A Peculiar Higher Order Differential of CLEFIA

Naoki SHIBAYAMA
Department of Electrical Engineering,
Faculty of Engineering,
Tokyo University of Science,
1-14-6 Kudankita, Chiyoda-ku,
Tokyo, 102-0073 Japan
Email: shiba@wit.ocn.ne.jp

Toshinobu KANEKO
Department of Electrical Engineering,
Faculty of Science and Technology,
Tokyo University of Science,
2641 Yamazaki, Noda,
Chiba, 278-8510 Japan
Email: kaneko@ee.noda.tus.ac.jp

***Abstract*—CLEFIA is a 128-bit block cipher proposed by Shirai et al. in 2007. In this paper, we focused on a higher order differential of CLEFIA. It has been reported that CLEFIA has 6-round saturation characteristics using 32-nd order differential. This paper introduces two new concepts for higher order differential (HOD) which are control transform for the input and observation transform for the output. With these concepts, we found a new 6-round HOD characteristic using 8-th order differential. By close examination of byte-value, we found the reason for this HOD. If we use the new HOD characteristic, instead of 32-nd order differential for the attack to 7-round CLEFIA, we can reduce to data and computational complexity around 2^{-23}, 2^{-15} of the conventional one, respectively.**

I. Introduction

Shirai et al. proposed a 128-bit block cipher CLEFIA supporting key lengths of 128, 192, 256 bits in 2007[1],[2]. A data processing part of CLEFIA consists of specified rounds of 4-branch type-2 generalized Feistel structure. The numbers of rounds are 18, 22, and 26 for 128-bit, 192-bit, and 256-bit keys, respectively. CLEFIA has been applied for cryptographic techniques towards the revision of the e-Gorvenment Recommended Ciphers List in FY 2013 in Japan[4].

The designer evaluated its strength against typical attack, such as differential cryptanalysis, linear cryptanalysis and so on. We analyzed its HOD property. It has been reported that CLEFIA has 6-round saturation characteristics using 32-nd order differential[7],[8],[10] and 9-round saturation characteristic theoretically[11].

This paper shows a peculiar HOD property of CLEFIA. Introducing two new concepts for HOD which are control transform for the input and observation transform for the output, we found a new 6-round HOD characteristic using synchronous 8-th order differential that has equivalent effects with the conventional 32-nd order differential. We also show that data and computational complexity for the new attack to 7-round CLEFIA can be reduced to around 2^{-23}, 2^{-15} of the conventional one, respectively.

II. CLEFIA

This section briefly describes the structure of CLEFIA.

Figure 1 shows data processing part of CLEFIA. Its input and ouput data are represented by $\mathrm{X}_i^{(1)}$ and $\mathrm{C}_i^{(r)}$ $(0 \leq i \leq 3)$, respectively. A bit length of $\mathrm{X}_i^{(1)}$ and $\mathrm{C}_i^{(r)}$ is 32. WK_i are whitening keys, and RK_i $(i = 0, 1, \cdots, 2r-1)$ are round keys, where r =18, 22, and 26 for 128-, 192-, and 256-bit key lengths, respectively. The functions F_i $(i = 0, 1)$ are bijective nonlinear functions with SP structures shown in Fig.2. Its input and output data are represented by x_{ij} and z_{ij} $(0 \leq j \leq 3)$, respectively. A bit length of x_{ij} and z_{ij} is 8. S_i $(i = 0, 1)$ denote S-boxes, which are bijective and nonlinear. The outputs of S_i are represented by y_{ij} $(0 \leq j \leq 3)$. M_i $(i = 0, 1)$ denote 4×4 nonsingular matrices. They transform y_{ij} to z_{ij} as

$$^{\mathrm{T}}(z_{i0}, z_{i1}, z_{i2}, z_{i3}) = M_i \, ^{\mathrm{T}}(y_{i0}, y_{i1}, y_{i2}, y_{i3}), \tag{1}$$

where

$$M_0 = \begin{bmatrix} 1 & 2 & 4 & 6 \\ 2 & 1 & 6 & 4 \\ 4 & 6 & 1 & 2 \\ 6 & 4 & 2 & 1 \end{bmatrix} \text{ and } M_1 = \begin{bmatrix} 1 & 8 & 2 & a \\ 8 & 1 & a & 2 \\ 2 & a & 1 & 8 \\ a & 2 & 8 & 1 \end{bmatrix}. \tag{2}$$

The uperscript T represents transposition of a vector or a matrix. The multiplications of a vector and matrix are performed in $\mathrm{GF}(2^8)$ defined by the primitive polynomial $z^8 + z^4 + z^3 + z^2 + 1$. Values in Eq.(2) are expressed in hexadecimal form.

III. Higher Order Differential Attack

This section gives an outline of HOD attack.

A. *Higher Order Differential* [5]

Let $E(\cdot)$ be an encryption function as follows.

$$Y = E(X; K), \tag{3}$$

where $X \in \mathrm{GF}(2)^n$, $Y \in \mathrm{GF}(2)^m$, and $K \in \mathrm{GF}(2)^s$. For a block cipher, X, K, and Y denote plaintext, key and ciphertext respectively. Let $\{A_1, A_2, \cdots, A_i\}$ be a set of linearly independent vectors in $\mathrm{GF}(2)^n$ and $V^{(i)}$ be the subspace spanned by these vectors. We define $\Delta^{(i)} E(X; K)$ as an i-th order differential of $E(X; K)$ with respect to X as follows.

$$\Delta^{(i)}_{V^{(i)}} E(X; K) = \bigoplus_{A \in V^{(i)}} E(X \oplus A; K) \tag{4}$$

In the following, we abbreviate $\Delta^{(i)}_{V^{(i)}}$ as $\Delta^{(i)}$, when it is clearly understood.

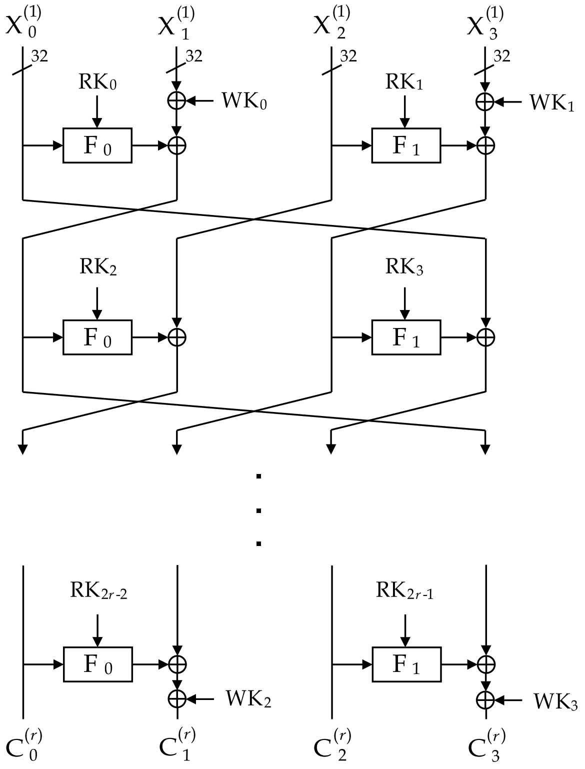
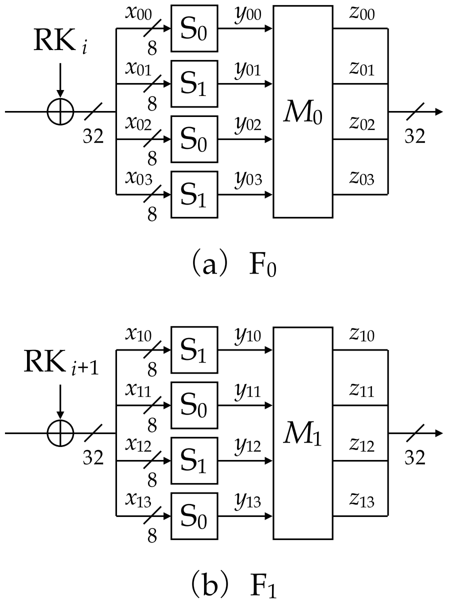


Fig. 1. Data processing part of CLEFIA



(a) F_0

(b) F_1

Fig. 2. (a) F_0, (b) F_1

In this paper, we use the following properties of the HOD.

Property 1 : If the degree of $E(X;K)$ with respect to X equals to N, then

$$deg_X\{E(X;K)\} = N \Rightarrow \begin{cases} \Delta^{(N+1)}E(X;K) & = 0, \\ \Delta^{(N)}E(X;K) & = const. \end{cases} \quad (5)$$

Property 2 : Higher order differential has a linear property on Exclusive-OR sum.

$$\begin{aligned} &\Delta^{(N)}\{E_1(X;K_1) \oplus E_2(X;K_2)\} \\ &\quad = \Delta^{(N)}E_1(X;K_1) \oplus \Delta^{(N)}E_2(X;K_2) \end{aligned} \quad (6)$$

B. Saturation Properties

We describe some definitions of saturation properties related to this paper.

Let a set of 2^N elements of N-bit values be $X = \{X_j | X_j \in \{0,1\}^N, 0 \leq j < 2^N\}$. Now we first categorize saturation properties of the set X into four types depending on conditions defined as follows.

- **Constant** (C) : if $\forall_{i,j}$, $X_i = X_j$
- **All** (A) : if $\forall_{i,j}$, $i \neq j \Leftrightarrow X_i \neq X_j$
- **Even** (E) : if $\forall_i$, $Y_i \equiv 0 \pmod 2$
- **Balance** (B) : if $\bigoplus_i X_i = 0$,

where Y_i denotes the number of occurrences of X_i.

In this paper, if the saturation property of 2^ℓ elements of N-bit values is ' A ', it is expressed as " $\mathrm{A}_{(\ell)}$ ". Further, when $\mathrm{A}_{(\ell)}$ is divided into $m\,(\geq 2)$-byte, it is written as follows.

$$\mathrm{A}_{(\ell)} = \begin{cases} (\mathrm{A}^0_{(8)}\, \mathrm{A}^1_{(8)} \cdots \mathrm{A}^{m-1}_{(8)}), & (\ell = 8m) \\ (\mathrm{A}^0_{(8)}\, \mathrm{A}^1_{(8)} \cdots \mathrm{A}^{m-1}_{(8)}\, \mathrm{A}^m_{(n)}), & (\ell = 8m + n) \end{cases} \quad (7)$$

where $0 < n < 8$. For example, 9-th order differential $\mathrm{A}_{(9)}$ is written as $(\mathrm{A}^0_{(8)}\, \mathrm{A}^1_{(1)})$.

C. Definition of ' all ' and ' Synchronous '

We define a new saturation property of 2^N elements of byte values, ' all ', as follows.

- **all** (a) : if $\forall_i$, $Y_i = 2^{N-8}$.

For example, $N = 16$ and $X = (x_0, x_1)$ is a 2-byte values, and its saturation property is $(\mathrm{A}^0_{(8)}\, \mathrm{A}^1_{(8)})$. It means the value of $0 \sim 2^{16} - 1$ appears once in (x_0, x_1). If its saturation property is (a a), it means the value of $0 \sim 2^8 - 1$ appears 2^8-time in x_0, x_1 respectively.

Let (X_0, X_1) be 2^N elements of two N-bit values, and the saturation property of X_0 be $\mathrm{A}_{(N)}$. We define a new saturation property, ' Synchronous ', for X_1 as follows.

- **Synchronous** (S) : if Eq.(8) holds.

$$X_0 \oplus X_1 = const \quad (8)$$

In the following, the property which synchronizes with $\mathrm{A}_{(\ell)}$ is written as " $\mathrm{S}_{(\ell)}$ ", and characteristics using $\mathrm{A}_{(\ell)}$ and $\mathrm{S}_{(\ell)}$ are called synchronous HOD characteristic.

D. others

- **Unknown** (U) : No specific condition is known.

In the following, if the saturation property of 1-byte values x_0 is $\mathrm{A}_{(8)}$, we express this as

$$\{x_0\} = \mathrm{A}_{(8)}. \quad (9)$$

For multiple-byte values, it is expressed as a similar manner. For example, if the saturation property of 4-byte values X is $(\mathrm{A}^0_{(8)}\ \mathrm{A}^1_{(8)}\ \mathrm{C}\ \mathrm{C})$, we express this as

$$\{X\} = (\mathrm{A}^0_{(8)}\,\mathrm{A}^1_{(8)}\,\mathrm{C}\,\mathrm{C}). \tag{10}$$

We also use the following expression.

$$\{X\} = (\mathrm{C}\,\mathrm{C}\,\mathrm{C}\,\mathrm{C}) = \mathbf{C}, \tag{11}$$

$$\{X\} = (\mathrm{A}^0_{(8)}\,\mathrm{A}^1_{(8)}\,\mathrm{A}^2_{(8)}\,\mathrm{A}^3_{(8)}) = \mathbf{A}_{(32)}, \tag{12}$$

where $\mathbf{A}_{(32)}$ follows expression rule of $\mathrm{A}_{(\ell)}$.

Property 3 : If saturation property of ciphertext Y is ‘C’, ‘A’, ‘E’, ‘B’, ‘a’, or ‘S’ using ℓ-th order differential, then

$$\Delta^{(\ell)}Y = 0. \tag{13}$$

E. Attack Equation

Consider an R-round interative block cipher. Let $H_{R-1}(X) \in \mathrm{GF}(2)^m$ be a part of the $(R-1)$-th round output and $C(X) \in \mathrm{GF}(2)^n$ be the ciphertext corresponding to the plaintext $X \in \mathrm{GF}(2)^n$. $H_{R-1}(X)$ is expressed as follows.

$$H_{R-1}(X) = E_{R-1}(X; K_1, K_2, \cdots, K_{(R-1)}), \tag{14}$$

where $K_i \in \mathrm{GF}(2)^s$ be the i-th round key and $E_i(\cdot)$ be a function of $\mathrm{GF}(2)^n \times \mathrm{GF}(2)^{s\times i} \rightarrow \mathrm{GF}(2)^m$.

If the degree of $E_{R-1}(\cdot)$ with respect to X is less than N, we have the following from Property 1.

$$\Delta^{(N)}H_{R-1}(X) = 0 \tag{15}$$

Let $\widetilde{E}(\cdot)$ be a function that calculates $H_{R-1}(X)$ from ciphertext $C(X) \in \mathrm{GF}(2)^n$.

$$H_{R-1}(X) = \widetilde{E}(C(X); K_R), \tag{16}$$

where $K_R \in \mathrm{GF}(2)^s$ denotes the R-th round key to decode $H_{R-1}(X)$ from $C(X)$. From Eqs.(15), (16), and (4), we can derive following equation and can determine K_R by solving it.

$$\bigoplus_{A \in V^{(N)}} \widetilde{E}(C(X \oplus A); K_R) = 0 \tag{17}$$

In the following, we refer to Eq.(17) as an attack equation.

IV. Higher Order Differential of CLEFIA

A. Previous Results

In the conventional analysis[7],[8],[10], saturation characteristics in 5-,6-round CLEFIA using 8-th, 32-nd order differential are written as

$$\begin{aligned}
&(\mathrm{A8-I}) && (\mathbf{C}\ (\mathrm{A}_{(8)}\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})\ \mathbf{C}\ \mathbf{C}) \xrightarrow{5r} (\mathbf{U}\ \mathbf{U}\ \mathbf{B}\ \mathbf{U}),\\
&(\mathrm{A8-II}) && (\mathbf{C}\ \mathbf{C}\ \mathbf{C}\ (\mathrm{A}_{(8)}\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})) \xrightarrow{5r} (\mathbf{B}\ \mathbf{U}\ \mathbf{U}\ \mathbf{U}),\\
&(\mathrm{A32-I}) && (\mathbf{C}\ \mathbf{A}_{(32)}\ \mathbf{C}\ \mathbf{C}) \xrightarrow{6r} (\mathbf{B}\ \mathbf{U}\ \mathbf{B}\ \mathbf{U}),\\
&(\mathrm{A32-II}) && (\mathbf{C}\ \mathbf{C}\ \mathbf{C}\ \mathbf{A}_{(32)}) \xrightarrow{6r} (\mathbf{B}\ \mathbf{U}\ \mathbf{B}\ \mathbf{U}).
\end{aligned}$$

B. New Characteristics

It is known that CLEFIA has 5-round HOD characteristics using 8-th order differential. We searched for HOD characteristics which extend 1-round of this HOD to the direction of plaintext. As a results, we found new 6-round HOD characteristics that have equivalent effect with the conventional 32-nd order differential.

16/12-th order differential

Using 16-th order differential, saturation characteristic from input to output of 6-round CLEFIA can be written as follows.

$$(\mathrm{A16})\ \ ((\mathrm{A}^0_{(8)}\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})\ \mathbf{a}^1_{(8)}\ \mathbf{C}\ \mathbf{C}) \xrightarrow{6r} (\mathbf{B}\ \mathbf{U}\ \mathbf{U}\ \mathbf{U}),$$

where $\mathbf{a}^i_{(8)} = (\mathrm{a}\,\mathrm{a}\,\mathrm{a}\,\mathrm{a})$ is the saturation property which is transformed $(\mathrm{A}^i_{(8)}\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})$ by M_{1-i}. This characteristic[1] is the same as the one in [11][12]. We also found a similar HOD characteristic, which is a 12-th order differential.

$$(\mathrm{A12})\ \ ((\mathrm{A}^0_{(4)}\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})\ \mathbf{a}^1_{(8)}\ \mathbf{C}\ \mathbf{C}) \xrightarrow{6r} (\mathbf{B}\ \mathbf{U}\ \mathbf{U}\ \mathbf{U}),$$

$$\mathrm{A}^0_{(4)} = \begin{cases} (\mathrm{A}^0_{(1)}\,\mathrm{A}^1_{(1)}\,\mathrm{A}^2_{(1)}\,\mathrm{A}^3_{(1)}\,\mathrm{C}\,\mathrm{C}\,\mathrm{C}\,\mathrm{C}), \\ \qquad\qquad \text{or} \\ (\mathrm{C}\,\mathrm{C}\,\mathrm{C}\,\mathrm{C}\,\mathrm{A}^0_{(1)}\,\mathrm{A}^1_{(1)}\,\mathrm{A}^2_{(1)}\,\mathrm{A}^3_{(1)}). \end{cases} \tag{18}$$

This is due to the structure of S_0, which has a S-P-S structure of 4-bit S-boxes.

C. Observation Transform : **9-th order differential**

If we decrease the order of differential $\mathrm{A}^0_{(4)}$ in Eq.(18) to $\mathrm{A}^0_{(1)}$, it is not a 6-round characteristic. It is a 5-round one as

$$(\mathrm{A9})\ \ ((\mathrm{A}^0_{(1)}\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})\ \mathbf{a}^1_{(8)}\ \mathbf{C}\ \mathbf{C}) \xrightarrow{5r} ((\mathrm{BEEE})\ \mathbf{U}\ \mathbf{B}\ \mathbf{U}).$$

The path is depicted in Fig.3. It can be transformed to 6-round HOD characteristic, using an observation transform mentioned below.

Let $\mathrm{X}^{(5)}_0$ be an input of round function F_0 in 5-th round. Let $\mathrm{Y}^{(5)}_0 = (y^{(5)}_{00}, y^{(5)}_{01}, y^{(5)}_{02}, y^{(5)}_{03})$ be an input of M_0 which is located in round function F_0 of 5-th round. If we use 9-th order differential (A9), byte-wise saturation property of $\mathrm{X}^{(5)}_0$ is $\{\mathrm{X}^{(5)}_0\} = (\mathrm{B}\,\mathrm{E}\,\mathrm{E}\,\mathrm{E})$. It passes through S-box layer. The property of $\mathrm{Y}^{(5)}_0$ is

$$\{\mathrm{Y}^{(5)}_0\} = (\mathrm{U}\,\mathrm{E}\,\mathrm{E}\,\mathrm{E}) = \begin{cases} \{y^{(5)}_{00}\} = \mathrm{U}, \\ \{(y^{(5)}_{01}, y^{(5)}_{02}, y^{(5)}_{03})\} = (\mathrm{E}\,\mathrm{E}\,\mathrm{E}). \end{cases} \tag{19}$$

Only $y^{(5)}_{00}$ has property ‘U’. This property defuses to the whole output of M_0. Though

$$\{\mathrm{X}^{(5)}_1\} = (\mathrm{a}\ \mathrm{a}\ \mathrm{a}\ \mathrm{a}), \tag{20}$$

[1] It has been reported that CLEFIA has a 9-round saturation characteristic using 112-nd order differential in [11] written as

$$(\mathrm{A112})\ \ (\mathbf{A}^0_{(32)}\ \mathbf{A}^1_{(32)}\ (\mathbf{a}^0_{(8)} \oplus \mathbf{a}^1_{(8)})\ \mathbf{A}^2_{(32)}) \xrightarrow{9r} (\mathbf{U}\ \mathbf{U}\ \mathbf{B}\ \mathbf{U}).$$

The characteristic is a 3-round extension of 6-round one using 16-th order differential. By using this characteristic, the 12 (13/14) -round CLEFIA with 128 (192/256) -bit secret key is attacked with 2^{113} blocks of chosen plaintext and $2^{116.7}$ $(2^{180.5}/2^{244.5})$ times of data encryption.

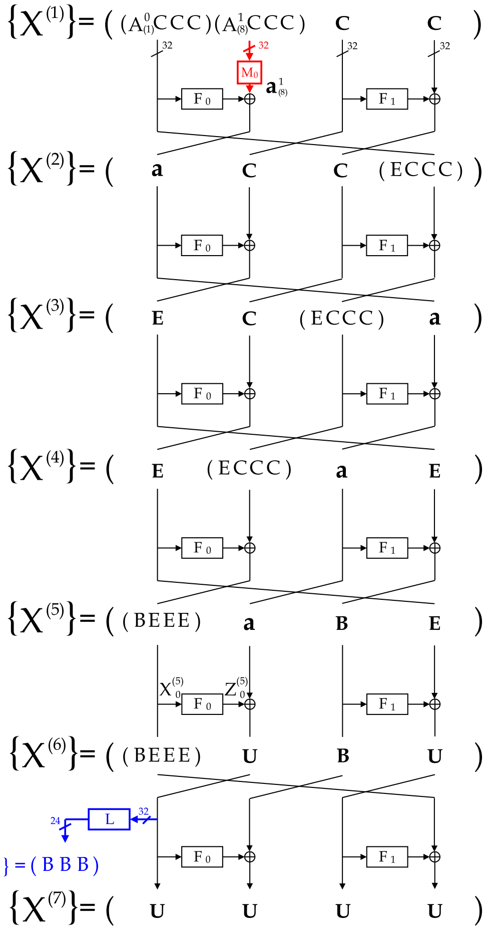


Fig. 3. 6-round HOD characteristic using 9-th order differential

the property of

$$\mathrm{X}_0^{(7)} = M_0\ {}^{\mathrm{T}}\mathrm{Y}_0^{(5)} \oplus \mathrm{X}_1^{(5)}, \tag{21}$$

turned to be $\{\mathrm{X}_0^{(7)}\} = (\mathrm{U\,U\,U\,U})$.

We apply a transformation L to eliminate $y_{00}^{(5)}$ in Eq.(21). From simple calculation, L can be written as

$$L = \begin{bmatrix} 2 & 1 & 3 & 2 \\ 4 & 3 & 1 & 1 \\ 6 & 2 & 1 & 1 \end{bmatrix}. \tag{22}$$

Let $\mathrm{H} = (h_0, h_1, h_2)$ be an output of L.

$${}^{\mathrm{T}}\mathrm{H} \ = \ L\ {}^{\mathrm{T}}\mathrm{X}_0^{(7)} = L\,M_0\ {}^{\mathrm{T}}\mathrm{Y}_0^{(5)} \oplus L\ {}^{\mathrm{T}}\mathrm{X}_1^{(5)} \tag{23}$$

$$= \begin{bmatrix} 0 & 7 & 9 & c \\ 0 & 9 & 19 & 17 \\ 0 & c & 17 & 1f \end{bmatrix} \begin{bmatrix} y_{00}^{(5)} \\ y_{01}^{(5)} \\ y_{02}^{(5)} \\ y_{03}^{(5)} \end{bmatrix} \oplus L\ {}^{\mathrm{T}}\mathrm{X}_1^{(5)} \tag{24}$$

As we chose L so that $L\,M_0\ {}^{\mathrm{T}}\mathrm{Y}_0^{(5)}$ does not contain $y_0^{(5)}$ from Eqs.(19), (20), and Property 2, we can conclude the property of H is

$$\{\mathrm{H}\} = (\mathrm{B\ B\ B}). \tag{25}$$

In this paper, linear transformation L of Eq.(23) is called **observation transform**. Using this transform and 9-th order differential, we found a 6-round HOD characteristic that has equivalent effects with the conventional 32-nd order differential. Note that this relation also holds if saturation property of $\mathrm{X}_1^{(5)}$ is $\{\mathrm{X}_1^{(5)}\} = (\mathrm{E\,E\,E\,E})$.

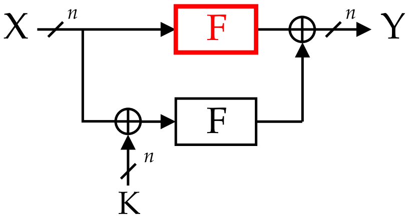


Fig. 4. Block diagram which generates ‘E’

D. Control Transform

From Fig.3 and the note after the Eq.(25), we focus on a structure which generates ‘E’. We transform plaintext input to make ‘E’ in internal round, and we call such transformation as **control transform**.

A structure which generates ‘E’

Figure 4 shows a structure which generates ‘E’, where X and Y are an input and output of this structure, K is a key and F is a bijective function.

When the saturation property of $\{\mathrm{X}\} = \mathrm{A}$, in the case of $\mathrm{K} = 0$, since the value of Y is always 0, the saturation property of $\{\mathrm{Y}\} = \mathrm{C}$. In the case of $\mathrm{K} \neq 0$, as $\{\mathrm{X}\} = \mathrm{A}$, for the pair of inputs $\mathrm{X} = x$ and $x \oplus \mathrm{K}$, the outputs are the same $\mathrm{Y} = \mathrm{F}(x) \oplus \mathrm{F}(x \oplus \mathrm{K})$. This means the saturation property of $\{\mathrm{Y}\} = \mathrm{E}$. In addition, for ‘C’, the same value appears 2^n-time. It means ‘C’ is a kind of ‘E’. Therefore, when the saturation property of $\{\mathrm{X}\} = \mathrm{A}$, the saturation property of $\{\mathrm{Y}\} = \mathrm{E}$.

Synchronous 8-th order differential

We add a structure of Fig.4 to CLEFIA, then we get Fig.5. In this figure, F_0 (as shown in red color) is a control transform for this HOD. In this scenario, saturation property of $\mathrm{X}_0^{(2)}$ is $\{\mathrm{X}_0^{(2)}\} = (\mathrm{E\,E\,E\,E})$ as we expected. We can easily confirm the existence of the following HOD characteristic.

$$\text{(S8)}\quad ((\mathrm{A}_{(8)}\mathrm{CCC})\ \mathbf{s}_{(8)}\ \mathbf{C}\ \mathbf{C}) \xrightarrow{6r} \{X_0^{(7)}\} \overset{L}{\mapsto} \{\mathrm{H}\} = (\mathrm{B\,B\,B}),$$

where $\mathbf{s}_{(8)} = (\mathrm{a\,a\,a\,a})$ is the saturation property which is transformed $(\mathrm{S}_{(8)}\mathrm{CCC})$ by F_0 to make ‘E’. Thus, by using control transform and observation transform, we get a peculiar 6-round HOD of synchronous 8-th order differential.

E. Necessary Number of Chosen Plaintexts and Computational Complexity

We evaluate the number of chosen plaintexts and computational complexity for the new attack to 7-round CLEFIA by using the peculiar HOD characteristic (S8).

Let $\mathrm{C}_j^{(7)} = (c_{j0}^{(7)}, c_{j1}^{(7)}, c_{j2}^{(7)}, c_{j3}^{(7)})$ be a ciphertext word (=4-byte) of 7-th round output. From Fig.5, we derive the attack

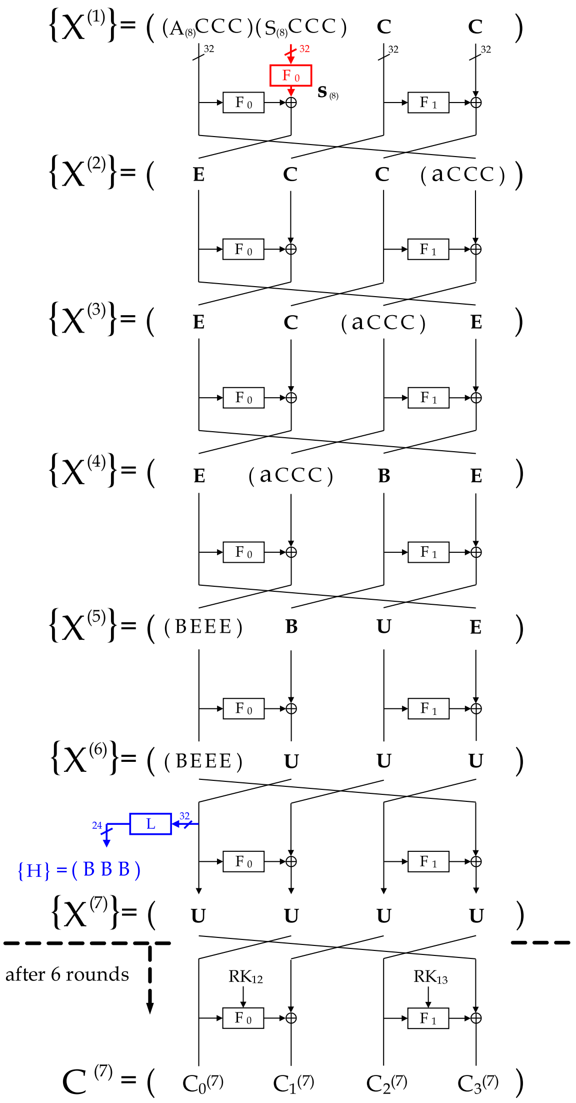


Fig. 5. 6-round HOD characteristic using synchronous 8-th order differential

equation using an observation transform as follows.

$$\bigoplus L\left(\mathrm{F}_1\left(\mathrm{C}_2^{(7)};\mathrm{RK}_{13}\right)\oplus \mathrm{C}_3^{(7)}\right)=0 \qquad (26)$$

There are 32-bit unknowns $\mathrm{RK}_{13} = (rk_{130}, rk_{131}, rk_{132}, rk_{133})$ in the equation. This can be rewritten as

$$\bigoplus L\, M_1 \begin{pmatrix} S_1(c_{20}^{(7)} \oplus rk_{130}) \\ S_0(c_{21}^{(7)} \oplus rk_{131}) \\ S_1(c_{22}^{(7)} \oplus rk_{132}) \\ S_0(c_{23}^{(7)} \oplus rk_{133}) \end{pmatrix} = \bigoplus L\, \mathrm{C}_3^{(7)}. \qquad (27)$$

This is a system of byte equations. Applying elementaly row operation to reduce unknowns in each byte equation, we can get a byte equation which contains 2-byte unknowns, for example, (rk_{130}, rk_{131}). If we solve it exhaustively, we need $3\,(> \frac{16}{8})$ sets of HOD (which needs $3 \times 2^8 \simeq 2^{9.6}$ chosen plaintexts) and $2^8 \times 2^{16} \times 2 = 2^{25}$ times of S-box operation. The left 2-byte keys (rk_{132}, rk_{133}) can recovery in similar manner.

Next, we describe an attack by using the conventional 32-nd order differential. The attack equation is given by

$$\bigoplus \mathrm{F}_1\left(C_2^{(7)};\mathrm{RK}_{13}\right) \oplus C_3^{(7)} = 0. \qquad (28)$$

As a similar manner, we can reduce the equation to a byte equation which contains 1-byte unknowns rk_{13i}. If we solve it, we need $2\,(> \frac{8}{8})$ sets of HOD (which needs $2 \times 2^{32} = 2^{33}$ chosen plaintexts) and $2^{32} \times 2^8 = 2^{40}$ times of S-box operation.

Therefore, the data and computational complexity are for the new attack are reducible about $\frac{2^{9.6}}{2^{33}} \simeq 2^{-23}$, $\frac{2^{25}}{2^{40}} = 2^{-15}$ of the conventional one, respectively.

V. Conclusion

We have studied a HOD property of CLEFIA. Introducing two new concepts for HOD which are control transform for the input and observation transform for the ouput, we found a new 6-round HOD characteristic using synchronous 8-th order differential that has equivalent effects with to the conventional 32-nd order differential. By close examination of byte-value, we found the reason for this HOD. We also show that data and computational complexity for the new attack to 7-round CLEFIA can be reduced to around 2^{-23}, 2^{-15} of the conventional one, respectively.

There is a left research problem to consider round extension of a peculiar 6-round HOD characteristic.

References

[1] T.Shirai, K.Shibutani, T.Akishita, S.Moriai, and T.Iwata, “The 128-bit Blockcipher CLEFIA,” FSE2007, LNCS4593, pp.181-195, Springer-Verlag, 2007.

[2] CLEFIA web home page, http://www.sony.net/Products/cryptography/clefia/

[3] The 128-bit Blockcipher CLEFIA Self Evaluation Report Ver.1.0, Sony Corporation, Jan. 2010. http://www.sony.net/Products/cryptography/clefia/technical/data/CRYPTREC_CLEFIA_submission.zip

[4] CRYPTREC topics, http://www.cryptrec.go.jp/english/topics/cryptrec_20101001_callforattack.html

[5] X.Lai, “Higher Order Derivatives and Differential Cryptanalysis,” Communications and Cryptography, pp.227-233, Kluwer Academic Publishers, 1994.

[6] K.Hwang, W.Lee, S.Lee, S.Lee, and J.Lim, “Saturation Attacks on Reduced Round Skipjack,” FSE2002, LNCS2365, pp.100-111, Springer-Verlag, 2002.

[7] Y.Tsunoo, E.Tsujihara, H.Kubo, M.Shigeri, and T.Kawabata, “Saturation Characteristics of Generalized Feistel Structure,” IEICE Trans. Fundamentals (Japanese Edition), Vol.J93-A, No.4, pp.269-276, April 2010.

[8] N.Shibayama, Y.Igarashi, T.Kaneko, and S.Hangai, “Security Evaluation of CLEFIA against Saturation Cryptanalysis,” Proc. SCIS2011, 2B1-4 (in Japanese).

[9] CRYPTREC technical report, “Evaluation of security level of CLEFIA,” http://www.cryptrec.go.jp/estimation/techrep_id2002.pdf

[10] Y.Igarashi, T.Kaneko, “Some Saturation Characteristics of XOR Sum of Balance Functions,” IEICE Trans. Fundamentals, Vol.E95-A, No.1, pp.2-7, 2012.

[11] Y.Li, W.Wu, and L.Zhang, “Improved Integral Attacks on Reduced-Round CLEFIA Block Cipher,” WISA2011, Lecture Notes in Computer Sicence, vol.7115, pp.28-39, Springer-Verlag, 2012.

[12] N.Shibayama, T.Kaneko, and S.Hangai, “A Peculiar Higher Order Differential Property of CLEFIA,” Proc. SCIS2012, 1C3-2 (in Japanese).