Discrete Mathematics 310 (2010) 988–1002

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Impossible differential cryptanalysis using matrix method[☆]

Jongsung Kim[a], Seokhie Hong[b,*], Jongin Lim[b]

[a] Division of e-Business, Kyungnam University, 449 Wolyeong-dong, Masan, Kyungnam, Republic of Korea

[b] Center for Information Security Technologies (CIST), Korea University, Anam Dong, Sungbuk Gu, Seoul, Republic of Korea

ARTICLE INFO

Article history:
Received 22 September 2008
Received in revised form 20 October 2009
Accepted 23 October 2009
Available online 19 November 2009

Keywords:
Cryptanalysis
Block ciphers
Impossible differential cryptanalysis
Matrix method
Feistel
Rijndael
Skipjack

ABSTRACT

The general strategy of impossible differential cryptanalysis is to first find impossible differentials and then exploit them for retrieving subkey material from the outer rounds of block ciphers. Thus, impossible differentials are one of the crucial factors to see how much the underlying block ciphers are resistant to impossible differential cryptanalysis. In this article, we introduce a widely applicable matrix method to find impossible differentials of block cipher structures whose round functions are bijective. Using this method, we find various impossible differentials of known block cipher structures: Nyberg's generalized Feistel network, a generalized CAST256-like structure, a generalized MARS-like structure, a generalized RC6-like structure, Rijndael structures and generalized Skipjack-like structures. We expect that the matrix method developed in this article will be useful for evaluating the security of block ciphers against impossible differential cryptanalysis, especially when one tries to design a block cipher with a secure structure.

© 2009 Elsevier B.V. All rights reserved.

1. Introduction

Differential cryptanalysis [5] and linear cryptanalysis [11] are known to be very powerful cryptanalytic tools for block ciphers. Since differential cryptanalysis and linear cryptanalysis were introduced in 1990 and in 1993, they have been applied to many known ciphers very effectively. So, designers have tried to build block ciphers secure against differential and linear cryptanalysis. Nyberg and Knudsen first proposed the concept of provable security against differential cryptanalysis and demonstrated provable security for a Feistel structure in 1992 [15].[1] Since then, many block cipher structures with provable security against differential and linear cryptanalysis have been studied [8,15–17], including the MISTY block cipher [12]. However, provable security against differential and linear cryptanalysis is not enough to guarantee the security of block ciphers, because other forms of cryptanalysis may be successfully applied to those not vulnerable to differential and linear cryptanalysis. For instance, differential and linear probabilities for a 3-round Feistel structure are upper-bounded by a small value under the assumption that its round functions are bijective and strong against differential and linear cryptanalysis [1,15]. However, there exists an impossible differential for a 5-round Feistel structure with any bijective round functions [9]. Similar observations hold for certain other block cipher structures.

Impossible differential cryptanalysis, which is a variant of differential cryptanalysis, was first introduced in 1998 by Knudsen to conduct a security evaluation of an AES candidate, DEAL [9], and was later extended in 1999 by Biham et. al.

☆ A preliminary version of this article was presented at Indocrypt 2003 with the title "Impossible Differential Cryptanalysis for Block Cipher Structures" and appeared in *Lecture Notes in Computer Science*, Vol. 2904, pp. 82–96, Springer-Verlag, 2003. This work was supported by the Second Brain Korea 21 Project.

* Corresponding author.
E-mail addresses: jongsungk@kyungnam.ac.kr (J. Kim), hsh@cist.korea.ac.kr (S. Hong), jilim@korea.ac.kr (J. Lim).

[1] Independently from the Nyberg-Knudsen method, in 1998, Vaudenay proposed another method for provable security against differential and linear cryptanalysis based on the decorrelation theory [18,19].

0012-365X/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2009.10.019

Table 1
Summary of some of our cryptanalytic results.

Structure	#subblocks	DC[a]	#F[c]	Ref.
GFN_n	$2n$	$r \geq 3n$	$f \geq 3n^2$	[16]
Skipjack-(A_n)	n	$r \geq n^2 - 1$	$f \geq n^2 - 1$	[17]
Structure	**#subblocks**	**IDC[b]**	**#F[c]**	**Ref.**
GFN_2	4	$r = 7$	$f = 14$	Section 5.1
GFN_n ($n \geq 3$)	$2n$	$r = 3n + 2$	$f = 3n^2 + 2n$	Section 5.1
Generalized CAST256	n	$r = n^2 - 1$	$f = n^2 - 1$	[17]
Generalized MARS	n	$r = 2n - 1$	$f = 2n - 1$	Section 5.1
Generalized RC6	$2n$	$r = 4n + 1$	$f = 4n^2 + n$	Section 5.1
Rijndael_{128}	16	$r = 3$	$f = 48$	[4]
Rijndael_{192}	24	$r = 4$	$f = 96$	Section 5.2
Rijndael_{256}	32	$r = 5$	$f = 160$	Section 5.2
Skipjack-(A_n)	n	$r = n^2 - 1$	$f = n^2 - 1$	[17]
Skipjack-(A_n)	n	$r = n^2$	$f = n^2$	Section 5.3
Skipjack-(nA_n, nB_n)	n	$r = 5n - 1$	$f = 5n - 1$	Section 5.3
Skipjack-($2nA_n, 2nB_n$)	n	$r = 4n - 3$	$f = 4n - 3$	Section 5.3
Skipjack-($3nA_n, 3nB_n$)	n	$r = 5n - 4$	$f = 5n - 4$	Section 5.3

DC: Differential cryptanalysis, IDC: Impossible DC. See Section 2 for the details of the structures stated in this table.
[a] The number of rounds (r) for which differential probabilities are upper bounded by a small value, if round functions are bijective and strong against DC.
[b] The number of rounds (r) for impossible differentials.
[c] The number of round functions (f) contained in r rounds.

to analyze iterative block ciphers such as IDEA and Skipjack [2,3]. Up to now, impossible differential cryptanalysis has been more effectively applied to many block ciphers like IDEA, Skipjack and AES than differential and linear cryptanalysis have been [2,3,10]. Security against impossible differential cryptanalysis depends on several factors such as the length of impossible differentials, specific input/output forms of impossible differentials and the strength of the round function. In general, the existence of impossible differentials is one of the most important factors affecting security against impossible differential cryptanalysis. They are usually built under a miss-in-the-middle approach[2]; an impossible differential is based on two consecutive probability-one differentials which contradict in the middle. Two such differentials are connected to form an impossible differential.

In this article, we focus on the impossible differential cryptanalysis for block cipher structures whose round functions are bijective. We provide a general cryptanalytic tool using matrices, which can find various impossible differentials of block cipher structures. We also provide an algorithm to compute the maximum length of impossible differentials that can be found using this matrix method.[3] We exploit the matrix method to find various impossible differentials of known block cipher structures. See Table 1 for a summary of our results: according to our results, the generalized MARS-like structure has the best resistance to the matrix method among all the analyzed structures stated in Table 1, from the viewpoint of the number of round functions (f) contained in r-round impossible differentials.

This article is organized as follows. In Section 2, we describe generalized Feistel, Rijndael and Skipjack-like structures. In Section 3, we introduce some basic notions for impossible differential cryptanalysis and the matrix method. In Section 4, we propose an algorithm to compute the maximum length of impossible differentials generated by the matrix method. In Section 5, we find various impossible differentials of generalized Feistel, Rijndael and Skipjack-like structures. In Section 6, we discuss how to apply the matrix method to other attacks, and in Section 7, we draw conclusions.

2. Descriptions of block cipher structures

2.1. Generalized Feistel structures

A generalized Feistel structure was first introduced by Nyberg [16]. Let $(X_0, X_1, \ldots, X_{2n-1})$ be the input to a round of the structure. Given n round functions $F_0, F_1, \ldots, F_{n-1}$ and n round keys $K_0, K_1, \ldots, K_{n-1}$, the output of the round $(Y_0, Y_1, \ldots, Y_{2n-1})$ is computed by the following formulas.

$$\begin{aligned} &Y_{2j} = X_{2j-2} && \text{for } 1 \leq j \leq n-1, \\ &Y_{2j-1} = F_j(X_{2j} \oplus K_j) \oplus X_{2j+1} && \text{for } 1 \leq j \leq n-1, \\ &Y_0 = F_0(X_0 \oplus K_0) \oplus X_1, && Y_{2n-1} = X_{2n-2}. \end{aligned}$$

We denote this generalized Feistel network with n round functions by GFN_n. If F_j is regarded as a keyed-round function F and $n = 4$, a round of GFN_4 is depicted as in Fig. 1.

[2] Not all impossible differentials are necessarily constructed under the miss-in-the-middle approach. Some other techniques include the shrinking technique [3], or simply using just one long differential that never results in a certain output difference.

[3] Note that the matrix method is one of the tools to find impossible differentials, which can then be used to carry out impossible differential cryptanalysis.

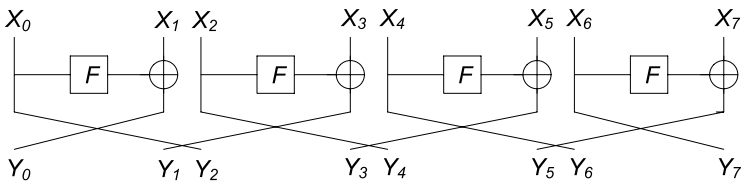

Fig. 1. A round of GFN_4.

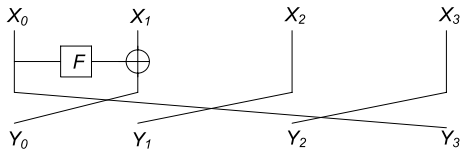

Fig. 2. A round of the CAST256-like structure ($n = 4$).

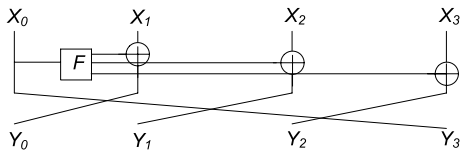

Fig. 3. A round of the MARS-like structure ($n = 4$).

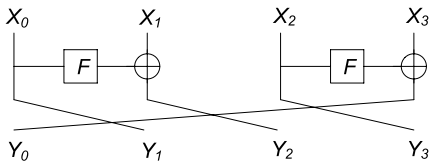

Fig. 4. A round of the RC6-like structure ($n = 2$).

We describe here three other existing generalized Feistel structures, named generalized CAST256-like, MARS-like and RC6-like structures [13].[4] Single rounds of these structures are described as follows (refer to Figs. 2–4).

Generalized CAST256-like Structure:

$$Y_0 = F(X_0) \oplus X_1, \quad Y_{n-1} = X_0,$$
$$Y_j = X_{j+1} \quad \text{for } 1 \le j \le n-2.$$

Generalized MARS-like Structure:

$$Y_j = F(X_0) \oplus X_{j+1} \quad \text{for } 0 \le j \le n-2,$$
$$Y_{n-1} = X_0.$$

Generalized RC6-like Structure:

$$Y_{2i-1} = X_{2i-2} \quad \text{for } 1 \le i \le n,$$
$$Y_{2j} = F(X_{2j-2}) \oplus X_{2j-1} \quad \text{for } 1 \le j \le n-1,$$
$$Y_0 = F(X_{2n-2}) \oplus X_{2n-1}.$$

2.2. Rijndael structures

Rijndael [6] is a block cipher with an SPN structure (the SPN structure modifies all the subblocks in a round, while the Feistel structure modifies only a subset of the subblocks). The length of the data block can be specified to be 128, 192, or 256 bits: we denote these structures with 128, 192 and 256-bit blocks by Rijndael_{128},[5] Rijndael_{192} and Rijndael_{256} structures,

[4] The block ciphers CAST256, MARS and RC6 were all the Advanced Encryption Standard (AES) candidates, and MARS and RC6 were in the five AES finalists.

[5] The block cipher Rijndael_{128} is the AES, which is the one of the most widely used encryption standards in the world.

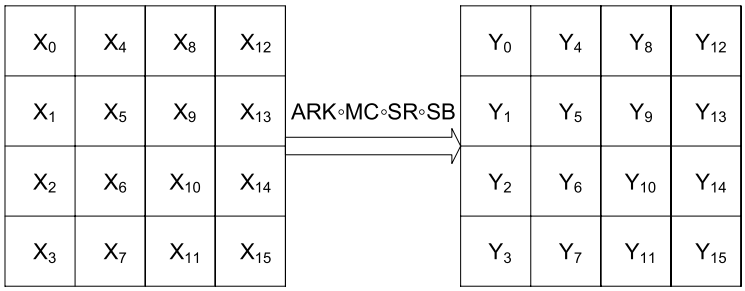

Fig. 5. A round of Rijndael with a 128-bit data block.

respectively. They are expressed as arrays of 4×4 bytes, 4×6 bytes, and 4×8 bytes. A round of Rijndael consists of four transformations: SubByte (SB), ShiftRow (SR), MixColumn (MC) and AddRoundKey (ARK).

- SB is a nonlinear byte-wise substitution that applies the same 8×8 S-box to every byte.
- SR is a cyclic shift of the ith row by i bytes to the left (for Rijndael_{256}, SR operates cyclic shifts of the 0th, 1st, 2nd and 3rd rows by 0, 1, 3 and 4 bytes to the left, respectively).
- MC is a matrix multiplication over a finite field applied to each column (its byte branch number is 5).
- ARK is an exclusive-or with the round key.

Refer to [6] for the details of these four transformations. A round of Rijndael_{128} is depicted in Fig. 5 (note that $(f \circ g)(x)$ represents $f(g(x))$).

In this article, we observe the structures of Rijndael whose nonlinear byte-wise substitutions, S-boxes, are considered as bijective black boxes. The S-boxes can be viewed as round functions F implying that Rijndael_{128}, Rijndael_{192} and Rijndael_{256} include 16, 24 and 32 F functions in each round.

2.3. Generalized Skipjack-like structures

Skipjack [14] is a 64-bit symmetric-key block cipher designed by the US National Security Agency (NSA), used in tamper-resistant Capstone and Clipper chips for US government communication purposes. It is an iterative block cipher using two types of rounds, called Rule A and Rule B. Within the Skipjack cipher, the data block is divided into four subblocks, and eight rounds of Rule A and eight rounds of Rule B are applied alternatively until the full 32 rounds are achieved. In this article, we consider various generalized Skipjack-like structures which use generalizations of Rule A and Rule B; we denote these generalizations of Rule A and Rule B by Rule A_n and Rule B_n. They are depicted in Fig. 6 and described as follows.

$$\text{Rule } A_n \begin{cases} Y_0 = F(X_0) \oplus X_{n-1}, \quad Y_1 = F(X_0), \\ Y_j = X_{j-1} \quad \text{for } 2 \le j \le n-1. \end{cases}$$

$$\text{Rule } B_n \begin{cases} Y_0 = X_{n-1}, \quad Y_1 = F(X_0), \quad Y_2 = X_0 \oplus X_1, \\ Y_j = X_{j-1} \quad \text{for } 3 \le j \le n-1. \end{cases}$$

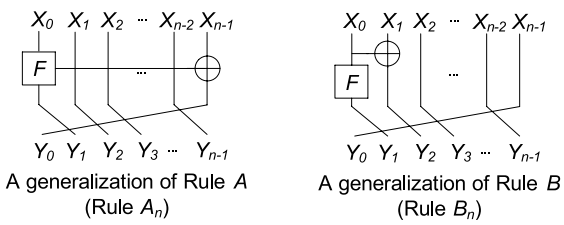

Fig. 6. Single rounds of Skipjack-(A_n) and Skipjack-(B_n).

We observe a generalized Skipjack-like structure which uses Rule A_n, iteratively. This structure was already presented in [17]. We denote this structure by Skipjack-(A_n). Naturally, we can also think of another generalized Skipjack-like structure, called Skipjack-(B_n), which uses Rule B_n, iteratively. Furthermore, we take into account some other generalizations of Skipjack which alternatively use Rule A_n and Rule B_n; precisely, we observe the structures which apply t rounds of Rule A_n and t rounds of Rule B_n, alternatively, until a desired number of rounds is achieved. We denote these structures by Skipjack-(tA_n, tB_n). In our notation, the original Skipjack structure is the 32-round Skipjack-$(8A_4, 8B_4)$.

3. Matrix method for impossible differential cryptanalysis

In this section, we introduce the matrix method for finding impossible differentials of block cipher structures. We assume that a block cipher structure $\mathcal{S}$ has n data subblocks, and thus the input and the output of a round are $(X_0, X_1, \ldots, X_{n-1})$ and $(Y_0, Y_1, \ldots, Y_{n-1})$, respectively. Throughout the article, we consider $\mathcal{S}$ whose round functions F are all bijective, and for which the operation to connect a subblock with another one is XOR, denoted $\oplus$. In order to obtain a general cryptanalytic tool for impossible differential cryptanalysis, we first define matrices which represent a round of a block cipher structure.

Definition 1. For a block cipher structure $\mathcal{S}$, the $n \times n$ Encryption Characteristic Matrix $\mathcal{E}$ and the $n \times n$ Decryption Characteristic Matrix $\mathcal{D}$ are defined as follows.

- **Constructing E**: If Y_j is affected by X_i (*affected* means $Y_j = X_i \oplus b$, where b is a certain value), the (i, j) entry of $\mathcal{E}$ is set to 1. In particular, if Y_j is affected by $F(X_i)$ or $F^{-1}(X_i)$, the (i, j) entry of $\mathcal{E}$ is set to 1_F instead of 1. If Y_j is not affected by X_i, the (i, j) entry of $\mathcal{E}$ is set to 0.
- **Constructing D**: If X_j is affected by Y_i, the (i, j) entry of $\mathcal{D}$ is set to 1. In particular, if X_j is affected by $F(Y_i)$ or $F^{-1}(Y_i)$, the (i, j) entry of $\mathcal{D}$ is set to 1_F instead of 1. If X_j is not affected by Y_i, the (i, j) entry of $\mathcal{D}$ is set to 0.

If the number of 1 entries in each column of the matrix is zero or one, we call it **property-one matrix** (note that the entry 1 is different from the entry 1_F).

Definition 1 shows that each entry of the encryption/decryption characteristic matrix has one of the three values, 0, 1 or 1_F, and the ith entry of column j represents whether or not the ith subblock of input affects the jth subblock of output (for the encryption direction X_i is the ith subblock of input, while for the decryption direction Y_i is the ith subblock of input).

For example, $\mathcal{E}$ and $\mathcal{D}$ of the Feistel structure depicted in Fig. 7 are computed as follows.

$$\mathcal{E} = \begin{pmatrix} 1_F & 1 \\ 1 & 0 \end{pmatrix}, \qquad \mathcal{D} = \begin{pmatrix} 0 & 1 \\ 1 & 1_F \end{pmatrix}.$$

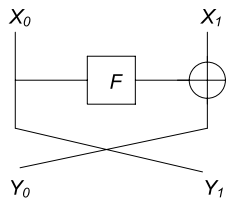

Fig. 7. A round of a Feistel structure.

According to Definition 1, the Feistel structure has property-one matrices $\mathcal{E}$ and $\mathcal{D}$. If $\mathcal{S}$ has property-one matrices $\mathcal{E}$ and $\mathcal{D}$, we can automatically find various impossible differentials of $\mathcal{S}$ by the matrix method. In this section, we assume that $\mathcal{S}$ has property-one matrices $\mathcal{E}$ and $\mathcal{D}$.

Next, we define difference vectors which represent the types of differences over rounds, and then explain how to calculate difference vectors by using the encryption/decryption characteristic matrix and prior difference vectors. Our focus is not on specific differences over rounds but on difference vectors which are useful for finding impossible differentials of $\mathcal{S}$.

For a given input difference, the possible output differences of each subblock after one or more rounds can be classified into five types of differences: (1) zero difference, (2) a nonzero nonfixed difference, (3) a nonzero fixed difference, (4) exclusive-or of a nonzero fixed difference and a nonzero nonfixed difference, and (5) a nonfixed difference (*fixed difference* represents a difference which has not been affected by any round key, i.e., by any F function, and *nonfixed difference* represents a difference which has been affected by at least one round key, i.e., by at least one F function). It is easy to see that any subblock difference belongs to one of these five types.

Definition 2. The five types of differences are defined as the entries of difference vectors in Table 2 (note that entry t in Table 2 is an integer greater than or equal to 2).

Table 2
Entries of difference vectors and corresponding differences.

Entries of difference vectors	Corresponding differences
0	zero diff. (denoted 0)
1	nonzero nonfixed diff. (denoted δ)
1^*	nonzero fixed diff. (denoted γ)
2^*	nonzero fixed diff. $\oplus$ nonzero nonfixed diff. (denoted $\gamma \oplus \delta$)
$t(\geq 2)$	nonfixed diff. (denoted ?)

Note that the symbols 0 and 1 can appear either as entries in the encryption/decryption characteristic matrix, or as entries in a difference vector. They have different meanings in these two different contexts.

The classification of the entries in Table 2 allows us to distinguish usable ones for finding impossible differentials (all the entries except for $t(\geq 2)$ are usable for it, which will be explained below). Throughout this article, we use the notation $0,\ \delta,\ \gamma$, and ? as the differences stated in Table 2; sometimes δ' (resp., γ') is used as the same kind of a difference δ (resp., γ). We will not be able to gain any information from the entry $t(\geq 2)$, as this entry can correspond to any subblock difference, however, in the cases of the entries $0,\ 1,\ 1^*$ and 2^*, we can gain some useful information for the construction of impossible differentials; more precisely, we are able to know the differences that these entries cannot correspond to. For example, if 2^* corresponds to $\gamma \oplus \delta$, then it cannot correspond to γ, since $\gamma \oplus \delta \neq \gamma$ (in fact, 2^* can correspond to any difference which is different from γ). This fact is useful for finding impossible differentials of $\mathcal{S}$.

For a given input difference α, we denote the r-round output difference by α^r, and denote the ith subblock of α (resp. α^r) by α_i (resp. α_i^r). Similarly, the difference vector which corresponds to α (resp. α^r) is denoted by $\vec{a}$ (resp. $\vec{a}^r$), and the ith entry of $\vec{a}$ (resp. $\vec{a}^r$), which corresponds to α_i (resp. α_i^r), is denoted by a_i (resp. a_i^r). If the same analysis is performed through the decryption process, we use the notation β, β_i, β^r, β_i^r, $\vec{b}$, b_i, $\vec{b}^r$, and b_i^r instead of α, α_i, α^r, α_i^r, $\vec{a}$, a_i, $\vec{a}^r$, and a_i^r, respectively (note that $\alpha = \alpha^0, \vec{a} = \vec{a}^0$ and $\beta = \beta^0, \vec{b} = \vec{b}^0$).

The following definition is a specific case for Definition 2.

Definition 3. Given an input difference $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ (resp. $\beta = (\beta_0, \beta_1, \ldots, \beta_{n-1})$), the difference vector $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$ (resp. $\vec{b} = (b_0, b_1, \ldots, b_{n-1})$) corresponding to α (resp. β) is defined as follows.

$$a_i \text{ (resp. } b_i) \triangleq \begin{cases} 0 & \text{if } \alpha_i = 0 \text{ (resp. } \beta_i = 0) \\ 1^* & \text{otherwise.} \end{cases}$$

Note that the reason why a_i and b_i contain only 0 or 1^* (fixed difference) is that the initial input differences α and β have not yet been affected by any round key (in our analysis, the key guessing phase for outer rounds of block ciphers is out of our focus: it follows that a_i and b_i cannot be 1, 2^* or $t(\geq 2)$).

In order to compute $\vec{a}^r$, we need to define a multiplication between a difference vector and an encryption characteristic matrix. (We omit the explanation for the decryption process, since it is the same as the encryption process.) A difference vector $\vec{a}^r$ can be successively computed as in Eq. (1).

$$\begin{aligned} \vec{a}^r &= ((((\vec{a} \cdot \overbrace{\mathcal{E}) \cdot \mathcal{E}) \cdots) \cdot \mathcal{E})}^{r \text{ times}} = ((((\vec{a}^1 \cdot \overbrace{\mathcal{E}) \cdot \mathcal{E}) \cdots) \cdot \mathcal{E})}^{r-1 \text{ times}} \\ &= \cdots = \vec{a}^{r-1} \cdot \mathcal{E} \end{aligned} \tag{1}$$

We define a multiplication of $\vec{a}^r$ and $\mathcal{E}$: $\vec{a}^r \cdot \mathcal{E} = (a_i^r)_{1\times n} \cdot (\mathcal{E}_{i,j})_{n\times n} = \left(\sum_i a_i^r \cdot \mathcal{E}_{i,j}\right)_{1\times n}$, where $r \geq 0$.

First, we consider a multiplication between an entry of difference vector a_i^r and an entry of matrix $\mathcal{E}_{i,j}$. The multiplication $a_i^r \cdot \mathcal{E}_{i,j}$ represents how the input difference of the ith subblock corresponding to a_i^r affects the output difference of the jth subblock after a round (this depends on the value of $\mathcal{E}_{i,j}$).

Definition 4. Table 3 illustrates the definition and the meaning of the multiplication $a_i^r \cdot \mathcal{E}_{i,j}$ (recall that the entry a_i^r corresponds to the difference α_i^r).

Table 3
Multiplication between a difference vector entry and a matrix entry ($k \in \{0, 1, 1^*, 2^*, t(\geq 2)\}$).

$a_i^r \cdot \mathcal{E}_{i,j}$	Meaning
$k \cdot 0 = 0$	The output difference of the jth subblock is not affected by the input difference α_i^r.
$k \cdot 1 = k$	The output difference of the jth subblock is affected by the input difference α_i^r.
$k \cdot 1_F$	The output difference of the jth subblock is affected by the difference after F when the input difference of F is α_i^r.
$0 \cdot 1_F = 0$	For zero difference, the output difference after F is also zero.
$1^* \cdot 1_F = 1$	For a difference γ, the output difference after F is δ.
$1 \cdot 1_F = 1$	For a difference δ, the output difference after F is δ'.
$2^* \cdot 1_F = 2$	For a difference $\gamma \oplus \delta$, the output difference after F is ?.
$t \cdot 1_F = t$	For a difference ?, the output difference after F is also ?.

Note that according to Table 3, $\mathcal{E}_{i,j} = 1$ if and only if $x^* \cdot \mathcal{E}_{i,j} = x^*$, where x^* represents the difference vector entry 1^* or 2^*. We say *the matrix entry 1 is $*$-preserving*. Other matrix entries are not $*$-preserving: $\mathcal{E}_{i,j} = 0$ if and only if $x^* \cdot \mathcal{E}_{i,j} = 0$, and $\mathcal{E}_{i,j} = 1_F$ if and only if $x^* \cdot \mathcal{E}_{i,j} = x$.

Second, we define an addition of $a_i^r \cdot \mathcal{E}_{i,j}$ and $a_{i'}^r \cdot \mathcal{E}_{i',j}$, where $i \neq i'$. Since the addition of entries represents XOR of corresponding differences, it can be naturally defined as follows.

Definition 5. The addition of two entries which have not $*$ is defined as the usual addition over the integers. If one entry, denoted e, has not $*$ and the other has $*$, then the addition of these two entries is defined as follows (below, when the two operands for the $+$ operator are both integers, the operator represents the usual integer addition).

- If the entry e is 0 or 1, then $e + 1^* \triangleq (e+1)^*$, otherwise $e + 1^* \triangleq e + 1$.
- If the entry e is 0, $e + 2^* \triangleq (e+2)^*$, otherwise, $e + 2^* \triangleq e + 2$.

Recall that $\mathcal{E}$ is a property-one matrix by our assumption, i.e., the number of 1 entries in each column of $\mathcal{E}$ is at most one, and only the matrix entry 1 is $*$-preserving. It follows that there does not exist the addition of two entries both of which have $*$ (that is why we have not dealt with this case in Definition 5). Table 4 illustrates the relation between the addition of entries and exclusive-or of corresponding differences. Definitions 2, 4 and 5 show that the multiplication and addition are well defined (in the sense of the correspondence between difference vectors and differences over rounds). It is easy to see that the multiplication and addition are all defined over the integers, if the optional symbols $*$ and F (used in 1^*, 2^* and 1_F) are ignored in the computations.

Table 4
Relation of addition and exclusive-or.

Addition	Exclusive-or
$0 + k = k$	$0 \oplus \Delta = \Delta$
$1 + 1 = 2$	$\delta \oplus \delta' = ?$
$1 + 1^* = 2^*$	$\delta \oplus \gamma = \delta \oplus \gamma$
$1 + 2^* = 3$	$\delta \oplus (\delta' \oplus \gamma) = ?$
$1 + t = 1 + t$	$\delta \oplus ? = ?$
$1^* + t = 1 + t$	$\gamma \oplus ? = ?$
$2^* + t = 2 + t$	$(\gamma \oplus \delta) \oplus ? = ?$
$t + t' = t + t'$	$? \oplus ? = ?$

($k \in \{0, 1, 1^*, 2^*, t\}$, $t,\ t' \geq 2$, and Δ is the corresponding difference for k.)

To help understand the new operations, we take the Feistel structure as an example. If the input difference vectors $\vec{a}$ and $\vec{b}$ are $(0, 1^*)$ and $(1^*, 0)$, then $\vec{a}^r$ and $\vec{b}^r$ are computed by Eqs. (2) and (3); refer to Fig. 8.

$$\begin{aligned}
\vec{a}^1 = \vec{a} \cdot \mathcal{E} &= (0 \cdot 1_F + 1^* \cdot 1,\ 0 \cdot 1 + 1^* \cdot 0) \\
&= (0 + 1^*, 0 + 0) = (1^*, 0), \\
\vec{a}^2 = \vec{a}^1 \cdot \mathcal{E} &= (1^* \cdot 1_F + 0 \cdot 1,\ 1^* \cdot 1 + 0 \cdot 0) \\
&= (1 + 0, 1^* + 0) = (1, 1^*), \\
\vec{a}^3 = \vec{a}^2 \cdot \mathcal{E} &= (1 \cdot 1_F + 1^* \cdot 1,\ 1 \cdot 1 + 1^* \cdot 0) \\
&= (1 + 1^*, 1 + 0) = (2^*, 1), \\
\vec{a}^4 = \vec{a}^3 \cdot \mathcal{E} &= (2^* \cdot 1_F + 1 \cdot 1,\ 2^* \cdot 1 + 1 \cdot 0) \\
&= (2 + 1, 2^* + 0) = (3, 2^*), \\
\vec{a}^5 = \vec{a}^4 \cdot \mathcal{E} &= (3 \cdot 1_F + 2^* \cdot 1,\ 3 \cdot 1 + 2^* \cdot 0) \\
&= (3 + 2^*, 3 + 0) = (5, 3).
\end{aligned} \tag{2}$$

$$\begin{aligned}
\vec{b}^1 = \vec{b} \cdot \mathcal{D} &= (1^* \cdot 0 + 0 \cdot 1,\ 1^* \cdot 1 + 0 \cdot 1_F) \\
&= (0 + 0, 1^* + 0) = (0, 1^*), \\
\vec{b}^2 = \vec{b}^1 \cdot \mathcal{D} &= (0 \cdot 0 + 1^* \cdot 1,\ 0 \cdot 1 + 1^* \cdot 1_F) \\
&= (0 + 1^*, 0 + 1) = (1^*, 1), \\
\vec{b}^3 = \vec{b}^2 \cdot \mathcal{D} &= (1^* \cdot 0 + 1 \cdot 1,\ 1^* \cdot 1 + 1 \cdot 1_F) \\
&= (0 + 1, 1^* + 1) = (1, 2^*), \\
\vec{b}^4 = \vec{b}^3 \cdot \mathcal{D} &= (1 \cdot 0 + 2^* \cdot 1,\ 1 \cdot 1 + 2^* \cdot 1_F) \\
&= (0 + 2^*, 1 + 2) = (2^*, 3), \\
\vec{b}^5 = \vec{b}^4 \cdot \mathcal{D} &= (2^* \cdot 0 + 3 \cdot 1,\ 2^* \cdot 1 + 3 \cdot 1_F) \\
&= (0 + 3, 2 + 3) = (3, 5).
\end{aligned} \tag{3}$$

We are ready to show how to use the entries of difference vectors for finding impossible differentials of $\mathcal{S}$. We denote an r-round impossible differential with an input difference $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ and an r-round output difference $\beta = (\beta_0, \beta_1, \ldots, \beta_{n-1})$ by $\alpha \nrightarrow_r \beta$.

Property 1. *Using Definition 2 and the encryption process, we can get the following four types of impossible differentials.*

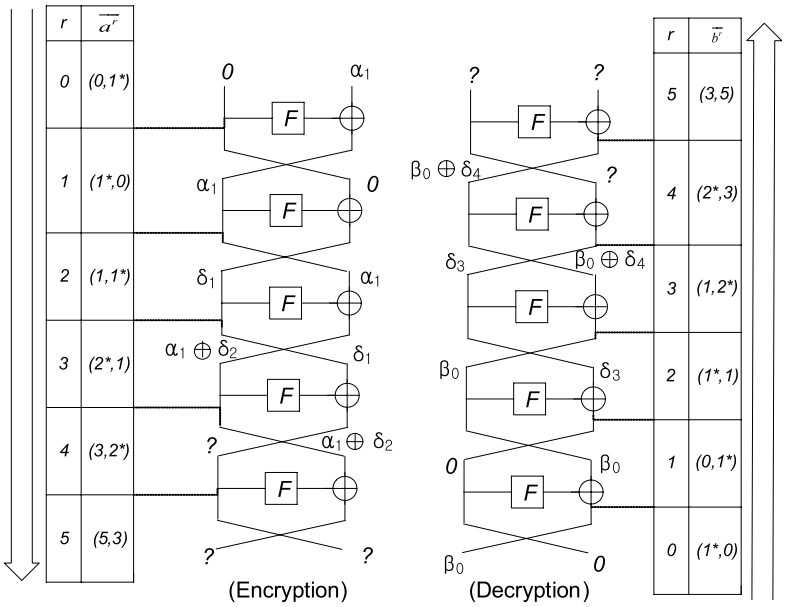

Fig. 8. Differences corresponding to $\vec{a}^r$ and $\vec{b}^r$, where $\vec{a} = (0, 1^*)$ and $\vec{b} = (1^*, 0)$ (α_1 and β_0 are nonzero fixed differences and δ_i are nonzero nonfixed differences).

- *If* $a_i^r = 0$, *then we have* $\alpha \nrightarrow_r \beta$, *where* $\beta_i \neq 0$.
- *If* $a_i^r = 1$, *then we have* $\alpha \nrightarrow_r \beta$, *where* $\beta_i = 0$.
- *If* $a_i^r = 1^*$, *say* γ, *then we have* $\alpha \nrightarrow_r \beta$, *where* $\beta_i \neq \gamma$.
- *If* $a_i^r = 2^*$, *say* $\gamma \oplus \delta$, *then we have* $\alpha \nrightarrow_r \beta$, *where* $\beta_i = \gamma$.

We can also get the other four types of impossible differentials by using the decryption process. As mentioned before, if $a_i^r = t (\geq 2)$, we cannot predict the difference corresponding to a_i^r. It follows that the entry t is useless for finding impossible differentials, however, the entries 0, 1, 1^* and 2^* are useful; we denote the set of these entries by $\mathcal{U} = \{0, 1, 1^*, 2^*\}$.

If $a_i^r \in \mathcal{U}$, as stated in Property 1, there exist r-round impossible differentials. Furthermore, $\mathcal{S}$ may have impossible differentials for more than r rounds, when $a_i^r \in \mathcal{U}$. To find these long impossible differentials, we need to define an auxiliary set $\bar{m}$ with respect to the entry $m \in \mathcal{U}$. $\bar{m}$ is defined with the following two properties: first, $\bar{m}$ is a subset of $\mathcal{U}$, and second, the elements of $\bar{m}$ correspond to the differences distinct from the specific difference associated with the entry m. Note that the second property for $\bar{m}$ does not mean that m should be excluded from $\bar{m}$. Consider $\bar{1^*}$ as an example. Assume that the entry 1^* corresponds to a nonzero fixed difference γ. Then, the entry 1^* cannot match the differences such as zero, $\gamma' (\neq \gamma)$ and $\gamma \oplus \delta$. So, we have $\bar{1^*} = \{0, 1^*, 2^*\}$. Similarly, we have $\bar{m}$ for other elements $m \in \mathcal{U}$.

Definition 6. For the entries $m \in \mathcal{U} = \{0, 1, 1^*, 2^*\}$, the entry sets $\bar{m}$ are defined as in Table 5.

Table 5
Differences corresponding to the entries $m \in \mathcal{U}$ and the entry sets $\bar{m}$.

m	Difference	$\bar{m}$	Difference
0	0	$\bar{0} = \{1, 1^*\}$	δ or γ
1	δ	$\bar{1} = \{0\}$	0
1^*	γ	$\bar{1^*} = \{0, 1^*, 2^*\}$	0 or $\gamma' (\neq \gamma)$ or $\gamma \oplus \delta$
2^*	$\gamma \oplus \delta$	$\bar{2^*} = \{1^*\}$	γ

How can we find impossible differentials for more than r rounds using $m \in \mathcal{U}$ and $\bar{m}$, when $a_i^r \in \mathcal{U}$? The solution is simple: we can obtain such long impossible differentials using both encryption and decryption difference vectors. Assume that $a_i^r = 2^*$ and $b_i^{r'} \in \bar{2^*}$. Recall that $a_i^r = 2^*$ means $\alpha_i^r = \alpha_j \oplus \delta$, where $\alpha_j \neq 0$ for some j, and $b_i^{r'} \in \bar{2^*}$ means $\beta_i^{r'} = \beta_k$, where $\beta_k \neq 0$ for some k (refer to Fig. 8). Hence, there exists an $(r + r')$-round impossible differential $\alpha \nrightarrow_{r+r'} \beta$, where $\alpha_j = \beta_k$. Similarly, this kind of impossible differential can be made by other elements of $\mathcal{U}$, and thus we have the following property.

Property 2. *For any element* $m \in \mathcal{U}$,

- *If* $a_i^r = m$ *and* $b_i^{r'} \in \bar{m}$ *for some* i, *then there exists* $\alpha \nrightarrow_{r+r'} \beta$.

- *If* $a_i^r \in \bar{m}$ *and* $b_i^{r'} = m$ *for some i, then there exists* $\alpha \nrightarrow_{r+r'} \beta$.

In order to compute the maximum number of rounds for impossible differentials that can be found using the matrix method,[6] we define the following.

Definition 7. Given an input difference vector $\vec{a}$, an entry $m \in \mathcal{U}$ and a set $\bar{m}$ in the encryption process,

$$\mathcal{ME}_i(\vec{a}, m) \triangleq max_r\{r | a_i^r = m\},$$
$$\mathcal{ME}_i(\vec{a}, \bar{m}) \triangleq max_{l \in \bar{m}}\{\mathcal{ME}_i(\vec{a}, l)\},$$
$$\mathcal{ME}_i(m) \triangleq max_{\vec{a} \neq 0}\{\mathcal{ME}_i(\vec{a}, m)\},$$
$$\mathcal{ME}_i(\bar{m}) \triangleq max_{\vec{a} \neq 0}\{\mathcal{ME}_i(\vec{a}, \bar{m})\}.$$

Given an input difference vector $\vec{b}$, an entry $m \in \mathcal{U}$ and a set $\bar{m}$ in the decryption process,

$$\mathcal{MD}_i(\vec{b}, m) \triangleq max_r\{r | b_i^r = m\},$$
$$\mathcal{MD}_i(\vec{b}, \bar{m}) \triangleq max_{l \in \bar{m}}\{\mathcal{MD}_i(\vec{b}, l)\},$$
$$\mathcal{MD}_i(m) \triangleq max_{\vec{b} \neq 0}\{\mathcal{MD}_i(\vec{b}, m)\},$$
$$\mathcal{MD}_i(\bar{m}) \triangleq max_{\vec{b} \neq 0}\{\mathcal{MD}_i(\vec{b}, \bar{m})\}.$$

We denote $max_{i,m}\{\mathcal{ME}_i(\vec{a}, m) + \mathcal{MD}_i(\vec{b}, \bar{m})\}$ by $\mathcal{M}(\vec{a}, \vec{b})$. Then, clearly it holds that $\mathcal{M}(\vec{a}, \vec{b}) = max_{i,m}\{\mathcal{ME}_i(\vec{a}, \bar{m}) + \mathcal{MD}_i(\vec{b}, m)\}$.

Let $max_{\vec{a} \neq 0, \vec{b} \neq 0}\{\mathcal{M}(\vec{a}, \vec{b})\}$ be denoted by $\mathcal{M}$, then $\mathcal{M}$ can be computed by Eq. (4), which will be used in the next section.

$$\begin{aligned} \mathcal{M} &= max_{i,m}\{\mathcal{ME}_i(m) + \mathcal{MD}_i(\bar{m})\} \\ &= max_{i,m}\{\mathcal{ME}_i(\bar{m}) + \mathcal{MD}_i(m)\}. \end{aligned} \tag{4}$$

Thus, we have the following theorem.

Theorem 1. *If a round function of a block cipher structure* $\mathcal{S}$ *is considered as a bijective black box and* $\mathcal{S}$ *has property-one matrices* $\mathcal{E}$ *and* $\mathcal{D}$*, then the maximum number of rounds for impossible differentials that can be found using the matrix method is* $\mathcal{M}$.

Toy example: If a round function of the Feistel structure is bijective, then the length $\mathcal{M}$ for the cipher is 5.

Using Eqs. (2) and (3), we have $\mathcal{M}((0, 1^*), (1^*, 0)) = 5$ induced from $a_1^3 = 2^*$ and $b_1^2 = 1^* \in \bar{2}^*$. Similarly, we can solve the equations related to other difference vectors, $\vec{a}$ and $\vec{b}$; using the equations, we can check that $\mathcal{M}(\vec{a}, \vec{b}) \leq 4$. So, we have $\mathcal{M} = max_{\vec{a} \neq 0, \vec{b} \neq 0}\{\mathcal{M}(\vec{a}, \vec{b})\} = 5$. Hence, the Feistel structure has a 5-round impossible differential whose form is $(0, \alpha_1) \nrightarrow_5 (\beta_0, 0)$, where $\alpha_1 = \beta_0 \neq 0$ (refer to Fig. 8). Note that this 5-round impossible differential has been observed in [9].

Note. The matrix method is also applicable to block cipher structures which use different operations rather than the XOR operation for the diffusion between different subblocks. For instance, when the + operation is used, the matrix method can be applied by adopting subtraction differences instead of XOR differences.

4. Algorithm to compute the length $\mathcal{M}$

In this section, we propose an algorithm to compute the length $\mathcal{M}$. The algorithm is applied to any block cipher structure $\mathcal{S}$ whose round functions are bijective, and encryption and decryption characteristic matrices $\mathcal{E}$ and $\mathcal{D}$ are property-one matrices.[7] We assume that the round functions of $\mathcal{S}$ are all bijective and $\mathcal{S}$ has property-one matrices $\mathcal{E}$ and $\mathcal{D}$.

The algorithm consists of five steps: (1) the first step is to form the encryption characteristic matrix, (2) the second step is to compute the values of $\mathcal{ME}_i(m)$, (3) the third step is to form the decryption characteristic matrix, (4) the fourth step is to compute the values of $\mathcal{MD}_i(\bar{m})$, and (5) the last step is to output the length $\mathcal{M}$ by applying the $\mathcal{ME}_i(m)$ and $\mathcal{MD}_i(\bar{m})$ computed in the previous steps to Eq. (4). See Algorithm 1. In step 1, the algorithm uses two variables to represent each entry of the matrix; a variable $e_{i,j}$ and an auxiliary variable $\widetilde{e}_{i,j}$ are assigned to represent $\mathcal{E}_{i,j}$: $e_{i,j} = 0$ if $\mathcal{E}_{i,j} = 0$, and $e_{i,j} = 1$ if $\mathcal{E}_{i,j} = 1$ or 1_F. $\widetilde{e}_{i,j}$ is determined to be 0 or 1 by whether or not $\mathcal{E}_{i,j}$ leads to the $*$-preserving property: $\widetilde{e}_{i,j} = 0$ if $\mathcal{E}_{i,j} = 1$ (which is $*$-preserving), and $\widetilde{e}_{i,j} = 1$ if $\mathcal{E}_{i,j} = 0$ or 1_F (which is not $*$-preserving). See the upper part of Table 6. Similarly, in step 2, for the ith entry of difference vector $\vec{a}^r$, a variable $a^{r,i}$ is assigned as its integer (after removing the symbol $*$ if it

[6] As stated above, one can construct impossible differentials using the encryption and decryption characteristic matrices, and difference vectors (i.e., using Properties 1 and 2). We call such a method "the matrix method".

[7] In fact, we may compute the number of rounds $\mathcal{M}$ by modifying the algorithm even though $\mathcal{E}$ and $\mathcal{D}$ are not property-one matrices (refer to Section 5.3.)

```
Step 1: Form the matrix ℰ = (ℰ_{i,j})_{n×n}.
for i = 0 to n − 1
   for j = 0 to n − 1
      if ℰ_{i,j} = 0, then e_{i,j} ← 0 and ẽ_{i,j} ← 1
      if ℰ_{i,j} = 1, then e_{i,j} ← 1 and ẽ_{i,j} ← 0
      if ℰ_{i,j} = 1_F, then e_{i,j} ← 1 and ẽ_{i,j} ← 1
Step 2: Compute the values of ℳℰ_i(m).
ℳℰ_i(m) ← 0, for 0 ≤ i ≤ n − 1, 0 ≤ m ≤ 3
/* The m's values 0, 1, 2, and 3 indicate the entries 0, 1, 1*, and 2* in 𝒰, respectively. */
For each input difference vector a⃗   /* a⃗ represents a⃗^0. */
   for i = 0 to n − 1
      if a_i^0 = 0, then a^{0,i} ← 0 and â^{0,i} ← 0
      if a_i^0 = 1*, then a^{0,i} ← 1 and â^{0,i} ← −1
      for m = 0 to 3
         ℳℰ_i(a⃗, m) ← 0
   r ← 0
   while (there exists some index l such that a^{l,r} ≤ 2.)
      for j = 0 to n − 1
         t_j ← 0, t̂_j ← 0
      /* t_j and t̂_j are the temporary parameters to compute the next difference vector a⃗^{r+1}. */
         for i = 0 to n − 1
            t_j ← t_j + a^{r,i} · e_{i,j}
            s_i ← â^{r,i} + ẽ_{i,j}
            if (s_i = 1)   s_i ← 0
            t̂_j ← t̂_j + s_i
      r ← r + 1
      a^{r,i} ← t_i, â^{r,i} ← t̂_i, for 0 ≤ i ≤ n − 1
      for i = 0 to n − 1
         if (a^{r,i} = 0)   ℳℰ_i(a⃗, 0) ← r
         if (a^{r,i} = 1 and â^{r,i} = 0)   ℳℰ_i(a⃗, 1) ← r
         if (a^{r,i} = 1 and â^{r,i} = −1)   ℳℰ_i(a⃗, 2) ← r
         if (a^{r,i} = 2 and â^{r,i} = −1)   ℳℰ_i(a⃗, 3) ← r
   for i = 0 to n − 1
      for m = 0 to 3
         if (ℳℰ_i(m) ≤ ℳℰ_i(a⃗, m))  ℳℰ_i(m) ← ℳℰ_i(a⃗, m)
Steps 3 and 4: Form the matrix 𝒟 = (𝒟_{i,j})_{n×n}, and compute the values of ℳ𝒟_i(m̄).
Compute the values of ℳ𝒟_i(m) by inserting the matrix 𝒟 into Steps 1 and 2.
for i = 0 to n − 1
   ℳ𝒟_i(0̄) ← max{ℳ𝒟_i(1), ℳ𝒟_i(2)}
   ℳ𝒟_i(1̄) ← ℳ𝒟_i(0)
   ℳ𝒟_i(2̄) ← max{ℳ𝒟_i(0), ℳ𝒟_i(2), ℳ𝒟_i(3)}
   ℳ𝒟_i(3̄) ← ℳ𝒟_i(2)
Step 5: Output the length ℳ. (Equation (4))
Output max_{0≤i≤n−1, 0≤m≤3}(ℳℰ_i(m) + ℳ𝒟_i(m̄))
```

Algorithm 1 to compute the length $\mathcal{M}$

Table 6
Meaning of variables used in Algorithm 1 ($x = 1$ or 2, $y \geq 0$).

Variable	Meaning
$e_{i,j} = 0$	$\mathcal{E}_{i,j} = 0$
$e_{i,j} = 1$	$\mathcal{E}_{i,j} = 1$ or 1_F
$\widetilde{e}_{i,j} = 0$	$\mathcal{E}_{i,j} = 1(x^* \cdot \mathcal{E}_{i,j} = x^*$preserves$*.)$
$\widetilde{e}_{i,j} = 1$	$\mathcal{E}_{i,j} = 0(x^* \cdot \mathcal{E}_{i,j} = 0)or\mathcal{E}_{i,j} = 1_F(x^* \cdot \mathcal{E}_{i,j} = x)$
	(These equations do not preserve $*$.)
$a^{r,i} = y$ (resp., x)	The$i$thentryofdifferencevector$\vec{a}^r$isy(resp.,x^*).
$\hat{a}^{r,i} = 0$	The$i$thentryofdifferencevector$\vec{a}^r$hasnot$*$.
$\hat{a}^{r,i} = -1$	The$i$thentryofdifferencevector$\vec{a}^r$has$*$.

has),[8] and an auxiliary variable $\hat{a}^{r,i}$ is assigned as 0 or -1 by whether or not it has $*$: $\hat{a}^{r,i} = 0$ if the entry has not $*$, and $\hat{a}^{r,i} = -1$ otherwise. See the lower part of Table 6. Note that the two auxiliary variables $\widetilde{e}_{i,j}$ and $\hat{a}^{r,i}$ are used to distinguish between entries with $*$ and entries without $*$.

With this setting, the algorithm first computes the variables $a^{r+1,j}$ by the matrix multiplication $\sum_i a^{r,i} \cdot e_{i,j}$ for each j. As explained in Section 3, $a^{r+1,j}$ larger than 2 are of no use in the matrix method. If $a^{r+1,j} \leq 2$, the remaining thing is to identify $*$ in the corresponding entry of the difference vector. In order to identify $*$ we exploit the forgoing auxiliary variables $\widetilde{e}_{i,j}$

[8] Note that the notation a_i^r represents an entry of difference vector, while the notation $a^{r,i}$ represents an integer.

Table 7
Multiplication between a difference vector entry and a matrix entry in Algorithm 1 (identifying $*$).

Entry c, $(\hat{a}^{r,i})$ of difference vectors	Entry d, $(\widetilde{e}_{i,j})$ of $\mathcal{E}$	$c \cdot d$	$\hat{a}^{r,i} + \widetilde{e}_{i,j} = s_i$ if $(s_i = 1)$ $s_i \leftarrow 0$
$x^*, (-1)$	$0, (1)$	0	0
$x^*, (-1)$	$1_F, (1)$	x	0
$x^*, (-1)$	$1, (0)$	x^*	-1
$x, (0)$	$0, (1)$	0	0
$x, (0)$	$1_F, (1)$	x	0
$x, (0)$	$1, (0)$	x	0

and $\hat{a}^{r,i}$; we consider $\hat{a}^{r,i} + \widetilde{e}_{i,j}$ in our algorithm. We define $s_i = 0$ if $\hat{a}^{r,i} + \widetilde{e}_{i,j} = 1$, and $s_i = \hat{a}^{r,i} + \widetilde{e}_{i,j}$ otherwise. Then, s_i can be -1 or 0. It implies that $s_i = -1$ represents $*$-preserving and $s_i = 0$ represents non $*$-preserving (see Table 7). Recall that $*$-preserving can be occurred only if $\mathcal{E}_{i,j} = 1$ which is laid at most once in each column of property-one matrix. Thus, at most one of s_i can be -1 and the rest of s_i are all 0. It follows that the jth entry of output difference vector for the rth round has $*$ if and only if $s_0 + s_1 + \cdots + s_{n-1} = -1$ and $a^{r+1,j} = 1$ or 2. Using this logic, we identify $*$ in entries of difference vectors, and compute $\mathcal{ME}_i(m)$ and $\mathcal{MD}_i(\bar{m})$. Once we obtain $\mathcal{ME}_i(m)$ and $\mathcal{MD}_i(\bar{m})$, we compute the length $\mathcal{M}$ in the last step by using Eq. (4). Note that in Algorithm 1, we can store the input difference vector in the last *if* statement of step 2 (and of step 4 as well) to obtain specific forms of input and output differences for $\mathcal{M}$-round impossible differentials.

Complexity of Algorithm 1. The running time of Algorithm 1 is dominated by steps 2 and 4, in which the algorithm iterates by the values of input difference vectors $\vec{a}$ and $\vec{b}$. The number of these iterations depends on the number of subblocks of the input difference vectors; more precisely, Algorithm 1 runs 2^n iterations to compute $\mathcal{ME}_i(m)$ and $\mathcal{MD}_i(m)$ each, and thus it is in the $\mathcal{O}(2^n)$ time bound. We expect that for any block cipher structure it is not difficult to carry out the computer experiments for $n \leq 32$.

5. Results for some block cipher structures

In this section, we present specific forms of impossible differentials for some existing generalized block cipher structures. We have experimentally found impossible differentials on them within a small number of subblocks. Based on our simulation results, extended results are given for any number of subblocks. Our extensions are due to the fact that a generalized block cipher structure has a regular structural feature.

5.1. Generalized Feistel structures

Nyberg's GFN_n has property-one matrices $\mathcal{E}$ and $\mathcal{D}$, and thus we can apply Algorithm 1 to the network. As stated above, the running time of Algorithm 1 depends on steps 2 and 4. However, using the fact that the encryption process of GFN_n is similar to the decryption process, $\mathcal{MD}_i(m)$ in step 4 can be easily computed from the values of $\mathcal{ME}_i(m)$. So, we can reduce half of the running time. For finding the length $\mathcal{M}$ for GFN_{16}, we have executed a program written in Visual C 6.0 and running on a set of 10 Windows PCs. From this, we have found the length $\mathcal{M}$ for GFN_{16} in about 4 hours. In our simulations, we have also obtained specific forms of various impossible differentials of GFN_n, where $2 \leq n \leq 16$. The following proposition is a result based on our simulations.

Proposition 1. (1) *If a round function of GFN_2 is bijective, then the length $\mathcal{M}$ for the cipher is* 7.(2) *If a round function of GFN_n is bijective and $n \geq 3$, then the length $\mathcal{M}$ for the cipher is $(3n + 2)$. The generalized forms of the differentials are described in Table 8.*

Furthermore, we have performed a series of simulations on the generalized CAST256-like, MARS-like and RC6-like structures. It is easy to check that all these structures have property-one matrices $\mathcal{E}$ and $\mathcal{D}$.

Proposition 2 ([17]). *If a round function of generalized CAST256-like structure ($n \geq 3$) is bijective, then the length $\mathcal{M}$ for the cipher is $(n^2 - 1)$, and an $\mathcal{M}$-round impossible differential is of the form $(0, \ldots, 0, \alpha_{n-1}) \nrightarrow_{(n^2-1)} (\beta_0, 0, \ldots, 0)$, where $\alpha_{n-1} \neq 0$ and $\beta_0 \neq 0$. This differential is caused by $(0, \ldots, 0, \alpha_{n-1}) \rightarrow_{3n-3} (c, \delta, c, \ldots, c) \nleftrightarrow (c, 0, c, \ldots, c) \leftarrow_{n^2-3n+2} (\beta_0, 0, \ldots, 0)$.*

Proposition 3. *If a round function of generalized MARS-like structure ($n \geq 3$) is bijective, then the length $\mathcal{M}$ for the cipher is $(2n - 1)$, and an $\mathcal{M}$-round impossible differential is of the form $(0, \ldots, 0, \alpha_{n-1}) \nrightarrow_{(2n-1)} (\beta_0, 0, \ldots, 0)$, where $\alpha_{n-1} \neq 0$ and $\beta_0 \neq 0$. This differential is caused by $(0, \ldots, 0, \alpha_{n-1}) \rightarrow_{n+1} (c, \ldots, c, \delta) \nleftrightarrow (c, \ldots, c, 0) \leftarrow_{n-2} (\beta_0, 0, \ldots, 0)$.*

Proposition 4. *If a round function of generalized RC6-like structure is bijective, then the length $\mathcal{M}$ for the cipher is $(4n + 1)$, and $\mathcal{M}$-round impossible differentials are of the forms $(0, \ldots, 0, \alpha_i, 0, \ldots, 0) \nrightarrow_{(4n+1)} (0, \ldots, 0, \beta_{i+1}, 0, \ldots, 0)$, where $\alpha_i = \beta_{i+1} \neq 0$ and i is an odd number. This differential is caused by $(0, \ldots, 0, \alpha_i, 0, \ldots, 0) \rightarrow_{2n+2} (c, \ldots, c, \alpha_i \oplus \delta, c, \ldots, c) \nleftrightarrow (c, \ldots, c, \beta_{i+1}, c, \ldots, c) \leftarrow_{n-2} (0, \ldots, 0, \beta_{i+1}, 0, \ldots, 0)$, where the positions of $\alpha_i \oplus \delta$ and β_{i+1} in the contradicted differences are the same.*

Table 8
Impossible differentials for GFN_n.

	GFN_2
Im.D. 1	$(0,0,0,\alpha_3) \nrightarrow_7 (\beta_0',0,\beta_2',0)$
Reason	$(0,0,0,\alpha_3) \rightarrow_6 (c,c,c,\delta) \not\Leftrightarrow (c,c,c,0) \leftarrow_1 (\beta_0',0,\beta_2',0)$
Im.D. 2	$(0,0,\alpha_2,0) \nrightarrow_7 (\beta_0',0,\beta_2',0)$
Reason	$(0,0,\alpha_2,0) \rightarrow_4 (c,\delta,c,c) \not\Leftrightarrow (c,0,c,c) \leftarrow_3 (\beta_0',0,\beta_2',0)$
Im.D. 3	$(0,0,\alpha_2,\alpha_3) \nrightarrow_7 (\beta_0,0,0,0)$
Reason	$(0,0,\alpha_2,\alpha_3) \rightarrow_3 (c,0,c,c) \not\Leftrightarrow (c,\delta,c,c) \leftarrow_4 (\beta_0,0,0,0)$
Im.D. 4	$(0,0,\alpha_2,\alpha_3) \nrightarrow_7 (0,0,\beta_2,0)$
Reason	$(0,0,\alpha_2,\alpha_3) \rightarrow_3 (c,0,c,c) \not\Leftrightarrow (c,\delta,c,c) \leftarrow_4 (0,0,\beta_2,0)$
Im.D. 5	$(0,\alpha_1,\alpha_2,0) \nrightarrow_7 (\beta_0'',0,0,0)$
Reason	$(0,\alpha_1,\alpha_2,0) \rightarrow_2 (c,\alpha_2,c,c) \not\Leftrightarrow (c,\beta_0''\oplus\delta,c,c) \leftarrow_5 (\beta_0'',0,0,0)$
Im.D. 6	$(0,\alpha_1,\alpha_2,\alpha_3) \nrightarrow_7 (\beta_0'',0,0,0)$
Reason	$(0,\alpha_1,\alpha_2,\alpha_3) \rightarrow_2 (c,\alpha_2,c,c) \not\Leftrightarrow (c,\beta_0''\oplus\delta,c,c) \leftarrow_5 (\beta_0'',0,0,0)$
	GFN_n $(n \geq 3)$
Im.D. 1	$(0,0,0,\ldots,0,\alpha_{2n-1}) \nrightarrow_{3n+2} (\beta_0',0,\beta_2',0,\ldots,0)$
Reason	$(0,0,0,\ldots,0,\alpha_{2n-1}) \rightarrow_{2n} (c,\ldots,c,\delta,c,c,c) \not\Leftrightarrow$ $(c,\ldots,c,0,c,c,c) \leftarrow_{n+2} (\beta_0',0,\beta_2',0,\ldots,0)$
Im.D. 2	$(0,0,\ldots,0,\alpha_{2n-2},0) \nrightarrow_{3n+2} (\beta_0,0,0,\ldots,0,0)$
Reason	$(0,0,\ldots,0,\alpha_{2n-2},0) \rightarrow_{2n-1} (c,\ldots,c,0,c,c) \not\Leftrightarrow$ $(c,\ldots,c,\delta,c,c) \leftarrow_{n+3} (\beta_0,0,\ldots,0)$
Im.D. 3	$(0,\ldots,0,\alpha_{2n-2},\alpha_{2n-1}) \nrightarrow_{3n+2} (\beta_0,0,0,0,\ldots 0)$
Reason	$(0,\ldots,0,\alpha_{2n-2},\alpha_{2n-1}) \rightarrow_{2n-1} (c,\ldots,c,0,c,c) \not\Leftrightarrow$ $(c,\ldots,c,\delta,c,c) \leftarrow_{n+3} (\beta_0,0,\ldots,0)$

– Im.D.: Impossible differential, $\alpha_i \neq 0$, $\beta_i \neq 0$, $(\beta_0',\beta_2') \neq (0,0)$, $\beta_0'' = \alpha_2$.
– $A \rightarrow_r B$: r-round probability-one differential $(A \rightarrow B)$ for encryption process.
– $B \leftarrow_r A$: r-round probability-one differential $(A \rightarrow B)$ for decryption process.
– c: unconcerned difference, $A \not\Leftrightarrow B$: contradiction between differences A and B.

5.2. *Rijndael structures*

For one round of Rijndael, each of output subblocks is affected by four input subblocks due to its linear layer composed of the SR and MC transformations; more precisely, each output subblock is linearly[9] affectedby four subblocks after the SB transformation. Thus, the Rijndael structures have property-one matrices $\mathcal{E}$ and $\mathcal{D}$ whose columns have all zeroes but four $1_F'$s each. It follows that Algorithm 1 can be applied to the Rijndael structures. Following is our simulation result.

Proposition 5. (1) *(*Rijndael$_{128}$ *structure* [4]*) Given two plaintexts which are equal at all bytes but one, the ciphertexts after* 3 *rounds cannot be equal in any column. This* 3*-round impossible differential is caused by the fact that given two plaintexts which are equal at all bytes but one, the number of active bytes*[10] *after* 2 *rounds (forward direction) is* 16*, while given two ciphertexts which are equal in any column, the number of active bytes after 1 round (backward direction) is at most* 12. (2) *(*Rijndael$_{192}$ *structure) Given two plaintexts which are equal at all bytes but one, the ciphertexts after* 4 *rounds cannot be equal in any three columns. This* 4*-round impossible differential is caused by the fact that given two plaintexts which are equal at all bytes but one, the number of active bytes after* 3 *rounds (forward direction) is at least* 14*, while given two ciphertexts which are equal in any three columns, the number of active bytes after* 1 *round (backward direction) is at most* 12. (3) *(*Rijndael$_{256}$ *structure) Given two plaintexts which are equal at all bytes but one, the ciphertexts after* 5 *rounds cannot be equal in any seven columns. This* 5*-round impossible differential is caused by the fact that given two plaintexts which are equal at all bytes but one, the number of active bytes after* 3 *rounds (forward direction) is at least* 24*, while given two ciphertexts which are equal in any seven columns, the number of active bytes after* 2 *rounds (backward direction) is at most* 16.

Note. The impossible differentials presented in Proposition 5 are not the longest ones for the Rijndael structures. Indeed, there exist 4-round impossible differentials for Rijndael$_{128}$ [4], 5-round impossible differentials for Rijndael$_{192}$ and 6-round impossible differentials for Rijndael$_{256}$. They are each formed by one-round extensions at the ends of the impossible differentials in Proposition 5. One-round extensions are done by giving linear restrictions on the ciphertext differences. However, these extended forms of impossible differentials are not identified by our general matrix method, as they are rather from the inherent characteristics for the linear transformations of Rijndael.

9 As mentioned before, even though the connection operation is not $\oplus$, the matrix method can be applied.
10 Active bytes represent bytes with nonzero differences.

Table 9
Impossible differentials for generalized Skipjack-like structures.

	Skipjack-(nA_n, nB_n)
Im.D. Reason	$(0, \alpha_1, 0, \ldots, 0) \nrightarrow_{5n-1} (\beta_0, \beta_1, 0, \ldots, 0)$ $(0, \alpha_1, 0, \ldots, 0) \rightarrow_{3n-1} (c, \ldots, c, \delta) \not\Leftrightarrow$ $(c, \ldots, c, 0) \leftarrow_{2n} (\beta_0, \beta_1, 0, \ldots, 0)$
	Skipjack-$(nA_n, nB_n)_{-j}$
Im.D. Reason	$(0, \ldots, 0, \alpha_{j+1}, 0, \ldots, 0) \nrightarrow_{5n-1-j} (\beta_0, \beta_1, 0, \ldots, 0)$ $(0, \ldots, 0, \alpha_{j+1}, 0, \ldots, 0) \rightarrow_{3n-1-j} (c, \ldots, c, \delta) \not\Leftrightarrow$ $(c, \ldots, c, 0) \leftarrow_{2n} (\beta_0, \beta_1, 0, \ldots, 0)$
	Skipjack-$(2nA_n, 2nB_n)$
Im.D. Reason	$(0, \alpha_1, 0, \ldots, 0) \nrightarrow_{4n-3} (\beta_0, 0, \ldots, 0)$ $(0, \alpha_1, 0, \ldots, 0) \rightarrow_{3n-1} (c, \delta, c, \ldots, c) \not\Leftrightarrow$ $(c, 0, c, \ldots, c) \leftarrow_{n-2} (\beta_0, 0, \ldots, 0)$
	Skipjack-$(2nA_n, 2nB_n)_{-n}$
Im.D. Reason	$(0, \alpha_1, 0, \ldots, 0) \nrightarrow_{6n} (\beta_0, 0, \ldots, 0)$ $(0, \alpha_1, 0, \ldots, 0) \rightarrow_{5n-4} (c, \ldots, c, \delta) \not\Leftrightarrow$ $(c, \ldots, c, 0) \leftarrow_{n+4} (\beta_0, 0, \ldots, 0)$
	Skipjack-$(3nA_n, 3nB_n)$, $(n \geq 4)$
Im.D. Reason	$(0, \alpha_1, 0, \ldots, 0) \nrightarrow_{5n-4} (\beta_0, 0, \ldots, 0)$ $(0, \alpha_1, 0, \ldots, 0) \rightarrow_{3n-3} (c, \ldots, c, \delta) \not\Leftrightarrow$ $(c, \ldots, c, 0) \leftarrow_{2n-1} (\beta_0, 0, \ldots, 0)$
	Skipjack-$(3nA_n, 3nB_n)_{-j}$, $(n \geq 4)$
Im.D. Reason	$(0, \ldots, 0, \alpha_{j+1}, 0, \ldots, 0) \nrightarrow_{5n-4-j} (\beta_0, 0, \ldots, 0)$ $(0, \ldots, 0, \alpha_{j+1}, 0, \ldots, 0) \rightarrow_{3n-3-j} (c, \ldots, c, \delta) \not\Leftrightarrow$ $(c, \ldots, c, 0) \leftarrow_{2n-1} (\beta_0, 0, \ldots, 0)$

$(\alpha_i \neq 0, \beta_i \neq 0, \beta_0 = \beta_1$, and $0 \leq j \leq n-2.)$

5.3. Generalized Skipjack-like structures

Sung et al. [17] conjectured that the maximum length of impossible differentials for Skipjack-(A_n) is $(n^2 - 1)$ rounds. However, we have experimentally found an n^2-round impossible differential. The length of this differential cannot be found by Algorithm 1, since the number of entry 1 for the last column of $\mathcal{D}$ is two, i.e., $\mathcal{D}$ is not property-one matrix. However, in each column except for the last column of $\mathcal{D}$, the number of entry 1 is zero or one. By modifying Algorithm 1 to Algorithm 2 below,[11] we can find the length of this impossible differential for Skipjack-(A_n). Using a structural duality between Rule A_n and Rule B_n, we can find an n^2-round impossible differential for Skipjack-(B_n). The following proposition is a result based on our simulations.

Proposition 6. *If a round function of Skipjack-(A_n) (resp., Skipjack-(B_n)) is bijective, then the length $\mathcal{M}$ is n^2, and an $\mathcal{M}$-round impossible differential is of the form $(0, \alpha_1, 0, \ldots, 0) \nrightarrow_{n^2} (\beta_0, \beta_1, 0, \ldots, 0)$, where $\alpha_1 \neq 0$ and $\beta_0 = \beta_1 \neq 0$ (resp., $(\alpha_0, \alpha_1, 0, \ldots, 0) \nrightarrow_{n^2} (0, \beta_1, 0, \ldots, 0)$, where $\alpha_0 = \alpha_1 \neq 0$ and $\beta_1 \neq 0$); this differential is due to $(0, \alpha_1, 0, \ldots, 0) \rightarrow_{3n-3} (c, \ldots, c, \delta) \not\Leftrightarrow (c, \ldots, c, 0) \leftarrow_{n^2-3n+3} (\beta_0, \beta_1, 0, \ldots, 0)$ (resp., $(\alpha_0, \alpha_1, 0, \ldots, 0) \rightarrow_{n^2-3n+3} (c, \ldots, c, 0) \not\Leftrightarrow (c, \ldots, c, \delta) \leftarrow_{3n-3} (0, \beta_1, 0, \ldots, 0)$).*

We have also experimentally found various impossible differentials for other generalizations of Skipjack, denoted Skipjack-(nA_n, nB_n), Skipjack-$(2nA_n, 2nB_n)$ and Skipjack-$(3nA_n, 3nB_n)$. Even though these structures do not have property-one matrices (note that these structures have two matrices for encryption and decryption each — one matrix is for Rule A_n and the other matrix is for Rule B_n), we can use the matrix method to find various impossible differentials on them as in the extension from Algorithm 1 to Algorithm 2. Table 9 shows impossible differentials on Skipjack-(nA_n, nB_n), $(2nA_n, 2nB_n)$ and $(3nA_n, 3nB_n)$ as well as on their modified structures, which have been found by our simulations. In Table 9, the Skipjack-$(tA_n, tB_n)_{-l}$ structures are the same as Skipjack-(tA_n, tB_n) except that they employ $(t-l)A_n$ instead of the first tA_n.

According to our results, Skipjack-(A_n) and (B_n) are more vulnerable to impossible differential cryptanalysis than the structures which employ both of Rule A_n and Rule B_n. Among the latter three structures using both of Rule A_n and Rule B_n, the Skipjack-$(2nA_n, 2nB_n)$ structure has the best resistance to impossible differential cryptanalysis. Note that the 24-round impossible differential $(0, \alpha_1, 0, 0) \nrightarrow_{24} (\beta_0, 0, 0, 0)$ of Skipjack-$(8A_4, 8B_4)_{-4}$ was already presented in [3] (the 24-round impossible differential used in [3] starts from the fifth round).

[11] We have added 4 lines more to Algorithm 1: the added lines sort out the problem when the entry 1^* is XORed with the same entry 1^*; our solution is $1^* + 1^* = 0$ for obtaining stronger impossible differentials, and this kind of event cannot occur except for the first decryption round.

Steps 1 and 2 in the algorithm of Section 4: Compute $\mathcal{ME}_i(m)$.

Steps 3 and 4: Compute the values of $\mathcal{MD}_i(\bar{m})$.
For each input difference vector $\vec{b}$
  if $(b_i^0 = 0)\ \hat{b}_i^0 \leftarrow 0$, for $0 \le i \le n-1$
  else if $(b_i^0 = 1)\ \hat{b}_i^0 \leftarrow -1$, for $0 \le i \le n-1$
  $\mathcal{MD}_i(\vec{b}, m) \leftarrow 0$, for $0 \le i \le n-1, 0 \le m \le 3$
  $r \leftarrow 0$
  if $(b_0^0 = 1$ and $b_1^0 = 1)$
    $b_0^1 \leftarrow 1, \hat{b}_0^1 \leftarrow 0, b_{n-1}^1 \leftarrow 0, \hat{b}_{n-1}^1 \leftarrow 0$
    $b_i^1 \leftarrow b_{i+1}^1, \hat{b}_i^1 \leftarrow \hat{b}_{i+1}^1$, for $1 \le i \le n-2$
    $r \leftarrow 1$
  while (): same as in Algorithm 1 of Section 4.
Compute $\mathcal{MD}_i(m)$ and $\mathcal{MD}_i(\bar{m})$.

Step 5 in the algorithm of Section 4:
Output $max_{0 \le i \le n-1, 0 \le m \le 3}(\mathcal{ME}_i(m) + \mathcal{MD}_i(\bar{m}))$

Algorithm 2 to compute the length $\mathcal{M}$ for Skipjack $-$ (A_n)

6. Discussions

An interesting property of the matrix method is that it can be converted to a tool for the SQUARE attack [7]. Consider a block cipher structure whose round functions are bijective. If a saturated input subblock is considered as the entry 1^* and a constant input subblock is considered as the entry 0, then the output states after r rounds are represented by the entries defined in Section 3: the entry 0 corresponds to a constant value, and the entries 1 and 1^* correspond to a saturated set, and the entries 2 and 2^* correspond to a balanced set. Based on this fact, we have performed simulations for the block cipher structures which were dealt with in this article, and found that the maximum length of square distinguishers is shorter than that of impossible differentials on each cipher (for example, GFN_n $(n \ge 3)$ has a $(2n+3)$-round square distinguisher, while it has $(3n+2)$-round impossible differentials). We expect that the possibility of applying the matrix method to other attacks may be of interest.

7. Conclusions

In this article, we have devised a general impossible differential cryptanalysis tool using matrices, which is widely applicable to find impossible differentials for block cipher structures. Using the matrix method, we have presented various impossible differentials on some existing block cipher structures such as Nyberg's generalized Feistel network, generalized CAST256-like, MARS-like, RC6-like structures, Rijndael structures and generalized Skipjack-like structures: according to our simulation results, the generalized MARS-like structure has the best resistance to the matrix method, due to its high diffusion effect.

We believe that the matrix method developed in this article is not only useful for evaluating the security of block ciphers against impossible differential cryptanalysis, but that it can also play an important role in inventing general tools for other attacks.

References

[1] K. Aoki, K. Ohta, Strict evaluation of the maximum average of differential probability and the maximum average of linear probability, Proc. of IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, No. 1, 1997, pp. 2–8.
[2] E. Biham, A. Biryukov, A. Shamir, Miss in the middle attacks on IDEA, Khufu and Khafre, in: Proc. of FSE'99, in: LNCS, vol. 1636, Springer-Verlag, 1999, pp. 124–138.
[3] E. Biham, A. Biryukov, A. Shamir, Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials, in: Advances in Cryptology – Proc. of EUROCRYPT'99, in: LNCS, vol. 1592, Springer-Verlag, 1999, pp. 12–23.
[4] E. Biham, N. Keller, Cryptanalysis of Reduced Variants of Rijndael. http://csrc.nist.gov./encryption/aes/round2/conf3/aes3papers.html.
[5] E. Biham, A. Shamir, Differential cryptanalysis of DES like cryptosystems, in: Advances in Cryptology – Proc. of CRYPTO'90, in: LNCS, vol. 537, Springer-Verlag, 1991, pp. 2–21.
[6] J. Daemen, V. Rijnmen, The Design of Rijndael: AES – The Advanced Encryption Standard, Springer-Verlag, 2002.
[7] J. Daemen, L.R. Knudsen, V. Rijmen, The block cipher square, in: Proc. of FSE'97, in: LNCS, Springer-Verlag, 1997, pp. 149–165.
[8] S. Hong, S. Lee, J. Lim, J. Sung, D. Choen, I. Cho, Provable security against differential and linear cryptanalysis for the SPN structure, in: Proc. of FSE'00, in: LNCS, vol. 1978, Springer-Verlag, 2000, pp. 273–283.
[9] L.R. Knudsen, DEAL — A 128-bit block cipher, AES Proposal, 1998.
[10] J. Lu, O. Dunkelman, N. Keller, J. Kim, New impossible differential attacks on AES, in: Proc. of Indocrypt'06, in: LNCS, vol. 5365, Springer-Verlag, 2008, pp. 279–293.

[11] M. Matsui, Linear cryptanalysis method for DES cipher, in: Advances in Cryptology – Proc. of EUROCRYPT'93, in: LNCS, vol. 765, Springer-Verlag, 1994, pp. 386–397.
[12] M. Matsui, New structure of block ciphers with provable security against differential and linear cryptanalysis, in: Proc. of FSE'96, in: LNCS, vol. 1039, Springer-Verlag, 1996, pp. 205–218.
[13] S. Moriai, S. Vaudenay, On the pseudorandomness of top-level schemes of block ciphers, in: Advances in Cryptology – Proc. of ASIACRYPT'00, in: LNCS, vol. 1976, Springer-Verlag, 2000, pp. 289–302.
[14] National Security Agency, Skipjack and KEA Algorithm Specifications, Version 2.0, 29 May 1998. http://csrc.ncsl.nist.gov/encryption/skipjack-1.pdf.
[15] K. Nyberg, L.R. Knudsen, Provable security against differential cryptanalysis, in: Advances in Cryptology – Proc. of CRYPTO'92, in: LNCS, vol. 740, Springer-Verlag, 1992, pp. 566–574.
[16] K. Nyberg, Generalized Feistel networks, in: Advances in Cryptology – Proc. of ASIACRYPT'96, in: LNCS, vol. 1163, Springer-Verlag, 1996, pp. 91–104.
[17] J. Sung, S. Lee, J. Lim, S. Hong, S. Park, Provable security for the Skipjack-like structure against differential cryptanalysis and linear cryptanalysis, in: Advances in Cryptology – Proc. of ASIACRYPT'00, in: LNCS, vol. 1976, Springer-Verlag, 2000, pp. 274–288.
[18] S. Vaudenay, Provable security for block ciphers by decorrelation, in: Proc. of STACS'98, in: LNCS, vol. 1373, Springer-Verlag, 1998, pp. 249–275.
[19] S. Vaudenay, Decorrelation: A theory for block cipher security, Journal of Cryptology 16 (4) (2003) 249–286.