Improved Related-Key Differential Attacks on Reduced-Round LBlock*

Shusheng Liu, Zheng Gong, and Libin Wang

School of Computer Science,
South China Normal University. 510631 Guangzhou, China
{liushusheng914,cis.gong,lbwang}@gmail.com

Abstract. At ACNS 2011, Wu and Zhang proposed a new lightweight block cipher which is named LBlock. The design rationale of LBlock considers the trade-offs between security against cryptanalyses and performance in low-resource implementations. In this paper, we present new attacks on reduced-round LBlock using related-key differential cryptanalysis. Firstly, we construct a new related-key boomerang distinguishing attack on 16-round LBlock. Secondly, we construct a key recovery attack on 22-round LBlock based on a 16-round related-key truncated differential. In contrast to the published cryptanalysis results of reduced-round LBlock, our attacks have advantages on data and computational complexities.

Keywords: Lightweight block cipher, Differential analysis, Related-key boomerang attack, LBlock.

1 Introduction

Due to a growing requirement of ciphers suited for constrained environment, the design and analysis of lightweight block cipher have received a lot of attention. Many lightweight block ciphers have been proposed such as PRESENT [4], KLEIN [6], LED [7], LBlock [14], Piccolo [11] and KATAN & KTANTAN [5].

LBlock is a lightweight block cipher with the Feistel structure, which is proposed by Wu and Zhang at ACNS 2011 [14,15]. The components of LBlock represent the trade-off between fast diffusion and performance in resource-constrained environment. For the differential analysis, The authors of LBlock proved that the probability of 15-round characteristic can be lower than 2^{-64} [14]. For the impossible differential analysis, a 14-round impossible differential is used to mount a key recovery attack on 20-round LBlock [14]. For the integral attack, a 15-round integral distinguisher is used to mount a key recovery attack on 20-round LBlock [14]. Although Shibutani et al.'s paper mentioned they can break 22-round LBlock using integral analysis [12], the details of the attack has not been publicly verifiable yet. Thus the complexities of Shibutani et al.'s attack are described as "?" in Table 1. Recently, a key recovery attack on 22-round LBlock is presented in [9], which takes advantage of a 14-round related-key impossible differential. Table 1 includes the existing attacks of LBlock.

* The authors are supported by NSFC 61100201 and Foundation for distinguished Young Talents in Higher Education of Guangdong (LYM11053), China.

T.W. Chim and T.H. Yuen (Eds.): ICICS 2012, LNCS 7618, pp. 58–69, 2012.

In this paper, we present new related-key differential attacks on reduced-round LBlock. We first propose a 16-round related-key boomerang distinguishing attack, which has a successful probability of 2^{-60}. The distinguisher exploits two 8-round related-key characteristics. Then we present a key recovery attack on 22-round LBlock, which uses a 16-round related-key truncated differential. The time and data complexities of our key recovery attack are 2^{67} and $2^{64.1}$ respectively, which are better than the previous attacks on 22-round LBlock.

Table 1. Summary of the existing attacks on LBlock

Rounds	Time	Data	Type	Reference
13	2^{53}	-	related-key differential distinguisher	[14]
16	2^{60}	-	related-key boomerang distinguisher	this paper
20	$2^{63.7}$	$2^{63.7}$	integral key recovery	[14]
22	?	?	integral attack	[12]
22	2^{70}	2^{68}	related-key impossible key recovery	[9]
22	2^{67}	$2^{64.1}$	related-key differential key recovery	this paper

2 Preliminary

In this section, we first list some notions and notation which will be used in the following analysis. Next, a brief description of LBlock is presented. Finally, the method of the related-key boomerang attack is recalled in short.

2.1 Notations

1. V_i is a 64-bit word, which denotes the input of round i. Moreover, $V_{i,l}$ and $V_{i,r}$ are 32-bit words, where $V_i = V_{i,l} \| V_{i,r}$.
2. K denotes the 80-bit master key and $subkey_i$ is 32-bit subkey of round i. Furthermore, $subkey_i^j$ is the j-th nibble of $subkey_i$ and $subkey_i^{j,k}$ is the k-th bit of $subkey_i^j$.
3. For $0 \leq i \leq 9$, s_i denotes a 4-bit input-output S-box, and s_i^{-1} is its inverse.
4. Δx denotes the difference between two values of x. X denotes an active nibble with an uncertain difference.
5. $\lll 8$ denotes an 8-bit cyclic left rotation, $\oplus$ denotes the bitwise exclusive-or (XOR) operation, and $\|$ is the concatenation of two binary strings.

2.2 A Brief Description of LBlock

The first introduction of the LBlock proposal was described by Wu and Zhang at ACNS 2011 [14]. In [15], some literal flaws of the initial proposal were fixed. Here we briefly recall the illustration of LBlock. The i-th round of the LBlock is shown in the left of Fig. 1, and the F function is shown in the right of Fig. 1. The block length of LBlock is 64-bit, and the key length is 80-bit. Where $V_i = V_{i,l} \| V_{i,r}$ is the input of round i. The round function F first computes $V_{i,l} \oplus subkey_i$, then applies eight different 4-bit S-boxes. The round function F finally applies a permutation P, which exchanges the places of the eight nibbles.

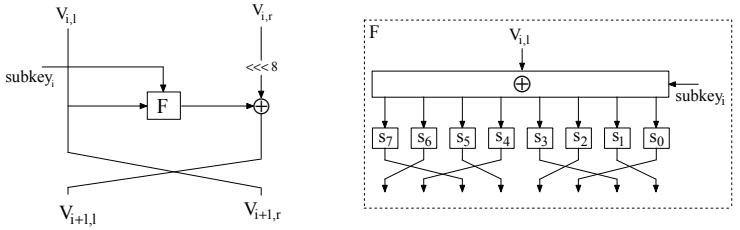

Fig. 1. Left of the figure is the i-th round of LBlock and right of the figure is the F function

The key schedule stores an 80-bit master key K in key register, which is denoted by $K = k_{79}k_{78}k_{77}k_{76} \cdots\cdots k_1k_0$. It repeats the following operations for $i = 1$ to 32:

1. Output the leftmost 32 bits of current register K as $subkey_i$.
2. $K \lll 29$
3. $[k_{79}k_{78}k_{77}k_{76}] = s_9[k_{79}k_{78}k_{77}k_{76}]$, $[k_{75}k_{74}k_{73}k_{72}] = s_8[k_{75}k_{74}k_{73}k_{72}]$
4. $[k_{50}k_{49}k_{48}k_{47}k_{46}] = [k_{50}k_{49}k_{48}k_{47}k_{46}] \oplus [i]_2$

where s_8 and s_9 are two 4-bits S-boxes and $[i]_2$ is a binary counter.

2.3 The Related-Key Boomerang Attack

The related-key attack was first introduced by Biham in [1]. The attack allows adversary to encrypt plaintexts and decrypt ciphertexts under multiple secret keys, but the relation between the secret keys is known to (or even chosen by) the adversary. The boomerang attack was introduced by Wagner in [13]. By extending the boomerang attack in the

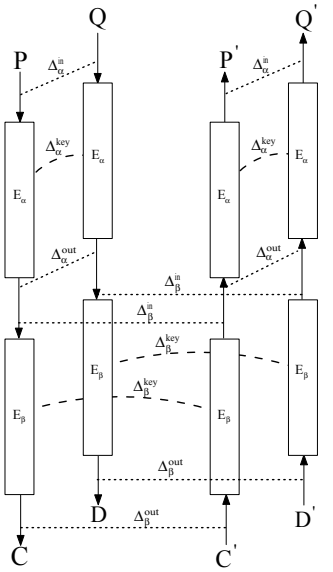

Fig. 2. A schematic of related-key boomerang attack

related-key model [2], Biham *et al.* proposed the related-key boomerang attack. As shown in Fig. 2, the related-key boomerang attack views a cipher E as a decomposition into two sub-ciphers, such that $E = E_\alpha \circ E_\beta$. In each of two sub-ciphers, there exists a high probability related-key differential for constructing a boomerang attack. Based on the boomerang technique, algorithms can be built to distinguishing a "weak" block cipher from an ideal cipher. The examples of boomerang distinguishing attacks can be found in [3,8].

If the probability of the E_α differential $(\Delta_\alpha^{in}, \Delta_\alpha^{out}, \Delta_\alpha^{key})$ is p and the probability of the E_β differential $(\Delta_\beta^{in}, \Delta_\beta^{out}, \Delta_\beta^{key})$ is q, it was proven that the probability of the corresponding related-key boomerang attack is close to $(p \cdot q)^2$.

3 Related-Key Boomerang Attack on 16-Round LBlock

In [9], Minier and Naya-Plasencia found that ones are able to construct subkey differences with a very low general weight. Thus, here we consider a related-key boomerang distinguisher, which exploits the weakness of key scheduling.

Let E denote the 16 rounds of LBlock and E_α denote the first eight rounds (1 to 8) of E. E_β is viewed as the sub-cipher of the following 8 rounds (9 to 16). In this section, we first introduce the subkey differences that are used in our boomerang attack. Then we present an 8-round related-key characteristic of E_α and E_β, separately. Finally, we propose the related-key boomerang distinguishing attack on 16-round LBlock.

3.1 The Subkey Differences

The following differences Δ_α^{key} and Δ_β^{key} are selected for constructing the 8-round related-key differential of E_α and E_β, respectively.

$$\Delta_\alpha^{key} = 0x00000200000000000000,\ \Delta_\beta^{key} = 0x0000c000000000000000$$

According to the key schedule of LBlock, the subkey differences of E_α, which can be obtained from Δ_α^{key}, have probability 1. The subkey differences of E_α are given in the left of Table 2. According to the key schedule of LBlock, the equation $s_9(0x3) = 0x8$ in $subkey_7$ is satisfied with a probability of 2^{-2}. Thus, the subkey differences of E_β, which are obtained from Δ_β^{key}, have a probability of 2^{-2}. The subkey differences of E_β are given in the right of Table 2.

Table 2. The subkey differentials for the related-key boomerang distinguishing attack

Δ_α^{key} :00000200000000000000	Δ_β^{key} :0000c000000000000000	
$\Delta subkey_1$: 0 0 0 0 0 2 0 0	$\Delta subkey_1$: 0 0 0 0 c 0 0 0	$\Delta subkey_9$: 0 0 0 0 0 2 0 0
$\Delta subkey_2$: 0 0 0 0 0 0 0 0	$\Delta subkey_2$: 0 0 0 0 0 0 0 0	$\Delta subkey_{10}$: 0 0 0 0 0 0 0 0
$\Delta subkey_3$: 0 0 0 0 0 0 0 0	$\Delta subkey_3$: 0 0 0 0 0 0 0 0	$\Delta subkey_{11}$: 0 0 0 0 0 0 0 0
$\Delta subkey_4$: 0 0 0 1 0 0 0 0	$\Delta subkey_4$: 0 0 6 0 0 0 0 0	$\Delta subkey_{12}$: 0 0 0 1 0 0 0 0
$\Delta subkey_5$: 0 0 0 0 0 0 0 0	$\Delta subkey_5$: 0 0 0 0 0 0 0 0	$\Delta subkey_{13}$: 0 0 0 0 0 0 0 0
$\Delta subkey_6$: 0 0 0 0 0 0 0 0	$\Delta subkey_6$: 0 0 0 0 0 0 0 1	$\Delta subkey_{14}$: 0 0 0 0 0 0 0 0
$\Delta subkey_7$: 0 0 8 0 0 0 0 0	$\Delta subkey_7$: 8 0 0 0 0 0 0 0	$\Delta subkey_{15}$: 0 0 8 0 0 0 0 0
$\Delta subkey_8$: 0 0 0 0 0 0 0 0	$\Delta subkey_8$: 0 0 0 0 0 0 0 0	$\Delta subkey_{16}$: 0 0 0 0 0 0 0 0

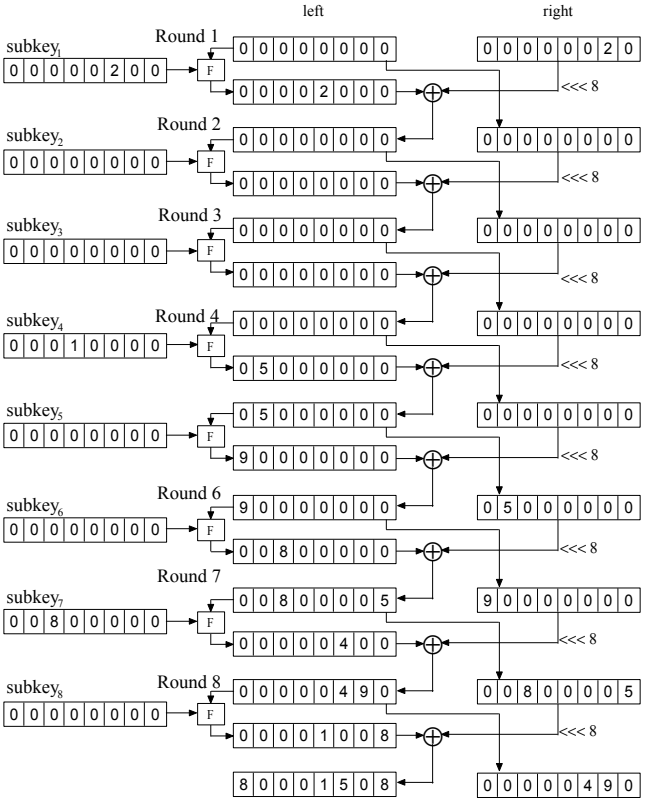

Fig. 3. An 8-round related-key characteristic of E_α. The 8-round related-key characteristic of E_β is the same as E_α. In other words, the difference $\Delta subkey_i$ of E_β is equal to the difference $\Delta subkey_{i-8}$ of E_α and the difference of round i of E_β is equal to the difference of round i-8 of E_α, for $9 \leq i \leq 16$.

3.2 The 16-Round Related-Key Boomerang Distinguisher

The 8-round related-key characteristic of E_α shown in Fig. 3 works for the subkey differences of Δ_α^{key}. It contains seven active S-boxes, and the probability of the seven active S-boxes are equal to 2^{-2}. Therefore the 8-round related-key characteristic of E_α has probability 2^{-14}.

We choose Δ_β^{key} to ensure the $\Delta subkey_i$ of Δ_β^{key} equals the $\Delta subkey_{i-8}$ of Δ_α^{key}, for $9 \leq i \leq 16$. Thus, we can reuse the 8-round related-key characteristic of E_α as the related-key characteristic of E_β. As a result, we obtain an 8-round related-key characteristic of E_β, which has a probability of 2^{-16}.

Based on the related-key differential of E_α and E_β, the corresponding differences in Fig. 2 are derived as follows.

$$\Delta_\alpha^{in} = 0x0000000000000020 \quad \Delta_\alpha^{out} = 0x8000150800000490$$
$$\Delta_\beta^{in} = 0x0000000000000020 \quad \Delta_\beta^{out} = 0x8000150800000490$$

The related-key differential of E_α $(\Delta_\alpha^{in}, \Delta_\alpha^{out}, \Delta_\alpha^{key})$ has a probability of 2^{-14}, and the one of E_β $(\Delta_\beta^{in}, \Delta_\beta^{out}, \Delta_\beta^{key})$ has a probability of 2^{-16}. Thus, the related-key boomerang distinguisher of 16-round LBlock succeeds with a probability of $(2^{-14} \times 2^{-16})^2 = 2^{-60}$. As a result, the boomerang distinguisher works as follows.

1. Chooses a random message P and calculates $Q = P \oplus \Delta_\alpha^{in}$.
2. Encrypts P and Q, obtain $C = E_k(P)$ and $D = E_{k \oplus \Delta_\alpha^{key}}(Q)$.
3. Selects $C' = C \oplus \Delta_\beta^{out}$ and $D' = D \oplus \Delta_\beta^{out}$.
4. Decrypts C' and D', obtains $P' = E^{-1}_{k \oplus \Delta_\beta^{key}}(C')$ and $Q' = E^{-1}_{k \oplus \Delta_\alpha^{key} \oplus \Delta_\beta^{key}}(D')$.
5. Checks if $P' \oplus Q' = \Delta_\alpha^{in}$.

For ideal ciphers with 64-bit block size, the probability of the final equation $P' \oplus Q' = \Delta_\alpha^{in}$ must be 2^{-64}. On the other hand, the final equation is expected to hold with a probability of $(2^{-14} \times 2^{-16})^2 = 2^{-60}$ in the related-key boomerang distinguisher, which is apparently lower than exhaustive search. Therefore, an adversary can distinguish 16-round LBlock and an ideal cipher by executing the above boomerang attack.

4 Related-Key Differential Attack on 22-Round LBlock

In [9], a related-key impossible attack, which exploits the weakness of the key schedule, was presented on reduced-round LBlock. Since the key schedule of LBlock does not provide a fast diffusion [9], it is possible to construct a 16-round related-key truncated differential. In this section, a new key-recovery attack on 22-round is proposed by exploiting a 16-round related-key truncated differential.

4.1 The Subkey Differences

The difference $\Delta K = 0x00000010000000000000$ is selected for constructing the 16-round related-key truncated differential, which will be described in the next subsection. According to the key schedule, we obtain a subkey differences in the first 22 round from ΔK, which is shown in Table 3. Since the equation $s_8(0x2) = 0x2$ in $subkey_{10}$ is satisfied with probability 2^{-2}, the subkey differences has probability 2^{-2} as well.

Table 3. The subkey differences in the first 22 round of LBlock

Δ_K : 00000010000000000000		
$\Delta subkey_1$: 0 0 0 0 0 0 1 0	$\Delta subkey_8$: 0 0 0 0 0 0 0 0	$\Delta subkey_{15}$: 0 0 0 0 0 4 0 0
$\Delta subkey_2$: 0 0 0 0 0 0 0 0	$\Delta subkey_9$: 0 0 0 0 0 0 0 0	$\Delta subkey_{16}$: 0 0 0 0 0 0 0 0
$\Delta subkey_3$: 0 0 0 0 0 0 0 0	$\Delta subkey_{10}$: 0 2 0 0 0 0 0 0	$\Delta subkey_{17}$: 0 0 0 0 0 0 0 0
$\Delta subkey_4$: 0 0 0 0 0 8 0 0	$\Delta subkey_{11}$: 0 0 0 0 0 0 0 0	$\Delta subkey_{18}$: 0 0 0 2 0 0 0 0
$\Delta subkey_5$: 0 0 0 0 0 0 0 0	$\Delta subkey_{12}$: 0 0 0 0 0 0 0 8	$\Delta subkey_{19}$: 0 0 0 0 0 0 0 0
$\Delta subkey_6$: 0 0 0 0 0 0 0 0	$\Delta subkey_{13}$: 0 0 0 0 0 0 0 0	$\Delta subkey_{20}$: 0 0 0 0 0 0 0 0
$\Delta subkey_7$: 0 0 0 4 0 0 0 0	$\Delta subkey_{14}$: 0 0 0 0 0 0 0 0	$\Delta subkey_{21}$: 0 X 0 0 0 0 0 0
		$\Delta subkey_{22}$: 0 0 0 0 0 0 0 0

4.2 The 16-Round Related-Key Truncated Differential

The detail of the 16-round related-key truncated differential is depicted in Fig. 4, which is used for our 22-round key recovery attack. In Fig. 4, numeral represents a nibble with this specific difference. Such as, a numeral 1 in the $subkey_1$ denotes that this nibble has difference 1. Zero-difference nibbles are represented by 0. The active nibbles ($\overline{X}$, $\underline{X}$, $\widehat{4}$) represent three different conditions on their differences, which are described as follows.

- One active nibble $\overline{X}$ xor the other active nibble $\overline{X}$ produces difference 0 with probability $1/15 \approx 2^{-3.9}$. We call it *vanished condition*.
- One active nibble $\underline{X}$ xor the other active nibble $\underline{X}$ produces a non-zero difference with probability $14/15 \approx 2^{-0.1}$. We call it *unvanished condition*.
- A specific difference 4 marked by $\widehat{4}$ in Fig. 4 is a input difference of S-box. The equation $s_2(4) = 1$ satisfies with probability 2^{-2}. We call it *S-box condition*.

The 16-round related-key truncated differential in Fig. 4 has 14 vanished conditions, 1 S-box condition and 3 unvanished conditions. Based on the probabilities of the subkey differences, the 16-round related-key truncated differential has a probability of about $((1/15)^{14} \times 2^{-2} \times (14/15)^3 \times 2^{-2}) > 2^{-59}$.

4.3 The Key Recovery Attack for 22 Rounds

Combing our 16-round related-key truncated differential, we can mount a key recovery attack for 22 rounds. Our key recovery attack is based on the following observation. In the round function of LBlock, every 4-bit nibble in the underlying subkey only affects itself. In key-recovery procedure, one can guess one nibble of subkey each time, and then partially decrypts the corresponding nibble of ciphertext pairs. By checking the difference of the decrypted nibble, we rule out some ciphertext pairs. Therefore, the time complexity of the key recovery attack can be reduced.

Our key recovery attack is derived from the related-key truncated differential shown in Fig. 5. The key-recovery differential requests one vanished and two unvanished conditions. Thus a difference $\Delta_1 = (000X0000, 00000000)$ from round 17 to round 22 verifies the key-recovery differential with a probability of $(1/15) \times (14/15)^2 \approx 2^{-4.1}$. Since the 16-round related-key truncated differential has a probability of 2^{-59}. After the 22-th round, the output difference is $\Delta_2 = (V_{22,l}, V_{22,r}) = (XXXXXXX0, XX00XX0X)$ with a probability $2^{-59} \times 2^{-4.1} = 2^{-63.1}$. Therefore, there exist one pair of plaintexts verifies the 16-round related-key truncated differential and the key-recovery differential, when $2^{63.1}$ pairs of plaintexts with difference $\Delta_3 = (00000010, 00000004)$ are encrypted.

Without loss of generality, a pair satisfies the truncated difference Δ_2 with a probability of about $(15/16)^{12} \times (1/16)^4 \approx 2^{-17.1}$. Therefore, there exist about 2^{46} pairs satisfy the truncated difference Δ_2 after 22 rounds, when $2^{63.1}$ pairs of plaintexts with difference Δ_3 are encrypted. One pair of 22-round ciphertexts, which has a difference Δ_2, satisfies the key-recovery differential whit a probability of $((1/15)^{12} \times (14/15)^2 \approx 2^{-47}$, when decrypted from round 22 to round 17. If the subkeys are wrong, there exist one pair of 22-round ciphertexts satisfies the key-recovery differential with a probability of 2^{-1}, when the 2^{46} pairs of 22-round ciphertexts are decrypted from round 22 to round 17.

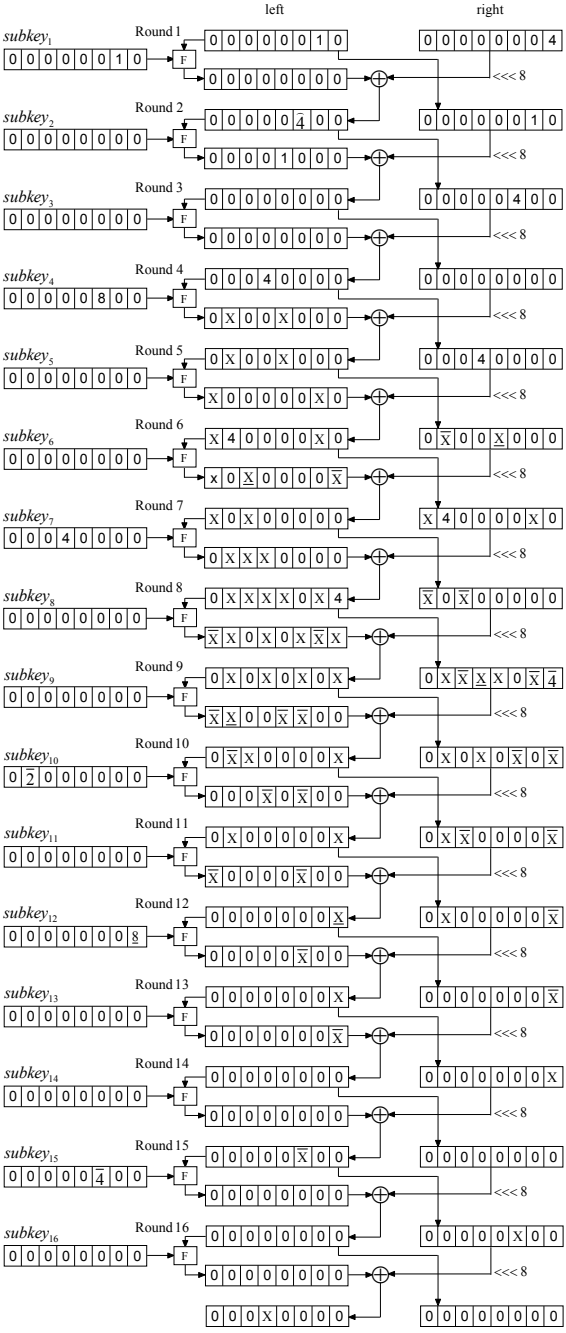

Fig. 4. A 16-round truncated differential path for the key recovery attack. The active nibbles ($\overline{X}$, $\underline{X}$, $\widehat{4}$) represent vanished, unvanished and S-box conditions on their differences, respectively.

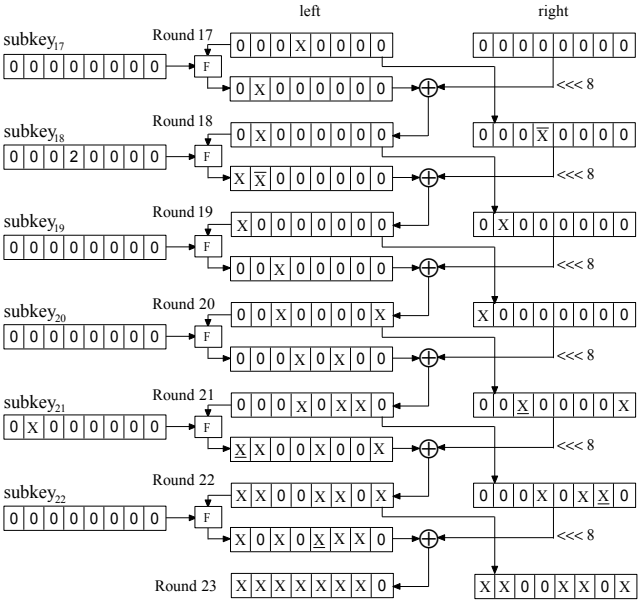

Fig. 5. A related-key differential from round 17 to round 22

Table 4. The relations among the subkey bits in the partial decryptions

The underline bits of $subkey_i$ can be obtained from the underline bits of $subkey_{22}$, where $17 \le i \le 21$								
$subkey_{17}$	$k_{15}k_{14}k_{13}k_{12}$	$k_{11}k_{10}k_9k_8$	$k_7k_6k_5k_4$	$k_3\underline{k_2k_1k_0}$	$k_{79}k_{78}k_{77}k_{76}$	$k_{75}k_{74}k_{73}k_{72}$	$k_{71}k_{70}k_{69}k_{68}$	$k_{67}k_{66}k_{65}k_{64}$
$subkey_{18}$	$k_{66}k_{65}k_{64}k_{63}$	$k_{62}k_{61}k_{60}k_{59}$	$k_{58}k_{57}k_{56}k_{55}$	$k_{54}\underline{k_{53}k_{52}}k_{51}$	$k_{50}k_{49}k_{48}k_{47}$	$k_{46}k_{45}k_{44}k_{43}$	$k_{42}k_{41}k_{40}k_{39}$	$k_{38}k_{37}k_{36}k_{35}$
$subkey_{19}$	$k_{37}k_{36}k_{35}k_{34}$	$k_{33}k_{32}k_{31}k_{30}$	$k_{29}k_{28}k_{27}k_{26}$	$k_{25}k_{24}k_{23}k_{22}$	$k_{21}k_{20}k_{19}k_{18}$	$k_{17}k_{16}k_{15}k_{14}$	$\underline{k_{13}k_{12}k_{11}k_{10}}$	$k_9k_8k_7k_6$
$subkey_{20}$	$k_8k_7k_6k_5$	$k_4k_3k_2k_1$	$\underline{k_0k_{79}k_{78}k_{77}}$	$k_{76}k_{75}k_{74}k_{73}$	$k_{72}k_{71}k_{70}k_{69}$	$k_{68}k_{67}k_{66}k_{65}$	$k_{64}k_{63}k_{62}k_{61}$	$k_{60}k_{59}k_{58}k_{57}$
$subkey_{21}$	$k_{59}k_{58}k_{57}k_{56}$	$k_{55}k_{54}k_{53}k_{52}$	$k_{51}k_{50}k_{49}k_{48}$	$k_{47}k_{46}k_{45}k_{44}$	$k_{43}k_{42}k_{41}k_{40}$	$k_{39}k_{38}k_{37}k_{36}$	$k_{35}k_{34}k_{33}k_{32}$	$k_{31}\underline{k_{30}k_{29}k_{28}}$
$subkey_{22}$	$\underline{k_{30}k_{29}k_{28}}k_{27}$	$k_{26}k_{25}k_{24}k_{23}$	$k_{22}k_{21}k_{20}k_{19}$	$k_{18}k_{17}k_{16}k_{15}$	$k_{14}\underline{k_{13}k_{12}k_{11}}$	$\underline{k_{10}}k_9k_8k_7$	$k_6k_5k_4k_3$	$\underline{k_2k_1k_0k_{79}}$

The underline bits of $subkey_i$ can be obtained from the underline bits of $subkey_{21}$, where $17 \le i \le 20$								
$subkey_{17}$	$k_{15}k_{14}k_{13}k_{12}$	$k_{11}k_{10}k_9k_8$	$k_7k_6k_5k_4$	$k_3k_2k_1k_0$	$k_{79}k_{78}k_{77}k_{76}$	$k_{75}k_{74}k_{73}k_{72}$	$k_{71}k_{70}k_{69}k_{68}$	$k_{67}k_{66}k_{65}k_{64}$
$subkey_{18}$	$k_{66}k_{65}k_{64}k_{63}$	$k_{62}k_{61}k_{60}k_{59}$	$k_{58}k_{57}k_{56}k_{55}$	$k_{54}k_{53}k_{52}k_{51}$	$k_{50}k_{49}k_{48}k_{47}$	$k_{46}k_{45}k_{44}k_{43}$	$k_{42}k_{41}k_{40}k_{39}$	$k_{38}k_{37}k_{36}k_{35}$
$subkey_{19}$	$\underline{k_{37}k_{36}k_{35}k_{34}}$	$k_{33}k_{32}k_{31}k_{30}$	$k_{29}k_{28}k_{27}k_{26}$	$k_{25}k_{24}k_{23}k_{22}$	$k_{21}k_{20}k_{19}k_{18}$	$k_{17}k_{16}k_{15}k_{14}$	$k_{13}k_{12}k_{11}k_{10}$	$k_9k_8k_7k_6$
$subkey_{20}$	$k_8k_7k_6k_5$	$k_4k_3k_2k_1$	$k_0k_{79}k_{78}k_{77}$	$k_{76}k_{75}k_{74}k_{73}$	$k_{72}k_{71}k_{70}k_{69}$	$k_{68}k_{67}k_{66}k_{65}$	$k_{64}k_{63}k_{62}k_{61}$	$k_{60}k_{59}k_{58}k_{57}$
$subkey_{21}$	$k_{59}k_{58}k_{57}k_{56}$	$k_{55}k_{54}k_{53}k_{52}$	$k_{51}k_{50}k_{49}k_{48}$	$k_{47}k_{46}k_{45}k_{44}$	$k_{43}k_{42}k_{41}k_{40}$	$k_{39}\underline{k_{38}k_{37}k_{36}}$	$\underline{k_{35}k_{34}}k_{33}k_{32}$	$k_{31}k_{30}k_{29}k_{28}$
$subkey_{22}$	$k_{30}k_{29}k_{28}k_{27}$	$k_{26}k_{25}k_{24}k_{23}$	$k_{22}k_{21}k_{20}k_{19}$	$k_{18}k_{17}k_{16}k_{15}$	$k_{14}k_{13}k_{12}k_{11}$	$k_{10}k_9k_8k_7$	$k_6k_5k_4k_3$	$k_2k_1k_0k_{79}$

The underline bits of $subkey_i$ can be obtained from the underline bits of $subkey_{20}$, where $17 \le i \le 19$								
Round 17	$k_{15}k_{14}k_{13}k_{12}$	$k_{11}k_{10}k_9k_8$	$k_7k_6k_5k_4$	$k_3k_2k_1k_0$	$k_{79}k_{78}k_{77}k_{76}$	$k_{75}k_{74}k_{73}k_{72}$	$k_{71}k_{70}k_{69}k_{68}$	$k_{67}k_{66}k_{65}k_{64}$
Round 18	$k_{66}k_{65}k_{64}k_{63}$	$k_{62}k_{61}\underline{k_{60}k_{59}}$	$k_{58}k_{57}k_{56}k_{55}$	$k_{54}k_{53}k_{52}k_{51}$	$k_{50}k_{49}k_{48}k_{47}$	$k_{46}k_{45}k_{44}k_{43}$	$k_{42}k_{41}k_{40}k_{39}$	$k_{38}k_{37}k_{36}k_{35}$
Round 19	$k_{37}k_{36}k_{35}k_{34}$	$k_{33}k_{32}\underline{k_{31}k_{30}}$	$k_{29}k_{28}k_{27}k_{26}$	$k_{25}k_{24}k_{23}k_{22}$	$k_{21}k_{20}k_{19}k_{18}$	$k_{17}k_{16}k_{15}k_{14}$	$k_{13}k_{12}k_{11}k_{10}$	$k_9k_8k_7k_6$
Round 20	$k_8k_7k_6k_5$	$k_4k_3k_2k_1$	$k_0k_{79}k_{78}k_{77}$	$k_{76}k_{75}k_{74}k_{73}$	$k_{72}k_{71}k_{70}k_{69}$	$k_{68}k_{67}k_{66}k_{65}$	$k_{64}k_{63}k_{62}k_{61}$	$\underline{k_{60}k_{59}}k_{58}k_{57}$
Round 21	$k_{59}k_{58}k_{57}k_{56}$	$k_{55}k_{54}k_{53}k_{52}$	$k_{51}k_{50}k_{49}k_{48}$	$k_{47}k_{46}k_{45}k_{44}$	$k_{43}k_{42}k_{41}k_{40}$	$k_{39}k_{38}k_{37}k_{36}$	$k_{35}k_{34}k_{33}k_{32}$	$k_{31}k_{30}k_{29}k_{28}$
Round 22	$k_{30}k_{29}k_{28}k_{27}$	$k_{26}k_{25}k_{24}k_{23}$	$k_{22}k_{21}k_{20}k_{19}$	$k_{18}k_{17}k_{16}k_{15}$	$k_{14}k_{13}k_{12}k_{11}$	$k_{10}k_9k_8k_7$	$k_6k_5k_4k_3$	$k_2k_1k_0k_{79}$

If the subkeys are guessed correctly, there exist one pair of 22-round ciphertexts satisfies the key-recovery differential, when the 2^{46} pairs of 22-round ciphertexts are decrypted from round 22 to round 17.

In the procedure of our key recovery, the adversary can partially decrypt one nibble each time. For better understanding, the relations among the subkey bits in the partial decryptions are described in Table 4. The procedure of the attack is described as follows.

1. encrypt $2^{63.1}$ pairs of plaintexts with a difference of Δ_3.
2. For the $2^{63.1}$ pairs of output, the adversary chooses the pairs that satisfy difference Δ_2. Without loss of generality, one pair satisfies Δ_2 with a probability of $(15/16)^{12} \times (1/16)^4 \approx 2^{-17.1}$. Thus, there remain 2^{46} pairs satisfy difference Δ_2.
3. The partial decryption of round 22 involves $subkey^0_{22}$, $subkey^2_{22}$, $subkey^3_{22}$, $subkey^4_{22}$, $subkey^5_{22}$, $subkey^6_{22}$, $subkey^7_{22}$.
   (a) For every guess of $subkey^0_{22}$, the adversary partially decrypts the 2-th nibble of $V_{23,l}$ of the 2^{46} pairs of 22-round ciphertexts and verifies if the difference of the decrypted nibbles equal to zero. Since this verification has one vanished condition, there remain $2^{46} \times 2^{-3.9} = 2^{42.1}$ pairs.
   (b) In similar, the partial decryption of the 1,5,7-th nibble of $V_{23,l}$ require three vanished condition. Consequently, there remain $2^{42.1} \times 2^{-3.9\times 3} = 2^{30.4}$ pairs.
   (c) For every guess of 12 bits ($subkey^2_{22}$, $subkey^4_{22}$, $subkey^5_{22}$), the adversary partially decrypts the 3,4,6-th nibbles of $V_{23,l}$ of the $2^{30.4}$ pairs and verify whether the differences of the decrypted nibbles not equal to zero. Since this verification has one unvanished condition, there remain $2^{30.4} \times 2^{-0.1} = 2^{30.3}$ pairs.

   After the partial decryption of round 22, there remain about $2^{30.3}$ pairs of 21-round ciphertexts, which satisfy $(\Delta V_{22,l}, \Delta V_{22,r})$ =($XX00XX0X$ $000X00XX0$).
4. The partial decryption of round 21 involves $subkey^0_{21}$, $subkey^1_{21}$, $subkey^2_{21}$, $subkey^4_{21}$, $subkey^6_{21}$. As shown in Table 4, the three subkey bits ($subkey^{0,0}_{21}$, $subkey^{0,1}_{21}$, $subkey^{0,2}_{21}$) can be obtained from $subkey^7_{22}$. Thus, the adversary needs to guess 17 bits in $subkey_{21}$. Similar to the decryption of round 22, the decryption of round 21 partially decrypt the 0,3,6-th nibbles of $V_{22,l}$. It requires three vanished condition. Then the adversary partially decrypts other nibbles in the decryption of round 21. Since this step has three vanished conditions and one unvanished condition, there remain about $2^{30.3} \times 2^{-11.8} = 2^{18.5}$ pairs of 20-round outputs after this verification, which satisfy $(\Delta V_{21,l}, \Delta V_{21,r})$=($000X0XX0$ $00X0000X$).
5. The partial decryption of round 20 involves $subkey^0_{20}$, $subkey^3_{20}$, $subkey^5_{20}$. As shown in Table 4, the two subkey bits ($subkey^{5,3}_{20}$, $subkey^{5,2}_{20}$) can be obtained from $subkey^{0,1}_{22}$, $subkey^{0,0}_{22}$. Thus, the adversary needs to guess 10 bits in $subkey_{20}$.
   Similar to the decryption of round 22, the adversary partially decrypts the 2,4-th nibble of $V_{21,l}$. It requires two vanished condition, and then the decryption of round 20 partially decrypts the 1-th nibble of $V_{21,l}$. Since this step has two vanished conditions, there remain $2^{18.5} \times (2^{-3.9})^2 = 2^{10.7}$ pairs of 19-round outputs after this verification, which satisfy $(\Delta V_{20,l}, \Delta V_{20,r})$ = ($00X0000X$ $X0000000$).
6. The partial decryption of round 19 involves $subkey^1_{19}$ and $subkey^7_{19}$. As shown in Table 4, $subkey^1_{19}$ can be obtained from ($subkey^{3,2}_{22}$, $subkey^{3,1}_{22}$, $subkey^{3,0}_{22}$, $subkey^{2,3}_{22}$) and $subkey^7_{19}$ can be obtained from ($subkey^{2,1}_{21}$, $subkey^{2,0}_{21}$, $subkey^{1,3}_{21}$, $subkey^{1,2}_{21}$) directly. Thus, no subkey nibbles need to be guessed.

After the partial decryption of round 19, the adversary verifies if the pairs of 18-round outputs satisfy $(\Delta V_{19,l}, \Delta V_{19,r}) = (X0000000, 0X000000)$. Since this step requires one vanished conditions, there remain $2^{10.7} \times 2^{-3.9} = 2^{6.8}$ pairs of 18-round outputs after this verification.

7. The partial decryption of round 18 involves $subkey_{18}^{4}$ and $subkey_{18}^{6}$. As shown in Table 4, $subkey_{18}^{6,1}$ can be obtained from $subkey_{20}^{0,3}$ and $subkey_{18}^{6,0}$ can be obtained from $subkey_{20}^{0,2}$ directly. Thus, the adversary needs to guess 6 bits of $subkey_{18}$.
   Similar to the decryption of round 22, the decryption of round 18 partially decrypt the 7-th nibble of $V_{19,l}$. It requires one vanished condition and the decryption of round 18 partially decrypt the 6-th nibble of $V_{19,l}$. Since this step requires one vanished conditions, there remain $2^{6.8} \times 2^{-3.9} = 2^{2.9}$ pairs of 17-round outputs after this verification, which satisfy $(\Delta V_{18,l}, \Delta V_{18,r}) = (0X000000, 000X0000)$.
8. the partial decryption of round 17 involves $subkey_{17}^{4}$. As shown in Table 4, ($subkey_{17}^{4,2}$, $subkey_{17}^{4,1}$ and $subkey_{17}^{4,0}$) can be obtained from ($subkey_{22}^{0,3}$, $subkey_{22}^{0,2}$, $subkey_{22}^{0,1}$). Thus, the adversary needs to guess 1 bit of $subkey_{17}$.
   For every guess of the 1-bit subkey partially decrypt round 17 to verify if the pairs of 16-round outputs satisfy $\Delta_1 = (\Delta V_{17,l}, \Delta V_{17,r}) = (000X0000, 00000000)$. Since this step has one vanished conditions, there exists one pair of 16-round outputs that satisfies difference Δ_1 with a probability of $2^{2.9} \times 2^{-3.9} = 2^{-1}$.
9. After the decryption of round 17, if there exists one pairs of 16-round outputs satisfy Δ_1, the adversary knows he has successfully recovered 62 subkey bits. The left 18 bits of the master key can be recovered by exhaustive searches.

Considering the equation of $s_8(0x2) = 0x2$ in $subkey_{10}$ has been satisfied, the adversary just needs to guess 2^2 pairs of $subkey_{18}^{4}$. According to the key schedule of LBlock, the 2^2 pairs of $subkey_{18}^{4}$ are obtained from the equation of $s_8(0x2) = 0x2$. In similar, the adversary only needs to guess 2^3 pairs of $subkey_{21}^{6}$.

The time complexity of the above partial decryption is about 2^{67}. Therefore, the 80-bit master key can be recovered with the time complexity of about $2^{67} + 2^{64} + 2^{18} \approx 2^{67}$. Since $2^{63.1}$ pairs of ciphertexts need to be stored during the attack, the data complexity of our key recovery attack is about $2^{64.1}$. Although the whole codebook is 2^{64} for a 64-bit cipher, the related-key pairs allow the attacker access $2 * 2^{64}$ pairs of plaintext and ciphertext. After the partial decryption of round 17, there exists one pair with a probability of 2^{-1}. Thus the success probability of our key recovery attack is 2^{-1}.

5 Conclusions

In this paper, we have proposed new related-key differential attacks on the reduced-round LBlock. First we constructed a boomerang distinguishing attack on 16-round LBlock, which exploits the slow diffusion of the key schedule. Then we presented a key recovery attack on 22-round LBlock by using the 16-round related-key truncated differential. Compares to the known results, the time and data complexities of our key recovery attack are both reduced. Although our attacks do not threaten the practical security of LBlock, future work may seek to extend the existing attacks to more rounds LBlock based on our related-key differentials.

References

1. Biham, E.: New types of cryptanalytic attacks using related keys. J. Cryptology 7(4), 229–246 (1994)
2. Biham, E., Dunkelman, O., Keller, N.: Related-Key Boomerang and Rectangle Attacks. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 507–525. Springer, Heidelberg (2005)
3. Biryukov, A., Nikolic, I., Roy, A.: Boomerang Attacks on BLAKE-32. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 218–237. Springer, Heidelberg (2011)
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: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
5. De Cannière, C., Dunkelman, O., Knežević, M.: KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 272–288. Springer, Heidelberg (2009)
6. Gong, Z., Nikova, S., Law, Y.W.: KLEIN: A New Family of Lightweight Block Ciphers. In: Juels, A., Paar, C. (eds.) RFIDSec 2011. LNCS, vol. 7055, pp. 1–18. Springer, Heidelberg (2012)
7. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.J.B.: The led block cipher. In: Preneel and Takagi [10], pp. 326–341
8. Lamberger, M., Mendel, F.: Higher-order differential attack on reduced sha-256. IACR Cryptology ePrint Archive, 37 (2011)
9. Minier, M., Naya-Plasencia, M.: A related key impossible differential attack against 22 rounds of the lightweight block cipher lblock. Inf. Process. Lett. 112(16), 624–629 (2012)
10. Preneel, B., Takagi, T. (eds.): CHES 2011. LNCS, vol. 6917, pp. 2011–2013. Springer, Heidelberg (2011)
11. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: Piccolo: An ultra-lightweight blockcipher. In: Preneel and Takagi [10], pp. 342–357
12. Suzaki, S.M.T., Minematsu, K., Kobayashi, E.: Twine: A lightweight, versatile block cipher. In: ECRYPT Workshop on Lightweight Cryptography (2011)
13. Wagner, D.: The Boomerang Attack. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999)
14. Wu, W., Zhang, L.: LBlock: A Lightweight Block Cipher. In: Lopez, J., Tsudik, G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 327–344. Springer, Heidelberg (2011)
15. Wu, W., Zhang, L.: Lblock: A lightweight block cipher *. Cryptology ePrint Archive, Report 2011/345 (2011), http://eprint.iacr.org