# Low Probability Differentials and the Cryptanalysis of Full-Round CLEFIA-128

Sareh Emami[2], San Ling[1], Ivica Nikolić[1⋆], Josef Pieprzyk[3] and Huaxiong Wang[1]

[1] Nanyang Technological University, Singapore
[2] Macquarie University, Australia
[3] Queensland University of Technology, Australia

**Abstract.** So far, low probability differentials for the key schedule of block ciphers have been used as a straightforward proof of security against related-key differential analysis. To achieve resistance, it is believed that for cipher with $k$-bit key it suffices the upper bound on the probability to be $2^{-k}$. Surprisingly, we show that this reasonable assumption is incorrect, and the probability should be (much) lower than $2^{-k}$. Our counter example is a related-key differential analysis of the well established block cipher `CLEFIA-128`. We show that although the key schedule of `CLEFIA-128` prevents differentials with a probability higher than $2^{-128}$, the linear part of the key schedule that produces the round keys, and the Feistel structure of the cipher, allow to exploit particularly chosen differentials with a probability as low as $2^{-128}$. `CLEFIA-128` has $2^{14}$ such differentials, which translate to $2^{14}$ pairs of weak keys. The probability of each differential is too low, but the weak keys have a special structure which allows with a divide-and-conquer approach to gain an advantage of $2^{7}$ over generic analysis. We exploit the advantage and give a membership test for the weak-key class and provide analysis of the hashing modes. The proposed analysis has been tested with computer experiments on small-scale variants of `CLEFIA-128`. Our results do not threaten the practical use of `CLEFIA`.

**Keywords:** CLEFIA, cryptanalysis, weak keys, CRYPTREC, differentials

## 1 Introduction

CLEFIA [13] is a block cipher designed by Sony. It is advertised as a fast encryption algorithm in both software and hardware and it is claimed to be highly secure. The efficiency comes from the generalized Feistel structure and the byte orientation of the algorithm. The security is based on the

⋆ The researcher is supported by the Singapore National Research Foundation Fellowship 2012 NRF-NRFF2012-06.

novel technique called Diffusion Switching Mechanism, which increases resistance against linear and differential attacks, in both single and related-key models. These and several other attractive features of `CLEFIA-128` have been widely recognized, and the cipher has been submitted for standardization (and already standardized) by several bodies: CLEFIA was submitted to IETF (Internet Engineering Task Force) [1], it is on the Candidate Recommended Ciphers List[4] of CRYPTREC (Japanese government standardization body), and it is one of the only two[5] lightweight block ciphers recommended by the ISO/IEC standard [8].

A significant body of analysis papers has been published on the round-reduced versions of CLEFIA [18, 19, 14, 17, 15, 10, 16, 9, 6], all for the single-key model, but the analysis based on related keys is missing. Often this type of analysis can cover a higher number of rounds but requires the cipher to have a relatively simple and almost linear key schedule. CLEFIA, however, has a highly non-linear key schedule, equivalent roughly to 2/3 of the state transformation and designed with an intention to make the cipher resistant against analysis based on related-key differentials. Using a widely accepted approach, the designers have proved that no such analysis could exist as the key schedule has only low probability ($\leq 2^{-128}$ for CLEFIA with 128-bit keys) differential characteristics. Note, we will not try to exploit the fact that some characteristics can be grouped into a differential that has a much higher probability than the individual characteristics. Our results go a step further and we show that key schedule differentials with a probability as low as $2^{-128}$, can still be used in analysis. This happens when they have a special structure, namely, the input/output differences of the differentials are not completely random, but belong to a set that, as in the case of `CLEFIA-128`, is described with a linear relation.

We exploit the special form of the key schedule: a large number of non-linear transformations at the beginning of the key schedule is followed by light linear transformations that are used to produce the round keys. In the submission paper of `CLEFIA-128`, the proof of related-key security is based only on the non-linear part as this part guarantees that the probability of any output difference is $2^{-128}$. In contrast, our analysis exploits the linear part and we show that there are $2^{14}$ of the above low probability differences which, when supplied to the linear part, produce a special type of iterative round key differences. `CLEFIA-128` is a Feistel cipher and, as shown in [5], iterative round key differences lead to an

[4] This is the final stage of evaluation, before becoming CRYPTREC standard.

[5] The second one is PRESENT [7].

iterative differential characteristic in the state that holds with probability 1. Therefore we obtain related-key differentials with probability 1 in the state and $2^{-128}$ in the key schedule. The low probability ($2^{-128}$) of each of the $2^{14}$ iterative round key differences means that for each of them there is only one pair of keys that produces such differences, or in total $2^{14}$ pairs for all of them – these pairs form the weak-key class of the cipher. When we target each pair independently, we cannot exploit the differentials. However, the whole set of $2^{14}$ pairs has a special structure and we can target independently two smaller sets of sizes $2^7$ and thus obtain the advantage of $2^7$ over generic analysis. As we will see in the paper, the special structure of the weak key class is due to the linear part of the key schedule, therefore we exploit the weakness of this part twice (the first time for producing iterative round key differences).

We further analyze the impact of the $2^{14}$ pairs of keys and the advantage of $2^7$ that we gain over generic analysis. First we show that `CLEFIA-128` instantiated with any pair of weak keys can be analyzed, namely we present a membership test for the weak class. Next, for the hashing mode of `CLEFIA-128`, i.e. when the cipher is used in single-block-length hash constructions, we show that differential multicollisions [4] can be produced with a complexity lower than for an ideal cipher.

The paper is organized as follows. We start with a description of `CLEFIA-128` given in Section 2. We present the main results related to the analysis of the key schedule and the production of the class of $2^{14}$ pairs of weak-keys in Section 3. The differential membership test is given in Section 4. We present the analysis of the hashing mode of the cipher in Section 5 and in Section 6 we conclude the paper.

## 2 Description of `CLEFIA-128`

`CLEFIA` is a 128-bit cipher that supports 128, 192, and 256-bit keys. We analyze `CLEFIA` with 128-bit keys that is referred as `CLEFIA-128`. Before we define the cipher, we would like to make an important note. To simplify the presentation, we consider `CLEFIA-128` without whitening keys [6]. Our analysis applies to the original `CLEFIA-128` as shown in Appendix B. We proceed now with a brief description of `CLEFIA-128`. It is an 18-round four-branch Feistel (see Fig. 3 of Appendix A) that updates two words per round. A definition of the state update function is irrelevant to our

[6] There are four whitening keys: two are added to the plaintext, and two to the ciphertext.

analysis (see [13] for a full description) and further we focus on the key schedule only.

A 128-bit master key $K$ is input to a 12-round Feistel $GFN_{4,12}$(with the same round function as the one in the state, refer to Fig. 3 of Appendix A) resulting in a 128-bit intermediate key $L$. All the 36 round keys[7] $RK_i, i = 0, \ldots, 35$ are produced by applying a linear transformation to the master key $K$ and the intermediate key $L$ as shown below ($\oplus$ stands for the XOR operation and $||$ is concatenation):

$$
\begin{aligned}
&RK_0||RK_1||RK_2||RK_3 && \leftarrow L && \oplus S_1,\\
&RK_4||RK_5||RK_6||RK_7 && \leftarrow \Sigma(L) \oplus K && \oplus S_2,\\
&RK_8||RK_9||RK_{10}||RK_{11} && \leftarrow \Sigma^2(L) && \oplus S_3,\\
&RK_{12}||RK_{13}||RK_{14}||RK_{15} && \leftarrow \Sigma^3(L) \oplus K && \oplus S_4,\\
&RK_{16}||RK_{17}||RK_{18}||RK_{19} && \leftarrow \Sigma^4(L) && \oplus S_5,\\
&RK_{20}||RK_{21}||RK_{22}||RK_{23} && \leftarrow \Sigma^5(L) \oplus K && \oplus S_6,\\
&RK_{24}||RK_{25}||RK_{26}||RK_{27} && \leftarrow \Sigma^6(L) && \oplus S_7,\\
&RK_{28}||RK_{29}||RK_{30}||RK_{31} && \leftarrow \Sigma^7(L) \oplus K && \oplus S_8,\\
&RK_{32}||RK_{33}||RK_{34}||RK_{35} && \leftarrow \Sigma^8(L) && \oplus S_9,
\end{aligned}
$$

where $S_i$ are predefined 128-bit constants, and $\Sigma$ is a linear function defined further. In short, each four consecutive round keys $RK_{4i}$, $RK_{4i+1}$, $RK_{4i+2}$, $RK_{4i+3}$ are obtained by XOR of multiple applications of $\Sigma$ to $L$, possibly the master key $K$, and the constant $S_i$. The resulting 128-bit sequence is divided into four 32-bit words and each is assigned to one of the round key words. The linear function $\Sigma$ (illustrated in Fig. 1) is a simple 128-bit permutation used for diffusion. The function $\Sigma : \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ is defined as follows:

$$
\begin{aligned}
&X_{128} \rightarrow Y_{128}\\
&Y = X[120-64]X[6-0]X[127-121]X[63-7],
\end{aligned}
$$

where $X[a-b]$ is a bit sequence from the $a$-th bit to the $b$-th bit of $X$.

We would like to make a note about the notations of XOR differences used throughout the paper. To emphasize that a difference is in the word $X$, we use $\Delta X$, otherwise, if it irrelevant or clear from the context we use simply $\Delta$.

[7] Two round keys are used in every round, thus there are $2 \cdot 18 = 36$ keys in total.

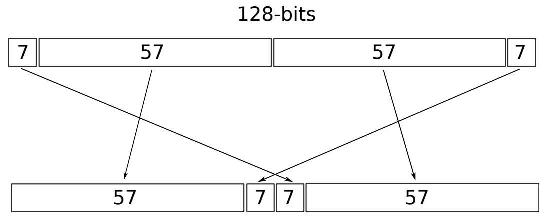


**Fig. 1.** The function $\Sigma$. The numbers denote the size of the bit sequence.

## 3 Weak Keys for `CLEFIA-128`

In the related-key model, the security of a cipher is analyzed by comparing two encryption functions obtained by two unknown but related keys. Given a specific relation[8] between keys, if the pair of encryption functions differs from a pair of random permutations, then the cipher has a weakness and can be subject to related-key analysis. Sometimes the analysis is applicable only when the pairs of related keys belong a relatively small subset of all possible pairs of keys. The subset is called the *weak-key class* of the cipher and the number of pairs of keys is the size of the class.

We will show that a weak-key class in `CLEFIA-128` consists of pairs of keys $(K, \tilde{K} = K \oplus \mathcal{L}_1(D))$, where $D$ can take approximately $2^{14}$ different 128-bit values, such that for *any* plaintext $P$, the following relation holds:

$$E_K(P) \oplus E_{\tilde{K}}(P \oplus \mathcal{L}_2(D)) = \mathcal{L}_3(D), \tag{1}$$

where $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$ are linear functions defined below. The property can be seen as a related-key differential, with the difference $\mathcal{L}_1(D)$ for the master key, $\mathcal{L}_2(D)$ for the plaintext and $\mathcal{L}_3(D)$ for the ciphertext. From Equation (1), it follows that once $D$ is defined, the probability of the differential is precisely one.

In the state of `CLEFIA-128`, the probability of a differential characteristic is one if in each Feistel round, there is no incoming difference to the non-linear round function. This happens when the differences in the state and in the round key cancel each other. Consequently, the input difference to the round function becomes zero[9]. An illustration of the technique for four rounds of `CLEFIA-128` is given in Fig. 2. Notice that the input state difference at the beginning of the first round $(\Delta_1, \Delta_2, \Delta_3, \Delta_4)$ is the same as the output difference after the fourth round, i.e. it is iterative with the

[8] Some relations are prohibited as they lead to trivial attacks, see [3] for details.
[9] A similar idea is given in [5].

period of 4 rounds. Therefore, we will obtain a differential characteristic with probability 1 (in the state) for the full-round `CLEFIA-128` if *we can produce 4-round iterative round key differences.*

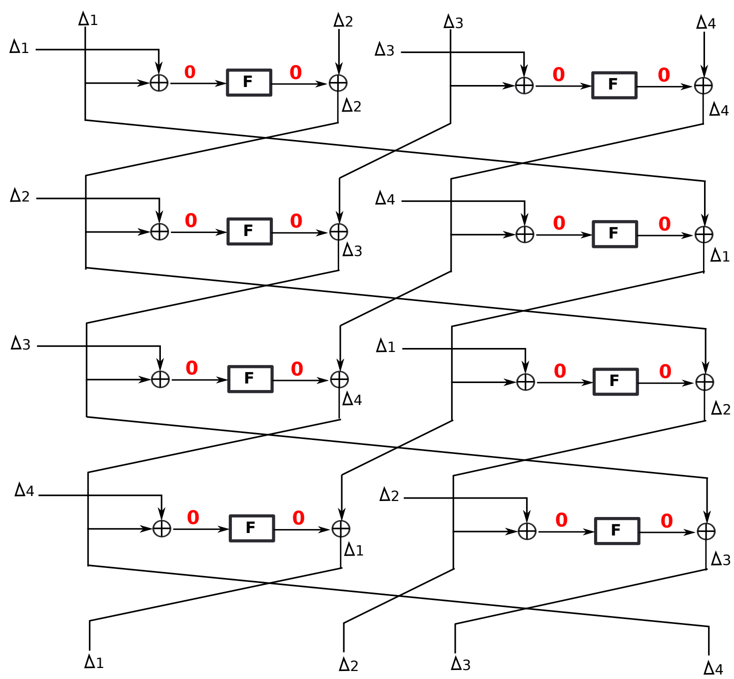


**Fig. 2.** Iterative related-key differential characteristic for 4 rounds of the `CLEFIA-128` that is true with probability 1. The symbols $\Delta_1, \Delta_2, \Delta_3, \Delta_4$ denote word differences.

Each round of the state uses two round keys, thus the above 4-round iterative characteristic requires the round key differences to have a period of 8, i.e. $\Delta RK_i = \Delta RK_{i+8}$. Moreover, an additional condition has to hold. Note that in Fig. 2, the differences in the consecutive round keys are $(\Delta_1, \Delta_3, \Delta_2, \Delta_4, \Delta_3, \Delta_1, \Delta_4, \Delta_2)$, that is among the 8 round key differences, the first four are different, while the remaining four are only permutations of the first. These two conditions can be summarized as follows:

**Condition 1** - For all $i$, it should hold $\Delta RK_i = \Delta RK_{i+8}$.
**Condition 2** - For all $i$ divisible by 8, it should hold $\Delta RK_i = \Delta RK_{i+5}$, $\Delta RK_{i+1} = \Delta RK_{i+4}$, $\Delta RK_{i+2} = \Delta RK_{i+7}$, $\Delta RK_{i+3} = \Delta RK_{i+6}$. This can be rewritten as $(\Delta RK_{i+4}, \Delta RK_{i+5}, \Delta RK_{i+6}, \Delta RK_{i+7}) =$

$\pi(\Delta RK_i, \Delta RK_{i+1}, \Delta RK_{i+2}, \Delta RK_{i+3})$, where $\pi$ is 4-word permutation $(0,1,2,3) \to (1,0,3,2)$.

Further we show how to find the set of differences for which the two conditions hold.

**Condition 1.** From the definition of the key schedule

$$\begin{aligned} RK_{8i+0}||RK_{8i+1}||RK_{8i+2}||RK_{8i+3} &\leftarrow \Sigma^{2i}(L) && \oplus S_{2i+1} \\ RK_{8i+8}||RK_{8i+9}||RK_{8i+10}||RK_{8i+11} &\leftarrow \Sigma^{2i+2}(L) && \oplus S_{2i+3}, \end{aligned}$$

it follows that Condition 1 for the first 4 (out of 8) round key differences in an octet of round keys can be expressed as

$$\Delta L = \Sigma^2(\Delta L). \tag{2}$$

We will obtain the same equation if we consider the remaining 4 round key differences. To satisfy Condition 1, we have to find possible values for $\Delta L$ such that Equation (2) holds. This can be achieved easily as (2) is a system of 128 linear equations with 128 unknowns (refer to the definition of $\Sigma$), and has solutions of the form (expressed as concatenation of bit sequences):

$$\Delta L = a_1 a_2 t b_2 b_1 b_2 b_1 b_2 b_1 b_2 a_2 a_1 a_2 a_1 a_2 a_1 a_2 t b_1 b_2, \tag{3}$$

where $a_1, a_2$ are any 7-bit values, $t$ is the most significant bit of $a_1$ and the 7-bit values $b_1, b_2$ are defined as $t b_2 b_1 = a_1 a_2 t$. Thus there are $2^7 \cdot 2^7 = 2^{14}$ solutions.

**Condition 2.** From the definition of the key schedule

$$\begin{aligned} RK_{8i+0}||RK_{8i+1}||RK_{8i+2}||RK_{8i+3} &\leftarrow \Sigma^{2i}(L) && \oplus S_{2i+1}, \\ RK_{8i+4}||RK_{8i+5}||RK_{8i+6}||RK_{8i+7} &\leftarrow \Sigma^{2i+1}(L) \oplus K && \oplus S_{2i+2}, \end{aligned}$$

we see that Condition 2 can be expressed as

$$\pi(\Delta L) = \Sigma(\Delta L) \oplus \Delta K,$$

where $\pi$ is 4-word permutation $(0,1,2,3) \to (1,0,3,2)$. Thus when $\Delta L$ is fixed (to one of the values from (3)), the difference in the master key $\Delta K$ can be determined as

$$\Delta K = \pi(\Delta L) \oplus \Sigma(\Delta L). \tag{4}$$

**Summary.** We have shown above that Conditions 1 and 2 can be achieved simultaneously as there are $2^{14}$ values for $\Delta L_i$ (see Equation (3)) with corresponding values of $\Delta K_i$ (see Equation (4)). It means that given the difference in the master key $\Delta K_i$ and the difference of the intermediate key $\Delta L_i$ (i.e. the differential in the 12-round Feistel $GFN_{4,12}$ of the key schedule is $\Delta K_i \rightarrow \Delta L_i$), the differences in the round keys are going to be of the requested form as shown below:

$$\begin{aligned}
\Delta RK_0||\Delta RK_1||\Delta RK_2||\Delta RK_3 &= \Delta_1||\Delta_3||\Delta_2||\Delta_4,\\
\Delta RK_4||\Delta RK_5||\Delta RK_6||\Delta RK_7 &= \Delta_3||\Delta_1||\Delta_4||\Delta_2,\\
&\dots\\
\Delta RK_{28}||\Delta RK_{29}||\Delta RK_{30}||\Delta RK_{31} &= \Delta_3||\Delta_1||\Delta_4||\Delta_2,\\
\Delta RK_{32}||\Delta RK_{33}||\Delta RK_{34}||\Delta RK_{35} &= \Delta_1||\Delta_3||\Delta_2||\Delta_4,
\end{aligned}$$

where $\Delta_1||\Delta_3||\Delta_2||\Delta_4 = \Delta L_i$. As a result, we have obtained the necessary differences in the round keys and we can use the 4-round iterative characteristic from Fig. 2.

Now we can easily specify the description of the weak-key class given by Equation (1). The value of $D$ coincides with the values of $\Delta L$ from Equation (3). Therefore the first linear function $\mathcal{L}_1$ is defined as $\mathcal{L}_1(D) = \pi(D) \oplus \Sigma(D)$. The input difference in the plaintext is the same as the input difference in the first four round keys (which is again $\Delta L$), but the order of the words is slightly different – instead of $(\Delta_1, \Delta_3, \Delta_2, \Delta_4)$ it is $(\Delta_1, \Delta_2, \Delta_3, \Delta_4)$, see Fig. 2. Hence, we introduce the 4-word permutation $\pi_2 : (0, 1, 2, 3) \rightarrow (0, 2, 1, 3)$ that corrects the order. With this notation, the second linear function $\mathcal{L}_2$ is defined as $\mathcal{L}_2(D) = \pi_2(D)$. Finally, $\mathcal{L}_3$ is defined similarly. `CLEFIA-128` has 18 rounds, thus the last 4-round iterative characteristic (for the rounds 17,18) will be terminated after the second round, with an output difference $(\Delta_2, \Delta_3, \Delta_4, \Delta_1)$. It differs from $\Delta L$ only in the order of the four words, hence we introduce $\pi_3 : (0, 1, 2, 3) \rightarrow (3, 1, 0, 2)$ and conclude that $\mathcal{L}_3(D) = \pi_3(D)$.

In the weak-key class the pairs of keys are defined as $(K, K \oplus \pi(D) \oplus \Sigma(D))$ and for any plaintext $P$, it holds

$$E_K(P) \oplus E_{K\oplus\pi(D)\oplus\Sigma(D)}(P \oplus \pi_2(D)) = \pi_3(D). \quad (5)$$

A pair of keys belongs to this class if for any of the $2^{14}$ values $D = \Delta L$ defined by Equation (3), the 12-round Feistel $GFN_{4,12}$ in the key schedule, on input difference $\Delta K = \pi(\Delta L) \oplus \Sigma(\Delta L)$ gives the output difference $\Delta L$, i.e. $GFN_{4,12}(K \oplus \pi(\Delta L) \oplus \Sigma(\Delta L)) \oplus GFN_{4,12}(K) = \Delta L$. Therefore not all of the keys $K$ have a related key and form a pair in the weak-key class, but only those for which the differential in the Feistel permutation holds.

We deal with a 12-round Feistel permutation and thus the probability of the differential $\pi(\Delta L) \oplus \Sigma(\Delta L) \rightarrow \Delta L$ is low. We assume it is $2^{-128}$ (as proven by the designers), which is the probability of getting fixed output difference from a fixed input difference in a random permutation. However, even when we model the Feistel permutation by a random one, *there still exist* $2^{14}$ *key schedule differentials that have a probability of* $2^{-128}$ *and that result in iterative round key differences.*

In `CLEFIA-128`, there are $2^{128}$ possible keys $K$, and therefore for a specific value of $D$, the number of related keys $(K, K \oplus \pi(D) \oplus \Sigma(D))$ is the same. The probability of the differential in the Feistel permutation is $2^{-128}$, thus among all of the pairs, only one will pass the differential. However, there are $2^{14}$ possible values for $D$, hence the size of the weak-key class is $2^{14}$.

## 4 Membership Test for the Weak-Key Class

An analysis technique that succeeds when the related keys belong to the weak-key class is called a membership test. For the weak-key class of `CLEFIA-128`, the membership test will be a differential distinguisher that succeeds always and whose data, time and memory complexities are equal to $2^8$. That is to say that we can decide with probability 1 whether the underlying cipher is `CLEFIA-128` with weak keys or other (possibly ideal) cipher.

Given a pair of weak keys $(K, K \oplus \pi(D) \oplus \Sigma(D))$, it is easy to distinguish `CLEFIA-128` (see Equation (5)) with only a single pair of related plaintexts $(P, P \oplus \pi_2(D))$ but $D$ has to be known. If it is unknown, we will have to try all $2^{14}$ possible values of $D$ (as $D$ coincides with one of $\Delta L_i$). Consequently, we are going to end up with a brute force attack on the space of weak keys. To address this problem, we have to be able to detect the correct value of $\Delta L$ efficiently.

Finding the correct $\Delta L_i$ can be performed much faster if we take into account the additional properties of the difference in the intermediate key. All $2^{14}$ values of $\Delta L_i$ (see Equation (3)) can be defined as XOR of two elements from two different sets each of cardinality $2^7$ as shown below

$$\begin{aligned}\Delta L_i = \Delta L_i(a_1, a_2) =& a_1 a_2 t b_2 b_1 b_2 b_1 b_2 b_1 b_2 a_2 a_1 a_2 a_1 a_2 a_1 a_2 t b_1 b_2 = \\ =& G^1(a_1) \oplus G^2(a_2), \\ & a_1 = 0, \ldots, 2^7 - 1, a_2 = 0, \ldots, 2^7 - 1,\end{aligned}$$

where $G^1(a_1)$ is a 128-bit word that is the same as $\Delta L$ on the bits that depend on $a_1$ and has 0's for the bits that depend on $a_2$ while $G^2(a_2)$ is the opposite, i.e. coincides with $\Delta L$ on bits for $a_2$ and has 0's for bits that depend on $a_1$[10].

Using the representation helps to detect the correct $\Delta L$ by finding collisions on two specific sets. Assume the pair $(K, \tilde{K} = K \oplus \pi(\Delta L) \oplus \Sigma(\Delta L))$ belongs to the weak-key class. For a randomly chosen plaintext $P$, let us define two pools, each with $2^7$ chosen plaintexts:

$$P_i^1 = \pi_2(P \oplus G^1(a_1^i)), a_1^i = 0, 1, \ldots, 2^7 - 1,$$
$$P_i^2 = \pi_2(P \oplus G^2(a_2^i)), a_2^i = 0, 1, \ldots, 2^7 - 1.$$

Next, we obtain two pools of ciphertexts with $(K, \tilde{K})$ as encryption keys, i.e. $C_i^1 = E_K(P_i^1), C_i^2 = E_{\tilde{K}}(P_i^2)$. Finally, we compute two sets $V^1, V^2$:

$$V^1 = \{V_i^1 | V_i^1 = \pi_2^{-1}(P_i^1) \oplus \pi_3^{-1}(C_i^1)\},$$
$$V^2 = \{V_i^2 | V_i^2 = \pi_2^{-1}(P_i^2) \oplus \pi_3^{-1}(C_i^2)\}.$$

The crucial observation is that the sets $V^1$ and $V^2$ will always collide, i.e. there exist $V_i^1$ and $V_j^2$ such that $V_i^1 = V_j^2$. This comes from the following sequence:

$$\begin{aligned}
&V_i^1 \oplus V_j^2 = \\
&= \pi_2^{-1}(P_i^1) \oplus \pi_3^{-1}(C_i^1) \oplus \pi_2^{-1}(P_j^2) \oplus \pi_3^{-1}(C_j^2) = \\
&= \pi_2^{-1}(P_i^1 \oplus P_j^2) \oplus \pi_3^{-1}(E_K(P_i^1) \oplus E_{\tilde{K}}(P_j^2)) = \\
&= \pi_2^{-1}(\pi_2(G^1(a_1^i) \oplus G^2(a_2^j))) \oplus \\
&\oplus \pi_3^{-1}(E_K(P_i^1) \oplus E_{\tilde{K}}(P_i^1 \oplus \pi_2(G^1(a_1^i) \oplus G^2(a_2^j)))) = \\
&= \Delta L' \oplus \pi_3^{-1}(E_K(P_i^1) \oplus E_{\tilde{K}}(P_i^1 \oplus \pi_2(\Delta L'))),
\end{aligned}$$

where $\Delta L' = G^1(a_1^i) \oplus G^2(a_2^i)$. Note that $\Delta L'$ can take all possible $2^{14}$ values (as $a_1^i, a_2^j$ take all $2^7$ values), and therefore for some particular $i, j$, it must coincide with $\Delta L$. In such case, the difference in the plaintext is $\pi_2(\Delta L)$, and thus for the ciphertext we obtain

$$E_K(P_i^1) \oplus E_{\tilde{K}}(P_i^1 \oplus \pi_2(\Delta L)) = \pi_3(\Delta L)$$

Then $V_i^1 \oplus V_j^2 = \Delta L \oplus \pi_3^{-1}(\pi_3(\Delta L)) = 0$.

The possibility to create the sets independently and then to find a collision between them is the main idea of the membership test on `CLEFIA-128`. It works according to the following steps.

[10] Recall that each bit of $b_1, b_2, t$ is equal to a single bit of either $a_1$ or $a_2$.

1. Choose at random a plaintext $P$.
2. Create a pool of $2^7$ plaintexts $P_i^1 = \pi_2(P \oplus G^1(a_1^i))$ and ask for the corresponding ciphertext $C_i^1$ obtained with encryption under the first key, i.e. $C_i^1 = E_K(P_i^1)$. Compute the set $V^1$ composed of elements $V_i^1 = \pi_2^{-1}(P_i^1) \oplus \pi_3^{-1}(C_i^1)$.
3. Create a pool of $2^7$ plaintexts $P_i^2 = \pi_2(P \oplus G^2(a_2^i))$ and ask for the corresponding ciphertext $C_i^2$ obtained with encryption under the second key, i.e. $C_i^2 = E_{\tilde{K}}(P_i^2)$. Compute the set $V^2$ composed of elements $V_i^2 = \pi_2^{-1}(P_i^2) \oplus \pi_3^{-1}(C_i^2)$.
4. Check for collisions between $V^1$ and $V^2$. If such a collision exists, then output that the examined cipher is `CLEFIA-128`. Otherwise, it is an ideal cipher.

The total data complexity of the membership test is $2^7 + 2^7 = 2^8$ plaintexts. The time complexity of each of the steps 2,3 is $2^7$ encryptions, while the collision at step 4 can be found with $2^7$ operations and $2^7$ memory that is used to store one of the sets $V^1$ or $V^2$. Therefore, given a pair of keys from the weak-key class, we can distinguish `CLEFIA-128` in $2^8$ data, time and memory.

To confirm the correctness of the membership test, we implemented it for a small-scale variant of `CLEFIA-128`. Each word was shrunk to 8-bit value, thus the whole state became 32 bits. The Sbox from AES was taken as the round function $F$, and random 8-bit values were chosen as constants. The chunks in the linear function $\Sigma$ were taken of size $5, 11$ (compared to the $7, 57$ in the original version). The expected size of the weak-key class in this toy version is $2^{10}$ (because $X = \Sigma^2(X)$ has $2^{10}$ solutions), while in practice we obtained $960 = 2^{9.9}$ solutions. For a random key pair chosen from this class, we were able to distinguish the cipher after $2^6$ encryptions which confirms our findings to a large extent.

## 5 Analysis of the Hashing Modes of `CLEFIA-128`

In this section we analyze the impact of the weak-key class on hashing modes of `CLEFIA-128`. We show that compression functions built upon single-block-length modes instantiated with `CLEFIA-128` exhibit non-random properties that come in a form of differential multicollisions. The analysis of hashing modes of a cipher is usually reduced to finding open-key distinguishers for the cipher. Note, open-key distinguishers come in a form of known-key (the adversary has the knowledge of the key, but cannot control it) and chosen-key (the adversary can choose the value of the key). Our analysis applies to the second case, i.e. we show non-randomness of the hashing modes of `CLEFIA-128` when the adversary can control the key.

First, let us find a pair of keys $(K_1, K_2)$ that belong to the weak-key class – we stress that the task is to find the pair explicitly, i.e. to produce the two values that compose a weak-key pair. From the previous analysis we have seen that a pair is a weak-key pair if for one of the $2^{14}$ values of $\Delta L$ defined previously: 1) the difference $\Delta K = K_1 \oplus K_2$ satisfies $\Delta K = \pi(\Delta L) \oplus \Sigma(\Delta L)$, and 2) the 12-round Feistel in the key schedule $GFN_{4,12}$ produces output difference $\Delta L$, i.e. $GFN_{4,12}(K_1) \oplus GFN_{4,12}(K_2) = \Delta L$. The two conditions can be generalized as search for a pair that satisfies the differential $\pi(\Delta L) \oplus \Sigma(\Delta L) \to \Delta L$ through the 12-round Feistel in the key schedule.

Recall that the difference $\Delta L$ is an XOR of two elements (defined as $G^1(a_1)$ and $G^2(a_2)$) from sets of size $2^7$, i.e. $\Delta L = G^1(a_1) \oplus G^2(a_2)$. Therefore we get that:

$$\begin{aligned}\Delta K = \pi(\Delta L) \oplus \Sigma(\Delta L) &= \pi(G^1(a_1) \oplus G^2(a_2)) \oplus \Sigma(G^1(a_1) \oplus G^2(a_2)) = \\ &= [\pi(G^1(a_1)) \oplus \Sigma(G^1(a_1))] \oplus [\pi(G^2(a_2)) \oplus \Sigma(G^2(a_2))] = \\ &= T^1(a_1) \oplus T^2(a_2),\end{aligned}$$

where $T^1(a_1) = \pi(G^1(a_1)) \oplus \Sigma(G^1(a_1)), T^2(a_2) = \pi(G^2(a_2) \oplus \Sigma(G^2(a_2))$ are two linear functions (as $\pi, \Sigma, G^1, G^2$ are linear), and therefore the difference in the keys of a weak-key pair is an XOR of two sets as well. Using this fact, we can find a weak-key pair as follows:

1. Create a set $\Delta\mathcal{K}$ of $2^{14}$ values $T^1(a_1) \oplus T^2(a_2), a_1 = 0, \ldots, 2^7 - 1, a_2 = 0, \ldots, 2^7 - 1$.
2. Randomly choose a key $K$.
3. Create a set $V_1$ of $2^7$ pairs

$$(K_1, K_1 \oplus \pi(GFN_{4,12}(K_1)) \oplus \Sigma(GFN_{4,12}(K_1))),$$

   where $K_1 = K \oplus T^1(a_1), a_1 = 0, \ldots, 2^7 - 1$. Index the set $V_1$ by the second elements.
4. Create a set $V_2$ of $2^7$ pairs

$$(K_2, K_2 \oplus \pi(GFN_{4,12}(K_2)) \oplus \Sigma(GFN_{4,12}(K_2))),$$

   where $K_2 = K \oplus T^2(a_2), a_2 = 0, \ldots, 2^7 - 1$. Index $V_2$ as well by the second elements.

5. Check for collisions between $V^1$ and $V^2$ on the second (and indexed) elements. If such a collision exists, then confirm the key pair is weak by checking if the xor difference of the first elements belongs to $\Delta\mathcal{K}$. If so, then output that found pair $(K_1, K_2)$ and exit. Otherwise, go to step 2.

The above algorithm will output a correct weak-key pair after repeating around $2^{114}$ times the steps 2-5. For each randomly chosen key $K$, there are $2^{14}$ pairs of keys $(K_1, K_2)$ with difference $K_1 \oplus K_2 = K \oplus T^1(a_1) \oplus K \oplus T^2(a_2) = T^1(a_1) \oplus T^2(a_2) = \pi(\Delta L_i) \oplus \Sigma(\Delta L_i)$. If the output difference of 12-round Feistel is precisely the same $\Delta L_i$ (an event that happens with probability $2^{-128}$), i.e. if $GFN_{4,12}(K_1) \oplus GFN_{4,12}(K_2) = \Delta L_i$, then

$$\pi(GFN_{4,12}(K_1) \oplus GFN_{4,12}(K_2)) \oplus \Sigma(GFN_{4,12}(K_1) \oplus GFN_{4,12}(K_2)) = \pi(\Delta L_i) \oplus \Sigma(\Delta L_i),$$

and therefore

$$K_1 \oplus K_2 = \pi(GFN_{4,12}(K_1) \oplus GFN_{4,12}(K_2)) \oplus \Sigma(GFN_{4,12}(K_1) \oplus GFN_{4,12}(K_2)),$$

which is equivalent to

$$K_1 \oplus \pi(GFN_{4,12}(K_1)) \oplus \Sigma(GFN_{4,12}(K_1)) = K_2 \oplus \pi(GFN_{4,12}(K_2)) \oplus \Sigma(GFN_{4,12}(K_2)).$$

Therefore a collision between $V_1$ and $V_2$ suggests a possible weak-key pair. The suggested pair is weak-key only if the input and the output differences satisfy the differential, thus with probability $2^{-128}$. As we take $2^{114}$ random keys $K$, and for each there are $2^{14}$ pairs, with overwhelming probability, one will be a weak-key pair. To avoid false positives, we add step 1 and the additional checking at step 5, i.e. we make sure that the difference between the keys is $\pi(\Delta L_i) \oplus \Sigma(\Delta L_i)$ for some of the $2^{14}$ good values of $\Delta L_i$. Hence, the algorithm will produce a weak-key pair in $2^{14} + 2^{114} \times 2 \times 2^7 \approx 2^{122}$ time and $2^{14}$ memory.

We can use the found pair to show weakness of `CLEFIA-128` when used for cryptographic hashing. More precisely, we consider hashing based on single-block-length[11] modes, where a compression function is built from a block cipher. If the compression function uses `CLEFIA-128` then we can find a pair of weak keys in $2^{122}$ time using the described algorithm.

[11] The state and key sizes in `CLEFIA-128` coincide, thus we can construct only single-block-length compression functions.

Once such pair $(K_1, K_2)$ is found, we can produce any number of differential multicollisions [4] for any of the 12 modes investigated by Preneel et al. [12], including the popular Davies-Meyer, Matyas-Meyer-Oseas modes. For instance, for the Davies-Meyer mode, i.e. when the compression function $C(H, M)$ is defined as $C(H, M) = E_M(H) \oplus H$, the differential multicollisions have the form

$$\begin{aligned}
&C(H_i, K_1) \oplus C(H_i \oplus \pi_2(\Delta L), K_1 \oplus \pi(\Delta L) \oplus \Sigma(\Delta L)) = \\
&= E_{K_1}(H_i) \oplus H_i \oplus E_{K_1 \oplus \pi(\Delta L) \oplus \Sigma(\Delta L)}(H_i \oplus \pi_2(\Delta L))) \oplus H_i \oplus \pi_2(\Delta L) = \\
&= E_{K_1}(H_i) \oplus E_{K_1 \oplus \pi(\Delta L) \oplus \Sigma(\Delta L)}(H_i \oplus \pi_2(\Delta L)) \oplus \pi_2(\Delta L) = \\
&= \pi_3(\Delta L) \oplus \pi_2(\Delta L),
\end{aligned}$$

for $i = 0, 1, \ldots$. Note that we do not need to call the compression functions as $C(H_i, K_1) \oplus C(H_i \oplus \pi_2(\Delta L), K_1 \oplus \pi(\Delta L) \oplus \Sigma(\Delta L)) = \pi_3(\Delta L) \oplus \pi_2(\Delta L)$ as long as $(K_1, K_1 \oplus \pi(\Delta L) \oplus \Sigma(\Delta L))$ form a weak-key pair. Consequently, we can produce an arbitrary number of differential multicollisions with the complexity $2^{122}$. On the other hand, the proven lower bound (see [4]) in the case of ideal cipher is $2^{128}$. A distinguisher for the hashing based on `CLEFIA-128` has already been presented by Aoki at ISITA'12 [2]. It works in the framework of middletext distinguishers [11] (open-key version of the integral attack), where the adversary starts with a set of particularly chosen states in the middle of the cipher, then from them (and the knowledge of the key) produces the set of plaintexts and the set of ciphertexts, and finally shows that these two sets have some property that cannot be easily reproduced if the cipher was ideal. For `CLEFIA-128`, Aoki showed how to choose $2^{112}$ starting middle states that result in 17-round middletext distinguisher, and then added one more round where he used subkey guesses, to obtain the 18-round distinguisher. We want to point out that there is a substantial difference, between our result and that of Aoki. We do not fix the values neither of the plaintexts nor of the ciphertexts, and our analysis is applicable as long as the pair of chaining values has the required difference – the values can be arbitrary and even unknown.

## 6 Conclusion

The analysis of `CLEFIA-128` presented in this paper shows existence of a weak-key class that consists of $2^{14}$ pairs of keys. We have shown how to exploit the pairs in two different scenarios: hashing mode of `CLEFIA-128` and membership test for the weak-key class. In the hashing mode (or open-key mode in general) we have shown that a weak-key pair can be found in around $2^{122}$ time, and such pair can be used to produce differential multicollisions faster than the generic $2^{128}$. Furthermore, we have shown a membership test for the weak-key class that has $2^8$ time and data complexity, compared to the generic $2^{14}$. The main ideas of the analysis have been verified with computer experiments on small-scale variants of `CLEFIA-128`.

The analysis is invariant of three important security features that presumably increase the strength of a cipher. First, the non-linear part of the key schedule can be any random permutation (not necessarily a 12-round Feistel). Our analysis would still work as we do not need high probability differentials for this permutation. Second, the state update functions (in `CLEFIA-128` $F_0, F_1$ are one round substitution-permutation networks) can be arbitrary functions or permutations, including several layers of SP – the difference never goes into them, hence, the probability of the characteristic in the state would stay 1. Finally, the number of rounds in `CLEFIA-128` plays absolutely no role in our analysis – even if `CLEFIA-128` had 1000 rounds, the complexity of the analysis would stay the same.

To prevent future analysis as ours, we have to clearly understand what are the main drawbacks of the design. The weak-key class and the three analysis invariances are results of these drawbacks (not their cause) and provide clues on what the actual cause might be. The invariance of the state update function is due to the Feistel structure of the cipher – this construction can lead to probability 1 characteristics as it can cancel round key and state differences. To maintain the cancellation through arbitrary number of rounds (invariance of the number of rounds), the round key differences have to be iterative. The key schedule prevents high probability iterative (or any fixed value) differences as they have to be produced from a difference in the key that goes initially through a 12-round Feistel modeled as random permutation. The Feistel, however, produces low probability ($2^{-128}$) differences (invariance of the random permutation), and $2^{14}$ of them become iterative round key differences due to the linear function used after the Feistel. That is, because of the linear function, with $2^{-128}$ we can have a special type of differences in 36 rounds keys (1152 bits !). Therefore, the analysis of `CLEFIA-128` holds due to the Feistel structure of the cipher and the weak linear function that is used to produce the round keys.

To conclude, our work shows that *low probability differentials (around $2^{-k}$ for a cipher with k-bit key and n-bit state) for the key schedule of Feistel ciphers, cannot be used as a sole proof of resistance against related-*

*key differential analysis.*. A safe upper bound on the probability of such differentials, which proves and provides security against related-key analysis, is not $2^{-k}$ but $2^{-2k-n}$ – this comes from the fact that there can be as many as $2^{2k}$ pairs of weak keys, and their combined probability should be below $2^{-n}$.

## References


1. RFC 6114. CLEFIA. http://www.rfc-editor.org/rfc/rfc6114.txt.
2. K. Aoki. A middletext distinguisher for full CLEFIA-128. In *ISITA*, pages 521–525. IEEE, 2012.
3. M. Bellare and T. Kohno. A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In E. Biham, editor, *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 491–506. Springer, 2003.
4. A. Biryukov, D. Khovratovich, and I. Nikolic. Distinguisher and related-key attack on the full AES-256. In S. Halevi, editor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 231–249. Springer, 2009.
5. A. Biryukov and I. Nikolic. Complementing Feistel ciphers. *FSE 2013*. To appear.
6. A. Bogdanov, H. Geng, M. Wang, L. Wen, and B. Collard. Correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA. *Selected Areas of Cryptography 2013*. To appear.
7. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In P. Paillier and I. Verbauwhede, editors, *CHES*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007.
8. ISO/IEC 29192-2. Information technology - Security techniques - Lightweight cryptography - Part 2: Block ciphers. `http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56552`.
9. 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.
10. H. Mala, M. Dakhilalian, and M. Shakiba. Impossible differential attacks on 13-round CLEFIA-128. *J. Comput. Sci. Technol.*, 26(4):744–750, 2011.
11. M. Minier, R. C.-W. Phan, and B. Pousse. Distinguishers for ciphers and known key attack against Rijndael with large blocks. In B. Preneel, editor, *AFRICACRYPT*, volume 5580 of *Lecture Notes in Computer Science*, pages 60–76. Springer, 2009.
12. B. Preneel, R. Govaerts, and J. Vandewalle. Hash functions based on block ciphers: A synthetic approach. In D. R. Stinson, editor, *CRYPTO*, volume 773 of *Lecture Notes in Computer Science*, pages 368–378. Springer, 1993.
13. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. The 128-bit blockcipher CLEFIA (Extended Abstract). In A. Biryukov, editor, *FSE*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer, 2007.
14. B. Sun, R. Li, M. Wang, P. Li, and C. Li. Impossible differential cryptanalysis of CLEFIA. *IACR Cryptology ePrint Archive*, 2008:151, 2008.
15. 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.
16. 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.

17. 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.
18. W. Wang and X. Wang. Improved impossible differential cryptanalysis of CLEFIA. *IACR Cryptology ePrint Archive*, 2007:466, 2007.
19. 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.

# A Specification on `CLEFIA-128`

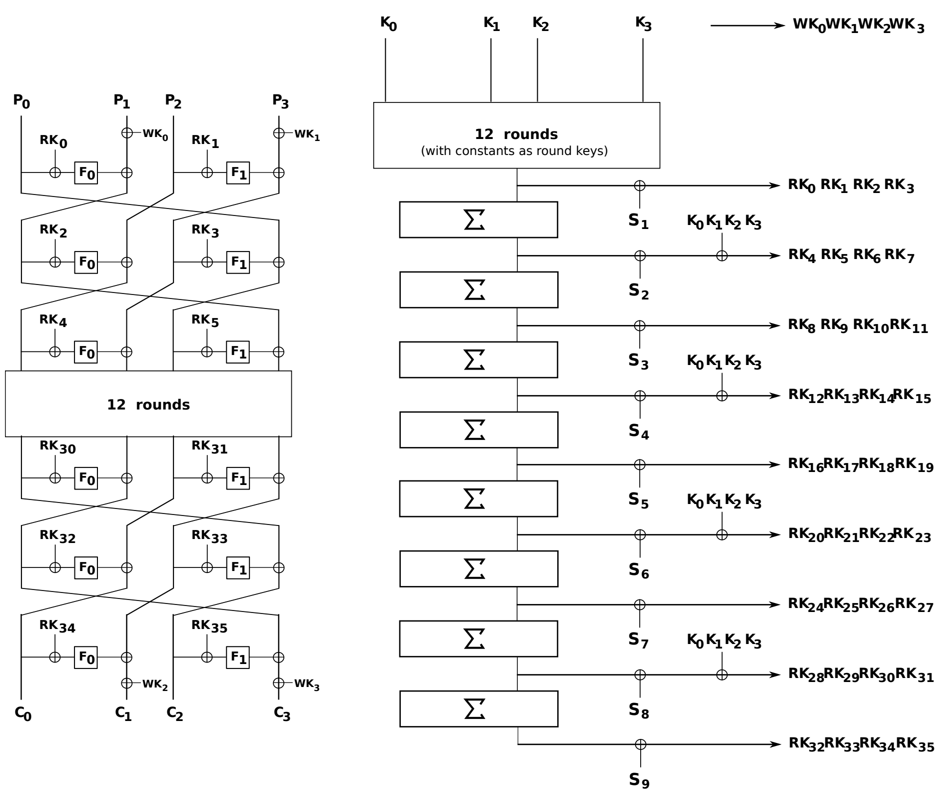


**Fig. 3.** The encryption function of `CLEFIA-128` at the left, and the key schedule at the right. $P_0, P_1, P_2, P_3$ are 32-bit plaintext words, $C_0, C_1, C_2, C_3$ are the ciphertext words, $K_0, K_1, K_2, K_3$ are the key words, $RK_i, WK_j$ are the round and whitening keys, respectively, and $S_i$ are 128-bit constants. Finally, $F_0, F_1$ are the two state update functions, while $\Sigma$ is a linear function (permutation).

## B Analysis of CLEFIA-128 with Whitening Keys

The whitening keys are the four words $WK_i, i = 0, 1, 2, 3$, defined as $WK_0||WK_1||WK_2||WK_3 = K$, i.e. they are the words of the master key $K$. The first two are XOR-ed to the second and the fourth plaintext words, and the remaining two to the second and the fourth ciphertext words (see Fig 3).

To index the whitening words, we define two linear functions on 128-bit words (or four 32-bit words). Assume $X$ is 128-bit word, such that $X = a|b|c|d$, where $a, b, c, d$ are 32-bit words. Then $l(X) : \{0,1\}^{128} \to \{0,1\}^{128}$ is defined as $l(X) = l(a|b|c|d) = 0|a|0|b$. Similarly $r(X) : \{0,1\}^{128} \to \{0,1\}^{128}$ is defined as $r(X) = r(a|b|c|d) = 0|c|0|d$.

Now we can easily specify the weak-key class:

- the key difference remains the same,
- the plaintext difference, instead of $\pi_2(\Delta L)$, should be $\pi_2(\Delta L) \oplus l(\Delta K)$,
- the ciphertext difference, instead of $\pi_3(\Delta L)$, should be $\pi_3(\Delta L) \oplus r(\Delta K)$.

As $\Delta K = \pi(\Delta L) \oplus \Sigma(\Delta L)$, it follows that the weak-key class for the original CLEFIA-128 is defined as $2^{14}$ pairs of keys $(K, K \oplus \pi(\Delta L) \oplus \Sigma(\Delta L))$ such that for any plaintext $P$ holds:

$$E_K(P) \oplus E_{K\oplus\pi(\Delta L)\oplus\Sigma(\Delta L)}(P \oplus \pi_2(\Delta L) \oplus l(\pi(\Delta L) \oplus \Sigma(\Delta L))) = \pi_3(\Delta L) \oplus r(\pi(\Delta L) \oplus \Sigma(\Delta L)).$$

Let us focus on the membership test. We define the plaintexts pools as:

$$P_i^1 = P \oplus \pi_2(G^1(a_1^i)) \oplus l(T^1(a_1^i)), a_1^i = 0, 1, \ldots, 2^7 - 1,$$
$$P_i^2 = P \oplus \pi_2(G^2(a_2^i)) \oplus l(T^2(a_2^i)), a_2^i = 0, 1, \ldots, 2^7 - 1.$$

This way, the difference between each two plaintext from two different pools is $\pi_2(\Delta L') \oplus l(\Delta K)$, i.e. it is as required by the class.

To define the sets $V^1, V^2$ that lead to a collision, first we have to understand how a collision can occur. In the previous membership test (on CLEFIA-128 without whitening keys), we used the trick that the difference in both the plaintext and the ciphertext is $\Delta L$, but with permuted words (that is why we applied $\pi_2^{-1}, \pi_3^{-1}$). Here it is not the same: in the plaintext the difference is $\Delta L$ and two more words of $\Delta K$, while in the ciphertext it is $\Delta L$ and the remaining two words of $\Delta K$. Hence, XOR of these values does not trivially produce zero as the two words from $l$ and the two from $r$ are different.

Nevertheless, we can achieve collisions. Assume $\Delta L = a|b|c|d$. Then the difference $\Delta_P$ in the plaintext is

$$\begin{aligned}\Delta_P =&\pi_2(a|b|c|d) \oplus l(\pi(a|b|c|d) \oplus \Sigma(a|b|c|d)) =\\ &a|c|b|d \oplus l(b|a|d|c) \oplus l(\Sigma(a|b|c|d)) =\\ &a|c+b|b|d+a \oplus l(\Sigma(a|b|c|d)).\end{aligned}$$

Note, $l(\Sigma(a|b|c|d)$ has zeros at the first and at the third words.

Similarly, the difference $\Delta_C$ in the ciphertext is

$$\begin{aligned}\Delta_C =&\pi_3(a|b|c|d) \oplus r(\pi(a|b|c|d) \oplus \Sigma(a|b|c|d)) =\\ &c|b|d|a \oplus r(b|a|d|c) \oplus r(\Sigma(a|b|c|d)) =\\ &c|b+d|d|a+c \oplus r(\Sigma(a|b|c|d)).\end{aligned}$$

Again, in the sum $r$ influences only the second and the fourth word.

Let us introduce a function $f$, that acts on the four 32-bit words of a 128-bit state and it XORs the first word to the fourth word, and the third word to the second word, i.e. $f(x|y|z|t) = (x|y+z|z|t+x)$. Then

$$\begin{aligned}f(\Delta_P) &= a|c|b|d \oplus l(\Sigma(a|b|c|d)),\\ f(\Delta_C) &= c|b|d|a \oplus r(\Sigma(a|b|c|d)).\end{aligned}$$

The function $\Sigma$ is linear and therefore $\Sigma(a|b|c|d) = \Sigma(a|0|0|0)+\Sigma(0|b|0|0)+\Sigma(0|0|c|0) + \Sigma(0|0|0|d)$. Let us denote these four values with $\Sigma_a, \Sigma_b, \Sigma_c$, and $\Sigma_d$. Furthermore, with superscripts we denote the four 32-bit words of $\Sigma_x$, e.g. $\Sigma_a^2$ is the second (most significant) word of $\Sigma_a$. This allows us to remove the functions $l, r$ from the terms, and as a result we obtain

$$\begin{aligned}f(\Delta_P) &= a|c + \Sigma_a^1 + \Sigma_b^1 + \Sigma_c^1 + \Sigma_d^1|b|d + \Sigma_a^2 + \Sigma_b^2 + \Sigma_c^2 + \Sigma_d^2,\\ f(\Delta_C) &= c|b + \Sigma_a^3 + \Sigma_b^3 + \Sigma_c^3 + \Sigma_d^3|d|a + \Sigma_a^4 + \Sigma_b^4 + \Sigma_c^4 + \Sigma_d^4.\end{aligned}$$

Next, we define a function $g(x|y|z|t)$ that from $x, z$ computes $\Sigma_x^1, \ldots, \Sigma_x^4$, $\Sigma_z^1, \ldots, \Sigma_z^4$ and it adds $\Sigma_x^4, \Sigma_z^4$ to the first word, $\Sigma_x^1, \Sigma_z^1$ to the second, $\Sigma_x^3, \Sigma_z^3$ to the third, and $\Sigma_x^2, \Sigma_z^2$ to the fourth. Similarly, for $\Delta_C$ we define $h(x|y|z|t)$ that from $x, z$ computes $\Sigma_x^1, \ldots, \Sigma_z^4$ and it adds $\Sigma_x^1, \Sigma_z^1$ to the first word, $\Sigma_x^3, \Sigma_z^3$ to the second, $\Sigma_x^2, \Sigma_z^2$ to the third, and $\Sigma_x^4, \Sigma_z^4$ to the fourth. Thus we get

$$\begin{aligned}g(f(\Delta_P)) &= a + \Sigma_a^4 + \Sigma_b^4|c + \Sigma_c^1 + \Sigma_d^1|b + \Sigma_a^3 + \Sigma_b^3|d + \Sigma_c^2 + \Sigma_d^2,\\ h(f(\Delta_C)) &= c + \Sigma_c^1 + \Sigma_d^1|b + \Sigma_a^3 + \Sigma_b^3|d + \Sigma_c^2 + \Sigma_d^2|a + \Sigma_a^4 + \Sigma_b^4.\end{aligned}$$

Obviously $h(f(\Delta_C)) = \pi_4(g(f(\Delta_P)))$, where $\pi_4(0, 1, 2, 3) \rightarrow (3, 0, 1, 2)$. Therefore the sets $V_1, V_2$ are defined as:

$$V^1 = \{V_i^1 | V_i^1 = \pi_4(g(f(P_i^1))) \oplus h(f(C_i^1))\},$$
$$V^2 = \{V_i^2 | V_i^2 = \pi_4(g(f(P_i^2))) \oplus g(f(C_i^2))\},$$

and a collision between this two sets suggests that $\Delta L'$ coincides with $\Delta L$. Thus the membership test for `CLEFIA-128` with whitening keys has the same complexity as before (without whitening).