The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA[⋆]

Cihangir Tezcan

École Polytechnique Fédérale de Lausanne
EDOC-IC BC 350 Station 14 CH-1015 Lausanne, Switzerland
cihangir.tezcan@epfl.ch

Abstract. In this paper we present a new statistical cryptanalytic technique that we call improbable differential cryptanalysis which uses a differential that is less probable when the correct key is used. We provide data complexity estimates for this kind of attacks and we also show a method to expand impossible differentials to improbable differentials. By using this expansion method, we cryptanalyze 13, 14, and 15-round CLEFIA for the key sizes of length 128, 192, and 256 bits, respectively. These are the best cryptanalytic results on CLEFIA up to this date.

Keywords : Cryptanalysis, Improbable differential attack, CLEFIA

1 Introduction

Statistical attacks on block ciphers make use of a property of the cipher so that an incident occurs with different probabilities depending on whether the correct key is used or not. For instance, differential cryptanalysis [1] considers characteristics or differentials which show that a particular output difference should be obtained with a relatively high probability when a particular input difference is used. Hence, when the correct key is used, the predicted differences occur more frequently. In a classical differential characteristic the differences are fully specified and in a truncated differential [2] only parts of the differences are specified.

On the other hand, impossible differential cryptanalysis [3] uses an impossible differential which shows that a particular difference cannot occur for the correct key (i.e. probability of this event is exactly zero). Therefore, if these differences are satisfied under a trial key, then it cannot be the correct one. Thus, the correct key can be obtained by eliminating all or most of the wrong keys.

In this paper we describe a new variant of differential cryptanalysis in which a given differential holds with a relatively small probability. Therefore, when the correct key is used, the predicted differences occur less

[⋆] This work was done when the author was a research assistant at Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey.

frequently. In this respect, the attack can be seen as the exact opposite of (truncated) differential cryptanalysis. For this reason, we call this kind of differentials *improbable differentials* and we call the method *improbable differential cryptanalysis*. Early applications of improbable events in differential attacks were mentioned in [4] and [5].

Accurate estimates of the data complexity and success probability for many statistical attacks are provided by Blondeau et al. in [6, 7] but these estimates work for the cases when an incident is more probable for the correct key. We make necessary changes on these estimates to be able to estimate data complexity and success probability of improbable differential attacks.

Moreover, we show that improbable differentials can be obtained when suitable differentials that can be put on the top or the bottom of an impossible differential exist. Expanding an impossible differential to an improbable differential in this way can be used to distinguish more rounds of the cipher from a random permutation; or it can be turned into an improbable differential attack that covers more rounds than the impossible differential attack.

CLEFIA [8] is a 128-bit block cipher developed by Sony Corporation that has a generalized Feistel structure of four data lines. Security evaluations done by the designers [8, 9] show that impossible differential attack is one of the most powerful attacks against CLEFIA for they provided 10, 11, and 12-round impossible differential attacks on CLEFIA for 128, 192, and 256-bit key lengths, respectively. In [10, 11], Tsunoo et al. provided new impossible differential attacks on 12, 13, and 14-round CLEFIA for 128, 192, and 256-bit key lengths, respectively. Moreover, in [12], Zhang and Han provided a 14-round impossible differential attack on 128-bit keyed CLEFIA but due to the arguments on the time complexity, it remains unknown whether this attack scenario is successful or not.

In this work, we expand the 9-round impossible differentials introduced in [10] to 10-round improbable differentials and use them to attack 13, 14, and 15-round CLEFIA for 128, 192, and 256-bit key lengths, respectively. To the best of our knowledge, these are the best cryptanalytic results on CLEFIA. The paper is organized as follows: The description of the improbable differential attack, estimates of the data complexity, and expansion of impossible differentials to improbable differentials are given in Sect. 2. The notation and the description of CLEFIA is given in Sect. 3. In Sect. 4, we expand 9-round impossible differentials on CLEFIA to 10-round improbable differentials and use them to attack 13, 14, and 15-round CLEFIA. We conclude our paper with Sect. 5.

2 Improbable Differential Cryptanalysis

Statistical attacks on block ciphers make use of a property of the cipher so that an incident occurs with different probabilities depending on whether the correct key is used or not. We denote the probability of observing the incident under a wrong key with p and p_0 denotes the probability of observing the incident under the correct key.

In previously defined statistical differential attacks on block ciphers, a differential is more probable for the correct key than a random key (i.e. $p_0 > p$). Moreover, an impossible differential attack uses an impossible differential that is not possible when tried with the correct key (i.e. $p_0 = 0$). We define the improbable differential attack as a statistical differential attack in which a given differential is less probable than a random key (i.e. $p_0 < p$). Hence, improbable differential attacks can be seen as the exact opposite of differential attacks.

We aim to find a differential with α input difference and β output difference so that these differences are observed with probability p_0 for the correct key and with probability p for a wrong key where $p_0 < p$. One way of obtaining such differences is by finding nontrivial differentials that have α input difference and an output difference other than β, or vice versa. Hence these differentials reduce the probability of observing the differences α and β under the correct key.

We define an improbable differential as a differential that does not have the output difference β with a probability p', when the input difference is α. Thus, p' denotes the total probability of nontrivial differentials having α input difference with an output difference other than β. Hence for the correct key, probability of observing the α and β differences (i.e. satisfying the improbable differential) becomes $p_0 = p \cdot (1 - p')$. Note that p_0 is larger than $p \cdot (1 - p')$ if there are nontrivial differentials having α input difference and β output difference. Hence the attacker should check the existance of such differentials.

An improbable differential can be obtained by using a miss in the middle [3] like technique which we call the almost miss in the middle technique. Let α difference becomes δ with probability p_1 after r_1 rounds of encryption and β difference becomes γ after r_2 rounds of decryption as shown in Fig. 1. With the assumption that these two events are independent, if δ is different than γ, then α difference does not become β with probability $p' = p_1 \cdot p_2$ after $r_1 + r_2$ rounds of encryption. Note that p_1 and p_2 equal to 1 in the miss in the middle technqiue. Furthermore, we define an expansion method for constructing an improbable differential from an impossible differential in Sect. 2.2.

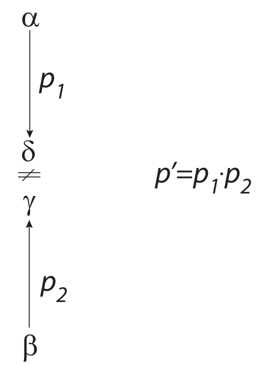

Fig. 1: Almost miss in the middle technique

Note that the impossible differential attacks can be seen as a special case of improbable differential attacks where the probability p' is taken as 1.

2.1 Data Complexity and Success Probability

Since p_0 is less than p, our aim is to use N plaintext pairs and count the hits that every guessed subkey gets and expect that the counter for the correct subkey to be less than a threshold T. Number of hits a wrong subkey gets can be seen as a random variable of a binomial distribution with parameters N, p (and a random variable of a binomial distribution with parameters N, p_0 for the correct subkey). We denote the *non-detection* error probability with p_{nd} which is the probability of the counter for the correct subkey to be higher than T. And we denote the *false alarm* error probability with p_{fa} which is the probability of the counter for a wrong subkey to be less than or equal to T. Therefore, the success probability of an improbable differential attack is $1 - p_{nd}$.

Accurate estimates of the data complexity and success probability for many statistical attacks are provided by Blondeau et al. in [6, 7] and these estimates can be used for improbable differential attacks with some modifications. Unlike improbable differential cryptanalysis, in most of the statistical attacks $p_0 > p$ and this assumption is made throughout [6]. Hence, we need to modify the approximations N', N'' and N_∞ of the number of required samples N that are given in [6] for the $p_0 < p$ case in order to use them for improbable differential attacks. We first define the Kullback-Leibler divergence which plays an important role in these estimates.

Definition 1 (Kullback-Leibler divergence [13]). *Let P and Q be two Bernoulli probability distributions of parameters p and q. The Kullback - Leibler divergence between P and Q is defined by*

$$D(p||q) = p \ \ln\left(\frac{p}{q}\right) + (1-p) \ \ln\left(\frac{1-p}{1-q}\right).$$

Secondly, we modify Algorithm 1 of [6] for the $p_0 < p$ case which computes the exact number of required samples N and corresponding relative threshold $\tau := \frac{T}{N}$ to reach error probabilities less than (p_{nd}, p_{fa}). The estimates for non-detection and false alarm error probabilities are denoted by $G_{nd}(N, \tau)$ and $G_{fa}(N, \tau)$.

Algorithm 1. [from [6], modified for the $p_0 < p$ Case]

```
Input: $p_0$, $p$, $p_{nd}$, $p_{fa}$
Output: $N$, $\tau$
$\tau_{min} := p_0$, $\tau_{max} := p$
repeat
    $\tau := \frac{\tau_{min}+\tau_{max}}{2}$
    Compute $N_{nd}$ such that $\forall N > N_{nd}$, $G_{nd}(N, \tau) \leq p_{nd}$
    Compute $N_{fa}$ such that $\forall N > N_{fa}$, $G_{fa}(N, \tau) \leq p_{fa}$
    if $N_{nd} > N_{fa}$ then $\tau_{min} = \tau$
    else $\tau_{max} = \tau$
until $N_{nd} = N_{fa}$
$N := N_{nd}$
Return $N$, $\tau$
```

N_{nd} and N_{fa} can be calculated by a dichotomic search and the following Equations 1 and 2 can be used for the estimates $G_{nd}(N, \tau)$ and $G_{fa}(N, \tau)$, respectively. The number of samples obtained from the algorithm with these estimates is denoted by N_∞.

Theorem 1 ([14]). *Let p_0 and p be two real numbers such that $0 < p_0 < p < 1$ and let τ such that $p_0 < \tau < p$. Let Σ_0 and Σ_k follow a binomial law of respective parameters (N, p_0) and (N, p). Then as $N \to \infty$,*

$$P(\Sigma_0 \geq \tau N) \sim \frac{(1-p_0)\sqrt{\tau}}{(\tau - p_0)\sqrt{2\pi N(1-\tau)}} e^{-ND(\tau||p_0)}, \tag{1}$$

and

$$P(\Sigma_k \leq \tau N) \sim \frac{p\sqrt{1-\tau}}{(p-\tau)\sqrt{2\pi N \tau}} e^{-ND(\tau||p)}. \tag{2}$$

A simple approximation N' of N is defined in [6] when the relative threshold is chosen as $\tau = p_0$ which makes non-detection error probability p_{nd} of order 1/2. We define N' for the $p_0 < p$ case as in [15]:

Proposition 1. *For a relative threshold $\tau = p_0$, a good approximation of the required number of pairs N to distinguish between the correctly keyed permutation and an incorrectly keyed permutation with false alarm probability less than or equal to p_{fa} is*

$$N' = -\frac{1}{D(p_0||p)}\left[\ln\left(\frac{\nu \cdot p_{fa}}{\sqrt{D(p_0||p)}}\right) + 0.5\ln(-\ln(\nu \cdot p_{fa}))\right] \tag{3}$$

where

$$\nu = \frac{(p - p_0)\sqrt{2\pi p_0}}{p\sqrt{(1 - p_0)}}.$$

In [6] a good approximation of N' which is also valid for the $p_0 < p$ case is defined as follows

$$N'' = -\frac{\ln(2\sqrt{\pi}p_{fa})}{D(p_0||p)}. \tag{4}$$

2.2 Improbable Differentials from Impossible Differentials

An improbable differential can be obtained by combining a differential (or two) with an impossible differential in order to obtain improbable differentials covering more rounds. Let $\delta \nrightarrow \gamma$ be an impossible differential and $\alpha \rightarrow \delta$ and $\gamma \leftarrow \beta$ be two differentials with probabilities p_1 and p_2, respectively. Then we can construct improbable differentials $\alpha \nrightarrow \gamma$, $\delta \nrightarrow \beta$ and $\alpha \nrightarrow \beta$ with probabilities p' equal to p_1, p_2 and $p_1 \cdot p_2$ as shown in Fig. 2.

This expansion method can be used to construct improbable differentials to distinguish more rounds of the cipher from a random permutation; or an impossible differential attack can be turned into an improbable differential attack on more rounds of the cipher when suitable differentials $\alpha \rightarrow \delta$ or $\gamma \leftarrow \beta$ exist. However, such a conversion might require more data to obtain the correct key and hence result in higher data and time complexity. If the size of the guessed key decreases in the converted improbable differential attack, so does the memory complexity. The guessed subkeys can be represented by one bit of an array in impossible differential attacks. However, we need to keep counters for the subkeys in improbable differential attacks and hence the memory complexity is higher when the same number of subkeys are guessed.

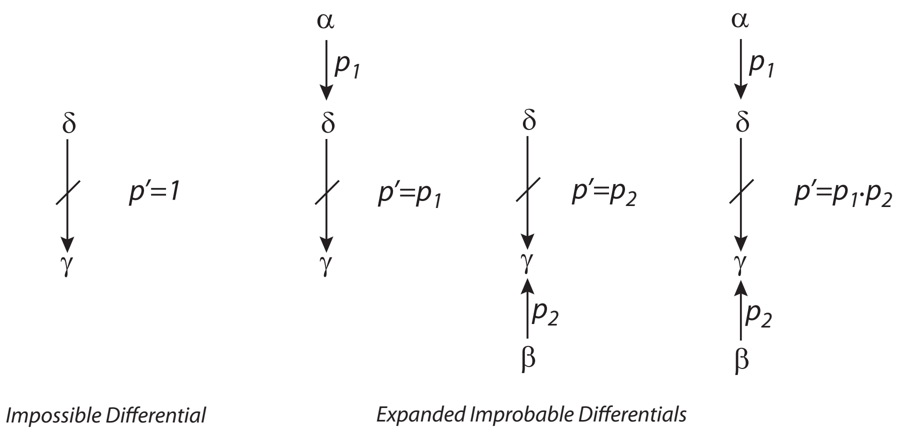

Fig. 2: Expansion of an impossible differential to improbable differentials

3 Notation and the CLEFIA

3.1 Notation

We use the following notations in the following sections.

Table 1: Notation

$a_{(b)}$	b denotes the bit length of a
$a\|b$	Concatenation of a and b
$[a, b]$	Vector representation of a and b
a^t	Transposition of a vector a
$a \oplus b$	Bitwise exclusive-OR (XOR) of a and b
$[x^{\{i,0\}}, x^{\{i,1\}}, x^{\{i,2\}}, x^{\{i,3\}}]$	i-th round output data
Δa	XOR difference for a

3.2 CLEFIA

CLEFIA is a 128-bit block cipher having a generalized Feistel structure with four data lines. For the key lengths of 128, 192, and 256 bits, CLEFIA has 18, 22, and 26 rounds. Each round contains two parallel F functions, F_0 and F_1 and their structures are shown in Fig. 3 where S_0 and S_1 are

8×8-bit S-boxes. The two matrices M_0 and M_1 that are used in the F-functions are defined as follows.

$$M_0 = \begin{pmatrix} 0x01 & 0x02 & 0x04 & 0x06 \\ 0x02 & 0x01 & 0x06 & 0x04 \\ 0x04 & 0x06 & 0x01 & 0x02 \\ 0x06 & 0x04 & 0x02 & 0x01 \end{pmatrix}, \qquad M_1 = \begin{pmatrix} 0x01 & 0x08 & 0x02 & 0x0a \\ 0x08 & 0x01 & 0x0a & 0x02 \\ 0x02 & 0x0a & 0x01 & 0x08 \\ 0x0a & 0x02 & 0x08 & 0x01 \end{pmatrix}.$$

The encryption function uses four 32-bit whitening keys (WK_0, WK_1, WK_2, WK_3) and $2r$ 32-bit round keys ($RK_0, \ldots, RK_{2r-1}$) where r is the number of rounds. We represent the bytes of a round key as $RK_i = RK_{i,0}|RK_{i,1}|RK_{i,2}|RK_{i,3}$. The encryption function ENC_r is shown in Fig. 4.

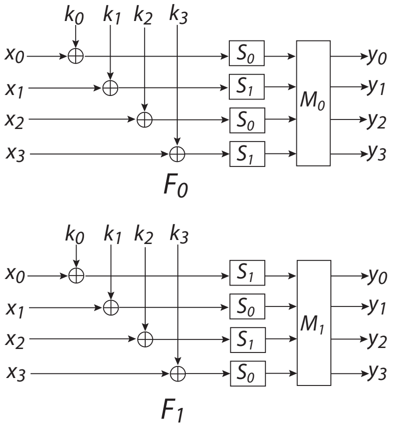

Fig. 3: F_0 and F_1 functions

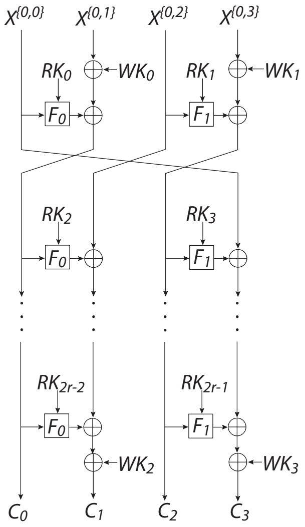

Fig. 4: Encryption function

4 Improbable Differential Attacks on CLEFIA

In this section, we present 10-round improbable differentials and introduce an improbable differential attack on 13-round CLEFIA with key length of 128 bits. We also introduce improbable differential attacks on 14 and 15-round CLEFIA for key lengths 196 and 256 bits in Appendix A and B. In these attacks our aim is to derive the round keys and we do not consider the key scheduling part as done in [9–11].

4.1 10-round Improbable Differentials

We will use the following two 9-round impossible differentials that are introduced in [10],

$$\begin{aligned}
&[0_{(32)}, 0_{(32)}, 0_{(32)}, [X, 0, 0, 0]_{(32)}] \nrightarrow_{9r} [0_{(32)}, 0_{(32)}, 0_{(32)}, [0, Y, 0, 0]_{(32)}] \\
&[0_{(32)}, 0_{(32)}, 0_{(32)}, [0, 0, X, 0]_{(32)}] \nrightarrow_{9r} [0_{(32)}, 0_{(32)}, 0_{(32)}, [0, Y, 0, 0]_{(32)}]
\end{aligned}$$

where $X_{(8)}$ and $Y_{(8)}$ are non-zero differences. We obtain 10-round improbable differentials by adding the following one-round differentials to the top of these 9-round impossible differentials,

$$\begin{aligned}
&[[\psi, 0, 0, 0]_{(32)}, \zeta_{(32)}, 0_{(32)}, 0_{(32)}] \rightarrow_{1r} [0_{(32)}, 0_{(32)}, 0_{(32)}, [\psi, 0, 0, 0]_{(32)}] \\
&[[0, 0, \psi, 0]_{(32)}, \zeta'_{(32)}, 0_{(32)}, 0_{(32)}] \rightarrow_{1r} [0_{(32)}, 0_{(32)}, 0_{(32)}, [0, 0, \psi, 0]_{(32)}]
\end{aligned}$$

which hold when the output difference of the F_0 function is ζ (resp. ζ') when the input difference is $[\psi, 0, 0, 0]$ (resp. $[0, 0, \psi, 0]$). We choose ψ and corresponding ζ and ζ' depending on the difference distribution table (DDT) of S_0 in order to increase the probability of the differential. One can observe that the values 10, 8, 6 and 4 appear 9, 119, 848 and 5037 times in the DDT of S_0, respectively. When ψ, ζ and ζ' is chosen according to these differences, the average probability of the 10-round improbable differentials becomes

$$p' = ((9 \cdot 10 + 119 \cdot 8 + 848 \cdot 6 + 5037 \cdot 4)/256)/6013 \approx 2^{-5.87}.$$

4.2 Improbable Differential Attack on 13-Round CLEFIA

We put one additional round on the plaintext side and two additional rounds on the ciphertext side of the 10-round improbable differentials to attack first 13 rounds of CLEFIA that captures RK_1, $RK_{23,1} \oplus WK_{2,1}$, RK_{24}, and RK_{25}.

We place the whitening key WK_2 at the XOR with the 11th-round output word $x^{\{11,2\}}$ and XOR with RK_{23}. Moreover, we place the whitening key WK_1 at the XOR with the first round output word $x^{\{1,2\}}$, as shown in Fig. 5. These movements are equivalent transformations.

Data Collection. For a single choice of ψ and corresponding ζ values, we choose 2^K structures of plaintexts where the first word $x^{\{1,0\}}$ and the second, third and fourth bytes of the second word $x^{\{1,1\}}$ are fixed (similarly, we fix the first, second and fourth bytes of the second word $x^{\{1,1\}}$ for a choice of ψ and ζ'). We construct pairs where the first byte (resp. third byte) of the second word $x^{\{1,1\}}$ has the difference ψ, the third

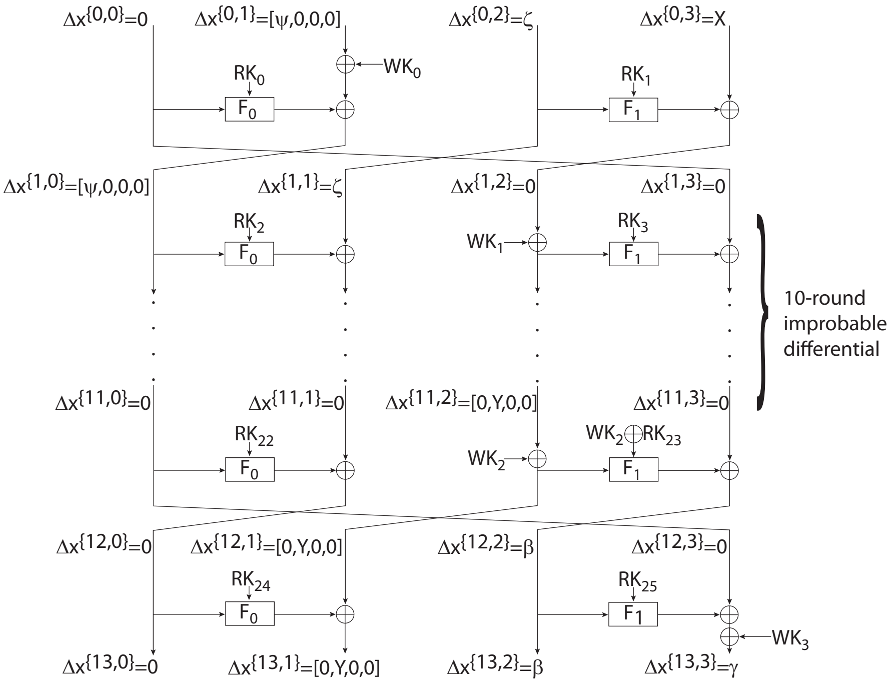

Fig. 5: Improbable differential attack on 13-round CLEFIA

word $x^{\{1,2\}}$ has the difference ζ (resp. ζ') and the fourth word $x^{\{1,3\}}$ has the same difference with the output of F_1, which is obtained from the guessed round key RK_1, when the input difference of F_1 is ζ (resp. ζ'). Such a structure proposes $2 \cdot 6013 \cdot 2^{71}$ pairs.

We keep the ciphertext pairs having the difference $[0,[0,Y,0,0],\beta,\gamma]$ where γ is non-zero and β represents every 255 difference value that can be obtained from the multiplication of M_1 with $[0,Y,0,0]^t$. Such a difference in the ciphertext pairs is observed with a probability of $1/2^{32} \cdot 255/2^{32} \cdot 255/2^{32} \cdot (2^{32}-1)/2^{32} \approx 2^{-80}$. Therefore, $6013 \cdot 2^{K-8}$ pairs remain.

Key Recovery. We keep counters for $RK_{23,1} \oplus WK_{2,1}|RK_{24}|RK_{25}$ for every guess of RK_1 and increase the corresponding counter when the improbable differential is obtained with a guessed key. Keys satisfying the improbable differential are obtained by differential table look-ups indexed on the input and the output differences of the 12th-round F_1 and 13th-round F_1. The probability of satisfying the improbable differential for a wrong key is $p = 2^{-40}$ from the average probabilities 2^{-8} and 2^{-32} for the 12th and 13th-round F_1 functions respectively. Therefore, the probability of obtaining the improbable differential for the correct key is $p_0 = p \cdot (1 - p') \approx 2^{-40.02}$.

During the attack we try to obtain the 104-bit round key, namely RK_1, $RK_{23,1} \oplus WK_{2,1}$, RK_{24}, RK_{25} and for the correct key to get the least number of hits, false alarm probability p_{fa} must be less than 2^{-104}. Feeding the Algorithm 1 with the inputs p, p_0, $p_{fa} = 2^{-105}$, and $p_{nd} = 1/100$ shows that when the threshold T is $673474 < 2^{20}$, $N_\infty \approx 2^{59.38}$ pairs are needed for the correct key to remain below the threshold and all of the wrong ones to remain above it with a success probability of 99%.

Attack Complexity. With the 2^{80} ciphertext filtering conditions, we need $2^{80} \cdot 2^{59.38} = 2^{139.38}$ pairs to perform the attack. Since we have 6013 choices for ψ, we need $2^K \approx 2^{54.83}$ structures so that $6013 \cdot 2^{72+K} = 2^{139.38}$. Hence, the data complexity of the attack is $2^{126.83}$ chosen plaintexts.

For every guess of RK_1 and RK_{24} and for every choice of ψ, we perform $2^{59.38}$ F-function computations which is $2^{64} \cdot 2^{59.38} \cdot 1/2 \cdot 1/13 \approx 2^{118.68}$ encryptions. However, the time complexity is $2^{126.83}$ encryptions for obtaining the ciphertexts.

The memory complexity of the attack comes from the 20-bit counters kept for the 104-bit round keys $RK_1 | RK_{23,1} \oplus WK_{2,1} | RK_{24} | RK_{25}$, which require $20 \cdot 2^{104} \approx 2^{108.32}$ bits.

5 Conclusion

In previously defined statistical differential attacks on block ciphers, attacker's aim is to find an incident that is more probable for the correct key than a random key. Moreover, an impossible differential attack uses an impossible differential that is not possible when tried with the correct key. However, in this paper we introduced the improbable differential attack in which a given differential is less probable when tried with the correct key. Hence the impossible differential attack is just a special case of the improbable differential attack. We also modified the data complexity estimates given for statistical attacks by Blondeau et al. in order to use them in improbable differential attacks.

Moreover, we defined the almost miss in the middle technique for obtaining improbable differentials and we introduced a method for expanding impossible differentials to improbable differentials when suitable differentials that can be put on the top or the bottom of an impossible differential exist. Finally, we proposed improbable differential attacks on 13, 14, and 15-round CLEFIA by using this expansion method. To the best of our knowledge, these are the best cryptanalytic results on CLEFIA. Results of these improbable differential attacks and the impossible differential attacks of [10] on CLEFIA are summarized in Table 2.

In order to provide security against improbable attacks, block cipher designers should ensure that their designs contain no good improbable differentials. Since the almost miss in the middle technique uses two truncated differentials, providing upper bounds for truncated differentials may be used to provide security against improbable attacks.

Table 2: Results of the impossible differential attacks of [10] and improbable differential attacks on CLEFIA

#Rounds	Attack Type	Key Length	Data Complexity	Time Complexity	Memory (blocks)	Success Probability	Reference
12	Impossible	128, 192, 256	$2^{118.9}$	2^{119}	2^{73}	-	[10]
13	Improbable	128, 192, 256	$2^{126.83}$	$2^{126.83}$	$2^{101.32}$	%99	Sect. 4.2
13	Impossible	192, 256	$2^{119.8}$	2^{146}	2^{120}	-	[10]
14	Improbable	192, 256	$2^{126.98}$	$2^{183.17}$	$2^{126.98}$	%99	App. A
14	Impossible	256	$2^{120.3}$	2^{212}	2^{121}	-	[10]
15	Improbable	256	$2^{127.40}$	$2^{247.49}$	$2^{127.40}$	%99	App. B

6 Acknowledgments

I would like to express my deep gratitude to Ali Aydın Selçuk for his review and invaluable comments. I would like to thank Céline Blondeau for providing additional information about complexity estimates. I am grateful to Kerem Varıcı, Onur Özen and Meltem Sönmez Turan for their helpful comments. I also would like to anonymous referee for pointing out the earlier works [4] and [5].

References

1. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. J. Cryptology **4**(1) (1991) 3–72
2. Knudsen, L.R.: Truncated and higher order differentials. In Preneel, B., ed.: FSE. Volume 1008 of Lecture Notes in Computer Science., Springer (1994) 196–211
3. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. J. Cryptology **18**(4) (2005) 291–311
4. Borst, J., Knudsen, L.R., Rijmen, V.: Two attacks on reduced IDEA. In: EUROCRYPT'97: Proceedings of the 16th annual international conference on Theory

and application of cryptographic techniques, Berlin, Heidelberg, Springer-Verlag (1997) 1–13

5. Knudsen, L.R., Rijmen, V.: On the decorrelated fast cipher (DFC) and its theory. In: FSE '99: Proceedings of the 6th International Workshop on Fast Software Encryption, London, UK, Springer-Verlag (1999) 81–94
6. Blondeau, C., Gérard, B.: On the data complexity of statistical attacks against block ciphers. In Kholosha, A., Rosnes, E., M.Parker, eds.: Workshop on Coding and Cryptography - WCC 2009, Ullensvang, Norway (May 2009) 469–488
7. Blondeau, C., Gérard, B., Tillich, J.P.: Accurate Estimates of the Data Complexity and Success Probability for Various Cryptanalyses. To appear in Journal of Designs, Codes and Cryptography
8. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (extended abstract). In Biryukov, A., ed.: FSE. Volume 4593 of Lecture Notes in Computer Science., Springer (2007) 181–195
9. Sony Corporation: The 128-bit Blockcipher CLEFIA, Security and Performance Evaluations, Revision 1.0, June 1 (2007), http://www.sony.net/Products/cryptography/clefia/
10. Tsunoo, Y., Tsujihara, E., Shigeri, M., Saito, T., Suzaki, T., Kubo, H.: Impossible differential cryptanalysis of CLEFIA. In Nyberg, K., ed.: FSE. Volume 5086 of Lecture Notes in Computer Science., Springer (2008) 398–411
11. Tsunoo, Y., Tsujihara, E., Shigeri, M., Suzaki, T., Kawabata, T.: Cryptanalysis of CLEFIA using multiple impossible differentials. In: International Symposium on Information Theory and Its Applications - ISITA 2008. (7-10 2008) 1–6
12. Zhang, W., Han, J.: Impossible differential analysis of reduced round CLEFIA. In Yung, M., Liu, P., Lin, D., eds.: Inscrypt. Volume 5487 of Lecture Notes in Computer Science., Springer (2008) 181–191
13. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley series in communications. Wiley (1991)
14. Arratia, R., Gordon, L.: Tutorial on large deviations for the binomial distribution. In: Bulletin of Mathematical Biology 51. (1989) 125–131
15. Blondeau, C.: Private communication (2009)

A Improbable Differential Attack on 14-Round CLEFIA

We expand our 13-round attack by one round on the ciphertext side to break 14-round CLEFIA for the key length of 192 or 256 bits. This attack captures 168 bits of the round keys, namely RK_1, $RK_{23,1}$, $RK_{24} \oplus WK_3$, $RK_{25} \oplus WK_2$, RK_{26}, and RK_{27}.

We move the whitening keys WK_1, WK_2, and WK_3 in the same way as in the 13-round attack.

Data Collection. We generate pairs in the same way as in the 13-round attack and we want 13th-round output difference to be $[[0, Y, 0, 0], \beta, \gamma, 0]$ to perform the attack. Consequently, we keep the ciphertext pairs satisfying the difference $[[0, Y, 0, 0], \beta', \gamma, \delta]$ where γ and δ are non-zero and β' is the XOR of β with the 255 possible values that can be obtained from the multiplication of M_0 with $[0, Y, 0, 0]^t$. Such a difference in ciphertext pairs is observed with a probability of $255/2^{32} \cdot ((255 \cdot 255)/2^{32} \cdot (2^{32} - 1)/2^{32} \cdot (2^{32} - 1)/2^{32} \approx 2^{-40}$. Therefore, $6013 \cdot 2^{K+32}$ pairs remain.

Key Recovery. We guess the second byte of RK_{24} and check if the second word of the output of 13th-round has difference β. The probability of this event is 2^{-8} and therefore, $6013 \cdot 2^{K+24}$ pairs remain. In order to check whether the 72-bit key $RK_{23,1}|RK_{25} \oplus WK_2|RK_{27}$ satisfies the improbable differential, we use differential tables indexed on the input and output differences of the 12th-round, 13th-round and 14th-round F_1 functions. The input values of these F_1 functions are obtained by the guesses of $RK_{24} \oplus WK_3$ and the first, third and fourth bytes of RK_{26}. The input of the 13th-round F_0 is obtained from RK_{27} candidates.

The probability of a candidate key to satisfy the improbable differential using three F_1 differential tables is $p = 2^{-72}$ from the average probabilities 2^{-8}, 2^{-32} and 2^{-32} for the 12th, 13th and 14th-round F_1 functions, respectively. Feeding the Algorithm 1 with the inputs p, p_0, $p_{fa} = 2^{-169}$, and $p_{nd} = 1/100$ shows that when the threshold T is $1022026 < 2^{20}$, $N_\infty \approx 2^{91.98}$ pairs are needed for the correct key to remain below the threshold and all of the wrong ones to remain above it with a success probability of 99%.

Keeping a key table for the attacked 168 key bits would require a memory that exceeds 2^{128} blocks where a block is 128 bits long. For this reason, we keep all of the $2^{126.98}$ plaintexts in a table, then guess RK_1 and choose the plaintext pairs for the attack.

Attack Complexity. We need $2^{91.98+40+8} = 2^{139.98}$ pairs in total to perform the attack. Since we have 6013 choices for ψ, we need $2^K \approx 2^{54.98}$ structures so that $6013 \cdot 2^{72+K} = 2^{139.98}$. Hence, the attack has data complexity of $2^{126.98}$ chosen plaintexts.

For every guess of RK_1, $RK_{24} \oplus WK_3$, and RK_{26}, we perform $2^{91.98}$ F-function computations which is $2^{96} \cdot 2^{91.98} \cdot 1/2 \cdot 1/14 \approx 2^{183.17}$ encryptions.

We keep 20-bit counters for the 72-bit keys $RK_{23,1}|RK_{25} \oplus WK_2|RK_{27}$ but the memory complexity is dominated by the ciphertext table of $2^{126.98}$ blocks.

B Improbable Differential Attack on 15-Round CLEFIA

We expand the 14-round improbable differential attack by one round on the ciphertext side to attack 15-round CLEFIA in which we exhaustively search for the 15th-round keys RK_{28} and RK_{29}. Our aim is to obtain the value of the 232-bit round key, namely RK_1, $RK_{23,1}$, RK_{24}, RK_{25}, $RK_{26} \oplus WK_3$, $RK_{27} \oplus WK_2$, RK_{28} and RK_{29}.

We move the whitening keys WK_1, WK_2, and WK_3 in the same way as in the 14-round attack.

For the inputs $p = 2^{-72}$, p_0, $p_{fa} = 2^{-233}$, and $p_{nd} = 1/100$, Algorithm 1 produces the outputs $N_\infty \approx 2^{92.40}$ and $T = 1361613 < 2^{21}$. Hence, the data complexity of the attack is $2^{127.40}$ chosen plaintexts and the memory complexity is $2^{127.40}$ blocks.

The time complexity of the attack comes from $2^{92.40}$ F-function computations for RK_1, RK_{24}, $RK_{26} \oplus WK_3$ guesses and the exhaustive search of RK_{28} and RK_{29}, which is $2^{92.40} \cdot 2^{96} \cdot 2 \cdot 2^{64} \cdot 1/2 \cdot 1/15 \approx 2^{247.49}$ encryptions.