Meet-in-the-Middle Technique for Truncated Differential and Its Applications to CLEFIA and Camellia

Leibo Li[1,3], Keting Jia[1], Xiaoyun Wang[2,3⋆], and Xiaoyang Dong[3]

[1] CCS, Department of Computer Science and Technology, Tsinghua University
ktjia@mail.tsinghua.edu.cn
[2] Institute for Advanced Study, Tsinghua University
xiaoyunwang@tsinghua.edu.cn
[3] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, China
{lileibo,dongxiaoyang}@mail.sdu.edu.cn

Abstract. As one of the generalizations of differential cryptanalysis, the truncated differential cryptanalysis has become a powerful toolkit to evaluate the security of block ciphers. In this article, taking advantage of the meet-in-the-middle like technique, we introduce a new method to construct truncated differential characteristic of block ciphers. Based on the method, we propose 10-round and 8-round truncated differential characteristics for CLEFIA and Camellia, respectively, which are ISO standard block ciphers. Applying the 10-round truncated differential characteristics for CLEFIA, we launch attacks on 14/14/15-round CLEFIA-128/192/256 with 2^{108}, 2^{135} and 2^{203} encryptions, respectively. For Camellia, we utilize the 8-round truncated differential to attack 11/12-round Camellia-128/192 including the FL/FL^{-1} and whiten layers with $2^{121.3}$ and $2^{185.3}$ encryptions. As far as we know, most of the cases are the best results of the attack on both ciphers.
Keywords: Block cipher, Cryptanalysis, Truncated Differential, CLEFIA, Camellia.

1 Introduction

Differential cryptanalysis is one of the principal attack methods on modern symmetric-key ciphers, which was firstly introduced by Biham and Shamir to analyze the block cipher DES in 1990 [5]. It exploits a differential trail ($\alpha \rightarrow \beta$) with high probability, where α is the input difference, and β is the output difference. Based on the differential attack, many methods have been developed to evaluate the security of block ciphers, such as the related-key differential attack [6,8,7], truncated differential attack [23], high-order differential attack [24], impossible differential attack [22,4], multiple differential attack [10] and so forth.

It is well known that the key point of the differential attack is to exploit the differential trial with high probability which covers as many rounds as possible. The traditional method is to find some short differential trials, and then connect these characteristics to form a long differential trial, such as the cryptanalysis of DES in [5]. Besides, evaluating the resistance of a block cipher against the differential attack has got a lot of attention from many cryptanalysts, which is usually carried out by calculating the minimum number of active S-boxes [12,1].

The truncated differential cryptanalysis was proposed by Knudsen in 1994 [23]. Different from the differential characteristic, the truncated differential includes a set of differential trails that have the same active S-boxes. Truncated differential attack has many similarities with differential attack, such as the method to construct the truncated differential, the complexity analysis and success rate evaluation.

Despite the fact that truncated differential cryptanalysis has been extensively employed, the tool to evaluate the security of block ciphers against the truncated differential cryptanalysis is worth further studying. Inspired by the impossible differential cryptanalysis, we introduce a new

⋆ Corresponding author

view to construct the truncated differential characteristic of block ciphers in this paper. In order to demonstrate the power of our method, we present its applications to the ISO standard block ciphers, CLEFIA and Camellia, and present the best results when compared with previous works. In detail, the contributions of our work are three-fold:

- **Meet-in-the-middle technique for truncated differential.** We split the encryption E into two parts and $E = E_1 \circ E_0$, and consider the truncated differentials $(\Gamma_0 \xrightarrow{E_0} \Gamma_1)$ and $(\Gamma_2 \xrightarrow{E_1^{-1}} \Gamma_1)$. If the truncated differential $\mathcal{P}_r(\Gamma_0 \xrightarrow{E_0} \Gamma_1) = p$, and $\mathcal{P}_r(\Gamma_2 \xrightarrow{E_1^{-1}} \Gamma_1) = 1$, we prove that the probability of the truncated differential $\mathcal{P}_r(\Gamma_0 \xrightarrow{E} \Gamma_2) = p \times |\Gamma_2|/|\Gamma_1|$ under the assumption of Markov cipher. The method is available to many block ciphers, especially, for Feistel structure ciphers.
- **Truncated differential cryptanalysis of CLEFIA.** CLEFIA was proposed by Sony Corporation in 2007 [44], and was selected as an international standard by ISO/IEC 29192-2 in 2011 [19] and e-Government recommended cipher by CRYPTREC project in 2013 [16]. The security of CLEFIA has attracted many attentions from worldwide cryptology researchers in previous years. Such as impossible differential cryptanalysis [13,49,48,38,46], improbable differential cryptanalysis [47,9], integral attack [31,41,50] and zero-correlation cryptanalysis [11]. In this paper, we apply the meet-in-the-middle technique to construct a 10-round truncated differential characteristic of CLEFIA. And then we launch the key recovery attacks on 13/14/15-round CLEFIA-128/192/256, which cost 2^{99} encryptions with 2^{99} chosen plaintexts for CLEFIA-128, 2^{135} encryptions with 2^{100} chosen plaintexts for CLEFIA-192, and 2^{203} encryptions with 2^{100} chosen plaintexts for CLEFIA-256. Furthermore, combined with the function reduction technique [20] and the subkey relations, we firstly achieve the attack on 14-round CLEFIA-128 with 2^{100} chosen plaintexts and 2^{108} encryptions.
- **Truncated differential cryptanalysis of Camellia.** Camellia was proposed by NTT and Mitsubishi in 2000 [2], and was selected as an e-government recommended cipher by CRYPTREC in 2002 [16], NESSIE block cipher portfolio in 2003 [40] and international standard by ISO/IEC 18033-3 in 2005 [18]. Many methods of cryptanalysis were applied to attack reduced-round Camellia in previous years, such as higher order differential attack [17], linear and differential attacks [43], truncated differential attack [45,26,21], collision attack [51], square attack [27,28], impossible differential attack [14,39,45,53,35,52,34,3,29,33,32], meet-in-the-middle attack [30,15,36,37], and zero-correlation linear cryptanalysis [11]. In this paper, combining the new observations of FL functions and meet-in-the-middle technique, we introduce an 8-round truncated differential of Camellia for 99.2% keys, and give the key recovery attacks on 11/12-round Camellia-128/192 with 2^{117} chosen plaintexts and $2^{121.3}$, $2^{185.3}$ encryptions, respectively. Both attacks are started from the first round and include the FL/FL^{-1} and whiten layers. Furthermore, using multiplied method proposed in [33], we extend the attacks to the full key space with 4 times of the time complexity.

Table 1 summarizes the major previously results of reduced-round CLEFIA and Camellia along with our results, where "†" means the attack works for 99.2% keys. The cryptanalysis results on Camellia start from the first round and include whitening keys and FL/FL^{-1} layers.

The rest of this paper is organized as follows. Section 2 gives some notations used in this paper and brief descriptions of CLEFIA and Camellia. We introduce the meet-in-the-middle technique to find the truncated differential for block ciphers in section 3. Section 4 presents the truncated differential cryptanalysis of round-reduced CLEFIA-128/192/256. The truncated differential attacks on 11/12-round Camellia-128/192 are given in section 5. Finally, we make a conclusion of the paper in section 6.

Table 1. Summary of the attacks on reduced-round CLEFIA and Camellia

Cipher	Rounds	Attack Type	Data	Time	Memory	Source
CLEFIA-128	12	Integral	2^{113}	$2^{116.7}$	N/A	[31]
	13	Impossible Diff	$2^{117.8}$	$2^{121.2}$	$2^{86.8}$	[38]
	13	Impossible Diff	$2^{116.16}$	$2^{114.58}$	$2^{83.16}$	[13]
	13	Truncated Diff	2^{99}	2^{99}	2^{80}	Section 4.2
	14	Truncated Diff	2^{100}	2^{108}	$2^{101.3}$	Section 4.4
CLEFIA-192	13	Impossible Diff	$2^{119.8}$	2^{146}	2^{120}	[48]
	13	Integral	2^{113}	$2^{180.5}$	N/A	[31]
	14	Multidim.ZC	$2^{127.5}$	$2^{180.2}$	2^{115}	[11]
	14	Truncated Diff	2^{100}	2^{135}	2^{131}	Section 4.3
CLEFIA-256	14	Impossible Diff	$2^{120.3}$	2^{212}	2^{121}	[48]
	14	Integral	2^{113}	$2^{244.5}$	N/A	[31]
	15	Multidim.ZC	$2^{127.5}$	$2^{244.2}$	2^{115}	[11]
	15	Truncated Diff	2^{100}	2^{203}	2^{139}	Section 4.5
Camellia-128	10	Impossible Diff	$2^{112.4}$	2^{120}	$2^{86.4}$	[33]
	11	ZC. FFT	$2^{125.3}$	$2^{124.8}$	2^{112}	[11]
	12	Impossible Diff	$2^{118.43}$	$2^{118.4}$	$2^{92.4}$	[13]
	11†	Truncated Diff	2^{117}	$2^{119.3}$	2^{119}	Section 5.2
	11	Truncated Diff	2^{117}	$2^{121.3}$	2^{119}	Section 5.2
Camellia-192	11	Impossible Diff	$2^{113.7}$	2^{184}	$2^{143.7}$	[33]
	12	ZC. FFT	$2^{125.7}$	$2^{188.8}$	2^{112}	[11]
	12	Meet-in-the-middle	2^{113}	2^{180}	2^{154}	[30]
	12	MITM	2^{113}CP	2^{180}	2^{158}	[54]
	12	Impossible Diff	$2^{119.7}$	$2^{161.06}$	$2^{150.7}$	[13]
	12†	Truncated Diff	2^{117}	$2^{183.3}$	2^{119}	Section 5.3
	12	Truncated Diff	2^{117}	$2^{185.3}$	2^{119}	Section 5.3

2 Preliminaries

This section lists some notations used throughout the paper, and presents brief descriptions of both block ciphers CLEFIA and Camellia.

2.1 Notations

The following notations are used in this paper:

$A_{r-1}, B_{r-1}, C_{r-1}, D_{r-1}$	the 4 input branches of the r-th round for CLEFIA
$L_{r-1},\ R_{r-1}$	the left and right 64-bit halves of the r-th round input for Camellia
$X^{[i]}$	the i-th byte of a bit string X, e.g., an $8l$-bit string $X = (X^{[0]}, \cdots, X^{[l-1]})$
$X^{\{i\}}$	the i-th bit of a bit string X, e.g., a l-bit string $X = X^{\{0\}} \| \cdots \| X^{\{l-1\}}$
Γ	a set of differences
E	the encryption or partial encryption of a block cipher
$M_0,\ M_1$	the Maximum Distance Separable (MDS) matrixes used by CLEFIA
$*$, 0, ?	' $*$ ' denotes the non-zero difference byte, '0' denotes the zero difference byte and '?' denotes the unknown byte
S_N	the signal-to-noise ratio
n_r	the number of rounds for a block cipher
$\mathcal{P}_r(X)$	the expected probability of the event X
ΔX	the difference of X and X'
$\oplus$, $\cap$, $\cup$	bitwise exclusive OR (XOR), AND, OR

$\|\Gamma\|$	the size of the set Γ
$x\|\|y$	bit string concatenation of x and y
$\lll l$	bit rotation to the left by l bits

2.2 Brief Description of CLEFIA

CLEFIA is a 128-bit block cipher with variable key lengths of 128, 192 and 256, which takes a 4-branch generalized Feistel network [44]. The number of rounds are 18/22/26 for CLEFIA-128/192/256, respectively. The procedure of encryption is described as follows.

A 128-bit plaintext P is split up into four 32-bit words P_0, P_1, P_2 and P_3. The input state of the first round $(A_0, B_0, C_0, D_0) = (P_0, P_1 \oplus kw_0, P_2, P_3 \oplus kw_1)$. For $r = 1$ to n_r, do the following steps:

$$A_r = B_{r-1} \oplus F_0(A_{r-1}, k_{2r-2}),\ B_r = C_{r-1},$$
$$C_r = D_{r-1} \oplus F_1(C_{r-1}, k_{2r-1}),\ D_r = A_{r-1}.$$

Finally, the 128-bit ciphertext C is computed as $C = (D_{n_r}, A_{n_r} \oplus kw_2, B_{n_r}, C_{n_r} \oplus kw_3)$.

The round function F_0 and F_1 take the SP structure (seen Fig. 1). There are two types of 8×8 S-boxes in substitution layer, and the order of s_0 and s_1 is different for both round functions. Specifically,

$$S_0(x_0, x_1, x_2, x_3) = (s_0(x_0), s_1(x_1), s_0(x_2), s_1(x_3)),$$
$$S_1(x_0, x_1, x_2, x_3) = (s_1(x_0), s_0(x_1), s_1(x_2), s_0(x_3)).$$

The diffusion layer uses two different Maximum Distance Separable (MDS) matrix, M_0 and M_1 in functions F_0 and F_1, respectively, and their branch number are both 5.

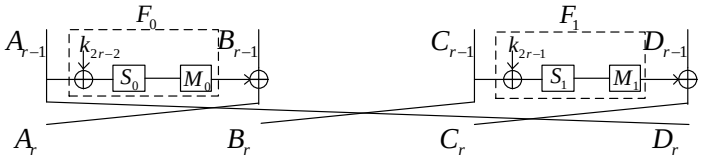

Fig. 1. The round function of CLEFIA

Key schedule. For 128-bit key size, a 128-bit intermediate key K_L is generated by the master key K and a 10-round 4-branch generalized Feistel network ($GFN_{4,10}$). Then K and K_L are used to generate the whitening key and round keys with a linear transformation. For 192 and 256 key sizes, two 128-bit values K_L and K_R are generated from the main key K. After that, a 10-round 8-branch generalized Feistel network ($GFN_{8,10}$) is applied on (K_L, K_R) to generate a 256-bit intermediate key (K_A, K_B). Then the whitening keys and the round keys are derived from (K_L, K_R, K_A, K_B) by some linear transformations. For more detailed description of CLEFIA, please refer to [44].

2.3 Brief Description of Camellia

Camellia is a 128-bit block cipher with variable key lengths of 128, 192 and 256, which takes a balanced Feistel network. The number of rounds are 18/24/24 for Camellia-128/192/256, respectively. For Camellia-128, the encryption procedure is as follows.

Firstly, a 128-bit plaintext is XORed with the whitening key (kw_0, kw_1) to get two 64-bit value L_0 and R_0. Then, for $r = 1$ to 18, except for $r = 6$ and 12, the following is carried out:

$$L_r = R_{r-1} \oplus F(L_{r-1}, k_{r-1}),\quad R_r = L_{r-1}.$$

For $r = 6$ and 12, do the following:

$$\begin{aligned} L'_r &= R_{r-1} \oplus F(L_{r-1}, k_{r-1}), \quad R'_r = L_{r-1}, \\ L_r &= FL(L'_r, kf_{r/3-2}), \qquad\quad R_r = FL^{-1}(R'_r, kf_{r/3-1}). \end{aligned}$$

Lastly, the 128-bit ciphertext is $(R_{18} \oplus kw_2, L_{18} \oplus kw_3)$.

The round function F is composed of a key-addition layer, a substitution transformation S and a diffusion layer P. There are four types of 8×8 S-boxes $s_1,\ s_2,\ s_3$ and s_4 in the S transformation layer, and a 64-bit data is substituted as follows:

$$S(x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7) = (s_0(x_0), s_1(x_1), s_2(x_2), s_3(x_3), s_1(x_4), s_2(x_5), s_3(x_6), s_0(x_7)).$$

The linear transformation $P : (\{0,1\}^8)^8 \to (\{0,1\}^8)^8$ maps $(y_0, \cdots, y_7) \to (z_0, \cdots, z_7)$, this transformation and its inverse P^{-1} are defined as follows:

$$\begin{aligned} z_0 &= y_0 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_7, & y_0 &= z_1 \oplus z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_7, \\ z_1 &= y_0 \oplus y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7, & y_1 &= z_0 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7, \\ z_2 &= y_0 \oplus y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7, & y_2 &= z_0 \oplus z_1 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_7, \\ z_3 &= y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6, & y_3 &= z_0 \oplus z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_6, \\ z_4 &= y_0 \oplus y_1 \oplus y_5 \oplus y_6 \oplus y_7, & y_4 &= z_0 \oplus z_1 \oplus z_4 \oplus z_6 \oplus z_7, \\ z_5 &= y_1 \oplus y_2 \oplus y_4 \oplus y_6 \oplus y_7, & y_5 &= z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_7, \\ z_6 &= y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_7, & y_6 &= z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6, \\ z_7 &= y_0 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6, & y_7 &= z_0 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_7. \end{aligned}$$

The FL function is defined as $(X_L \| X_R, kf_L \| kf_R) \mapsto (Y_L \| Y_R)$, where

$$Y_R = ((X_L \cap kf_L) \lll 1) \oplus X_R, \quad Y_L = (Y_R \cup kf_R) \oplus X_L.$$

Similar to Camellia-128, Camellia-192/256 have 24-round Feistel structure, where the FL/FL^{-1} function layer are inserted in the 6-th, 12-th and 18-th rounds. Before the first round and after the last round, there are pre- and post- whitening layers as well. For details of Camellia, we refer to [2].

3 Meet-in-the-Middle Technique for Truncated Differential

The key part of truncated differential attack is to find a high-probability truncated differential characteristic covering as many rounds as possible for a block cipher. Here we introduce an interesting approach by applying meet-in-the-middle like technique to find the truncated differential of block ciphers. We first recall the definition of truncated differential.

Definition 1. *[9] For the block cipher E with a parameter key K, the truncated differential characteristic $(\Gamma_{in} \xrightarrow{E} \Gamma_{out})$ is a set of differential trails, where Γ_{in} is a set of input differences, and Γ_{out} is a set of output differences. The expected probability of such truncated differential $(\Gamma_{in} \xrightarrow{E} \Gamma_{out})$ is defined by*

$$\begin{aligned} \mathcal{P}_r(\Gamma_{in} \xrightarrow{E} \Gamma_{out}) &= \frac{1}{|\Gamma_{in}|} \sum_{a \in \Gamma_{in}} \mathcal{P}_r((E_K(X) \oplus E_K(X \oplus a)) \in \Gamma_{out}) \\ &= \frac{1}{|\Gamma_{in}|} \sum_{a \in \Gamma_{in}} \mathcal{P}_r(a \to \Gamma_{out}). \end{aligned}$$

However, the average probability of the truncated differential characteristic for a random permutation is $\mathcal{P}_r(\Gamma_{in} \xrightarrow{E} \Gamma_{out}) = \frac{|\Gamma_{out}|}{2^n - 1}$, where n is the block size. When a truncated differential

characteristic with probability $\mathcal{P}_r(\Gamma_{in} \xrightarrow{E} \Gamma_{out}) = \frac{|\Gamma_{out}|}{2^n-1} + \varepsilon$ ($\varepsilon > 0$), it is used to identify the secret key.

Here, we assume that E is a Markov cipher [25], that means the probability of a differential trail is often computed by multiplying the probabilities round by round. We apply the meet-in-the-middle technique to find the truncated differential characteristic. The block cipher is divided into two parts, i.e., $E = E_1 \circ E_0$, and there is a truncated differential characteristic with probability 1 for E_1^{-1}, i.e., $\mathcal{P}_r(\Gamma_2 \xrightarrow{E_1^{-1}} \Gamma_1) = 1$, depicted in Fig. 2. Then we know

$$\mathcal{P}_r(\Gamma_0 \xrightarrow{E} \Gamma_2) = \mathcal{P}_r(\Gamma_0 \xrightarrow{E_0} \Gamma_1) \times \mathcal{P}_r(\Gamma_1 \xrightarrow{E_1} \Gamma_2). \tag{1}$$

In order to compute the probability $\mathcal{P}_r(\Gamma_1 \xrightarrow{E_1} \Gamma_2)$, we introduce the following assumption.

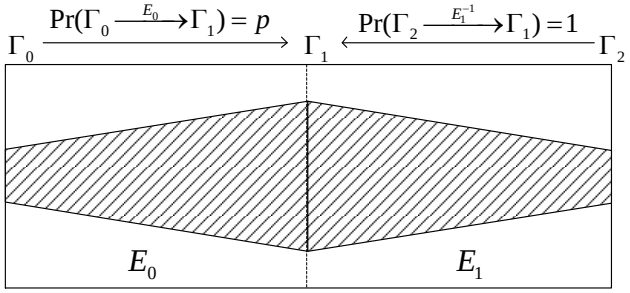

Fig. 2. Meet-in-the-Middle Technique for Truncated Differential

Assumption 1 *For the truncated differential $\Gamma_2 \xrightarrow{E_1^{-1}} \Gamma_1$ with high probability q, we assume that the expected probability of differential characteristic $\mathcal{P}_r(a \xrightarrow{E_1} b)$ are equal when E_1 is a Markov cipher for all $a \in \Gamma_1$, $b \in \Gamma_2$ with $a \neq 0$ and $b \neq 0$.*

Proposition 1. *Given a truncated differential $(\Gamma_2 \xrightarrow{E_1^{-1}} \Gamma_1)$ with probability 1, the expected probability of the truncated differential $(\Gamma_1 \xrightarrow{E_1} \Gamma_2)$ under Assumption 1 is*

$$\mathcal{P}_r(\Gamma_1 \xrightarrow{E_1} \Gamma_2) = \frac{|\Gamma_2|}{|\Gamma_1|},$$

where $|\Gamma_2| \leqslant |\Gamma_1|$.

Proof. Since $\mathcal{P}_r(\Gamma_2 \xrightarrow{E_1^{-1}} \Gamma_1) = 1$, then $\mathcal{P}_r(\Gamma_2 \xrightarrow{E_1^{-1}} b \notin \Gamma_1) = 0$. Equivalently,

$$\sum_{b \in \mathbb{F}_2^n \setminus \Gamma_1} \mathcal{P}_r(b \xrightarrow{E_1} \Gamma_2) = 0.$$

As a result,

$$\sum_{a \in \Gamma_1} \mathcal{P}_r(a \xrightarrow{E_1} \Gamma_2) = \sum_{a \in F_2^n} \mathcal{P}_r(a \xrightarrow{E_1} \Gamma_2) = |\Gamma_2|.$$

Therefore,

$$\mathcal{P}_r(\Gamma_1 \xrightarrow{E_1} \Gamma_2) = \frac{1}{|\Gamma_1|} \sum_{a \in \Gamma_1} \mathcal{P}_r(a \xrightarrow{E_1} \Gamma_2) = \frac{|\Gamma_2|}{|\Gamma_1|}.$$

Proposition 2. *For the block cipher $E = E_1 \circ E_0$, there are two truncated differential characteristics with high probability, i.e., $\mathcal{P}_r(\Gamma_0 \xrightarrow{E_0} \Gamma_1) = p$, and $\mathcal{P}_r(\Gamma_2 \xrightarrow{E_1^{-1}} \Gamma_1) = 1$, where Γ_0 is the input difference set of E, and Γ_1 and Γ_2 are the output difference sets of E_0 and E, respectively. Then the probability of the truncated differential $\Gamma_0 \xrightarrow{E} \Gamma_2$ is $p \times \frac{|\Gamma_2|}{|\Gamma_1|}$, where $|\Gamma_2| \leq |\Gamma_1|$.*

This proposition is easily obtained by the equation (1) and Proposition 1. It is obvious that when $\frac{p}{|\Gamma_1|} > 2^{-n}$, we can use Proposition 2 as distinguisher to recover the secret key. However, the impossible differential which exploits the differential characteristic of E_0 with probability zero, i.e., $\mathcal{P}_r(\Gamma_0 \xrightarrow{E_0} \Gamma_1) = 0$.

Proposition 3. *For the block cipher $E = E_1 \circ E_0$, there are two truncated differential characteristics with high probability, i.e., $\mathcal{P}_r(\Gamma_0 \xrightarrow{E_0} \Gamma_1) = p$, and $\mathcal{P}_r(\Gamma_2 \xrightarrow{E_1^{-1}} \Gamma_1) = q$. Then the probability of the truncated differential $\Gamma_0 \xrightarrow{E} \Gamma_2$ is larger than $pq \times \frac{|\Gamma_2|}{|\Gamma_1|}$, where $|\Gamma_2| \leq |\Gamma_1|$.*

This proposition is obviously deduced by Proposition 2. The truncated differential found by the meet-in-the-middle method may be also searched by the previous standard method, but this method is better for automation taking advantage of methods to find impossible differentials. Note that such feature could be discovered in many block ciphers, notably for Feistel structure block ciphers. We present the applications of our method to ISO standard block ciphers, CLEFIA and Camellia, for example.

4 Application to CLEFIA

In this section, we first construct a 10-round truncated differential of CLEFIA, then present the truncated differential cryptanalysis of reduced-round CLEFIA-128/192/256.

4.1 New Truncated Differentials of CLEFIA

Using the new method proposed in this paper, we introduce a 9-round truncated differential of CLEFIA, and then append one round to construct the 10-round truncated differential.

Proposition 4. *Let the input difference be $\Delta A_0 = \Delta C_0 = \Delta D_0 = (0,0,0,0)$ and $\Delta B_0 = (*,0,0,0)$, then after a 9-round encryption of CLEFIA, the probability of the output difference satisfying $\Delta B_9 = \Delta C_9 = \Delta D_9 = (0,0,0,0)$ and $\Delta A_9 = (*,0,0,0)$ is about 2^{-104}.*

Proof. As outlined in Fig. 3, we define the 9-round CLEFIA as E. The first five rounds of E is defined as E_0, the last four rounds as E_1. For the input differences

$$\Gamma_0 = (\Delta A_0, \Delta B_0, \Delta C_0, \Delta D_0) = (0,0,0,0,\ *,0,0,0,\ 0,0,0,0,\ 0,0,0,0),$$

the output differences after 5-round encryption satisfy

$$\Gamma_1 = (\Delta A_5, \Delta B_5, \Delta C_5, \Delta D_5) = (*,0,0,0,\ M_0(*,0,0,0) \oplus M_1(*,0,0,0),\ ?,?,?,?,\ ?,?,?,?)$$

with probability 2^{-24}. Similarly, for the differences

$$\Gamma_2 = (\Delta A_9, \Delta B_9, \Delta C_9, \Delta D_9) = (*,0,0,0,\ 0,0,0,0,\ 0,0,0,0,\ 0,0,0,0),$$

the corresponding output differences after 4-round decryption coincide to

$$\Gamma_1 = (\Delta A_5, \Delta B_5, \Delta C_5, \Delta D_5) = (*,0,0,0,\ M_0(*,0,0,0) \oplus M_1(*,0,0,0),\ ?,?,?,?,\ ?,?,?,?)$$

with probability 1.

Since $|\Gamma_1| = 2^{88}$, $|\Gamma_2| = 2^8$. Then, by the Proposition 2, the probability of truncated differential is

$$\mathcal{P}_r(\Gamma_0 \xrightarrow{E} \Gamma_2) = 2^{-24} \times 2^8 / 2^{88} = 2^{-104}.$$

□

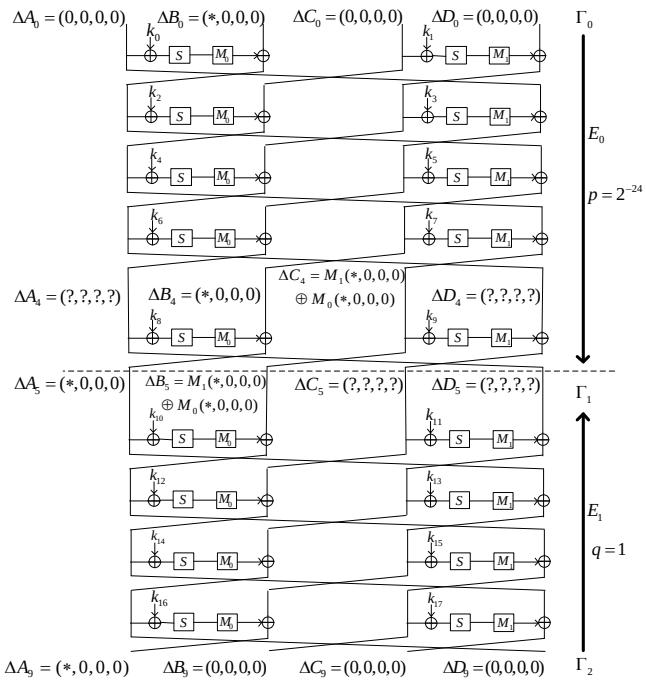

Fig. 3. The truncated differential of 9-round CLEFIA

Here, if we change the output difference ΔA_9 as $(0,*,0,0)$, $(0,0,*,0)$ or $(0,0,0,*)$, the probability $\mathcal{P}_r(\Gamma_0 \xrightarrow{E_1} \Gamma_1) = 0$. As introduced in [48], $(\Gamma_0 \xrightarrow{E} \Gamma_2)$ is an impossible differential. Similarly, if the difference $\Delta A_9 = \Delta B_0$ in Proposition 4, $(\Gamma_0 \xrightarrow{E} \Gamma_2)$ is also an impossible differential [44].

Proposition 5. *Let the input difference be* $\Delta A_0 = \Delta C_0 = \Delta D_0 = (0,0,0,0)$ *and* $\Delta B_0 = (*,0,0,0)$*, then after 10-round encryption of CLEFIA, the probability of the output difference satisfying* $\Delta A_{10} = M_0(*,0,0,0)$*,* $\Delta B_{10} = \Delta C_{10} = (0,0,0,0)$ *and* $\Delta D_{10} = (*,0,0,0)$ *is about* 2^{-104}*, which is greater than the uniform probability* 2^{-112}*.*

It is obviously for Proposition 5 that we append one round with probability 1 after 9-round truncated differential, and obtain the 10-round truncated differential.

Similarly, we get another 10-round truncated differential by swapping the values of ΔB_0 and ΔD_0, for example.

$$(0,0,0,0,\ 0,0,0,0,\ 0,0,0,0,\ *,0,0,0) \xrightarrow[2^{-104}]{\text{10 rounds}} (0,0,0,0,\ *,0,0,0\ M_0(*,0,0,0),\ 0,0,0,0).$$

4.2 The Truncated Differential Attack on 13-Round CLEFIA-128

Based on the 10-round truncated differential, we add one round on the top and two rounds on the bottom to attack 13-round CLEFIA-128 (see Fig. 4). We build a table T_1 to store 2^{16} differences $(M_0(b,0,0,0) \oplus M_1(a,0,0,0), a)$, where $a, b = 1, \ldots, 255$. The attack procedure is described as follows.

1. Choose 2^x structures of plaintexts, and each structure contains 2^{16} plaintexts with

$$A_0 = (x_0, x_1, x_2, x_3), \quad B_0 = (x_4, x_5, x_6, x_7),$$
$$C_0 = (\alpha_0, x_8, x_9, x_{10}), \quad D_0 = M_1(\alpha_1, x_{11}, x_{12}, x_{13}),$$

   where $x_i (i = 0, \ldots, 13)$ is constant, while $\alpha_j (j = 0, 1)$ takes all possible values. Ask for the encryption of the plaintexts for each structure, and store them in a hash table H indexed by

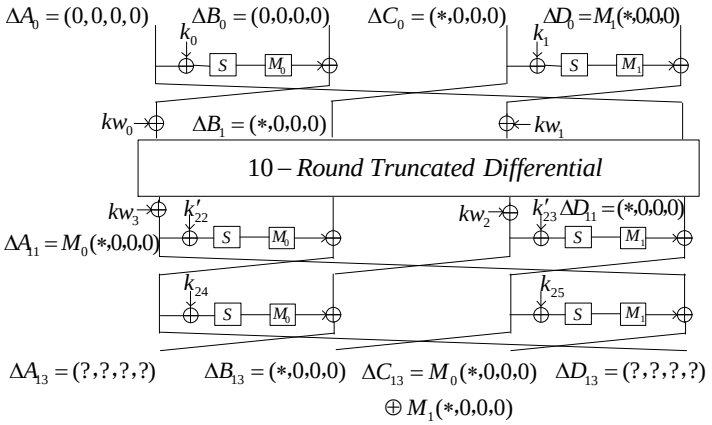

Fig. 4. The truncated differential attack on 13-round CLEFIA-128

$B_{13}^{[1,2,3]}$. There are $2^{31+x} \times 2^{-24} = 2^{7+x}$ pairs on average which make $\Delta B_{13} = (*, 0, 0, 0)$. And then eliminate the pairs whose differences ΔC_{13} are not in T_1. There are about $2^{7+x} \times 2^{-16} = 2^{-9+x}$ pairs left.

2. Guess 24-bit subkey $k_{25}^{[1,2,3]}$, do the following substeps for every pair.
   (a) In the first round, deduce 8-bit subkey $k_1^{[0]}$ by the input and output differences of S-box.
   (b) In the 13-th round, get 32-bit subkey k_{24} by the input and output differences of S-boxes.
   (c) Deduce the subkey $k_{25}^{[0]}$, where the value of difference $M_1^{-1}(\Delta A_{11} \oplus \Delta C_{13})^{[0]}$ could be determined by the value of ΔC_{13}.
   (d) Compute A_{11} by partial encryption deduce the subkey k'_{22}, where $k'_{22} = k_{22} \oplus kw_3$, and increase the corresponding counter of 80-bit subkey $(k_1^{[0]}, k'_{22}, k_{24}, k_{25}^{[0]})$ by 1.
3. Choose the subkey whose count is the largest as the candidate of right key, then exhaustively search the rest unknown bits to obtain the master key.

Complexity analysis. If we choose $x = 83$, the expected count of the right key is $\mu = 2^{x+31-8-104} = 4$. In step 1, we need $2^{x+16} = 2^{99}$ chosen plaintexts, which cost 2^{99} encryptions. The time complexity of step 2 is about $2^{x-9+24} \times 2/13 = 2^{95.3}$ encryptions. The memory complexity of the attack is about 2^{80} which is used to store key counters. By key schedule, we know the 72 subkeys $(k_{24}, k_{25}, k_1^{[}0])$ only depend on K_L. Then step 3 needs $2^{128-72+24} = 2^{80}$ encryptions to find the right key. Therefore, the time complexity is about 2^{99} encryptions. According to the definition of signal-to-noise ratio proposed in [5], the signal-to-noise ratio S_N is $2^{-104} \times 2^{-112} = 2^8$. According to [42], the success probability is

$$Ps = \int_{-\frac{\sqrt{\mu S_N} - \Phi^{-1}(1-2^{-a})}{\sqrt{S_N+1}}}^{\infty} \Phi(x)dx = 0.91,$$

where $a = 80$, for we choose the subkey with the largest count as the right key.

4.3 The Truncated Differential Attack on 14-Round CLEFIA-192

In this subsection, we give a truncated differential attack on 14-round CLEFIA-192 by prefixing one round on the top of the 13-round attack, illustrated in Fig. 6. In order to reduce the time complexity, we apply the partial function reduction technique proposed in [20].

Partial function reduction technique. The partial function reduction technique is firstly proposed by Isobe and Shibutani at Asiacrypt 2013, which is used to reduce the guessed key involved

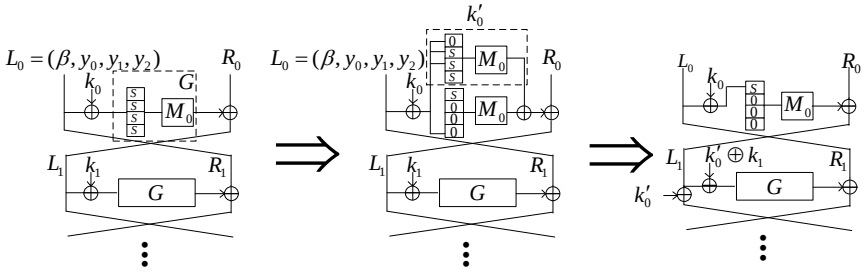

Fig. 5. Partial function reduction technique

in the attack for Feistel structure ciphers, of which the round function is composed of a S-box layer and a linear layer, such as Camellia and CLEFIA. For a group of chosen plaintexts, assume the left value is $L_0 = (\beta, y_0, y_1, y_2)$, where $y_i (i = 0, 1, 2)$ are fixed values and β is a variable. Since

$$\begin{aligned} &M_0(s(k_0^{[0]} \oplus \beta), s(k_0^{[1]} \oplus y_0), s(k_0^{[2]} \oplus y_1), s(k_0^{[2]} \oplus y_2) \\ &= M_0(0, s(k_0^{[1]} \oplus y_0), s(k_0^{[2]} \oplus y_1), s(k_0^{[3]} \oplus y_2)) \oplus M_0(s(k_0^{[0]} \oplus \beta), 0, 0, 0), \end{aligned}$$

then $k_0^{[1,2,3]}$ is treated as an equivalent key k_0', i.e.,$k_0' = M_0(0, s(k_0^{[1]} \oplus y_0), s(k_0^{[2]} \oplus y_1), s(k_0^{[3]} \oplus y_2)$. As a result, only 40 bits of the 64-bit subkey (k_0, k_1) are involved in the key recovery attack, equivalent to $(k_0^{[0]}, k_0' \oplus k_1)$ (see Fig. 5).

The Attack on 14-Round CLEFIA-192. Utilizing the partial function reduction technique, we mount a 14-round attack by adding one round on the top of the 13-round attack. As illustrated in Fig. 6, we choose 2^x structures of plaintexts, and each structure contains 2^{48} plaintexts with

$$\begin{aligned} &A_0 = M_1(\alpha_0, x_0, x_1, x_2), \ B_0 = (\alpha_1, \alpha_2, \alpha_3, \alpha_4), \\ &C_0 = (x_3, y_0, y_1, y_2), \qquad D_0 = (\alpha_5, x_4, x_5, x_6), \end{aligned}$$

where x_i and y_j are fixed values, α_i takes all possible values. In order to reduce the number of guessed subkey, let $y_j (j = 0, 1, 2)$ be constants for all structures, and then there are 2^{56} structures to be collected at most. According to partial function reduction technique, the equivalent key $k_1' = M_1(0, s_0(k_1^{[1]} \oplus y_0), s_1(k_0^{[2]} \oplus y_1), s_0(k_0^{[3]} \oplus y_2))$, and k_1' are equal for all structures. On the basic of this view, the attack on 14-round CLEFIA-192 is described as follows.

1. Ask for the encryption of the plaintexts for each structure, and store them in a hash table H indexed by $B_{14}^{[1,2,3]}$. There are $2^{95+x} \times 2^{-24} = 2^{71+x}$ pairs on average which make $\Delta B_{14} = (*, 0, 0, 0)$.
2. Eliminate the pairs whose differences ΔC_{14} do not conform to $M_0(*, 0, 0, 0) \oplus M_1(*, 0, 0, 0)$. There are about $2^{71+x} \times 2^{-16} = 2^{55+x}$ pairs left after this step.
3. Guess 8-bit subkey $k_1^{[0]}$, compute the difference ΔC_1 for every pair, then do the following substeps.
   (a) For a pair, compute 32-bit subkey k_0 by the input and output differences of S-boxes in the first round.
   (b) Deduce the input values C_1 by partial encryption, and get 8-bit equivalent key $(k_3' \oplus k_1')^{[0]}$ by the input and output differences of S-box, where k_3' is $k_3 \oplus kw_1$.
   (c) In the 14-th round, compute the 32-bit subkey k_{26} by the input and output difference of S-boxes.
   (d) Get the output difference of S-box by lookup table T_1 with ΔC_{14}, and then deduce 8-bit subkey $k_{27}^{[0]}$.

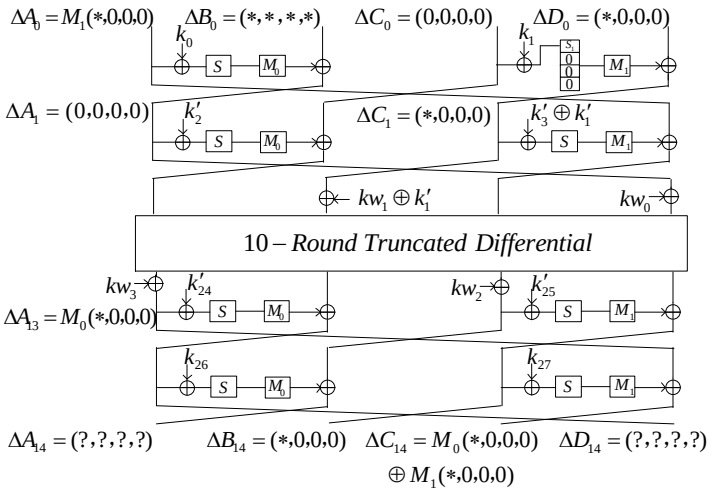

Fig. 6. The attack on 14-round CLEFIA-192

(e) Guess 24-bit subkey $k_{27}^{[1,2,3]}$ to deduce 32-bit subkey k'_{24}, where k'_{24} is $k_{24} \oplus kw_3$ by partial decryption.
(f) Increase the corresponding counter of 136-bit subkey $(k_0, (k'_3 \oplus k'_1)^{[0]}, k'_{24}, k_{26}, k_{27})$ by 1.
(g) Choose the subkey whose counter is the largest as the candidate of the right key, then verify whether it is the master key by exhaustive search. If not, try the next guess of $k_1^{[0]}$.

Complexity analysis. If we choose $x = 52$, the expected counter of the right key is $\mu = 2^{x+95-40} \times 2^{-104} = 8$, then the success probability is about 0.97. The data complexity of the attack is $2^{52+48} = 2^{100}$ chosen plaintexts. The time complexity of the attack is dominated by the Step 3. (e), which is equivalent to $2^{52+55+32} \times 2^{-4} = 2^{135}$ 14-round encryptions. The memory complexity of the attack is about $2^{52+55+24} = 2^{131}$ 136-bit words since the counters could be reused for every guess of $k_1^{[0]}$.

4.4 The Truncated Differential Attack on 14-Round CLEFIA-128

Considering the subkey relations, the 14-round attack could also be applied to CLEFIA-128. By the key schedule, we know the subkey $(k_0, k_1^{[0]}, k_{26}, k_{27})$ is determined by the following information:

$$\begin{array}{ll} k_0 : K_L^{\{0\sim31\}}, & k_{26} : K_L^{\{35\sim41\}} \| K_L^{\{28\sim34\}} \| K_L^{\{21\sim27\}} \| K_L^{\{14\sim20\}} \| K_L^{\{7\sim10\}}, \\ k_1^{[0]} : K_L^{\{32\sim39\}}, & k_{27} : K_L^{\{11\sim13\}} \| K_L^{\{0\sim6\}} \| K_L^{\{64\sim85\}}. \end{array}$$

It is obvious that there are 40 bits redundance, and the key involved in the attack is only 104 bits. The attack procedure is similar to the attack of 14-round CLEFIA-192.

1. Collect $2^{48+52} = 2^{100}$ plaintexts, then encrypt them and store the plaintext-ciphertext pairs in a table.
2. For every possible values of $k_{27}^{[0]}$, do the following substeps.
   (a) For each structure, compute the value $X = M_0^{-1}(M_1(s_1(B_{14}^{[0]} \oplus k_{27}^{[0]}), 0, 0, 0) \oplus C_{14})$, then restore the plaintext-ciphertext pairs indexed by 48-bit value $(B_{14}^{[1,2,3]}, X^{[1,2,3]})$. Thus, we can collect about $2^{52} \times 2^{95} \times 2^{-48} = 2^{99}$ pairs for each $k_{27}^{[0]}$, and each pair satisfies that $\Delta B_{14} = (*, 0, 0, 0)$ and ΔC_{14} belongs to the set $M_0(*, 0, 0, 0) \oplus M_1(*, 0, 0, 0)$.
   (b) Deduce 64-bit subkey (k_0, k_{26}) by partial encryption and decryption. Since these 72-bit subkey $(k_0, k_{26}, k_{27}^{[0]})$ only takes 42-bit information, then we filter more wrong pairs. There are about $2^{99} \times 2^{-30} = 2^{69}$ pairs remaining.

(c) For every pair, deduce 8-bit equivalent key $(k'_3 \oplus k'_1)^{[0]}$, where 8-bit information of subkey $k_1^{[0]}$ have been deduced in the above step.
(d) By subkey relations, guess 22-bit value $K_L^{\{64\sim85\}}$ instead of subkey $k_{27}^{[1,2,3]}$ to deduce 32-bit subkey k'_{24}.
(e) Increase the corresponding counter of 104-bit information of subkey by 1.

3. After operations of all possible $k_{27}^{[0]}$, choose the subkey whose counter is the largest as the candidate of right key, and exhaustively search to obtain the master key.

Complexity analysis. The data complexity of the attack is $2^{52+48} = 2^{100}$ chosen plaintexts. The time complexity of the attack is dominated by the Step 2. (a) and (b), which is equivalent to $2^{100} \times 2^8 = 2^{108}$ 14-round encryptions. The memory complexity of the attack is dominated by Step 1 and Step 2. (e) which is about $2^{100} \times 2 + 2^{99} = 2^{101.3}$ 128-bit words.

4.5 The Truncated Differential Attack on 15-Round CLEFIA-256

The attack on 15-round CLEFIA-256 is constructed by appending one round at the bottom of the 14-round attack. The attack procedure is similar to 14-round attack. We first choose 2^{52} structures of plaintexts and obtain the corresponding ciphertexts. Guess the subkey of last round function (k_{28}, k_{29}), then decrypt the ciphertexts to get the intermediate value $(A_{14}, B_{14}, C_{14}, D_{14})$ and store them in a hash table H indexed by $B_{14}^{[1,2,3]}$. For the collected pairs, filter the pairs whose differences ΔC_{14} don't belong to the set $M_0(*, 0, 0, 0) \oplus M_1(*, 0, 0, 0)$. After that, the number of remaining pairs is about 2^{107}. Then as described in the 14-round attack, we can obtain 2^{32} values of 144-bit subkey for each pair. Then choose the subkey whose counter is the largest under every 64-bit key guess, and verify whether it is the correct key. If not, try to the next key guess of (k_{28}, k_{29}). The data complexity of the attack is $2^{52+48} = 2^{100}$ chosen plaintexts. The time complexity of the attack is equivalent to $2^{107} \times 2^{64} \times 2^{32} = 2^{203}$ 15-round encryptions. The memory complexity of the attack is about 2^{139} 144-bit words.

5 Application to Camellia

In this section, we propose a 8-round truncated differential of Camellia, based on which, we introduce the truncated differential attack on reduced-round Camellia-128/192.

5.1 The Truncated Differential of Camellia

We first introduce a 7-round differential of Camellia for 99.2% keys, based on which we give an 8-round truncated differential by appending one round at the bottom. The new differential is based on two interesting observations of FL function.

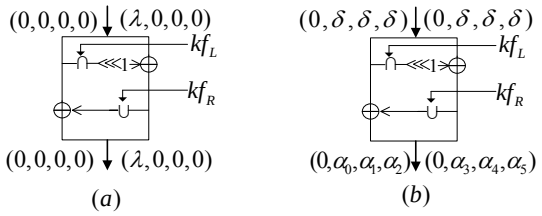

Fig. 7. Observations of FL function

Observation 1 *Let the input difference of FL function be $(0,0,0,0,\lambda,0,0,0)$, where $\lambda = 2^{7-i}, i = 0,1,\ldots,7$. If the corresponding bit of inserted key $kf_R^{\{i\}} = 1$, then the output difference must be $(0,0,0,0,\lambda,0,0,0)$.*

For 8 values of λ whose hamming weight is 1, there are $2^{32} - 2^{24}$ values for kf_R (the hamming weight of $kf_R^{[0]}$ is not zero) keeping the output difference $(0,0,0,0,\lambda,0,0,0)$, which takes a fraction of $(1 - 2^{-8})$. The observation is available to FL^{-1} function.

Observation 2 *There are about 99.6% values of (kf_L, kf_R) satisfying that if the input difference of FL function is $(0,\delta,\delta,\delta,0,\delta,\delta,\delta)$, then the probability that the output difference is $(0,\alpha_0,\alpha_1,\alpha_2,0,\alpha_3,\alpha_4,\alpha_5)$ is greater than 2^{-2}, where $\delta \neq 0$, $\alpha_i \neq 0$, and there exist at least a pair of (α_i,α_j) with $\alpha_i \neq \alpha_j$, $i,j = 0,1,\ldots,5, i \neq j$.*

We verify this observation by experiment on a PC. For a given key (kf_L, kf_R), we compute the output difference by traversing all the values of δ, and keep the δ which makes the output difference satisfying Observation 2. Let $S_\delta = \{\delta | (0,\alpha_0,\alpha_1,\alpha_2,0,\alpha_3,\alpha_4,\alpha_5) = FL(0,\delta,\delta,\delta,0,\delta,\delta,\delta), \alpha_i \neq 0, \exists 0 \leq i < j \leq 5, s.t. \alpha_i \neq \alpha_j\}$. Let $N_\delta = |S_\delta|$ be the set size. When $N_\delta > 64$, we denote the key as a weak key, vice versa. In our experiment, we choose 2^{32} values of (kf_L, kf_R) randomly, and exhaustive 255 values of input difference for each key to get the statistical result. On average, there are about 2^{24} values of (kf_L, kf_R) are not weak key. That means the fraction of weak key space is about $(1 - 2^{-8}) \approx 0.996$. In the following, we denote the full key space of FL function as K_{fl}, and the weak key space as $\widehat{K_{fl}}$. For the attacker, it is easy to obtain all the values of $\widehat{K_{fl}}$ by exhaustive search, the complexity is 2^{64} simple computations.

However, we list some examples of key which are not content with Observation 2. For instance, the key $kf_L^{\{i\}} = 0$, $kf_R^{\{i\}} = 1$ $(i = 0 \sim 31)$, since the output difference would be $(0,\delta,\delta,\delta,0,\delta,\delta,\delta)$ with probability 1 for any nonzero value δ in such case.

Based on the two Observations, we build a 7-round differential for Camellia.

Proposition 6. *Given the 7-round Camellia encryption with a FL/FL^{-1} layer inserted between the fifth and sixth round, if the input differences of first round are $(0,0,0,0,0,0,0,0,\ 0,0,0,0,\lambda,0,0,0)$ and the output differences of 7-th round are $(0,0,0,0,\lambda,0,0,0,\ \ 0,0,0,0,0,0,0,0)$, then the 7-round differential holds with probability 2^{-114} for 99.2% fraction of the full key space, where $\lambda = 2^i, i = 0,1,\ldots,7$.*

Proof. We divide the 7-round Camellia into two parts $E = E_1 \circ E_0$, where the first 4 rounds of E are denoted as E_0, and the last 3 rounds of E as E_1, illustrated in Fig. 8. Let the output differences of E be

$$\Gamma_2 = (0,0,0,0,\lambda,0,0,0,0,0,0,0,0,0,0,0),$$

where $\lambda = 0x80$. By Observation 1, we know $\Delta L_5' = (0,0,0,0,\lambda,0,0,0)$ when $kf_{0R}^{\{0\}} = 1$. By partial decryption, we get $\Delta R_5 = (0,\delta,\delta,\delta,0,\delta,\delta,\delta)$. By Observation 2, we know the output differences set S_δ with the size $N_\delta > 64$ hold with probability larger than 2^{-2} for a given weak key kf_1. Let $\Delta R_5' = S_\delta$.

Then the output differences of E_1^{-1} are

$$\Gamma_1 = (\Delta R_5',\ P(0,*,*,*,0,*,*,*) \oplus (0,0,0,0,\lambda,0,0,0)),$$

where there are N_δ values for $\Delta R_5'$. It is obviously $Pr(\Gamma_2 \xrightarrow{E_1^{-1}} \Gamma_1) = 2^{-2}$.

Let the input difference of E be $\Gamma_0 = (0,0,0,0,0,0,0,0,\ \ 0,0,0,0,\lambda,0,0,0)$, and the output difference after E_0 be Γ_1. We know the probability $Pr(\Gamma_0 \xrightarrow{E_0} \Gamma_1) = N_\delta \times 2^{-64}$.

Since $|\Gamma_1| = 2^{48} \times N_\delta$, $|\Gamma_2| = 1$, the probability of the 7-round differential is

$$\mathcal{P}_r(\Gamma_0 \xrightarrow{E} \Gamma_2) = 2^{-2} \times 2^{-64} \times N_\delta / (2^{48} \times N_\delta) = 2^{-114}.$$

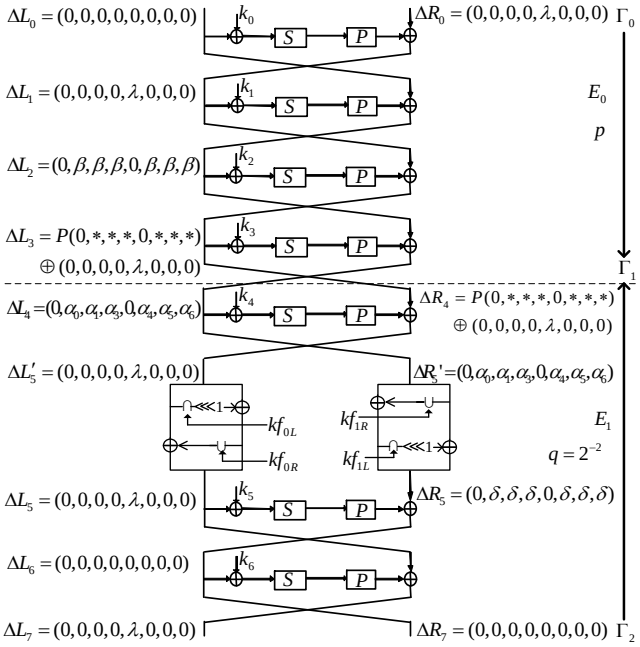

Fig. 8. Difference characteristic of 7-round Camellia

according to Proposition 3.

Considering the FL/FL^{-1} functions, the 7-round differential holds only for the weak key (kf_0, kf_1) by Observation 1 and 2.

Similarly, the 7-round differentials of Camellia also hold with probability 2^{-114}, when $\lambda = 2^i, i = 0, 1, \ldots, 6$. Since the independent of the subkey kf_0 and kf_1, all the 8 7-round differentials of Camellia cover the key space is about $(1 - 2^{-8}) \times (1 - 2^{-8}) = 1 - 2^{-7} = 99.2\%$.

□

Proposition 7. *Given the 8-round Camellia encryption with a FL/FL^{-1} layer inserted between the fifth and sixth round, if the input differences of first round are* $(0,0,0,0,0,0,0,0,\ 0,0,0,0,\lambda,0,0,0)$ *and the output differences of 8-th round are* $(0,\eta,\eta,\eta,0,\eta,\eta,\eta,0,0,0,0,\lambda,0,0,0)$*, then the 8-round differential holds with probability* 2^{-114} *for a fraction of* $(1 - 2^{-7})$ *full key space, where* $\lambda = 2^i, i = 0, 1, \ldots, 7$*.*

Proof. On the basic of 7-round differential, we append one round after it with probability 1 and obtain the 8-round truncated differential. It is noted that the uniform probability of such truncated differential characteristic is 2^{-120}, which is smaller than 2^{-114}. □

Similarly, there are three other 8-round truncated differentials in the following.

$$(0,0,0,0,0,0,0,0,\ 0,0,0,0,0,\lambda,0,0) \xrightarrow[2^{-114}]{8\text{ ounds}} (\eta,0,\eta,\eta,\eta,0,\eta,\eta,0,0,0,0,0,\lambda,0,0),$$
$$(0,0,0,0,0,0,0,0,\ 0,0,0,0,0,0,\lambda,0) \xrightarrow[2^{-114}]{8\text{ ounds}} (\eta,\eta,0,\eta,\eta,\eta,0,\eta,0,0,0,0,0,0,\lambda,0),$$
$$(0,0,0,0,0,0,0,0,\ 0,0,0,0,0,0,0,\lambda) \xrightarrow[2^{-114}]{8\text{ ounds}} (\eta,\eta,\eta,0,\eta,\eta,\eta,0,0,0,0,0,0,0,0,\lambda).$$

5.2 The Truncated Differential Attack on 11-Round Camellia-128

We first give an attack on 11-round Camellia-128 for weak key space, where we assume that the inserted key of FL/FL^{-1} layer (kf_1, kf_2) are weak key which takes a fraction of 99.2%. Then

we present the attack on the full key space by multiplied method given in [33]. The attack is mounted by adding one round on the top and two rounds on the bottom of the 8-round differential characteristic (see Fig. 9). The attack procedure is as follows.

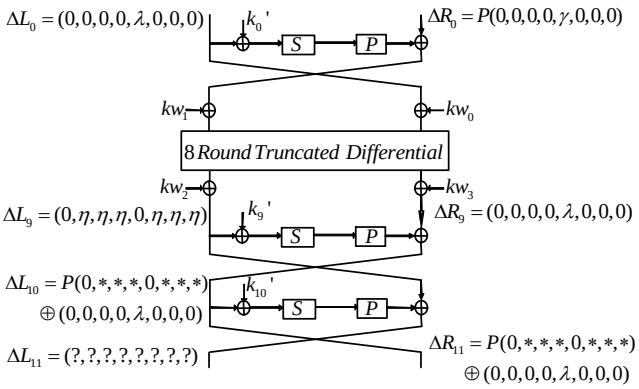

Fig. 9. The attack on 11-round Camellia-128

1. Choose 2^n structures of plaintexts, and each structure contains 2^{16} plaintexts

$$(L_0, R_0) = (x_0, x_1, x_2, x_3, \alpha_0, x_4, x_5, x_6, P(x_7, x_8, x_9, x_{10}, \alpha_1, x_{11}, x_{12}, x_{13})),$$

   where $x_i (i = 1, \ldots, 13)$ are fixed values in each structure, while $\alpha_i (i = 1, 2)$ take all the possible values.
2. Ask for the encryption of these plaintexts and store them in a table.
3. For $i = 32 \sim 39$, do the following substeps.
   (a) Restore 2^{n+16} plaintext-ciphertext pairs in a hash table H which is indexed by 15-bit value of ciphertext $(P^{-1}(R_{11})^{[0]}, P^{-1}(R_{11})^{\{32\sim(i-1),(i+1)\sim 39\}})$. By birthday paradox, we get $2^{n+31} \times 2^{-15} = 2^{n+16}$ pairs whose differences satisfy $P^{-1}(\Delta R_{11}) = (0,*,*,*,0,*,*,*) \oplus P^{-1}(0,0,0,0,\lambda,0,0,0)$, where "$\lambda$" denotes the nonzero differences with $\lambda^{\{j\}} = 0$ $(j \neq i-32)$.
   (b) Delete the pairs whose differences don't satisfy $\Delta L_0^{\{32\sim(i-1),(i+1)\sim 39\}} \neq 0$. Then number of remaining pairs is about 2^{n+9}. After that, all pairs satisfy $(\Delta L_0, \Delta R_0) = (0,0,0,0,\lambda,0,0,0, P(0,0,0,0,\gamma,0,0,0))$ and $\Delta R_{11} = P(0,*,*,*,0,*,*,*) \oplus (0,0,0,0,\lambda,0,0,0)$.
   (c) For each pair, deduce the equivalent key $k_0'^{[4]}$, where $k_0' = k_0 \oplus kw_0$.
   (d) For 2^8 possible values of η, do the following substeps.
      i. Deduce the equivalent key k_{10}', where $k_{10}' = k_{10} \oplus kw_3$.
      ii. Deduce the equivalent key $k_9'^{[1,2,3,5,6,7]}$, where $k_9' = k_9 \oplus kw_2$.
   (e) Increase the corresponding counter of 120-bit information of subkey by 1.
   (f) After computations of all proper pairs, choose the subkey whose counter is the largest as the candidate of right key, and verify it by trivial test. If succeed, output the right key; otherwise, another value of i should be tried. It is noted that if $kf_{0R}^{\{i-32\}} = 1$, the attack should succeed for such i.

Complexity analysis. If we choose $n = 101$, the expected counter of the right key is $\mu = 4$, and then the success probability is about 0.91. The data complexity of the attack is $2^{101+16} = 2^{117}$ chosen plaintexts. Step 2 needs about 2^{117} 11-round encryptions, which also needs 2^{118} 128-bit words to store all plaintext-ciphertext pairs. The time complexity of step 3 is equivalent to $2^3 \times 2^{118} \times 2^{-2} = 2^{119}$ 11-round encryptions. The memory requirement of step 3 is about 2^{118}

120-bit words since all counters could be reused for each value of i. In total, the time complexity of the attack is about $2^{119.3}$ 11-round encryptions and the memory complexity is about 2^{119}.

The attack for the full key space. For above attack, if the target key satisfies that (kf_{1L}, kf_{1R}) belongs to $\widehat{K_{fl}}$ and at least one bit of $kf_{0R}^{[0]}$ is 1, the attack would succeed. If failed, we conclude that $(kf_{1L}, kf_{1R}) \in K_{fl}/\widehat{K_{fl}}$ or $kf_{0R}^{[0]} = 0$. Thus, using this information, the attack could be extended to the full key space by multiplied method, which is as follows.

- **Phase 1.** Try to perform above truncated differential attack for weak key space. If success, obtain the correct key. Otherwise perform the next phase.
- **Phase 2.** Search the key set $K_{fl}/\widehat{K_{fl}}$. There are about 2^{56} values of (kf_{1L}, kf_{1R}) belong to this set. Then exhaustively search to get the master key. The time complexity of this step is about 2^{120}. If failed, perform the next phase.
- **Phase 3.** Announce the subkey $kf_{0R}^{[0]} = 0$, then exhaustively search for the remaining 120-bit value to obtain the master key.

The time complexity of the whole attack is about $2^{119.3} + 2^{120} + 2^{120} = 2^{121.3}$ 11-round encryptions. The data complexity is 2^{117} chosen plaintexts and the memory requirement is 2^{119} 128-bit words.

5.3 The Truncated Differential Attack on 12-Round Camellia-192

We add one round on the bottom of 11-round attack, and present a 12-round attack on Camellia-192 for the 99.2% fraction of key space. The attack procedure is similar to the 11-round attack. First we choose 2^{117} plaintexts and encrypt the plaintexts to obtain the corresponding ciphertexts, then guess the 64-bit value k'_{11} and compute the intermediate value R_{11} for every plaintext-ciphertext pairs. After that, apply the 11-round attack to collect the proper pairs and deduce the equivalent key for every pair. The time complexity is equivalent to $2^{64} \times 2^{119.3} = 2^{183.3}$ 12-round encryptions. The memory could be reused in every guess of 64-bit value k'_{11}, which is about 2^{119} 128-bit words. The data complexity is about 2^{117} chosen plaintexts. Similarly, the time complexity of the attack for the full key space is about $2^{183.3} + 2^{184} + 2^{184} \approx 2^{185.3}$.

6 Conclusion

In this paper, inspired by the impossible differential attack, we find an interesting way to construct the truncated differential of block ciphers by the meet-in-the-middle like technique. Therefore, we present the truncated differential cryptanalysis of ISO standards CLEFIA and Camellia. For CLEFIA, we introduce a 10-round truncated differential characteristic to attack 14/14/15-round CLEFIA-128/192/256 with 2^{108}, 2^{135} and 2^{203} encryptions, respectively. For Camellia, we give an 8-round truncated differential to attack 11/12-round Camellia-128/192 including the FL/FL^{-1} and whiten layers with $2^{121.3}$ and $2^{185.3}$ encryptions. It is noted that the truncated differential introduced in our attack, in some cases, is very resembled to the impossible differential proposed in previous works. Nevertheless, the point focused on for the attacker is different in the two methods, one is the zero probability event but the other is the high probability event. It is also significant for us to study the more applications of the method. For example, the applications to Feistel block ciphers SMS4, TEA, XTEA, SIMON, etc.

7 Acknowledgments

We would like to thank anonymous reviewers for their very helpful comments on the paper. This work is supported by the National Natural Science Foundation of China (No. 61133013) and 973 Program (No.2013CB834205), and the National Natural Science Foundation of China (No. 61402256 and 61272035).

References

1. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: Specification of Camellia - a 128-bit Block Cipher. version 2.0, 2001
2. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. In: Stinson, D.R., Tavares, S.E. (eds.) SAC 2000. LNCS, vol. 2012, pp. 39–56. Springer (2001)
3. Bai, D., Li, L.: New Impossible Differential Attacks on Camellia. In: Ryan, M.D., Smyth, B., Wang, G. (eds.) ISPEC 2012. LNCS, vol. 7232, pp. 80–96. Springer (2012)
4. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In: Stern, J. (ed.) EUROCRYPT '99. LNCS, vol. 1592, pp. 12–23. Springer (1999)
5. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 90. LNCS, vol. 537, pp. 2–21. Springer (1991)
6. Biham, E., Shamir, A.: New types of cryptanalytic attacks using related keys. J. Cryptology 7(4), 229–246 (1994)
7. Biryukov, A., Khovratovich, D.: Related-Key Cryptanalysis of the Full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1–18. Springer (2009)
8. Biryukov, A., Khovratovich, D., Nikolic, I.: Distinguisher and Related-Key Attack on the Full AES-256. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 231–249. Springer (2009)
9. Blondeau, C.: Improbable Differential from Impossible Differential: On the Validity of the Model. In: Paul, G., Vaudenay, S. (eds.) INDOCRYPT 2013. LNCS, vol. 8250, pp. 149–160. Springer (2013)
10. Blondeau, C., Gérard, B.: Multiple Differential Cryptanalysis: Theory and Practice. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 35–54. Springer (2011)
11. Bogdanov, A., Geng, H., Wang, M., Wen, L., Collard, B.: Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA. In: Lange, T., Lauter, K.E., Lisonek, P. (eds.) SAC 2013. LNCS, vol. 8282, pp. 306–323. Springer (2013)
12. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., Yalçin, T.: PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208–225. Springer (2012)
13. Boura, C., Naya-Plasencia, M., Suder, V.: Scrutinizing and improving impossible differential attacks: Applications to clefia, camellia, lblock and simon. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology C ASIACRYPT 2014, Lecture Notes in Computer Science, vol. 8873, pp. 179–199. Springer Berlin Heidelberg (2014)
14. Chen, J., Jia, K., Yu, H., Wang, X.: New Impossible Differential Attacks of Reduced-Round Camellia-192 and Camellia-256. In: Parampalli, U., Hawkes, P. (eds.) ACISP 2011. LNCS, vol. 6812, pp. 16–33. Springer (2011)
15. Chen, J., Li, L.: Low Data Complexity Attack on Reduced Camellia-256. In: Susilo, W., Mu, Y., Seberry, J. (eds.) ACISP 2012. LNCS, vol. 7372, pp. 101–114. Springer (2012)
16. Cryptography Research and Evaluation Committees: Http://www.cryptrec.go.jp/english/index.html
17. Hatano, Y., Sekine, H., Kaneko, T.: Higher Order Differential Attack of Camellia (II). In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 129–146. Springer (2003)
18. International Standardization of Organization (ISO): International Standard- ISO/IEC 18033-3, Information technology-Security techniques-Encryption algorithms -Part 3: Block ciphers (2010)
19. International Standardization of Organization (ISO): International Standard- ISO/IEC 29192-2, Information technology-Security techniques-Lightweight cryptography -Part 2: Block ciphers (2011)
20. Isobe, T., Shibutani, K.: Generic Key Recovery Attack on Feistel Scheme. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 464–485. Springer (2013)
21. Kanda, M., Matsumoto, T.: Security of Camellia against Truncated Differential Cryptanalysis. In: Matsui, M. (ed.) FSE 2002. LNCS, vol. 2355, pp. 286–299. Springer (2001)
22. Knudsen, L.: DEAL - A 128-bit Block Cipher. NIST AES Proposal (1998)
23. Knudsen, L.R.: Truncated and Higher Order Differentials. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196–211. Springer (1995)
24. Lai, X.: Higher order derivatives and differential cryptanalysis. In: Blahut, R., Costello, DanielJ., J., Maurer, U., Mittelholzer, T. (eds.) Communications and Cryptography, The Springer International Series in Engineering and Computer Science, vol. 276, pp. 227–233. Springer US (1994)

25. Lai, X., Massey, J.L.: Markov Ciphers and Differentail Cryptanalysis. In: Davies, D.W. (ed.) EUROCRYPT '91. LNCS, vol. 547, pp. 17–38. Springer (1991)
26. Lee, S., Hong, S., Lee, S., Lim, J., Yoon, S.: Truncated Differential Cryptanalysis of Camellia. In: Kim, K. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 32–38. Springer (2002)
27. Lei, D., Li, C., Feng, K.: New Observation on Camellia. In: Preneel, B., Tavares, S.E. (eds.) SAC 2005. LNCS, vol. 3897, pp. 51–64. Springer (2006)
28. Lei, D., Li, C., Feng, K.: Square Like Attack on Camellia. In: Qing, S., Imai, H., Wang, G. (eds.) ICICS 2007. LNCS, vol. 4861, pp. 269–283. Springer (2007)
29. Li, L., Chen, J., Jia, K.: New Impossible Differential Cryptanalysis of Reduced-Round Camellia. In: Lin, D., Tsudik, G., Wang, X. (eds.) CANS 2011. LNCS, vol. 7092, pp. 26–39. Springer (2011)
30. Li, L., Jia, K.: Improved Meet-in-the-Middle Attacks on Reduced-Round Camellia-192/256. IACR Cryptology ePrint Archive 2014/292 (2014)
31. Li, Y., Wu, W., Zhang, L.: Improved Integral Attacks on Reduced-Round CLEFIA Block Cipher. In: Jung, S., Yung, M. (eds.) WISA 2011
32. Liu, Y., Gu, D., Liu, Z., Li, W.: Improved results on impossible differential cryptanalysis of reduced-round Camellia-192/256. Journal of Systems and Software 85(11), 2451–2458 (2012)
33. Liu, Y., Li, L., Gu, D., Wang, X., Liu, Z., Chen, J., Li, W.: New Observations on Impossible Differential Cryptanalysis of Reduced-Round Camellia. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 90–109. Springer (2012)
34. Lu, J., Kim, J., Keller, N., Dunkelman, O.: Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1. In: Malkin, T. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 370–386. Springer (2008)
35. Lu, J., Wei, Y., Fouque, P.A., Kim, J.: Cryptanalysis of reduced versions of the Camellia block cipher. IET Information Security 6(3), 228–238 (2012)
36. Lu, J., Wei, Y., Kim, J., Pasalic, E.: The Higher-Order Meet-in-the-Middle Attack and Its Application to the Camellia Block Cipher. In: Galbraith, S.D., Nandi, M. (eds.) INDOCRYPT 2012. LNCS, vol. 7668, pp. 244–264. Springer (2012)
37. Lu, J., Wei, Y., Pasalic, E., Fouque, P.A.: Meet-in-the-Middle Attack on Reduced Versions of the Camellia Block Cipher. In: IWSEC 2012. LNCS, vol. 7631, pp. 197–215. Springer (2012)
38. Mala, H., Dakhilalian, M., Shakiba, M.: Impossible Differential Attacks on 13-Round CLEFIA-128. J. Comput. Sci. Technol. 26(4), 744–750 (2011)
39. Mala, H., Shakiba, M., Dakhilalian, M., Bagherikaram, G.: New Results on Impossible Differential Cryptanalysis of Reduced-Round Camellia-128. In: Jr., M.J.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 281–294. Springer (2009)
40. New European Schemes for Signatures, Integrity, and Encryption: Final Report of European project IST-1999-12324. Https://www.cosic.esat.kuleuven.be/nessie/Bookv015.pdf
41. Sasaki, Y., Wang, L.: Meet-in-the-Middle Technique for Integral Attacks against Feistel Ciphers. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 234–251. Springer (2012)
42. Selçuk, A.A.: On Probability of Success in Linear and Differential Cryptanalysis. J. Cryptology 21(1), 131–147 (2008)
43. Shirai, T.: Differential, linear, boomerang and rectangle Cryptanalysis of Reduced- Round Camellia. In: the Third NESSIE Workshop (2002)
44. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-Bit Blockcipher CLEFIA (Extended Abstract). In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181–195. Springer (2007)
45. Sugita, M., Kobara, K., Imai, H.: Security of Reduced Version of the Block Cipher Camellia against Truncated and Impossible Differential Cryptanalysis. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 193–207. Springer (2001)
46. Tang, X., Sun, B., Li, R., Li, C.: Impossible Differential Cryptanalysis of 13-Round CLEFIA-128. Journal of Systems and Software 84(7), 1191–1196 (2011)
47. Tezcan, C.: The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA. In: Gong, G., Gupta, K.C. (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 197–209. Springer (2010)
48. Tsunoo, Y., Tsujihara, E., Shigeri, M., Saito, T., Suzaki, T., Kubo, H.: Impossible Differential Cryptanalysis of CLEFIA. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 398–411. Springer (2008)
49. Wang, W., Wang, X.: Improved Impossible Differential Cryptanalysis of CLEFIA. IACR Cryptology ePrint Archive 2007/466 (2007)

50. Wang, W., Wang, X.: Saturation cryptanalysis of CLEFIA. Journal on Communications 29(10), 88–92 (2008)
51. Wu, W., Feng, D., Chen, H.: Collision Attack and Pseudorandomness of Reduced-Round Camellia. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 252–266. Springer (2004)
52. Wu, W., Zhang, L., Zhang, W.: Improved Impossible Differential Cryptanalysis of Reduced-Round Camellia. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 442–456. Springer (2008)
53. Wu, W., Zhang, W., Feng, D.: Impossible Differential Cryptanalysis of Reduced-Round ARIA and Camellia. J. Comput. Sci. Technol. 22(3), 449–456 (2007)
54. Xiaoyang Dong, Leibo Li, K.J., Wang, X.: Improved attacks on reduced-round camellia-128/192/256. In: CT-RSA (to appear). Springer (2015)