Security Analysis of the Block Cipher CLEFIA

VERSION 1.1

FINAL REPORT

Alex Biryukov
University of Luxembourg, Luxembourg

Ivica Nikolić
Nanyang Technological University, Singapore

Contents

1 Introduction **3**

1.1 Description . . . 3

1.2 Known Analysis . . . 3

1.3 Analysis of the Transformations . . . 4

1.3.1 S-box Analysis . . . 4

1.3.2 Analysis of the Linear Transformations . . . 4

2 Analysis Against Various Attacks **5**

2.1 Differential Cryptanalysis . . . 5

2.1.1 Single-key Differentials . . . 5

2.1.2 Related-key Differentials . . . 7

2.2 Boomerang Cryptanalysis . . . 9

2.3 Truncated Differential Cryptanalysis . . . 9

2.4 Slide Attacks . . . 10

2.5 Rotational Attacks . . . 11

3 Conclusion **12**

Chapter 1

Introduction

In this chapter is given a short description of *CLEFIA* along with known cryptanalytical results. A preliminary analysis of the operations used in *CLEFIA* is provided.

1.1 Description

CLEFIA is 128-bit Feistel-like block cipher with a number of rounds that depends on the key size: 18 rounds for 128-bit keys, 22 rounds for 192-bit keys, and 26 rounds for 256-bit keys. All the transformations in the cipher can be divided into two parts:

1. **State transforms.** *CLEFIA* follows the four branch Generalized Feistel design and in each round half of the state (i.e. 64 bits or 8 bytes) is updated by two distinct round function F_0, F_1 which are byte-oriented SP network: after the XOR of the round key, the S-layer with 4 S-boxes in parallel is applied, followed by the P-layer which is a matrix multiplication.

2. **Key schedule transforms.** An intermediate key is produced from the master key with a Feistel-like transforms as in the state. Then the round keys are obtained from the intermediate key, with XOR and bit permutations.

All of the state transformations in *CLEFIA* are byte oriented. This simplifies the analysis of *CLEFIA* against single-key attacks. However the bit permutations in the key schedule, make the analysis of related-key attacks complex.

1.2 Known Analysis

Aside from the thorough analysis presented by the designers (see [4]), there are several published attacks on round-reduced versions of *CLEFIA*. Most of the attacks are impossible differential attacks on 11-14 rounds [9, 10, 5, 8, 6, 2]. Additional improbable differential attack on 13-15 rounds [7], and integral attack on 11-14 rounds [1] were published as well.

1.3 Analysis of the Transformations

To estimate the resistance of *CLEFIA* against various attack, first we focus on each of the transformations used in the cipher. In particular, we analyze the S-boxes and the linear transformations.

1.3.1 S-box Analysis

The complexity of the differential attacks on a cipher is tightly related to the differential properties of the S-boxes used in the cipher. There are 2 different types of 8x8 non-linear bijective S-boxes used in *CLEFIA*. The maximal differential propagation probability is $2^{-4.67}$ for the first, and 2^{-6} for the second S-box. The probability of the first S-box is suboptimal.

1.3.2 Analysis of the Linear Transformations

There are two different linear transformations in the round function F and an additional linear function *DoubleSwap* Σ in the key schedule. The linear transformations in F are multiplication by matrices M_0, M_1 and have a branch number of 5. This number is optimal, and it assures maximal diffusion among the bytes. The *DoubleSwap* function is a simple bit permutation, hence it can neither introduce nor cancel active bits/bytes. However, this function destroys the byte orientation of the cipher and makes the analysis of related-key attacks much more complex.

Chapter 2

Analysis Against Various Attacks

In this chapter an analysis of the resistance of *CLEFIA* against different single-key and related-key attacks is given. In particular, we focus on:

- Classical Differential Cryptanalysis
- (Amplified) Boomerang Cryptanalysis
- Truncated Differential Cryptanalysis
- Slide Attack
- Rotational Attacks

2.1 Differential Cryptanalysis

Differential attacks are the most popular form of cryptanalysis for block ciphers. A widely accepted approach for designing a byte-oriented cipher resistant against differential attacks is to ensure that each differential characteristic has a certain number of active S-boxes. Except for the differential properties of the S-boxes, this number also depends on the size of the state in the single key scenario, and on the size of the key in the related-key scenario. In the sequel we give probabilities of the best differential trails based on the number of active S-boxes.

2.1.1 Single-key Differentials

In the single-key scenario we assume there is no difference in the key, and there is some initial difference in the plaintext. We use an advanced brute-force approach, based on Matsui's technique used to find the best characteristics in DES (see [3]), to find the probabilities and the number of active S-boxes

Table 2.1: The number of active S-boxes in the best round-reduced single-key differential characteristics for *CLEFIA*.

Rounds	Active S-boxes
1	0
2	1
3	2
4	6
5	8
6	12
7	12
8	13
9	14
10	18
11	20
12	24
13	24
14	25
15	26
16	30

in the best round-reduced single-key characteristics. We use the term "best" with regards to the characteristics with the highest probability. As mentioned previously, *CLEFIA* uses two different type of S-boxes: the maximal differential probability of the first S-box is around $2^{-4.67}$, while for the second type is 2^{-6}. We use these probabilities as estimations for the active S-boxes. The best single-key characteristics, in terms of the minimal number of active S-boxes, are presented at Tbl. 2.1. The best characteristics, in terms of probability, are given at Tbl. 2.2.

Notice, the characteristics with the minimal number of active S-boxes are the ones that have the highest probability as well. This does not have to be the case, as the S-boxes have different probability, however, in the case of *CLEFIA* the characteristics coincide. Interestingly, starting from round 7, the best round-reduced characteristics found by our approach differ from the best characteristics presented in the evaluation paper of *CLEFIA* (see [4]). This may be due to the fact that our characteristics are not checked if they comply with the properties of the diffusion layer, i.e. some characteristics may not be possible as there are two different diffusion matrices, each with a branch number of 5, and hence two active bytes (or columns) cannot always cancel (or produce the required combination of active-nonactive bytes). Our results, however can still be used as reliable upper bounds on the probabilities of the best characteristics. For example, we can be sure that no characteristic exists on 10 rounds with probability higher than $2^{-92.03}$ as the best characteristic (even without the linear filters) should satisfy such bound.

Table 2.2: The number of active S-boxes in the best round-reduced single-key differential characteristics for *CLEFIA*.

Rounds	$-log_2$ probability	Active S-boxes
1	0	0
2	4.67	1
3	9.34	2
4	30.68	6
5	40.01	8
6	60.02	12
7	61.36	12
8	66.02	13
9	70.69	14
10	92.03	18
11	101.37	20
12	121.48	24
13	122.71	24
14	127.38	25
15	132.05	26
16	153.39	30

Given the tables, we can easily give upper bounds on the best differential attacks based on differential characteristics:

Observation 1 *For all key sizes of CLEFIA, no single-key differential characteristic can exist on more than 14 rounds.*

The theory of computation of differential characteristics is far ahead of computing the same probabilities of differentials. Hence, we cannot give a precise bound on the number of rounds sufficient for resistance of *CLEFIA* against differential attacks. However under the standard assumptions, that the number of characteristics within a differential is low and the relatively high margin for the best characteristic on more than 15 rounds, we expect *CLEFIA* to be resistant against single-key differential attacks.

2.1.2 Related-key Differentials

The transformations in the key schedule of *CLEFIA-128*, in particular the generation of the extended key L, are based on the same Feistel construction as in the state – only the subkey additions are replaced with additions of constants. Therefore a differential characteristic in the key schedule has the same probability as the differential characteristic in the single-key case. Since *CLEFIA* requires the generation of the extended key L (it is unclear how to analyze simplified key schedule), any related-key differential characteristic with a difference in the master key, has to pass the 12 rounds of the Feistel and therefore its prob-

Table 2.3: The probability of the best characteristics for $GFN_{8,10}$ used in the key schedule of *CLEFIA-192* and *CLEFIA-256*.

Rounds	$-log_2$ probability	Active S-boxes
1	0	0
2	4.67	1
3	9.34	2
4	30.68	6
5	40.01	8
6	60.02	12
7	70.69	14
8	90.70	18
9	106.04	21
10	126.05	25

ability only in the key schedule cannot be higher than $2^{-121.48}$ (see Tbl.2.2). Thus, to launch a related-key differential attack, the number of active S-boxes in the state cannot be higher than 1 – otherwise the total probability of the related-key differential characteristic would become lower than 2^{-128}. In order to find the maximal number of rounds in the state with only one active S-box we have implemented another brute-force search. We have fixed the position of the active bytes in the master key, as well as the position of the active bytes in the extended key L – these positions are the one from the 12-round characteristic with highest probability. In total there are 588 characteristics for the key schedule that have a probability higher than 2^{-128}. We also go through all possible combinations of active bytes in the plaintext and see how many rounds we can reach with only one active S-box in the state. The DoubleSwap function was replaced with a similar, but byte oriented function, where 7 bit rotations were replaced with 8 bit. The search resulted in a characteristic on at most 4 rounds. Hence we can conclude that:

Observation 2 *For CLEFIA-128 with byte oriented key schedule, no related-key differential characteristic exists on more than 4 rounds.*

The impact on replacing Σ with byte-oriented Σ is unclear, and related-key characteristics on higher number of rounds might exist for the original key schedule. However, we expect that if such characteristic exists then the number of rounds it covers cannot be much larger than 4 – under very optimistic scenario it can reach as high as 8, but not more.

For *CLEFIA-192* and *CLEFIA-256*, in the key schedule, eight-branch ten-round Feistel is used for generation of the extended key L. Therefore, we have to slightly modify our brute-force in order to find the best characteristic for this key schedule. The result of the search is given at Tbl.2.3.

Note that for the full ten rounds, the probability of the best characteristic is $2^{-126.05}$, i.e. we can conclude that:

Observation 3 *For CLEFIA-192 and CLEFIA-256, the probability of any related-key differential characteristic is lower than* 2^{-126}.

In theory, to claim resistance against related-key differential characteristic attack, the probability of the characteristic should be lower than 2^{-256} (respectively 2^{-192} for 192-bit keys). Otherwise, it might be possible to launch key recovery attack in a weak-key class with a heavy filtering. Thus we cannot deduce a clear conclusion of the resistance against key-recovery attacks. However, we can state that no related-key differential distinguisher is applicable to *CLEFIA-192* and *CLEFIA-256* as on reasonably high number of rounds there would be at least one active S-box in the state making the total probability of the related-key differential characteristic lower than 2^{-128}.

2.2 Boomerang Cryptanalysis

In boomerang attacks, the characteristics do not have to cover the full cipher. Indeed, the number of rounds they cover should be chosen such that the probability of the boomerang is maximal. As we already have the probabilities of the best round-reduced characteristics, we can easily find the probability (and respectively the complexities) of the best boomerang attacks.

The case of related-key boomerangs is trivial. As the probabilities of the best characteristics in the key schedule are low, any related-key boomerang would have probability much lower than 2^{-128} (respectively lower than 2^{-192}, 2^{-256} for longer keys). Hence, no related-key boomerang attack is applicable to full-round *CLEFIA*.

To find the best single-key boomerang we should take into account the results from Tbl.2.2. When the top characteristic is on 3 rounds and the bottom on 5 rounds, i.e. 8 rounds in total, the probability of the boomerang is higher than 2^{-128} (only under the assumption that all of the active S-boxes hold with maximal probability). For any other choice of rounds (with sum greater than 8), the probability of the boomerang is lower than 2^{-128}. Hence, we can conclude that no boomerang exist on 9 rounds. Using some advanced techniques, an attacker might be able to skip rounds at the beginning, middle and at the end of the boomerang. However, the security margin is very high, and therefore we can conclude that approximately 12 rounds of *CLEFIA* are sufficient for resistance against boomerang attacks. The case of amplified boomerangs gives no advantage over the classical boomerangs to the attacker.

2.3 Truncated Differential Cryptanalysis

In truncated differential attacks, instead of following the propagation of certain difference through the rounds of the cipher and specifying how the initial difference changes after each transformation, the attacker only examines the position of the bytes with differences (i.e. active bytes) through the rounds. Hence the linear transformations in the cipher have the main and the only impact on the

Table 2.4: The probabilities of the best round-reduced truncated differentials for *CLEFIA*.

Rounds	$-log_2$ probability
1	0
2	0
3	24
4	56
5	64
6	96
7	120
8	120
9	144

probability of a characteristic. To find the best round-reduced truncated differentials we have used again Matsui's approach combined with the following standard assumptions:

1. S-boxes have no effect on the probability, i.e. they cannot change active byte into non-active and vice versa;
2. XOR can cancel two active bytes with probability 2^{-8};
3. The matrix multiplication can produce output column with t active bytes with probability $2^{-8(4-t)}$.

The result of the search is presented at Tbl.2.4. Therefore we can conclude that:

Observation 4 *For CLEFIA, no truncated differentials exist on more than 8 rounds.*

Note that the truncated differentials presented in the table have exactly specified positions of active bytes. By relaxing some of the positions, it might be possible to construct differentials for higher number of rounds. However, we expect that if such differentials are achievable, then the number of rounds they cover should not be significantly higher than 8. Taking into account the high security margin of *CLEFIA*, we can conclude that the full round cipher is resistant against truncated differential attacks.

2.4 Slide Attacks

Slide attacks are applicable to ciphers that have similar rounds. This is not the case for *CLEFIA* because of the key schedule. Although the key schedule can be slid by two rounds, every round uses different constants to produce the subkeys. Hence, we can conclude that *CLEFIA* is resistant against slide attacks.

2.5 Rotational Attacks

So far rotational attacks have been applied only to addition-rotation-XOR primitives. To apply this type of attacks to substitution-permutations ciphers with byte-oriented structure the rotational input pairs have to differ by multiple of 8. Though *CLEFIA* satisfies this requirement, it uses high number of round constants in the key schedule that are not rotational. Therefore we believe rotational attacks cannot be applied to *CLEFIA*.

Chapter 3

Conclusion

The analysis presented in the previous chapter allows us to make the following conclusions regarding the security of *CLEFIA*.

- **Single-key differentials.** Although the best standard differential trails we have found cover a significant number of rounds of *CLEFIA*-128, they are obtained under certain assumptions that usually give more advantage to the attacker than he/she has in practice. Even in such scenario, *CLEFIA* is resistant against single-key differential attacks based on standard differential trails. Also, the truncated trails cover only around one half of the total number of rounds. Even with some advanced techniques, when the attacker can pass a few more rounds, the security margin of *CLEFIA* is high, hence the cipher is resistant against attacks based on differential trails. We note that *CLEFIA* applies standard cryptographic design techniques, and as there is no known analysis on such ciphers showing a significant advantage of differential attacks over the attacks based on differential trails, we believe that *CLEFIA* is secure against differential attacks as well. A similar conclusion applies to the case of boomerang attacks as they are differential-based attacks.

- **Related-key differentials.** For the version of the cipher with 128-bit key, our analysis shows that no related-key differential attacks exists. In the case of longer keys, a class of weak keys might exist. However, due to the low probability of the related-key differential, i.e. below 2^{-128}, it is very likely that the attacker would not be able to detect if a certain key belongs to the class, hence cannot mount an attack on the cipher.

- **Other attacks.** *CLEFIA* is resistant against slide attacks and rotational attacks, as this type of cryptanalysis in the best scenario is applicable to the cipher on a few rounds only.

Bibliography

[1] Y. Li, W. Wu, and L. Zhang. Improved integral attacks on reduced-round CLEFIA block cipher. In S. Jung and M. Yung, editors, *WISA*, volume 7115 of *Lecture Notes in Computer Science*, pages 28–39. Springer, 2011.

[2] H. Mala, M. Dakhilalian, and M. Shakiba. Impossible differential attacks on 13-round CLEFIA-128. *J. Comput. Sci. Technol.*, 26(4):744–750, 2011.

[3] M. Matsui. On correlation between the order of s-boxes and the strength of DES. In A. D. Santis, editor, *EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 366–375. Springer, 1994.

[4] Sony Corporation. Security and performance evaluations. *http://www.sony.net/Products/cryptography/clefia/download/data/clefia-eval-1.0.pdf.*

[5] B. Sun, R. Li, M. Wang, P. Li, and C. Li. Impossible differential cryptanalysis of CLEFIA. *IACR Cryptology ePrint Archive*, 2008:151, 2008.

[6] X. Tang, B. Sun, R. Li, and C. Li. Impossible differential cryptanalysis of 13-round CLEFIA-128. *Journal of Systems and Software*, 84(7):1191–1196, 2011.

[7] C. Tezcan. The improbable differential attack: Cryptanalysis of reduced round CLEFIA. In G. Gong and K. C. Gupta, editors, *INDOCRYPT*, volume 6498 of *Lecture Notes in Computer Science*, pages 197–209. Springer, 2010.

[8] Y. Tsunoo, E. Tsujihara, M. Shigeri, T. Saito, T. Suzaki, and H. Kubo. Impossible differential cryptanalysis of CLEFIA. In K. Nyberg, editor, *FSE*, volume 5086 of *Lecture Notes in Computer Science*, pages 398–411. Springer, 2008.

[9] W. Wang and X. Wang. Improved impossible differential cryptanalysis of CLEFIA. *IACR Cryptology ePrint Archive*, 2007:466, 2007.

[10] W. Zhang and J. Han. Impossible differential analysis of reduced round CLEFIA. In M. Yung, P. Liu, and D. Lin, editors, *Inscrypt*, volume 5487 of *Lecture Notes in Computer Science*, pages 181–191. Springer, 2008.