SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

January 2020, Vol. 63 112104:1–112104:11
https://doi.org/10.1007/s11432-018-9758-4

New insights on linear cryptanalysis

Zhiqiang LIU[1,2], Shuai HAN[1], Qingju WANG[1], Wei LI[3*], Ya LIU[4] & Dawu GU[1]

[1]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240*, China;*
[2]*State Key Laboratory of Cryptology, P.O. Box* 5159*, Beijing* 100878*, China;*
[3]*School of Computer Science and Technology, Donghua University, Shanghai* 201620*, China;*
[4]*Department of Computer Science and Engineering, University of Shanghai for Science and Technology, Shanghai* 200093*, China*

Received 17 September 2018/Accepted 14 January 2019/Published online 25 December 2019

Abstract Linear cryptanalysis is one of the most important cryptanalytic tools against block ciphers, thus modern block ciphers are always deliberately devised to avoid good long linear characteristics so as to resist linear cryptanalysis and its extensions. Differential-linear cryptanalysis, a powerful extension of linear cryptanalysis, has drawn much attention due to its applicability even in certain case that there is no good long linear characteristic of block ciphers. To further refine differential-linear cryptanalysis, we investigate the correlation distribution of differential-linear hull over random permutation and derive a concrete and concise correlation distribution accordingly. Theoretically, this could make differential-linear cryptanalysis more reasonable and precise. Moreover, the newly-proposed correlation distribution could lead to an interesting potential for improving the effectiveness of differential-linear cryptanalysis.

Keywords block cipher, linear cryptanalysis, differential-linear cryptanalysis, correlation distribution, key-dependent differential-linear hull

Citation Liu Z Q, Han S, Wang Q J, et al. New insights on linear cryptanalysis. Sci China Inf Sci, 2020, 63(1): 112104, https://doi.org/10.1007/s11432-018-9758-4

1 Introduction

Linear cryptanalysis [1], proposed by Matsui in 1993, is one of the most important cryptanalytic tools against block ciphers. By exploiting certain linear relation between the input and output of an n-bit block cipher, this approach can distinguish the cipher with n-bit random permutation. So far, many efforts have been made to generalize linear cryptanalysis to make it more powerful. One approach is to adopt multiple linear approximations instead of one in linear cryptanalysis [2,3]. Further, Baignères et al. [4] and Hermelin et al. [5–8] presented the idea of using multidimensional probability distributions of linear approximations, in which the "independence" constraint of multiple linear approximations in [3] can be removed, leading to more efficient cryptanalytic tools.

The second approach is to utilize non-linear approximations in linear cryptanalysis or replace the linear expressions with so-called I/O sums (For a single round of a block cipher, an I/O sum is the XOR (exclusive OR) of a balanced boolean function of the round input and a balanced boolean function of the round output). In 1995, Harpes et al. [9] used the idea of I/O sums to generalize linear cryptanalysis. In 1996, Knudsen et al. [10] proposed an efficient attack on LOKI91 by applying non-linear approximations in linear cryptanalysis. In 2004, Courtois [11] presented bi-linear cryptanalysis in which probabilistic bi-linear equations are exploited instead of linear equations.

* Corresponding author (email: liwei.cs.cn@gmail.com)

The third approach is to combine linear cryptanalysis with other powerful cryptanalytic approach elaborately. In 1994, Langford et al. [12] introduced differential-linear cryptanalysis by combining a differential characteristic with probability 1 with a linear approximation delicately. With this technique they have succeeded in analyzing 8-round DES (data encryption standard) using only 512 chosen plaintexts in a few seconds on a personal computer. In 2002, Biham et al. [13] extended differential-linear cryptanalysis by using differential characteristic with probability p ($0 < p \leqslant 1$) in building differential-linear distinguisher. Later in 2009, Liu et al. [14] further improved [13] by taking into account multiple linear approximations in differential-linear cryptanalysis. In 2012 and 2015, Lu [15, 16] presented a new methodology to deal with the intermediate layer of differential-linear approximation more generally by removing an assumption posed by Biham et al. in [13], resulting in a more reasonable interpretation of differential-linear cryptanalysis. In 2014 and 2017, Blondeau et al. [17, 18] revisited and generalized the differential-linear cryptanalysis by providing an exact expression of the bias of a differential-linear approximation as well as introducing a multidimensional model of differential-linear cryptanalysis which is defined for multiple input differences and multidimensional linear output masks. In 2016, Leurent [19] improved the complexity of differential-linear cryptanalysis for ARX (add-rotate-XOR) ciphers by refining the partitioning technique proposed by Biham and Carmeli [20].

The fourth approach is to exploit linear approximations with zero correlation instead of linear characteristics (hulls) with high correlations used in traditional linear cryptanalysis. Zero-correlation linear cryptanalysis is one of the recent cryptanalytic methods introduced by Bogdanov and Rijmen [21], and it can be considered as the projection of impossible differential cryptanalysis to linear cryptanalysis. Later in [22,23], Bogdanov et al. proposed new models that can decrease the data complexity of zero-correlation linear cryptanalysis, leading to better cryptanalytic results of block ciphers [24–27].

The fifth approach is to find and build the links between linear cryptanalysis and other cryptanalytic techniques. In 1994, Chabaud and Vaudenay [28] presented a theoretical link between differential and linear cryptanalysis. In 2011, Leander [29] showed that statistical saturation distinguishers are averagely equivalent to multidimensional linear distinguishers. Later in [22, 30–33], more practical links between integral and zero-correlation linear distinguishers, impossible differential and zero-correlation linear distinguisher, truncated differential and multidimensional linear properties were proposed, which could significantly facilitate the task of evaluating security of block ciphers against various cryptanalytic tools. Recently, efforts have been made to provide more accurate estimates of data complexity of simple, multiple, and multidimensional linear cryptanalysis [34], or to improve the accuracy of estimated success probability of linear key-recovery attacks [35].

Meanwhile, modern block ciphers are always deliberately designed to avoid good long linear characteristics so as to resist linear cryptanalysis and its extensions. In this context, how to establish linear distinguishers covering as many rounds of a block cipher as possible becomes particularly interesting. As a powerful extension of linear cryptanalysis, differential-linear cryptanalysis was proposed to meet this goal even in certain case that there is no good long linear characteristic of block ciphers. In this paper, we aim to further refine differential-linear cryptanalysis. On the one hand, inspired by the correlation distribution theory presented by Daemen and Rijmen in [36], we investigate the correlation distribution of differential-linear hull over random permutation and derive a concrete and concise correlation distribution accordingly. Theoretically, this could make differential-linear cryptanalysis more reasonable and precise (As it is always assumed that a differential-linear hull over random permutation has correlation 0, which is not actually true). On the other hand, we show that with this newly-proposed correlation distribution, it is possible to strengthen the effectiveness of differential-linear cryptanalysis by exploiting key-dependent differential-linear hull.

The remainder of this paper is organized as follows. In Section 2, we give necessary notations and a brief description of SIMON cipher. Section 3 derives the correlation distribution of differential-linear hull over random permutation. In Section 4, we show key-dependent differential-linear hull by experimentally deriving the correlation of a differential-linear hull of 23-round SIMON32/64 for different keys, and present a potential statistical model to exploit key-dependent differential-linear hull. Finally, we conclude this paper in Section 5.

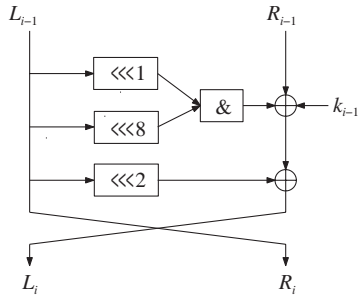

Figure 1 The round function of SIMON.

2 Preliminaries

2.1 General notations

The following notations are used throughout the paper.
– $\oplus$ denotes bitwise exclusive OR (XOR).
– 0x denotes the hexadecimal notation.
– $\|$ denotes the concatenation operation.
– $\cdot$ denotes bitwise inner product.
– $\circ$ denotes the composition operation.
– & denotes bitwise AND operation.
– $X \lll_m$ denotes left rotation of X by m bits.
– $X \ggg_m$ denotes right rotation of X by m bits.
– $\#S$ denotes the cardinality of a set S.
– $\lfloor x \rfloor$ denotes the integer such that $x - 1 < \lfloor x \rfloor \leqslant x$.

2.2 A brief description of SIMON

SIMON [37], introduced by NSA in 2013, is a family of lightweight block ciphers. It adopts balanced Feistel network with simple round function which is defined as follows:

$$L_i = (L_{i-1} \lll 1) \& (L_{i-1} \lll 8) \oplus (L_{i-1} \lll 2) \oplus R_{i-1} \oplus k_{i-1}, \quad R_i = L_{i-1},$$

where (L_{i-1}, R_{i-1}) and (L_i, R_i) represent the inputs of round $i-1$ and round i, respectively, and k_{i-1} denotes the subkey used in round $i-1$. Figure 1 shows the structure of the round function of SIMON.

SIMON supports variable block sizes and key sizes. We use SIMON2n to represent the SIMON cipher adopting n-bit words (i.e., block size is $2n$ bits), with $n \in \{16, 24, 32, 48, 64\}$, and denote SIMON2$n$ with m-word key size as SIMON2n/mn. The number of rounds of SIMON depends on block size and key size, for instance, SIMON32/64 adopts 32 rounds, SIMON48/72 adopts 36 rounds, etc. The key schedule of SIMON is shown as

$$k_{i+m} = c \oplus (z_j)_i \oplus k_i \oplus Y_m \oplus (Y_m \lll 1), \quad Y_m = \begin{cases} k_{i+1} \lll 3, & \text{if } m = 2, \\ k_{i+2} \lll 3, & \text{if } m = 3, \\ k_{i+3} \lll 3 \oplus k_{i+1}, & \text{if } m = 4, \end{cases}$$

where k_i denotes the subkey used in round i, the first m subkeys are directly derived from the secret key, the value c is a constant `0xff...fc`, and $(z_j)_i$ represents the i-th least significant bit of the constant sequence z_j $(0 \leqslant j \leqslant 4)$.

3 Correlation distribution of differential-linear hull over random permutation

Let E be an n-bit block cipher. Let $\triangle, \Gamma_C$ be two given non-zero n-bit values. Consider a differential-linear hull (we denote it as $\triangle \to \Gamma_C$) of E which is expressed as follows:

$$\Gamma_C \cdot C_1 \oplus \Gamma_C \cdot C_2 = 0, \tag{1}$$

where C_1 and C_2 are the ciphertexts of plaintexts P_1 and P_2 under E, respectively, and $P_1 \oplus P_2 = \triangle$.

Generally, differential-linear hull $\triangle \to \Gamma_C$ for E (E is divided into two parts E_{r_1} and E_{r_2}) is built by concatenating differentials with input difference being $\triangle$ for E_{r_1} and linear hulls with output mask being Γ_C for E_{r_2} (taking into account all the possibilities of intermediate layer, i.e., all possible output differences for E_{r_1} with input difference being $\triangle$, and all possible input masks for E_{r_2} with output mask being Γ_C), where E_{r_1} represents the first r_1 rounds of E, and E_{r_2} represents the last r_2 rounds of E succeeding E_{r_1}. We can see that a differential-linear hull is only determined by three parameters, i.e., input difference, output mask, and the number of rounds it covers.

If the differential-linear hull given in (1) can be used to distinguish E from an n-bit random permutation efficiently (say, better than exhaustive attack), we call it an effective linear property. Note that in the traditional differential-linear cryptanalysis, it is always assumed that a differential-linear hull $\triangle \to \Gamma_C$ over an n-bit random permutation has correlation 0, which is not actually true. To make differential-linear cryptanalysis more reasonable and precise, we need to derive the correlation distribution of differential-linear hull for an n-bit random permutation. Firstly, we introduce the following definitions.

Definition 1. The correlation of the differential-linear hull $\triangle \to \Gamma_C$ given in (1) is defined as follows:

$$\begin{aligned}\mathrm{Cor}_{\triangle\to\Gamma_C} &= 2 \times \mathrm{Pr}_{P\in\mathbb{F}_2^n}(\Gamma_C \cdot E(P) \oplus \Gamma_C \cdot E(P\oplus\triangle) = 0) - 1\\ &= \frac{1}{2^n}(\#\{P|\Gamma_C \cdot (E(P) \oplus E(P\oplus\triangle)) = 0,\ P \in \mathbb{F}_2^n\}\\ &\quad -\#\{P|\Gamma_C \cdot (E(P) \oplus E(P\oplus\triangle)) = 1,\ P \in \mathbb{F}_2^n\}).\end{aligned}$$

Definition 2. The imbalance of the differential-linear hull $\triangle \to \Gamma_C$ given in (1) is defined as follows:

$$\begin{aligned}\mathrm{Imb}_{\triangle\to\Gamma_C} &= \frac{1}{2}(\#\{P|\Gamma_C \cdot (E(P) \oplus E(P\oplus\triangle)) = 0,\ P \in \mathbb{F}_2^n\}\\ &\quad -\#\{P|\Gamma_C \cdot (E(P) \oplus E(P\oplus\triangle)) = 1,\ P \in \mathbb{F}_2^n\}).\end{aligned}$$

Hence for the differential-linear hull $\triangle \to \Gamma_C$, we have $\mathrm{Cor}_{\triangle\to\Gamma_C} = \mathrm{Imb}_{\triangle\to\Gamma_C} \times 2^{1-n}$.

Calculating $\mathrm{Cor}_{\triangle\to\Gamma_C}$ over random permutation. For a set S, let $U(S)$ denote the uniform distribution over S, and let $X \sim U(S)$ denote that X is distributed according to $U(S)$.

For an n-bit Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, define the sets of pre-images of 0 and 1 under f, respectively, as

$$\mathsf{Zero}_f := \{P \in \mathbb{F}_2^n \mid f(P) = 0\}, \quad \mathsf{One}_f := \{P \in \mathbb{F}_2^n \mid f(P) = 1\}.$$

The sets Zero_f and One_f determine the Boolean function f completely.

Let Perm_n denote the set of all n-bit permutations, and let BaBF_n denote the set of all n-bit balanced Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$. We have the following lemmas.

Lemma 1. Let $\alpha : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an n-bit permutation. Let Γ_C be a given non-zero n-bit value and $f_\alpha : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function defined as $f_\alpha(P) := \Gamma_C \cdot \alpha(P),\ P \in \mathbb{F}_2^n$. If $\alpha \sim U(\mathsf{Perm}_n)$, then $f_\alpha \sim U(\mathsf{BaBF}_n)$.

Proof. Since α is a permutation, f_α is "balanced", i.e., $\#\mathsf{Zero}_{f_\alpha} = \#\mathsf{One}_{f_\alpha} = 2^{n-1}$. Consider the map

$$\pi : \alpha \in \mathsf{Perm}_n \mapsto f_\alpha \in \mathsf{BaBF}_n,$$

which maps permutations α to balanced Boolean functions f_α. Firstly, we show that π is a "regular" map, i.e., for any $f \in \mathsf{BaBF}_n$, f has the same number of pre-images $\alpha \in \mathsf{Perm}_n$ under π, such that $f_\alpha = f$. To this end, let α be an arbitrary n-bit permutation that maps elements in Zero_f to $\mathsf{Zero}_{f_{\mathsf{id}}}$ bijectively and maps elements in One_f to $\mathsf{One}_{f_{\mathsf{id}}}$ bijectively, where $f_{\mathsf{id}} : P \mapsto \Gamma_C \cdot \mathsf{id}(P) = \Gamma_C \cdot P$.

• For such α, it holds that $f_\alpha = f$. The reason is as follows. For any $P \in \mathsf{Zero}_f$, $\alpha(P) \in \mathsf{Zero}_{f_{\mathsf{id}}}$, then $f_\alpha(P) = \Gamma_C \cdot \alpha(P) = f_{\mathsf{id}}(\alpha(P)) = 0$; for any $P \in \mathsf{One}_f$, $\alpha(P) \in \mathsf{One}_{f_{\mathsf{id}}}$, then $f_\alpha(P) = \Gamma_C \cdot \alpha(P) = f_{\mathsf{id}}(\alpha(P)) = 1$. Thus $\mathsf{Zero}_{f_\alpha} = \mathsf{Zero}_f$ and $\mathsf{One}_{f_\alpha} = \mathsf{One}_f$, which implies $f_\alpha = f$.

• There are $(2^{n-1})! \times (2^{n-1})!$ choices of such α. Because both f and f_{id} are balanced, $\#\mathsf{Zero}_f = \#\mathsf{One}_f = 2^{n-1} = \#\mathsf{Zero}_{f_{\mathsf{id}}} = \#\mathsf{One}_{f_{\mathsf{id}}}$, both the number of bijections from Zero_f to $\mathsf{Zero}_{f_{\mathsf{id}}}$ and that from One_f to $\mathsf{One}_{f_{\mathsf{id}}}$ are $(2^{n-1})!$.

Therefore, for any $f \in \mathsf{BaBF}_n$, we have already found $(2^{n-1})! \times (2^{n-1})!$ pre-images $\alpha \in \mathsf{Perm}_n$ such that $f_\alpha = f$. In addition, observe that

$$(2^{n-1})! \times (2^{n-1})! \times \#\mathsf{BaBF}_n = (2^{n-1})! \times (2^{n-1})! \times \tbinom{2^n}{2^{n-1}} = (2^n)! = \#\mathsf{Perm}_n,$$

thus f has exactly $(2^{n-1})! \times (2^{n-1})!$ pre-images $\alpha \in \mathsf{Perm}_n$. The number of pre-images is independent of the particular f, so the map π is regular.

Since $\pi : \mathsf{Perm}_n \to \mathsf{BaBF}_n$ is a regular function, as α is uniformly distributed over Perm_n, $f_\alpha = \pi(\alpha)$ is uniformly distributed over BaBF_n. This completes the proof of Lemma 1.

Lemma 2. Let $\triangle$ be a given non-zero n-bit value. For a randomly chosen balanced Boolean function $f \in \mathsf{BaBF}_n$, $n \geqslant 3$, it holds that

$$\Pr_{f \sim U(\mathsf{BaBF}_n)}\left[\#\{P \in \mathbb{F}_2^n \mid f(P) \oplus f(P \oplus \triangle) = 0\} = 2^{n-1} + z\right] = \begin{cases} \frac{\binom{2^{n-1}}{2^{n-2}+2x} \times \binom{2^{n-2}+2x}{2^{n-3}+x} \times 2^{2^{n-2}-2x}}{\binom{2^n}{2^{n-1}}}, & \text{if } z = 4x, \\ 0, & \text{otherwise,} \end{cases}$$

where $x \in \{-2^{n-3}, \ldots, -1, 0, 1, \ldots, 2^{n-3}\}$.

Proof. Firstly, we introduce several notations.

• We call $P \in \mathbb{F}_2^n$ "ball P", and imagine the mapping $P \mapsto f(P)$ as painting the ball P "red" (in the case that $f(P) = 0$) or "blue" (in the case that $f(P) = 1$).

• For any ball P, we "group" the two balls P and $P \oplus \triangle$ together.

• Each group contains exactly two balls, since $(P \oplus \triangle) \oplus \triangle = P$.

• There are 2^{n-1} disjoint groups in total.

Denote the group containing P and $P \oplus \triangle$ by an unordered tuple $(P, P \oplus \triangle)$. Note that the way how the balls are grouped is totally determined by the given value $\triangle$, and is independent of f.

• We call $f(P) \oplus f(P \oplus \triangle)$ "the value of group $(P, P \oplus \triangle)$".

• If P and $P \oplus \triangle$ are colored the same, the group is of value 0.

• If P and $P \oplus \triangle$ are differently colored, the group is of value 1.

We want to compute the fraction of $f \in \mathsf{BaBF}_n$ such that

$$\#\{P \in \mathbb{F}_2^n \mid f(P) \oplus f(P \oplus \triangle) = 0\} = 2^{n-1} + z. \tag{2}$$

The total number of balanced Boolean functions is $\#\mathsf{BaBF}_n = \binom{2^n}{2^{n-1}}$. We now compute the number of $f \in \mathsf{BaBF}_n$ satisfying (2), i.e., the number of ways to paint the balls such that Eq. (2) holds.

• Since $f \in \mathsf{BaBF}_n$, there are exactly 2^{n-1} red balls and 2^{n-1} blue balls in total.

• Denote by g_0 the number of groups of value 0 and g_1 $(= 2^{n-1} - g_0)$ the number of groups of value 1. Then Eq. (2) is equivalent to $2g_0 = 2^{n-1} + z$, i.e., $g_0 = 2^{n-2} + z/2$ and $g_1 = 2^{n-2} - z/2$.

• For each group $(P, P \oplus \triangle)$ of value 1, P and $P \oplus \triangle$ are differently colored, i.e., one of the two balls is red and another one is blue. Thus in groups of value 1, there are exactly g_1 red balls (one red ball in each group) and g_1 blue balls (one blue ball in each group).

• Since there are 2^{n-1} red balls and 2^{n-1} blue balls in total, in groups of value 0, there are exactly $2^{n-1} - g_1$ $(= g_0)$ red balls and $2^{n-1} - g_1$ $(= g_0)$ blue balls. For each group $(P, P \oplus \triangle)$ of value 0, P and $P \oplus \triangle$ are colored the same, i.e., both of the two balls are red or blue. Thus in groups of value 0, there are exactly $g_0/2$ groups containing two red balls and $g_0/2$ groups containing two blue balls.

In summary, the process of painting the balls such that Eq. (2) holds can be decomposed into three steps.

(1) Select groups:

- Select g_0 groups taking value 0, and the remaining groups taking value 1.
- The number of possibilities in this step is $\binom{2^{n-1}}{g_0}$, where $g_0 = 2^{n-2} + z/2$ and $g_1 = 2^{n-2} - z/2$.

(2) Paint balls in groups of value 0:

- Select $g_0/2$ groups with two balls painted red, and the remaining groups with two balls painted blue.
- The number of possibilities in this step is $\binom{g_0}{g_0/2}$.

(3) Paint balls in groups of value 1:

- For each group, select one of the two balls painted red and the other one painted blue.
- The number of possibilities in this step is $\binom{2}{1}^{g_1}$.

Following the multiplication principle, the number of ways to paint the balls such that Eq. (2) holds is

$$\binom{2^{n-1}}{g_0} \times \binom{g_0}{g_0/2} \times \binom{2}{1}^{g_1} = \binom{2^{n-1}}{2^{n-2}+z/2} \times \binom{2^{n-2}+z/2}{2^{n-3}+z/4} \times 2^{2^{n-2}-z/2}.$$

This number is meaningful only when z is a multiple of 4. For $z = 4x$, $x \in \{-2^{n-3}, \ldots, -1, 0, 1, \ldots, 2^{n-3}\}$, the number is

$$\binom{2^{n-1}}{2^{n-2}+2x} \times \binom{2^{n-2}+2x}{2^{n-3}+x} \times 2^{2^{n-2}-2x},$$

and consequently, the fraction of $f \in \mathsf{BaBF}_n$ such that Eq. (2) holds is

$$\frac{\binom{2^{n-1}}{2^{n-2}+2x} \times \binom{2^{n-2}+2x}{2^{n-3}+x} \times 2^{2^{n-2}-2x}}{\binom{2^n}{2^{n-1}}}.$$

This completes the proof of Lemma 2.

With the above two lemmas, we obtain the following theorem.

Theorem 1. Let $\triangle, \Gamma_C$ be two given non-zero n-bit values. For an n-bit random permutation with $n \geqslant 3$, the imbalance $\mathrm{Imb}_{\triangle\to\Gamma_C}$ of a differential-linear hull $\triangle \to \Gamma_C$ is a stochastic variable with the following distribution:

$$\Pr\left[\mathrm{Imb}_{\triangle\to\Gamma_C} = 4x\right] = \frac{\binom{2^{n-1}}{2^{n-2}+2x} \times \binom{2^{n-2}+2x}{2^{n-3}+x} \times 2^{2^{n-2}-2x}}{\binom{2^n}{2^{n-1}}}, \tag{3}$$

where $x \in \{-2^{n-3}, \ldots, -1, 0, 1, \ldots, 2^{n-3}\}$.

Proof. Let $\alpha : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an n-bit permutation and $f_\alpha : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function defined as $f_\alpha(P) := \Gamma_C \cdot \alpha(P),\ P \in \mathbb{F}_2^n$. Thus f_α is "balanced", and $\mathrm{Imb}_{\triangle\to\Gamma_C}$ for α can be calculated as

$$\begin{aligned}\mathrm{Imb}_{\triangle\to\Gamma_C} = \frac{1}{2}\big(&\#\{P \in \mathbb{F}_2^n \mid \Gamma_C \cdot (\alpha(P) \oplus \alpha(P \oplus \triangle)) = 0\} \\ &-\#\{P \in \mathbb{F}_2^n \mid \Gamma_C \cdot (\alpha(P) \oplus \alpha(P \oplus \triangle)) = 1\}\big).\end{aligned} \tag{4}$$

For an integer z, we want to compute the fraction of permutations α among all n-bit permutations such that $\mathrm{Imb}_{\triangle\to\Gamma_C} = z$, and it suffices to compute the fraction of permutations α such that

$$\#\{P \in \mathbb{F}_2^n \mid f_\alpha(P) \oplus f_\alpha(P \oplus \triangle) = 0\} = 2^{n-1} + z.$$

Thus we have

$$\begin{aligned}&\Pr\left[\mathrm{Imb}_{\triangle\to\Gamma_C} = z\right] \\ &= \Pr_{\alpha\sim U(\mathsf{Perm}_n)}\left[\#\{P \in \mathbb{F}_2^n \mid f_\alpha(P) \oplus f_\alpha(P \oplus \triangle) = 0\} = 2^{n-1} + z\right].\end{aligned}$$

According to Lemmas 1 and 2 we immediately get (3), which ends our proof.

In order to make the distribution given in (3) more concise and thus more applicable, we further provide two flavors of approximations for this distribution.

Corollary 1. Let $\triangle, \Gamma_C$ be two given non-zero n-bit values. For an n-bit random permutation with $n \geqslant 6$, the imbalance $\mathrm{Imb}_{\triangle\to\Gamma_C}$ of a differential-linear hull $\triangle \to \Gamma_C$ is a stochastic variable with a distribution that can be approximated as follows:

$$\Pr\left[\mathrm{Imb}_{\triangle\to\Gamma_C} = z\right] \approx 4\sqrt{\frac{2^{n-1}}{2^{n-1}+z}} \times Z\left(\frac{z}{2^{(n-1)/2}}\right), \tag{5}$$

for $z = 4x$ with $x \in \{-2^{n-3}+1, \ldots, -1, 0, 1, \ldots, 2^{n-3}\}$ and zero otherwise, where Z distribution denotes the standard normal distribution.

Proof. We start with the expression of (3). If 2^{n-1} is large and $2^{n-3}+x > 0$ (i.e., $x \neq -2^{n-3}$), we have

$$\binom{2^{n-1}}{2^{n-2}+2x} \approx 2^{2^{n-1}} \times Z\left(\frac{2x}{2^{(n-3)/2}}\right),$$

$$\binom{2^{n-2}+2x}{2^{n-3}+x} \approx 2^{2^{n-2}+2x} \times \frac{1}{\sqrt{2\pi}} \times \sqrt{\frac{4}{2^{n-2}+2x}},$$

and

$$\binom{2^n}{2^{n-1}} \approx 2^{2^n} \times \frac{2^{-(n-2)/2}}{\sqrt{2\pi}}.$$

Thus,

$$\Pr\left[\mathrm{Imb}_{\triangle\to\Gamma_C} = 4x\right] \approx 2\sqrt{\frac{2^{n-2}}{2^{n-2}+2x}} \times Z\left(\frac{2x}{2^{(n-3)/2}}\right) = 4\sqrt{\frac{2^{n-1}}{2^{n-1}+4x}} \times Z\left(\frac{4x}{2^{(n-1)/2}}\right).$$

This implies (5) when substituting $4x$ by z.

Corollary 2. Let $\triangle, \Gamma_C$ be two given non-zero n-bit values. For an n-bit random permutation with $n \geqslant 30$, the imbalance $\mathrm{Imb}_{\triangle\to\Gamma_C}$ of a differential-linear hull $\triangle \to \Gamma_C$ is a stochastic variable with a distribution that can be approximated as

$$\Pr\left[\mathrm{Imb}_{\triangle\to\Gamma_C} = z\right] \approx 4Z\left(\frac{z}{2^{(n-1)/2}}\right), \tag{6}$$

for $z = 4x$ with x being an integer and $x \in \{-2^{2n/3}, \ldots, -1, 0, 1, \ldots, 2^{2n/3}\}$, and zero otherwise.

Proof. We can further simplify the expression (5) in Corollary 1 as follows. Let $n \geqslant 30$, we have

- For $z = 4x$ with $x \in \{-2^{2n/3}, \ldots, -1, 0, 1, \ldots, 2^{2n/3}\}$, we have

$$1 \approx \sqrt{\frac{1}{1+2^{-n/3+3}}} = \sqrt{\frac{2^{n-1}}{2^{n-1}+4\times 2^{2n/3}}} \leqslant \sqrt{\frac{2^{n-1}}{2^{n-1}+z}} \leqslant \sqrt{\frac{2^{n-1}}{2^{n-1}-4\times 2^{2n/3}}} = \sqrt{\frac{1}{1-2^{-n/3+3}}} \approx 1,$$

It follows that

$$4\sqrt{\frac{2^{n-1}}{2^{n-1}+z}} \times Z\left(\frac{z}{2^{(n-1)/2}}\right) \approx 4Z\left(\frac{z}{2^{(n-1)/2}}\right). \tag{7}$$

- For $z = 4x$ with $x \notin \{-2^{2n/3}, \ldots, -1, 0, 1, \ldots, 2^{2n/3}\}$, $z^2 > 2^{4n/3+4}$, then

$$\begin{aligned} 4\sqrt{\frac{2^{n-1}}{2^{n-1}+z}} \times Z\left(\frac{z}{2^{(n-1)/2}}\right) &\leqslant 4\sqrt{2^{n-1}} \times Z\left(\frac{z}{2^{(n-1)/2}}\right) = 4\sqrt{2^{n-1}} \times \frac{1}{2^{(n-1)/2}\sqrt{2\pi}} \mathrm{e}^{-\frac{z^2}{2^n}} \\ &= \frac{4}{\sqrt{2\pi}} \mathrm{e}^{-\frac{z^2}{2^n}} < \frac{4}{\sqrt{2\pi}} \mathrm{e}^{-2^{n/3+4}} \approx 0. \end{aligned} \tag{8}$$

Combining (7) and (8), we obtain Corollary 2 immediately.

With Corollary 2 we can easily obtain the following result.

Proposition 1. Let $\triangle, \Gamma_C$ be two given non-zero n-bit values. For an n-bit random permutation with $n \geqslant 30$, the correlation $\mathrm{Cor}_{\triangle \to \Gamma_C}$ of a differential-linear hull $\triangle \to \Gamma_C$ is a stochastic variable with a distribution that can be measured as follows:

$$\Pr\left[\mathrm{Cor}_{\triangle \to \Gamma_C} = x \times 2^{3-n}\right] \approx \frac{1}{\sqrt{2\pi} 2^{\frac{n-5}{2}}} \mathrm{e}^{-\frac{x^2}{2^{n-4}}}, \tag{9}$$

for x is an integer between $-2^{2n/3}$ and $2^{2n/3}$ and zero otherwise.

4 Key-dependent differential-linear hull and its possible application

4.1 Key-dependent differential-linear hull

For the differential-linear hull $\triangle \to \Gamma_C$ (as shown in (1)) over the n-bit block cipher E, firstly we need to explore whether this linear hull is key-independent (i.e., for any secret key used in E, the absolute value of correlation of the linear hull keeps same or has a deviation much smaller than the absolute value of the correlation) or not (i.e., key-dependent).

So far there has not been any effective way to determine whether a differential-linear hull is key-independent or not. However, for block ciphers with small block size such as SIMON32/64, we can investigate correlation of linear hull experimentally (i.e., experimentally derive the correlation under each fixed key). Here we use a 13-round differential (0x0000, 0x0040) $\to$ (0x4000, 0x0000) given in [38], and a 10-round zero-correlation linear hull (0x0000, 0x0001) $\to$ (0x0000, 0x0080) given in [39], to construct a differential-linear hull of 23-round SIMON32/64 (rounds $0 \sim 22$) which is described as follows:

$$(\text{0x0000, 0x0080}) \cdot C_1 \oplus (\text{0x0000, 0x0080}) \cdot C_2 = 0, \tag{10}$$

where C_1 and C_2 are the ciphertexts of plaintexts P_1 and P_2 under 23-round SIMON32/64 encryption, respectively, and $P_1 \oplus P_2 = (\text{0x0000, 0x0040})$.

To derive the correlation of the linear hull given in (10), we implement a group of 2^{20} experiments, and the description of the group of experiments is given as follows:

- Randomly choose a secret key and for all possible pairs (P_1, P_2) satisfying $P_1 \oplus P_2 = (\text{0x0000, 0x0040})$, obtain the corresponding ciphertext pairs (C_1, C_2) under 23-round SIMON32/64. Then calculate the correlation of the linear hull given in (10).
- Repeat the above procedure 2^{20} times.

We find that among all the 2^{20} experiments, the values of $|\mathrm{Cor}|$ range from 0 to 2^{-13} and almost all of them are different from each other. Thus this linear hull is actually key-dependent. More specifically, in our experiments, a rough distribution of the correlations under 2^{20} different keys is given as follows:

- About $2^{-14.1}$ satisfies $2^{-13.5} < |\mathrm{Cor}| < 2^{-13}$;
- About $2^{-4.96}$ satisfies $2^{-14.4} < |\mathrm{Cor}| < 2^{-13}$;
- About $2^{-4.82}$ satisfies $0 < |\mathrm{Cor}| < 2^{-20}$;
- About $2^{-5.8}$ satisfies $0 < |\mathrm{Cor}| < 2^{-21}$;
- About $2^{-6.82}$ satisfies $0 < |\mathrm{Cor}| < 2^{-22}$;
- About $2^{-7.81}$ satisfies $0 < |\mathrm{Cor}| < 2^{-23}$;
- About $2^{-8.81}$ satisfies $0 < |\mathrm{Cor}| < 2^{-24}$;
- About $2^{-9.84}$ satisfies $0 < |\mathrm{Cor}| < 2^{-25}$;
- About $2^{-10.76}$ satisfies $0 < |\mathrm{Cor}| < 2^{-26}$.

4.2 Exploiting key-dependent differential-linear hull

For an n-bit block cipher, it is always intriguing to build a long differential-linear hull and then use it to distinguish the cipher (or reduced version of the cipher) from an n-bit random permutation. However, it seems that such a long differential-linear hull is much likely a kind of key-dependent linear hull, and there has not been any known means to make full use of this kind of linear hull so far. With the correlation

distribution of differential-linear hull over random permutation given in (9), we now propose a possible way to exploit key-dependent differential-linear hull.

Proposition 2. Let E be an n-bit ($n \geqslant 30$) block cipher with k-bit ($k > n$) key size. Suppose that $\triangle \to \Gamma_C$ is a key-dependent differential-linear hull of E which is expressed as

$$\Gamma_C \cdot C_1 \oplus \Gamma_C \cdot C_2 = 0,$$

where C_1 and C_2 are the ciphertexts of plaintexts P_1 and P_2 under E, respectively, and $P_1 \oplus P_2 = \triangle$. Let $\mathrm{Cor}_{\triangle\to\Gamma_C}$ denote the correlation of $\triangle \to \Gamma_C$. If there exist some values α ($0 < \alpha \leqslant 1$) and t (t is an integer, $0 \leqslant t \leqslant 2^{2n/3}$) such that

- For about $\alpha \times 2^k$ secret keys, $|\mathrm{Cor}_{\triangle\to\Gamma_C}| \geqslant t \times 2^{3-n}$,
- Let $\beta \triangleq \sum_{x=t}^{\lfloor 2^{2n/3}\rfloor} \frac{1}{\sqrt{2\pi}2^{\frac{n-5}{2}}}\mathrm{e}^{-\frac{x^2}{2^{n-4}}} + \sum_{x=-\lfloor 2^{2n/3}\rfloor}^{-t} \frac{1}{\sqrt{2\pi}2^{\frac{n-5}{2}}}\mathrm{e}^{-\frac{x^2}{2^{n-4}}}$, β is small enough satisfying $\alpha \times \beta^{-1} > 1$,

or

- For about $\alpha \times 2^k$ secret keys, $|\mathrm{Cor}_{\triangle\to\Gamma_C}| \leqslant t \times 2^{3-n}$,
- Let $\beta \triangleq \sum_{x=0}^{t} \frac{1}{\sqrt{2\pi}2^{\frac{n-5}{2}}}\mathrm{e}^{-\frac{x^2}{2^{n-4}}} + \sum_{x=-t}^{0} \frac{1}{\sqrt{2\pi}2^{\frac{n-5}{2}}}\mathrm{e}^{-\frac{x^2}{2^{n-4}}}$, β is small enough satisfying $\alpha \times \beta^{-1} > 1$,

then the linear hull $\triangle \to \Gamma_C$ can be used to distinguish E from an n-bit random permutation with an advantage of $(\log_2 \frac{\alpha}{\beta})$ bits.

Proof. For an n-bit random permutation, according to Proposition 1 in Section 3, the probability that $|\mathrm{Cor}_{\triangle\to\Gamma_C}| \geqslant t \times 2^{3-n}$ can be measured as

$$\beta = \sum_{x=t}^{\lfloor 2^{2n/3}\rfloor} \frac{1}{\sqrt{2\pi}2^{\frac{n-5}{2}}}\mathrm{e}^{-\frac{x^2}{2^{n-4}}} + \sum_{x=-\lfloor 2^{2n/3}\rfloor}^{-t} \frac{1}{\sqrt{2\pi}2^{\frac{n-5}{2}}}\mathrm{e}^{-\frac{x^2}{2^{n-4}}},$$

while for the block cipher E, there are about α fraction of all possible secret keys always satisfying $|\mathrm{Cor}_{\triangle\to\Gamma_C}| \geqslant t \times 2^{3-n}$, which comes to our result if combining with the condition that $\alpha \times \beta^{-1} > 1$.

Similarly, for the case that in Proposition 2 α is relatively small and β satisfies $\alpha^{-1} \times \beta > 1$, the linear hull $\triangle \to \Gamma_C$ can also be used to distinguish E from an n-bit random permutation.

5 Conclusion

In this paper, we studied a powerful extension of linear cryptanalysis — differential-linear cryptanalysis, and refined it by deriving a concrete and concise correlation distribution of differential-linear hull over random permutation. This could make differential-linear cryptanalysis more reasonable and precise (As it is always assumed that a differential-linear hull over random permutation has correlation 0, which is not actually true). Moreover, we demonstrated that with this newly-proposed correlation distribution, it is possible to make differential-linear cryptanalysis more applicable by exploiting key-dependent differential-linear hull.

While determining whether a differential-linear hull is key-independent or not, as well as applying key-dependent differential-linear hull to cryptanalysis of specific block ciphers, we leave them as open problems for further research on linear cryptanalysis.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61672347, 61772129, 61472250, 61402288). The authors are grateful to the reviewers for their valuable suggestions and comments.

References

1 Matsui M. Linear cryptanalysis method for DES cipher. In: Advances in Cryptology – EUROCRYPT 1993. Berlin: Springer, 1994. 386–397

2 Kaliski B S, Robshaw M J B. Linear cryptanalysis using multiple aprroximations. In: Advances in Cryptology – CRYPTO 1994. Berlin: Springer, 1994. 26–39

3 Biryukov A, de Cannière C, Quisquater M. On multiple linear approximations. In: Advances in Cryptology – CRYPTO 2004. Berlin: Springer, 2004. 1–22

4 Baignères T, Junod P, Vaudenay S. How far can we go beyond linear cryptanalysis? In: Advances in Cryptology – ASIACRYPT 2004. Berlin: Springer, 2004. 432–450

5 Hermelin M, Cho J Y, Nyberg K. Multidimensional linear cryptanalysis of reduced round Serpent. In: Proceedings of Australasian Conference on Information Security and Privacy – ACISP 2008. Berlin: Springer, 2008. 203–215

6 Hermelin M, Cho J Y, Nyberg K. Statistical tests for key recovery using multidimensional extension of Matsui's algorithm 1. In: Advances in Cryptology – EUROCRYPT 2009 – Poster Session, 2009

7 Cho J Y, Hermelin M, Nyberg K. A new technique for multidimensional linear cryptanalysis with applications on reduced round Serpent. In: Proceedings of International Conference on Information Security and Cryptology – ICISC 2008. Berlin: Springer, 2009. 383–398

8 Hermelin M, Cho J Y, Nyberg K. Multidimensional extension of Matsui's algorithm 2. In: Fast Software Encryption – FSE 2009. Berlin: Springer, 2009. 209–227

9 Harpes C, Kramer G, Massey J. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma. In: Advances in Cryptology – EUROCRYPT 1995. Berlin: Springer, 1995. 24–38

10 Knudsen L, Robshaw M. Non-linear approximations in linear cryptanalysis. In: Advances in Cryptology – EUROCRYPT 1996. Berlin: Springer, 1996. 224–236

11 Courtois N T. Feistel schemes and bi-linear cryptanalysis. In: Advances in Cryptology – CRYPTO 2004. Berlin: Springer, 2004. 23–40

12 Langford S K, Hellman M E. Differential-linear cryptanalysis. In: Advances in Cryptology – CRYPTO 1994. Berlin: Springer, 1994. 17–25

13 Biham E, Dunkelman O, Keller N. Enhancing differential-linear cryptanalysis. In: Advances in Cryptology – ASIACRYPT 2002. Berlin: Springer, 2002. 254–266

14 Liu Z Q, Gu D W, Zhang J, et al. Differential-multiple linear cryptanalysis. In: Proceedings of International Conference on Information Security and Cryptology – INSCRYPT 2009. Berlin: Springer, 2010. 35–49

15 Lu J Q. A methodology for differential-linear cryptanalysis and its applications - (extended abstract). In: Fast Software Encryption – FSE 2012. Berlin: Springer, 2012. 69–89

16 Lu J Q. A methodology for differential-linear cryptanalysis and its applications. Designs Codes Cryptogr, 2015, 77: 11–48

17 Blondeau C, Leander G, Nyberg K. Differential-linear cryptanalysis revisited. In: Fast Software Encryption – FSE 2014. Berlin: Springer, 2015. 411–430

18 Blondeau C, Leander G, Nyberg K. Differential-linear cryptanalysis revisited. J Cryptol, 2017, 30: 859–888

19 Leurent G. Improved differential-linear cryptanalysis of 7-round Chaskey with partitioning. In: Advances in Cryptology – EUROCRYPT 2016. Berlin: Springer, 2016. 344–371

20 Biham E, Carmeli Y. An improvement of linear cryptanalysis with addition operations with applications to FEAL-8X. In: Selected Areas in Cryptography – SAC 2014. Berlin: Springer, 2014. 59–76

21 Bogdanov A, Rijmen V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Des Codes Cryptogr, 2014, 70: 369–383

22 Bogdanov A, Leander G, Nyberg K, et al. Integral and multidimensional linear distinguishers with correlation zero. In: Advances in Cryptology – ASIACRYPT 2012. Berlin: Springer, 2012. 244–261

23 Bogdanov A, Wang M Q. Zero correlation linear cryptanalysis with reduced data complexity. In: Fast Software Encryption – FSE 2012. Berlin: Springer, 2012. 29–48

24 Wang Y F, Wu W L. Improved multidimensional zero-correlation linear cryptanalysis and applications to LBlock and TWINE. In: Proceedings of Australasian Conference on Information Security and Privacy – ACISP 2014. Berlin: Springer, 2014. 1–16

25 Wen L, Wang M Q, Bogdanov A, et al. Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: improved cryptanalysis of an ISO standard. Inf Process Lett, 2014, 114: 322–330

26 Yi W T, Chen S Z. Multidimensional zero-correlation linear cryptanalysis of the block cipher KASUMI. 2016, 10: 215–221

27 Tolba M, Abdelkhalek A, Youssef A M. Multidimensional zero-correlation linear cryptanalysis of reduced round SPARX-128. In: Selected Areas in Cryptography – SAC 2017. Berlin: Springer, 2017. 423–441

28 Chabaud F, Vaudenay S. Links between differential and linear cryptanalysis. In: Advances in Cryptology – EUROCRYPT 1994. Berlin: Springer, 1995. 356–365

29 Leander G. On linear hulls, statistical saturation attacks, PRESENT and a cryptanalysis of PUFFIN. In: Advances in Cryptology – EUROCRYPT 2011. Berlin: Springer, 2011. 303–322

30 Blondeau C, Nyberg K. New links between differential and linear cryptanalysis. In: Advances in Cryptology – EURO-

CRYPT 2013. Berlin: Springer, 2013. 388–404
31 Blondeau C, Bogdanov A, Wang M Q. On the (in)equivalence of impossible differential and zero-correlation distinguishers for Feistel- and Skipjack-type ciphers. In: Applied Cryptography and Network Security – ACNS 2014. Berlin: Springer, 2014. 271–288
32 Blondeau C, Nyberg K. Links between truncated differential and multidimensional linear properties of block ciphers and underlying attack complexities. In: Advances in Cryptology – EUROCRYPT 2014. Berlin: Springer, 2014. 165–182
33 Sun B, Liu Z Q, Rijmen V, et al. Links among impossible differential, integral and zero-correlation linear cryptanalysis. In: Advances in Cryptology – CRYPTO 2015. Berlin: Springer, 2015. 95–115
34 Blondeau C, Nyberg K. Joint data and key distribution of simple, multiple, and multidimensional linear cryptanalysis test statistic and its impact to data complexity. Des Codes Cryptogr, 2017, 82: 319–349
35 Blondeau C, Nyberg K. Improved parameter estimates for correlation and capacity deviates in linear cryptanalysis. IACR Trans Symmetric Cryptol, 2017, 2016: 162–191
36 Daemen J, Rijmen V. Probability distributions of correlation and differentials in block ciphers. J Math Cryptol, 2007, 1: 221–242
37 Beaulieu R, Shors D, Smith J, et al. The SIMON and SPECK families of lightweight block ciphers. IACR Cryptol ePrint Archive, 2013, 2013: 404
38 Biryukov A, Roy A, Velichkov V. Differential analysis of block ciphers SIMON and SPECK. In: Fast Software Encryption – FSE 2014. Berlin: Springer, 2015. 546–570
39 Wang Q J, Liu Z Q, Varıcı K, et al. Cryptanalysis of reduced-round SIMON32 and SIMON48. In: Progress in Cryptology – INDOCRYPT 2014. Berlin: Springer, 2014. 143–160