Hindawi
Security and Communication Networks
Volume 2018, Article ID 7393401, 11 pages
https://doi.org/10.1155/2018/7393401

Research Article

On the Complexity of Impossible Differential Cryptanalysis

Qianqian Yang[1,2,3] **Lei Hu**[1,2,3] **Danping Shi**[1,2,3] **Yosuke Todo**[4] **and Siwei Sun**[1,2,3]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China*
[2]*Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing, China*
[3]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China*
[4]*NTT Secure Platform Laboratories, Tokyo, Japan*

Correspondence should be addressed to Lei Hu; hu@is.ac.cn

Received 12 September 2017; Accepted 20 December 2017; Published 17 April 2018

Academic Editor: Jiankun Hu

While impossible differential attack is one of the most well-known and familiar techniques for symmetric-key cryptanalysts, its subtlety and complicacy make the construction and verification of such attacks difficult and error-prone. We introduce a new set of notations for impossible differential analysis. These notations lead to unified formulas for estimation of data complexities of ordinary impossible differential attacks and attacks employing multiple impossible differentials. We also identify an interesting point from the new formulas: in most cases, the data complexity is only related to the form of the underlying distinguisher and has nothing to do with how the differences at the beginning and the end of the distinguisher propagate in the outer rounds. We check the formulas with some examples, and the results are all matching. Since the estimation of the time complexity is flawed in some situations, in this work, we show under which condition the formula is valid and give a simple time complexity estimation for impossible differential attack which is always achievable.

1. Introduction

Impossible differential attack, introduced by Knudsen [1] and Biham et al. [2] independently, is one of the most well-known cryptanalytic techniques for symmetric-key cryptanalysts [3–9]. Generally, in impossible differential cryptanalysis, we guess some key bits involved in the outer rounds of the target cipher. Then the guess is rejected if it leads to impossible differentials at the inner rounds. Despite its extensive application in symmetric-key cryptanalysis, errors in the analysis are often discovered and many papers in the literature presented subtle flaws. Note that the flaws typically arise in the estimation of the time and data complexities rather than in the distinguisher, similar to searching differential and linear characteristic [10–13], the methodology of searching for impossible differential is fairly mature, and automatic tools are available [14–17]. To relieve the difficulty of the complexity analysis, Boura et al. presented generic complexity analysis formulas along with the development of new ideas for optimizing impossible differential cryptanalysis [18]. However, at FSE 2016, Derbez identified some flaws in the formulas for the time complexity estimation given in [18], and concrete examples were presented such that the time complexities estimated with the formulas given in [19] are not achievable.

Our contribution follows Boura, Naya-Plasencia, Suder, and Derbez's work at ASIACRYPT 2014, FSE 2016, and ESC 2017; we investigate further some aspects of the estimation of the impossible differential attack which have not been explored or stated explicitly in previous work.

Firstly, we introduce a new set of notations for impossible differential analysis. With these notations, there is no difference between ordinary impossible differentials and multiple impossible differentials. Under some reasonable assumptions (the same assumptions were made implicitly in [18, 19]), we modify the formula in [18] for calculating the data complexity into a form getting rid of the parameters of the number of bit-conditions (the c_{in} and c_{out} notations in [18]) that have to be verified to follow some specified behavior in the outer rounds of a target cipher. Moreover, in the formulas derived with the new notations, we identify

a very interesting and somehow strange point: in most cases, the data complexity is only related to the form of the underlying distinguisher and has nothing to do with how the differences at the beginning and the end of the distinguisher propagate in the outer rounds. That is, in most cases, the data complexity can be completely determined by the underlying impossible differential distinguisher employed in the attack. Hence, estimating the data complexity with the new formulas is much more easier and straightforward than that of [18].

Secondly, since Derbez showed concrete examples where Boura et al.'s formula of the time complexity of impossible differential attack is invalid, we are interested in the condition under which the estimation of Boura et al. is correct, and we prove that the time complexity of the key-sieving process given by Boura et al. is not only achievable but also optimal if the key bits involved in the outer rounds are independent. Using the early abort technique presented by Lu et al. in [20, 21], we give the optimal result with detailed process.

Finally, we give a formula to estimate the time complexity of the key-sieving process in the case where the key bits involved in the outer rounds are not independent. The estimation is not guaranteed to be equal to the complexity of the optimal attack as discussed by Derbez in [19], but it is always achievable. Therefore, the formula serves to give a rough estimation of an impossible differential attack without diving into complicated calculations and time-consuming search algorithms, which should be very useful in fast prototyping in cryptanalysis.

We present a new set of notations for impossible differential analysis in Section 2. Section 3 briefly shows impossible differential attacks. In Section 4, we modify the data formula, which is related to a few parameters and unifies multiple impossible differential attacks with ordinary impossible differential attacks. In Section 5 we prove that the formula of the time complexity is achievable and optimal with the key bits independent and give a rough estimation formula for the key bits without independence. At last we conclude the paper in Section 6.

2. Notations

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field of two elements. For a set A, its number of elements is denoted by $|A|$, and let $\|A\| = \log_2(|A|)$. Also, for an integer n, let $\|n\| = \log_2(n)$.

In addition, we use some notations like regular expression to represent a set of bit strings. For example, $\mathtt{1}$ is equivalent to the set $\{1\}$, $\mathtt{0}$ is equivalent to $\{0\}$, and $\mathtt{0001}$ is equivalent to $\{000001, 000011, 000101, 000111\}$, which is alternatively denoted by $\mathtt{0}_3*_2\mathtt{1}$, where the subscript tells the number of occurrences of the symbol concerned.

Definition 1. Let $\mathscr{E}_K(\cdot)$ be a block cipher and $\alpha, \beta \in \mathbb{F}_2^n$; if $\forall K$, $E_K(x \oplus \alpha) \oplus \mathscr{E}_K(x) \neq \beta$ for all $x \in \mathbb{F}_2^n$, we call (α, β) an impossible differential of $\mathscr{E}$, which is denoted by $\alpha \nrightarrow \beta$. More generally, let $\mathbb{A}, \mathbb{B} \subseteq \mathbb{F}_2^n$; we call $(\mathbb{A}, \mathbb{B})$ an impossible differential, denoted by $\mathbb{A} \nrightarrow \mathbb{B}$, if for any $\alpha \in \mathbb{A}$, $\exists \beta \in \mathbb{B}$, such that $\alpha \nrightarrow \beta$, and for any $\beta \in \mathbb{B}$, $\exists \alpha \in \mathbb{A}$, such that $\alpha \nrightarrow \beta$.

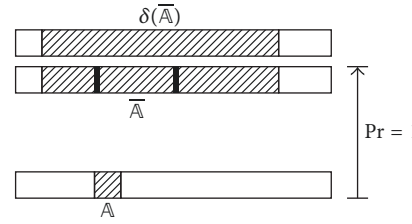

Figure 1: The relationship in $\mathbb{A}$, $\overline{\mathbb{A}}$, and $\delta(\mathbb{A})$.

Note that this notation is different from the notation of impossible differential we typically see in the literature, since in our notation, it is possible that $\exists\alpha \in \mathbb{A}$ and $\exists\beta \in \mathbb{B}$, such that $\alpha \to \beta$ is not an impossible differential.

Let $\mathsf{ID}_{E_K}(\mathbb{A}, \mathbb{B}) = \{(\alpha, \beta) : \alpha \nrightarrow \beta, \alpha \in \mathbb{A}, \beta \in \mathbb{B}\}$, where ID_{E_K} is simply written as ID if E_K is clear from the context. Then we have $\|\mathsf{ID}(\mathbb{A}, \mathbb{B})\| \leq \|\mathbb{A}\| + \|\mathbb{B}\|$, and $\|\mathsf{ID}(\mathbb{A}, \mathbb{B})\| = \|\mathbb{A}\| + \|\mathbb{B}\|$ in the special case for any $\alpha \in \mathbb{A}$ and $\beta \in \mathbb{B}$, $\alpha \nrightarrow \beta$. It is worth mentioning, with the new notation, that we can unify ordinary impossible differentials and multiple impossible differentials in impossible differential cryptanalysis.

For example, if $0011 \nrightarrow 0001$, $0011 \nrightarrow 0010$, and $0011 \to 0011$, with the new notation, we call $(0011, 00**)$ an impossible differential, and $\|\mathsf{ID}(0011, 00**)\| = \log_2(2) = 1$.

Definition 2. Let $\overline{\mathbb{A}} \subseteq \mathbb{F}_2^n$, and the structure $\delta(\overline{\mathbb{A}})$ derived from $\overline{\mathbb{A}}$ is defined to be the set of all n-bit strings $y = y_0 \cdots y_{n-1}$ such that $y_i \equiv 0$ for all $i \in \{j : \forall x \in \overline{\mathbb{A}}, x_j = 0\}$. Given a bit string $x \in \mathbb{F}_2^n$, $\delta_x(\overline{\mathbb{A}})$ is defined to be the set $x + \delta(\overline{\mathbb{A}}) = \{x \oplus y : y \in \delta(\overline{\mathbb{A}})\}$.

For example, if $\overline{\mathbb{A}} = \{0010, 0011, 1010, 1011\}$ and $x = 0100$, then

$$\delta\left(\overline{\mathbb{A}}\right) = \{0000, 0001, 0010, 0011, 1000, 1001, 1010, 1011\} \tag{1}$$

and $\delta_{0100}(\overline{\mathbb{A}}) = \{0100, 0101, 0110, 0111, 1100, 1101, 1110, 1111\}$. Recall that, in differential type of cryptanalysis, if we want to get many pairs of data whose differences are in a set $\overline{\mathbb{A}}$, we typically first prepare a structure $\delta(\overline{\mathbb{A}})$ from which the needed pairs will be generated. From Figure 1, we can see the relationship in $\mathbb{A}$, $\overline{\mathbb{A}}$, and $\delta(\overline{\mathbb{A}})$.

3. Impossible Differential Attack

In contrast to ordinary differential attack which relies on differentials with high probability, impossible differential attack reduces the key space by identifying wrong key guesses with the aid of differentials which never occur.

We show how to convert an impossible differential distinguisher into a key-recovery attack in Figure 2. Firstly, we need to append some outer rounds (E_1 with r_{in} rounds and E_3 with r_{out} rounds) around the distinguisher $(\mathbb{A}, \mathbb{B})$ with r_Δ rounds covering E_2. Then we propagate the differences in $\mathbb{A}$

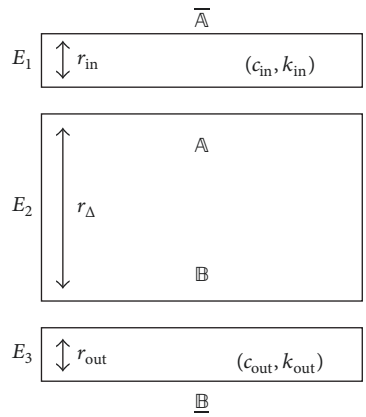

Figure 2: Generic vision of impossible differential attack.

and $\mathbb{B}$ to both directions in the outer rounds to get $\overline{\mathbb{A}}$ and $\underline{\mathbb{B}}$, where $\overline{\mathbb{A}}$ is the set of all differences having the possibility of creating an intermediate difference in $\mathbb{A}$ at the beginning of E_2, and $\underline{\mathbb{B}}$ is defined similarly. For fixed outer rounds, $\overline{\mathbb{A}}$ and $\underline{\mathbb{B}}$ are not dependent on the involved secret key bits in the outer rounds. Actually they can be computed by propagating the difference patterns upwards and downwards according to the differential distribution table of the components of the cipher. Now we can identify the involved secret key bits in the outer rounds. These key bits are the secret information we are going to recover in the attack, which we call the *targeted key bits*. Finally, we prepare some structures $\delta_x(\overline{\mathbb{A}})$ and encrypt the plaintexts in $\delta_x(\overline{\mathbb{A}})$ to get the corresponding ciphertexts. For each pair (P, P') of plaintexts in $\delta_x(\overline{\mathbb{A}})$ satisfying $P \oplus P' \in \overline{\mathbb{A}}$, guess the secret key information $k_{\text{in}} \cup k_{\text{out}}$ involved in the outer rounds. If the partial encryption/decryption of (P, P') and $(E(P), E(P'))$ leads to impossible differentials, the guess is certainly incorrect. With this strategy, hopefully we can reject lots of wrong guesses of $k_{\text{in}} \cup k_{\text{out}}$, and the key space is therefore reduced. To calculate complexity of the attack, we define c_{in} which is the number of bit-conditions that have to be verified to obtain $\mathbb{A}$ from $\overline{\mathbb{A}}$. In other words, the differences $\overline{\mathbb{A}}$ are propagated from $\mathbb{A}$ with probability 1 while the differential $\mathbb{A} \leftarrow \overline{\mathbb{A}}$ is verified with probability $1/2^{c_{\text{in}}}$. Similarly, we can get the definition of c_{out}.

4. On the Data Complexity of Impossible Differential Attack

Assuming that we have identified an impossible differential $\mathbb{A} \nrightarrow \mathbb{B}$, we propagate $\mathbb{A}$ and $\mathbb{B}$ differentials to both directions to get $\overline{\mathbb{A}}$ and $\underline{\mathbb{B}}$. Then we prepare many structures $\delta_x(\overline{\mathbb{A}})$ by varying $x \in \mathbb{F}_2^n$. For each structure $\delta_x(\overline{\mathbb{A}})$, there are $2^{2\|\delta(\overline{\mathbb{A}})\|-1}$ pairs of plaintexts (P, P') satisfying $P \oplus P' \in \delta(\overline{\mathbb{A}})$. Filtering the pairs by the condition that the differences of ciphertexts pairs are in $\delta(\underline{\mathbb{B}})$, we can get approximately

$$\frac{2^{2\|\delta(\overline{\mathbb{A}})\|-1}}{2^{n-\|\delta(\underline{\mathbb{B}})\|}} = 2^{2\|\delta(\overline{\mathbb{A}})\|+\|\delta(\underline{\mathbb{B}})\|-n-1} \tag{2}$$

plaintext pairs (P, P') such that

$$\begin{aligned} P \oplus P' &\in \delta\left(\overline{\mathbb{A}}\right), \\ E(P) \oplus E\left(P'\right) &\in \delta\left(\underline{\mathbb{B}}\right). \end{aligned} \tag{3}$$

Moreover, there are approximately

$$\begin{aligned} &2^{2\|\delta(\overline{\mathbb{A}})\|+\|\delta(\underline{\mathbb{B}})\|-n-1} \cdot \frac{2^{\|\overline{\mathbb{A}}\|} \cdot 2^{\|\underline{\mathbb{B}}\|}}{2^{\|\delta(\overline{\mathbb{A}})\|} \cdot 2^{\|\delta(\underline{\mathbb{B}})\|}} \\ &= 2^{\|\delta(\overline{\mathbb{A}})\|+\|\overline{\mathbb{A}}\|+\|\underline{\mathbb{B}}\|-n-1} \end{aligned} \tag{4}$$

pairs satisfying $P \oplus P' \in \overline{\mathbb{A}}$ and $E(P) \oplus E(P') \in \underline{\mathbb{B}}$.

Definition 3. A pair of plaintexts (P, P') is $(\mathbb{A}, \mathbb{B})$-effective if and only if $P \oplus P' \in \overline{\mathbb{A}}$ and $E(P) \oplus E(P') \in \underline{\mathbb{B}}$.

According to the definitions of $\overline{\mathbb{A}}$ and $\underline{\mathbb{B}}$, only $(\mathbb{A}, \mathbb{B})$-effective pairs have the potential to suggest wrong key guesses, since it is only possible for such pairs to lead to the impossible differential $\mathbb{A} \nrightarrow \mathbb{B}$ under wrong key guesses. From the above discussion, we have the following fact.

Fact 4. From one structure $\delta_x(\overline{\mathbb{A}})$, approximately $2^{\|\delta(\overline{\mathbb{A}})\|+\|\overline{\mathbb{A}}\|+\|\underline{\mathbb{B}}\|-n-1}$ $(\mathbb{A}, \mathbb{B})$-effective pairs can be generated.

For an $(\mathbb{A}, \mathbb{B})$-effective pair (P, P'), the probability that $E_1(P) \oplus E_1(P') \in \mathbb{A}$ under some random guess of the key information involved in E_1 can be estimated as $|\mathbb{A}|/|\overline{\mathbb{A}}| = 2^{\|\mathbb{A}\|-\|\overline{\mathbb{A}}\|}$. Similarly, let (C, C') be the ciphertexts of the $(\mathbb{A}, \mathbb{B})$-effective pair (P, P'). Then the probability that $E_3^{-1}(C) \oplus E_3^{-1}(C') \in \mathbb{B}$ under some random guess of the key information involved in E_3 can be estimated as $|\mathbb{B}|/|\underline{\mathbb{B}}| = 2^{\|\mathbb{B}\|-\|\underline{\mathbb{B}}\|}$.

Fact 5. The probability that an $(\mathbb{A}, \mathbb{B})$-effective pair (P, P') leads to an impossible differential $(\alpha, \beta) \in \mathsf{ID}(\mathbb{A}, \mathbb{B})$ after partial encryption/decryption with a random key guess is

$$\frac{2^{\|\mathbb{A}\|}}{2^{\|\overline{\mathbb{A}}\|}} \cdot \frac{2^{\|\mathbb{B}\|}}{2^{\|\underline{\mathbb{B}}\|}} \cdot \frac{2^{\|\mathsf{ID}(\mathbb{A},\mathbb{B})\|}}{2^{\|\mathbb{A}\|+\|\mathbb{B}\|}} = 2^{\|\mathsf{ID}(\mathbb{A},\mathbb{B})\|-\|\overline{\mathbb{A}}\|-\|\underline{\mathbb{B}}\|}; \tag{5}$$

that is, there are $c_{\mathsf{ID}} = \|\overline{\mathbb{A}}\| + \|\underline{\mathbb{B}}\| - \|\mathsf{ID}(\mathbb{A}, \mathbb{B})\|$ bit-conditions that need to be verified for an $(\mathbb{A}, \mathbb{B})$-effective pair to satisfy an impossible differential in $\mathsf{ID}(\mathbb{A}, \mathbb{B})$.

Note that $c_{\mathsf{ID}} = \|\overline{\mathbb{A}}\| - \|\mathbb{A}\| + \|\underline{\mathbb{B}}\| - \|\mathbb{B}\|$ is coincidence to the notation of $c_{\text{in}} + c_{\text{out}}$ presented in [18] for any $\alpha \in \mathbb{A}$ and $\beta \in \mathbb{B}$, $\alpha \nrightarrow \beta$. Hence, the notion of $c_{\text{in}} + c_{\text{out}}$ is actually a special case of our notion c_{ID}. This is demonstrated by the following two concrete examples.

Example 6 (on the bit-conditions). Take the impossible differential attacks on SIMON [22] presented in Appendix A.3 in [18] as an example. The impossible differential used in the attack and the outer rounds are redrawn in Figure 3, from which we have $\mathbb{A} = \{0000000000000000\ 0000000000000001\}$, $\mathbb{B} = \{0000000010000000\ 0000000000000000\}$,

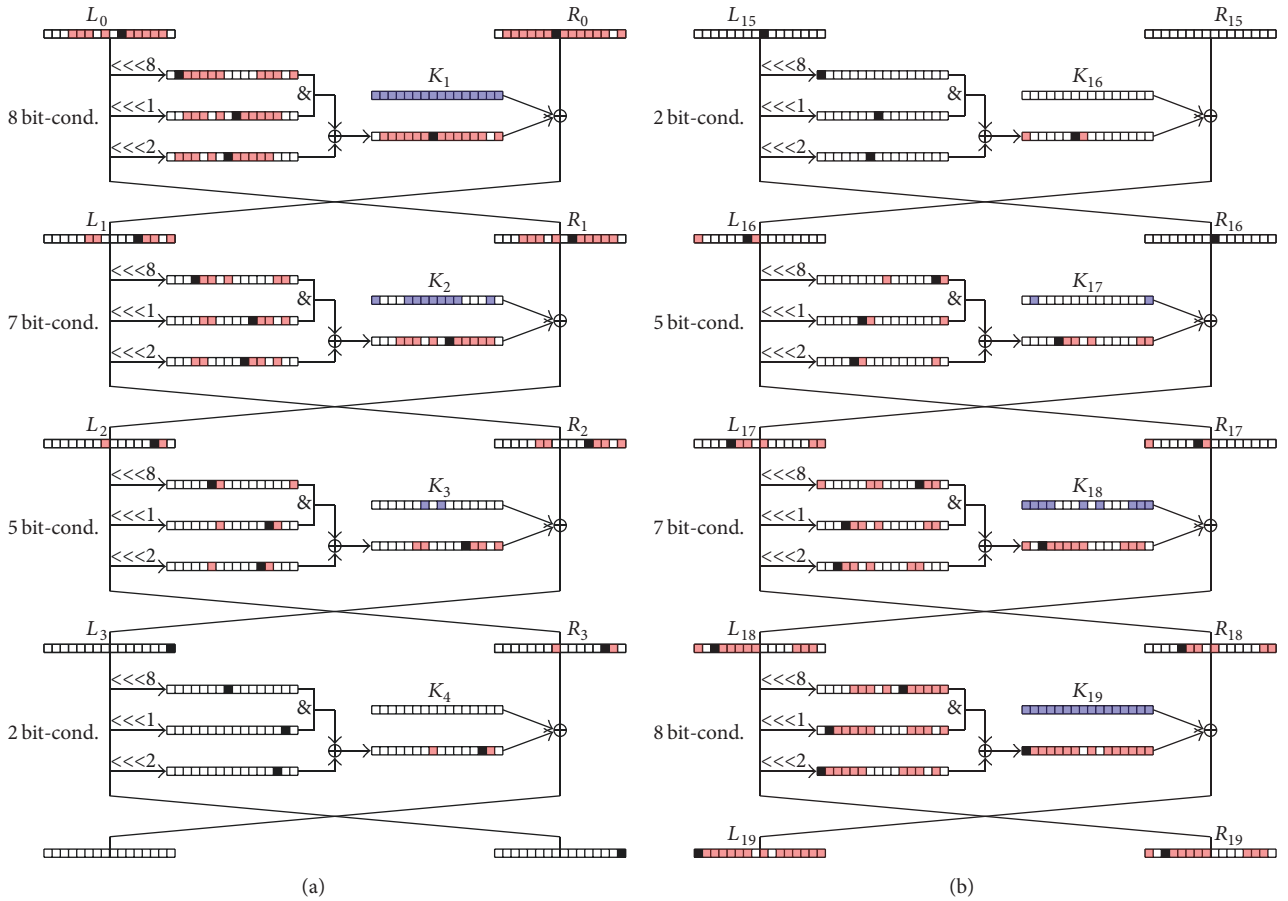

Figure 3: The initial rounds (a) and the final rounds (b) of the attack on SIMON32/64.

$$\overline{\mathbb{A}} = 000 * * * 0 * 01 * * * * * 0 \;\; 0 * * * * * * 1 * * * * * * 0 *$$
$$\underline{\mathbb{B}} = 1 * * * * * * 0 * 0 * * * * * * \;\; * 01 * * * * * 0000 * * * 0 \tag{6}$$

Therefore, $c_{\mathrm{ID}} = \|\overline{\mathbb{A}}\| - \|\mathbb{A}\| + \|\underline{\mathbb{B}}\| - \|\mathbb{B}\| = 22 - 0 + 22 - 0 = 44$, which is the same as [18] where c_{ID} is calculated as $c_{\mathrm{in}} + c_{\mathrm{out}} = (8 + 7 + 5 + 2) + (2 + 5 + 7 + 8) = 44$. As can be seen in Figure 3, $c_{\mathrm{in}} + c_{\mathrm{out}} = c_0 + \cdots + c_3 + c_{15} + \cdots + c_{18}$, where c_i is the number of bit-conditions in ith round.

Example 7 (on the bit-conditions). Take the impossible differential attacks on 13-round CLEFIA-128 [23] presented in Section 3.2 of [18], for example. The impossible differentials used in the attack and the outer rounds are redrawn in Figure 4, from which we have $\mathbb{A} = 0_{96} *_8 0_{24}$, $\mathbb{B} = 0_{72} *_8 0_{48}$, $\overline{\mathbb{A}} = 0_{32} *_8 0_{24} \| M_0(*_8 0_{24}) \| *_{32}$, and $\underline{\mathbb{B}} = 0_{40} *_8 0_{16} \| M_1(0_8 *_8 0_{16}) \| *_{32}$. Therefore, $c_{\mathrm{ID}} = \|\overline{\mathbb{A}}\| - \|\mathbb{A}\| + \|\underline{\mathbb{B}}\| - \|\mathbb{B}\| = 48 - 8 + 48 - 8 = 80$, which is the same as [18], where c_{ID} is calculated as $c_{\mathrm{in}} + c_{\mathrm{out}} = 40 + 40 = 80$ which are depicted in Figure 4.

For an $(\mathbb{A}, \mathbb{B})$-effective pair (P, P'), we can guess the key bits involved in E_1 and E_3 and get $E_1(P) \oplus E_1(P')$ and $E_3^{-1}(C) \oplus E_3^{-1}(C')$. If $(E_1(P) \oplus E_1(P'), E_3^{-1}(C) \oplus E_3^{-1}(C')) \in \mathrm{ID}(\mathbb{A}, \mathbb{B})$, the key guess must be incorrect and therefore can be removed from the candidate key space safely. In this case, we say that a key guess is rejected by a set $\mathscr{P}$ of plaintext pairs if and only if the guess is rejected by at least one pair in $\mathscr{P}$. Let $k_{\mathrm{in}} \cup k_{\mathrm{out}}$ be the target key space, and let $\mathscr{P}$ be the set of $(\mathbb{A}, \mathbb{B})$-effective pairs generated from the chosen plaintexts. The goal of an impossible differential attack is to reject as many as possible keys in $k_{\mathrm{in}} \cup k_{\mathrm{out}}$ such that the target key space can be reduced significantly.

According to Fact 5, the probability that a key guess for $k_{\mathrm{in}} \cup k_{\mathrm{out}}$ is rejected by a given $(\mathbb{A}, \mathbb{B})$-effective pair $(P, P') \in \mathscr{P}$ is $2^{-c_{\mathrm{ID}}}$. Therefore, the probability that a guess is not rejected by $\mathscr{P}$ is $(1 - 2^{-c_{\mathrm{ID}}})^{|\mathscr{P}|}$.

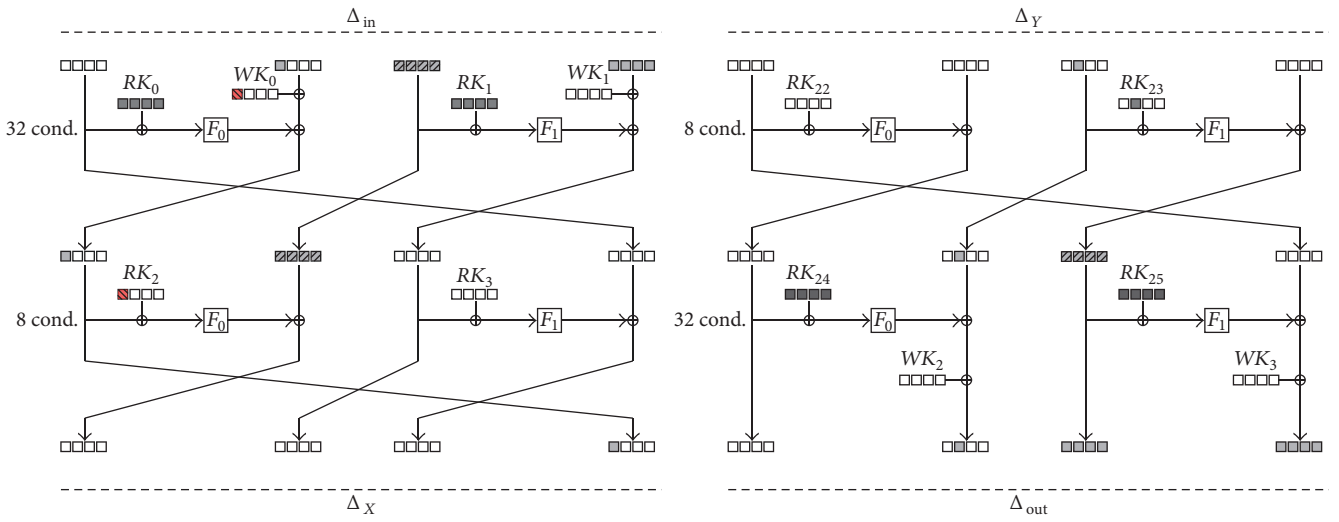

Figure 4: The attack on CLEFIA-128.

Therefore, the number of candidates keys in the target key space after performing the impossible differential analysis is $(1-2^{-c_{\mathrm{ID}}})^{|\mathcal{P}|}|k_{\mathrm{in}} \cup k_{\mathrm{out}}|$. In the literature, we typically regard $(1-2^{-c_{\mathrm{ID}}})^{2^{c_{\mathrm{ID}}}}$ approximately as e^{-1}. Consequently, we need approximately

$$\zeta_{-1} = 2^{c_{\mathrm{ID}}} = 2^{\|\overline{\mathbb{A}}\|+\|\underline{\mathbb{B}}\|-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|} \tag{7}$$

$(\mathbb{A},\mathbb{B})$-effective pairs to reduce the target key space by $\log_2 e$ bit.

Theorem 8. *With the probability $Pr = e^{-1} = 2^{-\log_2 e}$, in other words, to reduce $\log_2 e$-bit information of the space of key candidates, the data complexity is $C_{N_{\zeta_{-1}}}$, where*

$$C_{N_{\zeta_{-1}}} = \begin{cases} 2^{(n+1+\|\delta(\overline{\mathbb{A}})\|-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|)/2}, & \left\|\delta\left(\overline{\mathbb{A}}\right)\right\| \geq n+1-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|; \\ 2^{n+1-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|}, & \left\|\delta\left(\overline{\mathbb{A}}\right)\right\| \leq n+1-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|. \end{cases} \tag{8}$$

Proof. We are now ready to have a careful look at the data complexity needed to reduce at least $\log_2 e$ bit of information of the space of key candidates by considering two cases.

In the first case, 1 structure $\delta(\overline{\mathbb{A}})$ is enough to generate ζ_{-1} $(\mathbb{A},\mathbb{B})$-effective pairs. That is,

$$2^{\|\delta(\overline{\mathbb{A}})\|+\|\overline{\mathbb{A}}\|+\|\underline{\mathbb{B}}\|-n-1} \geq 2^{\|\overline{\mathbb{A}}\|+\|\underline{\mathbb{B}}\|-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|}, \tag{9}$$

namely, $\|\delta(\overline{\mathbb{A}})\| \geq n+1-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|$. Assuming that we need $N_{\zeta_{-1}}$ plaintexts from $\delta(\overline{\mathbb{A}})$, then

$$\begin{aligned} N_{\zeta_{-1}} \cdot \frac{N_{\zeta_{-1}}}{2} \cdot \frac{2^{\|\delta(\underline{\mathbb{B}})\|}}{2^n} \cdot \frac{2^{\|\overline{\mathbb{A}}\|} \cdot 2^{\|\underline{\mathbb{B}}\|}}{2^{\|\delta(\overline{\mathbb{A}})\|} \cdot 2^{\|\delta(\underline{\mathbb{B}})\|}} \\ = 2^{\|\overline{\mathbb{A}}\|+\|\underline{\mathbb{B}}\|-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|}, \end{aligned} \tag{10}$$

from which we can get $N_{\zeta_{-1}} = 2^{(n+1+\|\delta(\overline{A})\|-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|)/2}$.

In the second case, 1 structure is not enough to produce ζ_{-1} $(\mathbb{A},\mathbb{B})$-effective pairs, and we need 2^s structures. In this case, we have

$$2^s \cdot 2^{\|\delta(\overline{\mathbb{A}})\|+\|\overline{\mathbb{A}}\|+\|\underline{\mathbb{B}}\|-n-1} = \zeta_{-1} = 2^{\|\overline{\mathbb{A}}\|+\|\underline{\mathbb{B}}\|-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|}. \tag{11}$$

Therefore, we need $2^s \cdot 2^{\|\delta(\overline{\mathbb{A}})\|} = 2^{n+1-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|}$ plaintexts.

From the above two cases, we can obtain formula (8). □

Corollary 9. *With the probability $Pr = e^{-2^\alpha} = 2^{-2^\alpha \cdot \log_2 e}$, in other words, to reduce $2^\alpha \cdot \log_2 e$-bit information of the space of key candidates, the data complexity is $C_{N_{\zeta_{-\alpha}}}$, where*

$$C_{N_{\zeta_{-\alpha}}} = \begin{cases} 2^{(n+1+\|\delta(\overline{\mathbb{A}})\|-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|)/2} \cdot 2^{\alpha/2}, & \left\|\delta\left(\overline{\mathbb{A}}\right)\right\| \geq n+1-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|+\alpha; \\ 2^{n+1-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|} \cdot 2^{\alpha}, & \left\|\delta\left(\overline{\mathbb{A}}\right)\right\| \leq n+1-\|\mathrm{ID}(\mathbb{A},\mathbb{B})\|+\alpha. \end{cases} \tag{12}$$

From Theorem 8, we can get Corollary 9 easily with the same method. According to Theorem 8, while $\|\mathbb{A}\| = \|\mathbb{B}\| = 0$, namely, for one bit-level impossible differential, the minimum data complexity is 2^{n+1}. Obviously, the amount of all data is 2^n, which is less than the minimum data complexity needed for a feasible impossible differential attack.

Table 1: Impossible differential characteristics for SIMON32/64.

Number	ID
(1)	0000000000000000 0000000000000001 $\nrightarrow$ 0000000010000000 0000000000000000
(2)	0000000000000000 0000000010000000 $\nrightarrow$ 0000000010000000 0000000000000000
(3)	0000000000000000 0000000100000000 $\nrightarrow$ 0000000010000000 0000000000000000
(4)	1000000000000000 0000000000000000 $\nrightarrow$ 0000000010000000 0000000000000000
(5)	0000000000000000 0000000000000001 $\nrightarrow$ 0000001000000000 0000000000000000
(6)	0000000000000000 0000000010000000 $\nrightarrow$ 0000001000000000 0000000000000000
(7)	0000000000000000 0000000100000000 $\nrightarrow$ 0000001000000000 0000000000000000
(8)	1000000000000000 0000000000000000 $\nrightarrow$ 0000001000000000 0000000000000000

Table 2: Differential values for α_{in} and α_{out}.

0	α_{in}	α_{out}
(1)	$[0_8, 0_8, 0_8, x_8]$	$[0_8, 0_8, y_8, 0_8], [0_8, y_8, 0_8, 0_8], [y_8, 0_8, 0_8, 0_8]$
(2)	$[0_8, 0_8, x_8, 0_8]$	$[0_8, 0_8, 0_8, y_8], [0_8, y_8, 0_8, 0_8], [y_8, 0_8, 0_8, 0_8]$
(3)	$[0_8, x_8, 0_8, 0_8]$	$[0_8, 0_8, 0_8, y_8], [0_8, 0_8, y_8, 0_8], [y_8, 0_8, 0_8, 0_8]$
(4)	$[x_8, 0_8, 0_8, 0_8]$	$[0_8, 0_8, 0_8, y_8], [0_8, y_8, 0_8, 0_8], [0_8, 0_8, y_8, 0_8]$

Corollary 10. *If only using one bit-level impossible differential, which is* $\|\mathbb{A}\| = \|\mathbb{B}\| = 0$*, then there does not exist a successful impossible differential attack.*

In our formulas, the computation of the data complexity for standard impossible differential analysis and attacks based on multiple impossible differentials are unified. Moreover, our formulas reveal some interesting facts which have not been spotted previously. Taking formula (8), for example, in almost all papers [9, 20, 24–28], it is the case that

$$\left\|\delta\left(\overline{\mathbb{A}}\right)\right\| \leq n + 1 - \|\mathsf{ID}(\mathbb{A}, \mathbb{B})\|. \tag{13}$$

This is very reasonable, since the cryptanalysts cannot propagate $\mathbb{A}$ upwards too much; otherwise $\delta(\overline{\mathbb{A}})$ would contain almost all strings in $\mathbb{F}_2^n$, which is obviously an unpleasant situation. Therefore, in most cases, the data complexity can be computed from the distinguisher $(\mathbb{A}, \mathbb{B})$ directly and has nothing to do with how $\mathbb{A}/\mathbb{B}$ propagate upwards/downwards. This formula offers an extremely simple procedure for computing the data complexity of impossible differential attack. Let us show some examples.

Example 11 (multiple impossible differential attack on SIMON32/64 and SIMON96/96). In [18], Boura et al. used multiple impossible differentials to attack SIMON32/64. There are 8 independent input patterns by one original 11-round impossible differential

$$\begin{aligned} &0000000000000000\ 0000000000000001 \nrightarrow \\ &0000000010000000\ 0000000000000000; \end{aligned} \tag{14}$$

we can see the detail in Table 1. It is obvious that $\|\mathsf{ID}(\mathbb{A}, \mathbb{B})\| = \log_2(4 \times 2) = 3$. Thus the data complexity is approximately $2^{n+1-\|\mathsf{ID}(\mathbb{A},\mathbb{B})\|} \cdot 2^{\alpha} = 2^{32+1-3} \cdot 2^1 = 2^{31}$ to reduce $2 \cdot \log_2 e \approx 2.88$–*bit* information of the key candidates space from formula (12). Similarly, using 8 16-round impossible differentials, to reduce the target key space by approximately $\log_2 e$ bit, the data complexity is approximately $2^{96+1-3} = 2^{94}$. These data complexities are in accordance with the results proposed in [18].

Example 12 (multiple impossible differential attack on CLEFIA-128). In [24], Tsunoo et al. mounted an impossible differential attack on CLEFIA [23] by using multiple impossible differentials discovered in [29]. There are the following two 9-round impossible differentials in CLEFIA

$$\begin{aligned} &[0_{32}, 0_{32}, 0_{32}, \alpha_{\text{in}}] \nrightarrow [0_{32}, 0_{32}, 0_{32}, \alpha_{\text{out}}], \\ &[0_{32}, \alpha_{\text{in}}, 0_{32}, 0_{32}] \nrightarrow [0_{32}, \alpha_{\text{out}}, 0_{32}, 0_{32}]. \end{aligned} \tag{15}$$

Only considering that there is one active byte in α_{in} and α_{out} presented in Table 2, we will show how to use our formula to determine the data complexity of an impossible differential attack based on these differentials.

From Table 3, we can see that

$$\|\mathsf{ID}(\mathbb{A}, \mathbb{B})\| = \log_2\left(2^8 \times 2^8 \times 24\right) \approx 20.58. \tag{16}$$

Therefore, to reduce the target key space by approximately $\log_2 e$ bit, the minimal number of data complexity is approximately $2^{128+1-20.58} = 2^{108.42}$, which matches the results presented in [18, 24] perfectly.

5. On the Time Complexity of Impossible Differential Attack

The time complexity of the impossible differential attack is estimated by Boura et al. with the formula

$$\begin{aligned} T_{\text{comp}} = {} & C_N C_E + \left(N + 2^{\|k_{\text{in}} \cup k_{\text{out}}\|} \frac{N}{2^{c_{\text{in}} + c_{\text{out}}}}\right) C_E' C_E \\ & + 2^{\|K\|} P C_E, \end{aligned} \tag{17}$$

Table 3: Impossible differential characteristics for CLEFIA-128.

Number	ID
(1)	$[0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, 0_8, x_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, y_8, 0_8]]$
(2)	$[0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, 0_8, x_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [0_8, y_8, 0_8, 0_8]]$
(3)	$[0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, 0_8, x_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [y_8, 0_8, 0_8, 0_8]]$
(4)	$[0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, x_8, 0_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, 0_8, y_8]]$
(5)	$[0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, x_8, 0_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [0_8, y_8, 0_8, 0_8]]$
(6)	$[0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, x_8, 0_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [y_8, 0_8, 0_8, 0_8]]$
(7)	$[0_{32}, 0_{32}, 0_{32}, [0_8, x_8, 0_8, 0_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, 0_8, y_8]]$
(8)	$[0_{32}, 0_{32}, 0_{32}, [0_8, x_8, 0_8, 0_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, y_8, 0_8]]$
(9)	$[0_{32}, 0_{32}, 0_{32}, [0_8, x_8, 0_8, 0_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [y_8, 0_8, 0_8, 0_8]]$
(10)	$[0_{32}, 0_{32}, 0_{32}, [x_8, 0_8, 0_8, 0_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, 0_8, y_8]]$
(11)	$[0_{32}, 0_{32}, 0_{32}, [x_8, 0_8, 0_8, 0_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [0_8, 0_8, y_8, 0_8]]$
(12)	$[0_{32}, 0_{32}, 0_{32}, [x_8, 0_8, 0_8, 0_8]] \nrightarrow [0_{32}, 0_{32}, 0_{32}, [0_8, y_8, 0_8, 0_8]]$
(13)	$[0_{32}, [0_8, 0_8, 0_8, x_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [0_8, 0_8, y_8, 0_8], 0_{32}, 0_{32}]$
(14)	$[0_{32}, [0_8, 0_8, 0_8, x_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [0_8, y_8, 0_8, 0_8], 0_{32}, 0_{32}]$
(15)	$[0_{32}, [0_8, 0_8, 0_8, x_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [y_8, 0_8, 0_8, 0_8], 0_{32}, 0_{32}]$
(16)	$[0_{32}, [0_8, 0_8, x_8, 0_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [0_8, 0_8, 0_8, y_8], 0_{32}, 0_{32}]$
(17)	$[0_{32}, [0_8, 0_8, x_8, 0_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [0_8, y_8, 0_8, 0_8], 0_{32}, 0_{32}]$
(18)	$[0_{32}, [0_8, 0_8, x_8, 0_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [y_8, 0_8, 0_8, 0_8], 0_{32}, 0_{32}]$
(19)	$[0_{32}, [0_8, x_8, 0_8, 0_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [0_8, 0_8, 0_8, y_8], 0_{32}, 0_{32}]$
(20)	$[0_{32}, [0_8, x_8, 0_8, 0_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [0_8, 0_8, y_8, 0_8], 0_{32}, 0_{32}]$
(21)	$[0_{32}, [0_8, x_8, 0_8, 0_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [y_8, 0_8, 0_8, 0_8], 0_{32}, 0_{32}]$
(22)	$[0_{32}, [0_8, x_8, 0_8, 0_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [0_8, 0_8, 0_8, y_8], 0_{32}, 0_{32}]$
(23)	$[0_{32}, [0_8, x_8, 0_8, 0_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [0_8, 0_8, y_8, 0_8], 0_{32}, 0_{32}]$
(24)	$[0_{32}, [0_8, x_8, 0_8, 0_8], 0_{32}, 0_{32}] \nrightarrow [0_{32}, [y_8, 0_8, 0_8, 0_8], 0_{32}, 0_{32}]$

where C_N is the amount of needed data for obtaining the N pairs, $2^{\|k_{\text{in}} \cup k_{\text{out}}\|}$ is the number of candidate keys, C_E' is the ratio of the partial encryption to the full encryption, $2^{\|K\|}P$ is the key candidates needed to exhaustive search, and C_E is the full encryption. The first term is the cost of generating N $(\mathbb{A}, \mathbb{B})$-effective pairs. The second term corresponds to the cost of the key-sieving procedure. Finally, the third term is the cost of exhaustive search for the key candidates which are not removed by the key-sieving procedure. Among these three terms, the second one is the most obscure part. Next, we focus attention on the second part. So before we go further, we would like to give some comments on it. Note that the comments are never meant to be precise, but try to get some intuitive understanding.

Let $\mathbf{Q}_0, \ldots, \mathbf{Q}_{N-1}$ be N $(\mathbb{A}, \mathbb{B})$-effective plaintext pairs. We create $2^{\|k_{\text{in}} \cup k_{\text{out}}\|}N$ tuples of the form $\mathbf{W}_{i,j} = (\mathbf{Q}_i, j)$, where $0 \le i \le N-1$ and $0 \le j \le 2^{\|k_{\text{in}} \cup k_{\text{out}}\|} - 1$. We arrange these tuples into N rows as follows:

$$\mathbf{W}_{i,0}, \mathbf{W}_{i,1}, \ldots, \mathbf{W}_{i,2^{|k_{\text{in}} \cup k_{\text{out}}|}-1}. \tag{18}$$

No matter how we perform the impossible differential attack, the partial encryption and decryption of the plaintext pairs $\mathbf{Q}_i$ with guessed key $k_{\text{in}} \cup k_{\text{out}} = j$ will be performed inevitably for those (i, j) such that j is rejected by $\mathbf{Q}_i$. Let

$$\mathbf{W}^* = \left\{ \mathbf{W}_{i,j} : j \text{ is rejected by } \mathbf{Q}_i,\ 0 \le i \le N-1,\ 0 \le j \le 2^{|k_{\text{in}} \cup k_{\text{out}}|} - 1 \right\}. \tag{19}$$

Then $|\mathbf{W}^*|$ is approximately $2^{\|k_{\text{in}} \cup k_{\text{out}}\|}(N/2^{c_{\text{in}}+c_{\text{out}}})$. Therefore, the time complexity of the key-sieving process is at least $2^{\|k_{\text{in}} \cup k_{\text{out}}\|}(N/2^{c_{\text{in}}+c_{\text{out}}})C_E'C_E$, which is optimal. That is, the second term of Boura et al.'s formula is in some sense a minimum estimation of the complexity of the key-sieving process.

In [19], Derbez presented some concrete examples where there is no attack whose complexity is as low as Boura et al.'s estimation. Consequently, we want to ask the question: under which condition is Boura et al.'s estimation valid? The following shows that when the key bits are independent Boura et al.'s formula is valid and achievable. For the other case when the key bits are not independent we give a simple discussion.

5.1. When the Key Bits Are Independent

Assumption 13. In order to give a technique to achieve the optimal time complexity, there are some assumptions in the

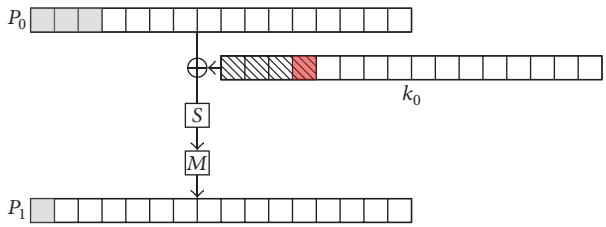

Figure 5: Example: grey color stands for nibbles with nonzero difference.

target cipher. We focus our attention on these ciphers which consist of subkey XOR, nonlinear, and linear operations. For nonlinear layer, it should be composed by S-boxes or bitwise AND. In other words, the difference values of nonlinear operation should be shown in a table with less storage and we can ignore the time complexity of creating table. Therefore, most block ciphers satisfy this assumption.

Let us assume that Δ_{i+1} is the $(i+1)$th round input set and Δ_i is the set propagated by Δ_{i+1} with probability 1. During the key filtering phase of impossible differential attack, k_i includes two parts: one involved the value of difference Δ_i and the other part involved no difference but need to get these values. Therefore, for target ciphers satisfying our assumption

$$\begin{aligned} c_i &= \|\Delta_i\| - \|\Delta_{i+1}\|, \\ \|k_i\| &= \|k_{i\Delta\neq 0}\| + \|k_{i\Delta=0}\| = \|\Delta_i\| + \|k_{i\Delta=0}\|. \end{aligned} \tag{20}$$

An example is depicted in Figure 5, where $\|k_0\| = \|k_0[0,1,2] + k_0[3]\| = \|k_{i\Delta\neq 0}\| + \|k_{i\Delta=0}\|$.

In the following, we present *the early abort technique* in which the time complexity will achieve the optimal result if the involved key bits are independent. Assuming that there are l outer rounds, let k_i denote the involved key bits and let c_i denote the number of bit-conditions. Given $N(\mathbb{A},\mathbb{B})$-effective plaintext pairs $\mathbf{Q}_0,\ldots,\mathbf{Q}_{N-1}$, for each $\mathbf{Q} \in \{\mathbf{Q}_0,\ldots,\mathbf{Q}_{N-1}\}$, completes the following steps:

(i) Step 0: derive $\mathbf{W}^{(0)} = \{(\mathbf{Q}, k'_{\sigma(i)}) : \text{the } c_{\sigma(0)} \text{ bits of conditions are verified}\}$ by table look-up. $|W^{(0)}| \approx 2^{\|k_{\sigma(0)}\| - c_{\sigma(0)}}$. In detail, at first guess the value of $\Delta_{\sigma(0)}$ and decrypt the corresponding plaintext pairs partially to calculate the output difference after nonlinear operation, then get the value of $k_{\Delta\neq 0}$ by table look-up technique and finally guess the value of $k_{i\Delta=0}$ to get $\mathbf{W}^{(0)}$.

(ii) Step 1: derive $\mathbf{W}^{(1)} = \{(\mathbf{Q}, k'_{\sigma(0)} \cup k'_{\sigma(1)}) : \text{the } c_{\sigma(1)} \text{ bits of conditions are verified}\}$ by table look-up. $|W^{(1)}| \approx 2^{\|k_{\sigma(0)} \cup k'_{\sigma(1)}\| - c_{\sigma(0)} - c_{\sigma(1)}}$.

(iii) $\cdots$

(iv) Step $l-1$: derive $\mathbf{W}^{(l-1)} = \{(\mathbf{Q}, \bigcup_{i=0}^{l-1} k'_{\sigma(i)}) : \text{the } c_{\sigma(l-1)} \text{ bits of conditions are verified}\}$ by table look-up. $|W^{(l-1)}| \approx 2^{\|\bigcup_{i=0}^{l-1} k'_{\sigma(i)}\| - \sum_{i=0}^{l-1} c_{\sigma(i)}}$.

For Step 0, the time complexity is

$$N\left(2^{\|\Delta_{i+1}\|} \times C_E^0\right) \times 2^{\|k_{\Delta=0}\|} C_E = N 2^{\|k_{\sigma(0)}\| - \|c_{\sigma(0)}\|} C_E^0 C_E. \tag{21}$$

Therefore, the complexity of the whole procedure with a given permutation σ is

$$N\left(\sum_{j=0}^{l-1} 2^{\|\bigcup_{i=0}^{j} k'_{\sigma(i)}\| - \sum_{i=0}^{j} c_{\sigma(i)}} C_E^j\right) C_E \approx N 2^{d_\sigma} C'_E C_E, \tag{22}$$

where $d_\sigma = \max_{0\le j\le l-1}\{\|\bigcup_{i=0}^{j} k'_{\sigma(i)}\| - \sum_{i=0}^{j} c_{\sigma(i)}\}$ and $C'_E = \sum_{j=0}^{l-1} C_E^j$. Obviously, C'_E is the ratio of the cost of partial encryption to the full encryption.

Combining (20) with *the early abort technique*, $\forall i$, $\|k_{\sigma(i)}\| - c_{\sigma(i)} \ge 0$. Hence $d_\sigma = \max_{0\le j\le l-1}\{\|\bigcup_{i=0}^{j} k'_{\sigma(i)}\| - \sum_{i=0}^{j} c_{\sigma(i)}\} = \sum_{i=0}^{l-1}(\|k_{\sigma(i)}\| - c_{\sigma(i)}) = \sum_{i=0}^{l-1}(\|k_i\| - c_i) = \|k_{\text{in}} \cup k_{\text{out}}\| - c_{\text{in}} - c_{\text{out}}$.

Fact 14. If the involved key bits are independent, then $d_\sigma = \|k_{\text{in}} \cup k_{\text{out}}\| - c_{\text{in}} - c_{\text{out}}$.

From Fact 14, we know that there is a permutation σ such that the time complexity of the key-sieving process is approximately

$$2^{\|k_{\text{in}} \cup k_{\text{out}}\|} \frac{N}{2^{c_{\text{in}} + c_{\text{out}}}} C'_E C_E \tag{23}$$

which is the same as Boura's formula. Without considering the time complexity of the key schedule, if the target ciphers are under our assumption and the involved key bits are independent, we can conclude that Boura et al.'s formula is correct.

Example 15 (impossible differential attack on a toy cipher). Let us consider the toy block cipher E used by Derbez in [19] as an example which is defined as follows:

$$E = E' \circ \text{MC} \circ \text{SR} \circ \text{SB} \circ \text{AK}, \tag{24}$$

where E' is a 128-bit block cipher and where AK, SB, SR, and MC, respectively, are the AddRoundKey, SubBytes, ShriftRows, and MixColumns operations from the AES:

(i) AddRoundKey (AK): XORing the state with round key;

(ii) SubBytes (SB): nonlinearity transformation using 8-bit to 8-bit invertible S-Box;

(iii) ShiftRows (SR): permutation with cyclic shift of each row to the left;

(iv) MixColumns (MC): linearity transformation to mix all the column by 4×4 invertible matrix.

Assume that there is an impossible differential $(\mathbb{A},\mathbb{B})$ over E' where $\mathbb{A}$ has one active byte. As shown in Figure 6, appending one round on the top of the distinguisher we give an impossible differential cryptanalysis. The bit-condition c_{in} is 24 and there are 32 key bits. In the case that the key bits

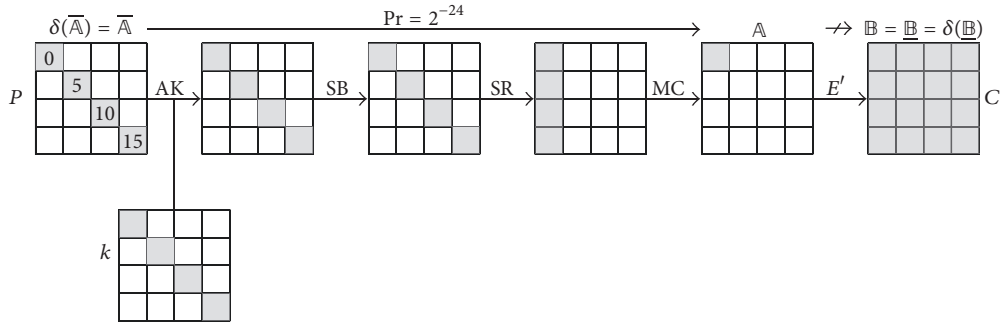

Figure 6: Impossible differential attack against the toy cipher E.

are independent, we give the time complexity of the attack as follows:

(i) Step 1: guess $\mathbb{A}$; there are 2^8 values. For each value of $\mathbb{A}$, decrypt pairs to calculate the difference value after SB operation. Thus the input difference and output difference of S-Box are both known in nibbles 0, 5, 10, and 15 for each pair.

(ii) Step 2: by table look-up four times, get the values of k_0, k_5, k_{10}, and k_{15} in turn.

Step 1 and Step 2 are the detailed explanation about *Step 0*. For $N(\mathbb{A}, \mathbb{B})$-effective pairs, the time complexity in above steps is

$$\begin{aligned} & N \times 2^8 \times (1+1+1+1) \times \frac{1}{16} \times \frac{1}{r} C_E \\ & \quad = N \times 2^8 \times C'_E C_E \end{aligned} \tag{25}$$

which is in conformity with formula (23).

5.2. When the Key Bits Are Not Independent. The previous section shows in some sense that the estimation of Boura is not only achievable but also optimal when the key bits involved are independent.

In the following, we give a formula to estimate the complexity of the key-sieving process which is always valid regardless whether the involved key bits are independent or not

$$2^{\beta} \times 2^{\|k_{\text{in}} \cup k_{\text{out}}\|} \frac{N}{2^{c_{\text{in}}+c_{\text{out}}}} C'_E C_E. \tag{26}$$

We show how to determine β by example.

Example 16 (multiple impossible differential attack on CLEFIA-128). From Figure 4 showing the attack on CLEFIA-128 by using multiple impossible differentials, there are 4 outer rounds. For k_{in} there are 32 bits of RK_1, 32 bits of RK_0, and 8 bits of $RK_2 \oplus WK_0$ to be guessed. Similarly, for k_{out} we also need to guess 8 bits of $RK_{23} \oplus WK_2$, 32 bits of RK_{24}, and 32 bits of RK_{25}. Therefore, $\|k_{\text{in}}\| = 72$ and $\|k_{\text{out}}\| = 72$. Considering the relationship between the subkeys, the subkeys RK_1 and RK_{24} share 22 bits in common. Thus the number of information key bits is $\|k_{\text{in}} \cup k_{\text{out}}\| = 72 + 72 - 22 = 122$ and for each round the bit-conditions are $c_1 = 32$, $c_2 = 8$, $c_{12} = 8$, and $c_{13} = 32$. Because the key bits are not independent, we should calculate 2^{d_σ} by steps, which could not calculate by the formula $2^{\|k_{\text{in}} \cup k_{\text{out}}\| - c_{\text{in}} - c_{\text{out}}}$.

The process to calculate 2^{d_σ} is as follows:

(i) Step 0: guess the subkeys of the first round, $\|k_{\sigma(0)}\| = \|k_1\| = 64$ and $c_{\sigma(0)} = c_1 = 32$; thus $|W^{(0)}| \approx 2^{\|k_{\sigma(0)}\| - c_{\sigma(0)}} = 2^{64-32} = 2^{32}$.

(ii) Step 1: guess the subkeys of the second round, $\|k_{\sigma(1)}\| = \|k_2\| = 8$ and $c_{\sigma(1)} = c_2 = 8$; thus $|W^{(1)}| \approx 2^{\|k_{\sigma(0)} \cup k'_{\sigma(1)}\| - c_{\sigma(0)} - c_{\sigma(1)}} = 2^{64+8-32-8} = 2^{32}$.

(iii) Step 2: guess the subkeys of the 13th round, $\|k_{\sigma(2)}\| = \|k_{13}\| = 64-22 = 42$ and $c_{\sigma(2)} = c_{13} = 32$; thus $|W^{(2)}| \approx 2^{\|\bigcup_{i=0}^{2} k'_{\sigma(i)}\| - \sum_{i=0}^{2} c_{\sigma(i)}} = 2^{64+8+42-32-8-32} = 2^{42}$.

(iv) Step 3: guess the subkeys of the 12th round, $\|k_{\sigma(3)}\| = \|k_{12}\| = 8$ and $c_{\sigma(3)} = c_{12} = 8$; thus $|W^{(3)}| \approx 2^{\|\bigcup_{i=0}^{3} k'_{\sigma(i)}\| - \sum_{i=0}^{3} c_{\sigma(i)}} = 2^{64+8+42+8-32-8-32-8} = 2^{42}$.

The above steps show $2^{d_\sigma} = \max_{0 \le j \le 3}\{|W^{(j)}|\} = 2^{42}$ which is equal to $2^{\|k_{\text{in}} \cup k_{\text{out}}\| - c_{\text{in}} - c_{\text{out}}}$; thus $2^{\beta} = 1$. The key point is that in Step 2 $\|k_{\sigma(2)}\| = \|k_{13}\| = 42 \ge c_{13} = 32$, it does not generate greater value than $2^{\|k_{\text{in}} \cup k_{\text{out}}\| - c_{\text{in}} - c_{\text{out}}}$, and the time complexity of the key-sieving process is $1 \times 2^{\|k_{\text{in}} \cup k_{\text{out}}\|}(N/2^{c_{\text{in}}+c_{\text{out}}})C'_E C_E$. To trade-off the data complexity and the time complexity, choosing $\alpha = 2.6$, the time complexity is

$$\begin{aligned} & C_N C_E + \left(N + 2^{\|k_{\text{in}} \cup k_{\text{out}}\|} \frac{N}{2^{c_{\text{in}}+c_{\text{out}}}}\right) C'_E C_E + 2^{\|K\|} P C_E \\ & \quad \approx 2^{122.07} C_E \end{aligned} \tag{27}$$

with $C_N = 2^{108.42} \times 2^{2.6} = 2^{111.06}$, $N = 2^{80} \times 2^{2.6} = 2^{82.6}$, $C'_E = 18/104$, and $P = 2^{-2^{\alpha} \log_2 e} \approx 2^{-8.75}$, which is as a result presented in [18].

6. Conclusion

Thanks to the new notations, we give a unified data complexity formula for both the ordinary impossible differential

attacks and attacks based on multiple impossible differentials. This formula not only is more convenient to use, but also reveals an interesting fact that the data complexity of an impossible differential attack can be derived by the mere knowledge of the underlying impossible differential distinguisher in most cases. Moreover, we show under which condition Boura et al.'s formula is valid and give a simple time complexity estimation for impossible differential attack which is always achievable. We believe that these results make the evaluation of the impossible differential attack more straightforward and reliable.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The work of this paper was supported by the National Natural Science Foundation of China (Grants 61732021, 61472417, 61772519, 61472415, and 61402469), the Fundamental Theory and Cutting Edge Technology Research Program of Institute of Information Engineering, CAS (Grant no. Y7Z0251103), and the State Key Laboratory of Information Security, Chinese Academy of Sciences. The work of Siwei Sun is supported by the Youth Innovation Promotion Association of Chinese Academy of Sciences and the Institute of Information Engineering (Qing-Nian-Zhi-Xing project).

References

[1] L. Knudsen, "DEAL-a 128-bit block cipher," *Complexity*, vol. 258, no. 2, 1998.

[2] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials," in *Advances in Cryptology - EUROCRYPT '99, Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*, pp. 12–23, Prague, Czech Republic, May 1999.

[3] L. Wen, M.-Q. Wang, and J.-Y. Zhao, "Related-key impossible differential attack on reduced-round LBlock," *Journal of Computer Science and Technology*, vol. 29, no. 1, pp. 165–176, 2014.

[4] J. Zhao, M. Wang, J. Chen, and Y. Zheng, "New impossible differential attack on SAFER block cipher family," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E98A, no. 3, pp. 843–852, 2015.

[5] Y. Todo, "Impossible differential attack against 14-round Piccolo-80 without relying on full code book," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E99A, no. 1, pp. 154–157, 2016.

[6] K. Kondo, Y. Sasaki, Y. Todo, and T. Iwata, "Analyzing key schedule of SIMON: Iterative key differences and application to related-key impossible differentials," in *Advances in Information and Computer Security, Proceedings of the 12th International Workshop on Security, IWSEC 2017*, pp. 141–158, Hiroshima, Japan, August 2017.

[7] B. Sun, Z. Liu, V. Rijmen et al., "Links among impossible differential, integral and zero correlation linear cryptanalysis," in *the Advances in Cryptology - CRYPTO 2015, Proceedings of 35th Annual Cryptology Conference*, pp. 95–115, Santa Barbara, CA, USA, August 2015.

[8] B. Sun, M. Liu, J. Guo, V. Rijmen, and R. Li, "Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis," in *Advances in Cryptology - EUROCRYPT 2016, Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 196–213, Springer, Vienna, Austria, May 2016.

[9] S. Bing, L. Ruilin, M. Wang, L. Ping, and L. Chao, "Impossible differential cryptanalysis of CLEFIA," *Cryptology ePrint Archive*, vol. 151, 2008.

[10] N. Mouha, Q. Wang, D. Gu, and B. Preneel, "Differential and linear cryptanalysis using mixed-integer linear programming," in *Information Security and Cryptology, Proceedings of the 7th International Conference, Inscrypt 2011*, pp. 57–76, Beijing, China, November 2011.

[11] W. Shengbao and W. Mingsheng, "Security evaluation against differential cryptanalysis for block cipher structures," *Cryptology ePrint Archive*, vol. 551, 2011.

[12] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song, "Automatic security evaluation and (related-key) differential characteristic search: Application to simon, present, lblock, DES(L) and other bit-oriented block ciphers," in *Advances in Cryptology - ASIACRYPT 2014, Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 158–178, Kaoshiung, Taiwan, December 2014.

[13] K. Fu, M. Wang, Y. Guo, S. Sun, and L. Hu, "MILP-based automatic search algorithms for differential and linear trails for speck," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 9783, pp. 268–288, 2016.

[14] J. Kim, S. Hong, J. Sung, S. Lee, J. Lim, and S. Sung, "Impossible differential cryptanalysis for block cipher structures," in *Cryptology - INDOCRYPT 2003, Proceedings of the 4th International Conference on Cryptology in India*, pp. 82–96, New Delhi, India, December 2003.

[15] Y. Luo, X. Lai, Z. Wu, and G. Gong, "A unified method for finding impossible differentials of block cipher structures," *Information Sciences*, vol. 263, pp. 211–220, 2014.

[16] Y. Sasaki and Y. Todo, "New impossible differential search tool from design and cryptanalysis aspects - revealing structural properties of several ciphers," in *Advances in Cryptology - EUROCRYPT 2017, Proceedings of the 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 185–215, Paris, France, April 2017.

[17] C. Tingting, J. Keting, F. Kai, C. Shiyao, and W. Meiqin, "New automatic search tool for impossible differentials and zero-correlation linear approximations," Tech. Rep., Cryptology ePrint Archive, 2016, http://eprint.iacr.org/2016/689.

[18] C. Boura, M. Naya-Plasencia, and V. Suder, "Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon," in *Advances in Cryptology - ASIACRYPT 2014, Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security*, Part I, pp. 179–199, Kaoshiung, Taiwan, December 2014.

[19] P. Derbez, "Note on impossible differential attacks," in *Fast Software Encryption, Proceedings of the 23rd International Conference, FSE 2016*, vol. 9783, pp. 416–427, Bochum, Germany, March 2016.

[20] J. Lu, O. Dunkelman, N. Keller, and J. Kim, "New impossible differential attacks on AES," in *Progress in Cryptology - INDOCRYPT 2008, Proceedings of the 9th International Conference on Cryptology in India*, pp. 279–293, Kharagpur, India, December 2008.

[21] J. Lu, J. Kim, N. Keller, and O. Dunkelman, "Improving the efficiency of impossible differential cryptanalysis of reduced camellia and MISTY1," in *Topics in Cryptology - CT-RSA 2008, Proceedings of The Cryptographers' Track at the RSA Conference 2008*, vol. 4964, pp. 370–386, San Francisco, CA, USA, April 2008.

[22] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers, "The SIMON and SPECK families of lightweight block ciphers," *IACR Cryptology ePrint Archive*, vol. 404, 2013.

[23] T. Shirai, A. Toru, K. Shibutani, and I. Tetsu, "The 128-bit blockcipher CLEFIA (extended abstract)," in *Fast Software Encryption, Proceedings of the 14th International Workshop, FSE 2007*, pp. 181–195, Luxembourg, 2007.

[24] Y. Tsunoo, E. Tsujihara, M. Shigeri, T. Suzaki, and T. Kawabata, "Cryptanalysis of CLEFIA using multiple impossible differentials," in *Proceedings of the 2008 International Symposium on Information Theory and its Applications, ISITA2008*, 6, 1 pages, Auckland, New Zealand, December 2008.

[25] S. Siwei and D. Gerault, "Pascal Lafourcade, Qianqian Yang, Yosuke Todo, Kexin Qiao, and Lei Hu. Analysis of aes, skinny, and others with constraint programming," *IACR Trans. Symmetric Cryptol*, vol. 2017, no. 1, pp. 281–306, 2017.

[26] Y. Liu, L. Li, D. Gu et al., "New observations on impossible differential cryptanalysis of reduced-round camellia," in *Fast Software Encryption, Proceedings of the 19th International Workshop, FSE 2012*, pp. 90–109, Washington, DC, USA, March 2012.

[27] B. Bahrak and M. R. Aref, "Impossible differential attack on seven-round AES-128," *IET Information Security*, vol. 2, no. 2, pp. 28–32, 2008.

[28] J. Chen, Y. Futa, A. Miyaji, and C. Su, "Improving impossible differential cryptanalysis with concrete investigation of key scheduling algorithm and its application to lblock," in *Proceedings of the 8th International Conference, NSS 2014*, pp. 184–197, Xi'an, China, October 2014.

[29] K. Nyberg, T. Etsuko, S. Maki, and S. Teruo, "Impossible differential cryptanalysis of CLEFIA," in *Fast Software Encryption, Proceedings of the 15th International Workshop, FSE 2008*, Lausanne, Switzerland, February 2008.