2.2 Overview of LBlock-s

LBlock-s is an improved version of LBlock with a variant of Feistel structure. It consists of 32-round iterative, with the block length 64-bit and the master key length 80-bit. The encryption procedure is as follows, and the general structure is illustrated in **Fig. 1**.

1. Input $P = X_1||X_0$;
2. For $i = 2,3,\cdots 33$, do the following calculation:
$$X_i = F(X_{i-1}, K_{i-1}) \oplus (X_{i-2} <<< 8);$$
3. Output $C = X_{33}||X_{32}$;

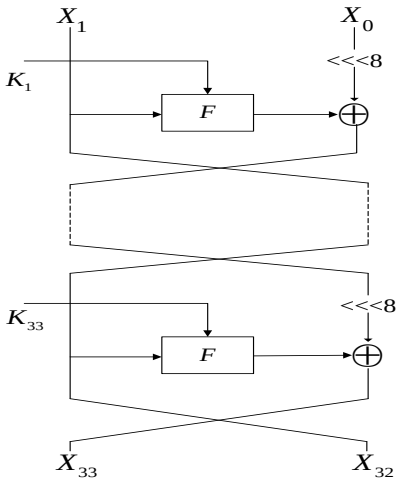

Fig. 1. Structure of LBlock-s

The round function F is defined as $F(X_i, K_i) = P(S(X_i \oplus K_i))$ (see **Fig. 2**), which includes three basic functions: key-addition layer, nonlinear transformation and linear diffusion function. The confusion function S includes 8 identical 4-bit S-boxes in parallel which is the first S-box used in LBlock (see **Table 1**, in hexadecimal notation), and the function P is a 4-bit word-wise permutation illustrated in **Fig. 2** in detail.

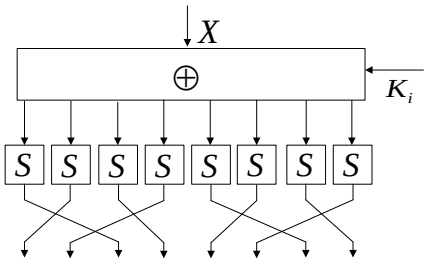

Fig. 2. Round function F

Table 1. Contents of the S-box

i	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(i)$	E	9	F	0	D	4	A	B	1	2	8	3	7	6	C	5

The decryption algorithm of LBlock-s is the inverse of the encryption algorithm. Thus, here is only a brief description: Let $\mathrm{C} = X_{32}||X_{33}$ denote the ciphertext. For $i = 31,30,\cdots 1,0$, do the calculation: $X_i = F(X_{i+1}, K_{i+1}) \oplus (X_{i+2} >>> 8)$. Finally, output $\mathrm{P} = X_1||X_0$ as the plaintext.

2.3 Key Schedule Algorithm

LBlock-s uses an improved key schedule algorithm with better diffusion property against

biclique cryptanalysis. The key schedule of LBlock-s updates 16 bits each time, and these updated bits are affected by 32 bits of the key register. In contrast, the original key schedule only updates 13 bits based on 13 bits of the key register. The master key $K = (k_{79}k_{78}\cdots k_1k_0)$ is stored in the key register. Output the leftmost 32 bits as the subkey K_1. For $i = 1,2,\cdots,31$, update the key register as follows:

1. $K <<< 24$;
2. $[k_{55}k_{54}k_{53}k_{52}] = S[k_{79}k_{78}k_{77}k_{76}] \oplus [k_{55}k_{54}k_{53}k_{52}]$,
   $[k_{31}k_{30}k_{29}k_{28}] = S[k_{75}k_{74}k_{73}k_{72}] \oplus [k_{31}k_{30}k_{29}k_{28}]$,
   $[k_{67}k_{66}k_{65}k_{64}] = [k_{71}k_{70}k_{69}k_{68}] \oplus [k_{67}k_{66}k_{65}k_{64}]$,
   $[k_{51}k_{50}k_{49}k_{48}] = [k_{11}k_{10}k_9k_8] \oplus [k_{51}k_{50}k_{49}k_{48}]$;
3. $[k_{54}k_{53}k_{52}k_{51}k_{50}] = [k_{54}k_{53}k_{52}k_{51}k_{50}] \oplus [i]_2$;
4. Output the leftmost 32-bit of the register *K* as round subkey K_{i+1}.

Where the S-box is the same as the S-box used in encryption algorithm.

3. The Related-key Impossible Boomerang Cryptanalysis

Related-key impossible boomerang cryptanalysis involves related-key cryptanalysis, impossible differential cryptanalysis and boomerang cryptanalysis. As depicted in **Fig. 3**, this technique treats a cipher *E* as two sub-ciphers E_0 and E_1, namely $E = E_0 \circ E_1$. Typically, each sub-cipher consists of two related-key differential characteristics with probability 1. They are shown as following:

- $\Delta\alpha \to \Delta\beta$ is the first related-key differential characteristic for E_0;
- $\Delta\alpha' \to \Delta\beta'$ is the second related-key differential characteristic for E_0;
- $\Delta\delta \to \Delta\gamma$ is the first related-key differential characteristic for E_1^{-1};
- $\Delta\delta' \to \Delta\gamma'$ is the second related-key differential characteristic for E_1^{-1},

where $\alpha, \alpha', \beta, \beta', \delta, \delta', \gamma$ and γ' are n-bit blocks. The corresponding keys used in the four characteristics are K_A, K_B, K_C and K_D. When β, β', γ and γ' meet the condition $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$, a related-key impossible boomerang distinguisher is constructed. Then an attack could be mounted by adding rounds at the top and at the bottom. Using the extended parts to guess the keys, we can eliminate the keys which satisfy the whole characteristics until only the correct key is left.

Related-key impossible boomerang cryptanalysis takes full advantage of the three cryptanalysis methods. In this attack, instead of using a single key differential characteristic with a large probability for *E*, attackers need to find four key differential characteristics and the master key differences are $K_A \oplus K_B = \Delta K_\alpha$, $K_C \oplus K_D = \Delta K_{\alpha'}$ and $K_A \oplus K_C = \Delta K_\beta$, $K_B \oplus K_D = \Delta K_{\beta'}$ for E_0 and E_1 respectively, which are not necessarily related. In other words, for any possible key difference selected for E_0, the various key differences for E_1 can be chosen. Thus related-key impossible boomerang cryptanalysis is more conducive to find related-key differential characteristics for ciphers with key schedule algorithm with

better diffusion property, compared with the related-key impossible differential cryptanalysis.

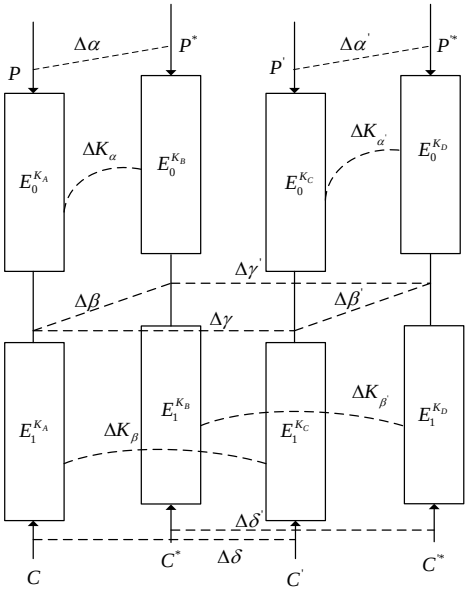

Fig. 3. Related-key impossible boomerang distinguisher

4. Related-key Impossible Boomerang Cryptanalysis on LBlock-s

This section describes the related-key impossible boomerang attack on LBlock-s in detail. In the rest of the paper, "*" is used to denote a non-zero 4-bit nibble whereas "?" is used to denote a 4-bit nibble that can assume any value. By analyzing the structure and round function of LBlock-s, we take a 15-round related-key impossible boomerang distinguisher: ((00000000,00000000),(00000000,00000000))↛((00000*00,00000000),(*0000000,00000000)) with the key differences $\Delta K_\alpha = \Delta K_{\alpha'} =$ (11000000000000000000) and $\Delta K_\beta = \Delta K_{\beta'} =$ (00000000000000000000). By extending 4 rounds at the top and 3 rounds at the bottom of this distinguisher, an attack on 22-round LBlock-s is achieved.

4.1 15-round related-key impossible boomerang distinguisher

Through an in-depth study on the key schedule algorithm of LBlock-s, we found that if there is no non-zero difference passing through S-boxes, two zero key differences followed one non-zero key difference will appear for some master key differences. To decrease the number of active S-boxes, we select the key differences $\Delta K_\alpha = \Delta K_{\alpha'} =$ (11000000000 00000000) to construct low-weight key differential characteristics. Subkey differences for round 1 to 13 generated by ΔK_α are shown in **Table 2**. Since the key schedule algorithm has a faster diffusion, we choose the other key differences $\Delta K_\beta = \Delta K_{\beta'} =$ (00000000000 00000000) to increase the number of rounds for the attack. That is, we construct a related-key impossible

boomerang distinguisher such that $K_A = K_C$ and $K_B = K_D$, which means that the distinguisher involves two keys.

Table 2. Subkey differences for round 1 to 13

ΔK_α	11000000000000000000
ΔK_1	11000000
ΔK_2	00000000
ΔK_3	00000000
ΔK_4	00100000
ΔK_5	00000000
ΔK_6	00000000
ΔK_7	00001000
ΔK_8	00000000
ΔK_9	00000000
ΔK_{10}	00000010
ΔK_{11}	100000*0
ΔK_{12}	*00000*0
ΔK_{13}	*00000*0

Combined with the selected key differences, we carefully choose the input differences and output differences. Let the input differences of $\Delta\alpha \to \Delta\beta$ and $\Delta\alpha' \to \Delta\beta'$ for E_0 be both (00000000,00000000), then non-zero difference diffusion will not happen in the fifth and sixth round. While letting the first output difference for E_1 be (00000*00,00000000), and the second output difference for E_1 be (*0000000,00000000), then the positions of some non-zero nibbles for the related-key differential characteristic $\Delta\delta \to \Delta\gamma$ will be the same as that for the other related-key differential characteristics $\Delta\delta' \to \Delta\gamma'$ in the same round, which makes more quartets be filtered in each step for subkey-recovery.

In this attack, E denotes the 15-round related-key impossible boomerang distinguisher of LBlock-s, E_0 denotes round 5 to 13, and E_1 denotes round 14 to 19.

Theorem 1. Let the two related-key differential characteristics $\Delta\alpha \to \Delta\beta$ and $\Delta\alpha' \to \Delta\beta'$ for E_0 be both (00000000,00000000)→(????????,0*????*?) with the key differences $\Delta K_\alpha = \Delta K_{\alpha'} =$ (11000000000000000000), the first related-key differential characteristic $\Delta\delta \to \Delta\gamma$ for E_1^{-1} be (00000*00,00000000)→(0***0*0*,0**?****) with the key difference $\Delta K_\beta =$ (00000000000000000000), and the second related-key differential characteristic $\Delta\delta' \to \Delta\gamma'$ for E_1^{-1} be (*0000000,00000000) → (*0*0*0**,*?****0*0) with the key difference $\Delta K_{\beta'} =$ (00000000000000000000). Then the four differential characteristics constitute a 15-round related-key impossible boomerang distinguisher for LBlock-s.

The detailed related-key differential characteristics for E_0 and E_1^{-1} are shown in **Table 3** and **Table 4** respectively.

Proof. From the direction of encryption, ΔX_{13}^7 in $\Delta\alpha \to \Delta\beta$ and $\Delta\alpha' \to \Delta\beta'$ are both 0. As for the direction of decryption, ΔX_{13}^7 in the first related-key differential $\Delta\delta \to \Delta\gamma$ is 0, but in the second related-key differential $\Delta\delta' \to \Delta\gamma'$is *. Obviously, $0\oplus0\oplus0\oplus*=*$, which is not equal to 0. Thus, there is a conflict when these four related-key differential characteristics meet in the middle, which satisfy the principle of related-key impossible boomerang cryptanalysis.

Table 3. Related-key differential characteristic for E_0

Round	ΔX_i	ΔX_{i-1}	ΔK_i
5	00000000	00000000	00000000
6	00000000	00000000	00000000
7	00000000	00000000	00001000
8	000000*0	00000000	00000000
9	0000000*	000000*0	00000000
10	0000**00	0000000*	00000010
11	0000****	0000**00	100000*0
12	00?****?	0000****	*00000*0
13	0*????*?	00?****?	*00000*0
14	????????	0*????*?	00000000

Table 4. Related-key differential characteristic for E_1^{-1} when ΔX_{20}^2= * and ΔX_{20}^7= *

Round	ΔX_{20}^2= *			ΔX_{20}^7= *		
	ΔX_i	ΔX_{i-1}	ΔK_{i-1}	ΔX_i	ΔX_{i-1}	ΔK_{i-1}
20	00000*00	00000000	00000000	*0000000	00000000	00000000
19	00000000	0000000*	00000000	00000000	00*00000	00000000
18	0000000*	0000000*	00000000	00*00000	00000*00	00000000
17	0000000*	0*00000*	00000000	00000*00	0000*0*0	00000000
16	0*00000*	0**0000*	00000000	0000*0*0	**00000*	00000000
15	0**0000*	0***0*0*	00000000	**00000*	*0*0*0**	00000000
14	0***0*0*	0**?****	*00000*0	*0*0*0**	*?****0*	*00000*0

Therefore, the four related-key differential characteristics described above constitute an 15-round related-key impossible boomerang distinguisher for LBlock-s: ((00000000,00000000),(00000000,00000000))↛((00000*00,00000000),(*0000000,00000000)) with the key differences $\Delta K_\alpha = \Delta K_{\alpha'} =$ (1100000000000000000) and $\Delta K_\beta = \Delta K_{\beta'} =$ (00000000000000000000).

4.2 Related-key impossible boomerang attacks on 22-round LBlock-s

An attack on 22-round LBlock-s is achieved by adding 4 rounds at the top and 3 rounds at the bottom of the distinguisher described above. The extended differential characteristics are shown in **Fig. 4** and **Fig. 5**. Since the two related-key differential characteristics for E_0 are chosen to be the same, the input differences of the two characteristics are both given as $(\Delta X_1, \Delta X_0) = (0*00000*,*0?0*00*)$. The attack procedure can be elaborated as follows.

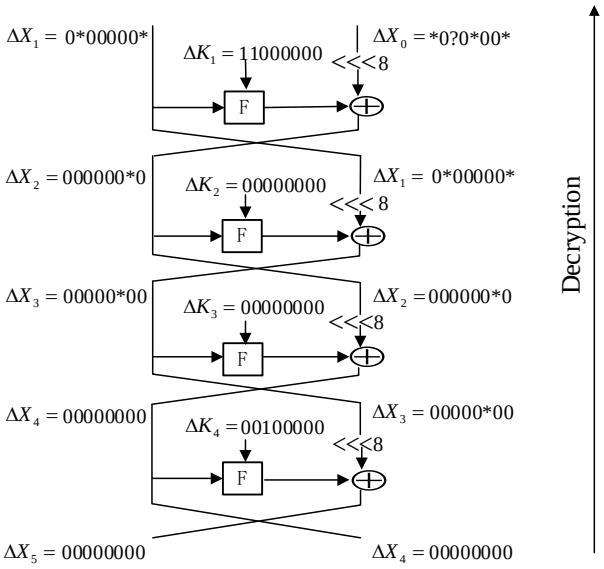

Fig. 4. 4 rounds added at the top of the distinguisher

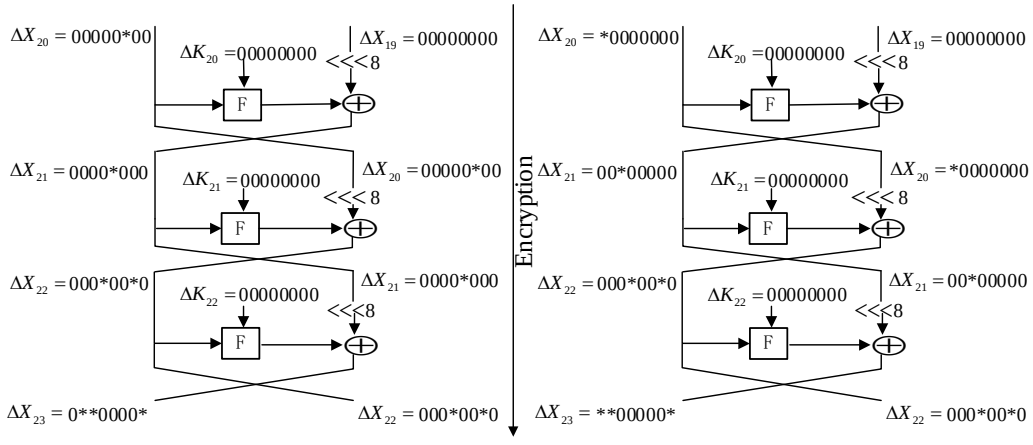

Fig. 5. 3 rounds added at the bottom of the distinguisher

Step 1. Select a set of 2^{24} plaintexts to produce a structure, where the nibbles X_0^0, X_0^3, X_0^5, X_0^7, X_1^0 and X_1^6 take all possible values of $\mathbb{F}_2^4$ and the other nibbles take constants. Thus each structure contains $2^{24} \times 2^{24} \times 1/2 = 2^{47}$ plaintext pairs. Choose 2^n structures

described above, there will be $2^n \times 2^{47} = 2^{n+46.1}$ plaintext pairs denoted as $(\mathrm{P}, \mathrm{P}^*)$. Similarly, choose 2^n more structures which contain 2^{n+47} plaintext pairs denoted as $(\mathrm{P}', \mathrm{P}'^*)$. Then 2^{2n+94} plaintext quartets $((\mathrm{P}, \mathrm{P}^*), (\mathrm{P}', \mathrm{P}'^*))$ are constructed. We take 2^{n+1} structures, so there are 2^{2n+94} plaintext quartets in total.

Step 2. Encrypt these plaintext quartets for 22 rounds with keys K_A, K_B, K_C and K_D to obtain the corresponding ciphertext quartets denoted as $((\mathrm{C}, \mathrm{C}^*), (\mathrm{C}', \mathrm{C}'^*))$. Then filter the ciphertext quartets by checking if the differences of ciphertext quartets are ((0**0 000*,000*00*0), (**00000*,000*00*0)).

Then, the number of remaining ciphertext quartets is $2^{2n+94} \times 2^{-4\times 22} = 2^{2n+6}$.

Step 3. Guess the subkey K_{22}^1 and K_{22}^4.

(a) Partially decrypt C and C' of the remaining quartets for one round and filter the quartets by the equation

$$S(X_{22}^1 \oplus K_{22}^1) \oplus S(X_{22}^1 \oplus K_{22}^1 \oplus \Delta X_{22}^1) = \Delta X_{23}^0.$$

Do the same operation on C^* and C'^* with the subkey $K_{22}^1 \oplus \Delta K_{22}^1$.

(b) For the remaining ciphertext quartets, then partially decrypt C and C' for one round and filter the quartets by the equation

$$S(X_{22}^4 \oplus K_{22}^4) \oplus S(X_{22}^4 \oplus K_{22}^4 \oplus \Delta X_{22}^4) = \Delta X_{23}^6.$$

Do the same operation on C^* and C'^* with the subkey $K_{22}^4 \oplus \Delta K_{22}^4$.

Thus there remain about $2^{2n+6} \times 2^{-4\times 4} = 2^{2n-10}$ quartets, and the time complexity is $(2^{2n+6} \times 2^4 + 2^{2n-2} \times 2^8) \times 1/8 \times 1/22 \approx 2^{2n+2.63}$

Step 4. Guess the subkey K_1^0, K_1^6 and K_1^7.

(a) Partially encrypt P and P^* of the remaining quartets for one round and filter the quartets by the equation

$$S(X_1^0 \oplus K_1^0) \oplus S(X_1^0 \oplus K_1^0 \oplus \Delta X_1^0 \oplus \Delta K_1^0) = \Delta X_0^0.$$

Do the same operation on P' and P'^* with the same subkey.

(b) For the remaining quartets, partially encrypt P and P^* for one round and filter the quartets by the equation

$$S(X_1^6 \oplus K_1^6) \oplus S(X_1^6 \oplus K_1^6 \oplus \Delta X_1^6 \oplus \Delta K_1^6) = \Delta X_0^5.$$

Do the same operation on P' and P'^* with the same subkey.

(c) Then partially encrypt P and P^* of the remaining plaintext quartets for one round and filter the quartets by the equation

$$S(X_1^7 \oplus K_1^7) \oplus S(X_1^7 \oplus K_1^7 \oplus \Delta X_1^7 \oplus \Delta K_1^7) = \Delta X_0^3.$$

Do the same operation on P' and P'^* with the same subkey.

Thus, there remain about $2^{2n-10} \times 2^{-4\times 6} = 2^{2n-34}$ quartets, and the time complexity is $(2^{2n-10} \times 2^{12} + 2^{2n-18} \times 2^{16} + 2^{2n-26} \times 2^{20}) \times 1/8 \times 1/22 \approx 2^{2n-5.37}$.

Step 5. Guess the subkey K_2^1 and K_1^3.

Partially encrypt P and P^* of remaining plaintext quartets for two rounds and filter the quartets by the equation

$$S(X_2^1 \oplus K_2^1) \oplus S(X_2^1 \oplus K_2^1 \oplus \Delta X_2^1 \oplus \Delta K_2^1) = \Delta X_1^6,$$

where $X_2^1 = S(K_1^3 \oplus X_1^3) \oplus X_0^7$.

Do the same operation on P' and P'^* with the same subkey.

Thus there are about $2^{2n-34} \times 2^{-4\times2} = 2^{2n-42}$ remaining quartets, and the time complexity is $2^{2n-34} \times 2^{28} \times 2/8 \times 1/22 \approx 2^{2n-12.46}$.

Step 6. Guess the subkey K_3^2, K_2^0 and K_1^1.

Partially encrypt P and P^* of the remaining plaintext quartets for three rounds and filter the quartets by the equation

$$S(X_3^2 \oplus K_3^2) \oplus S(X_3^2 \oplus K_3^2 \oplus \Delta X_3^2 \oplus \Delta K_3^2) = \Delta X_2^1,$$

where $X_3^2 = S(K_2^0 \oplus X_2^0) \oplus X_1^0$ and $X_2^0 = S(K_1^1 \oplus X_1^1) \oplus X_0^6$.

Do the same operation on P' and P'^* with the same subkey.

Thus, there are about $2^{2n-42} \times 2^{-4\times2} = 2^{2n-50}$ remaining quartets, and the time complexity is $2^{2n-42} \times 2^{40} \times 3/8 \times 1/22 \approx 2^{2n-7.88}$.

Step 7. Guess the subkey K_{21}^3, K_{22}^7, K_{21}^5 and K_{22}^6.

(a) Partially decrypt C and C' of the remaining quartets for two rounds and filter the quartets by the equation

$$S(X_{21}^3 \oplus K_{21}^3) \oplus S(X_{21}^3 \oplus K_{21}^3 \oplus \Delta X_{21}^3) = \Delta X_{22}^1,$$

where $X_{21}^3 = S(K_{22}^7 \oplus X_{22}^7) \oplus X_{23}^5$.

(b) Then partially decrypt C^* and C'^* of the remaining quartets for two rounds and filter the quartets by the equation

$$S\left(X_{21}^5 \oplus K_{21}^5 \oplus \Delta K_{21}^5\right) \oplus S\left(X_{21}^5 \oplus K_{21}^5 \oplus \Delta K_{21}^5 \oplus \Delta X_{21}^5\right) = \Delta X_{22}^4,$$

where $X_{21}^5 = S(K_{22}^6 \oplus \Delta K_{22}^6 \oplus X_{22}^6) \oplus X_{23}^7$.

Thus there are about $2^{2n-50} \times 2^{-4\times2} = 2^{2n-58}$ remaining quartets, and the time complexity is $(2^{2n-50} \times 2^{48} + 2^{2n-54} \times 2^{56}) \times 2/8 \times 1/22 \approx 2^{2n-4.37}$.

Step 8. Guess the subkey K_{20}^2, K_{21}^5, K_{22}^6, K_{20}^7、K_{21}^3 and K_{22}^7. Since the subkey K_{21}^5, K_{22}^6, K_{21}^3 and K_{22}^7 have been guessed, thus just need guess the remaining 8-bit key.

(a) Partially decrypt C and C' of the remaining quartets for three rounds and filter the quartets by the equation

$$S(X_{20}^2 \oplus K_{20}^2) \oplus S(X_{20}^2 \oplus K_{20}^2 \oplus \Delta X_{20}^2) = \Delta X_{21}^3,$$

where $X_{20}^2 = S(K_{21}^5 \oplus X_{21}^5) \oplus X_{22}^4$ and $X_{21}^5 = S(K_{22}^6 \oplus X_{22}^6) \oplus X_{23}^7$.

(b) Then partially decrypt C^* and C'^* of the remaining quartets for three rounds and filter the quartets by the equation

$$S(X_{20}^7 \oplus K_{20}^7 \oplus \Delta K_{20}^7) \oplus S(X_{20}^7 \oplus K_{20}^7 \oplus \Delta K_{20}^7 \oplus \Delta X_{20}^7) = \Delta X_{21}^5,$$

where $X_{20}^7 = S(K_{21}^3 \oplus \Delta K_{21}^3 \oplus X_{21}^3) \oplus X_{22}^1$ and $X_{21}^3 = S(K_{22}^7 \oplus \Delta K_{22}^7 \oplus X_{22}^7) \oplus X_{23}^5$.

Thus there are about $2^{2n-58} \times 2^{-4\times2} = 2^{2n-66}$ remaining quartets, and the time complexity is $(2^{2n-58} \times 2^{60} + 2^{2n-62} \times 2^{64}) \times 3/8 \times 1/22 \approx 2^{2n-2.88}$.

Step 9. Guess the nibble X_4^5 to determine the subkey K_4^5. Since there are 2^4 possible values for X_4^5 in $\mathbb{F}_2^4$, there are $2^4 \times 2^4 = 2^8$ possible values for X_4^5 in this attack. Partially encrypt the remaining quartets for four rounds, and keep only the quartets that satisfy the condition $F\left(\Delta X_4^5 \oplus \Delta K_4^5\right) \oplus \Delta X_3^2 = 0$. According to the difference distribution table of the S-boxes, the equation above holds with probability of $1/6$, so $2^{2n-66} \times 2^8 \times$

$1/6 \approx 2^{2n-60.58}$ quartets will be remained. The time complexity is $2^{2n-66} \times 2^8 \times 2^{64} \times 1/8 \times 1/22 \approx 2^{2n-1.46}$.

If there still quartets left after filtering, it shows that these subkeys being guessed satisfy the related-key impossible boomerang distinguisher, so these subkeys need to be removed and other candidate subkeys should be tried.

If we choose 2^{34} structures, that is, n = 33, the time complexity of this attack is about $2^{2n+2.63} + 2^{2n-5.37} + 2^{2n-12.46} + 2^{2n-7.88} + 2^{2n-4.37} + 2^{2n-2.88} + 2^{2n-1.46} = 2^{2n+2.76} = 2^{68.76}$ 22-round encryptions and the data complexity is $2^{n+1+24} = 2^{58}$ chosen plaintexts. **Table 5** shows summary of the number of bits guessed in steps 3-9.

Table 5. The number of bits guessed in steps 3-9

Step	Subkey	The number of guessed bits	The remaining pairs	The time complexity
3	K_{22}^1, K_{22}^4	8	2^{56}	$2^{68.63}$
4	K_1^0, K_1^6, K_1^7	12	2^{32}	$2^{60.63}$
5	K_2^1, K_1^3	8	2^{24}	$2^{53.54}$
6	K_3^2, K_2^0, K_1^1	12	2^{16}	$2^{58.12}$
7	$K_{21}^3, K_{22}^7, K_{21}^5, K_{22}^6$	16	2^8	$2^{61.63}$
8	$K_{20}^2, K_{21}^5, K_{22}^6, K_{20}^7, K_{21}^3, K_{22}^7$	8	2^0	$2^{63.12}$
9	K_4^5	4	$2^{5.42}$	$2^{64.54}$

5. Conclusions

Table 6. Summary of attacks on LBlock-s

Attack Type	Rounds	Time	Data	Reference
multidimensional zero-correlation linear	23	$2^{73.75}$	$2^{62.3}$	[5]
impossible differential	21	$2^{67.71}$	2^{63}	[6]
impossible differential	22	$2^{78.86}$	2^{58}	[6]
related-key impossible boomerang	22	$2^{68.76}$	2^{58}	this paper

This paper presents a 15-round related-key impossible boomerang distinguisher for the first time, based on which we attack on 22-round LBlock-s by combining the advantages of the related-key impossible boomerang attack with the weaknesses of the structure of encryption and key schedule algorithm. Analysis results indicate this attack only needs $2^{68.76}$ encryptions and 2^{58} chosen plaintexts. And there are 68 key bits recovered in this attack. **Table 6** shows summary of attack results on LBlock-s. Compared with the impossible

differential attack on 22-round LBlock-s in [6], the complexity of the attack on 22-round LBlock-s proposed in this paper presents a substantial reduction. And this is the first time to apply related-key impossible boomerang attack on LBlock-s. Thus, our research on LBlock-s could provide some suggestions for the design of lightweight block ciphers and the improvement of key schedule algorithms. For the future work, we will improve the characteristics search algorithm to achieve higher rounds attacks on LBlock-s and other block ciphers, and evaluate the security of the LAC.

References

[1] Lei Zhang, Wenling Wu, Yanfeng Wang, Shengbao Wu and Jian Zhang, "LAC: a lightweight authenticated encryption cipher," *Submission to CAESAR*, March 15, 2014. Article (CrossRef Link).

[2] Wenling Wu and Lei Zhang, "LBlock: a lightweight block cipher," in *Proc. of 9th Int. Conf. on Applied Cryptography and Network Security*, pp. 327–344, June 7-10, 2011. Article (CrossRef Link).

[3] Jinyong Shan, Lei Hu, and Sun Siwei, "Security of LBlock-s against related-key differential attack," in *Proc. of 2nd Int. Conf. on Electronics and Communication Systems*, pp. 1278-1283, February 26-27, 2015. Article (CrossRef Link).

[4] Zhen Xiao, "Research on several authentication encryption algorithms," *Shandong Normal University*, 2016.

[5] Lingcheng Li, Wenling Wu and Yanfeng Wang, "Improved multidimensional zero-correlation linear cryptanalysis and application to 23-round LBlock-s," *Chinese Journal of Computers*, vol. 40, no. 5, pp. 1192-1202, May, 2017. Article (CrossRef Link).

[6] Ping Jia, Hong Xu and Xuejia Lai, "Impossible differential cryptanalysis of reduced-round LBlock-s," *Acta Electronica Sinica*, vol. 45, no. 4, pp. 97-108, April, 2017.

[7] Lars Ramkilde Knudsen, "Crypatanalysis of LOKI," in *Proc. of Int. Conf. on the Theory and Application of Cryptology*, pp, 22-35, November 11-14, 1991. Article (CrossRef Link).

[8] Eli Biham, "New types of cryptanalytic attacks using related keys," *Journal of Cryptology*, vol. 7, no. 4, pp. 229-246, December, 1994. Article (CrossRef Link).

[9] Lars Ramkilde Knudsen, "DEAL A 128-bit block cipher," *Technical Report 151*, Department of Informatics, University of Bergen, Bergen, Norway, February, 1998. Article (CrossRef Link).

[10] Eli Biham, Alex Biryukov and Adi Shamir, "Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials," in *Proc. of Int. Conf. on the Theory and Applications of Cryptographic Techniques*, pp. 12-23, May 2-6, 1999. Article (CrossRef Link).

[11] Kai Zhang, Lin Ding, Junzhi Li and Jie Guan, "Real time related key attack on hummingbird-2," *KSII Transactions on Internet and Information Systems*, vol. 6, no. 8, pp. 1946-1963, August, 2012. Article (CrossRef Link).

[12] Jongsung Kim, Seokhie Hong, Jaechul Sung, Sangjin Lee, Jongin Lim and Soohak Sung, "Impossible differential cryptanalysis for block cipher structures," in *Proc. of Int. Conf. on Cryptology in India*, pp. 82-96, December 8-10, 2003. Article (CrossRef Link).

[13] Kai Zhang, Jie Cuan and Bin Hu, "Impossible differential cryptanalysis on DVB-CSA," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 4, pp. 1944-1956, April, 2016. Article (CrossRef Link).

[14] Masroor Hajari, Seyyed Arash Azimi, Poorya Aghdaie, Mahmoud Salmasizadeh and Mohammad Reza Aref, "Impossible differential cryptanalysis of reduced-round TEA and XTEA," in *Proc. of 12th Int. Iranian Society of Cryptology Conf. on Information Security and Cryptology*, pp. 58-63, September 8-10, 2015. Article (CrossRef Link).

[15] Min Xie, Jingjing Li, and Yuechuan Zang, "Related-key impossible differential cryptanalysis of LBlock," *Chinese Journal of Electronics*, vol. 26, no. 1, pp. 235-41, January, 2017. Article (CrossRef Link).
[16] Saeed Rostami, Sadegh Bamohabbat Chafjiri and Seyed Amir Hossein Tabatabaei, "Related-key impossible differential cryptanalysis of full-round HIGHT," in *Proc. of Int. Conf. on Security and Cryptography*, pp. 537-542, July 29-31, 2013. Article (CrossRef Link).
[17] Lu Cheng, Peng Xu and Yuechuan Wei, "New related-key impossible differential attack on MIBS-80," in *Proc. of Int. Conf. on Intelligent Networking and Collaborative Systems*, pp. 203-206, September 7-9, 2016. Article (CrossRef Link).
[18] David Wagner, "The boomerang attack," in *Proc. of Int. Workshop on Fast Software Encryption*, pp. 156-170, March 24-26, 1999. Article (CrossRef Link).
[19] Jiqiang Lu, "The (related-key) impossible boomerang attack and its application to the AES block cipher," *Designs, Codes and Cryptography*, vol. 60, no. 2, pp. 123-143, August, 2011. Article (CrossRef Link).
[20] Min Xie, Yanli Mu, " Related-key impossible boomerang cryptanalysis on LBlock," *Journal on Communications*, vol. 38, no. 5, pp. 66-71, May, 2017. Article (CrossRef Link).

Min Xie received the Ph.D. degree in applied mathematics from Graduate University of Chinese Academy of Sciences. She is now an associate professor with the school of Telecommunications Engineering, Xidian University. Her research interests include coding and cryptography.

Qiya Zeng received the B.E. degree from Southwest University of Science and Technology. She is now a M.S. candidate of Xidian University. Her research interests include block cipher and cryptanalysis.