Impossible Differential Cryptanalysis for Block Cipher Structures

Jongsung Kim[1], Seokhie Hong[1], Jaechul Sung[2], Sangjin Lee[1], Jongin Lim[1], and Soohak Sung[3]

[1] Center for Information Security Technologies(CIST),
Korea University, Seoul, Korea
{joshep,hsh,sangjin,jilim}@cist.korea.ac.kr
[2] Korea Information Security Agency(KISA), Seoul, KOREA,
sjames@kisa.or.kr
[3] Beajea University, Deajoan, KOREA,
sungsh@mail.paichai.ac.kr

Abstract. Impossible Differential Cryptanalysis(IDC) [4] uses impossible differential characteristics to retrieve a subkey material for the first or the last several rounds of block ciphers. Thus, the security of a block cipher against IDC can be evaluated by impossible differential characteristics. In this paper, we study impossible differential characteristics of block cipher structures whose round functions are bijective. We introduce a widely applicable method to find various impossible differential characteristics of block cipher structures. Using this method, we find various impossible differential characteristics of known block cipher structures: Nyberg's generalized Feistel network, a generalized CAST256-like structure [14], a generalized MARS-like structure [14], a generalized RC6-like structure [14], and Rijndael structure.

Keyword : Impossible Differential Cryptanalysis(IDC), impossible differential characteristic, block cipher structures

1 Introduction

The most powerful known attacks on block ciphers are differential cryptanalysis(DC) [3] and linear cryptanalysis(LC) [12]. These attacks have been applied to many known ciphers very efficiently. So, one has tried to make a block cipher secure against DC and LC. Nyberg and Knudsen first proposed the conception of a provable security against DC and gave a provable security for a Feistel structure in 1992 [16]. Since then, many block cipher structures with a provable security against DC and LC have been studied [8,9,13,16,17,19]. However, a provable security against DC and LC is not enough to give the security of block ciphers, because other cryptanalyses may be applied to them not vulnerable to DC and LC. For instance, the 3-round Feistel structure whose round functions are bijective has a provable security against DC and LC [2], but there exists a 5-round

T. Johansson and S. Maitra (Eds.): INDOCRYPT 2003, LNCS 2904, pp. 82–96, 2003.

impossible differential characteristic [10]. This fact is also applied to some other structures. In this paper, we focus on IDC for block cipher structures whose round functions are bijective. We provide a general tool, called $\mathcal{U}$-method, which can find various impossible differential characteristics of block cipher structures with a certain property. We also provide an algorithm to compute the maximum length of impossible differential characteristics that can be found in the $\mathcal{U}$-method. (By modifying the algorithm, we can find the specific forms of impossible differential characteristics.) We use it to find various impossible differential characteristics of known block cipher structures. See Table 1 for a summary of our results. Furthermore, we use impossible differential characteristics of Rijndael which can be found in our algorithm to improve the previous result [6].

This paper is organized as follows. In Section 2, we describe a generalized Feistel network and Rijndael structure. In Section 3, we introduce some basic notions for IDC and the $\mathcal{U}$-method. In Section 4, we propose an algorithm to compute the maximum length of impossible differential characteristics which can be found in the $\mathcal{U}$-method. In Section 5, we find various impossible differential characteristics of known block cipher structures. In Section 6, we discuss how to apply the $\mathcal{U}$-method to an integral attack.

Table 1. Summary of our cryptanalytic results. (A: The number(r) of rounds to have the property that the maximum average of differential probability is bounded by p^{2n} where p is the maximum average of differential probability of a round function. B: The number(r) of rounds for impossible differential characteristics. See Section 2 for the details of GFN_n, Rijndael$_{128}$, Rijndael$_{192}$, and Rijndael$_{256}$ and refer to [14] for the details of a generalized CAST256-like structure, a generalized MARS-like structure, and a generalized RC6-like structure.)

Block Cipher Structure	DC (A)	comment
GFN_n	$r \geq 3n$	conjecture([17])

Block Cipher Structure	IDC (B)	comment
GFN_2	$r = 7$	This paper
GFN_n	$r = 3n + 2$ ($n \geq 3$)	This paper
Rijndael$_{128}$	$r = 3$	[6]
Rijndael$_{192}$	$r = 4$	This paper
Rijndael$_{256}$	$r = 5$	This paper
Generalized CAST256	$r = n^2 - 1$ ($n \geq 3$)	[19]
Generalized MARS	$r = 2n - 1$ ($n \geq 3$)	This paper
Generalized RC6	$r = 4n + 1$	This paper

2 Descriptions of Block Cipher Structrues

2.1 A Generalized Feistel Network

A generalized Feistel network was introduced by Nyberg [17]. Let $(X_0, X_1, \cdots, X_{2n-1})$ be the input to one round of the network. Given n round functions

$F_0, F_1, \cdots, F_{n-1}$ and n round keys $K_0, K_1, \cdots, K_{n-1}$, the output of the round $(Y_0, Y_1, \cdots, Y_{2n-1})$ is computed by the following formulas.

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

We call X_i and Y_j as the i^{th} subblock of input and the j^{th} subblock of output, respectively. 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 in Figure 1.

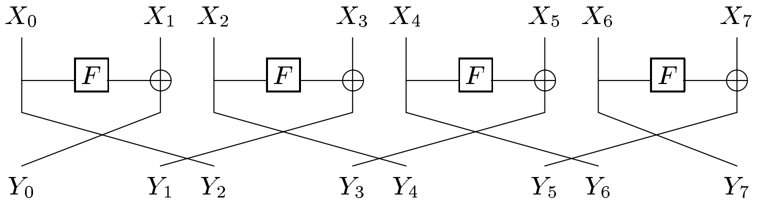
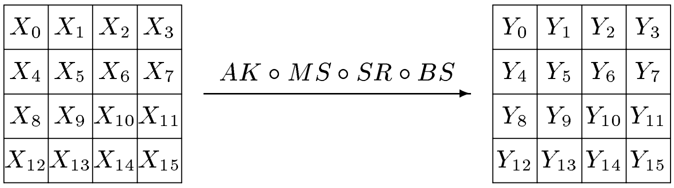


Fig. 1. A round of GFN_4

2.2 Rijndael Structure

Rijndael is a block cipher composed of SPN structure. The length of the data block can be specified to be 128, 192, or 256 bits. They are expressed as arrays of 4 × 4 bytes, 4 × 6 bytes, and 4 × 8 bytes, respectively. A round of Rijndael consists of 4 transformations, i.e., ByteSubstitution(BS), ShiftRow(SR), MixColmn(MC), and AddroundKey(AK). A round of Rijndael with 128-bit data block is depicted in Figure 2. Here, $(f \circ g)(x)$ represents $f(g(x))$.



X_0	X_1	X_2	X_3
X_4	X_5	X_6	X_7
X_8	X_9	X_{10}	X_{11}
X_{12}	X_{13}	X_{14}	X_{15}

$\xrightarrow{AK \circ MS \circ SR \circ BS}$

Y_0	Y_1	Y_2	Y_3
Y_4	Y_5	Y_6	Y_7
Y_8	Y_9	Y_{10}	Y_{11}
Y_{12}	Y_{13}	Y_{14}	Y_{15}

Fig. 2. A round of Rijndael with a 128-bit data block

In this paper 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, e.g., each round includes 16 F functions. We call these structures Rijndael$_{128}$ structure, Rijndael$_{192}$ structure, and Rijndael$_{256}$ structure, respectively.

3 New Basic Notions for IDC

In this section, we will introduce some notions, which are a bit intricate but very available. We assume that a block cipher structure $\mathcal{S}$ has n data subblocks, e.g., the input and the output of one round are $(X_0, X_1, \cdots, X_{n-1})$ and $(Y_0, Y_1, \cdots, Y_{n-1})$, respectively. Throughout the paper, we consider $\mathcal{S}$ whose round function F is bijective, and operation to connect a subblock with another one is $\oplus$.

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. If Y_j is affected by X_i, the (i, j) entry of $\mathcal{E}$ is set to 1, and if not, the (i, j) entry is set to 0. Especially, if Y_j is affected by $F(X_i)$, the (i, j) entry of $\mathcal{E}$ is set to 1_F instead of 1. Reversely, if X_j is affected by Y_i, the (i, j) entry of $\mathcal{D}$ is set to 1, and if not, the (i, j) entry is set to 0. Especially, 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 the number of entry $1 (\neq 1_F)$ in each column of the matrix is zero or one, we call it* **1-property matrix***.*

For example, $\mathcal{E}$ and $\mathcal{D}$ of the Feistel structure depicted in Figure 3 are as follows. (According to Definition 1, the Feistel structure has 1-property matrices $\mathcal{E}$ and $\mathcal{D}$.)

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

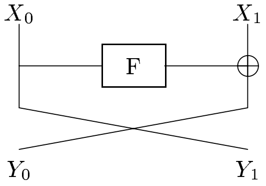


Fig. 3. A round of a Feistel structure

If $\mathcal{S}$ has 1-property matrices $\mathcal{E}$ and $\mathcal{D}$, we can easily find various impossible differential characteristics of $\mathcal{S}$ in our method. In this section, we assume that $\mathcal{S}$ has 1-property matrices $\mathcal{E}$ and $\mathcal{D}$.

Definition 2. *Given an input difference* $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$*, the input difference vector* $\boldsymbol{a} = (a_0, a_1, \cdots, a_{n-1})$ *corresponding to* α *is defined as follows.*

$$a_i = \begin{cases} 0 & \textit{if } \alpha_i = 0 \\ 1^* & \textit{otherwise} \end{cases}$$

We denote the output difference after r rounds for α by α^r, and denote the value of the i^{th} subblock of α^r by α^r_i. Naturally, the difference vector which corresponds to α^r is denoted $\boldsymbol{a}^r$ (The meaning of the values of $\boldsymbol{a}^r$ will be explained below.), and the i^{th} entry of $\boldsymbol{a}^r$ which corresponds to α^r_i is denoted a^r_i. If the same work is performed to decryption process, we use the notations β, β^r, β^r_i, $\boldsymbol{b}$, $\boldsymbol{b}^r$, and b^r_i instead of α, α^r, α^r_i, $\boldsymbol{a}$, $\boldsymbol{a}^r$, and a^r_i, respectively.

Given an input difference, the possible output differences of each subblock after r rounds can be classified by five types of differences: zero difference, a nonzero nonfixed difference, a nonzero fixed difference, exclusive-or of a nonzero fixed difference and a nonzero nonfixed difference, and a nonfixed difference. As the extended one of the notations used in Definition 2, the five types of differences stated above are denoted by the entries of difference vectors in Table 2.

Table 2. Entries of difference vectors and corresponding differences.

Entry (a^r_i or b^r_i)	Corresponding difference (α^r_i or β^r_i)
0	zero difference (denoted 0)
1	nonzero nonfixed difference (denoted δ)
1^*	nonzero fixed difference (denoted γ)
2^*	nonzero fixed difference $\oplus$ nonzero nonfixed difference ($\gamma \oplus \delta$)
$t(\geq 2)$	nonfixed difference (denoted ?)

Throughout this paper, we will use the notations 0, δ, γ, and ? as the differences stated in Table 2 (sometimes δ' (resp., γ') is used as the same kind of a difference δ (resp., γ)). According to Table 2, in the case of the entry t, we cannot predict the corresponding difference, in other words, we cannot know the difference to which the entry t does not correspond. On the other hand, in the cases of the entries $0, 1, 1^*$, and 2^*, we can predict the difference to which each entry does not correspond. For example, 2^* cannot correspond to γ, since $\gamma \oplus \delta \neq \gamma$. These facts are of use to find impossible differential characteristics of $\mathcal{S}$. In our method, we concentrate on difference vectors rather than the specific forms of differences.

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

$$\boldsymbol{a}^r = ((((\boldsymbol{a} \cdot \overbrace{\mathcal{E}) \cdot \mathcal{E}) \cdots) \cdot \mathcal{E})}^{r \text{ times}} = ((((\boldsymbol{a}^1 \cdot \overbrace{\mathcal{E}) \cdot \mathcal{E}) \cdots) \cdot \mathcal{E})}^{r-1 \text{ times}} = \cdots = \boldsymbol{a}^{r-1} \cdot \mathcal{E} \qquad (1)$$

Without loss of generality, we define a multiplication of $\boldsymbol{a}$ and $\mathcal{E}$ (e.g, $\boldsymbol{a} \cdot \mathcal{E}{=}(a_i)_{1\times n} \cdot (\mathcal{E}_{i,j})_{n\times n} = (\sum_i a_i \cdot \mathcal{E}_{i,j})_{1\times n}$)

First, we consider a multiplication between an entry of difference vector a_i and an entry of matrix $\mathcal{E}_{i,j}$. The multiplication $a_i \cdot \mathcal{E}_{i,j}$ represents the relation between the input difference of the i^{th} subblock and the output difference of the j^{th} subblock. Table 3 illustrates the meaning of the multiplication.

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

$a_i \cdot \mathcal{E}_{i,j}$	Meaning
$k \cdot 0 = 0$	The output difference of the j^{th} subblock is not affected by the input difference of the i^{th} subblock.
$k \cdot 1 = k$	The output difference of the j^{th} subblock is affected by the input difference of the i^{th} subblock.
$k \cdot 1_F$	The output difference of the j^{th} subblock is affected by the difference after F for the input difference of the i^{th} subblock.
$0 \cdot 1_F = 0$	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 ?.

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

1. The addition of two entries which have not $*$ is defined over the integer.
2. If one entry, denoted e, has not $*$ and the other has $*$, then the addition of these two entries is defined as follows.
   - If the entry e is 0 or 1, then $e + 1^* = (e+1)^*$, otherwise, $e + 1^* = e + 1$.
   - If the entry e is 0, $e + 2^* = (e+2)^*$, otherwise, $e + 2^* = e + 2$.

According to Table 3, $*$ is preserved (e.g, $x^* \cdot 1 = x^*$ where x^* represents the entry 1^* or 2^*.) only if $\mathcal{E}_{i,j} = 1$. And $\mathcal{E}$ is 1-property matrix by our assumption. Thus, there does not exist the addition of two entries which have $*$. Table 4 illustrates the relation between the addition of entries and exclusive-or of corresponding differences. We can easily verify that these operations, $\cdot$ and $+$, are well defined.

To help understand new operations, we consider the Feistel structure. If the input difference vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ are $(0, 1^*)$ and $(1^*, 0)$, respectively, then $\boldsymbol{a}^r$ and $\boldsymbol{b}^r$ are computed by the Equations (2) and (3), respectively. Figure 4 describes these equations.

Table 4. Relation of addition and exclusive-or ($k \in \{0, 1, 1^*, 2^*, t\}$, $t' \geq 2$, and Δ is the corresponding difference for k.)

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

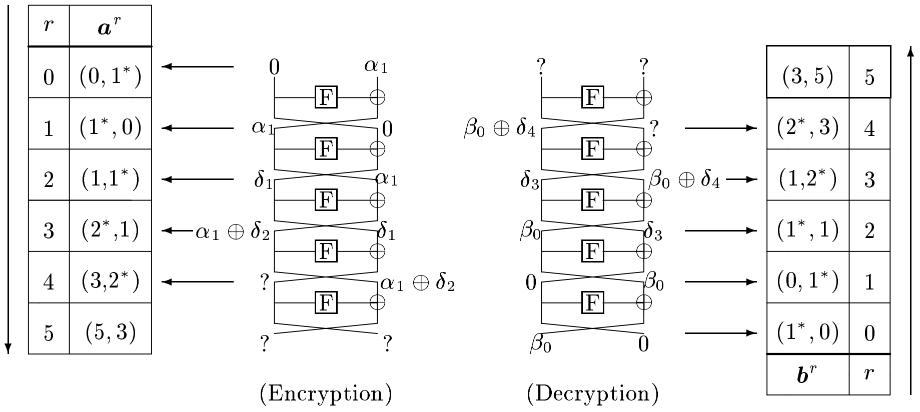
$$\begin{aligned}
\boldsymbol{a}^1 &= \boldsymbol{a} \cdot \mathcal{E} = (0 \cdot 1_F + 1^* \cdot 1,\ 0 \cdot 1 + 1^* \cdot 0) = (0 + 1^*, 0 + 0) = (1^*, 0) \\
\boldsymbol{a}^2 &= \boldsymbol{a}^1 \cdot \mathcal{E} = (1^* \cdot 1_F + 0 \cdot 1,\ 1^* \cdot 1 + 0 \cdot 0) = (1 + 0, 1^* + 0) = (1, 1^*)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

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

Now, we show how to use the entries of difference vectors for finding impossible differential characteristics of $\mathcal{S}$. We denote a r-round impossible differential characteristic with an input difference $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$ and an output difference $\beta = (\beta_0, \beta_1, \cdots, \beta_{n-1})$ by $\alpha \nrightarrow_r \beta$. Using the forgoing definitions and the encryption process, we can get the following four types of impossible differential characteristics. (We can also get the other four types of impossible differential characteristics by using the decryption process.)

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

As mentioned before, if $a_i^r \geq 2$, we cannot predict the corresponding difference for a_i^r. It follows that we cannot find an impossible differential characteristic using the entry $t (\geq 2)$. However, the entries 0,1,1^*, and 2^* are useful to find impossible differential characteristics of $\mathcal{S}$. We denote the set of these entries by



r	$\boldsymbol{a}^r$
0	$(0,1^*)$
1	$(1^*,0)$
2	$(1,1^*)$
3	$(2^*,1)$
4	$(3,2^*)$
5	$(5,3)$

$\boldsymbol{b}^r$	r
$(3,5)$	5
$(2^*,3)$	4
$(1,2^*)$	3
$(1^*,1)$	2
$(0,1^*)$	1
$(1^*,0)$	0

Fig. 4. Corresponding differences to $\boldsymbol{a}^r$ and $\boldsymbol{b}^r$ where $\boldsymbol{a} = (0,1^*)$ and $\boldsymbol{b} = (1^*,0)$ (α_1 is a nonzero fixed difference and δ_i are nonzero nonfixed differences.)

$\mathcal{U} = \{0,1,1^*,2^*\}$. Other entries except for the elements of $\mathcal{U}$ will not be concerned.

If $\boldsymbol{a}_i^r \in \mathcal{U}$, as stated above, there exist r-round impossible differential characteristics. Furthermore, $\mathcal{S}$ may have impossible differential characteristics for more than r rounds when $a_i^r \in \mathcal{U}$. To find these long characteristics, we need to define an auxiliary set $\bar{m}$ with respect to the entry $m \in \mathcal{U}$. $\bar{m}$ has following two properties. First, $\bar{m}$ is a subset of $\mathcal{U}$. Second, the elements of $\bar{m}$ correspond to the differences which can not be represented by the entry m. Consider $\bar{1}^*$. Assume that the entry 1^* corresponds to a nonzero fixed difference γ. Then, the entry 1^* can not correspond to the differences such as zero, $\gamma'(\neq \gamma)$, or $\gamma \oplus \delta$. So, we have $\bar{1}^* = \{0,1^*,2^*\}$. Similarly, we have $\bar{m}$ for other element m as like Table 5.

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

Entry (m)	Difference	Entry set ($\bar{m}$)	Differences
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 differential characteristics for more than r rounds using the notations $m \in \mathcal{U}$ and $\bar{m}$, when $\boldsymbol{a}_i^r \in \mathcal{U}$? For example, assume $a_i^r = 2^*$ and $b_i^{r'} \in \bar{2}^*$. (Recall that only if $\mathcal{E}_{i,j} = 1$, $*$ is preserved, and $\mathcal{E}$ is 1-property matrix by our assumption.) $a_i^r = 2^*$ 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. Hence, there exists a

$(r+r')$-round impossible differential characteristic $\alpha \not\rightarrow_{r+r'} \beta$ where $\alpha_j = \beta_k$. Similarly, we can check the following properties.

- If $a_i^r = m$ and $b_i^{r'} \in \bar{m}$, then there exists $\alpha \not\rightarrow_{r+r'} \beta$.
- If $a_i^r \in \bar{m}$ and $b_i^{r'} = m$, then there exists $\alpha \not\rightarrow_{r+r'} \beta$.

We call this method that uses the elements of $\mathcal{U}$ to find impossible differential characteristics as **$\mathcal{U}$-method**.

Definition 3. *Given an input difference vector $\boldsymbol{a}$, the maximum number of encryption rounds with respect to $\boldsymbol{a}$ and the entry $m \in \mathcal{U}$ (or the set $\bar{m}$) is defined by*

$$\mathcal{ME}_i(\boldsymbol{a}, m) \triangleq max_r\{r|a_i^r = m\},$$
$$\mathcal{ME}_i(\boldsymbol{a}, \bar{m}) \triangleq max_{u\in\bar{m}}\{\mathcal{ME}_i(\boldsymbol{a}, u)\}.$$

Also, the maximum number of encryption rounds with respect to $m \in \mathcal{U}$ (or the set $\bar{m}$) is defined by

$$\mathcal{ME}_i(m) \triangleq max_{\boldsymbol{a}\neq 0}\{\mathcal{ME}_i(\boldsymbol{a}, m)\},$$

$$\mathcal{ME}_i(\bar{m}) \triangleq max_{\boldsymbol{a}\neq 0}\{\mathcal{ME}_i(\boldsymbol{a}, \bar{m})\}.$$

Similarly, each maximum number of decryption rounds is defined by

$$\mathcal{MD}_i(\boldsymbol{b}, m) \triangleq max_r\{r|b_i^r = m\},\ \mathcal{MD}_i(\boldsymbol{b}, \bar{m}) \triangleq max_{u\in\bar{m}}\{\mathcal{MD}_i(\boldsymbol{b}, u)\}.$$

$$\mathcal{MD}_i(m) \triangleq max_{\boldsymbol{b}\neq 0}\{\mathcal{MD}_i(\boldsymbol{b}, m)\},\ \mathcal{MD}_i(\bar{m}) \triangleq max_{\boldsymbol{b}\neq 0}\{\mathcal{MD}_i(\boldsymbol{b}, \bar{m})\}.$$

We denote $max_{i,m}\{\mathcal{ME}_i(\boldsymbol{a}, m) + \mathcal{MD}_i(\boldsymbol{b}, \bar{m})\}$ by $\mathcal{M}(\boldsymbol{a}, \boldsymbol{b})$. Then, clearly it holds that $\mathcal{M}(\boldsymbol{a}, \boldsymbol{b}) = max_{i,m}\{\mathcal{ME}_i(\boldsymbol{a}, \bar{m}) + \mathcal{MD}_i(\boldsymbol{b}, m)\}$. Let $max_{\boldsymbol{a}\neq 0, \boldsymbol{b}\neq 0}\{\mathcal{M}(\boldsymbol{a}, \boldsymbol{b})\}$ be denoted $\mathcal{M}$, then $\mathcal{M}$ can be computed by Equation (4). This equation will be used in the next section.

$$\mathcal{M} = max_{i,m}\{\mathcal{ME}_i(m) + \mathcal{MD}_i(\bar{m})\} = max_{i,m}\{\mathcal{ME}_i(\bar{m}) + \mathcal{MD}_i(m)\} \qquad (4)$$

So, 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 1-property matrices $\mathcal{E}$ and $\mathcal{D}$, then the maximum number of rounds for impossible differential characteristics that can be found in the $\mathcal{U}$-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 the Equations (2) and (3), we have $\mathcal{M}((0, 1^*), (1^*, 0)) = 5$. Similarly, we can solve the equations related to other difference vectors, $\boldsymbol{a}$ and $\boldsymbol{b}$. Using the equations, we can check $\mathcal{M}(\boldsymbol{a}, \boldsymbol{b}) \leq 4$. So, we have $\mathcal{M} = max_{\boldsymbol{a}\neq 0, \boldsymbol{b}\neq 0}\{\mathcal{M}(\boldsymbol{a}, \boldsymbol{b})\} = 5$. Hence the Feistel structure has a 5-round impossible differential characteristic whose form is $(0, \alpha_1) \not\rightarrow_5 (\beta_0, 0)$ where $\alpha_1 = \beta_0 \neq 0$ (Refer to Figure 4).

4 Algorithm to Compute the Length $\mathcal{M}$

In this section, we propose an algorithm to compute the maximum number of rounds for the impossible differential characteristics which can be found in the $\mathcal{U}$-method. The algorithm is applied to a block cipher structure $\mathcal{S}$ whose round function is bijective, and encryption characteristic matrix $\mathcal{E}$ and decryption characteristic matrix $\mathcal{D}$ are 1-property matrices. [4] We assume that a round function of $\mathcal{S}$ is bijective and $\mathcal{S}$ has 1-property matrices $\mathcal{E}$ and $\mathcal{D}$.

To perform the algorithm, we need some variables. Table 6 illustrates the meaning of variables used in the algorithm. The main part of the algorithm is to distinguish between entries x and x^* where $x = 1$ or 2. Using the variable s_i in Table 7, we can distinguish between entries x and x^*, i.e., the j^{th} entry of output difference vector for the r^{th} round has $*$ if and only if $s_0 + s_1 + \cdots + s_{n-1} = -1$, because $\mathcal{E}$ and $\mathcal{D}$ are 1-property matrices.

Table 6. The meaning of variables used in Algorithm 1. ($y \geq 0$)

Variables	Meanings
$e_{i,j} = 0$	$\mathcal{E}_{i,j} = 0$
$e_{i,j} = 1$	$\mathcal{E}_{i,j} = 1$ 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 $*$.)
$a_i^r = y$ (resp., x)	The i^{th} entry of difference vector $\boldsymbol{a^r}$ is y (resp., x^*).
$\hat{a}_i^r = 0$	The i^{th} entry of difference vector $\boldsymbol{a^r}$ has not $*$.
$\hat{a}_i^r = -1$	The i^{th} entry of difference vector $\boldsymbol{a^r}$ has $*$.

Table 7. Multiplication between an entry of difference vector and an entry of matrix in Algorithm 1.

A entry c,($\hat{a}_i^r$) of difference vectors	A entry d,($\widetilde{e}_{i,j}$) of $\mathcal{E}$	$c \cdot d$	$\hat{a}_i^r + \widetilde{e}_{i,j} = s_i$ 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

[4] In fact, we may compute the number of rounds $\mathcal{M}$ by modifying the algorithm even though $\mathcal{E}$ and $\mathcal{D}$ are not 1-property matrices.

```
Step 1 : Input the encryption characteristic matrix $\mathcal{E} = (\mathcal{E}_{i,j})_{n\times n}$

for $i = 0$ to $n-1$
    for $j = 0$ to $n-1$
        if $\mathcal{E}_{i,j} = 0$, then $e_{i,j} \leftarrow 0$ and $\widetilde{e}_{i,j} \leftarrow 1$
        if $\mathcal{E}_{i,j} = 1$, then $e_{i,j} \leftarrow 1$ and $\widetilde{e}_{i,j} \leftarrow 0$
        if $\mathcal{E}_{i,j} = 1_F$, then $e_{i,j} \leftarrow 1$ and $\widetilde{e}_{i,j} \leftarrow 1$

Step 2 : Compute the values of $\mathcal{ME}_i(m)$ where $0 \le i \le n-1$ and $m \in \mathcal{U}$.

$\mathcal{ME}_i(m) \leftarrow 0$,  for $0 \le i \le n-1$, $0 \le m \le 3$
/* The $m's$ values 0,1,2, and 3 indicate the entries $0, 1, 1^*$, and $2^*$, respectively. */
For each input difference vector $\boldsymbol{a}$      /* $\boldsymbol{a}$ represents $\boldsymbol{a^0}$. */
    for $i = 0$ to $n-1$
        if $(a_i^0 = 0)$ $\hat{a}_i \leftarrow 0$
        else if $(a_i^0 = 1)$ $\hat{a}_i \leftarrow -1$
        for $m = 0$ to 3
            $\mathcal{ME}_i(\boldsymbol{a}, m) \leftarrow 0$
    $r \leftarrow 0$
    while (there exists some index $l$ such that $a_l^r \le 2$.)
        for $j = 0$ to $n-1$
            $t_j \leftarrow 0$, $\hat{t}_j \leftarrow 0$
        /* $t_j$ and $\hat{t}_j$ are the temporary parameters to compute $\boldsymbol{a^{r+1}}$ and $\hat{\boldsymbol{a}}^{r+1}$. */
            for $i = 0$ to $n-1$
                $t_j \leftarrow t_j + a_i^r \cdot e_{i,j}$
                $s_i \leftarrow \hat{a}_i^r + \widetilde{e}_{i,j}$
                if $(s_i = 0)$    $s_i \leftarrow 0$
                $\hat{t}_j \leftarrow \hat{t}_j + s_i$
        $r \leftarrow r + 1$
        $a_i^r \leftarrow t_i$,  $\hat{a}_i^r \leftarrow \hat{t}_i$, for $0 \le i \le n-1$
        for $i = 0$ to $n-1$
            if $(a_i^r = 0)$    $\mathcal{ME}_i(\boldsymbol{a}, 0) \leftarrow r$
            if $(a_i^r = 1$ and $\hat{a}_i^r = 0)$    $\mathcal{ME}_i(\boldsymbol{a}, 1) \leftarrow r$
            if $(a_i^r = 1$ and $\hat{a}_i^r = -1)$    $\mathcal{ME}_i(\boldsymbol{a}, 2) \leftarrow r$
            if $(a_i^r = 2$ and $\hat{a}_i^r = -1)$    $\mathcal{ME}_i(\boldsymbol{a}, 3) \leftarrow r$
    for $i = 0$ to $n-1$
        for $m = 0$ to 3
            if $(\mathcal{ME}_i(m) \le \mathcal{ME}_i(\boldsymbol{a}, m))$    $\mathcal{ME}_i(m) \leftarrow \mathcal{ME}_i(\boldsymbol{a}, m)$

Step 3 : Compute the values of $\mathcal{MD}_i(\bar{m})$ where $0 \le i \le n-1$ and $m \in \mathcal{U}$.

Compute the values of $\mathcal{MD}_i(m)$ by inserting the matrix $\mathcal{D}$ into Steps 1 and 2.
for $i = 0$ to $n-1$
    $\mathcal{MD}_i(\bar{0}) \leftarrow max\{\mathcal{MD}_i(1), \mathcal{MD}_i(2)\}$
    $\mathcal{MD}_i(\bar{1}) \leftarrow \mathcal{MD}_i(0)$
    $\mathcal{MD}_i(\bar{2}) \leftarrow max\{\mathcal{MD}_i(0), \mathcal{MD}_i(2), \mathcal{MD}_i(3)\}$
    $\mathcal{MD}_i(\bar{3}) \leftarrow \mathcal{MD}_i(2)$
    /* Note $\bar{0}, \bar{1}, \bar{2}$, and $\bar{3}$ represent $\bar{0}, \bar{1}, \bar{1}^*$, and $\bar{2}^*$ in Table 5, respectively. */

Step 4 : Output the length $\mathcal{M}$. (Equation (4))

Output $max_{0 \le i \le n-1, 0 \le m \le 3}(\mathcal{ME}_i(m) + \mathcal{MD}_i(\bar{m}))$
```

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

5 Results for Some Block Cipher Structures

In this section, we present the specific forms of impossible differential characteristics for some block cipher structures such as a generalized Feistel network, a generalized CAST256-like structure, a generalized MARS-like structure, and a generalized RC6-like structure, and Rijndael structures. We experimentally find the impossible differential characteristics within a finite number of subblocks. However, we can generalize our simulation results, because a generalized block cipher structures has a regular structural feature.

5.1 Nyberg's Generalized Feistel Network (GFN_n)

GFN_n has 1-property matrices $\mathcal{E}$ and $\mathcal{D}$, so we can apply the network to Algorithm 1. The running time of Algorithm 1 is dominated by *Steps* 2 and 3. However, using the fact that the encryption process of GFN_n is almost same as the decryption process, $\mathcal{MD}_i(m)$ in Step 3 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 executed a program written in visual C 6.0 and running on a set of 10 PCs under Windows. From this, we found it in one computer with about 4 hours. The following proposition is a result based on our simulation.

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* $(3n+2)$.

By modifying Algorithm 1, we can get the specific forms of various impossible differential characteristics of GFN_n $(2 \leq n \leq 16)$, and we can generalize such characteristics as like Table 8.

Table 8. Impossible differential characteristics for GFN_n ($\alpha_i \neq 0$, $\beta_i \neq 0$, $(\beta'_0, \beta'_2) \neq (0,0)$, and $\beta''_0 = \alpha_2$.)

GFN_2	GFN_n $(n \geq 3)$
$(0,0,0,\alpha_3) \not\twoheadrightarrow_7 (\beta'_0,0,\beta'_2,0)$	$(0,0,0,\cdots,0,\alpha_{2n-1}) \not\twoheadrightarrow_{3n+2} (\beta'_0,0,\beta'_2,0,\cdots,0)$
$(0,0,\alpha_2,0) \not\twoheadrightarrow_7 (\beta'_0,0,\beta'_2,0)$	$(0,0,\cdots,0,\alpha_{2n-2},0) \not\twoheadrightarrow_{3n+2} (\beta_0,0,0,\cdots,0,0)$
$(0,0,\alpha_2,\alpha_3) \not\twoheadrightarrow_7 (\beta_0,0,0,0)$	$(0,\cdots,0,\alpha_{2n-2},\alpha_{2n-1}) \not\twoheadrightarrow_{3n+2} (\beta_0,0,0,0,\cdots 0)$
$(0,0,\alpha_2,\alpha_3) \not\twoheadrightarrow_7 (0,0,\beta_2,0)$	·
$(0,\alpha_1,\alpha_2,0) \not\twoheadrightarrow_7 (\beta''_0,0,0,0)$	·
$(0,\alpha_1,\alpha_2,\alpha_3) \not\twoheadrightarrow_7 (\beta''_0,0,0,0)$	·

We also performed Algorithm 1 for other generalized Feistel networks, e.g., a generalized CAST256-like structure, a generalized MARS-like structure, and a generalized RC6-like structure described in [14]. Table 9 shows the specific forms of impossible differential characteristics on each structure. Based on our experiment, we stress that the generalized MARS-like structure among the foregoing four structures has the most strong resistance against IDC.

Table 9. Impossible differential characteristics for other generalized Feistel networks ($\alpha_{n-1} \neq 0$, $\beta_0 \neq 0$. $\alpha_i = \beta_i \neq 0$ and i is an odd number.)

Structure	Impossible Differential Characteristic	Condition
Generalized CAST256	$(0,\cdots,0,\alpha_{n-1}) \not\rightarrow_{n^2-1} (\beta_0,0,\cdots,0)$	$n \geq 3$
Generalized MARS	$(0,\cdots,0,\alpha_{n-1}) \not\rightarrow_{2n-1} (\beta_0,0,\cdots,0)$	$n \geq 3$
Generalized RC6	$(0,\cdots,0,\alpha_i,0,\cdots,0) \not\rightarrow_{4n+1} (0,\cdots,0,\beta_i,0,\cdots,0)$	·

5.2 Rijndael Structure

The output subblock Y_i of Rijndael is affected by four input subblocks due to the linear layer composed of ShiftRow transformation and MixColumn transformation. Y_i is also affected by four subblocks after ByteSubstitution transformation. Thus, Rijndael structure has 1-property matrices $\mathcal{E}$ and $\mathcal{D}$ whose column has all zeros but four 1_F. It follows that Rijndael structure can be applied to Algorithm 1. Following is our simulation result.

Proposition 2. *(1) (Rijndael$_{128}$ structure [6]) Given plaintext pair which are equal at all bytes but one, the ciphertexts after 3 rounds cannot be equal in any of a column. (2) (Rijndael$_{196}$ structure) Given plaintext pair which are equal at all bytes but one, the ciphertexts after 4 rounds cannot be equal in any of three columns. (3) (Rijndael$_{256}$ structure) Given plaintext pair which are equal at all bytes but one, the ciphertexts after 5 rounds cannot be equal in any of seven columns.*

Note : Cheon et. al. [6] proposed an attack algorithm which uses the 3-round impossible differential characteristics of *Rijndael*$_{128}$ structure. (Note that the 4-round impossible differential characteristics proposed in [6] do not include the MixColumn and AddRoundKey transformations of the last round. These are the same characteristics for 3 rounds stated in Proposition 2.) In [6], sixteen of them are used to attack 6-round Rijndael with a data complexity of $2^{91.5}$ chosen plaintexts (CP) and a time complexity of 2^{122} encryptions. However we found other 3-round impossible differential characteristics to allow attacking 6-round Rijndael with less complexities. If we apply the 3-round impossible differential characteristics, $\alpha \not\rightarrow \beta$ or $\alpha \not\rightarrow \beta'$ [5] to the attack algorithm used in [6], then we can attack 6-round Rijndael which uses 128-bit data as like Table 10.

6 Further Research

An interesting property of the $\mathcal{U}$-method is that they can be converted to a tool of 1st order integral attack. Consider a block cipher structure whose round

[5] $\alpha = (0,\cdots,0,\alpha_i,0,\cdots,0)$ where $\alpha_i \neq 0$, and i is 0,4,8, or 12.
$\beta = (\beta_0,\beta_1,0,0,0,\beta_5,\beta_6,0,0,0,\beta_{10},0,\beta_{12},0,0,0)$,$(\beta_0,\beta_1,0,0,0,\beta_5,0,0,0,0,0,\beta_{11},\beta_{12},0,0,\beta_{15})$, $(\beta_0,0,0,0,0,0,\beta_6,0,0,0,\beta_{10},\beta_{11},\beta_{12},0,0,\beta_{15})$, or $(0,\beta_1,0,0,0,\beta_5,\beta_6,0,0,0,\beta_{10},\beta_{11},0,0,0,\beta_{15})$.
$\beta' = (0,0,0,0,0,\beta'_5,0,0,0,0,\beta'_{10},0,0,0,0,\beta'_{15})$,$(\beta'_0,0,0,0,0,0,0,0,0,0,\beta'_{10},0,0,0,0,\beta'_{15})$, $(\beta'_0,0,0,0,0,\beta'_5,0,0,0,0,0,0,0,0,0,\beta'_{15})$, or $(\beta'_0,0,0,0,0,\beta'_5,0,0,0,0,\beta'_{10},0,0,0,0,\beta'_{15})$ where $\beta_i \neq 0$ and $\beta'_i \neq 0$.

Table 10. Complexity of Impossible Differential Cryptanalysis on 6-Round Rijndael

3-round distinguishers used in the attack	Condition [a]	Data (CP)	Time (encryptions)
$\alpha \nrightarrow \beta$	8-byte	$2^{75.5}$	$2^{116.4}$
	9-byte	$2^{83.4}$	$2^{108.4}$
	10-byte	$2^{91.3}$	$2^{100.4}$
	11-byte	$2^{99.2}$	$2^{92.4}$
	12-byte	$2^{107.1}$	$2^{84.4}$
$\alpha \nrightarrow \beta'$	12-byte	$2^{99.1}$	$2^{84.4}$
	13-byte	$2^{107.0}$	$2^{76.4}$
	14-byte	$2^{114.9}$	$2^{68.4}$

[a] The number of bytes of ciphertext to be used for filtering out wrong pairs.

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 entry 0 in the set $\mathcal{U}$ corresponds to a constant value, and the entries 1 and 1^* corresponds to a saturated set, and the entries 2 and 2^* corresponds to a balanced set. Based on this fact, we performed simulations for the block cipher structures which were dealt with in this paper and found 1^{st} order integrals for less rounds than impossible differential characteristics on each cipher. (For example, GFN_n $(n \geq 2)$ has a $(2n+3)$-round 1^{st} order integral.)

Although we do not know of any other appliances of the method using the matrix, we expect that the possibility to apply the method to other attacks may be of interest.

References

1. C.M. Adams, *The CAST-256 Encryption Algorithm*, AES Proposal, 1998.
2. K. Aoki and K. Ohta, *Strict evaluation of the maximum average of differential probability and the maximem average of linear probability*, IEICE Transactions fundamentals of Electronics, Communications and Computer Sciences, No.1, 1997, pp 2-8.
3. E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Advances in Cryptology - CRYPTO'90, LNCS 537, Springer-Verlag, 1991, pp 2-21.
4. E. Biham, A. Biryukov, and A. Shamir, *Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials*, Advances in Cryptology - EUROCRYPT'99, LNCS 1592, Springer-Verlag, 1999, pp 12-23.
5. C. Burwick, D. Coppersmith, E. D'Avignon, R. Gennaro, S. Halevi, C. Jutla, S.M. Matyas, L. O'Connor, M. Peyravian, D. Safford, and N. Zunic, *MARS - A Candidate Cipher for AES*, AES Proposal, 1998.
6. J. Cheon, M. Kim, K. Kim, and J. Lee, *Improved Impossible Differential Cryptanalysis of Rijndael and Crypton,* ICISC'01, LNCS 2288, Springer-verlag, 2001, pp 39-49.
7. J. Daemen and V. Rijndael, *The Rijndael block cipher*, AES proposal, 1998.

8. S. Hong, S. Lee, J. Lim, J. Sung, D. Choen, and I. Cho, *Provable Security against Differential and Linear Cryptanalysis for the SPN structure*, FSE'00, LNCS 1978, Springer-Verlag, 2000, pp 273-283.
9. S. Hong, J. Sung, S. Lee, J. Lim, and J. Kim, *Provable Security for 13 round Skipjack-like Structure*, Information Processing Letters, vol 82, 2002, pp 243-246.
10. L.R. Knudsen, *DEAL - A 128-bit Block Cipher*, AES Proposal, 1998.
11. L. Knudsen and D. Wagner, *Integral cryptanalysis*, FSE'02, LNCS 2365, Springer-Verlag, 2002, pp 112-127.
12. M. Matsui, *Linear cryptanalysis method for DES cipher*, Advances in Cryptology - EUROCRYPT'93, LNCS 765, Springer-Verlag, 1994, pp 386-397.
13. M. Matsui, *New structure of block ciphers with provable security against differential and linear cryptanalysis*, FSE'96, LNCS 1039, Springer-Verlag, 1996, pp 205–218.
14. S. Moriai, S. Vaudenay , *On the Pseudorandomness of Top-Level Schemes of Block Ciphers*, Advances in Cryptology - ASIACRYPT'00, LNCS 1976, Springer-Verlag, 2000, pp 289-302.
15. National Security Agency. NSA Releases Fortezza Algorithms. Press Release, June 24, 1998. Available at http://csrc.ncsl.nist.gov/encryption/skipjack-1.pdf.
16. K. Nyberg and Lars R. Knudsen, *Provable security against differential cryptanalysis*, Advances in Cryptology - CRYPTO'92, LNCS 740, Springer-Verlag, 1992, pp 566–574.
17. K.Nyberg *Generalized Feistel Networks*, Advances in Cryptology - ASIACRYPT'96, LNCS 1163, Springer-Verlag, 1996, pp 91-104.
18. R.L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin, *The RC6 block cipher*, AES Proposal, 1998.
19. J. Sung, S. Lee, J. Lim, S. Hong, S. Park, *Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis*, Advances in Cryptology - ASIACRYPT'00, LNCS 1976, Springer-Verlag, 2000, pp 274-288.