Improved Impossible Differential Attack on Reduced-Round LBlock

Ning Wang[1,2], Xiaoyun Wang[1,2,3(✉)], and Keting Jia[4]

[1] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China
[2] School of Mathematics, Shandong University, Jinan 250100, China
wangning2012@mail.sdu.edu.cn
[3] Institute for Advanced Study, Tsinghua University, Beijing 100084, China
xiaoyunwang@mail.tsinghua.edu.cn
[4] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
ktjia@tsinghua.edu.cn

Abstract. LBlock is a 32-round lightweight block cipher with a 64-bit block size and an 80-bit key. This paper presents a new impossible differential attack on LBlock by improving the previous best result for 1 more round. Based on the nibble conditions, detailed differential properties of LBlock S-Boxes and thorough exploration of subkey relations, we set up well precomputation tables to collect the data needed and propose an optimal key-guessing arrangement to effectively reduce the time complexity of the attack. With these techniques, we launch an impossible differential attack on 24-round LBlock. To the best of our knowledge, this attack is currently the best in terms of the number of rounds attacked (except for biclique attacks).

Keywords: Lightweight block cipher · LBlock · Impossible differential cryptanalysis

1 Introduction

In the past few years, the wide applications of RFID tags and sensor networks have stimulated the needs of lightweight cryptographic primitives that require very limited resources (the area size on the chip, memory, power consumption etc.) while still providing good security. In accordance with this tendency, many lightweight block ciphers were proposed, such as TWINE [19], PRESENT [4], LED [7], LBlock [23], SIMON and SPECK [2] etc. For all of them, LBlock is a relatively recent proposal and its security analysis is still under the heated discussions.

N. Wang—Supported by National Key Basic Research Program of China (Grant No. 2013CB834205), and the National Natural Science Foundation of China (Grant No. 61133013 and 61402256).

S. Kwon and A. Yun (Eds.): ICISC 2015, LNCS 9558, pp. 136–152, 2016.
DOI: 10.1007/978-3-319-30840-1_9

The LBlock block cipher was introduced by Wu and Zhang at ACNS 2011 [23] and the designers gave corresponding cryptanalysis. As a lightweight primitive, LBlock has 64-bit block size and 80-bit key length. Since its proposal, the security of LBlock has been analyzed by various cryptanalysis methods, such as differential [11], impossible differential [5,6,8,12,14,22,23], integral [16,17,23], zero-correlation linear [18,20], cube cryptanalysis [10], biclique attacks [1,21] and so on.

Impossible differential cryptanalysis was independently introduced by Knudsen [9] and Biham et al. [3], which allowed the adversary to discard wrong keys as many as possible by distinguishing the impossible differential characteristics, and exhaustively search the rest of the keys. Up to date, the impossible differential attack is a relatively effective method in terms of attacked rounds of LBlock. Boura et al. proposed the latest impossible differential result to attack 23-round LBlock with a time complexity $2^{75.36}$ and a data complexity 2^{59} [5,6]. In [6], the authors provided new generic formulas to compute the data, time and memory complexities of impossible differential attacks. As to LBlock specifically, they presented some new key-bridging techniques for discarding wrong keys and therefore improved the time and data complexities of their attack. Boura et al.'s work simplified the computation of impossible differential cryptanalysis by a general equation. By comprehensive studying on their works of LBlock and utilizing the 14-round impossible differential in [6], we further found that the time complexity could be improved.

Our Contributions. The contributions of this paper are summarized in three folds as follows:

- In this paper, we thoroughly explore the relations of the subkeys involved to find an optimal arrangement for key guessing. Based on this and some precomputations, a new key-guessing technique based on nibble is proposed to reduce the guessed key space greatly, which is similar to dynamic key-guessing technique [15] that is valid for block ciphers based on bit operations such as SIMON.
- We make a more detailed investigation of the differential properties of S-Boxes. These properties enable us to build some precomputation tables that help us to collect available plaintext (ciphertext) pairs more efficiently and simplify the operations in the online phase.
- The number of bit-conditions ascends to 88 after extending the 14-round impossible differential to attack 24-round LBlock. According to the formulas given in [6], the smallest amount of input (or output) pairs N should be approximately 2^{88} so that the 24-round attack is seemingly unavailable. We lower the high data complexity and make the 24-round attack a success with $2^{77.50}$ encryptions and 2^{59} chosen plaintexts by using our techniques.

Table 1 outlines our impossible differential attack on 24-round LBlock compared with some previous cryptanalysis.

This paper is organized as follows, Sect. 2 reviews the LBlock cipher and investigates detailed differential properties of S-Boxes used in round function.

Table 1. Summary of some main attacks on LBlock

Model	Attacks	Rounds	Time	Data	Memory	Reference
Single-key	Impossible differential	20	$2^{72.7}$	$2^{63}CP$	2^{68}	[23]
		21	$2^{73.7}$	$2^{62.5}CP$	$2^{55.5}$	[12]
		21	$2^{69.5}$	$2^{63}CP$	2^{75}	[8]
		22	$2^{79.28}$	$2^{58}CP$	2^{76}	[8]
		23	$2^{75.36}$	$2^{59}CP$	2^{74}	[6]
		24	$2^{77.50}$	$2^{59}CP$	2^{75}	Sect. 3
	Integral	22	$2^{70.54}$	$2^{64}CP$	N/A	[23]
		22	$2^{71.27}$	$2^{62.1}CP$	2^{35}	[17]
		22	2^{79}	$2^{60}CP$	2^{63}	[16]
	Zero-correlation linear	20	$2^{63.7}$	$2^{64}KP$	2^{64}	[18]
		20	$2^{39.6}$	$2^{63.6}KP$	2^{64}	[18]
		22	2^{70}	$2^{61}KP$	2^{64}	[18]
		23	2^{76}	$2^{62.1}KP$	2^{60}	[20]
	Biclique attack	32	$2^{78.4}$	$2^{52}CP$	2^{8}	[21]
		32	$2^{78.338}$	$2^{2}KP$	$2^{7}FC$	[1]
Related-key	Differential	22	2^{67}	$2^{63.1}RKCP$	N/A	[11]
	Impossible differential	22	2^{70}	$2^{47}RKCP$	N/A	[14]
		23	$2^{78.3}$	$2^{61.4}RKCP$	$2^{61.4}$	[22]

CP: Chosen Plaintext; KP: Known Plaintext; $RKCP$: Related-Key Chosen Plaintext.

We give detailed analysis on 24-round LBlock in Sect. 3. Section 4 concludes the paper.

2 Preliminaries

In the first part of this section, we make a brief description of LBlock. In the second part, we present some detailed properties about LBlock S-Boxes which are helpful to launch our impossible differential attack.

2.1 Description of LBlock

Encryption Algorithm. LBlock adopts a 64-bit block with an 80-bit key, which is a variant of 32-round Feistel network. Let $P = L_0||R_0$ be the 64-bit plaintext, $L_{i-1}||R_{i-1}$ be the input of the i-th round, $L_i||R_i$ be the output, K_i be the subkey of the i-th round, and $L_i = (X_7^i, ..., X_0^i)$, $R_i = (X_{15}^i, ..., X_8^i)$, where $X_j^i (0 \leq j \leq 15)$ are 4-bit nibbles. We denote the j-th nibble subkey of i-th round as k_j^i. Then the data processing procedure is expressed as follows.

1. For $i = 1, 2, ..., 32$, do

$$L_i = F(L_{i-1}, K_i) \oplus (R_{i-1} \lll 8),$$
$$R_i = L_{i-1}$$

2. $C = (R_{32}, L_{32})$ as the 64-bit ciphertext.

Round Function. The round function F of LBlock is composed of three basic operations: subkey addition, S-Box transformation and nibble permutation. There are 8 different 4-bit bijective S-Boxes $(S_7, S_6, ..., S_0)$ in S-Box transformation. The round function is shown in Fig. 1.

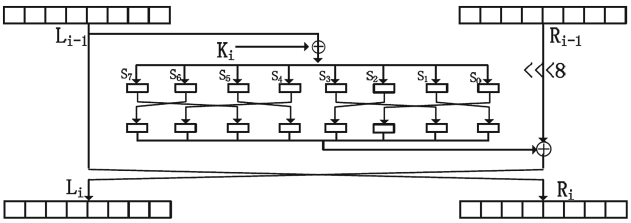

Fig. 1. Round function of LBlock

Key Schedule. The key schedule function takes an 80-bit masterkey K, and produces 32-bit subkeys for each round. Let $K^i (i = 1, ..., 32)$ be an 80-bit internal state for the key schedule function for the i-th round. Then, the 32-bit subkeys $K_i (i = 1, ..., 32)$ are derived as follows.

- $K^1 \leftarrow K$;
- $K_1 \leftarrow K^1[79, ..., 48]$;
- for $i = 2, ..., 32$ do
  - $K^i \leftarrow K^{i-1} \lll 29$;
  - $K^i[79, 78, 77, 76] \leftarrow S_9(K^i[79, 78, 77, 76])$;
  - $K^i[75, 74, 73, 72] \leftarrow S_8(K^i[75, 74, 73, 72])$;
  - $K^i[50, ..., 46] \leftarrow K^i[50, ..., 46] \oplus [i-1]_2$, where $[i-1]_2$ is the binary representation of $i - 1$;
  - $K_i \leftarrow K^i[79, ..., 48]$.

2.2 Observations on Differential Properties of S-Boxes

Some differential properties of LBlock S-Boxes have been given in [5]. Let A, B be the input and output of S-Boxes, i.e. $B = S_i(A)$ $(i = 0, ..., 7)$, and $\Delta A, \Delta B$ be the input and output differences respectively. We represent $\Delta A \xrightarrow{S_i} \Delta B$ for the pair $(\Delta A, \Delta B)$ satisfying difference transition of S_i excluding $(\Delta A, \Delta B) = (0, 0)$, which is available for difference transition of S_i.

Property 1. *(from [5]) For any given ΔA and ΔB, the probability $P_r\{\Delta A \xrightarrow{S_i} \Delta B\} = \frac{96}{256} \approx 2^{-1.41}$. For each differential pair $(\Delta A, \Delta B)$ satisfying following conditions,*

$$\begin{cases} S_i(A) \oplus S_i(A \oplus \Delta A) = \Delta B, \\ (\Delta A, \Delta B) \neq (0, 0). \end{cases} \tag{1}$$

there are on average $\frac{240}{96} \approx 2^{1.32}$ values that verify condition (1).

In this paper, we further investigate the detailed differential distribution tables of S-Boxes that draw connections between differences and exact values, and give the more detailed differential properties of LBlock S-Boxes which are useful in impossible differential attack of LBlock similar to the early abort technique proposed by Lu et al. [13]. For example, the detailed differential distribution table of S_0 is given in Table 5 in Appendix A.

Property 2. *For condition (1), the following differential properties of S-Boxes are derived:*

- *If* $\Delta A \neq 0$*, then the probability* $P_r\{\Delta A \xrightarrow{S_i} \Delta B \mid \Delta A \neq 0\} = \frac{96}{240} \approx 2^{-1.32}$*. Similarly,* $P_r\{\Delta A \xrightarrow{S_i} \Delta B \mid \Delta B \neq 0\} = \frac{96}{240} \approx 2^{-1.32}$*.*
- *If* $\Delta A \neq 0$ *and* $\Delta B \neq 0$*, then the probability* $P_r\{\Delta A \xrightarrow{S_i} \Delta B \mid \Delta A \neq 0, \Delta B \neq 0\} = \frac{96}{225} \approx 2^{-1.22}$*.*
- *Furthermore, for condition (1), when input and output differences of a S-Box are known, we could directly get the input values that satisfy the differential transition of the S-Box by looking up the detailed differential distribution tables.*

Example. For the differential equation $\Delta S_1(X_1^0 \oplus k_1^1) \oplus \Delta X_{14}^0 = 0$, and the given $(\Delta X_1^0, \Delta X_{14}^0)$ make the equation hold, we could directly get about $2^{1.32}$ values of $X_1^0 \oplus k_1^1$ by accessing the detailed differential distribution table of S_1. Furthermore, if X_1^0 is known, then corresponding values of k_1^1 that satisfy the differential equation could be also obtained by one table looking up.

3 Impossible Differential Cryptanalysis of 24-Round LBlock

In this section, we describe our attack on 24-round LBlock by utilizing the 14-round impossible differential in [6]. In the remainder of this paper, we denote a zero-difference nibble by "0", nonzero-difference nibble by "1" and unknown-difference (either 0 or 1) by "∗". Therefore, the 14-round impossible differential characteristic is represented as: $(00000000, 00001000) \nrightarrow (00000100, 00000000)$.

Before introducing the whole attack, we thoroughly explore the relations of the subkeys and build some precomputation tables. Based on these, we present an efficient data collection and a new key-guessing technique to mount an impossible differential attack on 24-round LBlock.

3.1 Conditions of Extended Impossible Differential Paths

We add 5 rounds to the top and bottom of the 14-round impossible differential respectively to attack 24-round LBlock (see Fig. 2). We find the sufficient nibble conditions to conform the extended 10-round differential propagation. Then,

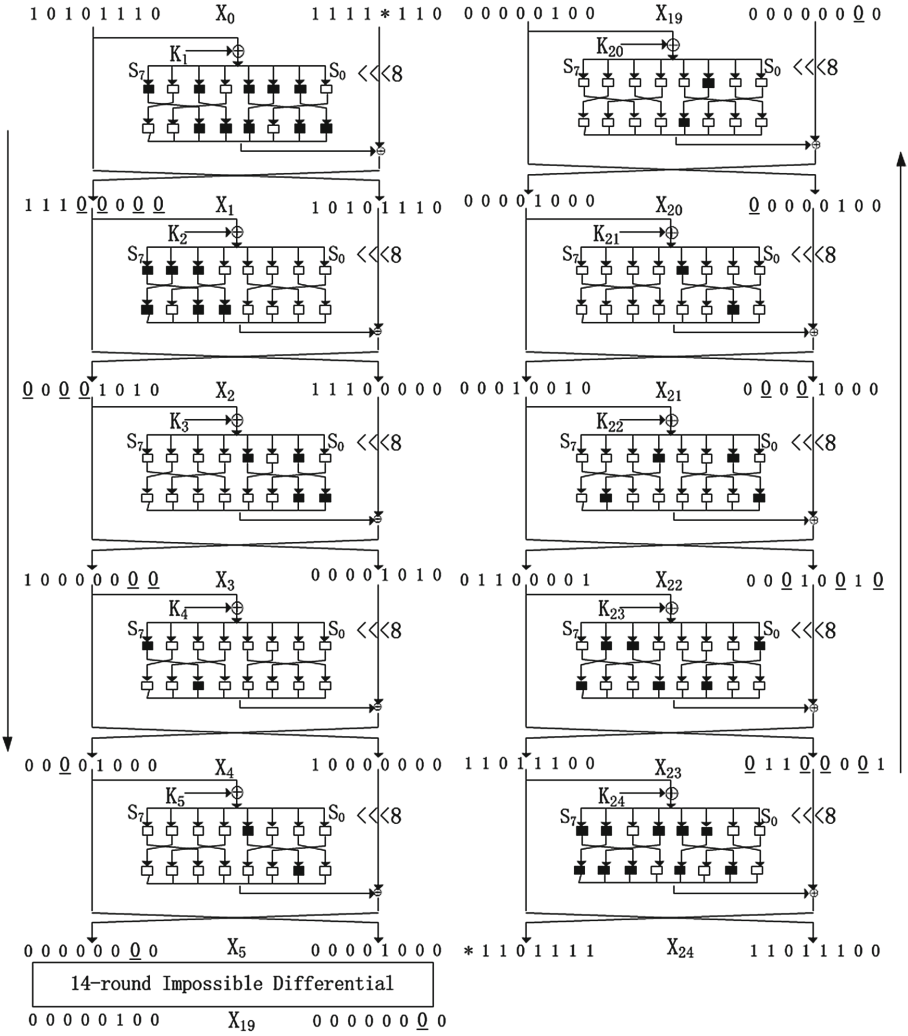

Fig. 2. Impossible differential attack against 24-round LBlock

we deduce the differential equations related to subkeys for chosen plaintext-ciphertext pairs from the nibble conditions. These equations are effective for filtering the incorrect subkey candidates. The acquired conditions, corresponding differential equations and subkeys involved in conditions are listed in Table 2. (**subkeys in bold** mean that the subkeys also involve in some other rounds).

3.2 Relationship Among Involved Subkeys

We reveal that 75 bits of key-information are well enough to deduce all the subkeys involved in the conditions by thoroughly exploring the relations among

Table 2. Differential conditions of extended impossible differential paths

Round	Nibble conditions (differential equations)	Subkeys involved in conditions	Known equations
1	$\Delta X_0^1 = 0 : \Delta S_1(X_1^0 \oplus k_1^1) \oplus \Delta X_{14}^0 = 0$	$\mathbf{k_1^1}$	
	$\Delta X_1^1 = 0 : \Delta S_3(X_3^0 \oplus k_3^1) \oplus \Delta X_{15}^0 = 0$	$\mathbf{k_3^1}$	
	$\Delta X_3^1 = 0 : \Delta S_2(X_2^0 \oplus k_2^1) \oplus \Delta X_9^0 = 0$	$\mathbf{k_2^1}$	
	$\Delta X_4^1 = 0 : \Delta S_5(X_5^0 \oplus k_5^1) \oplus \Delta X_{10}^0 = 0$	$\mathbf{k_5^1}$	
2	$\Delta X_4^2 = 0 : \Delta S_5(X_5^1 \oplus k_5^2) \oplus \Delta X_2^0 = 0$	k_5^2,$\mathbf{k_7^1}$	
	$\Delta X_5^2 = 0 : \Delta S_7(X_7^1 \oplus k_7^2) \oplus \Delta X_3^0 = 0$	k_7^2,k_6^1	$\Delta X_7^1 = \Delta X_{13}^0$
	$\Delta X_7^2 = 0 : \Delta S_6(X_6^1 \oplus k_6^2) \oplus \Delta X_5^0 = 0$	k_6^2,k_4^1	$\Delta X_6^1 = \Delta X_{12}^0$
3	$\Delta X_0^3 = 0 : \Delta S_1(X_1^2 \oplus k_1^3) \oplus \Delta X_{12}^0 = 0$	k_1^3,$\mathbf{k_3^2}$,$\mathbf{k_2^1}$	$\Delta X_1^2 = \Delta X_7^0$
	$\Delta X_1^3 = 0 : \Delta S_3(X_3^2 \oplus k_3^3) \oplus \Delta X_{13}^0 = 0$	k_3^3,k_2^2,k_0^1	$\Delta X_3^2 = \Delta X_1^0$
4	$\Delta X_5^4 = 0 : \Delta S_7(X_7^3 \oplus k_7^4) \oplus \Delta X_1^0 = 0$	k_7^4,k_6^3,k_4^2,$\mathbf{k_5^1}$,$\mathbf{k_7^1}$	$\Delta X_7^3 = \Delta X_5^1$
5	$\Delta X_1^5 = 0$	k_3^5, k_2^4, k_0^3, k_1^2,	$\Delta X_3^4 = \Delta X_7^0$
	$\Delta S_3(X_3^4 \oplus k_3^5) \oplus \Delta X_5^1 = 0$	$\mathbf{k_3^2}$, $\mathbf{k_2^1}$, $\mathbf{k_3^1}$, $\mathbf{k_1^1}$, $\mathbf{k_7^1}$	
23	$\Delta X_9^{23} = 0 : \Delta S_2(X_{10}^{24} \oplus k_2^{24}) \oplus \Delta X_3^{24} = 0$	$\mathbf{k_2^{24}}$	
	$\Delta X_{11}^{23} = 0 : \Delta S_7(X_{15}^{24} \oplus k_7^{24}) \oplus \Delta X_5^{24} = 0$	$\mathbf{k_7^{24}}$	
	$\Delta X_{12}^{23} = 0 : \Delta S_4(X_{12}^{24} \oplus k_4^{24}) \oplus \Delta X_6^{24} = 0$	$\mathbf{k_4^{24}}$	
	$\Delta X_{15}^{23} = 0 : \Delta S_3(X_{11}^{24} \oplus k_3^{24}) \oplus \Delta X_1^{24} = 0$	$\mathbf{k_3^{24}}$	
22	$\Delta X_{10}^{22} = 0 : \Delta S_5(X_{13}^{23} \oplus k_5^{23}) \oplus \Delta X_{12}^{24} = 0$	k_5^{23},$\mathbf{k_6^{24}}$	
	$\Delta X_8^{22} = 0 : \Delta S_0(X_8^{23} \oplus k_0^{23}) \oplus \Delta X_{10}^{24} = 0$	k_0^{23},k_0^{24}	$\Delta X_8^{23} = \Delta X_2^{24}$
	$\Delta X_{13}^{22} = 0 : \Delta S_6(X_{14}^{23} \oplus k_6^{23}) \oplus \Delta X_{15}^{24} = 0$	k_6^{23},k_1^{24}	$\Delta X_{14}^{23} = \Delta X_0^{24}$
21	$\Delta X_{12}^{21} = 0 : \Delta S_4(X_{12}^{22} \oplus k_4^{22}) \oplus \Delta X_0^{24} = 0$	k_4^{22},$\mathbf{k_4^{23}}$, $\mathbf{k_4^{24}}$	$\Delta X_{12}^{22} = \Delta X_{14}^{24}$
	$\Delta X_{14}^{21} = 0 : \Delta S_1(X_9^{22} \oplus k_1^{22}) \oplus \Delta X_2^{24} = 0$	k_1^{22},k_2^{23},k_5^{24}	$\Delta X_9^{22} = \Delta X_{11}^{24}$
20	$\Delta X_{15}^{20} = 0 : \Delta S_3(X_{11}^{21} \oplus k_3^{21}) \oplus \Delta X_{11}^{24} = 0$	k_3^{21},k_7^{22},k_3^{23},$\mathbf{k_7^{24}}$, $\mathbf{k_6^{24}}$	$\Delta X_{11}^{21} = \Delta X_{13}^{23}$
19	$\Delta X_9^{19} = 0$	k_2^{20},k_5^{21},k_6^{22},k_1^{23},	$\Delta X_{10}^{20} = \Delta X_{14}^{24}$
	$\Delta S_2(X_{10}^{20} \oplus k_2^{20}) \oplus \Delta X_{13}^{23} = 0$	$\mathbf{k_4^{23}}$, $\mathbf{k_4^{24}}$, $\mathbf{k_2^{24}}$, $\mathbf{k_3^{24}}$, $\mathbf{k_6^{24}}$	

subkeys. This enable us to find an optimal arrangement for key guessing in key recovery in order to reduce the time complexity of the attack. We show relations among subkeys involved in conditions and the masterkey in Table 3.

For a S-Box S and its input x, we denote the 4 output bits by $(S(x)^0, S(x)^1, S(x)^2, S(x)^3)$, simply as $((x)^0, (x)^1, (x)^2, (x)^3)$. In LBlock, a subkey bit may be both the s-th output bit of a S-Box and the boolean function of partial masterkey bits $K[i \sim j]$. On this occasion, we denote such a bit by $K(i \sim j)^s$. For example, $k_7^2 = S_9(47, 48, 49, 50)$, we denote its 4 bits by $S_9(47, 48, 49, 50)^0$, $S_9(47, 48, 49, 50)^1$, $S_9(47, 48, 49, 50)^2$, $S_9(47, 48, 49, 50)^3$ or simply $(47 \sim 50)^0$, $(47 \sim 50)^1$, $(47 \sim 50)^2$, $(47 \sim 50)^3$ without causing ambiguities.

3.3 Precomputation

Firstly, in the remainder of this paper, we refer a pair that makes an equation hold as an *available pair* for this equation. From Table 2, we observe that

Table 3. Relations among subkeys involved in conditions and masterkeys

Round	Relations between subkeys and masterkeys
1	$\mathbf{k_1^1} : (\mathbf{55}, \mathbf{54}, \mathbf{53}, \mathbf{52})$
	$\mathbf{k_3^1} : (\mathbf{63}, \mathbf{62}, \mathbf{61}, \mathbf{60})$
	$\mathbf{k_2^1} : (\mathbf{59}, \mathbf{58}, \mathbf{57}, \mathbf{56})$
	$\mathbf{k_5^1} : (\mathbf{71}, \mathbf{70}, \mathbf{69}, \mathbf{68})$
2	(k_5^2: $(42, 41, 40, 39)$, $\mathbf{k_7^1} : (\mathbf{79}, \mathbf{78}, \mathbf{77}, \mathbf{76})$)
	k_7^2: $S_9(47, 48, 49, 50)$, k_6^1: $(75, 74, 73, 72)$
	k_6^2: $S_8(43, 44, 45, 46)$, k_4^1: $(67, 66, 65, 64)$
3	k_1^3: $(77, 76, 75, 74)$,$\mathbf{k_3^2} : (\mathbf{34}, \mathbf{33}, \mathbf{32}, \mathbf{31})$, $\mathbf{k_2^1}$
	k_3^3: $(5, 4, 3, 2)$, k_2^2: $(30, 29, 28, 27)$, k_0^1: $(51, 50, 49, 48)$
4	k_7^4: $(S_9(69, 70, 71, 72)$, k_6^3: $(S_8(14, 15, 16, 17)$, k_4^2: $(38, 37, 36, 35)$, $\mathbf{k_5^1}, \mathbf{k_7^1}$
5	k_3^5: $(27, 26, 25, 24)$, k_2^4:$(52,51,(S_9(47, 48, 49, 50)^0, S_9(47, 48, 49, 50)^1)$,
	k_0^3: $(73, 72, 71, 70)$, k_1^2: $(26, 25, 24, 23)$, $\mathbf{k_3^2}, \mathbf{k_2^1}, \mathbf{k_3^1}, \mathbf{k_1^1}, \mathbf{k_7^1}$
23	$\mathbf{k_2^{24}} : ((\mathbf{29} \sim \mathbf{39})^{\mathbf{1}}, (\mathbf{29} \sim \mathbf{39})^{\mathbf{2}}, (\mathbf{26} \sim \mathbf{39})^{\mathbf{0}}, (\mathbf{26} \sim \mathbf{39})^{\mathbf{1}})$
	$\mathbf{k_7^{24}} : \mathbf{S_9}((\mathbf{47} \sim \mathbf{61})^{\mathbf{0}}, (\mathbf{47} \sim \mathbf{61})^{\mathbf{1}}, (\mathbf{47} \sim \mathbf{61})^{\mathbf{2}}, (\mathbf{47} \sim \mathbf{61})^{\mathbf{3}})$
	$\mathbf{k_4^{24}} : ((\mathbf{36} \sim \mathbf{46})^{\mathbf{0}}, (\mathbf{36} \sim \mathbf{46})^{\mathbf{1}}, (\mathbf{36} \sim \mathbf{46})^{\mathbf{2}}, (\mathbf{33} \sim \mathbf{46})^{\mathbf{0}})$
	$\mathbf{k_3^{24}} : ((\mathbf{33} \sim \mathbf{46})^{\mathbf{1}}, (\mathbf{33} \sim \mathbf{46})^{\mathbf{2}}, (\mathbf{33} \sim \mathbf{46})^{\mathbf{3}}, (\mathbf{29} \sim \mathbf{39})^{\mathbf{0}})$
22	k_5^{23}: $((69 \sim 76)^0, (69 \sim 76)^1, (69 \sim 76)^2, (69 \sim 76)^3)$,
	$\mathbf{k_6^{24}} : \mathbf{S_8}((\mathbf{43} \sim \mathbf{54})^{\mathbf{0}}, (\mathbf{43} \sim \mathbf{54})^{\mathbf{1}}, (\mathbf{43} \sim \mathbf{54})^{\mathbf{2}}, (\mathbf{43} \sim \mathbf{54})^{\mathbf{3}})$
	k_0^{23}: $((51 \sim 61)^2, (51 \sim 61)^3, (47 \sim 54)^0, 47 \sim 54)^1)$,
	k_0^{24}: $((22 \sim 32)^2, (22 \sim 32)^3, (18 \sim 25)^0, (18 \sim 25)^1)$
	k_6^{23}: $S_8((77 \sim 3)^3, (73 \sim 76)^0, (73 \sim 76)^1, (73 \sim 76)^2)$,
	k_1^{24}: $(26 \sim 39)^2, (26 \sim 39)^3, (22 \sim 32)^0, (22 \sim 32)^1)$
21	k_4^{22}: $((14 \sim 21)^0$,$(14 \sim 21)^1$,$(14 \sim 21)^2$,$(11 \sim 21)^0)$,
	$\mathbf{k_4^{23}} : ((\mathbf{65} \sim \mathbf{72})^{\mathbf{0}}, (\mathbf{65} \sim \mathbf{72})^{\mathbf{1}}, (\mathbf{65} \sim \mathbf{72})^{\mathbf{2}}, (\mathbf{62} \sim \mathbf{72})^{\mathbf{0}}), \mathbf{k_4^{24}}$
	k_1^{22}: $((4 \sim 17)^2, (4 \sim 17)^3, (0 \sim 10)^0, (0 \sim 10)^1)$,
	k_2^{23}: $((58 \sim 68)^1, (58 \sim 68)^2, (55 \sim 68)^0, (55 \sim 68)^1)$,
	k_5^{24}: $((40 \sim 50)^0, (40 \sim 50)^1, (40 \sim 50)^2, (40 \sim 50)^3)$
20	k_3^{21}: $(40 \sim 50)^1, (40 \sim 50)^2, (40 \sim 50)^3, (36 \sim 46)^0)$,
	k_7^{22}: $(26 \sim 39)^0, (26 \sim 39)^1, (26 \sim 39)^2, (26 \sim 39)^3)$,
	k_3^{23}: $(62 \sim 72)^1, (62 \sim 72)^2, (62 \sim 72)^3, (58 \sim 68)^0)$, $\mathbf{k_7^{24}}, \mathbf{k_6^{24}}$
19	k_2^{20}: $((65 \sim 72)^1, (65 \sim 72)^2, (62 \sim 72)^0, (62 \sim 72)^1)$,
	k_5^{21}: $((47 \sim 54)^0, (47 \sim 54)^1, (47 \sim 54)^2, (47 \sim 54)^3)$,
	k_6^{22}: $((22 \sim 32)^0, (22 \sim 32)^1, (22 \sim 32)^2, (22 \sim 32)^3)$,
	k_1^{23}: $((55 \sim 68)^2, (55 \sim 68)^3, (51 \sim 61)^0, (51 \sim 61)^1)$, $\mathbf{k_4^{23}}, \mathbf{k_4^{24}}, \mathbf{k_2^{24}}, \mathbf{k_3^{24}}, \mathbf{k_6^{24}}$

some conditions of extended impossible differential paths are closely related rather than independent. The input differences of some conditions could also be output differences of other conditions, and plaintext- (ciphertext-) differences have determined whether corresponding conditions held. Based on these, we construct well precomputation tables by combining some related conditions to provide higher efficiency for collecting available pairs. The connections between input/output differences and conditions of active S-Boxes are depicted in Fig. 3.

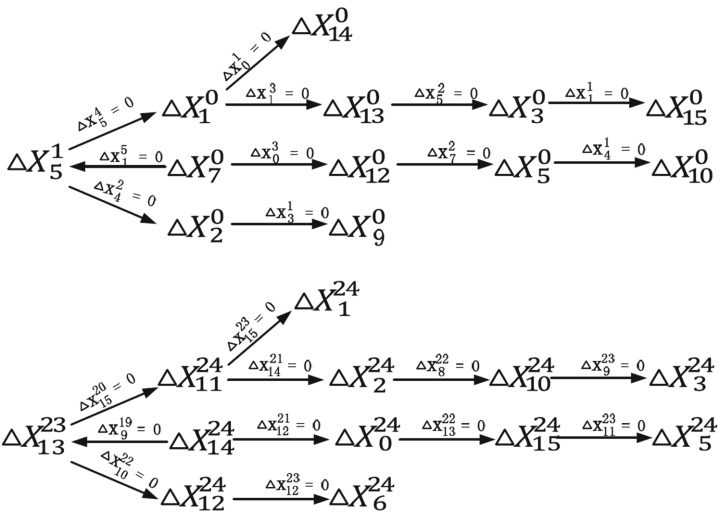

Fig. 3. Connections between input/output differences and conditions

Secondly, in order to reduce time complexity of key recovery phase, we set up five precomputation tables TK_i $(i = 1, 2, 3, 4, 5)$. When some key bits in a condition equation have been known, the other related key bits could be obtained by one table looking up rather than redundant online computations.

Precomputation Tables of Plaintext-Pairs. We first consider three conditions ($\Delta X_1^3 = 0$, $\Delta X_5^2 = 0$, $\Delta X_1^1 = 0$), and deduce follow equations,

$$\Delta S_3(X_3^2 \oplus k_3^3) \oplus \Delta X_{13}^0 = 0, \tag{2}$$

$$\Delta S_7(X_7^1 \oplus k_7^2) \oplus \Delta X_3^0 = 0, \tag{3}$$

$$\Delta S_3(X_3^0 \oplus k_3^1) \oplus \Delta X_{15}^0 = 0. \tag{4}$$

Since $\Delta X_3^2 = \Delta X_1^0$ and $\Delta X_7^1 = \Delta X_{13}^0$, the Eq. (2) holds with probability $2^{-1.41}$ for any given $(\Delta X_1^0, \Delta X_{13}^0)$ according to Property 1. When (2) holds, it is easy to verify that $\Delta X_{13}^0 \neq 0$. In this case, (3) holds with probability $2^{-1.32}$ according to Property 2. Similarly, the Eq. (4) holds with probability $2^{-1.32}$. Therefore, for any given $(\Delta X_1^0, \Delta X_{13}^0, \Delta X_3^0, \Delta X_{15}^0)$, all the three equations hold with probability $2^{-4.05}$. That is to say, for each value of $(X_1^0, X_{13}^0, X_3^0, X_{15}^0)$, there are about

$2^{11.95}$ values of ($X_1^0\prime$, $X_{13}^0\prime$, $X_3^0\prime$, $X_{15}^0\prime$) such that the corresponding differences (ΔX_1^0, ΔX_{13}^0, ΔX_3^0, ΔX_{15}^0) make all these three equations hold.

A table T_1 on nibbles (X_1^0, X_{13}^0, X_3^0, X_{15}^0) is set up. The row address of T_1 is natually

$$i = X_1^0 \| X_{13}^0 \| X_3^0 \| X_{15}^0, \tag{5}$$

the column index is

$$j = \Delta X_1^0 \| \Delta X_{13}^0 \| \Delta X_3^0 \| \Delta X_{15}^0 \tag{6}$$

where the nibble difference ($\Delta X_1^0, \Delta X_{13}^0, \Delta X_3^0, \Delta X_{15}^0$) conforms that all the three equations hold. We store ($X_1^0 \oplus \Delta X_1^0$, $X_{13}^0 \oplus \Delta X_{13}^0$, $X_3^0 \oplus \Delta X_3^0$, $X_{15}^0 \oplus \Delta X_{15}^0$) in the corresponding location of table T_1, denoted by $T_1(i, j)$. Therefore, there are 2^{16} rows, and about $2^{11.95}$ columns in each row of table T_1. The size of the table T_1 is about $2^{16} \times 2^{11.95} = 2^{27.95}$ words.

In the same way, considering the three equations

$$\begin{aligned} \Delta S_1(X_1^2 \oplus k_1^3) \oplus \Delta X_{12}^0 = 0, \\ \Delta S_6(X_6^1 \oplus k_6^2) \oplus \Delta X_5^0 = 0, \\ \Delta S_5(X_5^0 \oplus k_5^1) \oplus \Delta X_{10}^0 = 0 \end{aligned}$$

we also set up a table T_2 with (X_7^0, X_{12}^0, X_5^0, X_{10}^0) as row address, index of difference (ΔX_7^0, ΔX_{12}^0, ΔX_5^0, ΔX_{10}^0) satisfying the three equations as column address.

Precomputation Tables of Ciphertext-Pairs. We know that the three conditions ($\Delta X_{14}^{21} = 0$, $\Delta X_8^{22} = 0$, $\Delta X_9^{23} = 0$) in Table 2 hold with probability $2^{-4.05}$ for any given (ΔX_{11}^{24}, ΔX_2^{24}, ΔX_{10}^{24}, ΔX_3^{24}). A precomputation table T_3 is set up with

$$i = \Delta X_{11}^{24} \| \Delta X_2^{24} \| \Delta X_{10}^{24} \| \Delta X_3^{24} \tag{7}$$

being index and $T_3(i) = 1$ when (ΔX_{11}^{24}, ΔX_2^{24}, ΔX_{10}^{24}, ΔX_3^{24}) satisfy the three conditions, otherwise $T_3(i) = 0$. There are about $2^{11.95}$ "1"s out of 2^{16} locations in table T_3. In other words, ciphertext pair (C, C') is an available pair for the characteristic in Fig. 2 only if their nibble difference satisfying $T_3(i) = 1$ where i is defined as (7).

In the same way, for (ΔX_{14}^{24}, ΔX_0^{24}, ΔX_{15}^{24}, ΔX_5^{24}), we also set up a table T_4.

Precomputation Tables of Key Bits. For condition $\Delta X_5^2 = 0$ in round 2, by partially decrypting 2 rounds, we deduce that

$$\begin{cases} \Delta S_7(X_7^1 \oplus k_7^2) \oplus \Delta X_3^0 = 0, \\ X_7^1 = S_6(X_6^0 \oplus k_6^1) \oplus X_{13}^0, \\ \Delta X_7^1 = \Delta X_{13}^0. \end{cases} \tag{8}$$

According to the detailed difference properties of S-Box S_7, we could set up a precomputation table TK_1 with (ΔX_{13}^0, ΔX_3^0, X_6^0, X_{13}^0) as row address, store (k_7^2, k_6^1) satisfying (8) in the corresponding row. Therefore, there are 2^{16} rows, and about $2^{5.32}$ bytes in each row of table TK_1.

By using the same method, we also set up other precomputation tables used in key recovery phase, and list them in Table 6 in Appendix A.

3.4 Data Collection

In the data collection phase, we adopt the idea which is similar to the "preliminary sieving of pairs" in [5], but our method only needs to process those available pairs satisfying that all equations hold. By dividing the whole 2^{64} plaintexts into several sets according to some plaintext- and ciphertext-nibbles, and accessing precomputation tables T_i $(i = 1, 2, 3, 4)$, we apply the divide-and-conquer technique to collect available plaintext-ciphertext pairs such that the corresponding equations hold. This enables us to reduce the time complexity of collecting available pairs.

We demonstrate the available-pair-collecting procedure as follows.

1. Encrypt 2^n sets of plaintexts whose nibbles X_0^0, X_4^0, X_6^0, X_8^0 are constants while other nibbles traverse all 2^{48} values. We therefore acquire 2^{n+48} plaintexts P and their corresponding ciphertexts C.
2. Within each set, we collect the available pairs satisfying the extended conditions by taking the following steps:
   (a) The plaintexts/ciphertexts (P, C) of every set are divided into 2^{48} subsets according to $(X_4^{24}, X_8^{24}, X_9^{24}, X_{13}^{24}, X_1^0, X_{13}^0, X_3^0, X_{15}^0, X_7^0, X_{12}^0, X_5^0, X_{10}^0)$. There is about 1 plaintext/ciphertext in every subset.
   (b) For every subset A, we find corresponding subset A' by accessing tables T_1, T_2, and combine each element of A with each element of A' to construct pairs. Furthermore, for each obtained pair, we verify whether this pair is available by accessing tables T_3 and T_4. Therefore, we construct about $2^{48-1} \times 2^{11.95\times 2} \times 2^{-4.05\times 2} \approx 2^{62.8}$ pairs for each set, and need about $(2^{48+11.95\times 2}) \times 2 \approx 2^{72.9}$ times table looking-up equivalent to $2^{72.9}/(8\times 24) \approx 2^{65.3}$ 24-round encryptions.
   (c) For the $2^{62.8}$ remaining pairs, we verify whether condition equations ($\Delta X_0^1 = 0$, $\Delta X_3^1 = 0$, $\Delta X_{12}^{23} = 0$, $\Delta X_{15}^{23} = 0$) in Table 2 hold by testing corresponding plaintext (ciphertext) nibble differences appeared in conditions. According to Properties 1 and 2, there are about $2^{62.8} \times 2^{-1.41\times 2-1.32\times 2} \approx 2^{57.34}$ pairs remaining for each set.

In data collection phase, we could collect about $2^{n+57.34}$ pairs, the complexity of the data collection is about $2^{n+65.3}$ 24-round encryptions.

3.5 Key Recovery

By thoroughly exploring the relations of subkeys, we find that many key bits are determined accordingly only by solving some simple equations after some key bits have been guessed. Based on these, we present an optimal arrangement for guessing key bits and identifying wrong guesses as early as possible. With the optimal arrangement of guessing key and precomputation tables, we effectively reduce the key-guessing space in the procedure of "wrong key filtering" to reduce the time complexity of key recovery phase. We repeatedly follow steps of "wrong key filtering" for 2^n sets to calculate and discard wrong keys as many as possible, and exhaustively search the rest of the equivalent keys. The masterkey will be recovered with the key schedule after discarding wrong keys.

Wrong Key Filtering. From the round function of LBlock, we know that the calculations of X_5^1, ΔX_5^1, X_{13}^{23} and ΔX_{13}^{23} involved in the remaining six equations in Table 2 depend on (k_7^1, k_6^{24}). Hence, we guess (k_7^1, k_6^{24}) in advance to only store pairs that satisfy these 6 conditions. For each value of guessed (k_7^1, k_6^{24}), there are about $2^{57.34-1.22\times4-1.32\times2} \approx 2^{49.82}$ pairs such that these 6 equations hold. Therefore, within each set, we have $N_1 = 2^{49.82} \times 2^8 \approx 2^{57.82}$ available pairs with their corresponding (k_7^1, k_6^{24}) satisfying that all the equations in Table 2 have solutions.

For an available pair, we further guess other subkey bits and filter wrong keys by taking the following steps.

1. For conditions $\Delta X_0^1 = 0$, we get about $2^{1.32}$ values of k_1^1 with corresponding X_0^1 by accessing differential distribution table of S_1. Similar method is applied for 9 conditions ($\Delta X_1^1 = 0$, $\Delta X_3^1 = 0$, $\Delta X_4^1 = 0$, $\Delta X_4^2 = 0$, $\Delta X_9^{23} = 0$, $\Delta X_{11}^{23} = 0$, $\Delta X_{12}^{23} = 0$, $\Delta X_{15}^{23} = 0$, $\Delta X_{10}^{22} = 0$) in rounds 1, 2, 23, and 22 one by one, and we get about $2^{1.32}$ values for k_3^1, k_2^1, k_5^1, k_5^2, k_2^{24}, k_7^{24}, k_4^{24}, k_3^{24}, k_5^{23} with corresponding X_1^1, X_3^1, X_4^1, X_4^2, X_9^{23}, X_{11}^{23}, X_{12}^{23}, X_{15}^{23}, X_{10}^{22} respectively. For 2 conditions ($\Delta X_5^2 = 0$, $\Delta X_7^2 = 0$) in round 2, we get about $2^{5.32}$ values of (k_7^2, k_6^1) with (X_5^2, X_7^1) and $2^{5.32}$ values of (k_6^2, k_4^1) with (X_7^2, X_6^1) by accessing the corresponding precomputation tables TK_1,TK_2 respectively.
2. In this step, we combine partial obtained subkeys to diminish the candidate key space. Firstly, because k_5^{23} is determined by k_7^1, k_5^1, (k_7^2, k_6^1) according to relations among subkeys, we combine them to get $2^{(1.32\times3)}$ values of (k_7^1, k_5^1, k_7^2, k_6^1, k_5^{23}) and corresponding key information $K[47 \sim 50, 68 \sim 79]$. Secondly, we get $2^{(1.32\times5+1)}$ values of $K[43 \sim 55, 64 \sim 79]$ by combining them with k_1^1, (k_6^2, k_4^1) and guessing $K[51]$ to verify k_6^{24}. Thirdly, We get $2^{(1.32\times8-3)}$ values of $K[43 \sim 79]$ by further combining k_2^1, k_3^1 to verify k_7^{24}. In the end, we get $2^{(1.32\times9-3)}$ values of $K[39 \sim 79]$ by combining them with k_5^2.
3. For every subkey candidate obtained in step 2, we deduce k_3^{23}, $k_3^{21}[0, 1, 2]$ with corresponding X_{15}^{22} by the key schedule and partial decryptions. For condition $\Delta X_{15}^{20} = 0$ in round 20, we obtain about $2^{(1.32+1)}$ values of $(k_7^{22}, k_3^{21}[3])$ by accessing table TK_3. Therefore, we get about $2^{(1.32\times10-2)}$ values of $K[39 \sim 79]$, $K(26 \sim 39)^0$, $K(26 \sim 39)^1$, $K(26 \sim 39)^2$, $K(26 \sim 39)^3$, $K(36 \sim 46)^0$ in total.
4. Similarly, we get about $2^{(1.32\times13-6)}$ values of $K[26 \sim 79]$ by guessing 1 bit $K(26 \sim 32)^3$ and combining obtained subkeys of step 4 with k_2^{24}, k_4^{24}, k_3^{24} one by one. Then, we apply obtained values to verify condition $\Delta X_0^3 = 0$ in round 3 and get about $2^{1.32\times14-10}$ values of $K[26 \sim 79]$ with corresponding X_1^2.
5. We further compute k_1^{23}, k_4^{23}, k_5^{21}, k_2^{20} and X_{12}^{22}, X_{14}^{22} with the knowledge of the subkeys. For condition $\Delta X_9^{19} = 0$ in round 19, we get about $2^{1.32}$ values of k_6^{22} by accessing tables TK_4 for each one of guessed key and plaintext/ciphertext informations obtained. Because $K(26 \sim 32)^3$ could also be deduced from k_6^{22}, we get $2^{(1.32\times15-11)}$ values of $K[26 \sim 79]$, $K(22 \sim 32)^0$, $K(22 \sim 32)^1$, $K(22 \sim 32)^2$, $K(22 \sim 32)^3$.
6. Under each one of obtained subkeys of step 5, we deduce k_1^{24} and X_{14}^{23}. For condition $\Delta X_{13}^{22} = 0$ in round 22, and get about $2^{1.32}$ values of k_6^{23} by accessing the differential distribution table of S_6. Because k_6^{23} can also be computed from $K[73 \sim 79]$ and $(0 \sim 3)^3$ according to key schedule, we get about $2^{(1.32\times16-14)}$ values of $K[26 \sim 79]$, $K(22 \sim 32)^0$, $K(22 \sim 32)^1$, $K(22 \sim 32)^2$, $K(22 \sim 32)^3$, $K(0 \sim 3)^3$. Similar method is applied to $\Delta X_8^{22} = 0$, with repeated 2 bits of k_0^{24}, we get $2^{(1.32\times17-16)}$ values of

$K[26 \sim 79]$, $K(22 \sim 32)^0$, $K(22 \sim 32)^1$, $K(22 \sim 32)^2$, $K(22 \sim 32)^3$, $K(0 \sim 3)^3$, $K(18 \sim 25)^0$, $K(18 \sim 25)^1$.

7. We can deduce $K[22 \sim 25]$ by guessing $K(22 \sim 25)^3$ and above subkeys obtained, thus k_2^4, k_0^3 and k_1^2 and corresponding X_0^2, X_2^3, X_3^4 are known. For $\Delta X_1^5 = 0$ in round 5, we get about $2^{1.32}$ values of k_3^5 for each one of subkeys obtained by accessing the differential distribution table of S_3. Because 3 bits of k_3^5 are repeated, then we get $2^{(1.32\times 18-19)}$ values of $K[22 \sim 79]$, $K(0 \sim 3)^3$, $K(18 \sim 25)^0$, $K(18 \sim 25)^1$.
8. Similarly, we can acquire key materials step by step as follows:
   (a) For equation $\Delta X_5^4 = 0$ in round 4, we get $2^{(1.32\times 19-19)}$ values of $K[14 \sim 17, 22 \sim 79], K(0 \sim 3)^3, K(18 \sim 25)^0, K(18 \sim 25)^1$ by TK_5.
   (b) For $\Delta X_{12}^{21} = 0$ in round 21, we get $2^{(1.32\times 20-19)}$ values of $K[14 \sim 17, 22 \sim 79], K(0 \sim 3)^3, K(18 \sim 25)^0, K(18 \sim 25)^1, K(14 \sim 21)^0, K(14 \sim 21)^1, K(14 \sim 21)^2, K(11 \sim 21)^0$.
   (c) For $\Delta X_{14}^{21} = 0$ in round 21, we get $2^{(1.32\times 21-21)}$ values of $K[14 \sim 17, 22 \sim 79], K(0 \sim 3)^3, K(18 \sim 25)^0, K(18 \sim 25)^1, K(18 \sim 21)^3, K(11 \sim 21)^0, K(4 \sim 17)^2, K(4 \sim 17)^3, K(0 \sim 10)^0, K(0 \sim 10)^1$.
   (d) For $\Delta X_1^3 = 0$ in round 3, we get $2^{(1.32\times 22-21)}$ values of $K[2 \sim 5, 14 \sim 17, 22 \sim 79], K(0 \sim 3)^3, K(18 \sim 25)^0, K(18 \sim 25)^1, K(18 \sim 21)^3, K(11 \sim 21)^0, K(4 \sim 17)^2, K(4 \sim 17)^3, K(0 \sim 10)^0, K(0 \sim 10)^1$.

Therefore, for each available pair, there are about $2^{1.32\times 22} \times 2^{-21} \approx 2^{8.04}$ values of 75-bit keys ($K[2 \sim 5, 14 \sim 17, 22 \sim 79]$, $K(0 \sim 3)^3$, $K(18 \sim 25)^0$, $K(18 \sim 25)^1$, $K(18 \sim 21)^3$, $K(11 \sim 21)^0$, $K(4 \sim 17)^2$, $K(4 \sim 17)^3$, $K(0 \sim 10)^0$, $K(0 \sim 10)^1$) to be discarded.

Exhaustive Search. For every remaining candidate key after filtering wrong keys, we search the rest of key bits to recover the masterkey as follows.

According to key schedule, we deduce keys ($K(4 \sim 10)^3$,$K[0, 1, 2, 3]$) from each one of candidate keys ($K(0 \sim 10)^0$, $K(0 \sim 10)^1$), $K(0 \sim 3)^3$) and guessed 2-bit ($K(0 \sim 10)^2$, $K(0 \sim 10)^3$). Because subkeys $K[2, 3]$ are also involved in candidate subkeys, we get about 1 value of ($K(4 \sim 10)^3$,K[0,1]) for each remaining candidate key. Similarly, 2 values of K[18, 19, 20, 21], 1 value of ($K(7 \sim 17)^3$, $K(7 \sim 10)^3$, 6), and 2^4 values of subkeys $K[7, 8, 9, 10, 11, 12, 13]$ would be deduce in sequence.

Hence, there are 2^5 values of 80-bit masterkey left to be exhaustively searched by 24-round encryptions test for every remained candidate subkey.

3.6 Complexity Analysis

From wrong key filtering phase, there are about $2^{(1.32\times 22-21)} = 2^{8.04}$ values of the 75-bit keys to be discarded for each one of available pairs. In other words, for every available pair, a key is discarded with probability $P_1 = 2^{8.04-75} = 2^{-66.96}$. Thus, we let N be the amount of available plaintext-ciphertext pairs such that all equations hold rather than the previous sense of amount of pairs only satisfying input and output differences. By repeatedly processing with N different available plaintext-ciphertext pairs, the probability that one key is kept in the candidate set is

$$P = (1 - P_1)^N \simeq e^{-N\times P_1}.$$

Table 4. Complexity in wrong key filtering

Step	Time complexity
1	$N \times (\frac{2^{1.32}\times 10}{8\times 24} + \frac{2^{5.32}\times 2}{8\times 24})$ 24-round encryptions
2	$N \times (\frac{2^{(1.32\times 3+4)}}{8\times 24} + \frac{2^{(1.32\times 5+5)}}{8\times 24} + \frac{2^{(1.32\times 8+1)}}{8\times 24} + \frac{2^{(1.32\times 9-3)}}{8\times 24})$ 24-round encryptions
3	$N \times \frac{2^{(1.32\times 9-3)}\times 4}{8\times 24}$ 24-round encryptions
4	$N \times (\frac{2^{(1.32\times 11-2)}}{8\times 24} + \frac{2^{(1.32\times 12-4)}}{8\times 24} + \frac{2^{(1.32\times 13-4)}}{8\times 24} + \frac{2^{(1.32\times 13-6)}}{8\times 24}$ 24-round encryptions
5	$N \times \frac{2^{(1.32\times 14-10)}\times 8}{8\times 24}$ 24-round encryptions
6	$N \times (\frac{2^{(1.32\times 15-11)}\times 2}{8\times 24} + \frac{2^{(1.32\times 16-14)}\times 2}{8\times 24})$ 24-round encryptions
7	$N \times \frac{2^{(1.32\times 17-15)}\times 5}{8\times 24}$ 24-round encryptions
8	$N \times (\frac{2^{(1.32\times 18-19)}}{8\times 24} + \frac{2^{(1.32\times 19-19)}}{8\times 24} + \frac{2^{(1.32\times 20-19)}}{8\times 24} + \frac{2^{(1.32\times 21-21)}}{8\times 24})$ 24-round encryptions

When $N = \frac{2^{1.86}}{P_1} = 2^{68.82}$, we calculate:

$$P \simeq e^{2^{1.86}} \approx 2^{5.23},$$
$$n = N - N_1 = 68.82 - 57.82 = 11.$$

Thus we need $C = 2^{11+48} = 2^{59}$ plaintexts. The complexity of data collection is about $2^{65.3+11} = 2^{76.3}$ 24-round encryption. The complexity of exhaustive search is about $2^{80-2^{5.76}=2^{74.77}}$ 24-round encryption tests.

In the following Table 4 , we discuss the time complexity of each step in wrong key filtering phase.

From Table 4, we know that the total time complexity of wrong key filtering is about $2^{68.82+7.4} = 2^{76.22}$ 24-round encryptions.

Therefore, the total time complexity of the impossible differential attack on 24-round LBlock is: $2^{76.3}+2^{76.22}+2^{74.77} \approx 2^{77.50}$ 24-round encryptions. Its data complexity is 2^{59} chosen plaintexts.

4 Conclusion

In this paper, we propose a 24-round impossible differential attack on LBlock, one round more than the best previous result. This attack is achieved by employing several advanced techniques including dynamic key-guessing, more detailed properties of S-Boxes, optimal key-guessing arrangement etc. This attack is, to the best of our knowledge, the best result on LBlock (except biclique attacks) in terms of the number of attacked rounds.

A Detailed Differences Distribution of S-Box and Precomoutation Tables

Table 5. Distribution of input and output differences of S_0

Input difference	Values satisfying difference propagation	Available number	Unavailable number
0	(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15), 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0	0	16
1	0, (6, 7, 12, 13), 0, (8, 9), 0, 0, 0, (0, 1), 0, (4, 5, 14, 15), 0, (10, 11), 0, 0, 0, (2, 3)	6	10
2	0, (0, 2, 9, 11), 0, (13, 15), 0, 0, 0, (4, 6), 0, (1, 3, 8, 10), 0, (12, 14), 0, 0, 0, (5, 7)	6	10
3	0, 0, (8, 11, 12, 15), 0, 0, 0, (1, 2, 4, 7), 0, 0, 0, (9, 10, 13, 14), 0, 0, 0, (0, 3, 5, 6), 0	4	12
4	0, 0, 0, (0, 4), (9, 10, 13, 14), (2, 6), (8, 11, 12, 15), 0, 0, 0, 0, (3, 7), 0, (1, 5), 0, 0	6	10
5	0, 0, 0, 0, (1, 2, 4, 7), (9, 12), 0, (8, 13), 0, 0, (0, 3, 5, 6), 0, 0, (10, 15), 0, (11, 14)	6	10
6	0, 0, (1, 2, 4, 7), 0, (0, 3, 5, 6), (11, 13), 0, (9, 15), 0, 0, 0, 0, 0, (8, 14), 0, (10, 12)	6	10
7	0, 0, 0, (1, 6), (8, 11, 12, 15), (0, 7), 0, 0, 0, 0, 0, (2, 5), 0, (3, 4), (9, 10, 13, 14), 0	6	10
8	0, 0, (5, 13), (3, 11), 0, 0, (6, 14), (2, 10), 0, 0, (4, 12), (1, 9), 0, 0, (7, 15), (0, 8)	8	8
9	0, 0, 0, (5, 12), 0, 0, 0, (7, 14), (1, 3, 8, 10), 0, 0, (4, 13), (0, 2, 9, 11), 0, 0, (6, 15)	6	10
10	0, (4, 5, 14, 15), (3, 9), 0, 0, 0, (0, 10), 0, 0, 0, (1, 11), 0, 0, (6, 7, 12, 13), (2, 8), 0	6	10
11	0, (1, 3, 8, 10), 0, 0, 0, 0, 0, 0, (4, 5, 14, 15), 0, 0, 0, (6, 7, 12, 13), (0, 2, 9, 11), 0, 0	4	12
12	0, 0, (6, 10), (2, 14), 0, (3, 15), (5, 9), 0, (7, 11), (0, 12), 0, 0, (4, 8), 0, 0, (1, 13)	8	8
13	0, 0, 0, (7, 10), 0, (5, 8), 0, 0, (0, 13), (6, 11), (2, 15), 0, (3, 14), 0, (1, 12), (4, 9)	8	8
14	0, 0, (0, 14), 0, 0, (4, 10), (3, 13), (5, 11), (2, 12), (7, 9), 0, (6, 8), (1, 15), 0, 0, 0	8	8
15	0, 0, 0, 0, 0, (1, 14), 0, (3, 12), (6, 9), (2, 13), (7, 8), (0, 15), (5, 10), 0, (4, 11), 0	8	8

Table 6. Precomputation tables of keys

Table	Index	Content	Size
TK_1	$(\Delta X_{13}^0, \Delta X_3^0, X_6^0, X_{13}^0)$	(k_7^2, k_6^1)	$2^{16} \times 2^{5.32}$
TK_2	$(\Delta X_{12}^0, \Delta X_5^0, X_4^0, X_{12}^0)$	(k_6^2, k_4^1)	$2^{16} \times 2^{5.32}$
TK_3	$(\Delta X_{13}^{23}, \Delta X_{11}^{24}, X_{15}^{22}, X_{13}^{23}, k_3^{21}[0,1,2])$	$(k_7^{22}, k_3^{21}[3])$	$2^{19} \times 2^{2.32}$
TK_4	$(\Delta X_{14}^{24}, \Delta X_{13}^{23}, X_{14}^{22}, X_{15}^{23} \oplus k_5^{21}, X_{12}^{22} \oplus k_2^{20})$	k_6^{22}	$2^{20} \times 2^{1.32}$
TK_5	$(\Delta X_5^1, \Delta X_1^0, X_6^2, X_5^1 \oplus k_7^4)$	k_6^3	$2^{16} \times 2^{1.32}$

References

1. AlTawy, R., Tolba, M., Youssef, A.M.: A higher order key partitioning attack with application to LBlock. In: Hajji, S.E., Nitaj, A., Carlet, C., Souidi, E.M. (eds.) C2SI 2015. LNCS, vol. 9084, pp. 215–227. Springer, Heidelberg (2015)
2. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. IACR Cryptology ePrint Archive 2013/404 (2013)
3. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, p. 12. Springer, Heidelberg (1999)

4. Bogdanov, A.A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M., 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. Boura, C., Minier, M., Naya-Plasencia, M., Suder, V.: Improved impossible differential attacks against round-reduced LBlock. Cryptology ePrint Archive, Report 2014/279 (2014)
6. Boura, C., Naya-Plasencia, M., Suder, V.: Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 179–199. Springer, Heidelberg (2014)
7. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011)
8. Karakoç, F., Demirci, H., Harmancı, A.E.: Impossible differential cryptanalysis of reduced-round LBlock. In: Askoxylakis, I., Pöhls, H.C., Posegga, J. (eds.) WISTP 2012. LNCS, vol. 7322, pp. 179–188. Springer, Heidelberg (2012)
9. Knudsen, L.: DEAL - a 128-bit block cipher. In: NIST AES Proposal (1998)
10. Li, Z., Zhang, B., Yao, Y., Lin, D.: Cube cryptanalysis of LBlock with noisy leakage. In: Kwon, T., Lee, M.-K., Kwon, D. (eds.) ICISC 2012. LNCS, vol. 7839, pp. 141–155. Springer, Heidelberg (2013)
11. Liu, S., Gong, Z., Wang, L.: Improved related-key differential attacks on reduced-round LBlock. In: Chim, T.W., Yuen, T.H. (eds.) ICICS 2012. LNCS, vol. 7618, pp. 58–69. Springer, Heidelberg (2012)
12. Liu, Y., Gu, D., Liu, Z., Li, W.: Impossible differential attacks on reduced-round LBlock. In: Ryan, M.D., Smyth, B., Wang, G. (eds.) ISPEC 2012. LNCS, vol. 7232, pp. 97–108. Springer, Heidelberg (2012)
13. Lu, J., Kim, J.-S., Keller, N., Dunkelman, O.: Improving the efficiency of impossible differential cryptanalysis of reduced camellia and MISTY1. In: Malkin, T. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 370–386. Springer, Heidelberg (2008)
14. 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)
15. Wang, N., Xiaoyun Wang, K.: Differential attacks on reduced SIMON versions with dynamic key-guessing techniques. Cryptology ePrint Archive, Report 2014/448 (2014)
16. Sasaki, Y., Wang, L.: Comprehensive study of integral analysis on 22-round LBlock. In: Kwon, T., Lee, M.-K., Kwon, D. (eds.) ICISC 2012. LNCS, vol. 7839, pp. 156–169. Springer, Heidelberg (2013)
17. Sasaki, Y., Wang, L.: Meet-in-the-middle technique for integral attacks against feistel ciphers. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 234–251. Springer, Heidelberg (2013)
18. Soleimany, H., Nyberg, K.: Zero-correlation linear cryptanalysis of reduced-round LBlock. Des. Codes Crypt. **73**(2), 683–698 (2014)
19. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE: a lightweight block cipher for multiple platforms. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 339–354. Springer, Heidelberg (2013)
20. Wang, Y., Wu, W.: Improved multidimensional zero-correlation linear cryptanalysis and applications to LBlock and TWINE. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 1–16. Springer, Heidelberg (2014)

21. Wang, Y., Wu, W., Yu, X., Zhang, L.: Security on LBlock against biclique cryptanalysis. In: Lee, D.H., Yung, M. (eds.) WISA 2012. LNCS, vol. 7690, pp. 1–14. Springer, Heidelberg (2012)
22. Wen, L., Wang, M.Q., Zhao, J.Y.: Related-key impossible differential attack on reduced-round LBlock. J. Comput. Sci. Technol. **29**(1), 165–176 (2014)
23. 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)