An Upper Bound of the Longest Impossible Differentials of Several Block Ciphers

Guoyong Han[1,2], Wenying Zhang[1,*] and Hongluan Zhao[3]
[1] School of Information Science and Engineering, Shandong Normal University, Jinan, China
[e-mail: wenyingzh@sohu.com]
[2] School of Management Engineering, Shandong Jianzhu University, Jinan, China
[e-mail: hgy_126@126.com]
[3] School of Computer Science and Technology, Shandong Jianzhu University, Jinan, China
*Corresponding author: Wenying Zhang

Received January 29, 2018; revised June 6, 2018; accepted September 12, 2018; published January 31, 2019

Abstract

Impossible differential cryptanalysis is an essential cryptanalytic technique and its key point is whether there is an impossible differential path. The main factor of influencing impossible differential cryptanalysis is the length of the rounds of the impossible differential trail because the attack will be more close to the real encryption algorithm with the number becoming longer. We provide the upper bound of the longest impossible differential trails of several important block ciphers. We first analyse the national standard of the Russian Federation in 2015, Kuznyechik, which utilizes the 16-byte LFSR to achieve the linear transformation. We conclude that there is no any 3-round impossible differential trail of the Kuznyechik without the consideration of the specific S-boxes. Then we ascertain the longest impossible differential paths of several other important block ciphers by using the matrix method which can be extended to many other block ciphers. As a result, we show that, unless considering the details of the S-boxes, there is no any more than or equal to 5-round, 7-round and 9-round impossible differential paths for KLEIN, Midori64 and MIBS respectively.

Keywords: Impossible differential, SPN structure, Feistel structure, Kuznyechik, KLEIN, Midori, MIBS

http://doi.org/10.3837/tiis.2019.01.024 **ISSN : 1976-7277**

1. Introduction

Block ciphers play a large part in the process of constructing numerous symmetric cryptographic plans whose core security is determined by the ability of the underlying block ciphers to fight the existing cryptanalytic technologies. Differential cryptanalysis (DC) is one of the most essential cryptanalytic techniques [1]. Most block ciphers are currently designed to be resilient to the attack of the differential cryptanalysis. In order to verify the security of a block cipher resistance differential cryptanalysis, the usual way is to find a longest differential characteristics path which is able to differentiate from a random permutation. To a certain degree, the success of this attack depends chiefly on the opponents careful analysis of the internal structure of the encryption algorithm.

Impossible differential cryptanalysis (IDC) was first proposed by Biham et al. to attack Skipjack [2] and applied by Knudsen against DEAL [3]. It is a filtering way which utilizes differentials with probability zero to find the correct key by throwing away the wrong keys. Until now, a lot of well-known lightweight block ciphers being attacked using IDC, have been published, such as AES, Camellia [4], CLEFIA [5],ARIA[6] and Zodiac[7].

IDC is generally composed of two steps. To begin with, the adversary attempts to find out an impossible differential trail, i.e., the probability of the trail is zero. Next, after obtaining a serial of plaintext-ciphertext pairs, the opponent supposes some subkey sets involved in the outer rounds of the impossible differential path, and then encrypts/decrypts partially each pair of plaintext-ciphertext to verify whether the corresponding internal difference states are identical. Once the input and output differences of the impossible differentials are identical, the supposed subkey will be abandoned. The correct key must be found if we get rid of all incorrect keys.

The success of IDC is mainly depended on the number of the rounds of the impossible differential paths, the detail of input/output difference patterns and the strength of complexity of one-round encryption/decryption. Among them, one important aspect is the detail of input/output difference, because we can improve attacks [8] in the time/data complexities with higher possibilities. However, the core aspect of influencing IDC is the length of the rounds because the attack will be more close to the real encryption algorithm with the number becoming longer and has more practical significance, and this paper is aimed to explore an upper bound of the longest impossible differentials.

An important approach, which can be used to search for differential characteristics of the block cipher, is proposed by Sun et al. in ASIACRYPT 2014 [9] and it is based on MILP which can evaluate the security (obtain security bound) of a block cipher against the differential attacks. They successfully proved that they attained the security bounds for LBlock and PRESENT-80 against related-key differential attacks. Also, they presented a new approach to find characteristics for DESL, LBlock and PRESENT-128, which involved more rounds or higher probability than the previous results. There are several other automatic methods of the block ciphers to get the truncated impossible differentials effciently, such as U-method [10], UID-method [11] and WW-method [12]. The U-method was proposed by Kim et al. in Indocrypt 2003. Its goal is to search the impossible differentials through the miss-in-the-middle technique and the matrix operations. However, it has drawbacks in ascertaining some types of contradictions and several longer impossible differentials. The UID-method improved the evaluation of impossible differentials by removing some conditions in the U-method and making full use of more contradictory conditions. The WW-method was proposed by Wu et al. in Indocrypt 2012 and improved and extended the approach of the above two methods. The above methods are mainly used to search the differential characteristics or impossible differentials as more as possible.

In CRYPTO 2015, Sun et al. have proved that they found almost all impossible differentials of a block cipher [13]. And they first proposed the concept of structure, the independent of the choices of the S-boxes and the dual structure. The dual structure is used to link zero correlation linear hulls and impossible differentials. Constructing zero correlation linear hulls of the dual structure is equal with building impossible differentials of a structure.

In EUROCRYPT 2016, Sun et al. chiefly researched the security of structures resistance impossible differential [14]. They first proposed the problem whether there exists an r-round impossible differential. As a result, there does not exist any 5-round impossible differentials of AES or ARIA, and any 9-round independent impossible differentials of the Camellia without F L/F L^{-1} layer unless the details of the non-linear layer of them are considered.

Our Contribution. This paper aims to find an upper bound of the longest impossible differentials of Several Block Ciphers. We analyze several important block ciphers of the SPN and feistel structure in detail. Then, we apply the matrix to express the linear transformation layer of these block ciphers and give a detailed process.

We first analyse the national standard of the Russian Federation in 2015, Kuznyechik, which utilizes the 16-byte LFSR to achieve the linear transformation. By the analysis, we conclude that there is no any 3-round impossible differential of the Kuznyechik without the consideration of the specific S-boxes. We next ascertain the longest impossible differentials of several other important block ciphers by using the matrix method which can be extended to many other block ciphers. Finally, we provide technical support about IDC for a lot of block ciphers because we can quickly find the longest impossible differentials.

As a result, we show that, unless considering the details of the S-boxes, there is no impossible differential path more than or equal to 3-round, 5-round, 7-round and 9-round impossible differentials for Kuznyechik[15], KLEIN[16] [17], Midori64[18] and MIBS[19] [20] respectively.

Organization of the paper. Section 2 describes some notations used in this paper such as SPN structure, Feistel structure, the matrix of linear transformation and impossible differentials. Section 3 presents the impossible differentials cryptanalysis of the SPN structure and proves the upper bound of the longest impossible differential paths of Kuznyechik, KLEIN and Midori64. Then, Section 4 depicts the impossible differentials cryptanalysis of the Feistel structure and gives the upper bound of the longest impossible differential trails of MIBS. Finally, we draw our conclusion in Section 5.

2. Preliminaries

These notations and basic knowledge are used in this article.

Notations. F_{2^b} : a vector with length b.

$F_{2^b}^n$: the vector space over F_{2^b} with dimension n.

Z : the integer ring.

$\chi(X)$: the truncated characteristic of X .

P : the matrix of the linear layer of the block ciphers, where $P=(p_{ij})\in F_{2^b}^{n\times n}$

P^* : the characteristic matrix of P, where $P^*=(p^*_{ij})\in Z^{n\times n}$.

$||$: concatenation.

$\varepsilon_{SP}^{(r)}$: an r-round SPN structure.

$F_{SP}^{(r)}$: an r-round Feistel structure with SP-type round function.

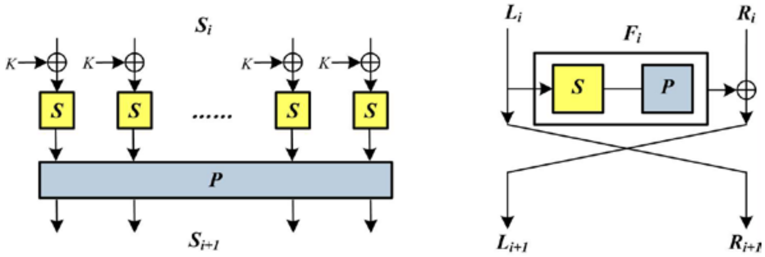

Fig. 1. The round structure of SPN and Feistel

The Block Ciphers of SPN Structure. The SPN structure is broadly used in cryptographic primitives' composition. One round of an SPN cipher typically has three layers (Fig. 1, Left): the SubkeyAddition layer, the nonlinear transformation Sbox-layer and the linear permutation layer *P*. The SubkeyAddition layer is omitted in this paper because it does not cause the propagation of differences. The Sbox-layer can accomplish confusion and *P*-layer can achieve diffusion. We divide the input a of Sbox-layer into n parts, i.e., a = (a_0,…,a_{n-1}), where a_i(0 <=i <= n - 1) is a b-bit byte.

To begin with, a_i is implemented by the non-linear transformation s_i as follows:

$$y=S(a)=(s_0(a_0),\dots,s_{n-1}(a_{n-1}))\in F_{2^b}^{n} \tag{1}$$

Then, y is transformed by $P(F_{2^b}^{m}\to F_{2^b}^{m})$. Additionally, we omit the last round linear permutation layer P since it does not influence the length of an impossible differential, i.e., an r-round SPN structure can be signified by $(S\circ P)^{(r-1)}\circ S$.

Specifically, the SP-type function is denoted as $f:F_{2^b}^{m}\to F_{2^b}^{m}$ in this paper.

The Block Ciphers of Feistel Structure. The Feistel structure is depicted on the right of Fig.1. Let $(L_i\,||\,R_i)\in F_{2^b}^{n}$ and $(L_{i+1}\,||\,R_{i+1})\in F_{2^b}^{n}$ be the input and output of the round function F of the i-th round, respectively, where $0\le i\le r-1$.

$$\begin{cases} L_{i+1}=F(L_i)\oplus R_i \\ R_{i+1}=L_i \end{cases} \tag{2}$$

Similar to the SPN structure, the SubkeyAddition is omitted. In order to keep the consistency of encryption and decryption process, the left and the right are not exchanged in the last round. Notice that the speed of encryption is slow since every bit can be encrypted with two rounds.

Impossible Differentials. Let $G:F_2^n\to F_2^m$, $\delta\in F_2^n$ and $\Delta\in F_2^m$. The probability of $\delta\to\Delta$ is defined as

$$p(\delta \to \Delta) = \#\left\{x \in F_2^n \mid G(x) \oplus G(x \oplus \delta) = \Delta\right\} / 2^n \qquad (3)$$

If $p(\delta \to \Delta) = 0$, then $\delta \to \Delta$ is called an impossible differential of G.

Definition 1([14]). Let $E: F_2^n \to F_2^n$ be a encryption algorithm of a block cipher, whose non-linear components are the bijective S-boxes. A structure $\varepsilon^E \in F_2^n$ is denoted as a group of block ciphers E′ which is equal to E, besides the S-boxes of E′ can take all possible bijective transformations. Let $\alpha, \beta \in F_2^n$. If for any E′ $\in \varepsilon^E$, $\alpha \mapsto \beta$ is an impossible differential of E′. Then $\alpha \mapsto \beta$ is called an impossible differential of ε^E.

Truncated Characteristic. $X = (x_0, ..., x_{n-1})$, where $X \in F_{2^b}^n$ and $x_i \in F_{2^b}\,(0 \le i \le n-1)$. Let $\theta: F_{2^b} \to F_2$ be defined as

$$\theta(x_i) = \begin{cases} 0 & x_i = 0 \\ 1 & x_i \neq 0 \end{cases} \qquad (4)$$

Then, $\chi(X)$ denotes the truncated characteristic of X, as follows:

$$\chi(X) = (\theta(x_0), ..., \theta(x_{n-1})) \in F_2^n \qquad (5)$$

The Matrix of Linear Permutation. Let the matrix P represent the linear permuation of the block cipher, where $P = (p_{ij}) \in F_{2^b}^{n \times n}$. For the block ciphers of SPN structure, the matrix P represents the linear permutation layer P, i.e., not including the SubkeyAddition layer and the nonlinear transformation Sbox-layer. For the block ciphers of Feistel structure, the matrix P represents the linear permutation layer P of the round function.

AES is one of the most popular SPN ciphers so far. The SubBytes(SB) is the only non-linear transformation. The linear permutation includes ShiftRows(SR) and MixColumns(MC). Let the state after SB be S which consists of a_i, where i = 0,1,2,…,15 and the length of a_i is 8 bits. The state after SR and MC can be described as follows:

$$S = \begin{bmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{bmatrix} \xrightarrow{SR} \begin{bmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_5 & a_9 & a_{13} & a_1 \\ a_{10} & a_{14} & a_2 & a_6 \\ a_{15} & a_3 & a_7 & a_{11} \end{bmatrix} \xrightarrow{MC} \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \bullet \begin{bmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_5 & a_9 & a_{13} & a_1 \\ a_{10} & a_{14} & a_2 & a_6 \\ a_{15} & a_3 & a_7 & a_{11} \end{bmatrix}$$

$$= \begin{bmatrix} 2a_0 + 3a_5 + a_{10} + a_{15} & 2a_4 + 3a_9 + a_{14} + a_3 & 2a_8 + 3a_{13} + a_2 + a_7 & 2a_{12} + 3a_1 + a_6 + a_{11} \\ a_0 + 2a_5 + 3a_{10} + a_{15} & a_4 + 2a_9 + 3a_{14} + a_3 & a_8 + 2a_{13} + 3a_2 + a_7 & a_{12} + 2a_1 + 3a_6 + a_{11} \\ a_0 + a_5 + 2a_{10} + 3a_{15} & a_4 + a_9 + 2a_{14} + 3a_3 & a_8 + a_{13} + 2a_2 + 3a_7 & a_{12} + a_1 + 2a_6 + 3a_{11} \\ 3a_0 + a_5 + a_{10} + 2a_{15} & 3a_4 + a_9 + a_{14} + 2a_3 & 3a_8 + a_{13} + a_2 + 2a_7 & 3a_{12} + a_1 + a_6 + 2a_{11} \end{bmatrix}$$

If we consider the 4 × 4 state S as a vector S′ in $F_{2^8}^{16}$, the linear permutation which includes the SR and the MC can be also written as the following P× S′, where the linear permutation matrix P is in $F_{2^8}^{16 \times 16}$ as follows:

$$P\times S'=\begin{bmatrix}2&0&0&0&0&3&0&0&0&0&1&0&0&0&0&1\\1&0&0&0&0&2&0&0&0&0&3&0&0&0&0&1\\1&0&0&0&0&1&0&0&0&0&2&0&0&0&0&3\\3&0&0&0&0&1&0&0&0&0&1&0&0&0&0&2\\0&0&0&1&2&0&0&0&0&3&0&0&0&0&1&0\\0&0&0&1&1&0&0&0&0&2&0&0&0&0&3&0\\0&0&0&3&1&0&0&0&0&1&0&0&0&0&1&0\\0&0&0&2&3&0&0&0&0&1&0&0&0&0&1&0\\0&0&1&0&0&0&0&1&2&0&0&0&0&3&0&0\\0&0&3&0&0&0&0&1&1&0&0&0&0&2&0&0\\0&0&2&0&0&0&0&3&1&0&0&0&0&1&0&0\\0&0&1&0&0&0&0&2&3&0&0&0&0&1&0&0\\0&3&0&0&0&0&1&0&0&0&0&1&2&0&0&0\\0&2&0&0&0&0&3&0&0&0&0&1&1&0&0&0\\0&1&0&0&0&0&2&0&0&0&0&3&1&0&0&0\\0&1&0&0&0&0&1&0&0&0&0&2&3&0&0&0\end{bmatrix}\bullet\begin{bmatrix}a_0\\a_1\\a_2\\a_3\\a_4\\a_5\\a_6\\a_7\\a_8\\a_9\\a_{10}\\a_{11}\\a_{12}\\a_{13}\\a_{14}\\a_{15}\end{bmatrix}=\begin{bmatrix}2a_0+3a_5+a_{10}+a_{15}\\a_0+2a_5+3a_{10}+a_{15}\\a_0+a_5+2a_{10}+3a_{15}\\3a_0+a_5+a_{10}+2a_{15}\\2a_4+3a_9+a_{14}+a_3\\a_4+2a_9+3a_{14}+a_3\\a_4+a_9+2a_{14}+3a_3\\3a_4+a_9+a_{14}+2a_3\\2a_8+3a_{13}+a_2+a_7\\a_8+2a_{13}+3a_2+a_7\\a_8+a_{13}+2a_2+3a_7\\3a_8+a_{13}+a_2+2a_7\\2a_{12}+3a_1+a_6+a_{11}\\a_{12}+2a_1+3a_6+a_{11}\\a_{12}+a_1+2a_6+3a_{11}\\3a_{12}+a_1+a_6+2a_{11}\end{bmatrix},$$

$$P^*=\begin{bmatrix}1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\end{bmatrix}$$

Similar to SPN, we can use the matrix P to represent the linear permutation operations of the round function of Feistel strucures with SP-type round functions.

Characteristic Matrix. Let $P^* = (p^*_{ij}) \in Z^{n\times n}$ denote the characteristic matrix of $P = (p_{ij}) \in F^{n\times n}$ for $0 \le i, j \le n-1$, where $p^*_{ij} = \theta(p_{ij})$, i.e., $p^*_{ij} = 0$ if $p_{ij} = 0$ and $p^*_{ij} = 1$ otherwise. Let the matrix $B = (b_{ij}) \in Z^{n\times n}$. B be non-negative if all b_{ij} are non-negative, and positive if all b_{ij} are positive. Obviously, P^* is always non-negative. Then the characteristic matrix P^* of AES as shown above.

3. Impossible Differentials of the SPN Structure

We use the matrix method to ascertain the upper bound of the longest impossible differentials for several SPN ciphers.

3.1 An Upper Bound for the Rounds of Impossible Differentials

Definition 2. Let $P \in F^{n\times n}_{2^b}$, P^* be the characteristic matrix of P, and

$$f_m(P^*) = (P^*)^m \tag{6}$$

Then the smallest integer m is called type 1 primitive index of P (for SPN structure), s.t. $f_m(P^*)$ is a positive matrix. For example, if m = 3, then $f_3(P^*) = (P^*)^3$ is a positive matrix, but $f_2(P^*) = (P^*)^2$ is not positive matrix.

Assume $\mu \to \nu$ is a possible differential of $\varepsilon^{(r)}_{SP}$. So, there is always a few α' and β', s.t.,

$$\mu \xrightarrow{\varepsilon^S} \mu' \xrightarrow{\varepsilon^{PS\cdots SP}} \nu' \xrightarrow{\varepsilon^S} \nu \tag{7}$$

is a possible differential of $\varepsilon^{(r)}_{SP}$. Thus for any μ^* and ν^* ,s.t., $\chi(\mu^*) = \chi(\mu)$ and $\chi(\nu^*) = \chi(\nu)$,

$$\mu^* \xrightarrow{\varepsilon^S} \mu' \xrightarrow{\varepsilon^{PS\cdots SP}} \nu' \xrightarrow{\varepsilon^S} \nu^* \tag{8}$$

is also a possible differential.

As discussed previously, we can ascertain the longest of impossible differentials. Next, we will present an upper bound for the length of impossible differentials with considering merely the property of the P layer for an SPN structure.

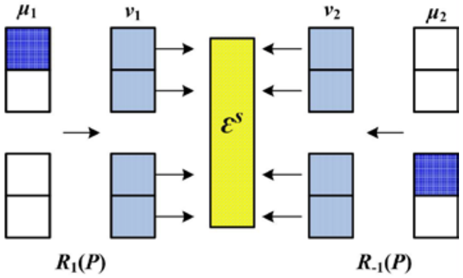

Fig. 2. (R1(P) + R-1(P) + 1)-round differential for ε_{SP}

Fig.2 describes the maximal length of impossible differential trail of an SPN cipher. Let the intermediate μ_1 be m bytes. If anyone byte of μ_1 has a difference, then each byte of ν_1 has a difference after encrypting $R_1(P)$ rounds, i.e., $|\chi(\mu_1)|=1$ and $|\chi(\nu_1)|=m$. In a similar way, if anyone byte of μ_2 has a difference, then each byte of ν_2 has a difference after decrypting $R_{-1}(P)$ rounds, i.e., $|\chi(\mu_2)|=1$ and $|\chi(\nu_2)|=m$. Since $|\chi(\nu_1)|=|\chi(\nu_2)|=m$, $\nu_1 \rightarrow \nu_2$ is a one-round possible differential. So the following theorem holds.

Theorem 1([14]). Let $R_1(P)$ and $R_{-1}(P)$ be the type 1 primitive indexes of P and P^{-1} respectively. There is no any impossible differential r of $\varepsilon_{SP}^{(r)}$ for $r \geq R(P)+R_{-1}(P)+1$ (As shown in Fig. 2).

For AES, we only consider the property of the P layer. The state is S$_0$ which consists of a_i for i =0,1,2,…15, where the length of a_i is 8 bits. The state after the Matrix P of Linear Permutation (one round) is S$_1$ which consists of b_i for i = 0,1,2,… ,15. Then the state after the Matrix P again is S$_2$ which consists of c_i for i = 0,1,2,…,15. S$_0$, S$_1$ and S$_2$ are depicted as follows.

$$S_0=\begin{bmatrix} a_0\\ a_1\\ a_2\\ a_3\\ a_4\\ a_5\\ a_6\\ a_7\\ a_8\\ a_9\\ a_{10}\\ a_{11}\\ a_{12}\\ a_{13}\\ a_{14}\\ a_{15} \end{bmatrix}, S_1=\begin{bmatrix} b_0\\ b_1\\ b_2\\ b_3\\ b_4\\ b_5\\ b_6\\ b_7\\ b_8\\ b_9\\ b_{10}\\ b_{11}\\ b_{12}\\ b_{13}\\ b_{14}\\ b_{15} \end{bmatrix}=\begin{bmatrix} 2a_0+3a_5+a_{10}+a_{15}\\ a_0+2a_5+3a_{10}+a_{15}\\ a_0+a_5+2a_{10}+3a_{15}\\ 3a_0+a_5+a_{10}+2a_{15}\\ 2a_4+3a_9+a_{14}+a_3\\ a_4+2a_9+3a_{14}+a_3\\ a_4+a_9+2a_{14}+3a_3\\ 3a_4+a_9+a_{14}+2a_3\\ 2a_8+3a_{13}+a_2+a_7\\ a_8+2a_{13}+3a_2+a_7\\ a_8+a_{13}+2a_2+3a_7\\ 3a_8+a_{13}+a_2+2a_7\\ 2a_{12}+3a_1+a_6+a_{11}\\ a_{12}+2a_1+3a_6+a_{11}\\ a_{12}+a_1+2a_6+3a_{11}\\ 3a_{12}+a_1+a_6+2a_{11} \end{bmatrix}, S_2=\begin{bmatrix} c_0\\ c_1\\ c_2\\ c_3\\ c_4\\ c_5\\ c_6\\ c_7\\ c_8\\ c_9\\ c_{10}\\ c_{11}\\ c_{12}\\ c_{13}\\ c_{14}\\ c_{15} \end{bmatrix}=\begin{bmatrix} 2b_0+3b_5+b_{10}+b_{15}\\ b_0+2b_5+3b_{10}+b_{15}\\ b_0+b_5+2b_{10}+3b_{15}\\ 3b_0+b_5+b_{10}+2b_{15}\\ 2b_4+3b_9+b_{14}+b_3\\ b_4+2b_9+3b_{14}+b_3\\ b_4+b_9+2b_{14}+3b_3\\ 3b_4+b_9+b_{14}+2b_3\\ 2b_8+3b_{13}+b_2+b_7\\ b_8+2b_{13}+3b_2+b_7\\ b_8+b_{13}+2b_2+3b_7\\ 3b_8+b_{13}+b_2+2b_7\\ 2b_{12}+3b_1+b_6+b_{11}\\ b_{12}+2b_1+3b_6+b_{11}\\ b_{12}+b_1+2b_6+3b_{11}\\ 3b_{12}+b_1+b_6+2b_{11} \end{bmatrix}$$

Obviously, if $|\chi(S_0)|=1$, then $|\chi(S_1)|=4$ and $|\chi(S_2)|=16$. In other words, P^* is not a positive matrix, however, $(P^*)^2$ is a positive matrix. So $R_1(P)=2$. Similarly, $R_{-1}(P)$ = 2.

3.2 Cryptanalysis of Kuznyechik Cipher

Kuznyechik [15] is the national standard [GOST R 34.12-2015] of the Russian Federation in 2015. It applies cryptographic techniques to process and protect information, including the confidentiality, authenticity, and integrity of data. The Standard complies with modern cryptographic requirements and is designed for efficient implementation of hardware and software.

Kuznyechik(see Fig.3) is a 128-bit block cipher with 256 bits key. The encryption algorithm is a replacement $E_{K_1,\cdots,K_{10}}$ which is defined on $F_{2^{128}}$, as shown below:

$$E_{K_1,\cdots,K_{10}}(a) = X[K_{10}]L \circ S \circ X[K_9]\cdots L \circ S \circ X[K_2]L \circ S \circ X[K_1](a) \tag{9}$$

where $a = a_{15} \| a_{14} \| a_{13} \cdots \| a_2 \| a_1 \| a_0$ and $a_i \in F_{2^8} (0 \le i \le 15)$.

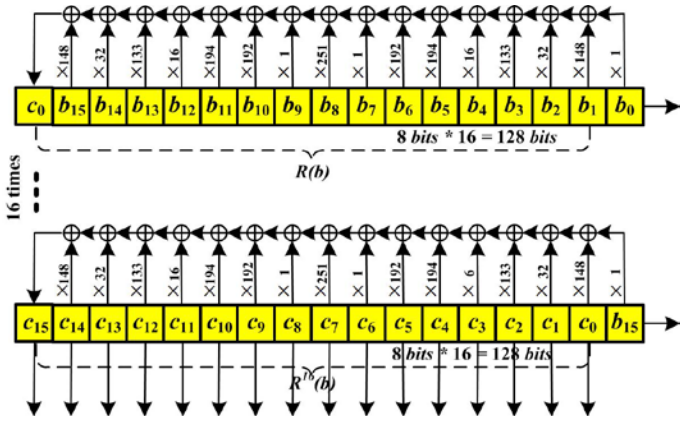
×148
× 32
×133
× 16
×194
×192
× 1
×251
× 1
×192
×194
× 16
×133
× 32
×148
× 1
c_0 b_{15} b_{14} b_{13} b_{12} b_{11} b_{10} b_9 b_8 b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0
8 bits * 16 = 128 bits
R(b)
16 times
×148
× 32
×133
× 16
×194
×192
× 1
×251
× 1
×192
×194
× 6
×133
× 32
×148
× 1
c_{15} c_{14} c_{13} c_{12} c_{11} c_{10} c_9 c_8 c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0 b_{15}
8 bits * 16 = 128 bits
$R^{16}(b)$

Fig. 3. The round function of Kuznyechik

Moreover, X denotes AddRoundKey, and S represents the bijective nonlinear mapping, i.e., $S(a) = S(a_{15} \| a_{14} \| a_{13} \cdots \| a_2 \| a_1 \| a_0) = b_{15} \| b_{14} \| b_{13} \cdots \| b_2 \| b_1 \| b_0$, where $b_i = \pi(a_i)(0 \le i \le 15)$. L means R^{16}, i.e., the linear transformation layer, where $R(b) = R(b_{15} \| b_{14} \| b_{13} \cdots \| b_2 \| b_1 \| b_0) = l(b_{15},\cdots,b_0) \| b_{15} \| b_{14} \| b_{13} \cdots \| b_2 \| b_1$ is a 16-byte LFSR. The register moves 8 bits each time, and the new state is denoted by the state of LFSR after moving 16 times. The detailed descriptions of LFSR are in **Fig. 4**.

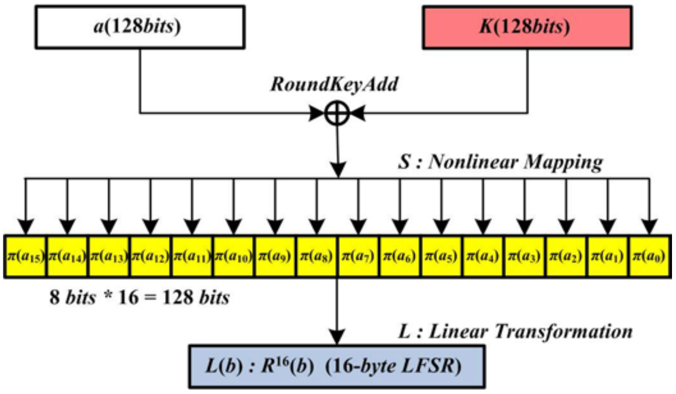
a(128bits)
K(128bits)
RoundKeyAdd
S : Nonlinear Mapping
π(a15) π(a14) π(a13) π(a12) π(a11) π(a10) π(a9) π(a8) π(a7) π(a6) π(a5) π(a4) π(a3) π(a2) π(a1) π(a0)
8 bits * 16 = 128 bits
L : Linear Transformation
L(b) : R16(b) (16-byte LFSR)

Fig. 4. The LFSR of the round function of Kuznyechik

For Kuznyechik, the P layer means the L operation, i.e., P = R^{16}. Then we consider the 16 states as a vector in $F_{2^8}^{16}$ and the irreducible polynomial over this finite fields is $x^8 + x^7 + x^6 + x + 1$. By calculation, the following matrix can be used to represent R, R^2 and R^{16}.

$$R(b) = \begin{bmatrix} 148&32&133&16&194&192&1&251&1&192&194&6&133&32&148&1 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \end{bmatrix} \bullet \begin{bmatrix} b_{15} \\ b_{14} \\ b_{13} \\ b_{12} \\ b_{11} \\ b_{10} \\ b_9 \\ b_8 \\ b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix}, \quad R^2(b) = \begin{bmatrix} 132&45&116&150&93&119&111&222&84&180&141&209&68&60&165&148 \\ 148&32&133&16&194&192&1&251&1&192&194&6&133&32&148&1 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \end{bmatrix} \bullet \begin{bmatrix} b_{15} \\ b_{14} \\ b_{13} \\ b_{12} \\ b_{11} \\ b_{10} \\ b_9 \\ b_8 \\ b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix}$$

For R, the 16 elements in row 0 are non-zero, and there are 15 zeros and one 1 in the other 15 rows. For R^2, the 16 elements in row 0 and row 1 are non-zero, and there are 15 zeros and one 1 in the other 14 rows. Note that the multiplication of any two nonzero numbers is still nonzero in the finite field.

$$R^{16}(b) = \begin{bmatrix} 207&152&116&191&147&142&242&243&10&191&246&169&234&142&77&110 \\ 110&32&198&218&144&72&137&156&193&100&184&45&134&68&208&162 \\ 162&200&135&112&104&67&28&43&161&99&48&107&159&48&227&118 \\ 118&51&16&12&28&17&214&106&166&215&246&73&70&20&232&114 \\ 114&242&107&202&32&235&2&164&141&212&196&1&101&221&76&108 \\ 108&118&236&12&197&188&175&110&163&225&144&88&14&2&195&72 \\ 72&213&98&23&6&45&196&231&213&235&153&120&82&245&22&122 \\ 122&230&78&26&187&46&241&190&212&175&55&177&212&42&110&184 \\ 184&73&135&20&203&141&171&73&9&108&42&1&96&142&75&93 \\ 93&212&184&47&141&18&238&246&8&84&15&243&152&200&127&39 \\ 39&159&190&104&26&124&173&201&132&47&235&254&198&72&162&189 \\ 189&149&94&48&233&96&191&16&239&57&236&145&127&72&137&16 \\ 16&233&208&217&243&148&61&175&123&255&100&145&82&248&13&221 \\ 221&153&117&202&151&68&90&224&48&166&49&211&223&72&100&132 \\ 132&45&116&150&93&119&111&222&84&180&141&209&68&60&165&148 \\ 148&32&133&16&194&192&1&251&1&192&194&16&133&32&148&1 \end{bmatrix} \bullet \begin{bmatrix} b_{15} \\ b_{14} \\ b_{13} \\ b_{12} \\ b_{11} \\ b_{10} \\ b_9 \\ b_8 \\ b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix}, \quad P^* = \begin{bmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \end{bmatrix}$$

By computing, there is no 0 element in R^{16}, i.e., R^{16} is a positive matrix. For Kuznyechik, the linear transformation of each round is iterated 16 times, which is equivalent to 16 rounds of other block cipher algorithms. Therefore, the characteristic matrix of R^{16} (i.e. P^*) is also the positive matrix. Then we have $R(P)$ = 1.. In a similar way, $R_{-1}(P) = 1$. Then we get the following conclusion:

Proposition 1. There is no any more than or equal to 3-round impossible differential of $\varepsilon^{Kuznyechik}$. Or equivalently, there is no any 3-round impossible differential of the Kuznyechik unless considering the details of the S-boxes.

3.3 Cryptanalysis of KLEIN Cipher

KLEIN family [16] is proposed by Gong et al. at RFIDSec 2011, with a fixed 64-bit block size. It supports three key of 64-bit, 80-bit and 96-bit, along with 12,16 and 20 rounds respectively. The experimental implementation results of hardware and software show that KLEIN has a good performance in constrained resource environments.

KLEIN uses 4-bit Sboxes and AES MixColumn in a SPN structure. Such a combination is low memory implementation in both hardware and software, but KLEIN family may exists serious risks and they are not validated with further external analysis. The present cryptanalysis results of KLEIN, shown by designers, are about 4-round differential and linear attacks, 5-round integral attack. The designers also considered the Key schedule attack, algebraic attack and side-channel attack. And we can apply the high order differential and the high order integral properties to improve the result of the integral analysis. Ahmadian et al. shown a full round attack on KLEIN by using a biclique [17].

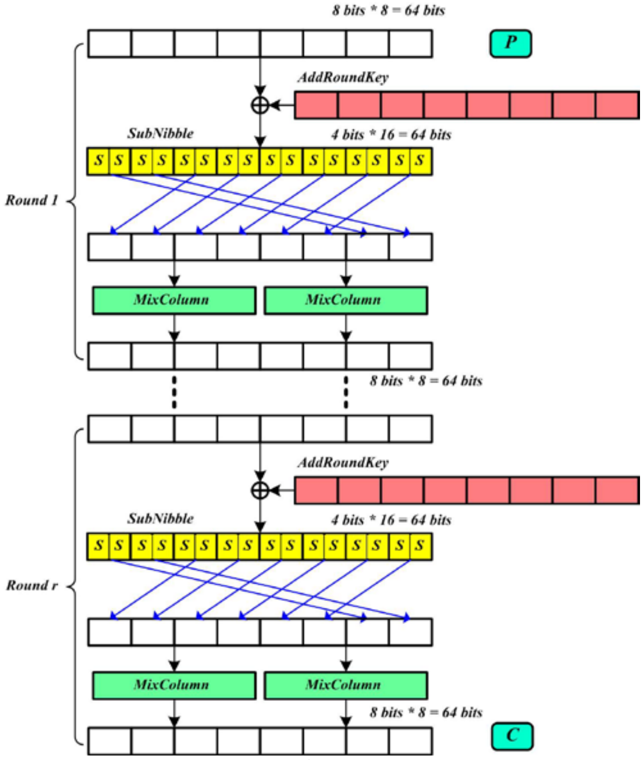

Fig. 5. The structure of the block cipher KLEIN

KLEIN supports 64-bit, 80-bit and 96-bit three key sizes but all of them are 64-bit block sizes. In this paper we focuse only on KLEIN-64 (see **Fig. 5**) whose round function consists of four steps as below.

(1) AddRoundKey(AK), the 64-bit state is XORed with a 64-bit round key.

(2) SubNibbles(SN), which divides the 64-bit intermediate state into sixteen 4-bit nibbles and puts them into the same sixteen 4 × 4 S-boxes.

(3) RotateNibbles(RN), the 64-bit state are rotated left 16 bits in every round.

(4) MixNibbles(MN), two AES MixColumn are applied concurrently, each 32-bit is operated by one AES Mix-Column.

The AES MixColumn operation is the following matrix(M1) multiplication in GF(28) and multiply modulo x4 + 1. The corresponding irreducible polynomial is : $x^8 + x^4 + x^3 + x + 1$.

Let the state after SN be S which consists of a_i for i = 0,1,2,…,7, where the length of a_i is 8 bits. These two operations of RN and MN can be denoted as follows:

$$S=\begin{bmatrix} a_0\ a_4\\ a_1\ a_5\\ a_2\ a_6\\ a_3\ a_7\end{bmatrix}\xrightarrow{RN}\begin{bmatrix} a_2\ a_6\\ a_3\ a_7\\ a_4\ a_0\\ a_5\ a_1\end{bmatrix}\xrightarrow{MN}\begin{bmatrix}02 & 03 & 01 & 01\\ 01 & 02 & 03 & 01\\ 01 & 01 & 02 & 03\\ 03 & 01 & 01 & 02\end{bmatrix}\bullet\begin{bmatrix}a_2\\ a_3\\ a_4\\ a_5\end{bmatrix}\,||\,\begin{bmatrix}02 & 03 & 01 & 01\\ 01 & 02 & 03 & 01\\ 01 & 01 & 02 & 03\\ 03 & 01 & 01 & 02\end{bmatrix}\bullet\begin{bmatrix}a_6\\ a_7\\ a_0\\ a_1\end{bmatrix}$$

$$=\begin{bmatrix}2a_2+3a_3+a_4+a_5 & 2a_6+3a_7+a_0+a_1\\ a_2+2a_3+3a_4+a_5 & a_6+2a_7+3a_0+a_1\\ a_2+a_3+2a_4+3a_5 & a_6+a_7+2a_0+3a_1\\ 3a_2+a_3+a_4+2a_5 & 3a_6+a_7+a_0+2a_1\end{bmatrix}.$$

If we consider the state S as a vector S' in $F_{2^8}^{8}$, the linear permutation, which includes RN and MN, can be also written as the following $P\times S'$, where the linear permutation matrix P is in $F_{2^8}^{8\times 8}$.

$$P\times S'=\begin{bmatrix}0\,0\,2\,3\,1\,1\,0\,0\\ 0\,0\,1\,2\,3\,1\,0\,0\\ 0\,0\,1\,1\,2\,3\,0\,0\\ 0\,0\,3\,1\,1\,2\,0\,0\\ 1\,1\,0\,0\,0\,0\,2\,3\\ 3\,1\,0\,0\,0\,0\,1\,2\\ 2\,3\,0\,0\,0\,0\,1\,1\\ 1\,2\,0\,0\,0\,0\,3\,1\end{bmatrix}\cdot\begin{bmatrix}a_0\\ a_1\\ a_2\\ a_3\\ a_4\\ a_5\\ a_6\\ a_7\end{bmatrix}=\begin{bmatrix}2a_2+3a_3+a_4+a_5\\ a_2+2a_3+3a_4+a_5\\ a_2+a_3+2a_4+3a_5\\ 3a_2+a_3+a_4+2a_5\\ 2a_6+3a_7+a_0+a_1\\ a_6+2a_7+3a_0+a_1\\ a_6+a_7+2a_0+3a_1\\ 3a_6+a_7+a_0+2a_1\end{bmatrix}$$

So,

$$P=\begin{bmatrix}0\,0\,2\,3\,1\,1\,0\,0\\ 0\,0\,1\,2\,3\,1\,0\,0\\ 0\,0\,1\,1\,2\,3\,0\,0\\ 0\,0\,3\,1\,1\,2\,0\,0\\ 1\,1\,0\,0\,0\,0\,2\,3\\ 3\,1\,0\,0\,0\,0\,1\,2\\ 2\,3\,0\,0\,0\,0\,1\,1\\ 1\,2\,0\,0\,0\,0\,3\,1\end{bmatrix},P^*=\begin{bmatrix}0\,0\,1\,1\,1\,1\,0\,0\\ 0\,0\,1\,1\,1\,1\,0\,0\\ 0\,0\,1\,1\,1\,1\,0\,0\\ 0\,0\,1\,1\,1\,1\,0\,0\\ 1\,1\,0\,0\,0\,0\,1\,1\\ 1\,1\,0\,0\,0\,0\,1\,1\\ 1\,1\,0\,0\,0\,0\,1\,1\\ 1\,1\,0\,0\,0\,0\,1\,1\end{bmatrix},(P^*)^2=\begin{bmatrix}2\,2\,2\,2\,2\,2\,2\,2\\ 2\,2\,2\,2\,2\,2\,2\,2\\ 2\,2\,2\,2\,2\,2\,2\,2\\ 2\,2\,2\,2\,2\,2\,2\,2\\ 2\,2\,2\,2\,2\,2\,2\,2\\ 2\,2\,2\,2\,2\,2\,2\,2\\ 2\,2\,2\,2\,2\,2\,2\,2\\ 2\,2\,2\,2\,2\,2\,2\,2\end{bmatrix}$$

Since P^* is negative and (P^*)^2 is positive, we have $R(P)$ = 2. Similarly, $R_{-1}(P)$ = 2. Then we get the following conclusion:

Proposition 2. There is no any more than or equal to 5-round impossible differential of ε^{KLEIN}. Or equivalently, there is no any 5-round impossible differential of the KLEIN unless considering the details of the S-boxes.

3.4 Cryptanalysis of Midori64 Cipher

The Midori64 [18] is another popular SPN ciphers and designed by Banik et al. at A SIACRYPT 2015. Midori family is also a lightweight block ciphe. Midori-64 support 64-bit block sizes and 128-bit keys along with 16 rounds. The designers try to optimize every part of the circuit in order to decrease the energy consumption and make both encryption and decryption achieved by a little adjustment in the circuit. The designers declared that there does not exist any more than 7-round impossible differential trail for Midori64.

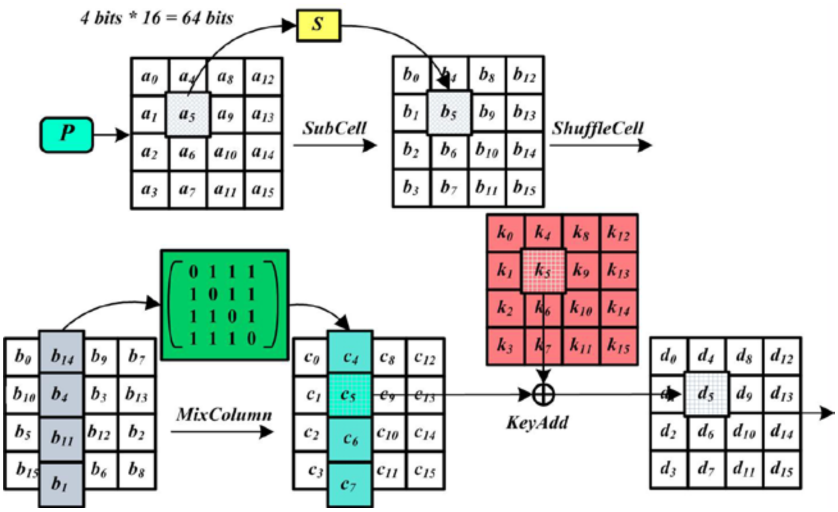

Fig. 6. The round function of Midori64

In this paper, we focus on Midori64(see Fig.6) whose round function consists of four steps as below.

(1) SubCell(SC), apply the same 16 non-linear S-boxes on the state in parallel.

(2) ShuffeCell(SFC), the shuffe is as follows: (a_0, a_1, a_2,… , a_{13}, a_{14}, a_{15}) ← (a_0, a_{10}, a_5, a_{15}, a_{14}, a_4, a_{11}, a_1, a_9, a_3, a_{12}, a_6, a_7, a_{13}, a_2, a_8).

(3) MixColumn(MC), Midori-64 utilizes the matrix M2 to confuse every 4-nibble column of the state S , i.e. ${}^t(a_i,a_{i+1},a_{i+2},a_{i+3}) \leftarrow M_2 \bullet {}^t(a_i,a_{i+1},a_{i+2},a_{i+3})$, where i = 0,4,8,12.

$$M_2=\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{bmatrix},\quad S=\begin{bmatrix}a_0&a_4&a_8&a_{12}\\a_1&a_5&a_9&a_{13}\\a_2&a_6&a_{10}&a_{14}\\a_3&a_7&a_{11}&a_{15}\end{bmatrix}$$

(4) AddKey(AK), the 64-bit state is XORed with a 64-bit round key.

Similar to KLEIN, we consider the 4 ×4 matrix of Midori-64 as the state $S \in F_{2^4}^{16}$, where the size of each cell of S is 4 bits. Let the state S after SC be described as shown above, and the state after SFC and MC can be written as follows.

$$S = \xrightarrow{SFC} \begin{bmatrix} a_0 & a_{14} & a_9 & a_7 \\ a_{10} & a_4 & a_3 & a_{13} \\ a_5 & a_{11} & a_{12} & a_2 \\ a_{15} & a_1 & a_6 & a_8 \end{bmatrix} \xrightarrow{MC} \begin{bmatrix} a_5+a_{10}+a_{15} & a_1+a_4+a_{11} & a_3+a_6+a_{12} & a_2+a_8+a_{13} \\ a_5+a_0+a_{15} & a_1+a_{11}+a_{14} & a_6+a_9+a_{12} & a_2+a_7+a_8 \\ a_0+a_{10}+a_{15} & a_1+a_4+a_{14} & a_3+a_6+a_9 & a_7+a_8+a_{13} \\ a_0+a_5+a_{10} & a_4+a_{11}+a_{14} & a_3+a_9+a_{12} & a_2+a_7+a_{13} \end{bmatrix}$$

The matix P of linear permutation can be written as the following 16 × 16 matrix over $F_{2^4}^{16\times16}$. It is clear that the characteristic matrix P^* of P equals P. By calculating, $(P^*)^2$ is negative, but $(P^*)^3$ is positive. So, we get $R(P)$ = 3. Similarly, $R_{-1}(P)$ = 3. Then we get the following conclusion:

Proposition 3. There is no any more than or equal to 7-round impossible differential of $\varepsilon^{Midori64}$. Or equivalently, there is no any 7-round impossible differential of the Midori64 unless considering the details of the S-boxes.

In 2016, Chen et al. used the path (0, a, 0, 0, 0, 0, 0, 0, 0, 0, 0, a, 0, 0, 0, 0) → (0, 0, 0, 0, 0,*, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0), a 6-round impossible differential path, to attack 10-round Midori64, where 0 denotes zero difference, a and * denote non-zero difference [21]. The impossible difference path is consistent with our conclusion in proposition 3.

4. Impossible Differentials of the Feistel Structures with SP-Type Round Functions

We use the matrix method to ascertain the upper bound of the longest impossible differentials of the Feistel Structures with SP-Type Round Functions.

4.1 An Upper Bound for the Rounds of Impossible Differentials

The principle to study the Feistel structure with SP-type round functions are almost the same as that of the SPN structure(As shown in **Fig. 7**).

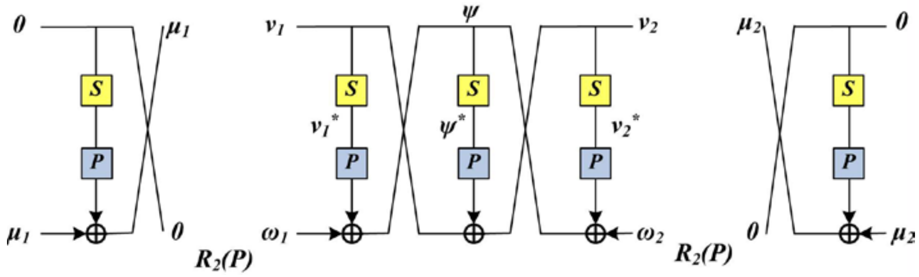

Fig. 7. (2R2(P) + 5)-round differential for F_{SP}

Definition 3. Let $P \in F_{2^b}^{n\times n}$, P^* be the characteristic matrix of P, and

$$g_m(P^*) = \begin{cases} \sum_{i=0}^{j} (P^*)^{2*i} & n = 2*j \\ \sum_{i=0}^{j} (P^*)^{2*i-1} & n = 2*j-1 \end{cases} \tag{10}$$

Then the smallest integer m is called type 2 primitive index of P, s.t. $g_m(P^*)$ is positive. For example, if m = 5, then j = 3. Thus $g_m(P^*)$ = $(P^*)^1 + (P^*)^3 + (P^*)^5$ is a positive matrix, whereas $(P^*)^0+(P^*)^2+(P^*)^4$ and $(P^*)^1+(P^*)^3$ are not positive matrix. if m = 6, then j = 3. Thus $g_m(P^*)=(P^*)^0+(P^*)^2+(P^*)^4+(P^*)^6$ is a positive matrix, whereas $(P^*)^1+(P^*)^3+(P^*)^5$ and $(P^*)^0+(P^*)^2+(P^*)^4$ are not positive matrix.

Theorem 2. Let $R_2(P)$ be the type 2 primitive indexes of P. Then, there is no any independent impossible differential r of $F_{SP}^{(r)}$ for $r \ge 2R_2(P)+5$ (detailed proof, see P12-14**[14]**).

4.2 Cryptanalysis of MIBS Cipher

MIBS [19] is proposed by M.Izadi et al. in CANS 2009. It is a lightweight block cipher with 64-bit block size and 32-round. MIBS supports two key sizes 64-bit and 80-bit. The experimental results show that MIBS has a good performance in constrained resource environments such as RFID tags and sensor networks. MIBS is a typical block cipher of the Feistel structure and its round function(**Fig. 8**) includes three steps:

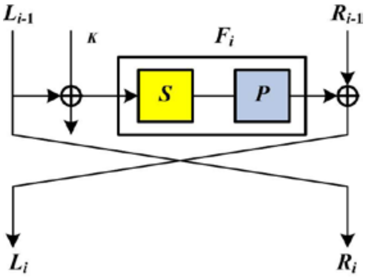

Fig. 8. The structure of the block cipher MIBS

(1) addroundkey, the 32-bit L_{i-1}, the left half of the state , is XORed with a 32-bit round key.

(2) S layer, the nonlinear S -boxes transformations, divides the 32-bit intermediate state into eight 4-bit nibbles and puts them into the same eight 4 × 4 S-boxes.

(3) P layer, linear transformations layer(with branch number 5).

Let the $b_i \in F_{2^4}$ and $c_i \in F_{2^4}$ be the input and output of the P layer, respectively, for i = 1,…,8. The linear permutations(**Fig. 9**) is as follows.

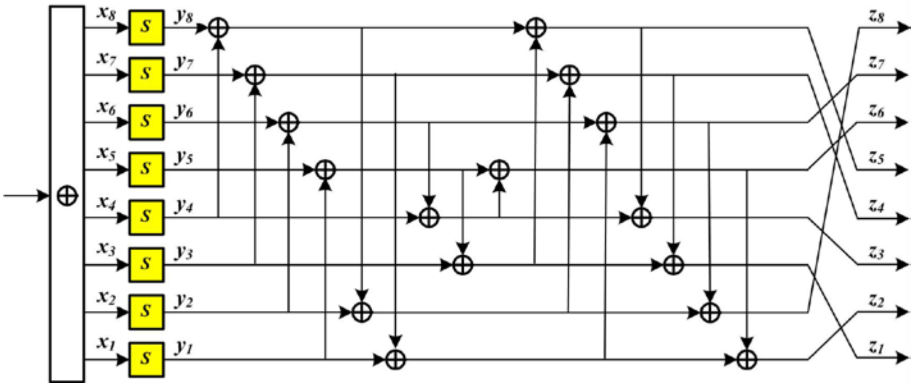

Fig. 9. The round function of MIBS

So, P can be also written 8 × 8 matrix over $F_{2^4}^{8\times 8}$. P and $(P^*)^2$ as followins.

$$P^* = P = \begin{bmatrix} 1&1&0&1&1&0&1&1 \\ 0&1&1&1&1&1&1&0 \\ 1&1&1&0&1&1&0&1 \\ 0&1&1&1&0&0&1&1 \\ 1&0&1&1&1&0&1&1 \\ 1&1&0&1&1&1&0&0 \\ 1&1&1&0&0&1&1&0 \\ 1&0&1&1&0&1&1&1 \end{bmatrix}, \quad (P^*)^2 = \begin{bmatrix} 4&4&5&5&3&3&5&4 \\ 4&5&5&4&4&4&3&3 \\ 5&4&4&5&5&4&3&4 \\ 3&4&5&3&2&4&4&3 \\ 4&3&4&4&3&2&3&5 \\ 3&4&3&5&4&2&3&3 \\ 4&5&3&3&4&4&3&2 \\ 5&5&4&4&3&4&4&4 \end{bmatrix}$$

Obviously, if $|\chi(\mathrm{Y})|=1$, then $|\chi(\mathrm{Z})|=8$. In other words, P^* is not a positive matrix, however, $(P^*)^2$ is a positive matrix. So, $(P^*)^2$ + I is positive, where I is the identity matrix. Then we have $R_2(P)$ = 2 and get the following conclusion:

Proposition 4. There is no any more than or equal to 9-round $(2R(P)+5)$ independent impossible differential of ε^{MIBS}. Or equivalently, there is no any 9-round independent impossible differential of the MIBS unless considering the details of the S-boxes.

In EUROCRYPT 2017, Yu Sasaki and Yosuke Todo presented a new tool searching for impossible differentials of MIBS [22]. They found an impossible difference path with a maximum of 8 rounds, such as (00000000, 000a0000)->(00000b00, 00000000). The impossible difference path is consistent with our conclusion in proposition 4.

5. Conclusion

In this paper, we mainly explored the security of structures against impossible differential and determined whether there exists an r-round impossible differential of an SPN structure or an independent impossible differential of a Feistel structure with SP-type round functions. The main factor of influencing impossible differential cryptanalysis is the length of the rounds of the impossible differentials because the attack will be more close to the real encryption algorithm with the number becoming longer.

We first analyse Kuznyechik, which is the national standard of the Russian Federation in 2015, and draw the conclusion that there is no any 3-round impossible differential of the Kuznyechik with only considering the linear permutations.

Although we are only interested in the truncated impossible differentials, we apply the matrix to express the linear transformation layer and use the matrix method to quickly ascertain the upper bound of the longest impossible differentials for several block ciphers ignoring the nonlinear transformations. The matrix method can be extended to many other block cipher.

As a result, we show that, unless considering the details of the S-boxes, there is no any 3-round, 5-round and 7-round impossible differentials for Kuznyechik, KLEIN and Midori64 respectively and there is no any 9-round independent impossible differential for MIBS.

Acknowledgements

This work is partially supported by National Natural Science Foundation of China (Nos. 61672330, 61602287 and 11771256), and the Key Research Development Project of Shandong Province (Nos.2015GGX101047 and 2016GGX101024).

References

[1] E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard," *Springer-Verlag*, pp. 1-151, 1993. Article(CrossRefLink).

[2] E. Biham and A. Biryukov and A. Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials," *Advances in Cryptology — EUROCRYPT '99*, Vol. 1592, pp. 12-23, 1999. Article(CrossRefLink).

[3] L.R. Knudsen, "DEAL-A 128-bit block cipher," *Complexity*, pp. 1-151, 1998.

[4] C. Blondeau, "Impossible differential attack on 13-round Camellia-192," I*nformation Processing Letters*, Vol. 115, pp.660-666, 2015. Article(CrossRefLink).

[5] C. Boura and M. Naya-Plasencia and V. Suder, "Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon," *ASIACRYPT*, Vol. 8873, pp. 179-199, 2014. Article(CrossRefLink).

[6] R. Li and B. Sun and C. Li, "Impossible differential cryptanalysis of SPN ciphers," *IET Information Security*, Vol. 5, pp. 111-120, 2011.

[7] B. Sun and P. Zhang and C. Li, "Impossible Differential and Integral Cryptanalysis of Zodiac," *Journal of Software*, Vol. 22, pp. 1911-1917, 2011.

[8] C. Du and J. Chen, "Impossible Differential Cryptanalysis of ARIA Reduced to 7 rounds," *CANS*, Vol.6467, pp. 20-30, 2010. Article(CrossRefLink).

[9] S. Sun and L. Hu and P. Wang, "Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers," *ASIACRYPT*, Vol. 8873, pp. 158-178, 2014. Article(CrossRefLink).

[10] J. Kim and S. Hong and J. Lim, "Impossible differential cryptanalysis using matrix method," *Discrete Mathematics*, Vol. 310, pp. 988-1002, 2010. Article(CrossRefLink).

[11] Y. Luo and X. Lai and Z. Wu and G. Gong, "A unified method for finding impossible differentials of block cipher structures," *Information Science*, Vol. 263, pp. 211-220, 2014. Article(CrossRefLink).

[12] S. Wu and M. Wang, "Automatic Search of Truncated Impossible Differentials for Word-Oriented Block Ciphers," *INDOCRYPT*, Vol. 7668, pp. 283-302, 2012. Article(CrossRefLink).

[13] B. Sun and Z. Liu and V. Rijmen and R. Li and L. Cheng and Q. Wang and H. AlKhzaimi and C. Li, "Links Among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis," *CRYPTO*, Vol.9215, pp. 95-115, 2015. Article(CrossRefLink).

[14] B. Sun and M. Liu and J. Guo and V. Rijmen and R. Li, "Provable Security Evaluation of Structures against Impossible Differential and Zero Correlation Linear Cryptanalysis," *EUROCRYPT*, Vol. 9665, pp. 196-213, 2016. Article(CrossRefLink).

[15] "Information technology CRYPTOGRAPHIC DATA SECURITY Block ciphers," *NATIONAL STANDARD OF THE RUSSIAN FEDERATION*, GOST R 34.12-2015, 2015.

[16] Z. Gong and S. Nikova and Y. Law, "KLEIN: A New Family of Lightweight Block Ciphers," *RFIDSec*, Vol. 7055, pp. 1-18, 2012. Article(CrossRefLink).

[17] Z. Ahmadian and M. Salmasizadeh and M.R. Aref, "Biclique Cryptanalysis of the Full-Round KLEIN Block Cipher," *Iet Information Security*, Vol. 9, pp. 294-301, 2015. Article(CrossRefLink).

[18] S. Banik and A. Bogdanov and T. Isobe and K. Shibutani and H. Hiwatari and T. Akishita and F. Regazzoni, "Midori: A Block Cipher for Low Energy (Extended Version)," *ASIACRYPT*, Vol. 9453, pp. 411-436, 2015. Article(CrossRefLink).

[19] M. Zadi and B. Sadeghiyan and S. Sadeghian, "MIBS: a new lightweight block cipher," *CANS*, Vol. 5888, pp. 334-348, 2009. Article(CrossRefLink).

[20] A. Bay and J. Nakahara and S. Vaudenay, "Cryptanalysis of reduced-round MIBS block cipher," *CANS*, Vol. 6467, pp. 1-19, 2010. Article(CrossRefLink) .

[21] Z. Chen and X. Wang, "Impossible differential cryptanalysis of midori," *Cryptology ePrint Archive*, Report 2016/535. Article(CrossRefLink).

[22] S. Yu and Y. Todo, "New Impossible Differential Search Tool from Design and Cryptanalysis Aspects," Vol. 2017, pp.185-215. Article(CrossRefLink).

Guoyong Han is a Ph.D. candidate in the School of Information Science and Engineering, Shandong Normal University, Jinan, China. He received the B.E. (2002), and the M.E.(2006)degrees from Shan dong University, Jinan, China. He is an Associate Professor in the School of Management Engineering of the Shandong Jianzhu University. His research interests include information security and analysis and design of block ciphers. He has published over 10 research papers in refereed academic journals and conferences.

Wenying Zhang received her Ph.D.degree in Cryptography in Department of Information Research, Information Engineering University of PLA in June 2004 in Zhengzhou, Henan, China.
From July 2004 to September 2006, she was a Postdoctoral Fellow at the Institute of Software, Chinese Academy of Sciences, Beijing, China. She is now a professor and Ph.d. supervisor of Shandong Normal University. Her research interests include cryptography, Boolean function, hash function analysis. (Email:wenyingzh@sohu.com)

Hongluan Zhao received her PhD from the School of Mathematics of the Shandong University in 2007. Currently, she is an Associate Professor in the School of Computer Science and Technology of the Shandong Jianzhu University. Her research interests include computer network and information security.