# Higher Order Differential Attack Using Chosen Higher Order Differences

Shiho Moriai[1], Takeshi Shimoyama[2], and Toshinobu Kaneko[2,3]

[1] NTT Laboratories
1-1 Hikari-no-oka, Yokosuka, 239-0847 Japan
shiho@isl.ntt.co.jp
[2] TAO
1-1-32 Shin-urashima-cho, Kanagawa-ku, Yokohama, 221-0031 Japan
shimo@yokohama.tao.go.jp
[3] Science University of Tokyo
2641 Yamazaki, Noda, Chiba, 278-8510 Japan
kaneko@ee.noda.sut.ac.jp

**Abstract.** This paper introduces an improved higher order differential attack using chosen higher order differences. We can find a lower order of the higher order differential by choosing higher order differences. It follows that the designers of a block cipher can evaluate the lower bound of the number of chosen plaintexts and the complexity required for the higher order differential attack. We demonstrate an improved higher order differential attack of a CAST cipher with 5 rounds using chosen higher order differences with fewer chosen plaintexts and less complexity. Concretely, we show that a CAST cipher with 5 rounds is breakable with $2^{16}$ plaintexts and $< 2^{24}$ times the computation of the round function, which half the values reported in Fast Software Encryption Workshop'98. We also show that it is breakable with $2^{13}$ plaintexts and about $2^{44}$ times the computation of the round function, which are $\frac{1}{16}$-th of those reported in Fast Software Encryption Workshop'97.

## 1 Introduction

Higher order differential attack is a powerful algebraic cryptanalysis. It is useful for attacking ciphers which can be represented as Boolean polynomials of low degrees. After Lai mentioned the cryptographic significance of derivatives of Boolean functions in [9], Knudsen used this notion to attack ciphers that were secure against conventional differential attacks [8]. At FSE'97 Jakobsen and Knudsen [7] gave an extension of Knudsen's attacks and broke ciphers using quadratic functions such as the cipher $\mathcal{KN}$ [12]. They were provably secure ciphers against differential and linear cryptanalysis. Furthermore, at Information Security Workshop'97 [13], we reduced the complexity required for the higher order differential attack of the cipher $\mathcal{KN}$ by solving the attack equation algebraically. At Fast Software Encryption Workshop'98 [11], we generalized it and applied it to a CAST cipher.

S. Tavares and H. Meijer (Eds.): SAC'98, LNCS 1556, pp. 106–117, 1999.

This paper introduces an improved higher order differential attack using chosen higher order differences. The higher order differential attack exploits the fact that a higher order differential (e.g., the $d$-th order differential) of an intermediate data is constant, or independent of the key. In this paper we call the order "$d$" *the order of the higher order differential.*

In the known higher order differential attack [7, Theorem 1], the order of the higher order differential was found from the algebraic degree of Boolean polynomials of the ciphertexts. That is, if a ciphertext bit is represented by a Boolean polynomial of plaintext bits of degree $d$, then $d+1$ is the order of the higher order differential, since the $(d+1)$-th order differential of the ciphertexts becomes 0. Furthermore, in the higher order differential attack described in [11], it was shown that if all subkeys are combined using operation XOR in a Feistel cipher, the order of the higher order differential is equal to the algebraic degree of the Boolean polynomials of ciphertexts. That is, if a ciphertext bit is represented by a Boolean polynomial of plaintexts of degree $d$, then $d$ is the order of the higher order differential, since the $d$-th order differential of the ciphertexts becomes 1. It is known that the order of the higher order differential determines the required number of plaintexts and ciphertexts pairs (p/c pairs) and complexity. Therefore, it is important to find the lowest order of the higher order differential to estimate the security of a cipher against the higher order differential attack.

This paper shows that we can find the lower order of the higher order differential by choosing higher order differences. For example, we demonstrate the higher order differential attack of a CAST cipher using chosen higher order differences with fewer chosen p/c pairs and less complexity. Concretely, we show that a CAST cipher with 5 rounds is breakable with $2^{16}$ plaintexts and $< 2^{24}$ times the computation of the round function, which half the values reported in Fast Software Encryption Workshop'98 [11]. We also show that it is breakable with $2^{13}$ plaintexts and about $2^{44}$ times the computation of the round function, which are $\frac{1}{16}$-th of those reported in Fast Software Encryption Workshop'97 [7]. The reason why we apply the improved higher order differential attack to a CAST cipher with 5 rounds is that we wan to to show how much improvement is achieved by choosing higher order differences. This attack is also applicable to other block ciphers. A similar improved higher order differential attack of a 5-round MISTY without FL functions is shown in [14].

## 2 Higher Order Differential Attack

This section gives an outline of the higher order differential attack. Fuller descriptions of the attack are presented in the references [7,9,11].

Let the target be a Feistel cipher with block size 64 bits and $r$ rounds. We assume that the right half 32-bit of the plaintext is fixed at any value. We denote the left half 32-bit of the plaintext by $x = (x_{31}, \ldots, x_0) \in GF(2)^{32}$, the ciphertext by $y = (y_L, y_R)$, $y_L, y_R \in GF(2)^{32}$, and the key by $k = (k_{l-1}, \ldots, k_0)$, where the key length is $l$ bits. Let $X$ and $K$ be sets of variables s.t. $X = \{x_{31}, \ldots, x_0\}$ and

$K = \{k_{l-1}, \ldots, k_0\}$. Let $k^{(i)} = (k_{31}^{(i)}, \ldots, k_0^{(i)})$ be the $i$-th round key. Throughout this paper, the subscript 0 indicates the least significant bit of the data.

When the key $k$ is fixed, an intermediate bit in the encryption process denoted by $z \in GF(2)$ can be represented as a Boolean polynomial with respect to $X$ whose coefficients are Boolean polynomials with respect to $K$, i.e., $z = g[k](x)$, where

$$g[k](x) = \sum c_{i_{31},\ldots,i_0}(k) \cdot x_{31}^{i_{31}} \cdots x_0^{i_0}.$$

Note that $c_{i_{31},\ldots,i_0}(k)$ is the coefficient of $x_{31}^{i_{31}} \cdots x_0^{i_0}$, and $i_{31}, \ldots, i_0$ is 0 or 1.

**Definition 1.** *We define the $i$-th order differential of $g[k](x)$ with respect to $X$, denoted by $\Delta^{(i)}_{(a_i,\ldots,a_1)} g[k](x)$, as follows;*

$$\Delta^{(1)}_{(a)} g[k](x) = g[k](x) + g[k](x+a),$$
$$\Delta^{(i)}_{(a_i,\ldots,a_1)} g[k](x) = \Delta^{(1)}_{(a_i)} \left( \Delta^{(i-1)}_{(a_{i-1},\ldots,a_1)} g[k](x) \right),$$

*where $a \in GF(2)^{32}$, and $\{a_i, \ldots, a_1\} \subseteq GF(2)^{32}$ are linearly independent. Let "+" denote bitwise XOR. In this paper, since we consider only the higher order differential with respect to $X$, we omit "with respect to $X$."*

**Definition 2.** *On $\Delta^{(i)}_{(a_i,\ldots,a_1)} g[k](x)$, which is the $i$-th order differential of $g[k](x)$, we define $i$ as the order of the higher order differential. Furthermore, we define $\{a_i, a_{i-1}, \ldots, a_1\}$ as the $i$-th order differences. The $i$-th order differences consist of $i$-tupple differences in $GF(2)^{32}$.*

The following theorems are known on the higher order differential of Boolean functions [9,13].

**Theorem 1.** [9] *The following equation holds for any $b \in GF(2)^{32}$ and $\{a_i, \ldots, a_1\} \subseteq GF(2)^{32}$.*

$$\Delta^{(i)}_{(a_i,\ldots,a_1)} g[k](b) = \sum_{x \in V^{(i)}[a_i,\ldots,a_1]} g[k](x+b).$$

*Note that $V^{(i)}[a_i, \ldots, a_1]$ denotes the $i$-dimensional subspace spanned by $\{a_i, \ldots, a_1\}$. In other words, it is the set of all $2^i$ possible linear combinations of $a_i, \ldots, a_1$, where each $a_i$ is in $GF(2)^{32}$ and linearly independent.*

**Theorem 2.** [13] *Let $d$ be a natural number. Let $\{a_{d+1}, \ldots, a_1\} \subseteq GF(2)^{32}$ be linearly independent. If the degree of $g[k](x)$ with respect to $X$ is $d$, then we have the following equations.*

$$\Delta^{(d)}_{(a_d,\ldots,a_1)} g[k](x) \in R[K], \quad \text{and}$$
$$\Delta^{(d+1)}_{(a_{d+1},\ldots,a_1)} g[k](x) = 0,$$

*where $R[K]$ is the Boolean polynomial ring of $K$.*

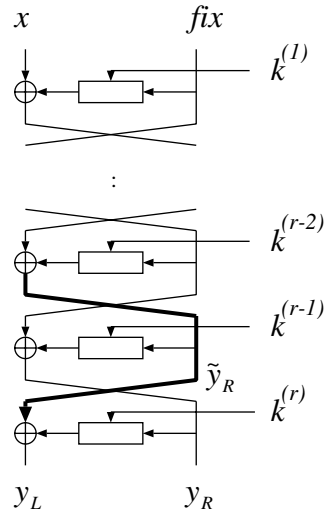


**Fig. 1.** A higher order differential attack of Feistel ciphers

**Attack Procedure.** In the improved higher order differential attack described in this paper, the last round key $k^{(r)}$ is recovered as follows (See also Fig.1.).

**Step 1.** Find the lowest order $d$ s.t. for the $d$-th order differences ${}^{\exists}\{a_d, \ldots, a_1\} \in GF(2)^{32}$ and ${}^{\exists}b \in GF(2)^{32}$, the $d$-th order differential of $\tilde{y}_R(b)$, i.e., $\Delta^{(d)}_{(a_d,\ldots,a_1)}\tilde{y}_R(b)$, is independent of the key.

**Step 2.** Construct attack equation (1) and solve it with respect to the last round key $k^{(r)}$.

$$\begin{aligned} & \Delta^{(d)}_{(a_d,\ldots,a_1)}F[k^{(r)}](y_R(b)) + \Delta^{(d)}_{(a_d,\ldots,a_1)}y_L(b) = \Delta^{(d)}_{(a_d,\ldots,a_1)}\tilde{y}_R(b) \\ \Longleftrightarrow & \sum_{x\in V^{(d)}[a_d,\ldots,a_1]+b} F[k^{(r)}](y_R(x)) + \sum_{x\in V^{(d)}[a_d,\ldots,a_1]+b} y_L(x) = \sum_{x\in V^{(d)}[a_d,\ldots,a_1]+b} \tilde{y}_R(x) \quad (1) \end{aligned}$$

One way to find the last round key $k^{(r)}$ is exhaustive search [7], where the attacker tries all $2^{32}$ possible candidates of $k^{(r)}$ and finds the correct key. Another way is the algebraic solution [13,11], where the attacker transforms the algebraic equations into the system of linear equations and solves it, for example.

## 3 CAST Ciphers

This section describes CAST ciphers, which we use for demonstrating the improved higher order differential attack.

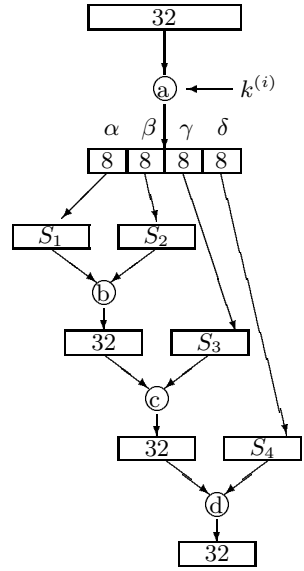


**Fig. 2.** Round function of CAST ciphers

CAST ciphers are a family of symmetric ciphers constructed using the CAST design procedure proposed by Adams and Tavares [1]. The CAST design procedure describes that they appear to have good resistance to differential cryptanalysis [5], linear cryptanalysis [10], and related-key cryptanalysis [4].

CAST ciphers are based on the framework of the Feistel cipher. The round function is specified as follows (See also Fig.2.). A 32-bit data half is input to the function along with a subkey $k^{(i)}$. These two quantities are combined using operation "a" and the 32-bit result is split into four 8-bit pieces. Each piece is input to a different $8 \times 32$ S-box ($S_1$, $S_2$, $S_3$, and $S_4$). S-boxes $S_1$ and $S_2$ are combined using operation "b"; the result is combined with $S_3$ using operation "c"; this second result is combined with $S_4$ using operation "d". The final 32-bit result is the output of the round function.

The CAST design procedure allows a wide variety of possible round functions: 4 S-boxes and 4 operations (a,b,c, and d). As for S-boxes, reference [3] suggested constructing the S-boxes from bent functions. Later, on reference [6] CAST ciphers with random S-boxes was proposed. In our attack, we use the S-boxes based on bent functions proposed for CAST-128. CAST-128 is a famous example CAST cipher used in several commercial applications, e.g., PGP5.0. As for operations, a simple way to define the round function is to specify that all operations are XORs, which is addition on $GF(2)$, although other operations may be used instead. Actually, according to reference [1], some care in the choice of operation "a" can conceivably give intrinsic immunity to differential and linear cryptanalysis.

As for the number of rounds, it seems that the CAST design procedure doesn't specify a concrete number. For example, CAST-128 has 12 or 16 rounds [2]. There are also several key schedules for CAST ciphers, but for the purpose of our attack the key schedule makes no difference.

# 4 Higher Order Differential Attacks of a 5-round CAST Cipher using Chosen Higher Order Differences

This section demonstrates an improved higher order differential attack using chosen higher order differences. The target is the CAST cipher with 5 rounds described in Section 3. The improvement consists in Step 1 in the attack procedure in Section 2.

## 4.1 How to find the lowest order of the higher order differential

**Using degree of Boolean polynomials** In the previously known higher order differential attack, the order of the higher order differential was derived using the degree of Boolean polynomials of $\tilde{y}_R(x)$ with respect to $X$.

The way to find the order of the higher order differential of the CAST cipher with 5 rounds is as follows. We begin by considering the degree of the round function. Let $S_1$, $S_2$, $S_3$, and $S_4$ be the functions of S-boxes: $GF(2)^8 \rightarrow GF(2)^{32}$. It is shown in [11] that for every S-box all output bits can be represented by Boolean polynomials of input bits of degree 4. Considering the structure of the round function (See Fig.2), all output bits of the round function can be represented by Boolean polynomials of input bits of degree 4, since we assume that operations "a", "b", "c", and "d" are XORs [11].

If we fix the right half of the plaintext at $0 \in GF(2)^{32}$, the right half of the output of the 4-th round $\tilde{y}_R(x) \in GF(2)^{32}$ can be represented as Eq. (2).

$$\tilde{y}_R(x) = f(f(x + f(k^{(1)}) + k^{(2)}) + k^{(3)}) + x + f(k^{(1)}), \tag{2}$$

where $f : GF(2)^{32} \rightarrow GF(2)^{32}$ is the round function. Since $f$ can be represented by Boolean polynomials of input bits of degree 4, the degree of $f(x+f(k^{(1)})+k^{(2)})$ with respect to $X = \{x_{31}, \ldots, x_0\}$ is 4, and the terms of the 4-th degree have the coefficient in $GF(2)^{32}$, which means that it is independent of the key. Hence, the degree of $\tilde{y}_R(x)$ with respect to $X$ is at most 16, and the terms of the 16-th degree included in Eq. (2) have the coefficient in $GF(2)^{32}$, which means that it is independent of the key. Therefore, the 16-th order differential of $\tilde{y}_R(x)$ is constant for any linearly independent 16-th order difference $\{a_{16}, a_{15}, \ldots, a_1\}$.

$$\Delta^{(16)}_{(a_{16},\ldots,a_1)} \tilde{y}_R(x) = \sum_{x \in V^{(16)}[a_{16},\ldots,a_1]} \tilde{y}_R(x) \quad = \; c \; \in GF(2)^{32} \quad (= \text{const.})$$

**Using chosen higher order differences** In this section, we show that if we choose higher order differences, some higher order differential attacks of the CAST cipher with 5 rounds are possible where the order of the higher order differential is less than 16. Whether a higher order differential attack is possible when the order of the higher order differential is less than 16 depends on whether a higher order differential of $\tilde{y}_R(x)$ is independent of the key for the order of the higher order differential less than 16.

[When the order of the higher order differential is 15] Let us consider the 15-th order differential of $\tilde{y}_R(x)$. First, we prove the following lemma.

**Lemma 1.** *If we choose* $\{e_{14}, e_{13}, \ldots, e_0\}$ *for the* 15*-th order differences* $\{a_{15}, a_{14}, \ldots, a_1\}$*, each bit of the* 15*-th order differential of* $\tilde{y}_R(x)$ *is constant or linear with respect to a key bit. Note that* $e_i$ *is defined as:*

$$e_i = (0, \ldots, \overset{i}{\check{1}}, \ldots, 0) \in GF(2)^{32}.$$

*Proof.* The 15-th order differential of $\tilde{y}_R(x)$ for 15-th order differences $\{e_{14}, e_{13}, \ldots, e_0\}$ is the same as the 15-th order differential of $\tilde{y}_R(x)$ with respect to $\{x_{14}, x_{13}, \ldots, x_0\}$. Therefore, the 15-th order differential of $\tilde{y}_R(x)$ doesn't have the terms that don't include all variables of $\{x_{14}, x_{13}, \ldots, x_0\}$. All the terms of $\tilde{y}_R(x)$ that remain in the 15-th order differential are as follows;

$$\text{degree-15: } c_1(k)x_{14}x_{13}\cdots x_0 \qquad \text{and} \tag{3}$$

$$\text{degree-16: } c_2(k)x_{15}x_{14}\cdot\cdots\cdot x_0. \tag{4}$$

First, we show why the terms such as $c_3(k)x_{\mathbf{16}}x_{14}\cdots x_0$ don't remain. Let $X_1, X_2, X_3$, and $X_4$ be sets of variables as follows:

$$X_1 = \{x_{31}, x_{30}, \ldots, x_{24}\},$$
$$X_2 = \{x_{23}, x_{22}, \ldots, x_{16}\},$$
$$X_3 = \{x_{15}, x_{14}, \ldots, x_8\},$$
$$X_4 = \{x_7, x_6, \ldots, x_0\}.$$

The terms of degree 16 included in $\tilde{y}_R(x)$ is the product of four terms of degree 4 with respect to $X$ in the output of the 2-nd round function, $f(x+f(k^{(1)})+k^{(2)})$. The terms in the output of the 2-nd round function consist of terms with respect to only $X_1$, terms with respect to only $X_2$, terms with respect to only $X_3$, terms with respect to only $X_4$, and constant terms depending on $k$. Therefore, the terms of degree 16 that contain variables $x_{16} \subset X_2$, $\{x_{15}, \ldots, x_8\} \subset X_3$, and $\{x_7, \ldots, x_0\} \subset X_4$ don't remain in the 15-th order differential of $\tilde{y}_R(x)$ for 15-th order differences $\{e_{14}, e_{13}, \ldots, e_0\}$.

Second, consider the coefficient of the degree-15 term $c_1(k)x_{14}x_{13}\cdots x_0$ (Eq. (3)). We begin by considering the terms included in the output of the 2-nd round function. The output of the 2-nd round function includes the terms in the following, as one example, since the input of the 2-nd round function is

$x + f(k^{(1)}) + k^{(2)}$. Let $f_i : GF(2)^{32} \to GF(2)$ be the function which outputs the $i$-th bit of the output of $f$.

degree-4:

$$(x_3+f_3(k^{(1)})+k_3^{(2)})(x_2+f_2(k^{(1)})+k_2^{(2)})(x_1+f_1(k^{(1)})+k_1^{(2)})(x_0+f_0(k^{(1)})+k_0^{(2)}) \quad (5)$$

degree-3:

$$(x_2+f_2(k^{(1)})+k_2^{(2)})(x_1+f_1(k^{(1)})+k_1^{(2)})(x_0+f_0(k^{(1)})+k_0^{(2)}) \quad (6)$$

The coefficients of the terms of degree-4 with respect to $X$ included in the output of the 2-nd round function are 1, if they exist, since they come from terms such as Eq. (5). The coefficients of the terms of degree-3 with respect to $X$ are the sum of the coefficients of the terms expanded from terms such as Eq. (5) and terms such as Eq. (6). The coefficient from the former is linear with respect to a key bit, and the coefficient from the latter is 1. Since the terms of degree 15 with respect to $X$ included in $\tilde{y}_R(x)$ are the products of three terms of degree 4 and one term of degree 3 included in the output of the 2-nd round function, from the discussion above, the coefficients of the terms of degree 15 are represented as

$$\alpha_1 \times k_i + \alpha_0,$$

where $k_i$ is a key bit and $\alpha_1, \alpha_0 \in GF(2)$.

From similar considerations, the coefficients of the terms of degree 16 included in $\tilde{y}_R(x)$ are 0 or 1.

In conclusion, considering

- the coefficient of the degree-15 term $c_1(k)$ is $\alpha_1 k_i + \alpha_0$, where $\alpha_1, \alpha_0 \in GF(2)$, and
- the coefficient of the degree-16 term $c_2(k)$ is 0 or 1

which remain in the Boolean polynomial of each bit of $\Delta^{(15)}_{(e_{14},\ldots,e_0)}\tilde{y}_R(x)$, each bit of $\Delta^{(15)}_{(e_{14},\ldots,e_0)}\tilde{y}_R(x)$ is one of the following:

$$\{x_{15} + k_i + 1, x_{15} + k_i, x_{15} + 1, x_{15}, k_i + 1, k_i, 1, 0\}.$$

Moreover, when the degree-16 term $x_{15}x_{14}\cdots x_0$ exists, $\alpha_1$ is always 1, since the input of the 2-nd round function is $x + f(k^{(1)}) + k^{(2)}$. Therefore, each bit of $\Delta^{(15)}_{(e_{14},\ldots,e_0)}\tilde{y}_R(x)$ is one of the following:

$$\begin{cases} x_{15} + k_i + 1 \\ x_{15} + k_i \\ 1 \\ 0 \end{cases}. \quad (7)$$

This proves that if we choose $\{e_{14}, \ldots, e_0\}$ for the 15-th order differences, each bit of the 15-th order differential of $\tilde{y}_R(x)$ is constant or linear with respect to a key bit. □

From Eq. (7) in the proof of Lemma 1, the following corollary is proved.

**Table 1.** The number of constant bits of the 15-th order differential of $\tilde{y}_R(x)$ for some chosen differences

| differences | $\{E_1, E_2\} \setminus e_i$ | $\{E_1, E_3\} \setminus e_i$ | $\{E_1, E_4\} \setminus e_i$ |
|---|---|---|---|
| # of constant bits | 15 | 13 | 12 |
| differences | $\{E_2, E_3\} \setminus e_i$ | $\{E_2, E_4\} \setminus e_i$ | $\{E_3, E_4\} \setminus e_i$ |
| # of constant bits | 11 | 14 | 9 |

**Corollary 1.** *if we choose* $\{e_{14}, \ldots, e_0\}$ *for the* 15*-th order differences, some bits of the* 15*-th order differential of* $\tilde{y}_R(x)$ *are constant, and the XORed values of any two bits of the other bits are also constant.*

A similar corollary is proved for the following 15-th order differences $\{a_{15}, \ldots, a_1\}$.

$$\{a_{15}, \ldots, a_1\} = \left\{ \bigcup_{\text{Two sets of } E_1,\ E_2,\ E_3, \text{ and } E_4} \{E_1, E_2, E_3, E_4\} \right\} \setminus (\text{one of chosen } e_i\text{'s}) \quad (8)$$

where $E_1 = \{e_{31}, e_{30}, \ldots e_{24}\}$, $E_2 = \{e_{23}, e_{22}, \ldots e_{16}\}$, $E_3 = \{e_{15}, e_{14}, \ldots e_8\}$, $E_4 = \{e_7, e_6, \ldots e_0\}$, and "\" denotes the exclusion from the set.

**Experimental verification.** We computed the 15-th order differential of $\tilde{y}_R(x)$ for all 15-th order differences represented by Eq. (8) by computer experiments. Table 1 shows the number of constant bits in the 15-th order differential of $\tilde{y}_R(x)$. Note that $\{E_1, E_2\} \setminus e_i$ denotes the set $\{E_1, E_2\}$ excluding an arbitrary difference $e_i$ in $\{E_1, E_2\}$. The number of constant bits and the bit-positions don't depend on the excluded $e_i$. This is obvious from the fact that the constant doesn't depend on $x_i$.

[When the order of the higher order differential is 14] For the 14-th order differential of $\tilde{y}_R(x)$, it is shown that if we choose $\{e_{13}, e_{12}, \ldots, e_0\}$ for the 14-th order differences, each bit of the 14-th order differential of $\tilde{y}_R(x)$ is quadratic with respect to key bits. Table 2 shows that the degree with respect to the key of each bit of the 14-th order differential of $\tilde{y}_R(x)$ for some chosen differences. Note that the 14-th order differences $\{a_{14}, a_{13}, \ldots, a_1\}$ are chosen from $\{e_{31}, e_{30}, \ldots, e_{16}\}$. The column "differences" in Table 2 holds the XORed values $a_{14} + a_{13} + \cdots + a_1$. Table 2 shows that some bits of the 14-th order differential of $\tilde{y}_R(x)$ are constant, or independent of the key, a fact that is exploited in the improved higher order differential.

[When the order of the higher order differential is 13] For the 13-th order differential of $\tilde{y}_R(x)$, it is shown that if we choose $\{e_{12}, e_{11}, \ldots, e_0\}$ for the 13-th order differences, each bit of the 13-th order differential of $\tilde{y}_R(x)$ is degree

**Table 2.** The degree of each bit of the 14-th order differential of $\tilde{y}_R(x)$

| differences | bit position of the 14-th order differential of $\tilde{y}_R(x)$ 31302928272625242322212019181716151413121110987654321 0 |
|---|---|
| 11111111111111 00 | 1 2 2 2 2 2 2 2 2 2 0 0 1 2 2 2 1 2 0 1 2 2 1 1220110121 |
| 11111111111110 10 | 1 2 2 2 2 2 2 2 2 2 1 0 1 2 2 2 1 2 1 0 2 2 1 1220111122 |
| 11111111111101 10 | 1 2 2 2 2 2 2 2 2 2 0 0 1 2 2 2 1 2 1 1 2 2 1 1221011120 |
| 11111111111011 10 | 1 2 2 2 2 2 2 2 2 2 0 1 1 2 2 2 1 2 0 0 2 2 1 1220111121 |

**Table 3.** The bit-position of constant bits of the 13-th order differential of $\tilde{y}_R(x)$

| differences | bit position of the 13-th order differential of $\tilde{y}_R(x)$ 31302928272625242322212019181716151413121110987654321 0 |
|---|---|
| 11111111111110 00 | 0 |
| 11111111111000 11 | 0 |
| 11111100011111 11 | 0 0 |

3 or less with respect to key bits. Table 3 shows that the bit positions where the 13-th order differential of $\tilde{y}_R(x)$ is constant for some chosen differences. Note that the 13-th order differences $\{a_{13}, a_{11}, \ldots, a_1\}$ are chosen from 13 differences of $\{e_{31}, e_{30}, \ldots, e_{16}\}$. The column "differences" in Table 3 holds the XORed values $a_{13} + a_{12} + \cdots + a_1$. Similarly, Table 3 shows that some bits of the 13-th order differential of $\tilde{y}_R(x)$ are constant, or independent of the key, a fact that is exploited in the improved higher order differential.

### 4.2 Construct the attack equation and find the last round key $k^{(5)}$

In this section we construct attack equation (1) using the higher order differences found in Step 1 (Section 4.1), and find the last round key $k^{(5)}$. If we find the last round key $k^{(5)}$ by checking all possible $2^{32}$ candidates exhaustively as shown in [7], higher order differential attacks are possible where the 13-th order differences given in Section 4.1 are used. The required number of chosen p/c pairs is only $2^{13}$, and the required complexity is about $\frac{1}{2} \times 2^{13} \times 2^{32} = 2^{44}$ times the computation of round function on average (see new result (II) in Table 4).

If we find the last round key $k^{(5)}$ by solving attack equation (1) algebraically as shown in [13,11], the required complexity can be reduced, though the required number of chosen p/c pairs increases slightly. Hereafter, let $k^{(5)} = (k_{31}, k_{30}, \ldots, k_0)$ denote the last round key, and define the set of variables $K^{(5)}$ as $K^{(5)} = \{k_{31}, k_{30}, \ldots, k_0\}$. According to reference [11], the degree of attack equation (1) is 3 with respect to $K^{(5)}$ and we have to solve algebraic equations of degree 3 with 32 unknown variables. If we transform it to a system of linear equations regarding all monomials on $k^{(5)}$ in attack equation (1) as independent unknown variables, all variables in $K^{(5)}$ can be determined uniquely. The number of unknown variables is 368 [11, Section 4.2], and we have to prepare 368 equations.

**Table 4.** Required # of chosen p/c pairs and complexity for attacking a 5-round CAST

| Attacks | # of p/c pairs | complexity |
|---|---|---|
| Jakobsen & Knudsen [7] | $2^{17}$ | $2^{48}$ |
| Moriai, Shimoyama & Kaneko [11] | $2^{17}$ | $2^{25}$ |
| New result (I) | $2^{16}$ | $2^{24}$ |
| New result (II) | $2^{13}$ | $2^{44}$ |

If we use one of the 15-th order differences given in Section 4.1, we can obtain 32 equations (equations for 32 bits) using $2^{15}$ chosen p/c pairs. For the remaining $368 - 32 = 336$ equations, we can choose 15 different $2^{14}$ chosen p/c pairs from the same $2^{15}$ p/c pairs as above, but it seems difficult to prepare 336 equations according to Table 2. Therefore, we use arbitrary 16-th order differences and obtain 32 equations using $2^{16}$ chosen p/c pairs, and for the remaining 336 equations, we obtain them using some 15-th order differences given in Section 4.1, which we can choose from the $2^{16}$ p/c pairs above. In this case, the required number of chosen p/c pairs is only $2^{16}$, and the required complexity is less than $2^{24}$ times the computation of round function (see new result (I) in Table 4). Deriving the required complexity is explained in reference [11]. Table 4 shows new results on the number of p/c pairs and the complexity required for attacking a 5-round CAST cipher and compares them with previous results.

## 5 Conclusion

This paper introduced an improved higher order differential attack using chosen higher order differences. We demonstrated a higher order differential attack of a CAST cipher with 5 rounds using chosen higher order differences with fewer chosen p/c pairs and less complexity than the previous results. It is open whether the attack can be extended beyond 5 rounds. The target cipher is an example of a family of symmetric ciphers constructed using the CAST design procedure. CAST-128, which is used in several commercial applications, e.g., PGP5.0, has a stronger round function and more rounds, hence the improved higher order differential attack seems difficult to mount against CAST-128.

We're working on how to find the lowest order of the higher order differential, which will lead to provably security against higher order differential attacks.

## References

1. C.M.Adams, "Constructing Symmetric Ciphers Using the CAST Design Procedure," Designs, Codes and Cryptography, Volume 12, Number 3, November, pp.283–316, Kluwer Academic Publishers, 1997.
2. C.M.Adams, "The CAST-128 Encryption Algorithm," Request for Comments (RFC) 2144, Network Working Group, Internet Engineering Task Force, May, 1997.

3. C.M.Adams and S.E.Tavares, "Designing S-boxes for ciphers resistant to differential cryptanalysis," In Proceedings of the 3rd symposium on State and Progress of Research in Cryptography, pp.181–190, 1993.
4. E.Biham, "New Types of Cryptanalytic Attacks Using Related Keys," Advances in Cryptology – EUROCRYPT'93, Lecture Notes in Computer Science 765, pp.398–409, Springer-Verlag, 1994.
5. E.Biham and A.Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, Volume 4, Number 1, pp.3–72, Springer-Verlag, 1991.
6. H.M.Heys and S.E.Tavares, "On the security of the CAST encryption algorithm," Canadian Conference on Electrical and Computer Engineering, pp.332–335, 1994.
7. T.Jakobsen and L.R.Knudsen, "The Interpolation Attack on Block Ciphers," Fast Software Encryption, FSE'97, Lecture Notes in Computer Science 1267, pp.28–40, Springer-Verlag, 1997.
8. L.R.Knudsen, "Truncated and Higher Order Differentials," Fast Software Encryption – Second International Workshop, Lecture Note in Computer Science 1008, pp.196–211, Springer-Verlag, 1995.
9. X.Lai, "Higher Order Derivatives and Differential Cryptanalysis," Communications and Cryptography, pp.227–233, Kluwer Academic Publishers, 1994.
10. M.Matsui, "Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology – EUROCRYPT'93, Lecture Notes in Computer Science 765, pp.386–397, Springer-Verlag, 1994.
11. S.Moriai, T.Shimoyama, and T.Kaneko, "Higher Order Differential Attack of a CAST Cipher," Fast Software Encryption, FSE'98, Lecture Notes in Computer Science 1372, pp.17–31, Springer-Verlag, 1998.
12. K.Nyberg and L.R.Knudsen, "Provable Security Against a Differential Attack," Journal of Cryptology, Vol.8, No.1, pp.27–37, Springer-Verlag, 1995.
13. T.Shimoyama, S.Moriai, and T.Kaneko, "Improving the Higher Order Differential Attack and Cryptanalysis of the $\mathcal{KN}$ Cipher," Information Security, First International Workshop, ISW'97, Lecture Notes in Computer Science 1396, pp.32–42, Springer-Verlag, 1998.
14. H.Tanaka, K. Hisamatsu, and Toshinobu Kaneko, "Higher Order Differential Attack of MISTY without FL functions," Technical Report of IEICE, ISEC98-5, The Institute of Electronics, Information and Communication Engineers, 1998. (in Japanese)