Improbable Differential from Impossible Differential: On the Validity of the Model

Céline Blondeau

Aalto University, School of Science,
Department of Information and Computer Science
celine.blondeau@aalto.fi

Abstract. Differentials with low probability are used in improbable differential cryptanalysis to distinguish a cipher from a random permutation. Due to large diffusion, finding such differentials for actual ciphers remains a challenging task. At Indocrypt 2010, Tezcan proposed a method to derive improbable differential distinguishers from impossible differential ones. In this paper, we discuss the validity of the assumptions made in the computation of the improbable differential probabilities. In particular, we show based on experiments that such improbable differential cryptanalysis can fail. The validity of the improbable differential cryptanalyses on PRESENT and CLEFIA is discussed.

Keywords:improbable differential, impossible differential, truncated differential, PRESENT, CLEFIA

1 Introduction

Since the introduction of differential cryptanalysis [2] in the beginning of the 90's, many generalizations of this attack have been proposed to cryptanalyse a large number of block ciphers. While most of them exploit differentials with high probability, in the impossible differential cryptanalysis context [1] attackers take advantage of zero-probability differentials. Recently a variation of this attack called improbable differential cryptanalysis have been introduced by Tezcan [21] at Indocrypt 2010 and by Mala, Dakhilalian and Shakiba [15]. In this context, differentials with low probabilities are used to distinguish the cipher from a random permutation.

While in theory this attack could be efficient on some ciphers, in practice, it may be hard to find differentials or truncated differentials with such small probabilities. In [15,21] a method based on the knowledge of impossible differentials is proposed. The computation of improbable differential probabilities is then obtained based on the assumption that all other differentials than the known impossible ones on the r_1 last rounds of the cipher are uniformly distributed.

In this paper, we recall and explain the assumptions made in [15,21] to derive improbable differentials from impossible ones. Based on experiments on SPN and Feistel ciphers, we show that the assumptions made in the computation of the improbable differential probabilities are not correct. In particular, the

validity of the improbable differential attack by Tezcan on 11, 12 and 13 rounds of PRESENT [22,23] and 13, 14 and 15 rounds of respectively CLEFIA-128, CLEFIA-192 and CLEFIA-256 [21] is discussed.

This paper is organized as follows. In Section 2, we recall the principle of improbable differential cryptanalysis and the method described in [21] to derive improbable differentials from impossible ones. In Section 3, based on experiments on a 24-bit block cipher, we show that the assumptions made in the computation of the improbable differential probabilities are not valid and that the corresponding key-recovery attack can fail. In Section 4, a comparison between the assumptions in truncated differential cryptanalysis and in the method proposed by Tezcan is made to support the discussion regarding the validity of the latter one. Section 5 is dedicated to the two improbable differential cryptanalyses proposed in the literature on PRESENT and CLEFIA and constructed from that model.

2 Improbable Differential Cryptanalysis

2.1 Improbable Differential Distinguisher

In this paper, iterated block ciphers E with block size n parameterized by a key K are considered. Among the different cryptanalyses on block ciphers, the statistical ones make use of a non-uniform behavior of the cipher. A key-recovery attack is often derived from a distinguisher that compares the probability of a particular characteristic, such as the probability of a differential with the uniform one. By a slight abuse of notation, as in this paper we will focus on the distinguishing part of the statistical attack (adaptation to a key-recovery attack can be done easily), we will denote by E the part of the cipher we aim at distinguishing.

While contemporary ciphers are designed to be resistant to the classical differential cryptanalysis, by improving the different existing methods, attackers are often able to show a non-random behavior of a reduced number of rounds of the cipher. Among the different generalizations of differential cryptanalysis, we focus in this paper on the truncated differential cryptanalysis [12], the impossible differential cryptanalysis [1], and the improbable differential cryptanalysis [22]. As all of these attacks rely on truncated differentials[1], we first recall the definition of a truncated differential.

Definition 1. *A* truncated differential *on E is a pair (A, C) where $A \subset (\mathbb{F}_2^n)^*$ (where $(\mathbb{F}_2^n)^* = \mathbb{F}_2^n \backslash \{0\}$) is a set of input differences and $C \subset (\mathbb{F}_2^n)^*$ a set of output differences.*

[1] Notice that in impossible differential cryptanalysis if only one output difference is taken into consideration, the complexity of the attack will be close to the full codebook, as in the case of the simple zero-correlation presented in [8].

The expected probability of the truncated differential (A, C) *on the cipher* E *is defined by*

$$p = P[A \xrightarrow{E} C] = \frac{1}{|A|} \sum_{a \in A} P_{\mathbf{X},\mathbf{K}}[E_K(X) \oplus E_K(X \oplus a) \in C]. \tag{1}$$

The probability of such truncated differential (A, C) for a random permutation is $p_U = \frac{|C|}{2^n - 1}$ and is usually called uniform probability.

Depending on the probability p different key-recovery attacks are implemented. As in the impossible differential setting $p = 0$, all the key candidates for which the truncated differential occurs are discarded. In the truncated and improbable differential key-recovery attacks a threshold T is introduced to reduce the set of potential candidates. The number S_k of occurrences of the truncated differential is then compared with the threshold T for each key candidate k. In classical truncated differential cryptanalysis, as $p > p_U$, the correct key should be among the ones such that $S_k \geq T$, whereas in improbable differential cryptanalysis, as $p < p_U$, the correct key should satisfy $S_k \leq T$. To avoid confusion, we call *"probable differential"* a truncated differential with probability $p > p_U$.

For most of the cases in the probable differential context or for the described improbable differential cryptanalyses in [21,22], the probability p of a truncated differential can be expressed relative to the uniform probability p_U. The sign of the bias $\varepsilon = p - p_U$ indicates if the truncated differential is probable or improbable.

The data complexity of such distinguishing attacks has been heavily studied. While tight estimates of their complexities can be obtained from the algorithms presented in [4] and [21], an asymptotic behavior can be derived from an expansion of the Kullback-Leibler divergence between two binomial distributions with respective probabilities p_U and $p_U \pm \varepsilon$. As presented in Table 3 of [4], the number N_S of samples[2] required to distinguish two distributions with probabilities p_U and $p = p_U \pm \varepsilon$ is proportional to $\frac{2p_U}{\epsilon^2}$.

The data complexity of an impossible differential distinguisher is inverse proportional to p_U. A discussion regarding the advantages and the disadvantages of an improbable, or almost impossible, differential in comparison with an impossible differential in key-recovery attack on the same number of rounds of a cipher is provided in [15].

2.2 Construction of Improbable Differentials: Using Impossible Differential

In practice, due to the large number of trails composing a differential, having a good estimate of its probability can be challenging. Based on assumptions, such as the *Markov assumption* [14], the probability of a differential trail is often computed by multiplying the probabilities round by round. Nevertheless, it is

[2] The ratio between the number N_S of samples and the data complexity depends of the number of input differences.

well known that this kind of assumption is not always true and in particular a key dependency can occur [11,3]. Although, finding all trails relative to a differential is impossible for almost all ciphers, underestimate of a differential probability can be obtained by summing up the probability of trails in a subset. Therefore, using standard methods, finding improbable differentials for a particular cipher can be a challenging task.

In [21,15], the authors proposed a method based on the knowledge of impossible differentials. Without loss of generality[3], we assume that an impossible distinguisher (B, C) on the r_1 last rounds of E is combined with a truncated differential (A, B) on the r_0 first rounds of E. We denote by E_0 and E_1 the corresponding partial ciphers: $E = E_1 \circ E_0$ and by q the probability of the truncated differential (A, B) on E_0: $q = P[A \overset{E_0}{\mapsto} B]$ (see Figure 1). From these two partial distinguishers, Tezcan proposed a method to compute the probability of the truncated differential (A, C) on E. While in [21], the following assumption is not explicitly written, this one seems necessary to compute the probability of the distinguisher as in Proposition 1.

Assumption 1 *For all $\bar{b} \notin B$, $\bar{b} \neq 0$, the probabilities $P[\bar{b} \overset{E_1}{\mapsto} C]$ on the r_1 rounds of E_1 are equal.*

Notice that for any permutation, for any fix input difference we have: $\sum_{c \in \mathbb{F}_2^n} P[b \to c] = 1$ and $\sum_{b \in \mathbb{F}_2^n} \sum_{c \in \mathbb{F}_2^n} P[b \to c] = 2^n$.

As depicted in Figure 1, in the improbable differential context of Tezcan the set $(\mathbb{F}_2^n)^* \backslash B$ of intermediate differences which are not in B play an important role. In the following, we denote by $\bar{B}$ this set: $\bar{B} = (\mathbb{F}_2^n)^* \backslash B$.

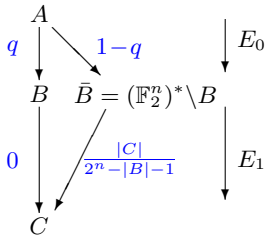


Fig. 1: Improbable differential from impossible differential

Based on the previous assumption, the probability of the improbable differential can be computed as followed:

Proposition 1. *Let $E = E_1 \circ E_0$ be a Markov cipher with probable truncated differential (A, B) on E_0 and impossible differential (B, C) on E_1 with $|B| < 2^n - |C| - 1$. Let $q = P[A \overset{E_0}{\to} B]$ be the probability of the differential (A, B).*

[3] A more general description can be found in [21].

Assuming independent rounds keys and under Assumption 1, the truncated differential (A, C) *has probability* $p = \dfrac{|C|}{2^n - |B| - 1}(1-q) \approx \dfrac{|C|}{2^n}(1-q)$ *and is improbable.*

Proof. Based on Assumption 1, as E_1 is a permutation of $\mathbb{F}_2^n$ we deduce from that for all $\bar{b} \notin B$, $\bar{b} \neq 0$, we have $P[\bar{b} \overset{E_1}{\mapsto} C] = \dfrac{|C|}{2^n - |B| - 1}$.

Then assuming that the cipher is a Markov cipher, we have

$$\begin{aligned} p &= \frac{1}{|A|} \sum_{a \in A} \sum_{c \in C} P[a \overset{E}{\mapsto} c] \\ &= \frac{1}{|A|} \sum_{a \in A} \sum_{\bar{b} \in \bar{B}} \sum_{c \in C} P[a \overset{E_0}{\mapsto} \bar{b}] P[\bar{b} \overset{E_1}{\mapsto} c] \\ &= \frac{|C|}{2^n - |B| - 1} \ \frac{1}{|A|} \sum_{a \in A} \sum_{\bar{b} \in \bar{b}} P[a \overset{E_0}{\mapsto} \bar{b}] \\ &= \frac{|C|}{2^n - |B| - 1}(1-q) \end{aligned}$$

□

In the following sections, the validity[4] of Assumption 1 is discussed using a comparison between the expected probability p of the improbable differential with the experimental one p_E for different ciphers. In particular, we show that the different cases can occur: $p_E = p$, $p_E < p$, $p_E > p$ and even $p_E > p_U$. In the last two cases, the attack can fail due to an overestimate of the data complexity or a wrong threshold selection.

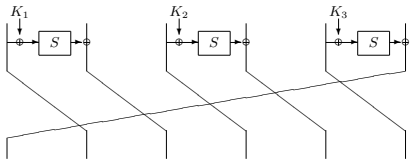
3 Experimental Improbable Distinguisher

As accurate experiments are possible on a 24-bit cipher, we design[5] a 24-bit generalized Feistel Network with 6 branches to test the validity of Assumption 1. The experiments aim at computing the probability of some 11-round improbable differential of the cipher with round function given by Figure 2. In order to limit the number of assumptions in the computation of the experimental probability, independent round keys have been selected. For the presented experimental results of this section, the 4-bit Sbox S of the cipher PRESENT [7] has been chosen[6]. Using an impossible differential on 10 rounds of this cipher, and a trun-

[4] In some cases Assumption 1 on the last rounds can be replaced by an assumption on the first rounds. The validity can nevertheless be discussed in the same way.

[5] This example is proposed in an illustrative and easy to understand purpose. For different reasons, experiments on reduced versions of existing ciphers such as CLEFIA may not reflect the behavior of the real ciphers.

[6] Experiments with different Sboxes have also been performed and the provided results are similar.



$$
\begin{array}{lcccccc}
A: & \mathrm{X} & \mathrm{Y} & 0 & 0 & 0 & 0 \\
 & & 1 \text{ round} \Downarrow & & q = 2^{-3.91} & & \\
B: & 0 & \mathrm{X} & 0 & 0 & 0 & 0 \\
 & & 10 \text{ rounds} \Downarrow & & \mathit{Impossible} & & \\
C: & 0 & 0 & 0 & \mathrm{Z} & 0 & 0
\end{array}
$$

Fig. 2: Round function of a 24-bit cipher build for experimental purpose and the 11-round improbable distinguisher where X, Y, Z are non-zero nibble values.

cated differential on the first round (see Figure 2) we conducted experiments to determine the probability p_E of the truncated differential (A, C).

The results of the experiments are shown in Table 1 for different sets of input differences. In this table we can see that the experimental probabilities are different from the theoretical ones. In particular, we always have that $p_E > p$ and $\varepsilon_E^2 > \varepsilon^2$. A theoretical estimate of the data complexity would then have been overestimated. The first attack setting presented in Table 1 illustrates a failed attack since $p_E > p_U$.

$X, Y \in \{$`0x1..0xF`$\}$ such that	q	p	p_E	$2^{-19.88}(1-q)$
All	$2^{-3.90}$	$2^{-20.10}$	$2^{-19.94}$	$2^{-19.98}$
$\delta(X, Y) \geq 2$	$2^{-2.68}$	$2^{-20.24}$	$2^{-20.14}$	$2^{-20.12}$
$\delta(X, Y) \geq 4$	2^{-2}	$2^{-20.42}$	$2^{-20.28}$	$2^{-20.29}$

Table 1: Experiments of 11 rounds of the experimental cipher for different sets of input differences defined regarding the quantity $\delta(a, b) = \#\{x \in (\mathbb{F}_2^4)^* | S(x) \oplus S(x \oplus a) = b\}$.

As Proposition 1 requires Assumption 1, these experiments show that this assumption may not be correct. More detailed experiments targeting the claim proposed in Assumption 1 confirm the non-equality of the probabilities $P[\bar{b} \xrightarrow{E_1} C]$. In particular, we observe a large deviation between expected probabilities $P[\bar{b} \xrightarrow{E_1} C]$ and the uniform probability p_U: while some are impossible, some are of order of magnitude $2^3 p_U$ or $2^{-3} p_U$.

As Assumption 1 has some similarities with the assumptions made in probable differential cryptanalysis, in the next section, we recall the assumptions made in the truncated differential cryptanalysis context and discuss the difference between the two cryptanalysis methods.

4 Validity of the Assumptions

Assumptions similar to Assumption 1 are made in probable differential cryptanalysis when computing truncated differential probabilities using a truncated differential trails. For this section, we denote by F_{K_i} $(1 \leq i \leq r)$ the round functions of the cipher E_K and by $(A_0, A_1, \cdots, A_{r-1}, A_r)$ a truncated differential trail. To compute the truncated differential probability of the differential (A_0, A_r), the following assumption is commonly made.

Assumption 2 *For all $a_i \in A_i$ and for all $a_{i+1} \in A_{i+1}$, the probabilities $P[a_i \overset{F_{K_i}}{\rightarrow} a_{i+1}]$ are equal.*

Proposition 2. *Assuming a Markov cipher for differential cryptanalysis. If the rounds keys are independent under Assumption 2 the probability of the truncated differential trail $(A_0, A_1, \cdots, A_{r-1}, A_r)$ is equal to $\prod_{i=0}^{r-1} P[A_i \overset{F_{K_i}}{\rightarrow} A_{i+1}]$.*

In many of the published truncated differential cryptanalysis (see for instance [18,17]) a comparison between the experimental probability of a truncated differential and the formula provided in Proposition 2 on a reduced number of rounds of the cipher is made to check if Assumption 2 can be bypassed. Some of them, such as [17], show that the experimental probabilities can be larger than the theoretical ones, which in the context of truncated differential cryptanalysis provides an underestimate of the attack complexity but does not challenge its validity.

By comparing Assumption 2 with Assumption 1, we observe that the latter is stronger and the probabilities $P[\bar{b} \overset{E_1}{\rightarrow} C]$ are less likely to be equal. Indeed a simple comparison between the different existing attacks show that often in truncated differential cryptanalysis, the sets A_i correspond to a small number of Sboxes while in improbable differential setting, the intermediate state is of size $2^n - |B|$ meaning that more probabilities are required to be equal. Since the diffusion grows with the number of rounds, the number r_1 of involved rounds in the improbable differential context may also influence deviations of the probabilities and contradiction with Assumption 2 may be more likely.

In the literature, there is no complete match between the truncated differentials $(A, \bar{B})$ on E_0 and $(\bar{B}, C)$ on E_1. In particular it may occur that the set D such that $P[A \overset{E_0}{\rightarrow} D] = 1$ is a small subset of $\mathbb{F}_2^n$. In that case, if we know the truncated probability $P[D \overset{E_1}{\rightarrow} C]$ (which may be different from $\frac{|C|}{2^n - |B| - 1}$) we may, based on Assumption 2, be able to compute the probability of the truncated differential (A, C).

To illustrate this behavior, we provide some explanations on the cryptanalysis presented in Section 3. In particular we show that based on Assumption 2, we are able to explain the experimental probabilities provided in Table 1. As $r_0 = 1$, it is easy to see from Figure 2 that $D = \{0XW000 \mid X, W \in \mathbb{F}_2^4,\ X \neq 0\}$. An experimental computation of the probability show that $P[D \backslash B \overset{E_1}{\rightarrow} C] =$

$2^{-19.88}$ and is far from the uniform probability $p_U = 2^{-20}$. Using Proposition 2, and the knowledge of $P[A \xrightarrow{E_0} B]$ we are able to compute the probability of the truncated differential (A, C). The results of this computation are provided in the last column of Table 1. The quasi-nonexistent deviation between these new theoretical probabilities and the experimental ones illustrates that a tight estimate of the probability $P[D \xrightarrow{E_1} C]$ is necessary to the computation, and can not be derived directly from the impossible differential (B, C).

5 Improbable Differential in the Literature

5.1 The Improbable Attack on PRESENT

PRESENT is a 64-bit lightweight block cipher designed in 2008 [7] by Bogdanov *et al.* The description of this cipher can be found in [7]. The security of a version reduced to 26 out of the 31 rounds have been threaten by a multidimensional linear cryptanalysis [10].

In [22], Tezcan presents an improbable differential cryptanalysis on this block cipher. This attack on a version reduced to 11 rounds is derived from a 9-round improbable distinguisher. In Table 2, we describe this distinguisher based on combination of a 3-round differential with the 6-round impossible differential.

A	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0001 0000 0000 0001	Differential with $q = 2^{-12}$
$X_{1,S}$	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1001 0000 0000 1001	
$X_{1,P}$	0000 0000 0000 1001 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1001	
$X_{2,S}$	0000 0000 0000 0100 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0100	
$X_{2,P}$	0000 0000 0000 0001 0000 0000 0000 0001 0000 0000 0000 0000 0000 0000 0000 0000	
$X_{3,S}$	0000 0000 0000 0011 0000 0000 0000 0011 0000 0000 0000 0000 0000 0000 0000 0000	
$X_{3,P}$	0000 0000 0000 0000 0000 0000 0000 0000 0000 1001 0000 0000 0000 1001 0000 0000	
B	0000 0000 0000 0000 0000 0000 0000 0000 0000 ???0 0000 0000 0000 ???0 0000 0000	Impossible
$X_{4,P}$	0000 0000 0?00 0000 0000 0000 0?00 0?00 0000 0000 0?00 0?00 0000 0000 0000 0000	
$X_{5,S}$	0000 0000 ???? ???? 0000 0000 ???? ???? 0000 0000 ???? ???? 0000 0000 0000 0000	
$X_{5,P}$	00?? 00?? 00?? 0000 00?? 00?? 00?? 0000 00?? 00?? 00?? 0000 00?? 00?? 00?? 0000	
$X_{6,S}$	???? ???? ???? 0000 ???? ???? ???? 0000 ???? ???? ???? 0000 ???? ???? ???? 0000	
$X_{6,P}$	???0 ???0 ???0 ???0 ???0 ???0 ???0 ???0 ???0 ???0 ???0 ???0 ???0 ???0 ???0 ???0	
$X_{6,P}$	???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???x ???x ???x ???x	
$X_{7,S}$	???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? 000x 000x 000x 000x	
$X_{7,P}$	???? ???? ???? 0000 ???? ???? ???? 0000 ???? ???? ???? 0000 ???? ???? ???? $xxxx$	
$X_{8,S}$	???? ???? ???? 0000 ???? ???? ???? 0000 ???? ???? ???? 0000 ???? ???? ???? ???1	
C	???0 ???0 ???0 ???? ???0 ???0 ???0 ???? ???0 ???0 ???0 ???? ???0 ???0 ???0 ???1	$p_U = 2^{-13}$
$X_{9,S}$	0101 0101 0101 ???? 0101 0101 0101 ???? 0101 0101 0101 ???? 0101 0101 0101 0001	$p_U = 2^{-48}$
$X_{9,P}$	000? 000? 000? 0000 111? 111? 111? 1110 000? 000? 000? 0000 111? 111? 111? 1111	

Table 2: A 3-round truncated differential combined with a 6-round impossible differential on PRESENT as in [22]. The four bits x can not be zero at the same time. $X_{i,S}$ denotes the state after the non-linear layer and $X_{i,P}$ after the permutation at round i.

As depicted in Table 2, the truncated output difference describes a set of size 2^{12}. Therefore, an experimental verification of the expected probability of this distinguisher on 9 rounds of PRESENT is out of reach since $p_U \approx 2^{-48}$.

Nevertheless, by piling-up only one round of this distinguisher, we are able to compute the probability of the 8 first rounds of the improbable distinguisher of Table 2. As depicted in Table 2, this distinguisher is derived from a 3-round differential composed with a 5-round impossible differential. As the uniform probability to obtain the truncated output differences is $p_U = 2^{-13}$, according to Proposition 1 if Assumption 1 was true, the theoretical probability of the truncated differential on the 8-round distinguisher would be smaller than p_U. Our experiments with 300 keys and 2^{32} plaintexts show that this truncated differential have a probability which vary depending of the key between $2^{-12.96}$ and $2^{-12.98}$ and is not improbable.

We thus believe that if the improbable differential distinguisher does not work on these 8 rounds, the proposed attack on 11 rounds of PRESENT derived from the 9-round distinguisher of Table 2 is not correct. From the fact that 22 rounds of PRESENT can be distinguished from a random permutation [10], we can also deduce that Assumption 1 is not true for 6 rounds.

In [23], Tezcan proposed an attack on 12 and 13 rounds of PRESENT. In this extended version of [22], Tezcan explains how to use undisturbed bits to find impossible differentials on some ciphers. Using the theory a 5-round and a 6-round impossible distinguisher on PRESENT are proposed. While the 6-round distinguisher correspond to the one of Table 2, the probability of the (5+5)-rounds distinguisher is estimated $p = 2^{-16}(1 - 2^{-17.84})$. No experiments on the full improbable distinguisher can be performed. To derive the attack on 12 and 13 rounds, the 5-round impossible distinguisher is combined with a 5-round differential. As based on the previous discussions, Assumption 1 is not valid on 5 rounds of PRESENT, the different cases presented at the end of Section 2.2 can occur.

As impossible differentials are harder to find on a large number of rounds of an SPN cipher with diffusion similar to the one of PRESENT than a linear or differential distinguisher (even using undisturbed bits as in [23]), it may be impossible to build improbable differentials using this technique for this type of cipher. Additionally due to the large diffusion, it is hard to believe that Assumption 1 can be true for SPN ciphers.

5.2 The Improbable Attack on CLEFIA

In Appendix C of [21], an experimental attack on 5 rounds of CLEFIA [19] is proposed to illustrate the theory developed in the same paper. In this section, we discuss the choices taken to run these experiments. The sets A, B, C chosen for the experimental attack in [21] are such that a truncated differential on 1 round with probability $q = \frac{10}{256}$ is combined with an impossible differential on 4 rounds. By the choice taken for the set C, the uniform probability $p_U = 1 - 2^{-32}$ is very close to 1 and is the deterministic factor which made this experimental attack succeed. Indeed under Assumption 1, the probability of the improbable differential is $p = (1 - 2^{-32})(1 - q) \approx (1 - q)$ and the conducted experiments confirm this probability. Notice that even if the probability $P[D \mapsto C]$ would be

slightly different from $(1-2^{32})$, it will only marginally influence the probability p which is close to $1-\frac{10}{256}$ and no experiment will be able to detect this deviation.

In [21], an attack on 13 rounds of CLEFIA-128 using an improbable distinguisher on 1+9 rounds is proposed. As CLEFIA is a 128-bit word oriented block cipher, it is more difficult to conduct sensible experiment on a reduced number of rounds than it is for the SPN cipher PRESENT. Nevertheless, the number of impossible differentials on 9 rounds of this cipher presented in [24] tends to induce that the probability of the truncated differential $(\bar{B}, C)$ is not close to the uniform one p_U. Based on this believe and on the discussion provided in Section 4, we want to say that the probability of the truncated differential (A, C) on 10 rounds of CLEFIA may be badly estimated. If this is the case, the whole improbable differential attack on this cipher may be wrong. Nevertheless others attacks [20,16] on 13 rounds of CLEFIA using one of the 9-round impossible differential are done by taking into consideration the key-schedule of the cipher. To our knowledge[7], in the single key model, the best known attack which were proposed at SAC 2013[6] are zero-correlation attacks on 14 rounds of CLEFIA-192 and 15 rounds of CLEFIA-256.

Similar arguments as the ones provided for CLEFIA, may hold for many generalized Feistel constructions since many impossible and multidimensional zero-correlation distinguishers[8] are often derived from the same number of rounds of the cipher and the validity of Assumption 1 can be challenged in the same way. Therefore, we claim that it may be hard to use the method proposed in [21] to derive an improbable distinguisher using impossible differentials.

6 Conclusion

In this paper, we discussed the assumptions made when deriving improbable differential distinguishers from impossible differential distinguishers. In particular we show that assuming that almost all differentials of the cipher have similar probability is a strong assumption which leads to a wrong estimate of the truncated differential probability and which can turn out to not be improbable.

Other improbable differential attacks exist in the literature [9,13]. As the computation of the truncated differential probability does not depend on the same assumption we believe that these attacks remain valid. This article provides then new insights on improbable differential cryptanalysis.

Acknowledgments. I would like to thank Kaisa Nyberg and Hadi Soleimany for the advices provided when writing this article.

[7] Notice that the recent proposed attack [25] on the full CLEFIA is not a valid one due to the involved complexities.

[8] Using the link between zero-correlation and impossible differential provided in [5] we can convert a zero-correlation distinguisher to an impossible differential one.

References

1. Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In Jacques Stern, editor, *EUROCRYPT*, volume 1592 of *LNCS*, pages 12–23. Springer, 1999.
2. Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO*, volume 537 of *LNCS*, pages 2–21. Springer, 1990.
3. Céline Blondeau and Benoît Gérard. Links Between Theoretical and Effective Differential Probabilities: Experiments on PRESENT. In *Ecrypt Workshop on Tools for Cryptanalysis*, 2010.
4. Céline Blondeau, Benoît Gérard, and Jean-Pierre Tillich. Accurate estimates of the data complexity and success probability for various cryptanalyses. *Des. Codes Cryptography*, 59(1-3):3–3 4, 2011.
5. Céline Blondeau and Kaisa Nyberg. New Links Between Differential and Linear Cryptanalysis. In Thomas Johansson and Phong Q. Nguyen, editors, *Eurocrypt 2013*, volume 7881, pages 388–404. Springer-Verlag, 2013.
6. Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen, and Baudoin Collard. Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA. In *SAC*, 2013. To appear.
7. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *CHES*, volume 4727 of *LNCS*, pages 450–466. Springer, 2007.
8. Andrey Bogdanov and Vincent Rijmen. Zero-Correlation Linear Cryptanalysis of Block Ciphers. *IACR Cryptology ePrint Archive*, 2011:123, 2011.
9. Johan Borst, Lars R. Knudsen, and Vincent Rijmen. Two Attacks on Reduced IDEA. In Walter Fumy, editor, *EUROCRYPT*, volume 1233 of *LNCS*, pages 1–13. Springer, 1997.
10. Joo Yeon Cho. Linear Cryptanalysis of Reduced-Round PRESENT. In Josef Pieprzyk, editor, *CT-RSA*, volume 5985 of *LNCS*, pages 302–317. Springer, 2010.
11. Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *J. Mathematical Cryptology*, 1(3):221–242, 2007.
12. Lars R. Knudsen. Truncated and Higher Order Differentials. In Bart Preneel, editor, *FSE*, volume 1008 of *LNCS*, pages 196–211. Springer, 1994.
13. Lars R. Knudsen and Vincent Rijmen. On the Decorrelated Fast Cipher (DFC) and Its Theory. In Lars R. Knudsen, editor, *FSE*, volume 1636 of *LNCS*, pages 81–94. Springer, 1999.
14. Xuejia Lai and Sean Murphy James L. Massey. Markov Ciphers and Differentail Cryptanalysis. In Donald W. Davies, editor, *EUROCRYPT*, volume 547 of *LNCS*, pages 17–38. Springer, 1991.
15. Hamid Mala, Mohammad Dakhilalian, and Mohsen Shakiba. Cryptanalysis of Block Ciphers Using Almost-Impossible Differentials. *IACR Cryptology ePrint Archive*, 2010:485, 2010.
16. Hamid Mala, Mohammad Dakhilalian, and Mohsen Shakiba. Impossible Differential Attacks on 13-Round CLEFIA-128. *J. Comput. Sci. Technol.*, 26(4):744–750, 2011.
17. Mitsuru Matsui and Toshio Tokita. Cryptanalysis of a Reduced Version of the Block Cipher E2, 1999.

18. Ben Reichardt and David Wagner. Markov Truncated Differential Cryptanalysis of Skipjack. In Kaisa Nyberg and Howard M. Heys, editors, *Selected Areas in Cryptography*, volume 2595 of *LNCS*, pages 110–128. Springer, 2002.
19. Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In Alex Biryukov, editor, *FSE*, volume 4593 of *LNCS*, pages 181–195. Springer, 2007.
20. Xuehai Tang, Bing Sun, Ruilin Li, and Chao Li. Impossible differential cryptanalysis of 13-round CLEFIA-128. *Journal of Systems and Software*, 84(7):1191–1196, 2011.
21. Cihangir Tezcan. The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA. In Guang Gong and Kishan Chand Gupta, editors, *INDOCRYPT*, volume 6498 of *LNCS*, pages 197–209. Springer, 2010.
22. Cihangir Tezcan. Improbable Differential Attack on PRESENT using Undisturbed Bits. In *International Conference on Applied and Computational Mathematics*, page Book of Abstracts, 2012. Ankara, TURKEY (3 October 2012) `http://cihangir.forgottenlance.com/papers/ICACM_Extended_Abstract.pdf`.
23. Cihangir Tezcan. Improbable differential attacks on PRESENT using undisturded bits. *Journal of Computational and Applied Mathematics*, 2013. In press.
24. Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Teruo Saito, Tomoyasu Suzaki, and Hiroyasu Kubo. Impossible Differential Cryptanalysis of CLEFIA. In Kaisa Nyberg, editor, *FSE*, volume 5086 of *LNCS*, pages 398–411. Springer, 2008.
25. Zheng Yuan, Xian Li, and Haixia Liu. Impossible Differential-Linear Cryptanalysis of Full-Round CLEFIA-128. *IACR Cryptology ePrint Archive*, 2013:301, 2013.