doi:10.3772/j.issn.1006-6748.2014.01.008

Sandwich-Boomerang attack on reduced round CLEFIA①

Mao Ming (毛 明)②, Qin Zhiguang
(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, P. R. China)

Abstract

CLEFIA (named after the French word "Clef" meaning "Key") is an efficient, highly secure block cipher proposed by SONY Corporation in the 14th International Workshop on Fast Software Encryption (FSE-2007) and many cryptanalyses have been used to analyze it. According to the property of CLEFIA, a new technique Sandwich-Boomerang cryptanalysis is used on it. An 8-round Sandwich-Boomerang distinguisher of CLEFIA is constructed using the best differential characteristic of CLEFIA. And then, based on the distinguisher, an attack against 10-round CLEFIA is proposed. The number of chosen plaintexts required is 2^{119} (or 2^{120}) and the time complexity is 2^{120} (or 2^{121}). Compared with a 7-round impossible Boomerang distinguisher presented by Choy in the 4th International Workshop on Security (IWSEC-2009), the differential characteristics used in the attack are all the best ones, so it is believed that the attack is the best result that the Boomerang attacks can get on CLEFIA at present.

Key words: block cipher, CLEFIA, Sandwich-Boomerang, distinguisher

0 Introduction

CLEFIA block cipher is designed by Sony Company in Japan and was published at FSE-2007[1]. Sony Company declared that CLEFIA could provide better security and need less encode/decode operation. The security of CLEFIA was initially analyzed by the algorithm designers, including differential cryptanalysis, linear cryptanalysis, impossible differential cryptanalysis and square attack, in which the impossible differential cryptanalysis is the most effective[2,3]. In FSE-2008 Tsunoo et al. improved the impossible differential crypt- analysis to 12-round of CLEFIA-128[2]. Later using the same impossible differential distinguisher, Zhang et al. presented an attack on 14-round CLEFIA-128 considering the weakness in the key schedule[4]. But the CLEFIA design team pointed out a flaw in their attack and showed that it was not successful[5]. In the 11th International Conference on Cryptology in India (IndoCrypt- 2010), Tezcan proposed an improbable differential cryptanalysis on reduced-round CLEFIA[6]. All these cryptanalyses were about the differential characteristic, yet it is important to study other cryptanalysis on CLEFIA in order to evaluate the security of the encryption structure, such as Square attack[7,8], Boomerang attack and so on. Recently Choy proposed an impossible Boomerang attack and a 7-round distinguisher of CLEFIA was presented[9].

Boomerang attack was first proposed by Wagner in FSE-1999[10]. Then it was improved by Biham[11]. Meanwhile, a new method of attack named Rectangle was proposed by him and applied in the attack on some block ciphers[12]. In the following years, this attack was combined with the related key to attack some famous block ciphers including AES by Kim and Biryukov respectively[13-17]. Biryukov *et al.* attacked the full AES-192/256 in theory in the 29th Annual International Cryptology Conference (Crypto-2009)[18]. In Crypto-2010, the 7-round Boomerang distinguisher with a middle slice was used by Dunkelman to attack on the KASUMI which was applied in the third generation mobile communication[19]. This distinguisher improves the effect of the attack to a large extent, which is named as Sandwich-Boomerang distinguisher. Therefore, it is necessary to re-evaluate the effects that this cryptanalytic technique may have on CLEFIA. In this paper the security of CLEFIA against Boomerang attack is first analyzed. According to the generalized Feistel structure and the characteristic of the round function of CLEFIA Cipher, an 8-round Sandwich- Boomerang distinguisher is first presented and 10-round attack on

① Supported by the National Science Foundation of China (No. 60973161), the Doctoral Fund of Ministry of Education of China (No. 200806140010), the National High Technology Research and Development Program of China (No. 2009AA01Z422).

② To whom correspondence should be addressed. E-mail: maomingdky@163.com

Received on Dec. 27, 2011

CLEFIA is proposed with the time complexity of 2^{120} (or 2^{121}) and the data complexity of 2^{119} (or 2^{120}) in this paper. The 8-round distinguisher is better than the impossible Boomerang distinguisher presented by Choy[9].

This paper is organized as follows: Section 1 provides a brief description of preliminaries. Section 2 introduces the 8- round Sandwich-Boomerang distinguisher of CLEFIA. Section 3 describes the attacks on reduced-round CLEFIA. Finally, Section 4 concludes this paper.

1 Preliminaries

1.1 Description of CLEFIA

CLEFIA is a 128-bit block cipher with its key length of 128, 192 and 256 bits, which is compatible to AES (Advanced encryption standard), denoted by CLEFIA-128 /192/256. The round function of CLEFIA includes two different functions: F_0 and F_1. An N-round CLEFIA iterates the round function N times, and in the first round and the last round there are 4 whitening key bytes.

The overall structure of CLEFIA is shown in Fig. 1. The round functions F_0 and F_1 of the SP substitution permutation structure are shown in Fig. 2.

F_0 and F_1 have the same SP structure and include three basic operations: round key addition, substitution layer and diffusion layer. However, in the substitution layer the order of S_0 and S_1 is different, and the permutation layers M_0 and M_1 are also different, which are MDS (maximum-distance-separable) on GF (generalized Feistel) (2^8).

In the encryption procedure of CLEFIA, since the relations between the round subkeys will not help in our attacks, we will omit the key scheduling algorithm here and interested readers can refer to Ref. [11].

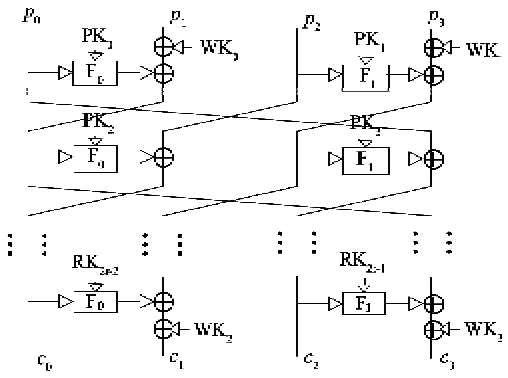
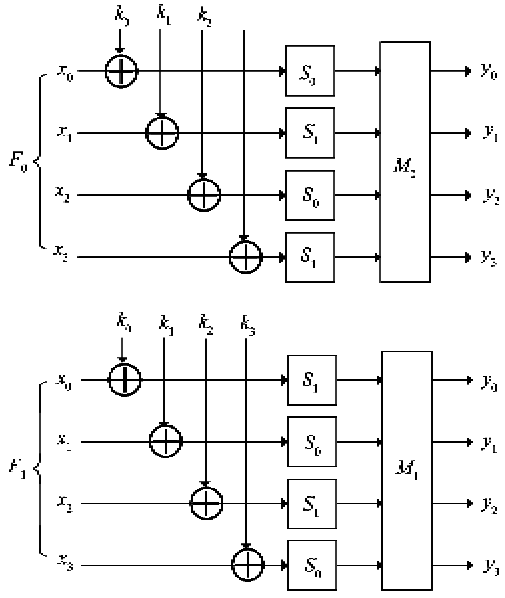


Fig. 1 The structure of CLEFIA



$$M_0 = \begin{bmatrix} 01 & 02 & 04 & 06 \\ 02 & 01 & 06 & 04 \\ 04 & 06 & 01 & 02 \\ 06 & 04 & 02 & 01 \end{bmatrix} \quad M_1 = \begin{bmatrix} 01 & 08 & 02 & 0a \\ 08 & 01 & 0a & 02 \\ 02 & 0a & 01 & 08 \\ 0a & 02 & 08 & 01 \end{bmatrix}$$

Fig. 2 The round function F_0 and F_1

1.2 Notations

The main notations in the paper are introduced in this section. Plaintext and ciphertext are denoted as P and C respectively, and other symbols are as follows:

p_i: the $(i+1)^{th}$ 32-bit word of the plaintext P;

c_i: the $(i+1)^{th}$ 32-bit word of the ciphertext C;

$x_{i,j}$: the $(j+1)^{th}$ byte of the $(i+1)^{th}$ round;

RK_i: the key of the $(i+1)^{th}$ 32-bit round;

$X_{i,j}$: the input of the $(j+1)^{th}$ round of the i^{th} plaintext, which is used in the construction of 8-round distinguisher, where $1 \leqslant i \leqslant 4$.

2 8-round Sandwich-Boomerang distinguisher for CLEFIA

2.1 Sandwich-Boomerang distinguisher

In 1999, Boomerang attack was proposed by David Wagner. The main idea is as follows: the plaintext is chosen as the adaptive plaintext; two short and high-probability differential paths are chosen to be connected. It is useful to analyze more rounds of the ciphers (shown in Fig. 3(a)).

Assume that $E = E_1 \cdot E_0$, there are $P(\alpha \rightarrow \beta) = p$, $P(\gamma \rightarrow \delta) = q$, and the procession of the attack is as follows:

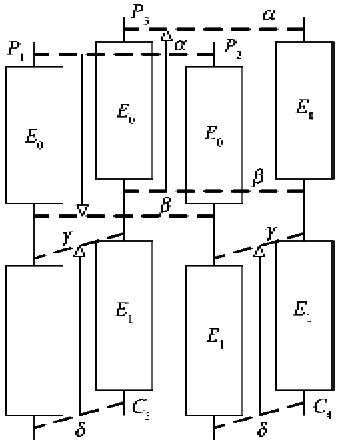
① Choose $P_1 \oplus P_2 = \alpha$, the corresponding cipher texts are (C_1, C_2);

② Compute $C_1 \oplus \delta = C_3$, and $C_2 \oplus \delta = C_4$, after decryption the corresponding plaintexts are (P_3, P_4);

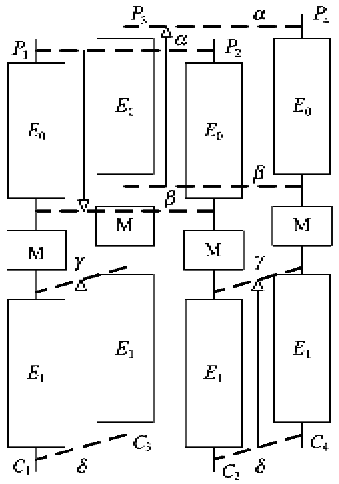
③ Check whether the equation $P_3 \oplus P_4 = \alpha$ is satisfied or not.

The total probability of this quartet of plaintexts and ciphertexts to satisfy the Boomerang conditions is $(pq)^2$. Meanwhile, the probability of the pair at random getting through the distinguisher is 2^{-n}. Therefore, the success condition of the attack is $(pq)^2 > 2^{-n}$.

In Crypto 2010, the 7-round Boomerang distinguisher with a middle slice is used by Dunkelman to attack on the KASUMI. This distinguisher improves the effect of the attack to a large extent, which is named as Sandwich -Boomerang distinguisher in this paper (shown in Fig. 3(b)). Middle slice M is one or more rounds of differential characters, and its probability used in Sandwich-Boomerang structure will be more than that used in E_0 or E_1.



(a) Boomerang distinguisher



(b) Sandwich-Boomerang distinguisher

Fig. 3 The distinguisher structure

In the next section it will introduce how to construct the Sandwich-Boomerang distinguisher for a block cipher. And the distinguisher of CLEFIA, for example, will be described in detail.

2.2 The 8-round distinguisher for CLEFIA

According to the structure of CLEFIA, it is possible to construct a 3 + 1 + 4 = 8 rounds Sandwich-Boomerang distinguisher, the probability of which is 2^{-92} and the probability in random case is 2^{-121}. Compared with the probabilities mentioned above, it is known that the construction of the distinguisher is successful.

The 8-round Sandwich-Boomerang distinguisher includes three parts: E_0, E_1 and the middle slice M, the numbers of the corresponding rounds are three, four and one. The differential path applied in the E_0 is $\alpha \rightarrow \beta$, shown in Fig. 4(a). During the procession of the encryption P_1, P_2, the differential probability of these three rounds is equal to that of getting P_3, P_4 from decryption, which is $p = 2^{-7}$. The differential path applied in E_1 is $\delta \rightarrow \gamma$, shown in Fig. 4(b), whose probability is $q = 2^{-7}$. Because γ is truncated differential, the probability of the following equations is 2^{-32}.

$$\begin{cases} (X^L_{1,4} \oplus X^L_{3,4}) \oplus (X^L_{2,4} \oplus X^L_{4,4}) = [0000, M_1(000?)] \\ (X^R_{1,4} \oplus X^R_{3,4}) \oplus (X^R_{2,4} \oplus X^R_{4,4}) = [0000, 0000] \end{cases} \tag{1}$$

The middle slice is shown in Fig. 4(c). Because the CLEFIA employs a generalized Feistel structure, the equivalent round function can be shown in Fig. 5.

In Fig. 5, the symbol " $<<<$ " means left shift rotation 32 bits. And it is obtained that

$$\beta = [0000, 000a, M_1(000b), 0000] \tag{2}$$

which can be denoted as $\beta = [0000, M_1(000b), 000a, 0000]$, separating left side and right side from each other.

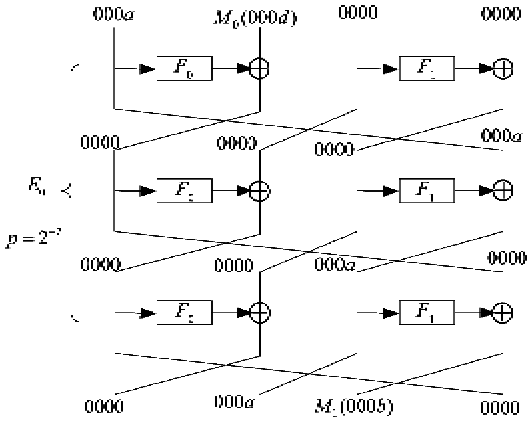
Let the condition be

$$\begin{aligned} X_{1,3} \oplus X_{2,3} &= \beta \\ &= [0000, M_1(000b), 000a, 0000] \\ X^L_{1,4} \oplus X^L_{2,4} &= [\Delta F_0(0000) \oplus 000a, \\ &\quad \Delta F_1(M_1(000b) \oplus 0000)] \\ &= [000A, ????], \end{aligned} \tag{3}$$

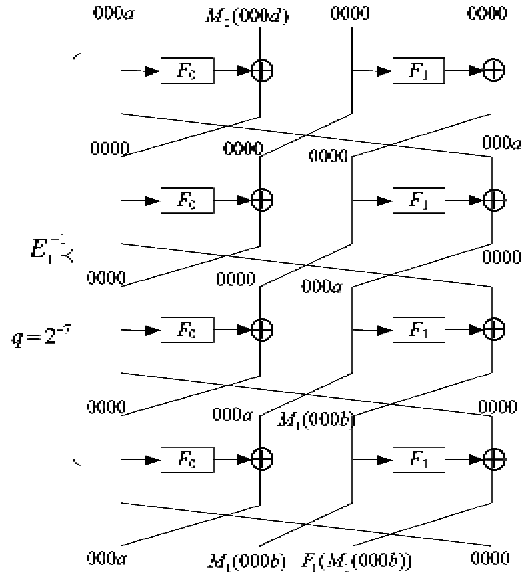
It can get $X_{1,4} \ominus X_{2,4} = [000a, ????, M_1(000b), 0000]$, and $X_{1,4} \oplus X_{3,4} = \gamma = X_{2,4} \oplus X_{4,4}$, so $X_{3,4} \oplus X_{4,4} = [000a, ????, M_1(000b), 0000]$. It is easy to obtain

$$\begin{aligned} X^L_{3,3} \oplus X^L_{4,3} &= X^L_{3,4} \oplus X^L_{4,4} \\ &= [0000, M_1(000b)] \\ &= X^L_{1,3} \oplus X^L_{2,3}, \\ X^R_{3,3} \oplus X^R_{4,3} &= [\Delta F_0(0000) \oplus 000a, \\ &\quad \Delta F_1(M_1(000b)) \oplus ????]. \end{aligned} \tag{4}$$

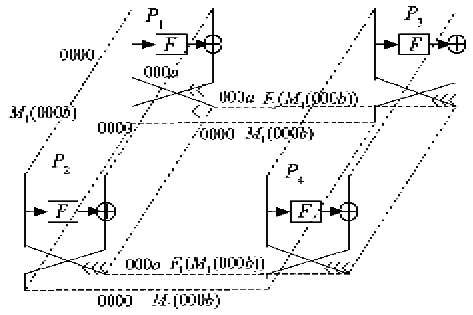
so $p(X_{3,3} \oplus X_{4,3} = \beta) = p(\Delta F_1(M_1(000b)) \oplus ???? = 0000) = 2^{-32}$.



(a) The differential path of the 3-rounds of E_0



(b) The differential path of the 4-rounds of E_1



(c) The middle layer M

Fig. 4 The differential paths of CLEFIA

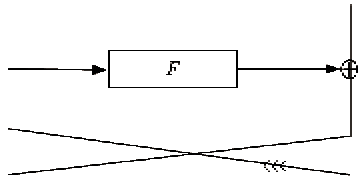


Fig. 5 The equivalent round function

The three parts mentioned above can construct the 8-round distinguisher, whose probability is $(2^{-7})^2 \times (2^{-7})^2 \times 2^{-32} \times 2^{-32} = 2^{-92}$, however, the probability at random is $p(P_3 \oplus P_4 = [000\alpha, M_0(000d), 0000, 0000]) = 2^{-121}$. It shows that the probability of attack success with the construction of the 8-round distinguisher is higher than that in random cases.

3 Boomerang attack on 10-round CLEFIA

3.1 Boomerang attack

Based on the 8-round distinguisher above, the attack on 10-round CLEFIA will be presented, which is shown in Fig. 6. The number of the key that should be guessed is 12 bytes in all.

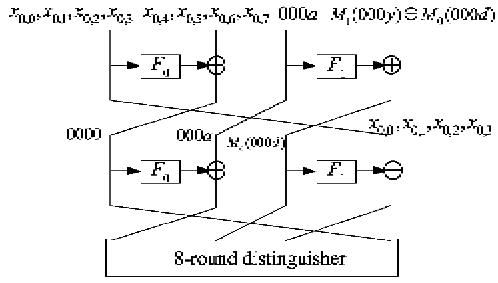


Fig. 6 10-Round Encryption of CLEFIA

1. Guess 32-bit RK_0, choose 2^{39} structures for every guessed key and there are $2^{32+16} = 2^{48}$ plaintexts in each structure. So these plaintexts compose $\binom{2^{48}}{2} = 2^{95}$ pairs. There are 2^{134} plaintext pairs composed of 2^{87} plaintexts. Encrypt each plaintext for 10 rounds and then get the ciphertexts C_i, and $C_i = E(P_i)$, corresponding to all the plaintexts.

2. Compute to get a new ciphertext $D_i = C_i \oplus \delta$ for each ciphertext C_i, where $\delta = (000\alpha, M_0(000d), 0000, 0000)$. And d is a random differential of the corresponding α. Encrypt each new ciphertext for 10 rounds and get all the corresponding plaintexts, that is $P'_i = E^{-1}(D_i)$. Because RK_0 is known, it can get $x'_{1,0}$, $x'_{1,1}$, $x'_{1,2}$, $x'_{1,3}$.

3. Compose P'_i of each structure, if equation $P'_i \oplus P'_j = \alpha *$ is satisfied, then save the corresponding plaintext quartet (P_i, P_j, P'_i, P'_j), and $\alpha * = (X'_{0,0}, X'_{1,0}, X'_{0,2}, X'_{0,3}) = (????, 0000, 000\alpha, M_1(000y) \oplus M_3(000d))$. This step should be filtered for 2^{-80} times. Therefore, for every guessed key, the number of the remaining plaintext quartets is $2^{134} \times 2^{-80} = 2^{54}$.

4. Guess the related key and make the remaining

plaintexts filtered:

(1) Guess the last byte of RK_1, two-way decrypt, that is, decrypt (P_i, P_j) and (P'_i, P'_j) at the same time, and the number of the remaining plaintext quartets is $2^{54} \times 2^{-16} = 2^{38}$.

(2) Guess the remaining three bytes of RK_1, and it can get the middle state value.

(3) Guess the first byte of RK_3, two-way decrypt, and the number of the remaining plaintext quartets is $2^{38} \times 2^{-16} = 2^{22}$.

(4) Guess the second byte of RK_3, two-way decrypt, and the number of the remaining plaintext quartets is $2^{22} \times 2^{-16} = 2^{6}$.

(5) Guess the third and fourth bytes of RK_3, two-way decrypt, and the number of the remaining plaintext quartets is $2^{6} \times 2^{-32} = 2^{-26}$.

5. After the four steps above, the remaining key is the correct key.

3.2 The Complexity and probability of success

For each 32-bit guessed key RK_0, it needs to encrypt and decrypt 2^{87} plaintexts respectively, so the number of the plaintexts is 2^{119}. The time of encryption is equal to that of decryption, and it needs 2^{120} 10-round decryption in the first and second step, that is the main time complexity. The third step is the process of filtering plaintexts, so it needs to save $2^{32} \times 2^{54} = 2^{86}$ plaintext quartets. The fourth step includes five substeps, and the sum of the time complexity is

$$2^{32} \times 2^{8} \times (2^{54} + 2^{24} \times 2^{8} \times (2^{38} + 2^{8} \times (2^{22} + 2^{16} \times 2^{6}))) \times \frac{1}{10} \times \frac{1}{8} \approx 2^{103.6}.$$

Compared with main time complexity, this part of complexity can be ignored. In conclusion, it can be seen that the data complexity of this attack is 2^{119} plaintext pairs and the time complexity is 2^{120} 10-round decryption.

Poisson distribution

$$P(X > n) = 1 - e^{-\lambda} \cdot \sum_{i=0}^{n} \frac{\lambda^i}{i!} \tag{5}$$

is used to analyze the probability of success as follows: for the correct guess of the keys, the number of remaining pairs after distinguisher is

$$\lambda = 2^{134} \times 2^{-8} \times 2^{-32} \times 2^{-92} = 4, \tag{6}$$

the probability of success is $P(X > 2) \approx 0.762$; for the wrong guess of the keys, the number of remaining pairs after distinguisher is $\lambda = 2^{-26}$, and the probability of success is $P(X > 2) \approx 0$. The more the selected plaintext, the higher probability of getting the correct keys. For example, choose 2^{120} plaintext pairs, and the probability of guessing the correct keys is 0.982, meanwhile, the probability of guessing the wrong keys is 0. Therefore, it is sensible to choose the number of the plaintexts according to actual needs.

4 Conclusions

According to the generalized Feistel structure and the characteristic of the round function of CLEFIA, 8-round Sandwich- Boomerang distinguisher is first presented and 10-round attack on CLEFIA is proposed. Then 10-round CLEFIA is successfully attacked with the probability of 0.762 (or 0.982), in which the data complexity and the time complexity are 2^{119} and 2^{120} (or 2^{120} and 2^{121}). Because the differential characteristics used in the attacks are all the best ones, it is believed that the attacks are the best results that the Boomerang attack can get on CLEFIA. In conclusion, the 8-round distinguisher is better than the impossible Boomerang distinguisher presented by Choy[9], which is shown in Table 1. However, our result also shows that the full round CLEFIA is safer and stronger against the Sandwich- Boomerang attack. The relation of Boomerang cryptanalysis and other cryptanalysis is our next studying work.

Table 1 The Boomerang attack results of CLEFIA

Attacks	*DRs*	*ARs*	*Time*	*Data*	*Pro*	*Sour*
Im-B	7	--	--	--	--	Ref. [9]
San-B	8	10	2^{120}	2^{119}	0.762	This paper
San-B	8	10	2^{121}	2^{120}	0.982	This paper

Im-B: *Impossible Boomerang*
San-B: *Sandwich- Boomerang*
DRs: *The rounds of distinguisher*
Pro: *The Probability of success*
Sour: *Source*

References

[1] SONY Corporation. The 128-bit block cipher CLEFIA: security and performance evaluations. http://www.sony.net/Products/clefia/technical/data/clef-ia-eval-1.0.pdf, 2007

[2] Tsunoo Y, Tsujihara E, Shigeri M, et al. Impossible differential cryptanalysis of CLEFIA. In: Proceedings of the 15th International Workshop on Fast Software Encryption, Heidelberg, Germany: Springer Berlin, 2008. 398-411

[3] Wang W, Wang X. Impossible differential cryptanalysis of CLEFIA-128/192/256. *Journal of Software*, 2009, 20 (9): 2587-2596

[4] Zhang W, Han J. Impossible differential analysis of reduced round CLEFIA. In: Proceedings of the 4th International Conferences on Information Security and Cryptology, Heidelberg, Germany: Springer Berlin, 2008. 181-191

[5] CLEFIA design team, Sony Corporation, Comments on the impossible differential analysis of reduced round

CLEFIA. In: Proceedings of the 4th International Conferences on Information Security and Cryptology, Heidelberg, Germany: Springer Berlin, 2009. 1-12

[6] Tezcan C. The improbable differential attack: cryptanalysis of reduced round CLEFIA. In: Proceedings of the 11th International Conference on Cryptology, Heidelberg, Germany: Springer Berlin, 2010, 197-209

[7] Wang W, Wang X. Saturation cryptanalysis of CLEFIA. *Journal on Communications*, 2008, 29(10): 88-92

[8] Tang X, Li Ch, Xie D. Square attack on CLEFIA. *Journal of Electronics& Information Technology*, 2009, 31(9): 2260-2263

[9] Choy J, Yap H. Impossible boomerang attack for block cipher structures. In: Proceeding of the 4th International Workshop on Security, Heidelberg, Germany: Springer Berlin, 2009. 22-37

[10] Wagner D. The boomerang attack. In: Proceedings of the 6th International Workshop on Fast Software Encryption, Heidelberg, Germany: Springer Berlin, 1999. 156-170

[11] Biham E, Dunkelman O, Keller N. New results on boomerang and rectangle attacks. In: Proceedings of the 9th International Workshop on Fast Software Encryption, Heidelberg, Germany: Springer Berlin, 2002. 1-16

[12] Biham E, Dunkelman O, Keller N. The rectangle attack-rectangling the Serpent. In: Proceedings of the 20th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Heidelberg, Germany: Springer Berlin, 2001. 340-357

[13] Biryukov A, Cannière Ch D, Dellkrantz G. Cryptanalysis of SAFER + +. In: Proceedings of the 23rd Annual International Cryptology Conference, Heidelberg, Germany: Springer Berlin, 2003. 195-211

[14] Kim J, Kim G, Hong S, et al. The related-key rectangle attack-application to SHACAL-1. In: Proceedings of Australasian Conference on Information Security and Privacy, Heidelberg, Germany: Springer Berlin, 2004. 123-136

[15] Hong S, Kim J, Kim G, et al. Related-key rectangle attacks on reduced versions of SHACAL-1 and AES-192. In: Proceedings of the 6th International Workshop on Fast Software Encryption, Heidelberg, Germany: Springer Berlin, 2005. 368-383

[16] Biryukov A. The boomerang attack on 5 and 6-round reduced AES. In: Proceedings of Advanced Encryption Standard 2004, Heidelberg, Germany: Springer Berlin, 2005. 11-15

[17] Biham E, Dunkelman O, Keller N. A related-key rectangle attack on the full KASUMI. In: Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security, Heidelberg, Germany: Springer Berlin, 2005. 443-461

[18] Biryukov A, Khovratovich D. Related-key cryptanalysis of the full AES-192 and AES-256. In: Proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security, Heidelberg, Germany: Springer Berlin, 2009. 1-18

[19] Dunkelman O, Keller N, Shamir A. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In: Proceedings of the 30th International Cryptology Conference, Heidelberg, Germany: Springer Berlin, 2010. 393-410

Mao Ming, born in 1963, professor. He is currently pursuing Ph. D. in School of Computer Science and Engineering of University of Electronic Science and Technology of China. His research interests are information security and cryptography.