Evaluation of security level of CLEFIA

An anonymous reviewer

Version 1.0 — January 25, 2011

Evaluation of security level of CLEFIA

Contents

Executive Summary

We have performed a security evaluation of the cryptographic block cipher CLEFIA as described in [28].

We have analysed the cipher with respect to the state-of-the-art cryptanalysis and we have found no serious weaknesses or attacks. It is further believed that the security margin is sufficient with respect to the currently known attacks.

Finally we would like to point out that this report is the result of a limited-time review.

References

[1] 3GPP. 3G TS 35.202 version 4.0.0: 3rd generation partnership project; technical specification group services and system aspects. 3G security; specification of the 3GPP confidentiality and integrity algorithms; document 2: KASUMI specification. Available at `www.3gpp.org`.

[2] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer, 1993.

[3] E. Biham. New types of cryptanalytic attacks using related keys (extended abstract). In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93,* volume 765 of *Lecture Notes in Computer Science,* Springer, pages 398–409, 1994.

[4] Alex Biryukov and Dmitry Khovratovich. *Related-Key Cryptanalysis of the Full AES-192 and AES-256.* In M. Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009,* volume 5912 of *Lecture Notes in Computer Science,* Springer, pages 1–18, 2009.

[5] Alex Biryukov and Orr Dunkelman and Nathan Keller and Dmitry Khovratovich and Adi Shamir. Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds. In H. Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010,* volume 6110 of *Lecture Notes in Computer Science,* Springer, pages 299–319, 2010.

[6] C. Cid and G. Leurent. An analysis of the XSL Algorithm. In *Bimal Roy, editor,* Advances in Cryptology - ASIACRYPT 2005, Lecture Notes in Computer Science, volume 3788, pages 333-352, Springer-Verlag, Chennai - India, December 2005.

[7] Nicolas T. Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In B. Preneel, editor, *Advances in Cryptology - Eurocrypt 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 392–407. Springer-Verlag, 2000.

[8] Nicolas T. Courtois and Josef Pieprzyk. Cryptoanalysis of Block Ciphers with Overdefined System of equations. In Y. Zheng, editor, *Advances in Cryptology -Asiacrypt 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 267–287. Springer-Verlag, 2002.

[9] Claus Diem. The XL-Algorithm and a Conjecture from Commutative Algebra. In P .J. Lee, editor, *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 323–337, 2004.

[10] ECRYPT Network of Excellence. ECRYPT Yearly Report on Algorithms and Keysizes (2009-2010). Available at `http://www.ecrypt.eu.org/documents/D.SPA.13.pdf`

[11] T. Jakobsen and L. Knudsen. The interpolation attack on block ciphers. In E. Biham, editor, *Fast Software Encryption, FSE 1997,* volume 1267 of *Lecture Notes in Computer Science,* Springer, pages 28–40, 1997.

[12] J. Kelsey, B. Schneier, and D. Wagner. Key-schedule cryptoanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In N. Koblitz, editor, *Advances in Cryptology - CRYPTO'96,* volume 1109 of *Lecture Notes in Computer Science,* Springer, pages 237–251, 1996.

[13] L. R. Knudsen. Truncated and higher order differentials. In B. Preneel, editor, *Fast Software Encryption, FSE 1994,* volume 1008 of *Lecture Notes in Computer Science,* Springer, pages 196–211, 1995.

[14] L. R. Knudsen and D. Wagner. Integral cryptanalysis. In J. Daemen and V. Rijmen, editors, *Fast Software Encryption, FSE 2002, February 2002,* volume 2365 of *Lecture Notes in Computer Science,* Springer, pages 112–127, 2002.

[15] L. R. Knudsen and Vincent Rijmen. Known-Key Distinguishers for Some Block Ciphers. In K. Kurosawa, editor, *Advances in Cryptology - ASIACRYPT 2007,* volume 4833 of *Lecture Notes in Computer Science,* Springer, pages 315–324, 2007.

[16] X. Lai. Higher order derivatives and differential cryptanalysis. In R. Blahut, editor, *Communication and Cryptography, Two Sides of One Tapestry.* Kluwer Academic Publishers, 1994. ISBN 0-7923-9469-0.

[17] C.-W. Lim and K. Khoo. An Analysis of XSL Applied to BES. *A. Biryukov (ed): Lecture Notes in Computer Science, FSE 2007, (4593), pages 242–253, Springer-Verlag Heidelberg Berlin, 2007.*

[18] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93,* volume 765 of *Lecture Notes in Computer Science,* Springer, pages 386–397, 1994.

[19] M. Matsui and A. Yamagishi. A new method for known plaintext attack of FEAL cipher. In R. Rueppel, editor, *Advances in Cryptology - EUROCRYPT'92,* volume 658 of *Lecture Notes in Computer Science,* Springer, pages 81–91, 1993.

[20] National Institute of Standards and Technology. Advanced encryption standard. Federal Information Processing Standard (FIPS), Publication 197, U.S. Department of Commerce, Washington D.C., November 2001.

[21] National Institute of Standards and Technology. Data encryption standard. Federal Information Processing Standard (FIPS), Publication 46, U.S. Department of Commerce, Washington D.C., January 1977.

[22] K. Nyberg and L. R. Knudsen. Provable security against a differential attack. *J. Cryptology*, 8(1):27–37, 1995.

[23] X. Lai, J. L. Massey, and S. Murphy. Markov ciphers and differential cryptanalysis. In D.W. Davies, editor, *Advances in Cryptology - EUROCRYPT'91,* volume 547 of *Lecture Notes in Computer Science,* Springer, pages 17–38, 1992.

[24] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1997.

[25] National Institute of Standards and Technology. Advanced encryption standard. FIPS 197, US Department of Commerce, Washington D.C., November 2001.

[26] R. L. Rivest. The RC5 encryption algorithm. In B. Preneel, editor, *Fast Software Encryption, FSE 1994,* volume 1008 of *Lecture Notes in Computer Science,* Springer, pages 86–96, 1995.

[27] R. L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin. The RC6 block cipher. Submitted as candidate for AES. Available at `http://www.nist.gov/aes`.

[28] Sony Corporation. The 128-bit Blockcipher CLEFIA. Algorithm Specification. Revision 1.0. January 29, 2010.

[29] Sony Corporation. The 128-bit Blockcipher CLEFIA. Security and Performance Evaluations Revision 1.0, June 1, 2007. Available from `http://www.sony.net/Products/cryptography/clefia/technical/data/clefia-eval-1.0.pdf`

[30] D. Wagner. A Generalized Birthday Problem. In M. Yung, editor, *Advances in Cryptology – Crypto 2002*, volume 2442 of *Lectures Notes in Computer Science*, pages 288–303. Springer, 2002.

[31] Wenying Zhang and Jing Han. Impossible Differential Analysis of Reduced Round CLEFIA. In M. Yung, P. Liu, and D. Lin, editors, *Inscrypt 2008*, volume 5487 of *Lectures Notes in Computer Science*, pages 181–191. Springer, 2009.

1 Introduction

This report presents the results of a limited evaluation of the block cipher CLEFIA. In the work order specification it is required that CLEFIA is evaluated with respect to the following attacks:

1.
   - Differential Attack (including Truncated Differential Attack, Impossible Differential Attack)
   - Linear Attack (including Truncated Linear Attack)
   - Higher Order Differential Attack
   - Interpolation Attack
   - Algebraic Attack (including XL attack and XSL attack)
   - Related Key Attack and
   - The existence of weak keys and semi-weak keys
2. (Optional) Any other attacks specific to CLEFIA and Heuristic security

In the following all these attacks are considered except for the truncated linear attack. We could only find one reference about this attack and this reference is not available to us.

2 CLEFIA - short

Here we describe CLEFIA in short. For full details the reader is referred to [28].

CLEFIA is block cipher with 128-bit blocks and a choice of 128-bit, 192-bit and 256-bit keys. The structure of the cipher is a so-called generalised Feistel network with four data lines, each carrying 32-bit words, see Figure 1. The functions F_0 and F_1 both take a 32-bit subkey and a 32-bit input, and both return a 32-bit word. First the subkey is combined with the data input using the exclusive-or operation. The 32-bit result is split into four bytes, and the bytes are evaluated through the S-boxes S_0 and S_1, such that, two bytes are substituted using S_0 and two bytes are substituted using S_1. The order of use of S_0 and S_1 is different for F_0 and F_1. The four substituted bytes are input to a linear transformation built from MDS codes. This element is borrowed from the AES and guarantees that the round function provides some level of an avalanche effect. Later we describe some more details about the generation of subkeys. We refer to [28] for further details.

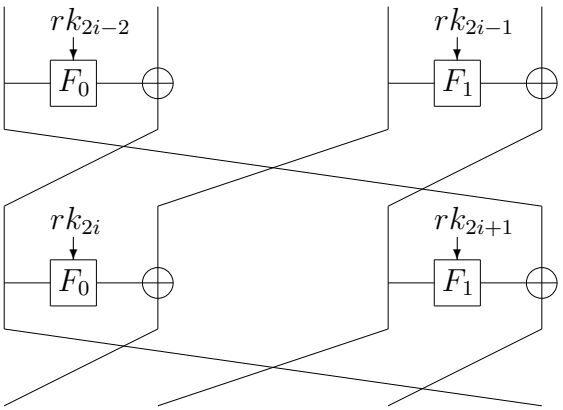


Figure 1: The CLEFIA network with two rounds. F_0 and F_1 are bijective mappings for fixed values of the rk_is.

3 Security aspects

In this section we report on some cryptanalytic findings in CLEFIA. CLEFIA is an iterated cipher which runs in either 18, 22, or 26 rounds depending on the choice of size of the key of 128, 192, respectively 256 bits.

3.1 Brute Force Attacks

We shall briefly comment on brute-force attacks against the 128-bit key. The European project ECRYPT issues a yearly report on algorithms and key sizes [10], and we base our evaluation on this report. We refer to [10] for many more details on this topic.

When studying the security of a key against an attacker who performs a simple brute-force attack, and exhaustive search for the key, the best thing is to get a good model of the nature of the attacker and of the computational resources the attacker is in possession of. An attacker could be a single human being which is trying to "hack" from a single PC, it could be a company doing industrial spionage using hundreds of computers, or to go to an extreme, it could be an intelligence agency with a huge budget and using special-constructed and dedicated hardward to search the key space. The conclusion of ECRYPT is that a 128-bit key provides long-term protection against all these adversaries. A 128-bit key size is a good, generic application-

independent recommendation, and should provide security for at least the next 20 years.

3.2 Differential cryptanalysis

The most general method of analysing conventional cryptosystems today is *differential cryptanalysis*, published by Biham and Shamir in 1990. The method has proved to be relatively efficient and has been applied to a wide range of iterated ciphers see e.g., [2]. Furthermore, it was the first attack which could (theoretically) recover DES keys in time less than the expected cost of exhaustive search [2]. In the following a brief description of differential cryptanalysis with respect to a general n-bit iterated cipher.

First, one defines a *difference* between two bit strings, s and s' of equal length as

$$\Delta s = s \oplus \tilde{s}^{-1}, \tag{1}$$

where $\oplus$ is the group operation on the group of bit strings used to combine the key with the text input in the round function and where t^{-1} is the inverse element of t with respect to $\oplus$. One of the main ideas behind this is, that the differences between the texts before the key is inserted and the difference between the texts after the key is inserted are equal, so the difference is independent of the key through this operation. In a strong encryption algorithm there will be some parts of the cipher where a difference cannot hold with certainty. In a differential attack one exploits that for certain differences in the input to the a particular function, the distribution of output differences of is non-uniform. One defines characteristics [2]:

Definition 1 *An r-round* characteristic *is a series of differences defined as an $r+1$-tuple $\{\alpha_0, \alpha_1, \ldots, \alpha_r\}$, where $\Delta c_0 = \alpha_0$, $\Delta c_i = \alpha_i$ for $1 \leq i \leq r$.*

Define p_i as the probability that inputs of difference α_{i-1} lead to output of difference α_i, where the probability is taken over all choices of the round key and the inputs to the ith round. In [23] the notion of a Markov cipher was introduced. In a Markov cipher this probability is independent of the actual inputs of the round and is calculated over all possible choices of the round key. Also in [23] it was shown that in a Markov cipher if the round keys are independent, the p_i's are also independent and

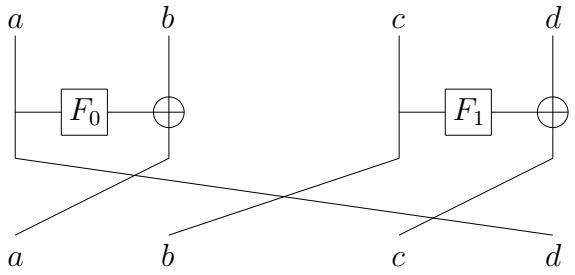
$$\Pr(\Delta c_r = \alpha_r \,|\, \Delta c_0 = \alpha_0) \;=\; \prod_{i=1}^{r} \Pr(\Delta c_i = \alpha_i \,|\, \Delta c_{i-1} = \alpha_{i-1}). \tag{2}$$

3.3 Differential characteristics for CLEFIA

We computed the maximum probabilities over the S-boxes of CLEFIA. From our implementations it follows that the maximum probability of a differential characteristic through S_0 is $10/256$. Also, the maximum probabilities of differentials over S_1 are 2^{-6}.

One of the most efficient ways to build differential characteristics is to identify so-called iterative characteristics over a small number of rounds, which can then be concatenated to cover more rounds. With identical inputs to the functions F_0 and F_1 one gets identical outputs, hence a differential characteristic of probability one can be established. In order to maximise the probability of differential characteristics one often tries to maximise the number of probability-one transitions. Next we examine iterative characteristics.

Consider a 1-round iterative characteristic



$$(a, b, c, d) \xrightarrow{1r} (a, b, c, d),$$

where the differences in the four 32-bit words are a, b, c, respectively d. It follows that it must hold that

$$a = d \text{ and } b = c$$

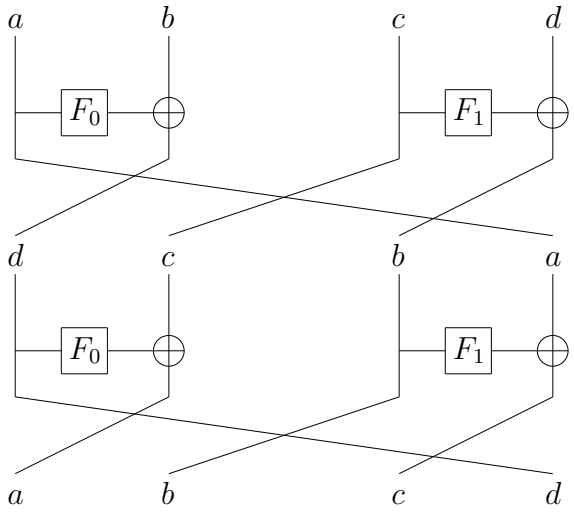
and that $a \xrightarrow{F_0} a \oplus b$ and $b \xrightarrow{F_1} a \oplus b$. Since F_0 and F_1 are bijective mappings, it must further hold that $a \neq 0, b \neq 0$ and $a \neq b$. From these observations and from the properties of F_0 and F_1 it follows that if a has one active S-box, then b has at least three active S-boxes. And if a has two active S-boxes, then b has at least one. Therefore one can conclude that for a one-round iterative characteristic there will be *at least* four active S-boxes per round. Such a characteristic will have a probability of at most $(\frac{10}{256})^2 \approx 2^{-18}$ for one

round. When iterated to 12 rounds this gives a probability of approximately 2^{-216}.

Consider next a 2-round iterative characteristic

$$(a, b, c, d) \xrightarrow{2r} (a, b, c, d),$$

which is depicted here:



It follows from this picture that the following four transitions must occur:

$$a \xrightarrow{F_0} b + d,$$
$$c \xrightarrow{F_1} b + d,$$
$$b \xrightarrow{F_1} a + c,$$
$$d \xrightarrow{F_0} a + c.$$

Also, if one of a, b, c, or d is zero, then the other three will also be zeros. In other words,

$$\text{if } a = 0 \text{ then } (b, c, d) = (0, 0, 0),$$
$$\text{if } b = 0 \text{ then } (a, c, d) = (0, 0, 0),$$
$$\text{if } c = 0 \text{ then } (a, b, d) = (0, 0, 0),$$
$$\text{if } d = 0 \text{ then } (a, b, c) = (0, 0, 0).$$

As an example, if $a = 0$ then $b = d$, which follows from the first transition, since F_0 is a bijection. If $b = d$, then $c = 0$, which follows from the second transition and from the fact that F_1 is a bijection. If $c = 0$, then $b = 0$, which follows from the third transition and it follows that then also $d = 0$.

If all four words are zero, then we have a trivial characteristic over two rounds with equal inputs and equal outputs. Therefore, to be of any use in cryptanalysis all four words must be nonzero. We conjecture, without proof, that the number of active S-boxes in such a 2-round characteristic must be at least six. Such a characteristic will have a probability of at most 2^{-28} for two rounds. When iterated to twelve rounds this gives a probability of at most 2^{-168}. Note that this is a bound and there is no guarantee that one can find such a characteristic.

Extending the above analysis to three rounds is possible but the number of possibilities to examine grows. Instead one can do a computer search for differential characteristics just counting the number of *active* S-boxes. This does not always lead to a real differential characteristic but it gives bounds for the best differential characteristics possible.

This computer search program starts from a number of active S-boxes in each of the four words of the plaintext difference. Then it allows for different transitions through the functions F_0 and F_1. Since the branch number of both these functions is five, with one active S-box in the input, there will be four active S-boxes in the output. With two active S-boxes in the input, there can be three or four active S-boxes in the output. With three active S-boxes in the input, there can be two, three or four active S-boxes in the output. And with four active S-boxes in the input, there can be between one and four active S-boxes in the output. The program tries all possibilities. Also, the xor operation of the right half of the round input and the otuput of the F_i $(i = 0, 1)$ functions can cancel active S-boxes or create new ones. Again, the program tries all possibilities. Our search shows that the number of active S-boxes for any 4-round differential characteristic is at least 6, for any 5-round differential characteristic the number is at least 8, and for any 6-round differential characteristic the number is at least 12. A 6-round differential characteristic will then have a probability of at most $(\frac{10}{256})^{12} \approx 2^{-56}$. When iterated to 12 rounds one gets a probability of at most 2^{-112}. This is low enough to conclude that any attack based on traditional differential characteristic will not be able to cryptanalyse any variant of CLEFIA.

Note that the above 6-round or 12-round characteristics might not exist and if they do they could be hard to find. Next we consider a 3-round

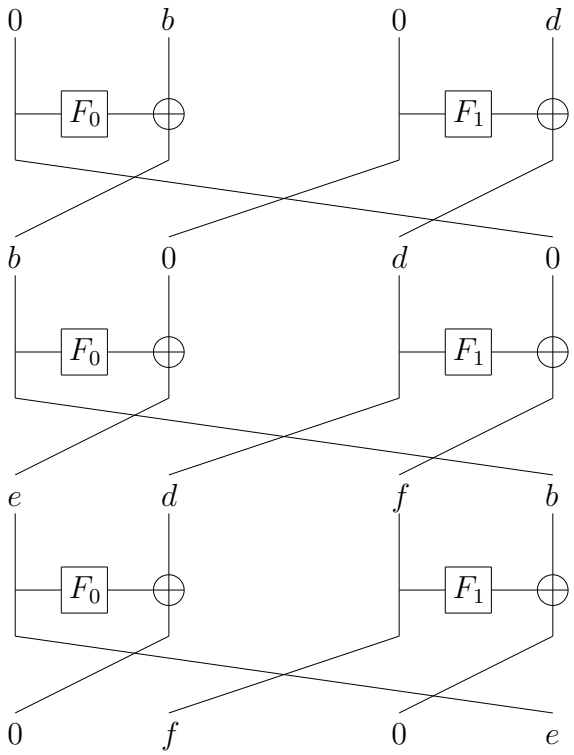


Figure 2: A 3-round differential characteristic.

iterative characteristic

$$(a, b, c, d) \xrightarrow{3r} (a, b, c, d),$$

for which we can easily bound the exact number of active S-boxes. Consider Figure 2.

We have chosen $a = c = 0$. Then, for some values of e and f, if the following transitions hold

$$b \xrightarrow{F_0} e,$$
$$e \xrightarrow{F_0} d,$$
$$d \xrightarrow{F_1} f,$$
$$f \xrightarrow{F_1} b,$$

then one can specify the following 3-round characteristic

$$(0, b, 0, d) \xrightarrow{3r} (0, f, 0, e).$$

This characteristic concatenated to itself yields a six-round iterative characteristic

$$(0, b, 0, d) \xrightarrow{6r} (0, b, 0, d).$$

It follows that to be useful in cryptanalysis both b and d must be nonzero. If $b = 0$, then $e = 0$, but then $d = 0$, and then $f = 0$. Similarly, if $d = 0$, then $f = 0$, but then $b = 0$, and then $e = 0$.

It is rather easy to estimate the number of active S-boxes for the above four transitions. The branch numbers of F_0 and F_1 are both five, so the number of active S-boxes for b and e in unison is five, and five also for d and f in unison. Consequently, there will be *at least* ten active S-boxes in the 3-round characteristic and the probability will be at most $(\frac{10}{256})^{10} \approx 2^{-48}$. When iterated to 12 rounds one gets a probability of at most 2^{-192}.

It is safe to conjecture that there are no useful differential characteristics for any variants of CLEFIA.

3.4 Linear Cryptanalysis

Linear cryptanalysis was proposed by Matsui in 1993 [18]. A preliminary version of the attack on FEAL was described in 1992 [19]. Linear cryptanalysis is a known plaintext attack in which the attacker exploits linear approximations of some bits of the plaintext and ciphertext. In the attack on iterated ciphers the linear approximations are obtained by combining approximations for each round under the assumption of independent round keys. The attacker hopes in this way to find an expression

$$(m \cdot \alpha) = (c \cdot \beta) \tag{3}$$

where α, β are n-bit strings and where '$\cdot$' denotes the dot product, which holds with probability $p \neq \frac{1}{2}$ over all keys, such that $|p - \frac{1}{2}|$, called the bias, is maximal. As in differential cryptanalysis one can define characteristics to be used in linear cryptanalysis. The number of known plaintexts needed such that the relation (3) can be effectively detected is approximately $|p - 1/2|^{-2}$.

We computed the maximum linear probabilities over the S-boxes of CLEFIA. From our implementations it follows that the maximum correlation of

a linear characteristic through S_0 is $(2 \cdot 28/256)^2 \simeq 2^{-4.39}$. [1] Also, the maximum correlations of linear characteristics over S_1 are 2^{-6}.

The detection of linear characteristics is very similar to the detection of differential characteristics. Since the highest correlation through one S-box is very close to the highest probability of a differential characteristic for one S-box ($10/256 \approx 2^{-4.67}$). Therefore, we feel that it is safe to conjecture that there are no useful linear characteristics for any of the variants of CLEFIA.

3.5 Truncated differential cryptanalysis

In some ciphers it is possible and advantageous to predict the values of only parts of the differences after each round of the cipher. Let $\{\alpha_0, \alpha_1, \ldots, \alpha_s\}$, be an s-round *characteristic*. Then $\{\alpha'_0, \alpha'_1, \ldots, \alpha'_s\}$ is called a truncated characteristic, if α'_i is a subsequence of α_i. Truncated characteristics were used to some extent in [2] but only in the outer rounds of a cipher. Note that a truncated characteristic is a collection of characteristics and therefore reminiscent of a differential. A truncated characteristic contains all characteristics $\{\alpha''_0, \alpha''_1, \ldots, \alpha''_s\}$ for which $\mathrm{trunc}(\alpha''_i) = \alpha'_i$, where $\mathrm{trunc}(x)$ is the truncated value of x, where the truncation is not further specified here. The notion of truncated characteristics extends in a natural way to truncated differentials introduced in [13].

We first restrict ourselves to truncated differentials with differences split into four 32-bit words, and the difference in each word is either zero or nonzero. It follows by easy computer simulations, that there is a five-round truncated differential of this type for CLEFIA. With equal values in the first (leftmost), the third and the fourth (rightmost) words, and different values in the second words, one gets that there is always a nonzero difference in the fourth words of the ciphertexts after five rounds of encryption. Consider Figure 3.

It follows that

$$\begin{aligned} b \neq 0 &\Rightarrow c \neq 0, \\ c \neq 0 &\Rightarrow d \neq 0, \text{ and} \\ d \neq 0 &\Rightarrow e \neq 0 \end{aligned}$$

[1] This correlation is defined as $(2(p - \frac{1}{2}))^2$ where $p - \frac{1}{2}$ denotes the bias of the linear approximation

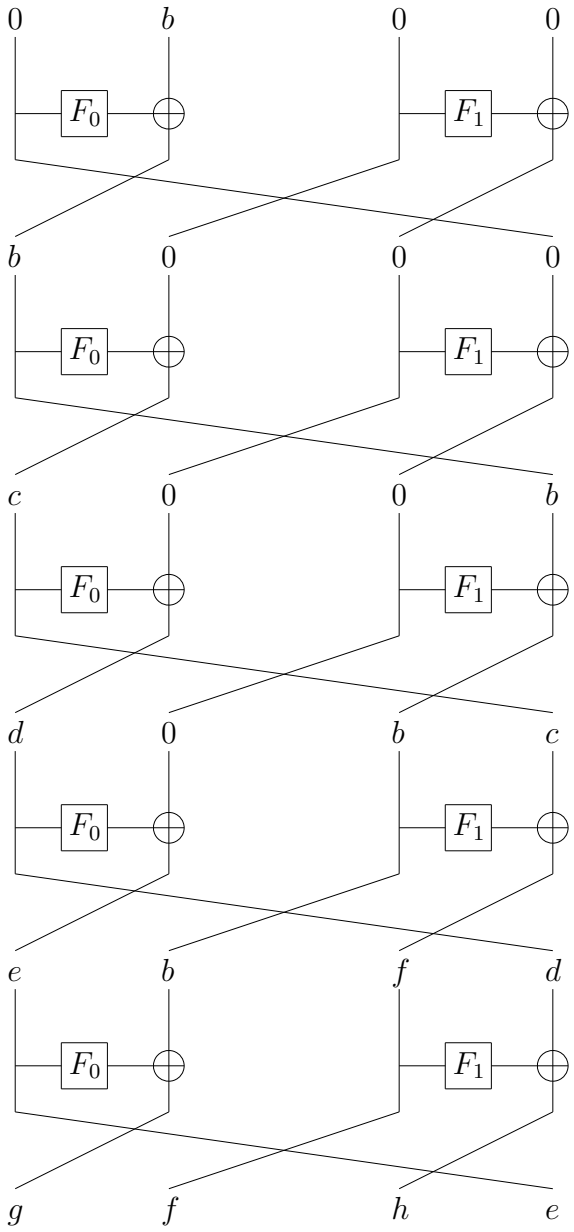


Figure 3: A 5-round truncated differential characteristic, where $b \neq 0$ and $e \neq 0$.

Evidently there is the possibility to split each word into four bytes and considering byte-differences. However, since the four bytes in each 32-bit word are mixed in a strong way via eight-bit S-boxes and MDS-matrices, there is little chance that the above five-round structure can be iterated to more than a few extra rounds. In our opinion it is safe to conclude that for CLEFIA reduced to ten rounds, there are no useful truncated differentials. As as special case of truncated differentials are the so-called *impossible differentials*, which we consider next.

3.6 Impossible differentials

Impossible differentials is another name for differential characteristics of probability zero. These differentials can be used in differential cryptanalysis and are in general as effective as high-probability differentials. However, differentials of very low probability are not trivial to find. One popular method is as follows. Imagine that a cipher can split into two parts, e_0 and e_1. Assume that one can find a differential through e_0, e.g.,

$$\alpha \stackrel{e_0}{\rightarrow} \beta$$

with probability one, and assume that one can find a differential through the inverse of e_1, e.g.,

$$\gamma \stackrel{e_1^{-1}}{\rightarrow} \eta$$

also with probability one. Then if $\beta \neq \eta$ one can establish a differential of probability zero through $e_1 \circ e_0$:

$$\alpha \stackrel{e_1 \circ e_0}{\rightarrow} \gamma$$

of probability zero.

3.6.1 Impossible differentials for CLEFIA

We implemented a search for impossible differentials for CLEFIA, or rather for ciphers with the same structure as CLEFIA, the generalized type-2 transformation. Our tests identify there are impossible differentials over 9 rounds of CLEFIA. Next we explain this phenomenon. Consider the 5-round trun-

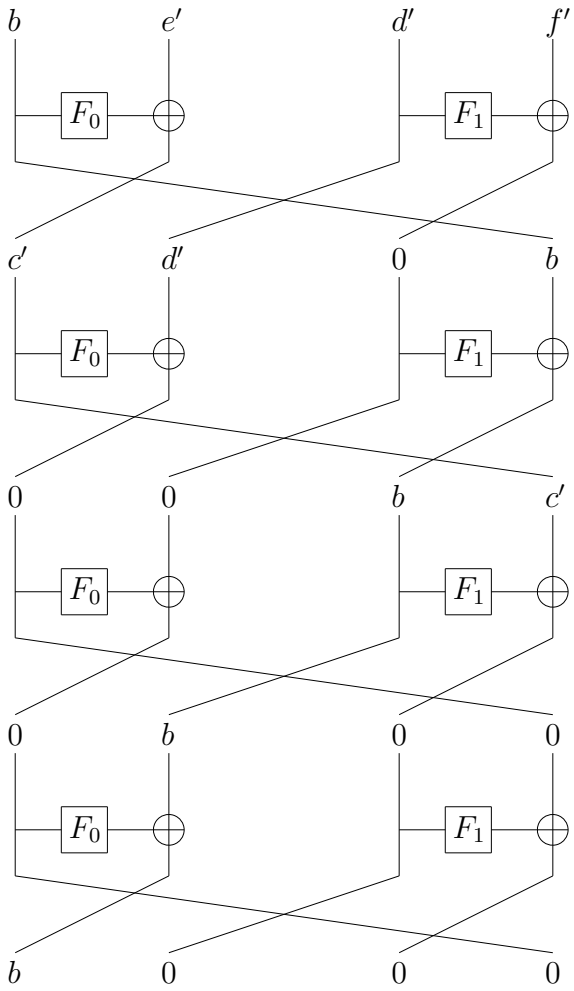


Figure 4: A 4-round truncated differential characteristic for the decryption operation, where $b \neq 0$.

cated differential of Figure 3 and the 4-round truncated differential of Figure 4. If we concatenate the two differentials, we require that

$$\begin{aligned} g &= b, \\ f &= e', \\ h &= d', \text{ and} \\ e &= f'. \end{aligned}$$

Note also, that $b \neq 0$ and $e \neq 0$. Consequently, it must be the case that two inputs to F_0 of nonzero difference e in the fifth round of the differential lead to equal outputs. However, since F_0 is a bijection for a fixed key, this is impossible. Hence the 9-round truncated differential

$$(0, b, 0, 0) \xrightarrow{9r} (b, 0, 0, 0)$$

has probability zero. This confirms the analysis made in [29].

Also, our tests confirm that for 10 rounds (or more) of this structure there are no impossible differentials. We stress that our tests were conducted with randomly chosen bijections (F-functions) in the round functions. Such tests for (real) CLEFIA would require computational resources out of our reach.

The 9-round impossible differentials can be used to recover key material for reduced-round versions of CLEFIA. The best such known attack appears to be the one of [31], which specifies a key-recovery attack for a variant of CLEFIA reduced to 14 rounds with a 128-bit key but where the key-whitening layers have been ignored.

3.7 Integral cryptanalysis

Let S be a multiset of vectors. An integral over S is defined as the sum of all vectors in S. In other words, the integral is

$$\int S = \sum_{v \in S} v,$$

where the summation is defined in terms of a particular group operation, for CLEFIA we consider the exclusive-or operation.

In an attack, one tries to predict the values in the integrals after a certain number of rounds of encryption. For this purpose it is advantageous to

distinguish between the three cases: where all ith words are equal, where all ith words are pairwise distinct, or where all ith words sum to a certain value predicted in advance.

Let us introduce the following symbols for words in an integral. For a first-order integral, the symbol '$\mathcal{C}$' (for "Constant") in the ith entry, means that the values of all ith words in the collection of texts are equal. The symbol '$\mathcal{A}$' (for "All") means that all words in the collection of texts are different, and the symbol '$\mathcal{B}$' (for "Balanced") means that the exclusive-or sum of all ith words is zero. Finally, we will write '?' when the sum of words can not be predicted. For more details, please consult [14].

3.7.1 Integrals for CLEFIA

We have identified a structure which can be used to distinguish CLEFIA from a randomly chosen permutation after eight rounds of encryption. The structure can be used in a key-recovery attack on CLEFIA reduced to nine and ten rounds of encryption.

There is the following six-round integral with 2^{32} texts

$$(\mathcal{C}, \mathcal{A}, \mathcal{C}, \mathcal{C}) \stackrel{6R}{\rightarrow} (\,?\,,\,?\,,\,?\,, \mathcal{B}),$$

where each symbol is indicating the values of particular 32-bit words. The round transitions are as follows:

$$\begin{aligned}
(\mathcal{C}, \mathcal{A}, \mathcal{C}, \mathcal{C}) &\stackrel{1r}{\rightarrow} (\mathcal{A}, \mathcal{C}, \mathcal{C}, \mathcal{C}) \\
&\stackrel{1r}{\rightarrow} (\mathcal{A}, \mathcal{C}, \mathcal{C}, \mathcal{A}) \\
&\stackrel{1r}{\rightarrow} (\mathcal{A}, \mathcal{C}, \mathcal{A}, \mathcal{A}) \\
&\stackrel{1r}{\rightarrow} (\mathcal{A}, \mathcal{A}, \mathcal{B}, \mathcal{A}) \\
&\stackrel{1r}{\rightarrow} (\mathcal{B}, \mathcal{B},\,?\,, \mathcal{A}) \\
&\stackrel{1r}{\rightarrow} (\,?\,,\,?\,,\,?\,, \mathcal{B})
\end{aligned}$$

This integral can be used to construct a seven-round integral with 2^{64} chosen plaintexts, which holds with probability one. Note that the rightmost and 2nd rightmost words of the inputs to one round map to the 2nd leftmost and 2nd rightmost words of the inputs to the following round. Consider a structure of 2^{64} chosen plaintexts which have constant values in the two leftmost words but which are pairwise different in the remaining 64 bits. Then

after one round of encryption one has a structure of 2^{64} chosen plaintexts which have constant values in leftmost and rightmost words but are pairwise different in the middle 64 bits. Thus this structure contains 2^{32} structures of each 2^{32} texts, and each such structure forms an integral with notation $(\mathcal{C}, \mathcal{A}, \mathcal{C}, \mathcal{C})$. Since the texts in each of these structures are balanced in the rightmost words after six rounds of encryption, so is the sum of all 2^{32} structures. Thus there is a 7-round integral of the form

$$(\mathcal{C}, \mathcal{C}, \mathcal{A}, \mathcal{A}) \stackrel{7R}{\rightarrow} (\,?\,,\,?\,,\,?\,, \mathcal{B}).$$

Using similar arguments one can show that there is an eight-round integral for CLEFIA which requires 2^{96} chosen plaintexts and which holds with probability one. It has the notation

$$(\mathcal{A}, \mathcal{C}, \mathcal{A}, \mathcal{A}) \stackrel{8R}{\rightarrow} (\,?\,,\,?\,,\,?\,, \mathcal{B}).$$

This structure can be used in a key-recovery attack on CLEFIA reduced to nine rounds of encryption. The attack requires a structure of 2^{96} chosen plaintexts and a running time of 2^{96} simple operations and finds 32 bits of the secret subkeys.

Attack on 9-round CLEFIA. The attack is constructed as follows.

1. Construct a set of 2^{96} chosen, different plaintexts x_i for $i = 1, \ldots, 2^{96}$, such that these texts have equal values in the second leftmost 32-bit word. Request the encryptions, y_i of x_i for $i = 1, \ldots, 2^{96}$.

2. Compute the exclusive-or of the rightmost 32-bit words of all y_is. Name this sum Y.

3. Count the frequencies of the values in the second rightmost 32-bit words of all ciphertexts. Make a list, L, of those 32-bit values which have odd frequencies. (Since we are computing exclusive-or sums of all words, those which occur an even number of times will cancel out).

4. For all values, t, of the last-round subkey rk_{2r-1}, here $r = 9$, do the following:

   (a) Compute the exclusive-or, Z, of the values $F_1(t, z)$ for all values $z \in L$.

(b) If $Z = Y$, then t is a candidate value for rk_{2r-1}. If $Z \neq Y$, then t is not the correct value for rk_{2r-1}.

Note that for the correct value of rk_{2r-1} one gets $Z = Y$, since the integral promises that the exclusive-or of the fourth words after eight rounds is zero. For an incorrect value of rk_{2r-1} we assume that one gets $Z = Y$ only with a probability of 2^{-32}. If more than one value of rk_{2r-1} remains after the above procedure, the attack can be repeated on another structure of 2^{96} plaintexts. Note that in step three above, we need not consider values of z which occur an even number of times, since the exclusive-or of these results through F_1 is zero.

The attack can be extended to CLEFIA reduced to ten rounds which finds 64 bits of the subkeys.

Attack on 10-round CLEFIA. The attack goes as follows.

1. Construct a set of 2^{96} chosen, different plaintexts x_i for $i = 1, \ldots, 2^{96}$, such that these texts have equal values in the second leftmost 32-bit word. Request the encryptions, y_i of x_i for $i = 1, \ldots, 2^{96}$.

2. Compute the exclusive-or, Y, of the rightmost 32-bit words of all y_is.

3. For all values, t_1, of the last-round subkey rk_{2r-2}, and for all values, t_2, of the subkey $wk_2 \oplus rk_{2r-3}$, here $r = 10$, do the following:

   (a) For each ciphertext $c_i = (c_{i,0}, c_{i,1}, c_{i,2}, c_{i,3})$ compute

   $$Z_i = F_0(rk_{2r-1}, c_{i,0}) \oplus c_{i,1},$$

   then compute

   $$Y_i = F_1(rk_{2r-3}, Z_i) \oplus c_{i,2}.$$

   Compute the exclusive-or of all Y_i, $Y = \sum_i Y_i$.

   (b) If $Y = 0$, then (t_1, t_2) are candidate values for rk_{2r-2}, and $wk_2 \oplus rk_{2r-3}$. If $Y \neq 0$, then (t_1, t_2) are not the correct values for rk_{2r-2}, and $wk_2 \oplus rk_{2r-3}$.

Each incorrect 64-bit value (t_1, t_2) will be a candidate value with a probability of 2^{-32}. Therefore the attack needs to be repeated at least once with a different set of chosen plaintexts. This attack finds 64 bits of information about the round keys. Note that for each key guess (64 bits) one needs to do

at most 2^{32} evaluations of F_0 and 2^{32} evaluations of F_1, and thus the overall complexity is close to 2^{128} evaluations of the function F.

In an extension to 11 rounds of CLEFIA, it appears that one has to guess on five subkeys of each 32 bits. Given the large amount of chosen plaintexts needed in this attack, such an attack is completely out of reach for even the most powerful attackers.

3.8 Higher order differential cryptanalysis

In [16] a definition of higher order derivatives of discrete functions was given. Later higher order differentials were used to cryptanalyse ciphers presumably secure against conventional differential attacks [13] and further developed in [11].

A dth order differential is a collection of 2^d (first-order) differentials. The main idea in the higher order differential attack is the fact that a dth order differential of a function of nonlinear order d is a constant. Consequently, a $d+1$st order differential of the function is zero. Assume that (a subset of) the output bits of the reduced cipher are expressible as a low-degree polynomial $p(x) \in GF(2)[x_1, x_2, \ldots, x_i]$, where $x_1, x_2, \ldots, x_i$ is a subset of input bits to the reduced cipher. If this polynomial has degree not higher than d, then

$$\sum_{x \in \mathcal{L}_d} p(x) = c,$$

where $\mathcal{L}_d$ denotes a d-dimensional subspace of $GF(2)^n$ and c a constant. This method was applied to the cipher example given in [22]. This cipher is "provably secure" against a differential attack but can be broken in a higher order differential attack with relatively low complexity.

3.8.1 Higher order differentials for CLEFIA

The success of attacks based on higher order differentials depends on the algebraic degrees of the nonlinear components in the cipher. The algebraic degrees of the bijective four-bit S-boxes, SS_i, are three, thus the algebraic degree of S_0 is at most six. For comparison, a randomly chosen, invertible eight to eight bit S-box has algebraic degree seven with high probability. We found no indication that the algebraic degree of six for S_0 is a weakness for CLEFIA. The algebraic degree of S_1 is seven. The two S-boxes used are both

8-bit bijections. It is known that seven is the maximum attainable algebraic degree for bijective eight-bit S-boxes.

It is not clear how the degrees will grow with the number of rounds in CLEFIA, but it appears that with 18 rounds of encryption it is extremely unlikely that attacks based on higher order differentials will prove successful.

3.8.2 Boomerang attack

The boomerang attack is a special case of a second-order differential. The boomerangs are effective in particular for ciphers for which a subpart (e.g., half) of the cipher has high-probability differentials. The penalty in the boomerang attack is the requirement for four differential paths throughout the particular subparts of the cipher. The very conservative estimates of differential probabilities are already low enough to conclude that the boomerang attack will not be superior to a classical differential attack.

The amplified boomerang attack and the rectangle attack are variants of the boomerang attack and we are convinced that these attacks are no threat for CLEFIA with the specified number of rounds.

3.9 Interpolation cryptanalysis

In [11] the interpolation attack was introduced based on the following well-known formula. Let R be a field. Given $2n$ elements $x_1, \ldots, x_n$, $y_1, \ldots, y_n \in R$, where the x_is are distinct. Define

$$f(x) = \sum_{i=1}^{n} y_i \prod_{1 \le j \le n, j \ne i} \frac{x - x_j}{x_i - x_j}. \tag{4}$$

$f(x)$ is the only polynomial over R of degree at most $n-1$ such that $f(x_i) = y_i$ for $i = 1, \ldots, n$. Equation (4) is known as the *Lagrange interpolation formula*.

In the interpolation attack an attacker constructs polynomials using inputs and outputs of the reduced cipher. This is particularly easy if the components in the cipher can be easily expressed as mathematical functions. The idea in the attack is, that if the constructed polynomials have a small degree, only few plaintexts and their corresponding ciphertexts are necessary to solve for the (key-dependent) coefficients of the polynomial. In an extended version of the attack meet-in-middle techniques are used to further reduce the degrees of the used polynomials [11].

The interpolation attacks are reminiscent of attacks based on higher order differentials and are effective mostly on ciphers for which all components can be written as polynomials in the inputs with few coefficients. Since this is clearly not the case for the S-boxes used in CLEFIA, there is no reason to believe that the interpolation attack is applicable to more than a few number of rounds of CLEFIA.

3.10 Algebraic cryptanalysis

The XL [7] and XSL [8] cryptanalytic attacks and variations of these are often also referred to as "algebraic attacks". Here one writes polynomial expressions in the inputs and outputs of each round of a cipher, then tries to solve these to find the secret key. The complexity of such an attack grows with the number of nonlinear components in the cipher. These methods are surrounded by controversy although there seems to be consensus that the XL method has some merit [6, 9, 17].

Here we first investigate algebraic expressions over the S-boxes in CLEFIA. The 8×8-bit S-box S_0 is constructed from four 4×4-bit S-boxes

$$SS_0, SS_1, SS_2, SS_3.$$

Let x be an eight-bit input, then the eight-bit output is computed as follows, where an eight-bit word, a, is divided into two four-bit words a_0 and a_1, cf. [28].

$$\begin{aligned} w &:= SS_0(x_0) \mid SS_1(x_1), \\ v &:= L(w_0, w_1), \\ y &:= SS_2(v_0) \mid SS_3(v_1), \end{aligned}$$

where L is a linear transformation. First of all, it has been confirmed that there are no deterministic relations of degrees maximum two in the bits of the input x and the bits of the output y of S_0. However, it is nonetheless possible to establish a set of equations of degree at most two over S_0. It is well-known that there are *at least* 21 deterministic relations of degrees maximum two in the bits of the input and output of a four to four bit S-box. This follows from the fact that from the constant one and from the eight bit variables one can form 37 terms of degrees at most two. There are one term of degree zero, eight terms of degree one and $\binom{8}{2} = 28$ terms of degree 2. Since there

are only 16 pairs of input and output over the S-box, one can establish 16 equations in 37 unknowns and the result follows. It was confirmed that for all four S-boxes SS_i there are exactly 21 quadratic equations in the input and output bits.

Therefore there are 21 quadratic equations over the bits in x_0 and w_0 and 21 quadratic equations over the bits in x_1 and w_1. Similarly there are 21 quadratic equations over the bits in y_0 and v_0 and 21 quadratic equations over the bits in y_1 and v_1. In total, one can establish a set of 84 quadratic equations in 24 bits, the eight bits of x, y, and v. Note that the bits of w and v are related by linear equations.

Also, it has been confirmed that there are 39 deterministic relations of degrees two in the input bits and output bits of S_1.

Algebraic attacks on block ciphers are surrounded by controversy and no real-life ciphers have yet been proved to be vulnerable to such an approach. For CLEFIA with 18 rounds, a total of 144 S-boxes are used. The Advanced Encryption Standard uses a total of 144 S-boxes in nine rounds of encryption. One might expect that the complexity of an algebraic attack on 18-round CLEFIA is similar to the complexity of an algebraic attack on 9-round AES [25].

Thus, it is safe to conclude that a breakthrough in algebraic cryptanalysis of CLEFIA also would mean a breakthrough in algebraic cryptanalysis of the AES. And it seems that an algebraic attack on AES is very far from being a realistic threat.

3.11 The key scheduling algorithm

The key schedules of the most popular ciphers can be categorised as follows.

1. Linear key schedules. These are where the round keys or subkeys are derived as affine transformations of the main key. Examples include the key schedules of DES [21] and KASUMI [1].

2. Non-linear key schedules. These are where the round keys or subkeys are generated as (simple) non-linear transformations of the main key. A prominent example is the key schedules of AES [20].

3. Complex key schedules. These are where the round keys or subkeys are generated as a complex, non-linear transformations of the main

key. Examples include the key schedules of RC5 [26] and CLEFIA among many others.

Here we describe briefly the 128-bit key schedule of CLEFIA. The user-selected key is denoted K. The whitening keys and the round keys are derived from a number of 128-bit values, denoted here by A_i.

First a derived key L is obtained, which is 128-bit value computed as the encryption of K in a 12-round cipher with a chosen constant as the key.

Then

$$\begin{aligned} A_0 &= K, \\ A_1 &= L \oplus C_1, \end{aligned}$$

and the rest of the values are computed as follows:

$$\begin{aligned} A_{2i} &= \Sigma^{2i-1}(L) \oplus K \oplus C_{2i}, \\ A_{2i+1} &= \Sigma^{2i}(L) \oplus C_{2i+1} \end{aligned}$$

for $i = 1, \ldots, 4$, where C_j are the constants defined in the key schedule. Σ is a bit permutation, which consists of two swaps ("The DoubleSwap Function").

3.11.1 Weak keys

For some ciphers there is a, usually small, subclass of keys which can be regarded *weak* as compared to other keys. E.g., in the Data Encryption Standard, DES, four values of the key have been identified for which the encryption operation equals the decryption operation, and it is not recommended to use these values with DES.

For CLEFIA we did identify pairs of keys for which many of the corresponding subkeys are related. We illustrate our findings on the 128-bit key version of CLEFIA, the key-schedules for the other key sizes have similar properties. The user-selected key K of 128 bits is encrypted (using constants as encryption keys) to generate a 2nd key L, also of 128 bits. The encryption used is invertible, such that given L, one can find a unique value of K. The 36 subkeys rk_i for $i = 0, \ldots, 35$ each of 32 bits and the four whitening keys wk_j for $j = 0, \ldots, 3$ each of 32 bits are generated from K and L, such that

wk_j depend only on K, rk_i for $i = 8k, \ldots, 8k+3$ depend only on L, and rk_i for $i = 8k+4, \ldots, 8k+7$ depend on both K and L, where $k \geq 0$.

Consider the value of K for which $L = 0$, let us call this value K_0. In this case, it follows that for $i = 0, \ldots, 4$:

$$\begin{aligned} A_{2i} &= K_0 \oplus C_{2i}, \\ A_{2i+1} &= C_{2i+1}, \end{aligned}$$

where C_j are the constants defined in the key schedule. Another example, is the value of K, say K_1, for which $L = \mathbf{1}$, meaning the string consisting of 128 1-bits.

In this case, it follows that for $i = 0, \ldots, 4$:

$$\begin{aligned} \tilde{A}_{2i} &= K_1 \oplus \overline{C_{2i}}, \\ \tilde{A}_{2i+1} &= \overline{C_{2i+1}}, \end{aligned}$$

Consequently, if one considers the exclusive-or of all A_i keys for the two keys K_0 and K_1 one gets a series of values $X_i = A_i \oplus \tilde{A}_i$:

$$\begin{aligned} X_{2i} &= K_0 \oplus K_1 \oplus \mathbf{1}, \\ X_{2i+1} &= \mathbf{1}, \end{aligned}$$

where $\mathbf{1}$ is the string of 128 1-bits. We found no reason to discourage the use of these keys for CLEFIA used for encryption.

Consider further two keys K and K' and the corresponding derived keys L and L'. Imagine that L and L' are different in s bits, in other words, the Hamming distance between the two strings is s. L and L' are both transformed using DoubleSwap a total of eight times. It follows that the Hamming distances of L and L' after each of these tranformations remain s. Thus if s is small, this means that all subkeys which depend on only L and L' have a small Hamming distance. The Hamming distances in all other subkeys on the other hand are expected to look random. We have found no way of exploiting these properties of related keys and they are not likely to pose a problem for CLEFIA when used for encryption.

Finally we report on a related-key property involving more than two keys. Consider the four pairwise, different keys K_0, K_1, K_2, K_3, where $K_0 \oplus K_1 \oplus$

$K_2 \oplus K_3 = 0$. Also, assume that the derived keys L_0, L_1, L_2, L_3 have the similar property that $L_0 \oplus L_1 \oplus L_2 \oplus L_3 = 0$. Consider the four whitening keys wk_0 for the four keys. It follows that the exclusive-or of these keys is zero. A similar property holds for any of the whitening keys and for any of the 32-bit round keys (rk_i). As an example, the key words $rk_{12}, rk_{13}, rk_{14}, rk_{15}$ are derived from $\sigma^3(L) \oplus K$ plus some constants. But

$$\begin{aligned} \sigma^3(L_0) \oplus K_0 \oplus \sigma^3(L_1) \oplus K_1 \oplus \sigma^3(L_2) \oplus K_2 \oplus \sigma^3(L_3) \oplus K_3 &= \\ \sum_{i=0}^{3} \sigma^3(L_i) \oplus \sum_{i=0}^{3} K_i &= 0. \end{aligned}$$

Note that the constants in the key-schedule cancel out above. Also note that similar properties hold for sets of any even number of keys. One can find such sets of 2^j keys efficiently for larger values of j using the techniques developed in [30]. However it is clear that for encryption such sets of keys are not likely to be used in practice and we have found no way of exploiting these properties of related keys and they are not likely to pose a problem for CLEFIA.

One possible drawback of the key scheduling algorithm is the use of many different constants, which must be stored or generated on the fly.

3.11.2 Related key attacks

There are several variants of this attack depending on how powerful the attacker is assumed to be.

1. Attacker gets encryptions under one key.
2. Attacker gets encryptions under several keys.
   (a) Known relation between keys.
   (b) Chosen relation between keys.

The concept of related-key attacks is from [3]. Later, related key attacks were reported on several other block ciphers [12] and latest a series of papers regarding the AES [4, 5].

Attacks based on related keys are regarded by some as impractical, since often it is required that an attacker can obtain the encryption of many chosen plaintexts, sometimes encrypted using many different, related keys. Usually

in cryptanalytic attacks on block ciphers it is assumed that the key is secret and that it is chosen uniformly at random. For the attacks of 2b above it is clear that this assumption can no longer be used. Nonetheless, many block ciphers are designed to (try to) avoid these attacks and the cryptographic community seems to support related-key attack results.

We have examined the key scheduling algorithm of CLEFIA, but found no evidence that this enables efficient related-key attack of any type. The above findings illustrate that there are collection of keys for which one can easily predict the relations between many subkeys. However, keys used for encryption should be chosen uniformly at random, and even if one allows for an attacker to choose an offset, say α, and get encryption under the keys k and $k \oplus \alpha$, the L-values are likely to be highly unpredictable and thus the relations between the subkeys for k and $k \oplus \alpha$ are likely to look random. Therefore, related-key attacks seem to be extremely hard to mount on CLEFIA.

3.12 Known key security

The known-key security concept was introduced in [15]. In this scenario it is assumed that the key is known and the task of the attacker is to find some "statistical weakness" in the block cipher using the particular key.

Consider the integral of Section 3.7.1.

$$\begin{aligned}
(\mathcal{C},\mathcal{A},\mathcal{C},\mathcal{C}) &\stackrel{1r}{\rightarrow} (\mathcal{A},\mathcal{C},\mathcal{C},\mathcal{C}) \\
&\stackrel{1r}{\rightarrow} (\mathcal{A},\mathcal{C},\mathcal{C},\mathcal{A}) \\
&\stackrel{1r}{\rightarrow} (\mathcal{A},\mathcal{C},\mathcal{A},\mathcal{A}) \\
&\stackrel{1r}{\rightarrow} (\mathcal{A},\mathcal{A},\mathcal{B},\mathcal{A}) \\
&\stackrel{1r}{\rightarrow} (\mathcal{B},\mathcal{B},?,\mathcal{A}) \\
&\stackrel{1r}{\rightarrow} (?,?,?,\mathcal{B})
\end{aligned}$$

This specifies that for a set of texts all different in the second words but with equal values in all other words, the exclusive-or of the rightmost ciphertext words after six rounds of encryption is zero.

One can also specify integrals through the decryption operation. It follows by easy calculations that the following integral through the decryption rounds

can be established.

$$\begin{aligned}(\mathcal{C},\mathcal{C},\mathcal{A},\mathcal{C}) &\overset{1r^{-1}}{\rightarrow} (\mathcal{A},\mathcal{C},\mathcal{C},\mathcal{A})\\ &\overset{1r^{-1}}{\rightarrow} (\mathcal{A},\mathcal{A},\mathcal{A},\mathcal{C})\\ &\overset{1r^{-1}}{\rightarrow} (\mathcal{A},\mathcal{A},\mathcal{B},\mathcal{A})\\ &\overset{1r^{-1}}{\rightarrow} (\,?\,,\mathcal{A},\mathcal{B},\mathcal{B})\\ &\overset{1r^{-1}}{\rightarrow} (\,?\,,\,?\,,\mathcal{B},\,?\,)\end{aligned}$$

When the key is known one can combine the two integrals and specify an 11-round integral

$$\begin{aligned}(\,?\,,\,?\,,\mathcal{B},\,?\,) &\overset{5r}{\rightarrow} (\mathcal{C},\mathcal{A},\mathcal{C},\mathcal{C})\\ &\overset{6r}{\rightarrow} (\,?\,,\,?\,,\,?\,,\mathcal{B})\end{aligned}$$

Note that after the first five rounds the halves are swapped, which is the reason why the above 5-round decryption integral is not identical to the first five rounds of the 11-round integeral. The existence of the 11-round integral means that if one knows the value of the key one can find a set of 2^{32} texts such that the second rightmost words of the plaintexts and the rightmost words of the ciphertexts are balanced. The time to find this set of texts is equivalent to doing 2^{32} evaluations of the cipher with a fixed key. If one has (oracle) access to a "randomly chosen" 128-bit bijection, then it is not too difficult to find a set of 2^{32} inputs such that the rightmost words of both inputs and outputs are balanced. If one considers one call to the oracle access as computationally equivalent to one encryption of the block cipher (for a fixed key), then the complexity is close to 2^{32} but very likely strictly larger than 2^{32}. So the 11-round integral is a distinguisher for the block cipher used with a fixed key. One can get stronger distinguishers for fewer rounds of the cipher by considering fewer rounds of the above integral. Also one can possibly extend the distinguishers to one additional round by considering integrals with 2^{64} or 2^{96} texts, but the relevance of such known-key distinguishers can be discussed and one is nowhere near a distinguisher on the full 18-round CLEFIA.

3.13 The overall structure

The high-level structure of CLEFIA is well-known as a generalised Feistel type construction. Also, this structure was used in the design of the block

cipher RC6 [27]. This structure appears to be sound and no important weaknesses are known for it.

3.13.1 The diffusion matrices

The matrices M_0 and M_1 are similar in nature to the diffusion matrices of the AES and have they same strong properties. No (serious) weakness is known for these constructions.

3.14 The number of rounds

The strongest on reduced-round variants of CLEFIA seems to be the ones based on impossible differentials. There are impossible differentials for CLEFIA reduced to up to nine rounds, but not for more than nine rounds. Let d denote the maximum number of rounds for which effective attacks exist for a block cipher. It is a well-known principle to choose the number of rounds in block ciphers well over d, one straight-forward, known rule of thumb is to choose $2d$ rounds. Since CLEFIA seems to be a very secure cipher when used with 18 rounds and at the same fast in implementation, we feel that this choice is justified. Adding four more rounds for the 192-bit key version and another four rounds for the 256-bit key version are natural choices and in correspondence with the choice made for the Advanced Encryption Standard (AES), where two rounds are added, and one round of AES has a similar complexity to two rounds of CLEFIA. Note that one round of CLEFIA modifies only half the block, while one round of the AES modifies the whole block.

3.15 Implementation aspects

The round function in CLEFIA bears some resemblance with the round function of the AES. From the latter it is known that the use eight-bit S-boxes together with the diffusion matrices allow for fast implementation in software. A similar technique can been used in the implementation of CLEFIA. As a result one gets a compact and fast implementation of CLEFIA in software. One point to mention is that an implementation on a 64-bit architecture does not seem to provide a significant speed-up compared to an implementation on a 32-bit architecture.