Improved Rectangle Attacks on SKINNY and CRAFT

Hosein Hadipour[1], Nasour Bagheri[2] and Ling Song[3]

[1] Department of Mathematics and Computer Science, University of Tehran, Tehran, Iran, hsn.hadipour@gmail.com
[2] Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran, Nabgheri@sru.ac.ir
[3] Jinan University, Guangzhou, China songling.qs@gmail.com

Abstract. The boomerang and rectangle attacks are adaptions of differential cryptanalysis in which the attacker divides a block cipher E into two sub-ciphers, i.e., $E = E_1 \circ E_0$, to construct a distinguisher for E with probability p^2q^2 by concatenating two short differential trails for E_0 and E_1 with probability p and q respectively. According to the previous research the dependency between these two differential characteristics have a great impact on the probability of boomerang and rectangle distinguishers. Dunkelman *et al.* proposed the sandwich attack to formalise such dependency that regards E as three parts, i.e., $E = \widetilde{E}_1 \circ E_m \circ \widetilde{E}_0$, where E_m contains the dependency between two differential trails, satisfying some differential propagation with probability r. Accordingly, the entire probability is p^2q^2r. Recently, Song *et al.* have proposed a general framework to identify the actual boundaries of E_m and systematically evaluate the probability of E_m with any number of rounds, and applied their method to improve the best boomerang distinguishers of SKINNY. In this paper, using a more advanced method to search for boomerang distinguishers, we show that the best previous boomerang distinguishers for SKINNY can be significantly improved. Given that SKINNY is a very important lightweight tweakable block cipher which is a basic module of many candidates of the Lightweight Cryptography (LWC) standardization project by NIST, and rectangle attack is one of the most efficient attacks on reduced-round of this cipher, using our boomerang distinguishers we improve the related tweakey rectangle attack on SKINNY to investigate the security of this cipher more accurately. CRAFT is another light weight tweakable block cipher for which we provide the security analysis against rectangle attack for the first time. Following the previous research regarding evaluation of switching in multiple rounds of boomerang distinguishers, we also introduce new tools called *Double Boomerang Connectivity Table* (DBCT), BDT* and DBT* to evaluate the boomerang switch through the multiple rounds more accurately. Using these new tools we provide theoretical proofs for our boomerang distinguishers for CRAFT and SKINNY.

Keywords: Lightweight block cipher · boomerang · rectangle · BCT · tweakable cipher · SKINNY · CRAFT

1 Introduction

The security of the Internet of Things (IoT) and other constrained environment such as RFID systems is an emerging concern which may not be possible to address using conventional solutions. To address this concern many solutions and primitives have been proposed by the designers so far. In this direction, The lightweight cryptography (LWC) competition of the National Institute of Standards and Technology (NIST) was started with the aim of standardization for such constrained environments and the first and the rounds candidates have been announced on April and September 2019, respectively. While NIST-LWC aims to standardize lightweight Authenticated Encryption with Associated Data and Hash functions, during last decade researchers have done an extensive efforts to provide a strong foundation for lightweight block ciphers and as the results dozen of elegant lightweight block ciphers has been design, to just name some, CRAFT [BLMR19], SKINNY [BJK+16a], PRESENT [BKL+07], MIBS [ISSK09], SIMON [BSS+15], SPECK [BSS+15], MIDORI [BBI+15], PRINTcipher [KLPR10], PRINCE [BCG+12] and GIFT [BPP+17].

SKINNY [BJK+16a] is a family of lightweight tweakable block ciphers using a substitution permutation network (SPN) structure. It has received a great deal of cryptanalytic attention following its elegant structure and efficiency. It also uses as the underlying block cipher of three submissions to the lightweight cryptography competition held by NIST, including SKINNY-AEAD [BJK+20], ForkAE [ALP+19], and Romulus [IKMP20]. On the other hands, many advances have been recently proposed for both distinguisher phase [BC18, CHP+18, SQH19, WP19], and key recovery phase [ZDM+20] of boomerang attack which is one of the most efficient attacks on reduced SKINNY. Therefore reevaluating the security of SKINNY against the boomerang attack is necessary. In this paper, using a better way to search for boomerang distinguishers of SKINNY in which switching, and clustering effects are considered, we improve the boomerang distinguishers of SKINNY [SQH19] under the related-tweak setting.

CRAFT is among the recent block ciphers, proposed at FSE 2019 by Beierle *et al.*. It is a tweakable lightweight block cipher (A tweakable block cipher maps a n-bit plaintext to a n-bit ciphertext using a k-bit secret key and a t-bit tweak). Besides the designers' extensive security analysis, independent researchers also analyzed the security of the cipher against various attacks. More precisely, Hadipour *et al.* ' [HSN+19] extended the designers' security analysis and provided more efficient distinguishers based on differential, zero correlation and integral based attacks. Moghaddam and Ahmadian [MA19] evaluated the security of this cipher against truncated differential cryptanalysis. Although the designers have not had any security claim against related-key attacks and even presented a full round deterministic related key distinguisher for the cipher, ElSheikh *et al.* [EY19] also presented new distinguishers for CRAFT in this mode and also extended it to full round key recovery attack. However, to the best of our knowledge, there is no publicly reported security evaluation of CRAFT against boomerang attacks. Hence, we are motivated to present the first security analysis of this cipher against the boomerang attack.

Our contribution

Applying a better strategy to search for boomerang distinguishers, we significantly improve the best published boomerang distinguishers of SKINNY-n-$2n$ and SKINNY-n-$3n$ [LGS17, SQH19] for $n \in \{64, 128\}$. For instance, while the best published boomerang distinguisher for 18 rounds of SKINNY-128-256 [LGS17, SQH19], has probability $2^{-77.83}$, we have provided a new boomerang distinguisher covering the same number of rounds of this variant of SKINNY with probability $2^{-40.77}$. Besides, our boomerang distinguishers for SKINNY-128-256 cover up to 21 rounds of this variant of SKINNY, whereas the best previous boomerang distinguisher for SKINNY-128-256 cover up to 19 rounds of this cipher [LGS17, SQH19][1]. Hence, we improve the boomerang distinguisher of SKINNY-128-256 by two rounds in this paper. As another example, while the best boomerang distinguisher for SKINNY-128-384 so far covers up to 24 rounds of this variant with probability $2^{-107.86}$ [LGS17, SQH19][2], we introduce a new boomerang dsitinguisher for the same number of rounds of SKINNY-128-384

[1] The best previous boomerang distinguisher for SKINNY-128-256, is an 18-round distinguisher proposed in [LGS17, SQH19], which can be extended up to 19 rounds with probability $2^{-97.53}$.

[2] The best previous boomerang distinguisher for SKINNY-128-384 is a 22-round distinguisher proposed in [LGS17, SQH19], which can be extended up to 24 rounds with probability $2^{-107.86}$.

with probability $2^{-87.39}$. In addition, we introduce a 25-round boomerang distinguisher for SKINNY-128-384 which improves the best previous boomerang distinguisher of this variant by one round. We also improved the boomerang distinguishers of SKINNY-64-128 and SKINNY-64-192 by one round. To the best of our knowledge, our boomerang distinguishers for SKINNY-n-$2n$ and SKINNY-n-$3n$ when $n \in \{64, 128\}$, are the best related tweakey distinguishers so far for these variants of SKINNY in terms of number of rounds. Table 6 summarizes our results for boomerang distinguishers of SKINNY.

In order to show the usefulness of our strategy to search for boomerang distinguishers, we applied our search algorithm on CRAFT and provide boomerang distinguishers for CRAFT for the first time. Interestingly, our finding shows that the boomerang attack is very promising on reduced CRAFT compared to other statistical attacks such as differential cryptanalysis, especially if we aim to provide a practical attack. For instance, while the probability of the best previously known distinguisher for 11 rounds of the cipher is $2^{-49.79}$, we present a boomerang distinguisher for the same number of rounds with the probability of $2^{-24.90}$ which is much higher and can be easily verified by an ordinary personal computer. for CRAFT It is clear that CRAFT has a strong boomerang effect in smaller number of rounds. As another example, while the best previous distinguisher for 9 rounds of the cipher in single tweak mode has the probability of $2^{-40.20}$, the boomerang distinguisher for the same number for rounds has the probability of $2^{-14.76}$.

In addition, we have introduced some new tools to formulate the dependency between upper and lower differential trails of boomerang distinguishers, including DBCT, DBT* and BDT*. Using these new tools we have provided theoretical proofs for the middle part of our distinguishers as well.

Outline.

The rest of the paper is organized as follows: in Section 2, we present the required preliminaries for boomerang and rectangle attacks. In Section 3 we discuss about our strategy to search for boomerang distinguishers. Section 4 is dedicated to a new concept for boomerang property of an S-box and we also introduce a 7-round distinguisher for CRAFT which is used in Section 5 to attacks various rounds of CRAFT. Section 5 also provides valid samples of boomerang distinguishers. In Section 6, after giving a brief description of SKINNY, we introduce new boomerang distinguisher for SKINNY-n-$2n$ and SKINNY-n-$2n$.Finally, we conclude the paper in Section 7.

2 Preliminaries

In this section we briefly review the boomerang attack.

2.1 Boomerang Attack and Sandwich Attack

The boomerang attack, proposed by David Wagner [Wag99], treats a block cipher E as the composition of two sub-ciphers E_0 and E_1, for which there exist short differentials $\Delta_1 \to \Delta_2$ and $\nabla_2 \to \nabla_3$ of probabilities p and q respectively. The two differentials are then combined in a chosen plaintext and ciphertext attack setting to construct a long boomerang distinguisher, as shown in Figure 1.

Let $E(P)$ and $E^{-1}(C)$ denote the encryption of P and the decryption of C, respectively. Then the boomerang framework works as follows.

- Repeat the following steps many times.
    1. $P_1 \leftarrow random()$ and $P_2 \leftarrow P_1 \oplus \Delta_1$.
    2. $C_1 \leftarrow E(P_1)$ and $C_2 \leftarrow E(P_2)$.

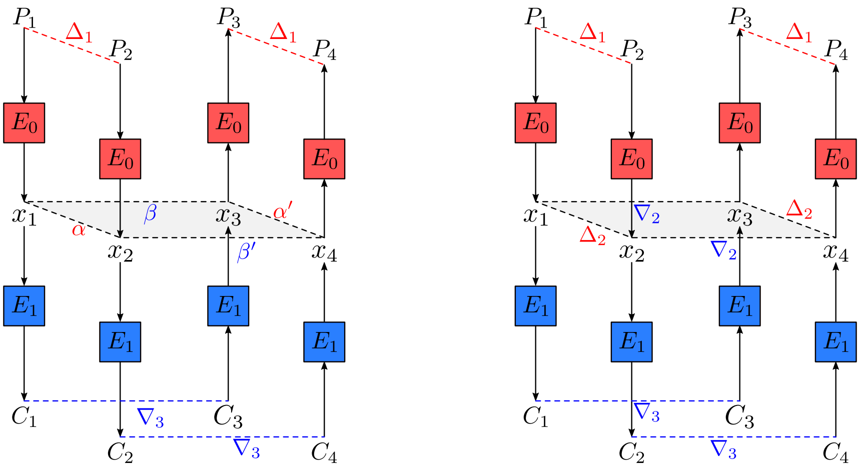

Figure 1: Basic boomerang attack

3. $C_3 \leftarrow C_1 \oplus \nabla_3$ and $C_4 \leftarrow C_2 \oplus \nabla_3$.
4. $P_3 \leftarrow E^{-1}(C_3)$ and $P_4 \leftarrow E^{-1}(C_4)$.
5. Check if $P_3 \oplus P_4 = \Delta_1$.

In the last step, if $P_3 \oplus P_4 = \Delta_1$ holds, then a *right quartet* (P_1, P_2, P_3, P_4) is found such that $P_1 \oplus P_2 = P_3 \oplus P_4 = \Delta_1$ and $C_1 \oplus C_3 = C_2 \oplus C_4 = \nabla_3$. Let's depict the following event by $e_{\alpha,\beta,\beta'}$:

$$(x_1 \oplus x_2 = \alpha) \wedge (x_1 \oplus x_3 = \beta) \wedge (x_2 \oplus x_4 = \beta'),$$

and $e_\alpha, e_\beta, e_{\beta'}$, depict the events $x_1 \oplus x_2 = \alpha, x_1 \oplus x_3 = \beta$, and $x_2 \oplus x_4 = \beta'$, respectively. The probability of $P_3 \oplus P_4 = \Delta_1$, in the above experiment, is obtained as follows:

$$\Pr(P_3 \oplus P_4 = \Delta_1) = \sum_{\alpha,\beta,\beta'} \Pr(P_3 \oplus P_4 = \Delta_1 | e_{\alpha,\beta,\beta'}). \Pr(e_{\alpha,\beta,\beta'}).$$

Note that, if the event $e_{\alpha,\beta,\beta'}$, occurs, then $\alpha' = x_3 \oplus x_4 = \alpha \oplus \beta \oplus \beta'$. If three conditions e_α, e_β, and $e_{\beta'}$, are independent, then:

$$\begin{aligned}
\Pr(P_3 \oplus P_4 = \Delta_1) &= \sum_{\alpha,\beta,\beta'} \Pr(\alpha' \xrightarrow{E_0^{-1}} \Delta_1). \Pr(\Delta_1 \xrightarrow{E_0} \alpha). \Pr(\nabla_3 \xrightarrow{E_1^{-1}} \beta). \Pr(\nabla_3 \xrightarrow{E_1^{-1}} \beta') \\
&\geq \sum_{\alpha,\beta} \Pr(\Delta_1 \xrightarrow{E_0} \alpha)^2. \Pr(\nabla_3 \xrightarrow{E_1^{-1}} \beta)^2 \\
&= \left(\sum_{\alpha} \Pr(\Delta_1 \xrightarrow{E_0} \alpha)^2 \right) . \left(\sum_{\beta} \Pr(\beta \xrightarrow{E_1} \nabla_3)^2 \right) \\
&\geq \Pr(\Delta_1 \xrightarrow{E_0} \Delta_2)^2. \Pr(\nabla_2 \xrightarrow{E_1} \nabla_3)^2 = p^2.q^2.
\end{aligned}$$

Therefore, $p^2.q^2$, is a lower bound for the probability of generating a right quartet.

In practical cases, the two differentials or differential trails of a boomerang distinguisher are not independent and the dependency between them can not be neglected as studied in [Mur11, BK09]. In order to handle the dependency, Dunkelman *et al.* proposed the *sandwich attack* [DKS10, DKS14]. As shown in Figure 2, the sandwich attack regards E as

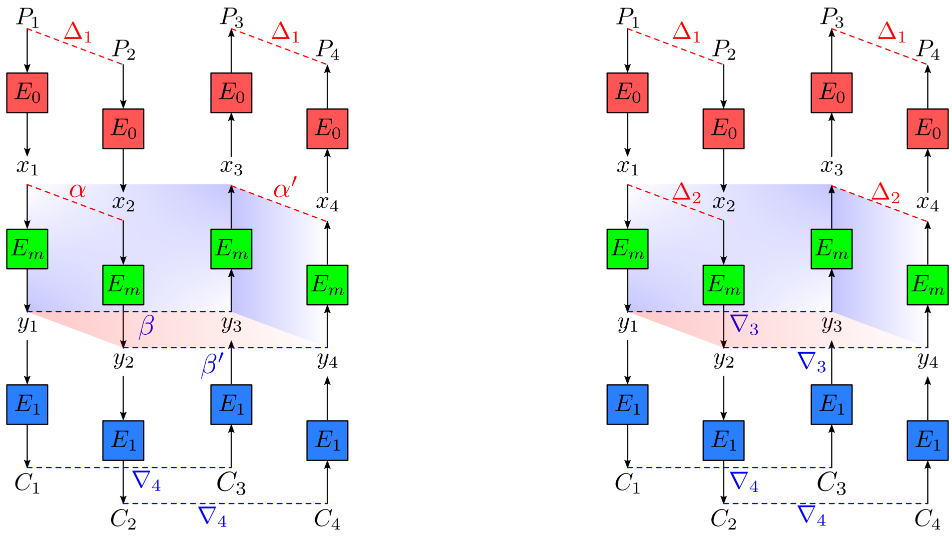

Figure 2: Sandwich attack

the composition of three sub-ciphers E_0, E_m and E_1, where the middle part E_m specifically handles the dependency and contains a relatively small number of rounds. Let r be the probability of generating a right quartet for E_m, when its input and output differences are fixed differences Δ_2, and ∇_3, respectively, i.e.:

$$r = \Pr\left(E_m^{-1}(E_m(x_1) \oplus \nabla_3) \oplus E_m^{-1}(E_m(x_2) \oplus \nabla_3) = \Delta_2 | x_1 \oplus x_2 = \Delta_2\right),$$

and the probability of the differential trail over E_0 and E_1 be p and q respectively. For the probability of the whole boomerang distinguisher we have:

$$\begin{aligned}\Pr\left(P_3 \oplus P_4 = \Delta_1\right) &= \sum_{\alpha,\alpha',\beta,\beta'} \Pr(P_3 \oplus P_4 = \Delta_1 | e_{\alpha,\alpha',\beta,\beta'}).\Pr(e_{\alpha,\alpha',\beta,\beta'})\\ &= \sum_{\alpha,\alpha',\beta,\beta'} \Pr(P_3 \oplus P_4 = \Delta_1 | e_{\alpha,\alpha',\beta,\beta'}).\Pr(e_{\alpha'}|e_\alpha, e_\beta, e_{\beta'}).\Pr(e_\alpha, e_\beta, e_{\beta'}),\end{aligned}$$

where $e_{\alpha,\alpha',\beta,\beta'}$, occurs, when the following condition is satisfied:

$$(x_1 \oplus x_2 = \alpha) \wedge (y_1 \oplus y_3 = \beta) \wedge (y_2 \oplus y_4 = \beta') \wedge (x_3 \oplus x_4 = \alpha'),$$

and events $x_1 \oplus x_2 = \alpha$, $y_1 \oplus y_3 = \beta$, $y_2 \oplus y_4 = \beta'$, and $x_3 \oplus x_4 = \alpha'$, are depicted by $e_\alpha, e_\beta, e_{\beta'}$, and $e_{\alpha'}$, respectively. It is supposed that e_α, e_β, and $e_{\beta'}$, are three independent events, and $\Pr(e_{\alpha'}|e_\alpha, e_\beta, e_{\beta'}) = r$, when $\alpha = \alpha' = \Delta_2$, and $\beta = \beta' = \nabla_3$. Therefore, the following inequalities will be hold:

$$\begin{aligned}&\sum_{\alpha,\alpha',\beta,\beta'} \Pr(\Delta_1 \xrightarrow{E_0} \alpha').\Pr(\Delta_1 \xrightarrow{E_0} \alpha).\Pr(e_{\alpha'}|e_\alpha, e_\beta, e_{\beta'}).\Pr(\nabla_4 \xrightarrow{E_1^{-1}} \beta).\Pr(\nabla_4 \xrightarrow{E_1^{-1}} \beta')\\ &\geq \sum_{\alpha,\beta} \Pr(\Delta_1 \xrightarrow{E_0} \alpha)^2.\Pr(e_{\alpha'}|e_\alpha, e_\beta, e_{\beta'}).\Pr(\beta \xrightarrow{E_1} \nabla_4)^2\\ &\geq \left(\Pr(\Delta_1 \xrightarrow{E_0} \Delta_2)\right)^2.r.\left(\Pr(\nabla_3 \xrightarrow{E_1} \nabla_4)\right)^2 = p^2.r.q^2.\end{aligned}$$

Therefore, $p^2.q^2.r$, is a lower bound for the probability of the whole boomerang distinguisher.

2.2 BCT Framework

The boomerang connectivity table (BCT) was introduced by Cid *et al.* in [CHP+18] to evaluate r theoretically when E_m is composed of a single S-box layer. Later, the BCT is extended and used to calculate r for E_m with multiple layers [SQH19, WP19]. Here, we recall some important tables of S-boxes and relevant definitions which play a core role when calculating the probability of boomerang distinguishers.

The differences of an S-box in the boomerang distinguisher are shown in Figure 3. Alternatively, we use arrows with superscripts to denote the relationship between differences. The difference distribution table (DDT) and the BCT are two basic tables of the S-box.

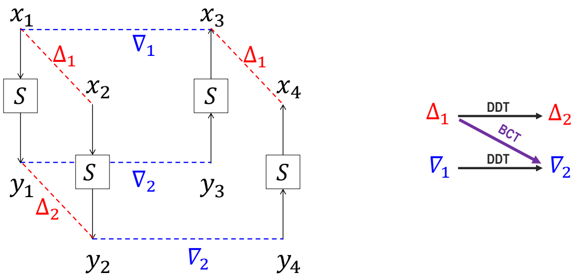

Figure 3: Differences of an S-box on four facets

Definition 1 (Difference Distribution Table)**.** Let S be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. The difference distribution table (DDT) is a two-dimensional table defined by

$$\mathtt{DDT}(\Delta_1, \Delta_2) = \#\{x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus \Delta_1) = \Delta_2\}, \text{ where } \Delta_1, \Delta_2 \in \mathbb{F}_2^n.$$

Definition 2 (Boomerang Connectivity Table [CHP+18])**.** Let S be a permutation of $\mathbb{F}_2^n$. The boomerang connectivity table (BCT) of S is a two-dimensional table defined by

$$\mathtt{BCT}(\Delta_1, \nabla_2) = \#\{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus \nabla_2) \oplus S^{-1}(S(x \oplus \Delta_1) \oplus \nabla_2) \ = \Delta_1\}, \text{ where } \Delta_1, \nabla_2 \in \mathbb{F}_2^n.$$

Let $\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2)$ and $\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta_2)$ denote the sets of valid inputs and outputs of differential $\Delta_1 \to \Delta_2$ respectively. Namely,

$$\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \triangleq \{x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus \Delta_1) = \Delta_2\},$$
$$\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \triangleq \{S(x) \in \mathbb{F}_2^n : x \in \mathbb{F}_2^n, S(x) \oplus S(x \oplus \Delta_1) = \Delta_2\}.$$

Then BCT can be calculated with $\mathcal{X}_{\mathtt{DDT}}$ or $\mathcal{Y}_{\mathtt{DDT}}$, as studied in [BC18, SQH19]. That is

$$\begin{aligned} \mathtt{BCT}(\Delta_1, \nabla_2) &= \sum_{\nabla_1} \#(\mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2) \cap (\mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2) \oplus \boldsymbol{\Delta_1})) \\ &= \sum_{\Delta_2} \#(\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \cap (\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \oplus \boldsymbol{\nabla_2})), \end{aligned} \tag{1}$$

where $\boldsymbol{\Delta_1}$ and $\boldsymbol{\nabla_2}$ are called *crossing differences* [SQH19]. As can be seen, whether the intersection of $\mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2)$ and $\mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2) \oplus \boldsymbol{\Delta_1}$ (resp. $\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta_2)$ and $\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \oplus \boldsymbol{\nabla_2}$) is empty or not depends on the crossing difference $\boldsymbol{\Delta_1}$ (resp. $\boldsymbol{\nabla_2}$). In particular, if the crossing difference $\boldsymbol{\Delta_1}$ (resp. $\boldsymbol{\nabla_2}$) for an S-box is random and uniformly distributed, the probability that the boomerang returns for this S-box is exactly $\sum_{\nabla_1}(\mathtt{DDT}(\nabla_1, \nabla_2)/2^n)^2$ (resp. $\sum_{\Delta_2}(\mathtt{DDT}(\Delta_1, \Delta_2)/2^n)^2$), which is the identical to the probability calculation of classical boomerang distinguisher.

To help calculate the probability of E_m with multiple rounds, two more tables were introduced in the literature.

Definition 3 (Difference Boomerang Table[3] [WP19]). Let S be a permutation of $\mathbb{F}_2^n$. The boomerang difference table (DBT) of S is a three-dimensional table defined by

$$\texttt{DBT}(\Delta_1, \Delta_2, \nabla_2) \triangleq \#\{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus \nabla_2) \oplus S^{-1}(S(x \oplus \Delta_1) \oplus \nabla_2) = \Delta_1, \\ S(x) \oplus S(x \oplus \Delta_1) = \Delta_2\} \text{ where } \Delta_1, \Delta_2, \nabla_2 \in \mathbb{F}_2^n.$$

Definition 4 (Boomerang Difference Table [SQH19]). Let S be a permutation of $\mathbb{F}_2^n$. The boomerang difference table (BDT) of S is a three-dimensional table defined by

$$\texttt{BDT}(\Delta_1, \nabla_2, \nabla_1) \triangleq \#\{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus \nabla_2) \oplus S^{-1}(S(x \oplus \Delta_1) \oplus \nabla_2) = \Delta_1, \\ x \oplus S^{-1}(S(x) \oplus \nabla_2) = \nabla_1\} \text{ where } \Delta_1, \nabla_2, \nabla_1 \in \mathbb{F}_2^n.$$

Based on the previous works, a new table of S-box will be proposed in the next section and used to calculate r for boomerang distinguishers of CRAFT, and SKINNY.

3 Our Strategy to Search for Boomerang Distinguishers

We use a heuristic approach to find a boomerang distinguisher which can be divided into the following steps:

1. The first step is searching for truncated differential characteristic with the minimum number of active Sboxes taking into account the switching effect in multiple rounds. For this step we borrow the idea of MILP-based automated search method for truncated differential characteristic proposed in [CHP+17], which takes into account the ladder switch effect in two middle rounds of boomerang distinguisher. However we change it a little to consider the switch effect in more than two rounds. We also use a weighted objective function in our model to obtain a boomerang distinguisher with higher probability.

   Suppose that we are looking for a boomerang distinguisher covering $r_0 + r_m + r_1$ rounds as illustrated in Figure 4. Firstly, we generate word-oriented MILP model consisting of constraints corresponding to truncated differential characteristics for the first $r_0 + r_m$, and last $r_1 + r_m$ rounds based on the independent binary variables respectively. Let $u_0, \ldots, u_{t-1}$ denote the activity of Sboxes in last r_m rounds of first $r_0 + r_m$ rounds and $l_0, \ldots, l_{t-1}$ denote the activity of Sboxes in first r_m rounds out of last $r_m + r_1$ rounds, such that u_i and l_i corresponds to the same Sbox for all $0 \leq i \leq t-1$. In order to model the switching effect in r-round middle part, which is highlighted in green in Figure 4, we introduce t new binary variables $s_0, \ldots, s_{t-1}$ such that for all $0 \leq i \leq t-1$:

   $$u_i - s_i \geq 0, \quad l_i - s_i \geq 0, \quad -u_i - l_i + s_i \geq -1.$$

   In other words $s_i = 1$ if and only of both x_i and y_i are 1, i.e. the Sbox corresponding to u_i and l_i is active in both first $r_0 + r_m$ and last $r_1 + r_m$ rounds. Let binary variables $\tilde{u}_0, \ldots, \tilde{u}_{m-1}$ and $\tilde{l}_0, \ldots, \tilde{l}_{n-1}$ denote the activity of Sboxes in the first r_0 and last r_1 rounds respectively. Assuming that w_0, w_1 and w are positive integer numbers, the objective is minimizing the following expression:

   $$\sum_{i=0}^{m-1} w_0.\tilde{u}_i + \sum_{j=0}^{t-1} w.s_j + \sum_{k=0}^{n-1} w_1.\tilde{l}_k.$$

   Given that the terms $\tilde{u} = \sum_{i=0}^{m-1} w_0.\tilde{u}_i$ and $\tilde{l} = \sum_{k=0}^{n-1} w_1.\tilde{l}_k$ are equally more effective than $s = \sum_{j=0}^{t-1} w.s_j$ in probability of the boomerang distinguisher, w_0, w_1 and w, are chosen such that $w_0 = w_1 \geq w$.

[3] In [WP19], this table is called BDT.

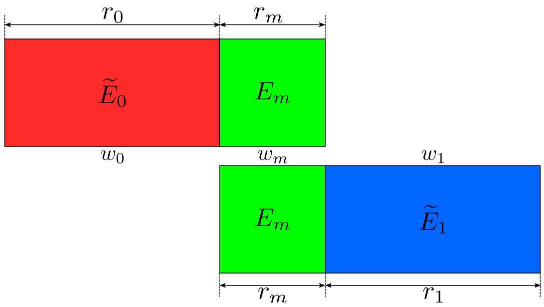

Figure 4: Main parameters of our word-oriented MILP tool to find boomerang distinguishers

2. Let $\widetilde{E}_0$ and $\widetilde{E}_1$ denote the first r_0 and last r_1 rounds respectively. At the second step, based on the discovered truncated differential characteristics corresponding to the $\widetilde{E}_0$ and $\widetilde{E}_1$, we look for the best actual differential trails satisfying the given active-cell positions for these parts which form upper and lower differential paths of boomerang distinguisher respectively. This is done using the separate bit-oriented MILP/SAT models for $\widetilde{E}_0$ and $\widetilde{E}_1$. Then, by fixing the input and output differences of actual differential paths for $\widetilde{E}_0$ and $\widetilde{E}_1$, and taking into account the clustering effect, we compute the differential effects for $\widetilde{E}_0$ and $\widetilde{E}_1$, which are represented by p and q respectively. Note that, there might not exist an actual differential characteristic corresponding to a discovered truncated differential characteristics. If so, we go to the first step and repeat the process by a new truncated differential characteristic.

3. Although the ladder switch effect is considered to obtain the upper and lower differential paths in our method, they are obtained using independent bit-oriented MILP/SAT models at step 2. Hence the upper and lower differential paths in a discovered boomerang distinguihser might be incompatible [Mur11]. The compatibility of the upper and lower differential paths in a discovered boomerang distinguisher is checked by experimentally evaluating the probability of the r-round middle part at this step. Assume that Δ_2 and ∇_3 are the output and input differences of upper and lower differential paths respectively, and E_m denotes the middle r_m rounds. In order to check the compatibility of the upper and lower differential paths we experimentally evaluate the following probability:

$$r = \Pr\left(E_m^{-1}(E_m(x_1) \oplus \nabla_3) \oplus E_m^{-1}(E_m(x_2) \oplus \nabla_3) = \Delta_2 | x_1 \oplus x_2 = \Delta_2\right),$$

   and go to the next step if $r > 0$. Otherwise, we go to the first step.

4. In order to correctly evaluate the size of E_m, where there exists a dependency between the upper and lower differential paths, we use the algorithm proposed by Song *et al.* in [SQH19] at this step. If this is done the formula p^2q^2r (where p and q are the probabilities of $\widetilde{E}_0$ and $\widetilde{E}_1$ respectively) will be a good estimate. Accordingly, additional rounds are added to E_m as long as the probability of the new E_m is higher than what is estimated by p^2q^2r.

5. If the size of E_m is changed at the previous step, we compute the probabilities p and q corresponding to new $\widetilde{E}_0$ and $\widetilde{E}_1$ respectively taking the clustering effect into account. Besides, using the `BCT` framework we provide a theoretical proof for the probability r, corresponding to the middle part E_m when it is possible from the computational complexity point of view. Finally, using the formula p^2q^2r, we compute the probability of the boomerang distinguisher.

4 New Tools for Modeling the Dependency in Boomerang Distinguishers

In this section, we introduce for S-boxes some new tables which can be used to model the dependency between upper and lower differential paths in boomerang distinguishers. When constructing boomerang distinguishers of SPN ciphers, there may exist two S-boxes in a row (in two rounds) which are active in both trails of the boomerang. Figure 5 (middle) shows the differences of such two S-boxes, where '$*$' stands for any possible difference, Δ_1 and ∇_3 are known.

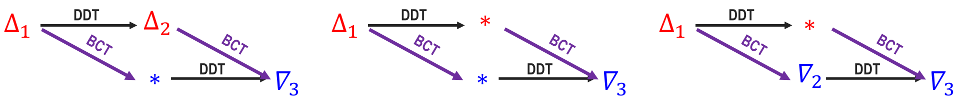

Figure 5: Differences of $\mathtt{DBCT}^{\vdash}$ (left), DBCT (middle) and $\mathtt{DBCT}^{\dashv}$ (right)

At first glance, we could build a two-dimensional table to record the number of values making the boomerang return for these two S-boxes. However, between two rounds usually, there is an operation of adding key material. Even though the key addition does not affect the differences before or after, but it is unknown and prevents us from building a table in the way that DDT and BCT are generated. However, in the case where the random subkey assumption holds, such a table can be built, as shown in algorithm 1. For convenience, we call this table *double boomerang connectivity table* (DBCT).

Algorithm 1: Building DBCT

Input: S-box S

1 Initialize an empty table DBCT with $2^n \times 2^n$ entries;
2 **for** $\Delta_1 = 0 \to 2^n - 1$ **do**
3   **for** $\nabla_3 = 0 \to 2^n - 1$ **do**
4     $num = 0$;
5   **for** $\Delta = 0 \to 2^n - 1$ **do**
6   **if** $\mathtt{DDT}(\Delta_1, \Delta) > 0$ *and* $\mathtt{BCT}(\Delta, \nabla_3) > 0$ **then**
7   **for** $\nabla = 0 \to 2^n - 1$ **do**
8           $\mathcal{Y}^{\cap}_{\mathtt{DDT}} = \mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta) \cap (\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta) \oplus \nabla)$;
9   **if** $\mathcal{Y}^{\cap}_{\mathtt{DDT}} \neq \emptyset$ **then**
10             $num \mathrel{+}= \mathtt{DDT}(\Delta_1, \Delta) \cdot \mathtt{BDT}(\Delta, \nabla_3, \nabla) \cdot \frac{\#\mathcal{Y}^{\cap}_{\mathtt{DDT}}}{\#\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta)}$;
11   **end**
12   **end**
13   **end**
14   **end**
15     $\mathtt{DBCT}(\Delta_1, \nabla_3) = num$;
16   **end**
17 **end**

Note that, if $\mathcal{Y}_{\mathtt{DDT}}$ forms an affine subspace, then the line 10 of algorithm 1 becomes $num \mathrel{+}= \mathtt{DDT}(\Delta_1, \Delta) \cdot \mathtt{BDT}(\Delta, \nabla_3, \nabla)$ as $\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta)$ equals $\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta) \oplus \nabla$ when their intersection is not empty. Recall that a mapping is *planar* if the $\mathcal{X}_{\mathtt{DDT}}$ and $\mathcal{Y}_{\mathtt{DDT}}$ of all its differentials form affine subspaces [DR07]. Particularly, S-boxes which only have nonzero DDT entries 2 and 4 are planar. Therefore, the S-box of CRAFT is planar, and each entry of its DBCT is an integer ranging from 0 to 2^{2n}.

Table 1: Summary of our results and the other known attacks on CRAFT. In this table, the attacks on single tweak mode, related tweak mode and related key mode are respectively denoted by ST , RT and RK and RT_i denotes RT mode that is started with TK_i. Moreover, boomerang, differential effect, truncated differential, linear hull, impossible differential, integral, and zero-correlation cryptanalysis are respectively denoted by B, D, TD, LH, ID, INT and ZC. For example, RT_1-D denotes differential effect of CRAFT in related tweak mode, starting with TK_1 and $ST - ID$ denoted impossible differential cryptanalysis in single tweak mode.

Attack	# Rounds	Probability	Reference
ST-D	10	$2^{-62.61}$	[BLMR19]
	9	$2^{-40.20}$	[HSN+19]
	10	$2^{-44.89}$	
	11	$2^{-49.79}$	
	12	$2^{-54.48}$	
	13	$2^{-59.13}$	
	14	$2^{-63.80}$	
ST-TD	12	2^{-36}	[MA19]
ST-LH	14	$2^{-62.12}$	[BLMR19]
ST-ID	13	-	
ST-INT	13	-	
ST-ZC	13	-	
ST-B	6	1	Section 5
	7	2^{-4}	
	8	2^{-8}	
	9	$2^{-14.76}$	
	10	$2^{-19.83}$	
	11	$2^{-24.90}$	
	12	$2^{-34.89}$	
	13	$2^{-44.89}$	
	14	$2^{-58.30}$	
RT_0-D	15	$2^{-55.14}$	[BLMR19]
RT_1-D	16	$2^{-57.18}$	
RT_2-D	17	$2^{-60.14}$	
RT_3-D	16	$2^{-55.14}$	
RT-ZC	14	-	[HSN+19]
RT-INT	14	-	[HSN+19]
RK-D	32	2^{-32}	[EY19]

Additionally, we introduce two variants of DBCT, *i.e.*, $\texttt{DBCT}^{\vdash}$ and $\texttt{DBCT}^{\dashv}$ as shown in Figure 5, where the differential of one S-box is fixed. Moreover, $\texttt{DBCT}^{\vdash}(\Delta_1, \Delta_2, \nabla_3), \texttt{DBCT}^{\dashv}(\Delta_1, \nabla_2, \nabla_3)$ can be precomputed by adapting algorithm 1, as shown in algorithm 2 and algorithm 3 in the appendix.

5 Boomerang Distinguishers for Reduced Rounds CRAFT

In this section, after giving a brief description of CRAFT, we introduce boomerang distinguishers for reduced rounds CRAFT covering up to 14 rounds of this cipher. The proposed distinguishers for our 9-/10-/11-/12-/13-/14-round boomerang distinguishers are based on the described E_m in Subsection 5.6. For other rounds, we present dedicated distinguishers, to maximize the success probabilities. Table 1 summarizes our results on boomerang distinguishers of CRAFT.

Table 2: Notations for `CRAFT`.

Symbol	Meaning
$\oplus$	XOR operation.
$\|\|$	Concatenation of bits.
%	modulo operation.
T	The 64-bit tweak input.
K	The 128-bit master key.
TK_i	The main tweaks that are made based on the T and K ($i = 0, 1, 2, 3$).
$TK^i_{i\%4}$	The 64-bit round tweakey which is used in round $\mathcal{R}_i$ ($i = 0, \ldots, 31$) and $TK^i_{i\%4}[j]$ represents the j-th cell ($j = 0, \ldots, 15$) of $TK^i_{i\%4}$.
X_i	The internal state before the Mix-Columns (MC) at round $\mathcal{R}_i$ ($i = 0, \ldots, 31$) and $X_i[j]$ represents the j-th cell ($j = 0, \ldots, 15$) of X^i.
Y_i	The internal state before the PermuteNibbles (PN) at round $\mathcal{R}_i$ ($i = 0, \ldots, 31$) and $Y_i[j]$ represents the j-th cell ($j = 0, \ldots, 15$) of Y_i.
Z_i	The internal state before the S-boxes (SB) at round $\mathcal{R}_i$ ($i = 0, \ldots, 31$) and $Z_i[j]$ represents the j-th cell ($j = 0, \ldots, 15$) of Z_i.
Δ	The forward difference.
∇	The backward difference.
ΔS	The forward difference at state S.
∇S	The backward difference at state S.
`Y`	Hexadecimal representation of arbitrary value $Y \in \mathbb{F}_2^4$, where we are using typewriter style.

5.1 Notations

Table 2 briefly describes the notations we use through this section.

5.2 A Brief Description of `CRAFT`

`CRAFT` is a lightweight tweakable block cipher which has been introduced in FSE 2018 by Beierle *et al.* [BLMR19], its round function is composed of involutory building blocks. This block cipher supports 64-bit message, 128-bit key and 64-bit tweak and its round function is composed of involutory building blocks. The input 64-bit plaintext $m = m_0\|m_1\| \cdots \|m_{14}\|m_{15}$ is used to initiate a 4×4 internal state $IS = I_0\|I_1\| \cdots \|I_{14}\|I_{15}$ as follows:

$$IS = \begin{pmatrix} I_0 & I_1 & I_2 & I_3 \\ I_4 & I_5 & I_6 & I_7 \\ I_8 & I_9 & I_{10} & I_{11} \\ I_{12} & I_{13} & I_{14} & I_{15} \end{pmatrix} = \begin{pmatrix} m_0 & m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 & m_7 \\ m_8 & m_9 & m_{10} & m_{11} \\ m_{12} & m_{13} & m_{14} & m_{15} \end{pmatrix}$$

where $I_i, m_i \in \mathbb{F}_2^4$. The internal state is then going through 32 rounds $\mathcal{R}_i, i \in 0, \cdots, 31$, to generate a 64-bit ciphertext. As is depicted in Figure 6, each round, excluding the last round, includes five functions, i.e., MixColumn (`MC`), AddRoundConstants (`ARC`), AddTweakey (`ATK`), PermuteNibbles (`PN`), and S-box (`SB`). The last round only includes `MC`, `ARC` and `ATK`, i.e., $\mathcal{R}_{31} = ATK_{31} \circ ARC_{31} \circ MC$, while for any $0 \leq i \leq 30$, $\mathcal{R}_i = SB \circ PN \circ ATK_i \circ ARC_i \circ MC$.

The `MC` layer is the multiplication of internal state by the following binary matrix:

$$MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Table 3: The S-box used in CRAFT in hexadecimal form.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	c	a	d	3	e	b	f	7	8	9	1	5	0	2	4	6

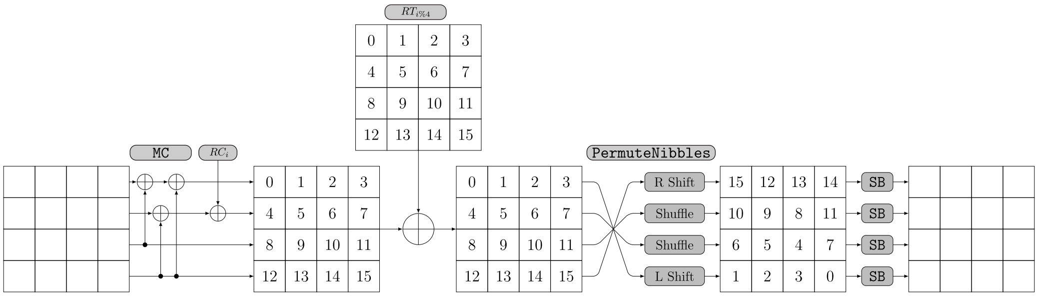

Figure 6: A round of CRAFT

In each round i, after MC, two round dependent constant nibbles $a_i = (a_3^i, a_2^i, a_1^i, a_0^i)$ and $b_i = (b_2^i, b_1^i, b_0^i)$ are XOR-ed with I_4 and I_5 respectively, where a_0^i and b_0^i are the least significant bits. A 4-bit LFSR is used to update a and a 3-bit LFSR is used to update b. They are initialized by values (0001) and (001), respectively and updated to $a_{i+1} = (a_1^i \oplus a_0^i, a_3^i, a_2^i, a_1^i)$, and $b_{i+1} = (b_1^i \oplus b_0^i, b_2^i, b_1^i)$ from i-th round to $i+1$-th round.

After AddRoundConstants (ARC), a 64-bit round tweakey is XOR-ed with IS. The tweakey schedule of CRAFT is rather simple. Given the secret key $K = K_0 \| K_1$ and the tweak $T \in \{0,1\}^{64}$, where $K_i \in \{0,1\}^{64}$, four round tweakeys $TK_0 = K_0 \oplus T$, $TK_1 = K_1 \oplus T$, $TK_2 = K_0 \oplus Q(T)$ and $TK_3 = K_1 \oplus Q(T)$ are generated, where given $T = T_0 \| T_1 \| \cdots \| T_{14} \| T_{15}$, $Q(T) = T_{12} \| T_{10} \| T_{15} \| T_5 \| T_{14} \| T_8 \| T_9 \| T_2 \| T_{11} \| T_3 \| T_7 \| T_4 \| T_6 \| T_0 \| T_1 \| T_{13}$. Then at the round $\mathcal{R}_i$, $TK_{i\%4}^i$ is XOR-ed with the IS, where the rounds start from $i = 0$.

The next function is PermuteNibbles (PN) which is applying an involutory permutation P over nibbles of IS, where given $IS = I_0 \| I_1 \| \cdots \| I_{14} \| I_{15}$, $P(IS) = I_{15} \| I_{12} \| I_{13} \| I_{14} \| I_{10} \| I_9 \| I_8 \| I_{11} \| I_6 \| I_5 \| I_4 \| I_7 \| I_1 \| I_2 \| I_3 \| I_0$.

The final function is a non-linear 4×4-bit S-box which has been borrowed from MIDORI [BBI+15]. The table representation of the S-box is given in Table 3.

Through this section, following Table 2, we represent the internal state at the input of round-r by $X_r = X_r[0] \| \cdots \| X_r[15]$, after MC by $Y_r = Y_r[0] \| \cdots \| Y_r[15]$ and after the PN layer by $Z_r = Z_r[0] \| \cdots \| Z_r[15]$. It is clear that the state after SB is the input of the next round which is X_{r+1}. The tweak which is used in round-r is denoted by $TK^r = TK_0^r \| TK_1^r \| \cdots \| TK_{14}^r \| TK_{15}^r$.

5.3 6-Round Boomerang Distinguisher

Figure 7 shows a 6-round boomerang distinguisher for CRAFT, where there is not any interaction between active cells of upper, and lower differential trails, and therefore a right quartet, can be generated with probability 1.

5.4 7-Round Boomerang Distinguisher

We obtained a 7-round distinguisher as depicted in Figure 8. The diffusion of differences in the upper differential trail depends on that whether $\gamma = \gamma'$ or not, and that's why there are two different differential trails in Figure 8, where each one shows one of the possible differential trails. Let's r_1, and r_2 be the probability of boomerang distinguisher, when

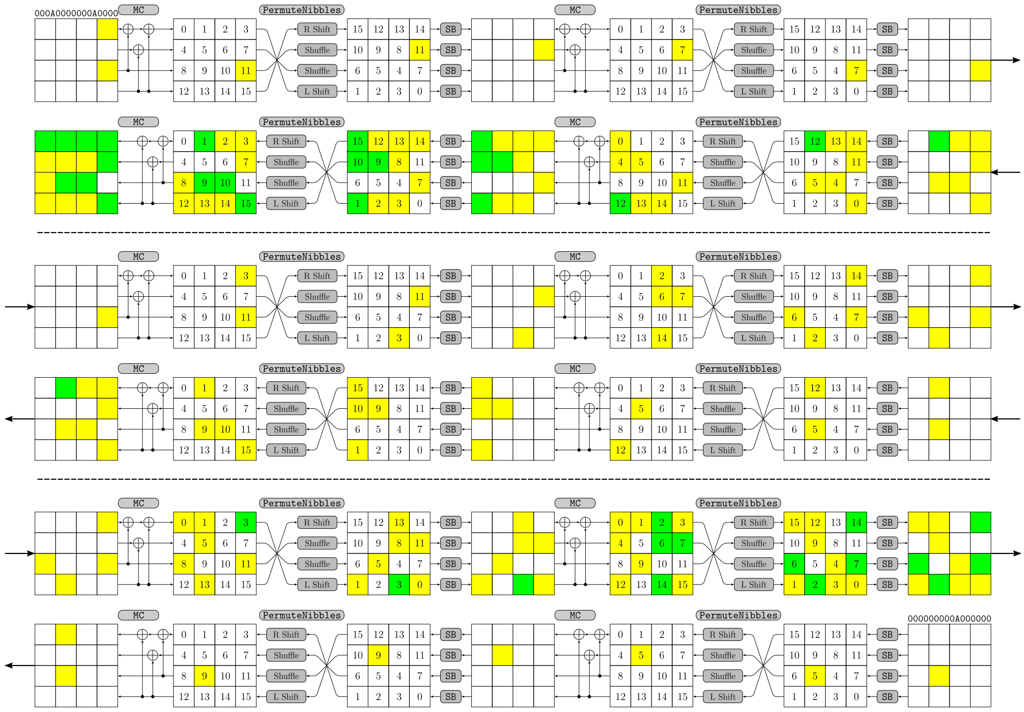

Figure 7: A 6-round boomerang distinguisher of `CRAFT`

$\gamma = \gamma'$, and $\gamma \neq \gamma'$ respectively. Therefore the probability of the given 7-round boomerang distinguisher is $r = r_1.\Pr(\gamma = \gamma') + r_2.\Pr(\gamma \neq \gamma')$.

In order to calculate r_1, one can consider the whole of the 7 rounds in Figure 8, as E_m. If $\gamma = \gamma'$, upper, and lower differential trails have only one active cell in common, which is denoted by γ, and β in upper, and lower differential trails respectively, and there is not any interaction between other active cells in upper, and lower differential trails. The red frames in the Figure 8, track the difference β, and show that it is not affected by the upper differential trial. From the other side, the distribution of β is very close to a uniform distribution. Therefore r_1 can be calculated as follows:

$$r_1 = \sum_{\gamma \in \{\mathtt{5,A,D,F}\}} \left(\frac{\mathtt{DDT}(\mathtt{A}, \gamma)}{2^4}\right)^2 = \sum_{\gamma \in \{\mathtt{5,A,D,F}\}} (2^{-2})^2 = 2^{-2}.$$

and $r_1.\Pr(\gamma = \gamma') = 2^{-2}.2^{-2} = 2^{-4}$. Since $0 \leq r_2.\Pr(\gamma \neq \gamma') \leq 1$, we can conclude that $r \geq 2^{-4}$. The experimental evaluations show that $r \approx 2^{3.98}$.

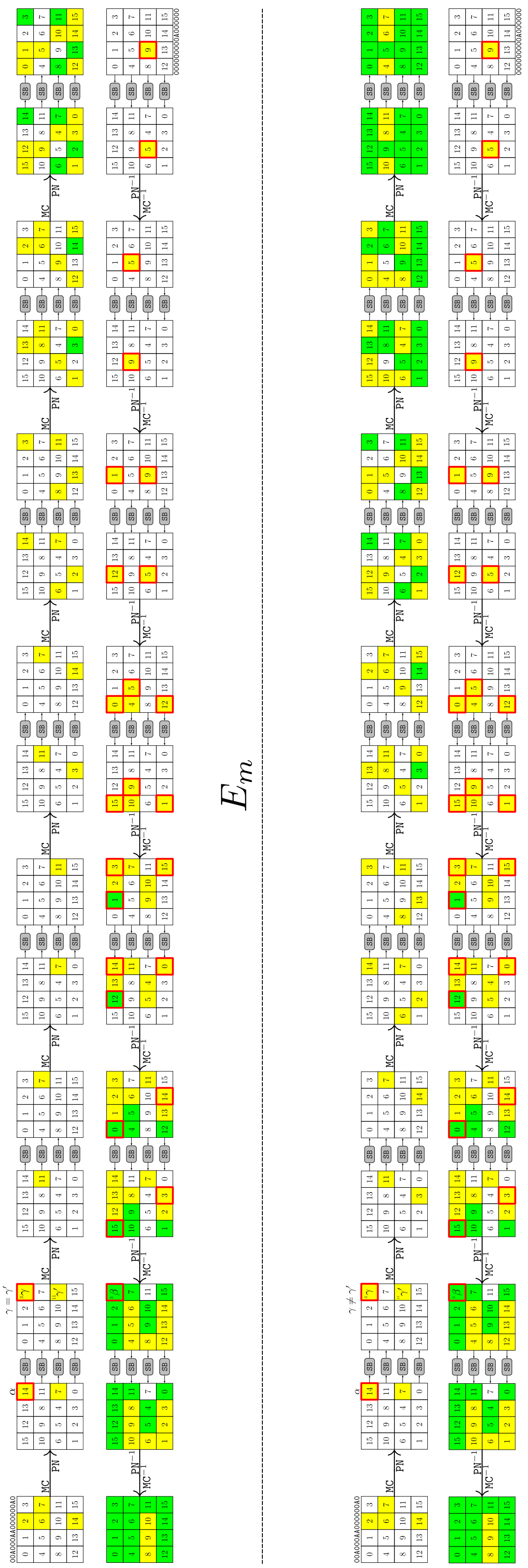

Figure 8: A dedicated 7-round boomerang distinguisher for CRAFT

5.5 8-Round Boomerang Distinguisher

Figure 9 shows an 8-round boomerang distinguisher. One can consider the whole 8 rounds as E_m. The diffusion of upper, and lower differential trails in this distinguisher, depends on that whether $(\gamma = \gamma') \wedge (\delta = \delta')$ or not. In the Figure 9, it is supposed that $(\gamma = \gamma') \wedge (\delta = \delta')$. Let r_1, and r_2 be the probability of this 8-round boomerang distinguisher, when $(\gamma = \gamma') \wedge (\delta = \delta')$, and $(\gamma \neq \gamma') \vee (\delta \neq \delta')$ respectively. Therefore, the total probability of the boomerang distinguisher is $r = r_1. \Pr((\gamma = \gamma') \wedge (\delta = \delta')) + r_2. \Pr((\gamma \neq \gamma') \vee (\delta \neq \delta'))$. Since two relations $\gamma = \gamma'$, and $\delta = \delta'$ are statistically independent, we have:

$$r = r_1. \Pr(\gamma = \gamma'). \Pr(\delta = \delta') + r_2. \Pr((\gamma \neq \gamma') \vee (\delta \neq \delta')).$$

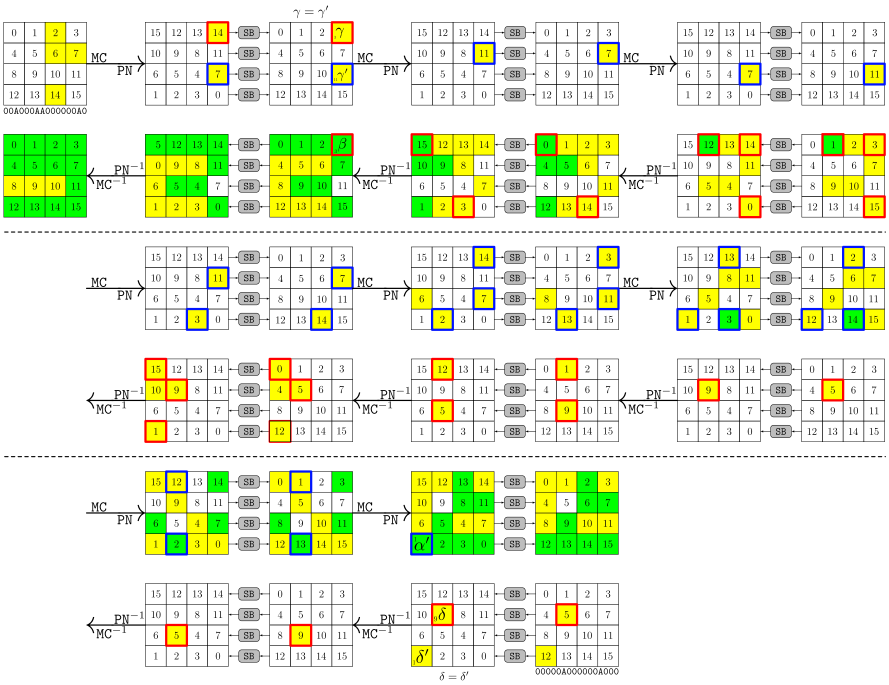

Figure 9: A dedicated 8-round boomerang distinguisher for `CRAFT`

The upper, and lower differential trails in Figure 9, have only two active cells in common, and there is not any interaction between other active cells in upper, and lower differential trails. The lower crossing difference β is uniformly distributed, and as it's depicted by the red frames, it is independent of the upper differential trail. The upper crossing difference α' is also uniformly distributed, and as it's depicted by blue frames, it is independent of the lower differential trail too. Therefore r_1, can be obtained as follows:

$$\begin{aligned} r_1 &= \sum_{\gamma \in \{\mathtt{5,A,D,F}\}} \sum_{\delta \in \{\mathtt{5,A,D,F}\}} \left(\frac{\mathtt{DDT}(\mathtt{A}, \gamma)}{2^4}\right)^2 . \left(\frac{\mathtt{DDT}(\delta, \mathtt{A})}{2^4}\right)^2 \\ &= \sum_{\gamma \in \{\mathtt{5,A,D,F}\}} \sum_{\delta \in \{\mathtt{5,A,D,F}\}} \left(2^{-2}\right)^2 . \left(2^{-2}\right)^2 = 2^{-4}. \end{aligned}$$

and $r_1. \Pr(\gamma = \gamma'). \Pr(\delta = \delta') = 2^{-4}.2^{-2}.2^{-2} = 2^{-8}$. Since $0 \leq r_2. \Pr((\gamma \neq \gamma') \vee (\delta \neq \delta')) \leq 1$, we can conclude that $r \geq 2^{-8}$. Experimental evaluations show that $r \approx 2^{-7.9}$.

5.6 Probability of A 7-Round Boomerang Distinguisher of CRAFT

Figure 10 shows a 7-round boomerang distinguisher which is also the E_m of our 9-/10-/11-/12-/13-/14-round boomerang distinguishers of CRAFT, in Section 5. Next, let us calculate the probability of this 7-round boomerang distinguisher.

In Figure 10, the input difference of the upper trail and the output difference of the lower trail is given; green squares denote any possible difference while yellow squares denote nonzero differences. Due to the weak diffusion of the linear layer of CRAFT, it can be seen that the difference after 7 rounds is not random enough as there are still nonzero differences in state a' and H (see Figure 10). That is, the crossing differences throughout the whole distinguisher are not random enough, which means there is a strong dependency between the upper trail and the lower trail.

We further investigate the dependency of the two trails with the help of notations $\xrightarrow{\texttt{DDT}}$ and $\xrightarrow{\texttt{BCT}}$. As can be seen from Figure 10, the dependency of the two trails can be modularized into two $\texttt{DBCT}^{\vdash}$ and two $\texttt{DBCT}^{\dashv}$ which affect each other.

Let $\texttt{DBCT}_{\text{total}}$ be the product of the four DBCT, *i.e.*,

$$\begin{aligned}\texttt{DBCT}_{\text{total}} = {} & \texttt{DBCT}^{\vdash}(A'_5, orange, c_5) \cdot \texttt{DBCT}^{\vdash}(orange, orchid, d_1)\cdot \\ & \texttt{DBCT}^{\dashv}(E'_1, cyan, rubine) \cdot \texttt{DBCT}^{\dashv}(F'_5, rubine, h_5),\end{aligned}$$

where the variables and colors are differences depicted in Figure 10 and particularly the each color denotes any variable marked by the box of that color. Let

$$\begin{aligned}\Pr_{\text{total}} = {} & \Pr(d_1 \xleftarrow{2\ \texttt{DDT}} cyan) \cdot \Pr(c_5 \xleftarrow{3\ \texttt{DDT}} cyan)\cdot \\ & \Pr(orchid \xrightarrow{2\ \texttt{DDT}} E'_1) \cdot \Pr(orchid \xrightarrow{3\ \texttt{DDT}} F'_5),\end{aligned}$$

then the probability of the 7-round boomerang distinguisher for a fixed pair of (A'_5, h_5) is

$$r = 2^{-8n} \cdot \sum_{orange}\sum_{orchid}\sum_{rubine}\sum_{cyan}\sum_{c_5}\sum_{d_1}\sum_{E'_1}\sum_{F'_5} \texttt{DBCT}_{\text{total}} \cdot \Pr_{\text{total}}.$$

When $(A'_5, h_5) = (\texttt{A}, \texttt{A})$, $r = 2^{-10.39}$. We also calculated the value of r for all $(A'_5, h_5) \in \{(i, j)|1 \le i \le 15, 1 \le j \le 15\}$, and arranged the results in a 15×15 matrix called $R^{7r} = [r]_{i,j}$, where $r_{i,j}$ is the value of r, when $(A'_5, h_5) = (i, j)$. This matrix is displayed in Appendix B, and Figure 11 is a visual representation of this matrix. We carry out experiments on this distinguisher, and arranged the experimental probabilities in matrix r_e^{7r} which is displayed in Appendix B. Comparing theoretical, and empirical probabilities, shows the theoretical probability matches the experimental probability very well, for almost all cases.

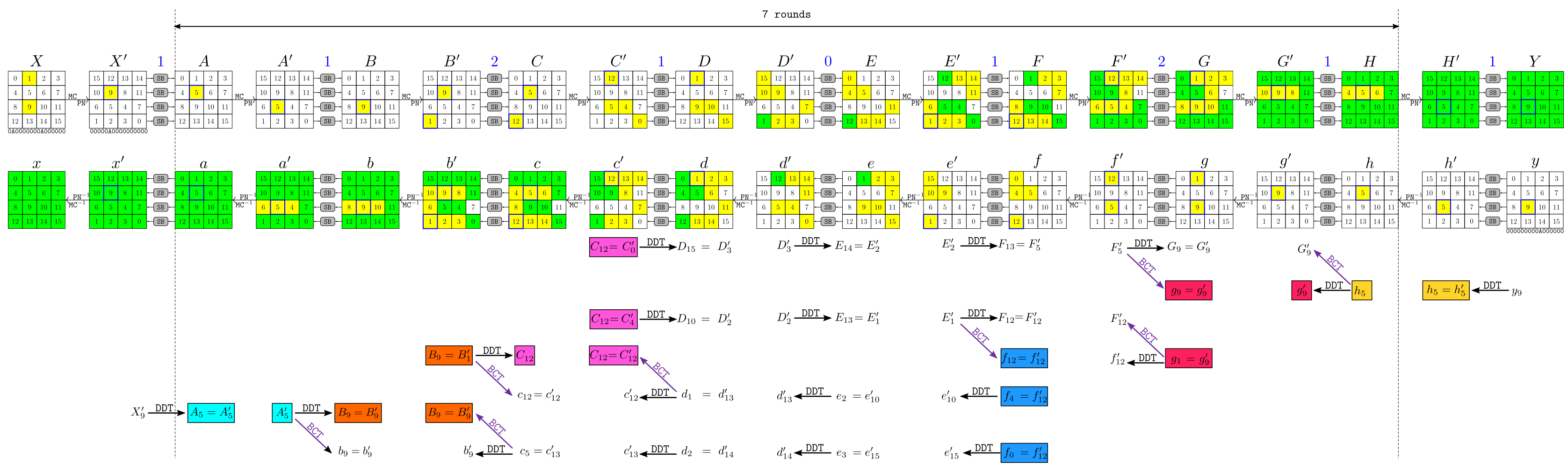

Figure 10: A 7-round E_m where two $\texttt{DBCT}^{\vdash}$ and two $\texttt{DBCT}^{\dashv}$ are involved

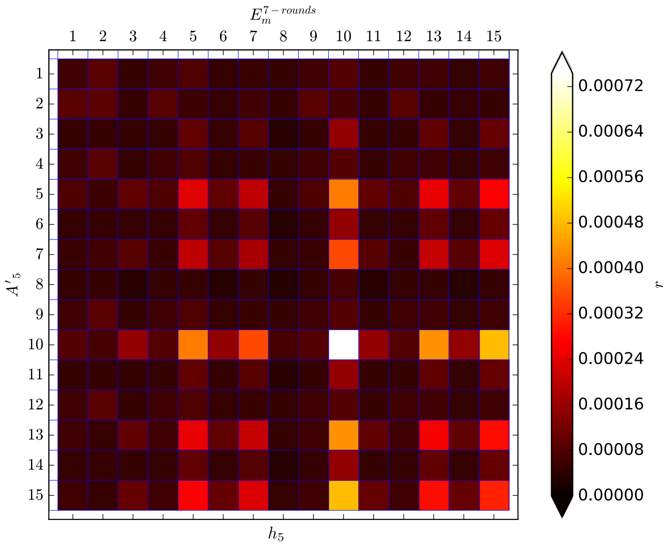

Figure 11: A visual representation of probability matrix r^{7r}

5.7 9-Round Boomerang Distinguisher

In order to construct a 9-round distinguisher for CRAFT, we extend the 7-round distinguisher E_m^{7r} in Section 4, by one round in both directions. Since the lower, and upper crossing differences in E_m^{7r}, are uniforly distributed after 7 rounds, the extended parts in the beginning, and the end of E_m^{7r}, can be considered as E_0, and E_1, respectively.

The input and output differences, in 9-round distinguisher are chosen as follows:

$$\Delta_1 = \texttt{0A00 0000 0A00 0000},\ \nabla_4 = \texttt{0000 0000 0A00 0000}.$$

The differences Δ_2, and ∇_3, are chosen according to the following templates:

$$\Delta_2 = \texttt{0000 0}\delta\texttt{00 0000 0000},\ \nabla_3 = \texttt{0000 0}\gamma\texttt{00 0000 0000},$$

where $\delta, \gamma \in \mathbb{F}_2^4 \setminus \{0\}$. If $\delta = \texttt{A}$, and $\gamma = \texttt{A}$, then a lower bound for the whole boomerang distinguisher is as follows:

$$\Big(\Pr(\Delta_1 \xrightarrow{E_0} \Delta_2)\Big)^2 . \Big(\Pr(\nabla_3 \xrightarrow{E_1} \nabla_4)\Big)^2 .R^{7r}_{10,10} = 2^{-4}.2^{-4}.2^{-10.39} = 2^{-18.39},$$

Where r^{7r} is the matrix corresponding to the E_m^{7r}, which is represented in Appendix B. Let Δ_2^i, and ∇_3^j, are chosen as follows:

$$\Delta_2^i = \texttt{0000 0}i\texttt{00 0000 0000},\ \nabla_3^j = \texttt{0000 0}j\texttt{00 0000 0000},$$

where $1 \leq i, j \leq 15$. By considering the clustering effect, similar to the Figure 12, we can improve our bound for probability of the whole boomerang distinguisher for 9 rounds of CRAFT, as follows:

$$\sum_{i=1}^{15}\sum_{j=1}^{15} \Big(\Pr(\Delta_1 \xrightarrow{E_0} \Delta_2^i)\Big)^2 . \Big(\Pr(\nabla_3^j \xrightarrow{E_1} \nabla_4)\Big)^2 .R^{7r}_{i,j} = 2^{-15.43}.$$

Let p_{bm}^{9r}, depicts the probability of boomerang distinguihser covering 9 rounds of CRAFT, when the input, and output differences are fixed as above. Therefor, we proved that

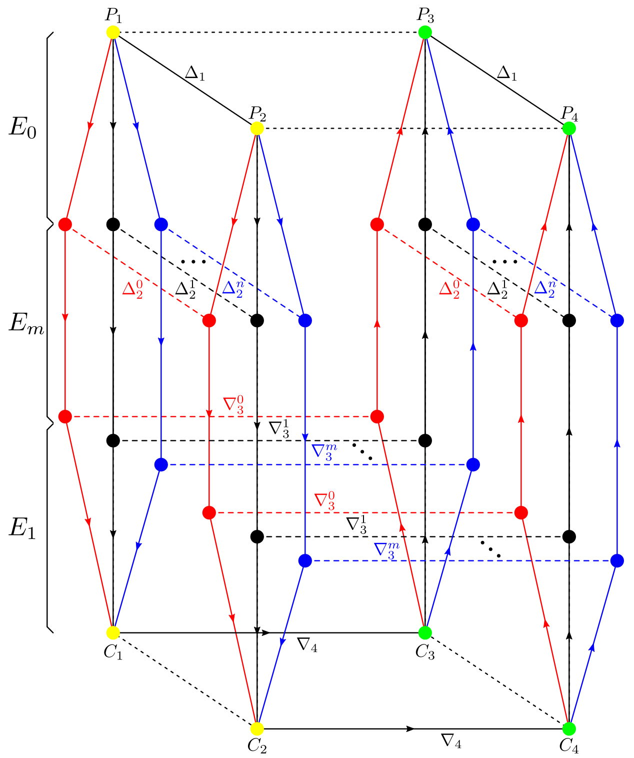

Figure 12: Cluster of sandwich distinguishers

$p_{bm}^{9r} \geq 2^{-15.43}$. However, the empirical value of p_{bm}^{9r}, is about $2^{-14.50}$. The main reason of this gap between the theoretical bound, and the empirical approximation of p_{bm}^{9r}, is considering differences to be equal in two sides of boomerang cube, while they can take different values indeed.

In other words, differences at positions A_5 and h_5 in Figure 10, can take different values in two sides of boomerang, when the 7-round boomerang distinguisher is extended by one round in both directions, to obtain a 9-round boomerang distinguisher. In order to obtain a more accurate bound for p_{bm}^{9r}, we introduce two new Sbox tables as follows:

$$\mathtt{DBT}^{\star}(\Delta_1, \Delta_1', \nabla_2, \Delta_2) := \#\{S(x) \in \mathbb{F}_2^n | S(x) \in \mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta_2) : \ S(x) \in \mathcal{Y}_{\mathtt{DDT}}(\Delta_1', \Delta_2) \oplus \nabla_2\}.$$
$$\mathtt{BDT}^{\star}(\Delta_1, \nabla_2, \nabla_2', \nabla_1) := \#\{x \in \mathbb{F}_2^n | x \in \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2) : \ x \in \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2') \oplus \Delta_1\}.$$

Using $\mathtt{DBT}^{\star}$ and $\mathtt{BDT}^{\star}$, we revise the probability calculation of 9-round boomerang distinguisher as follows.

$$\begin{aligned}\mathtt{BCT}_{\mathtt{tot}} = {} & \mathtt{DBT}^{\star}(A_{51}, A_{52}, b_9, B_9).\mathtt{DDT}(X_9', A_{51}).\mathtt{DDT}(X_9', A_{52}) \\ & .\mathtt{BDT}(B_9, c_5, b_9).\mathtt{DBT}(B_9, c_{12}, C_{12}).\mathtt{BDT}(C_{12}, d_1, c_{12}) \\ & .\mathtt{DBT}(E_1', f_{12}', F_{12}).\mathtt{BDT}(F_{12}, g_9', f_{12}').\mathtt{DBT}(F_5', g_9', G_9) \\ & .\mathtt{BDT}^{\star}(G_9, h_{51}, h_{52}, g_9').\mathtt{DDT}(h_{51}, y_9).\mathtt{DDT}(h_{52}, y_9).\end{aligned}$$

$$\begin{aligned}\mathtt{Pr}_{\text{total}} = {} & \Pr(d_1 \xleftarrow{2\ \mathtt{DDT}} cyan) \cdot \Pr(c_5 \xleftarrow{3\ \mathtt{DDT}} cyan) \cdot \\ & \Pr(orchid \xrightarrow{2\ \mathtt{DDT}} E_1') \cdot \Pr(orchid \xrightarrow{3\ \mathtt{DDT}} F_5'),\end{aligned}$$

where (A_{51}, A_{52}), and (h_{51}, h_{52}), are the values of differences at position A_5, and h_5 in two faces of boomerang respectively. Therefore, the total probability of 9-round boomerang distinguisher is calculated according to the following formula:

$$p^{9r}_{bm}(X'_9, y_9) = 2^{-12.n}.\sum_{A_{51}}\sum_{A_{52}}\sum_{b_9}\sum_{B_9}\sum_{c_5}\sum_{c_{12}}\sum_{C_{12}}\sum_{d_1}\sum_{E'_1}\sum_{f'_{12}}\sum_{F_{12}}\sum_{g'_9}\sum_{F'_5}\sum_{G_9}\sum_{h_{51}}\sum_{h_{52}}\mathtt{BCT}_{\mathtt{tot}}.\mathtt{Pr}_{\mathtt{tot}}.$$

Evaluating the above formula, when $(X'_9, y_9) = (\mathtt{0xA}, \mathtt{0xA})$, yields $p^{9r}_{bm} = 2^{-14.76}$, which is too close to the the experimental approximation of p^{9r}_{bm}. It also verifies our assumption that the dependency doesn't exist out of the the 7-round middle part.

The above observation, motivated us to model the 7-round middle part by a four dimensional matrix instead of a two dimensional matrix, using two new Sbox tables $\mathtt{DBT}^{\star}$, and $\mathtt{BDT}^{\star}$. Let A_{51}, and A_{52}, are differences in two sides of boomerang at position A_5. Similarly, h_{51}, and h_{52}, are differences in two sides of boomerang at position h_5. In order to obtain a more accurate bound for the boomerang distinguishers obtained by extending our 7-round boomerang distinguisher, We define the 4-dimensional matrix $R^{7r}_{i,j,k,l}$, as follows:

$$\begin{aligned}R^{7r}[i,j,k,l] = 2^{-8.n}.&\sum_{b_9}\sum_{B_9}\sum_{c_5}\sum_{c_{12}}\sum_{C_{12}}\sum_{d_1}\sum_{E'_1}\sum_{f'_{12}}\sum_{F_{12}}\sum_{g'_9}\sum_{f'_{12}}\sum_{F'_5}\sum_{G_9}\mathtt{DBT}^{\star}(A_{51}, A_{52}, b_9, B_9)\\ &.\mathtt{BDT}(B_9, c_5, b_9).\mathtt{DBT}(B_9, c_{12}, C_{12}).\mathtt{BDT}(C_{12}, d_1, c_{12})\\ &.\mathtt{DBT}(E'_1, f'_{12}, F_{12}).\mathtt{BDT}(F_{12}, g'_9, f'_{12}).\mathtt{DBT}(F'_5, g'_9, G_9)\\ &.\mathtt{BDT}^{\star}(G_9, h_{51}, h_{52}, g'_9)\\ &.\mathtt{Pr}_{\mathtt{tot}},\ \text{ where } A_{51} = i, A_{52} = j, h_{51} = k, h_{52} = l.\end{aligned}$$

A more efficient formula to calculate $R^{7r}[i,j,k,l]$, is given in Appendix E.

5.8 10-Round Boomerang Distinguisher

If the 7-round distinguisher E^{7r}_m, is extended by two rounds from the beginning, and by one round from the end, a 10-round boomerang distinguisher with the following input, and output differences is obtained:

$$\Delta_1 = \mathtt{A000\ AA00\ 0000\ A000},\ \nabla_4 = \mathtt{0000\ 0000\ 0A00\ 0000}.$$

Let E^{2r}_0, E^{1r}_1, show the extended parts, which cover two, and one round respectively. By considering the intermediate differences Δ^i_2, ∇^j_3, as follows:

$$\Delta^i_2 = \mathtt{0000\ 0}i\mathtt{00\ 0000\ 0000},\ \nabla^j_3 = \mathtt{0000\ 0}j\mathtt{00\ 0000\ 0000}, \tag{2}$$

where $0 \leq i, j \leq 15$, the following formula, gives a lower bound for the probability of the whole boomerang distinguisher, covering 10-rounds of CRAFT:

$$\sum_{i=1}^{15}\sum_{j=1}^{15}\left(\Pr(\Delta_1 \xrightarrow{E^{2r}_0} \Delta^i_2)\right)^2.\left(\Pr(\nabla^j_3 \xrightarrow{E^{1r}_1} \nabla_4)\right)^2.R^{7r}_{i,j} = 2^{-20.42}.$$

Let p^{10r}_{bm}, is the probability of our 10-round boomerang distinguisher, with the following input/output differences. The empirical value of p^{10r}_{bm} is approximately $2^{-18.17}$. Using the four dimensional matrix $R^7_{i,j,k,l}$, we can obtain a more accurate bound as follows:

$$\begin{aligned}\sum_{i=1}^{15}\sum_{j=1}^{15}\sum_{k=1}^{15}\sum_{l=1}^{15}&\Pr(\Delta_1 \xrightarrow{E^{2r}_0} \Delta^i_2).\Pr(\Delta_1 \xrightarrow{E^{2r}_0} \Delta^j_2)\\ &.\Pr(\nabla^k_3 \xrightarrow{E^{1r}_1} \nabla_4).\Pr(\nabla^l_3 \xrightarrow{E^{1r}_1} \nabla_4)\\ &.R^{7r}_{i,j,k,l} = 2^{-19.83}.\end{aligned}$$

However, the empirical approximation of p_{bm}^{10r}, is about $2^{-18.17}$. This gap between the theoretical bound, and the experimental approximation, is caused by assuming $X_1 = X_9$, in Figure 10, while they can take different values in our 10-round boomerang distinguisher. Therefore we've calculated the probability of one possible activity pattern, out of two possible patterns. In the second possible activity pattern, $X_1 \neq X_9$. Note that the theoretical calculation of the second activity pattern, is too complex, due to the high number of common active Sboxes between upper, and lower differential paths.

5.9 11-Round Boomerang Distinguisher

We have obtained a 11-round boomerang distinguisher for `CRAFT`, by extending the 7-round distinguisher E_m^{7r}, by two rounds, in both directions. The input, and output differences, in this 11-round boomerang distinguisher, are chosen as follows:

$$\Delta_1 = \texttt{A000 AA00 0000 A000},\ \nabla_4 = \texttt{0000 0A00 0000 A000}.$$

Let E_0^{2r}, and E_1^{2r}, depict the extended 2-round parts. By considering the intermediate differences Δ_2^i, and ∇_3^j, according to Equation 2, we can find a lower bound for the 11-round boomerang distinguisher as follows:

$$\sum_{i=1}^{15}\sum_{j=1}^{15}\left(\Pr(\Delta_1 \xrightarrow{E_0^{2r}} \Delta_2^i)\right)^2 . \left(\Pr(\nabla_3^j \xrightarrow{E_1^{2r}} \nabla_4)\right)^2 .R_{i,j}^{7r} = 2^{-25.40}.$$

Let p_{bm}^{11r}, depicts the probability of the above 11-round boomerang distinguisher. Using the 4-dimensional matrix $R_{i,j,k,l}^{7r}$, we can obtain a more accurate bound for p_{bm}^{11r} as follows:

$$\begin{aligned}\sum_{i=1}^{15}\sum_{j=1}^{15}\sum_{k=1}^{15}\sum_{l=1}^{15}\Pr(\Delta_1 \xrightarrow{E_0^{2r}} \Delta_2^i).\Pr(\Delta_1 \xrightarrow{E_0^{2r}} \Delta_2^j)&\\ .\Pr(\nabla_3^k \xrightarrow{E_1^{2r}} \nabla_4).\Pr(\nabla_3^l \xrightarrow{E_1^{2r}} \nabla_4)&\\ .R_{i,j,k,l}^{7r} = 2^{-24.90}.&\end{aligned}$$

However, the empirical approximation of p_{bm}^{11r} is about $2^{-21.50}$. To find the reason of this gap between the theoretical bound, and experimental approximation, note that in Figure 10, it is supposed that $X_1 = X_9$, and the input differences of Sbox layer in 11'th round are equal as well, while these constraints are not necessary in our 11-round boomerang distinguisher. Therefore we have calculated the probability of one activity pattern out of 4 possible activity patterns. Note that, the theoretical calculation of boomerang probability, in other three cases, where $X_1 \neq X_9$, or the input differences of Sbox layer in 11'th round are not equal, is too complex due to the high number of common active Sboxes between upper, and lower trails of boomerang distinguisher.

5.10 12-Round Boomerang Distinguisher

In order to construct a 12-round boomerang distinguisher, we extended the 7-round boomerang distinguisher E_m^{7r}, by 3, and 2 rounds, from the beginning, and end respectively. Input, and output differences of the obtained 12-round boomerang distinguisher are as follows:

$$\Delta_1 = \texttt{00AA 000A 0AA0 000A},\ \nabla_4 = \texttt{0000 0A00 0000 A000},$$

and the intermediate differences Δ_2^i, and ∇_2^j, are chosen according to Equation 2. A lower bound for the obtained 12-round distinguisher is calculated as follows:

$$\sum_{i=1}^{15}\sum_{j=1}^{15}\left(\Pr(\Delta_1 \xrightarrow{E_0^{3r}} \Delta_2^i)\right)^2 . \left(\Pr(\nabla_3^j \xrightarrow{E_1^{2r}} \nabla_4)\right)^2 .R_{i,j}^{7r} = 2^{-35.49}.$$

Let p_{bm}^{12r}, is the probability of the above 12-round boomerang distinguihser. Accordingly, $p_{bm}^{12r} \geq 2^{-35.49}$. However, using the 4-dimensional matrix $R_{i,j,k,l}^{7r}$, we can obtain a more tight bound for this probability as follows:

$$\sum_{i=1}^{15}\sum_{j=1}^{15}\sum_{k=1}^{15}\sum_{l=1}^{15} \Pr(\Delta_1 \xrightarrow{E_0^{3r}} \Delta_2^i).\Pr(\Delta_1 \xrightarrow{E_0^{3r}} \Delta_2^j)$$
$$\Pr(\nabla_3^k \xrightarrow{E_1^{2r}} \nabla_4).\Pr(\nabla_3^l \xrightarrow{E_1^{2r}} \nabla_4)$$
$$.R_{i,j,k,l}^{7r} = 2^{-34.89}.$$

5.11 13-Round Boomerang Distinguisher

If the 7-round boomerang distinguisher E_m^{7r}, is extedned by three rounds in both sides, a 13-round boomerang distinguisher, with the following input, and output differences is obtained:

$$\Delta_1 = \texttt{00AA 000A 0AA0 000A},\ \nabla_4 = \texttt{0A00 0000 0AA0 000A}.$$

By considering the intermediate differences Δ_2^i, and ∇_3^j, according to Equation 2, we can find a lower bound for the probability of the obtained 13-round boomerang distinguisher, as follows:

$$\sum_{i=1}^{15}\sum_{j=1}^{15}\left(\Pr(\Delta_1 \xrightarrow{E_0^{3r}} \Delta_2^i)\right)^2.\left(\Pr(\nabla_3^j \xrightarrow{E_1^{3r}} \nabla_4)\right)^2.R_{i,j}^{7r} = 2^{-45.59}.$$

Let p_{bm}^{13r}, depicts the probability of the above 13-round boomerang distinguisher. The above relation proves that $p_{bm}^{13r} \geq 2^{-45.59}$. However, using the 4-dimensional matrix $R_{i,j,k,l}^{7r}$, a more accurate bound for this probability can be obtained as follows:

$$\sum_{i=1}^{15}\sum_{j=1}^{15}\sum_{k=1}^{15}\sum_{l=1}^{15} \Pr(\Delta_1 \xrightarrow{E_0^{3r}} \Delta_2^i).\Pr(\Delta_1 \xrightarrow{E_0^{3r}} \Delta_2^j)$$
$$.\Pr(\nabla_3^k \xrightarrow{E_1^{3r}} \nabla_4).\Pr(\nabla_3^l \xrightarrow{E_1^{3r}} \nabla_4)$$
$$.R_{i,j,k,l}^{7r} = 2^{-44.89}.$$

5.12 14-Round Boomerang Distinguisher

We propose a 14-round boomerang distinguisher for `CRAFT`, which is obtained by extending the 7-round boomerang distinguisher E_m^{7r}, by 3 rounds from the beginning, and by 4 rounds from the end. The input, and output differences of the proposed 14-round boomerang distinguisher are as follows:

$$\Delta_1 = \texttt{00AA 000A 0AA0 000A},\ \nabla_4 = \texttt{A000 AA00 000A 0AA0}.$$

Let's depict the extended parts, by E_0^{3r}, and E_1^{4r}, that cover 3, and 4 rounds respectively, and choose the intermediate differences Δ_2^i, and ∇_3^j, according to Equation 2. A lower bound for the obtained 14-round distinguisher, is calculated as follows:

$$\sum_{i=1}^{15}\sum_{j=1}^{15}\left(\Pr(\Delta_1 \xrightarrow{E_0^{3r}} \Delta_2^i)\right)^2.\left(\Pr(\nabla_3^j \xrightarrow{E_1^{4r}} \nabla_4)\right)^2.R_{i,j}^{7r} = 2^{-60.96}.$$

Let p_{bm}^{14r} is the probability of the above 14-round boomerang distinguisher. The above relation proves that $p_{bm}^{14r} \geq 2^{-60.96}$. However, using the 4-dimensional matrix $R_{i,j,k,l}^{7r}$, we can obtain a more accurate bound for p_{bm}^{14r} as follows:

$$\sum_{i=1}^{15}\sum_{j=1}^{15}\sum_{k=1}^{15}\sum_{l=1}^{15} \Pr(\Delta_1 \xrightarrow{E_0^{3r}} \Delta_2^i).\Pr(\Delta_1 \xrightarrow{E_0^{3r}} \Delta_2^j)$$
$$\Pr(\nabla_3^k \xrightarrow{E_1^{4r}} \nabla_4).\Pr(\nabla_3^l \xrightarrow{E_1^{4r}} \nabla_4)$$
$$.R_{i,j,k,l}^{7r} = 2^{-60.33}.$$

5.13 A Dedicated Boomerang Distinguisher for 14 Rounds of `CRAFT`

In this section we provide a dedicated boomerang distinguisher for 14 rounds of `CRAFT` with a different active-cell pattern for the middle part. The specification of this distinguisher is described in Table 4. The active-cell pattern in three different parts of this distinguisher, i.e., E_0, E_1 and E_m have been also illustrated in Figure 13. As it can be seen, a lower bound for probability of this boomerang distinguisher is $2^{-58.30}$ which is much larger than our previous boomerang distinguisher for 14 rounds of `CRAFT`. It can be seen that, considering the clustering effect as we did before, one can obtain a more accurate bound for the probability of this distinguisher as well.

Table 4: Specification of a dedicated boomerang distinguisher for 14 rounds of `CRAFT`

$r_0 = 4, r_m = 7, r_1 = 3, p = 2^{-9.56},\ q = 2^{-9.54},\ r = 2^{-20.10},\ p^2.q^2.r = 2^{-58.30}$
$\Delta X_0 =$ `00AA 00A0 A00A 00A0` $\Delta X_4 =$ `0000 0000 A000 0000`
$\nabla X_{14} =$ `00A0 0000 0AA0 A000` $\nabla X_{11} =$ `0000 A000 0000 0000`

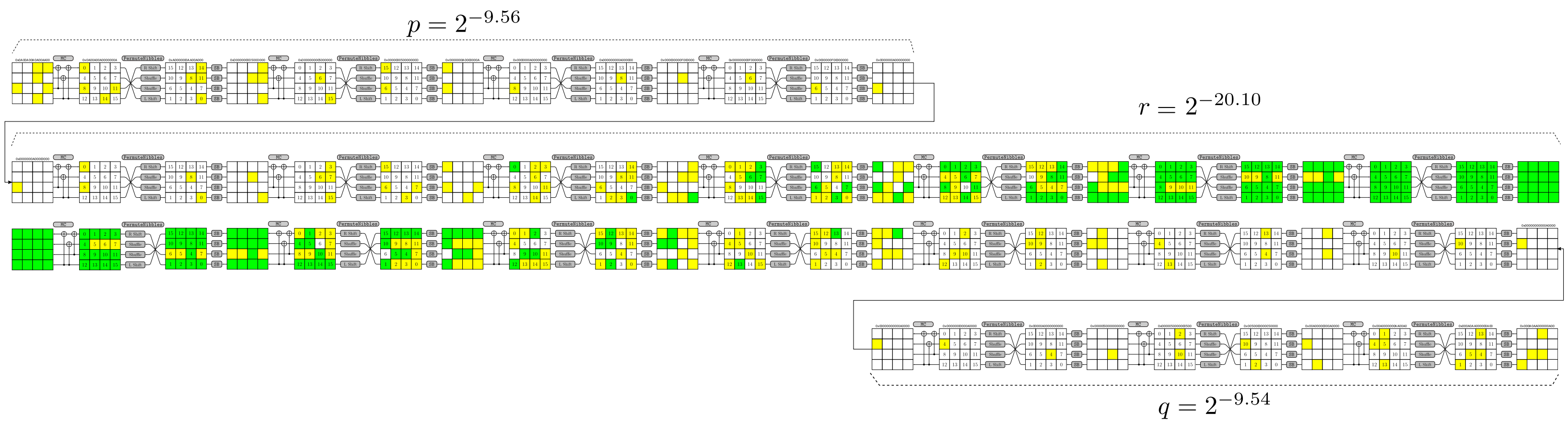

Figure 13: A dedicated boomerang distinguisher for 14 rounds of `CRAFT`

Table 5: Notations for SKINNY.

TKi	represents the i-th round tweakey. This is equal to the result of exclusive-ORing the first and the second rows of tk_1^i and tk_2^i and $TKi[j]$ represents the j-th cell $(0 \le j \le 15)$ of TKi.
X_i	represents the internal state before SC in round i and $X_i[j]$ represents the j-th cell $(0 \le j \le 15)$ of X_i.
Y_i	represents the internal state before ART in round i and $Y_i[j]$ represents the j-th cell $(0 \le j \le 15)$ of Y_i.
Z_i	represents the internal state before SR in round i and $Z_i[j]$ represents the j-th cell $(0 \le j \le 15)$ of Z_i.
W_i	represents the internal state before MC in round i and $W_i[j]$ represents the j-th cell $(0 \le j \le 15)$ of W_i.
ΔX_i	represents the forward difference at state X_i
∇X_i	represents the backward difference at state X_i
$\mathtt{Y}$	Hexadecimal representation of arbitrary value $Y \in \mathbb{F}_2^4$, where we are using typewriter style.

5.14 Boomerang Distinguisher in Related-Tweak Model

We have investigated the boomerang behavior of CRAFT in related-tweak mode also. However, the outcome was not promising in terms of number of rounds compared to the current best differential distinguishers. It shows that boomerang attack is less efficient for CRFAT in related-tweak model. It worth noting, we expected this behavior and it is not surprising. More precisely, although, in the related-tweak model, it may be possible to reach better probability for E_0 and E_1 parts of a boomerang distinguisher, however, given that the differences that are introduced by the tweak part in the middle part of the distinguisher propagate very fast to whole of the state, the existence of difference in the tweak part reduces the number of rounds that are covered by the middle part. In addition the clustering effect in related-tweak mode, is weaker in compare with the single-tweak mode for CRAFT. Hence, the outcome was not promising in this model, compared to the previous related-tweak differential cryptanalysis.

6 Boomerang Distinguishers for Reduced Rounds SKINNY

In this section, we first briefly review the specification of SKINNY, and it's previous boomerang distinguishers, and then present improved boomerang distinguishers for different variants of SKINNY.

6.1 Notations

Table 5 briefly describes the notations we use through this section of paper.

6.2 A Brief Description of SKINNY

SKINNY is a family of lightweight tweakable block ciphers using SPN strcuture, and following the tweakey framework from [JNP14], in its design. Each family member of SKINNY is represented by SKINNY-n-t, where n represents the block size ($n \in \{64, 128\}$) and t represents the tweakey size ($t \in \{n, 2n, 3n\}$). In other words, the six main variants of SKINNY are SKINNY-64-64, SKINNY-64-128, SKINNY-64-192, SKINNY-128-128, SKINNY-128-256, and SKINNY-128-384 with 32, $36, 40, 40, 48$, and 56 rounds, respectively.

The internal state of SKINNY is considered as a 4×4 matrix, where each entry is a nibble in the $n = 64$ case, or a byte in the $n = 128$ case. In both cases, the internal state $IS = I_0 \| I_1 \| \cdots \| I_{14} \| I_{15}$ is arranged row-wise according to the following order:

$$IS = \begin{pmatrix} I_0 & I_1 & I_2 & I_3 \\ I_4 & I_5 & I_6 & I_7 \\ I_8 & I_9 & I_{10} & I_{11} \\ I_{12} & I_{13} & I_{14} & I_{15} \end{pmatrix}$$

where $I_i \in \mathbb{F}_2^4$ (or $\mathbb{F}_2^8$). As illustrated in Figure 14, each round of SKINNY, performs five basic operations on the cipher internal state, including SubCells (SC), AddConstants (AC), AddRoundTweakey (ART), ShiftRows (SR), and MixColumns (MC). The first operation which is performed on the internal state in each round is SubCells (SC), in which depending on the block size, a 4-bit Sbox (for 64-bit block size) or a 8-bit Sbox (for 128-bit block size) is applied on each cell of the internal state. The next operation is AddConstant (AC) in which some round-dependent constants are XORed to the first column of the the cipher internal state. Then, in AddRoundTweakey (ART), as represented in Figure 14, the first and second rows of the tweakey state are XORed to the corresponding rows of the internal state. In ShiftRows (SR) layer, each cell in row j is rotated to the right by j cells. In MixColumns (MC) layer, each column of the internal state is multiplied by the following matrix:

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

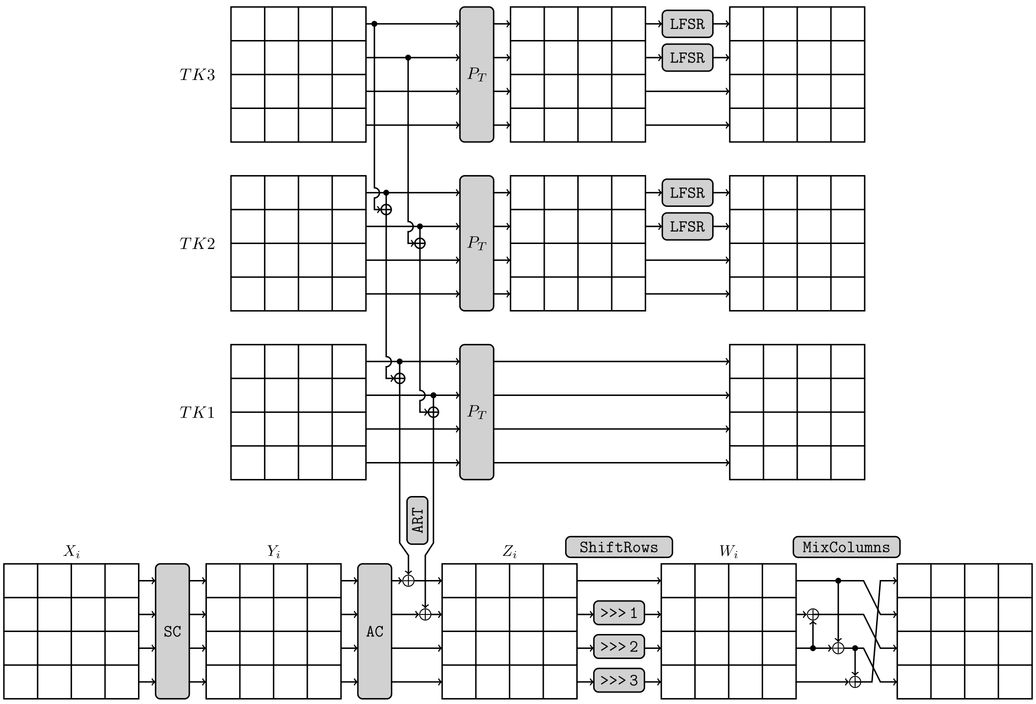

Figure 14: The round function and tweakey schedule of SKINNY

The tweakey state of SKINNY can contain both key and tweak materials and it is arranged as a collection of z 4×4 array of nibbles (for 64-bit block size) or bytes (for 128-bit block size), where $z = t/n$. The tweakey state arrays are denoted by $TK1$ when $z = 1$, $TK1$ and $TK2$ when $z = 2$, and finally $TK1, TK2$, and $TK3$ when $z = 3$. Let $TKi[j]$ represents the j'th cell of TKi where $i \in \{1, 2, 3\}$. The tweakey schedule of SKINNY is a linear algorithm in which, firstly, a cell-wised permutation P_T is applied on each tweakey state, i.e. $TKi[j] \leftarrow TKi[P_T[j]]$ for all $i \in \{1, 2, 3\}$ and $0 \leq j \leq 15$ where $P_T = [9, 15, 8, 13, 10, 14, 12, 11, 0, 1, 2, 3, 4, 5, 6, 7]$. Then, every cell of the first and second rows of $TK2$ (where $TK2$ is used) and $TK3$ (when $TK3$ is used) are individually updated with an LFSR. For complete details of the round function, and tweakey scheduling algorithm, one can refer to [BJK+16b].

In [LGS17] Liu *et al.* provided related tweakey rectangle attacks against SKINNY. In [CHP+18], Cid *et al.* introduced the BCT and applied it to accurately evaluate the probability of generating the right quartet for two middle rounds of boomerang distinguishers proposed in [LGS17]. At FSE 2019, Song *et al.* proposed a generalized framework to identify the actual boundaries of E_m which contains dependency of the two differential paths of boomerang distinguisher and systematically evaluate the probability of E_m with any number of rounds. Using their method, Song *et al.* proved that the probability of four boomerang distinguishers proposed in [LGS17] are much higher than previously evaluated. To the best of our knowledge, Song et. als' results in [SQH19] are the best published results for boomerang distinguishers of SKINNY so far. In this section we introduce new boomerang distinguishers for SKINNY-64-128, SKINNY-64-192, SKINNY-128-256 and SKINNY-128-284 which are better than the best previous boomerang distinguishers of SKINNY by a far distance.

Table 6: Summary of our results in comparison to the best published results in [SQH19] for boomerang distinguishers of SKINNY. The probability highlighted in red has been verified experimentally.

SKINNY version	n (block size)	#Rounds	probability	Reference
SKINNY-n-$2n$	64	17	$2^{-29.78}$	[SQH19]
	64	17	$\mathbf{2^{-26.54}}$ (II)	Subsection 6.4
	64	18	$\mathbf{2^{-37.9}}$ (II)	
	64	19	$\mathbf{2^{-51.08}}$ (II)	
	128	18	$2^{-77.83}$	[SQH19]
	128	18	$\mathbf{2^{-40.77}}$(II)	Subsection 6.4
	128	19	$\mathbf{2^{-58.33}}$(II)	
	128	20	$\mathbf{2^{-85.31}}$(I)	Subsection 6.3
	128	21	$\mathbf{2^{-114.07}}$(II)	Subsection 6.4
SKINNY-n-$3n$	64	22	$2^{-42.98}$	[SQH19]
	64	22	$\mathbf{2^{-40.67}}$(I)	Subsection 6.3
	64	23	$\mathbf{2^{-55.85}}$(I)	
	128	22	$2^{-48.30}$	[SQH19]
	128	22	$\mathbf{2^{-40.57}}$ (I)	Subsection 6.3
	128	23	$\mathbf{2^{-56.47}}$ (I)	
	128	24	$\mathbf{2^{-87.39}}$ (I)	
	128	25	$\mathbf{2^{-116.59}}$ (I)	

Applying our search algorithm for boomerang distinguishers, we could dramatically improve the best previous boomerang distinguishers of SKINNY-n-$2n$ and SKINNY-n-$3n$. Table 6 summarizes and compares our best results with the best previous results. We also discovered an interesting property using which we could find boomerang distinguishers for different variants of SKINNY having a common active-cell position in the middle part. In other words, we can find a suitable boomerang distinguisher covering 18 rounds of SKINNY-64-128 at first. Then, considering the active-cell positions for the middle part of the discovered boomerang distinguisher for SKINNY-64-128, we look for the best actual upper and lower differential paths in other variants of SKINNY including SKINNY-64-192, SKINNY-128-256 and SKINNY-128-384 satisfying the given active-cell position, instead of applying our search algorithm for other variants of SKINNY separately. This speeds up the searching part, since one has not to construct and solve word-oriented MILP models for each single variants of SKINNY to find a boomerang distinguisher, especially when constructing and solving the word-oriented model is a time consuming computation. In the reminder of this section we introduce two different boomerang distinguishers for both SKINNY-n-$2n$ and SKINNY-n-$3n$ ($n \in \{64, 128\}$).

6.3 Boomerang Distinguisher I for SKINNY

The middle part of boomerang distinguisher I have a common active-cell pattern for all versions of SKINNY-n-$2n$ and SKINNY-n-$3n$ when $n \in \{64, 128\}$, which is illustrated in Figure 15. Tables 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 and 19 briefly describe the specification of boomerang distinguisher I for SKINNY-n-$2n$ and SKINNY-n-$3n$ for $n \in \{64, 128\}$. The dependency graph between upper and lower differential paths in middle part of boomerang distinguisher I, has also been illustrated in Figure 15 which helps us to simply extract a formula to evaluate the probability of middle part using the BCT framework. As it can be seen in Figure 15, the dependency can be modeled using the new tools DBCT, DBT* and BDT*.

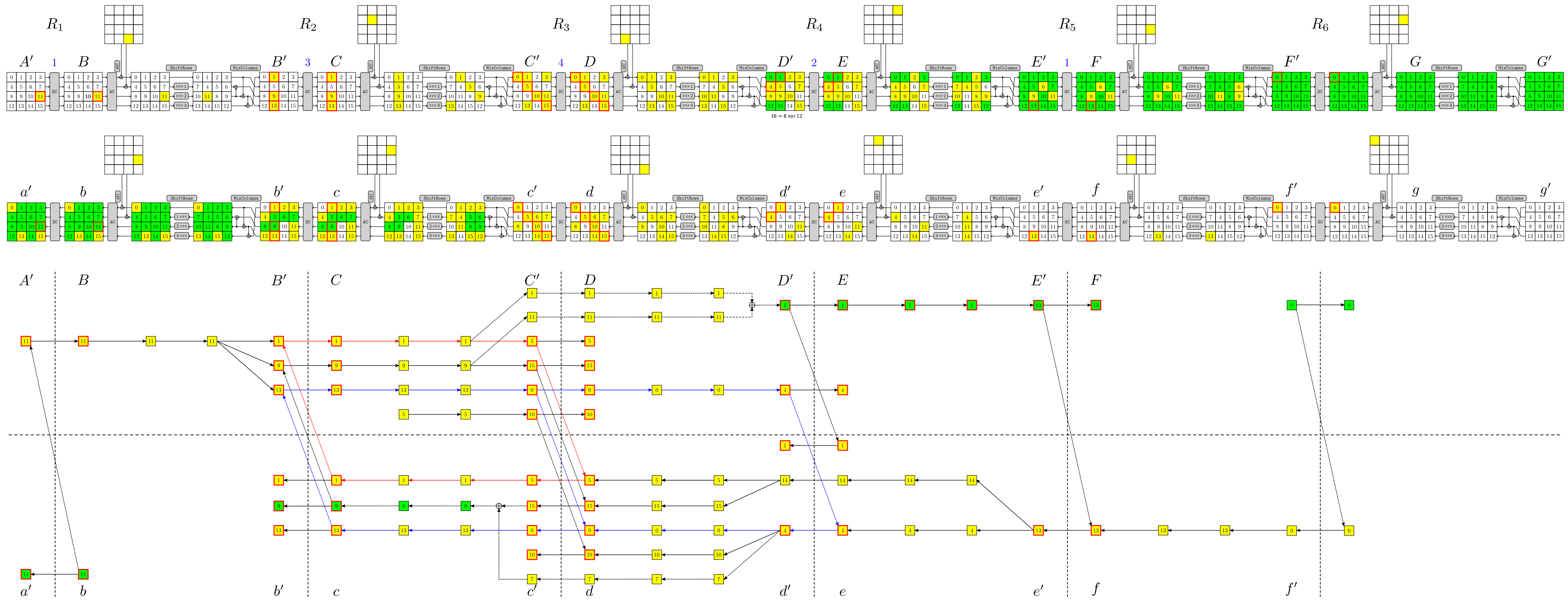

Figure 15: The middle part of boomerang distinguisher I for `SKINNY`

Table 7: Specification of boomerang distinguisher I for 17 rounds of SKINNY-64-128.

$r_0 = 6, r_m = 6, r_1 = 5, p = 2^{-2.41},\ q = 2^{-2},\ r = 2^{-19.10},\ p^2.q^2.r = 2^{-27.92}$
$\Delta X_0 =$ 0000000000000008
$\Delta TK1 =$ 00000000C0000000 $\Delta TK2 =$ 00000000F0000000
$\nabla X_{17} =$ 0009000000090009
$\nabla TK1 =$ 0000000000004000 $\nabla TK2 =$ 0000000000007000

Given that the probability of boomerang distinguisher I for SKINNY-64-128 is large enough, one can easily verifies it on a desktop. It can be seen that the values obtained from the formula $p^2.q^2.r$ and from the experiment are too close. Hence it confirms that the dependency doesn't exist out of the 6 rounds middle part where we considered as E_m (Figure 15).

Table 8: Specification of boomerang distinguisher I for 18 rounds of SKINNY-64-128

$r_0 = 6, r_m = 6, r_1 = 6, p = 2^{-2.41},\ q = 2^{-8},\ r = 2^{-19.10},\ p^2.q^2.r = 2^{-39.92}$
$\Delta X_0 =$ 0000000000000008
$\Delta TK1 =$ 00000000C0000000 $\Delta TK2 =$ 00000000F0000000
$\nabla X_{18} =$ 0454000404070404
$\nabla TK1 =$ 0000000000004000 $\nabla TK2 =$ 0000000000007000

Table 9: Specification of boomerang distinguisher I for 19 rounds of SKINNY-64-128

$r_0 = 7, r_m = 6, r_1 = 6, p = 2^{-9},\ q = 2^{-8},\ r = 2^{-19.10},\ p^2.q^2.r = 2^{-53.10}$
$\Delta X_0 =$ 2000001001001000 $\Delta TK1 =$ C000000000000000 $\Delta TK2 =$ F000000000000000
$\nabla X_{19} =$ 0454000404070404
$\nabla TK1 =$ 0000400000000000 $\nabla TK2 =$ 0000700000000000

Table 10: Specification of boomerang distinguisher I for 18 rounds of SKINNY-128-256

$r_0 = 6, r_m = 6, r_1 = 6, p = 2^{-3.68},\ q = 2^{-8},\ r = 2^{-19.15},\ p^2.q^2.r = 2^{-42.51}$
$\Delta X_0 =$ 00000000000000000000000000000080
$\Delta TK1 =$ 0000000000000000f000000000000000 $\Delta TK2 =$ 0000000000000000fc00000000000000
$\nabla X_{18} =$ 00202020000000200020000c00200020
$\nabla TK1 =$ 000000000000000000000000fc000000 $\nabla TK2 =$ 00000000000000000000000067000000

Table 11: Specification of boomerang distinguisher I for 19 rounds of SKINNY-128-256

$r_0 = 7, r_m = 6, r_1 = 6, p = 2^{-11.68},\ q = 2^{-8},\ r = 2^{-19.15},\ p^2.q^2.r = 2^{-58.51}$
$\Delta X_0 =$ 02000000000002000002000020000000
$\Delta TK1 =$ f0000000000000000000000000000000 $\Delta TK2 =$ fc000000000000000000000000000000
$\nabla X_{19} =$ 00202020000000200020000c00200020
$\nabla TK1 =$ 00000000fc0000000000000000000000 $\nabla TK2 =$ 00000000670000000000000000000000

Table 12: Specification of boomerang distinguisher I for 20 rounds of SKINNY-128-256

$r_0 = 8, r_m = 6, r_1 = 6, p = 2^{-25.08},\ q = 2^{-8},\ r = 2^{-19.15},\ p^2.q^2.r = 2^{-85.31}$
$\Delta X_0 =$ 00000100010100010100010000d50000
$\Delta TK1 =$ 000000000000000000f0000000000000
$\Delta TK2 =$ 000000000000000000fe000000000000
$\nabla X_{20} =$ 00202020000000200020000c00200020
$\nabla TK1 =$ 00000000000000000000fc0000000000
$\nabla TK2 =$ 0000000000000000000033000000000 0

Table 13: Specification of boomerang distinguisher I for 21 rounds of SKINNY-128-256

$r_0 = 8, r_m = 6, r_1 = 7, p = 2^{-25.08},\ q = 2^{-23.56},\ r = 2^{-19.15},\ p^2.q^2.r = 2^{-116.43}$
$\Delta X_0 =$ 00000100010100010100010000d50000
$\Delta TK1 =$ 000000000000000000f0000000000000
$\Delta TK2 =$ 000000000000000000fe000000000000
$\nabla X_{21} =$ 80910000008080808011008000918000
$\nabla TK1 =$ 00000000000000000000fc0000000000
$\nabla TK2 =$ 00000000000000000000330000000000

Table 14: Specification of boomerang distinguisher I for 22 rounds of SKINNY-64-192

$r_0 = 8, r_m = 6, r_1 = 8, p = 2^{-2.41},\ q = 2^{-7},\ r = 2^{-21.85},\ p^2.q^2.r = 2^{-40.67}$		
$\Delta X_0 =$ 0000000000000100		
$\Delta TK1 =$ 0000000007000000	$\Delta TK2 =$ 0000000003000000	$\Delta TK3 =$ 000000000B000000
$\nabla X_{22} =$ 5605060000450605		
$\nabla TK1 =$ 0000000000200000	$\nabla TK2 =$ 0000000000300000	$\nabla TK3 =$ 0000000000D00000

Table 15: Specification of boomerang distinguisher I for 23 rounds of SKINNY-64-192

$r_0 = 9, r_m = 6, r_1 = 8, p = 2^{-10},\ q = 2^{-7},\ r = 2^{-21.85},\ p^2.q^2.r = 2^{-55.85}$		
$\Delta X_0 =$ 0900200000020020		
$\Delta TK1 =$ 0700000000000000	$\Delta TK2 =$ 0300000000000000	$\Delta TK3 =$ 0B00000000000000
$\nabla X_{23} =$ 5605060000450605		
$\nabla TK1 =$ 0020000000000000	$\nabla TK2 =$ 0030000000000000	$\nabla TK3 =$ 00D0000000000000

Table 16: Specification of boomerang distinguisher I for 22 rounds of SKINNY-128-384

$r_0 = 8, r_m = 6, r_1 = 8, p = 2^{-3},\ q = 2^{-7},\ r = 2^{-20.57},\ p^2.q^2.r = 2^{-40.57}$
$\Delta X_0 =$ 00000000000000000000000000080000
$\Delta TK1 =$ 00000000000000000002a00000000000
$\Delta TK2 =$ 00000000000000000007900000000000
$\Delta TK3 =$ 00000000000000000003300000000000
$\nabla X_{22} =$ 10100010001000000000071000100010
$\nabla TK1 =$ 00000000000000000000540000000000
$\nabla TK2 =$ 00000000000000000000f00000000000
$\nabla TK3 =$ 00000000000000000000f80000000000

6.4 Boomerang Distinguisher II for SKINNY

Figure 16 illustrates the active-cell pattern in middle part of boomerang distinguisher II which is the same for all variants of SKINNY-n-$2n$ and SKINNY-n-$3n$ when $n \in \{64, 128\}$.

Table 17: Specification of boomerang distinguisher I for 23 rounds of SKINNY-128-384

$r_0 = 9, r_m = 6, r_1 = 8, p = 2^{-10.95},\ q = 2^{-7},\ r = 2^{-20.57},\ p^2.q^2.r = 2^{-56.47}$
$\Delta X_0 =$ 00110000020000000000000200000200
$\Delta TK1 =$ 002a0000000000000000000000000000
$\Delta TK2 =$ 00790000000000000000000000000000
$\Delta TK3 =$ 00330000000000000000000000000000
$\nabla X_{23} =$ 10100010001000000000071000100010
$\nabla TK1 =$ 00005400000000000000000000000000
$\nabla TK2 =$ 00000f00000000000000000000000000
$\nabla TK3 =$ 0000f800000000000000000000000000

Table 18: Specification of boomerang distinguisher I for 24 rounds of SKINNY-128-384

$r_0 = 10, r_m = 6, r_1 = 8, p = 2^{-26.41},\ q = 2^{-7},\ r = 2^{-20.57},\ p^2.q^2.r = 2^{-87.39}$
$\Delta X_0 =$ 80000000008080808000800000000c80
$\Delta TK1 =$ 0000000000000000000000000000002a
$\Delta TK2 =$ 0000000000000000000000000000003c
$\Delta TK3 =$ 00000000000000000000000000000067
$\nabla X_{24} =$ 10100010001000000000071000100010
$\nabla TK1 =$ 00000000000000005400000000000000
$\nabla TK2 =$ 00000000000000008700000000000000
$\nabla TK3 =$ 0000000000000000f000000000000000

Table 19: Specification of boomerang distinguisher I for 25 rounds of SKINNY-128-384

$r_0 = 10, r_m = 6, r_1 = 9, p = 2^{-26.41},\ q = 2^{-21.60},\ r = 2^{-20.57},\ p^2.q^2.r = 2^{-116.59}$
$\Delta X_0 =$ 80000000008080808000800000000c80
$\Delta TK1 =$ 0000000000000000000000000000002a
$\Delta TK2 =$ 0000000000000000000000000000003c
$\Delta TK3 =$ 00000000000000000000000000000067
$\nabla X_{25} =$ 08104040505000400840400058100040
$\nabla TK1 =$ 00000000000000005400000000000000
$\nabla TK2 =$ 00000000000000008700000000000000
$\nabla TK3 =$ 0000000000000000f000000000000000

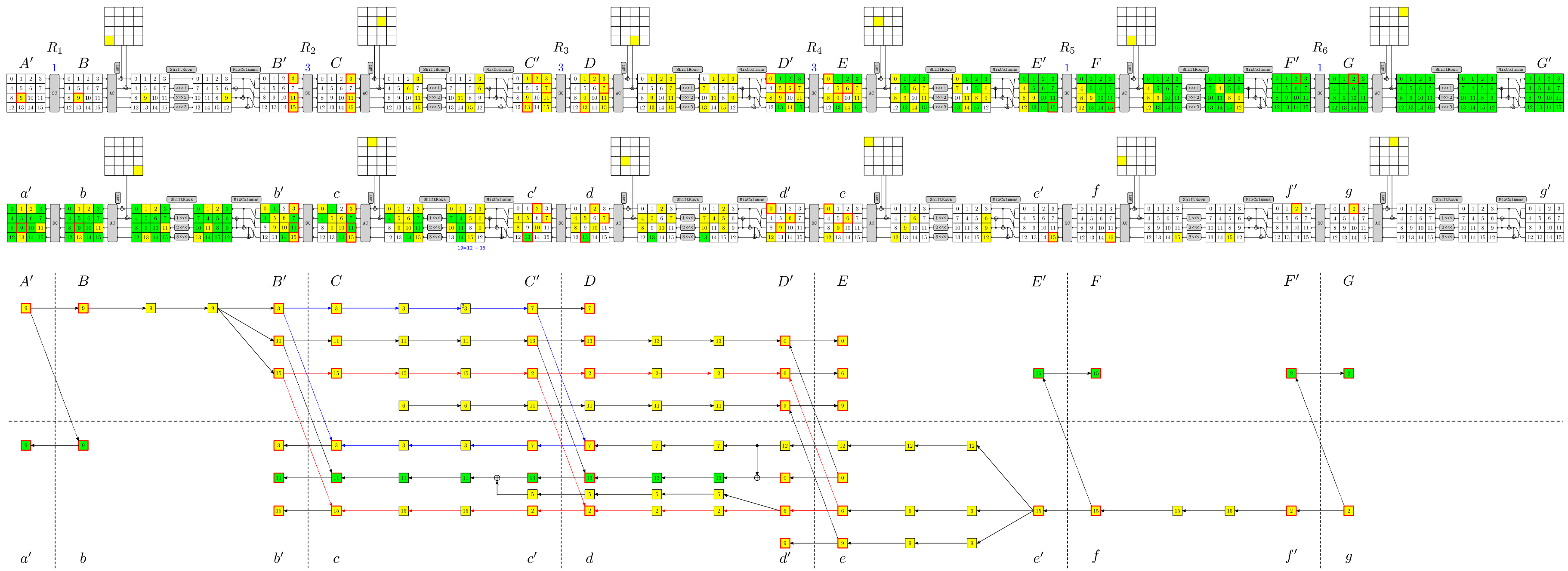

Figure 16: The middle part of boomerang distinguisher II for `SKINNY`

Tables 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30 and 31 briefly describe the specification of boomerang distinguisher II for SKINNY-n-$2n$ and SKINNY-n-$3n$ for $n \in \{64, 128\}$.

Table 20: Specification of boomerang distinguisher II for 17 rounds of SKINNY-64-128

$r_0 = 6, r_m = 6, r_1 = 5, p = 2^{-2.41},\ q = 2^{-2},\ r = 2^{-17.72},\ p^2.q^2.r = 2^{-26.54}$	
$\Delta X_0 =$ 0000000000000800	
$\Delta TK1 =$ 000000000C000000	$\Delta TK2 =$ 000000000F000000
$\nabla X_{17} =$ 0200000002000200	
$\nabla TK1 =$ 0000000000000040	$\nabla TK2 =$ 0000000000000070

As it can be seen in Table 20 the probability of boomerang distinguisher II for full 17-round of SKINNY-64-128 is $2^{26.54}$ which can be practically verified on a desktop. One can see that the experimental values for full 17-round boomerang distinguisher of SKINNY-64-128 is almost the same as the value obtained form the formula $p^2.q^2.r$. This observation also confirms that the dependency doesn't exist out of 6-round middle part where we have considered as E_m (Figure 16).

Table 21: Specification of boomerang distinguisher II for 18 rounds of SKINNY-64-128

$r_0 = 6, r_m = 6, r_1 = 6, p = 2^{-2.41},\ q = 2^{-7.68},\ r = 2^{-17.72},\ p^2.q^2.r = 2^{-37.90}$	
$\Delta X_0 =$ 0000000000000800	
$\Delta TK1 =$ 000000000C000000	$\Delta TK2 =$ 000000000F000000
$\nabla X_{18} =$ 3101010000710101	
$\nabla TK1 =$ 0000000000000040	$\nabla TK2 =$ 0000000000000070

Table 22: Specification of boomerang distinguisher II for 19 rounds of SKINNY-64-128

$r_0 = 7, r_m = 6, r_1 = 6, p = 2^{-9},\ q = 2^{-7.68},\ r = 2^{-17.72},\ p^2.q^2.r = 2^{-51.08}$	
$\Delta X_0 =$ 0200100000010010	
$\Delta TK1 =$ 0C00000000000000	$\Delta TK2 =$ 0F00000000000000
$\nabla X_{19} =$ 3101010000710101	
$\nabla TK1 =$ 0000004000000000	$\nabla TK2 =$ 0000007000000000

Table 23: Specification of boomerang distinguisher II for 18 rounds of SKINNY-128-256

$r_0 = 6, r_m = 6, r_1 = 6, p = 2^{-3},\ q = 2^{-7.29},\ r = 2^{-20.19},\ p^2.q^2.r = 2^{-40.77}$
$\Delta X_0 =$ 00000000000000000000000000200000
$\Delta TK1 =$ 00000000000000000002000000000000 $\Delta TK2 =$ 00000000000000000008000000000000
$\nabla X_{18} =$ 40400040004000000000184000400040
$\nabla TK1 =$ 0000000000000000000000000000f800 $\nabla TK2 =$ 0000000000000000000000000000cf00

7 Conclusion

In this paper, we extended the recent advances in boomerang cryptanalysis of block ciphers by introducing new concepts entitled *Double Boomerang Connectivity Table* (DBCT) (which is an extension to *Boomerang Connectivity Table* (BCT)) and BDT* and DBT*. We also applied a more advances method to search for boomerang distinguishers. We employed this technique and provided the first security analysis of CRAFT against the boomerang attack

Table 24: Specification of boomerang distinguisher II for 19 rounds of SKINNY-128-256

$r_0 = 7, r_m = 6, r_1 = 6, p = 2^{-11.78},\ q = 2^{-7.29},\ r = 2^{-20.19},\ p^2.q^2.r = 2^{-58.33}$
$\Delta X_0 =$ 00200000010000000000000100000100
$\Delta TK1 =$ 00020000000000000000000000000000 $\Delta TK2 =$ 00800000000000000000000000000000
$\nabla X_{19} =$ 40400040004000000000184000400040
$\nabla TK1 =$ 000000000000f8000000000000000000 $\nabla TK2 =$ 000000000000cf000000000000000000

Table 25: Specification of boomerang distinguisher II for 20 rounds of SKINNY-128-256

$r_0 = 8, r_m = 6, r_1 = 6, p = 2^{-27.32},\ q = 2^{-7.29},\ r = 2^{-20.19},\ p^2.q^2.r = 2^{-89.41}$
$\Delta X_0 =$ 04000000000404040400040000000104
$\Delta TK1 =$ 00000000000000000000000000000002 $\Delta TK2 =$ 00000000000000000000000000000040
$\nabla X_{20} =$ 40400040004000000000184000400040
$\nabla TK1 =$ 000000000000000000000000f8000000 $\nabla TK2 =$ 00000000000000000000000067000000

Table 26: Specification of boomerang distinguisher II for 21 rounds of SKINNY-128-256

$r_0 = 8, r_m = 6, r_1 = 7, p = 2^{-27.32},\ q = 2^{-19.62},\ r = 2^{-20.19},\ p^2.q^2.r = 2^{-114.07}$
$\Delta X_0 =$ 04000000000404040400040000000104
$\Delta TK1 =$ 00000000000000000000000000000002 $\Delta TK2 =$ 00000000000000000000000000000040
$\nabla X_{21} =$ 40000404040400044004040044000004
$\nabla TK1 =$ 000000000000000000000000f8000000 $\nabla TK2 =$ 00000000000000000000000067000000

Table 27: Specification of boomerang distinguisher II for 22 rounds of SKINNY-64-192

$r_0 = 8, r_m = 6, r_1 = 8, p = 2^{-3},\ q = 2^{-7},\ r = 2^{-22.15},\ p^2.q^2.r = 2^{-42.15}$
$\Delta X_0 =$ 0000000000000010
$\Delta TK1 =$ 0000000000000007 $\Delta TK2 =$ 0000000000000003 $\Delta TK3 =$ 000000000000000B
$\nabla X_{22} =$ 5052500400505054
$\nabla TK1 =$ 0000000000002000 $\nabla TK2 =$ 0000000000003000 $\nabla TK3 =$ 000000000000D000

Table 28: Specification of boomerang distinguisher II for 23 rounds of SKINNY-64-192

$r_0 = 9, r_m = 6, r_1 = 8, p = 2^{-10.68},\ q = 2^{-7},\ r = 2^{-22.15},\ p^2.q^2.r = 2^{-57.51}$
$\Delta X_0 =$ 0000020320000002
$\Delta TK1 =$ 0000000700000000 $\Delta TK2 =$ 0000000300000000 $\Delta TK3 =$ 0000000B00000000
$\nabla X_{23} =$ 5052500400505054
$\nabla TK1 =$ 0002000000000000 $\nabla TK2 =$ 0003000000000000 $\nabla TK3 =$ 000D000000000000

in single tweak mode, given that the designers also have not reported the security bound against this attack. Our analysis showed that reduced rounds of CRAFT have a strong boomerang effect. For example, we presented a deterministic distinguisher for 6 rounds of the cipher. For other rounds, up to 14 round, we also provided boomerang distinguishers that outperform other previously known distinguishers in single tweak mode, for the same number of rounds. Our distinguishers for rounds larger than 9 rounds were based on an identical middle part, E_m, to simplify the analysis. In addition, we provide a dedicated boomerang distinguisher for 9 rounds of the CRAFT with better probability compared to the

Table 29: Specification of boomerang distinguisher II for 22 rounds of SKINNY-128-384

$r_0 = 8, r_m = 6, r_1 = 8, p = 2^{-4},\ q = 2^{-7.30},\ r = 2^{-23.75},\ p^2.q^2.r = 2^{-46.35}$
$\Delta X_0 =$ 00000000000000000000000000000400
$\Delta TK1 =$ 00000000000000000000000000000040
$\Delta TK2 =$ 000000000000000000000000000000cf
$\Delta TK3 =$ 000000000000000000000000000000fe
$\nabla X_{22} =$ 4000405c4000001c000040004000401c
$\nabla TK1 =$ 00000000000000000000000050000000
$\nabla TK2 =$ 0000000000000000000000003c000000
$\nabla TK3 =$ 000000000000000000000000e0000000

Table 30: Specification of boomerang distinguisher II for 23 rounds of SKINNY-128-384

$r_0 = 9, r_m = 6, r_1 = 8, p = 2^{-13.65},\ q = 2^{-7.30},\ r = 2^{-23.75},\ p^2.q^2.r = 2^{-65.65}$
$\Delta X_0 =$ 00000000002000152000000000000020
$\Delta TK1 =$ 00000000000004000000000000000000
$\Delta TK2 =$ 00000000000000cf0000000000000000
$\Delta TK3 =$ 00000000000000fe0000000000000000
$\nabla X_{23} =$ 4000405c4000001c000040004000401c
$\nabla TK1 =$ 00000000500000000000000000000000
$\nabla TK2 =$ 000000003c0000000000000000000000
$\nabla TK3 =$ 00000000e00000000000000000000000

Table 31: Specification of boomerang distinguisher II for 24 rounds of SKINNY-128-384

$r_0 = 10, r_m = 6, r_1 = 8, p = 2^{-33.56},\ q = 2^{-7.30},\ r = 2^{-23.75},\ p^2.q^2.r = 2^{-105.51}$
$\Delta X_0 =$ 00400014400000400000004014000000
$\Delta TK1 =$ 00000000000000000000004000000000
$\Delta TK2 =$ 00000000000000000000006700000000
$\Delta TK3 =$ 0000000000000000000000fc00000000
$\nabla X_{24} =$ 4000405c4000001c000040004000401c
$\nabla TK1 =$ 00000000000000000000500000000000
$\nabla TK2 =$ 000000000000000000001e0000000000
$\nabla TK3 =$ 00000000000000000000c00000000000

distinguisher based on that E_m. However we didn't prove it theoretically. Hence, it could be considered as an opportunity for future work to provide better boomerang distinguishers for reduced rounds of CRAFT, based on other E_ms. Applying our search algorithm on SKINNY we also considerably improve the best previous boomerang distinguishers of SKINNY-n-$2n$ and SKINNY-n-$3n$.

References

[ALP+19] Elena Andreeva, Virginie Lallemand, Antoon Purnal, Reza Reyhanitabar, Arnab Roy, and Damian Vizár. Forkae v. *Submission to NIST Lightweight Cryptography Project*, 2019.

[BBI+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland,* *New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 411–436. Springer, 2015.

[BC18] Christina Boura and Anne Canteaut. On the Boomerang Uniformity of Cryptographic Sboxes. *IACR Transactions on Symmetric Cryptology*, 2018(3):290–310, Sep. 2018.

[BCG+12] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*, pages 208–225. Springer, 2012.

[BJK+16a] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

[BJK+16b] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

[BJK+20] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. Skinny-aead and skinny-hash. *IACR Transactions on Symmetric Cryptology*, pages 88–131, 2020.

[BK09] Alex Biryukov and Dmitry Khovratovich. Related-Key Cryptanalysis of the Full AES-192 and AES-256. In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, volume 5912 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2009.

[BKL+07] 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, *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007.

[BLMR19] Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh. CRAFT: lightweight tweakable block cipher with efficient protection against DFA attacks. *IACR Trans. Symmetric Cryptol.*, 2019(1):5–45, 2019.

[BPP+17] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT: A small present - towards reaching the limit of lightweight encryption. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pages 321–345. Springer, 2017.

[BSS+15] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK lightweight block ciphers. In *Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, June 7-11, 2015*, pages 175:1–175:6. ACM, 2015.

[CHP+17] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. A Security Analysis of Deoxys and its Internal Tweakable Block Ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(3):73–107, 2017.

[CHP+18] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang Connectivity Table: A New Cryptanalysis Tool. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 683–714. Springer, 2018.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*, pages 393–410. Springer, 2010.

[DKS14] Orr Dunkelman, Nathan Keller, and Adi Shamir. A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. *J. Cryptology*, 27(4):824–849, 2014.

[DR07] Joan Daemen and Vincent Rijmen. Plateau characteristics. *IET Information Security*, 1(1):11–17, 2007.

[EY19] Muhammad ElSheikh and Amr M. Youssef. Related-key differential cryptanalysis of full round CRAFT. In Shivam Bhasin, Avi Mendelson, and Mridul Nandi, editors, *Security, Privacy, and Applied Cryptography Engineering - 9th International Conference, SPACE 2019, Gandhinagar, India, December 3-7, 2019, Proceedings*, volume 11947 of *Lecture Notes in Computer Science*, pages 50–66. Springer, 2019.

[HSN+19] Hosein Hadipour, Sadegh Sadeghi, Majid M. Niknam, Ling Song, and Nasour Bagheri. Comprehensive security analysis of CRAFT. *IACR Trans. Symmetric Cryptol.*, 2019(4):1–28, 2019.

[IKMP20] Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, and Thomas Peyrin. Duel of the titans: The romulus and remus families of lightweight aead algorithms. *IACR Transactions on Symmetric Cryptology*, pages 43–120, 2020.

[ISSK09] Maryam Izadi, Babak Sadeghiyan, Seyed Saeed Sadeghian, and Hossein Arabnezhad Khanooki. MIBS: A new lightweight block cipher. In Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, editors, *Cryptology and Network Security, 8th International Conference, CANS 2009, Kanazawa, Japan, December 12-14, 2009. Proceedings*, volume 5888 of *Lecture Notes in Computer Science*, pages 334–348. Springer, 2009.

[JNP14] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 274–288. Springer, 2014.

[KLPR10] Lars R. Knudsen, Gregor Leander, Axel Poschmann, and Matthew J. B. Robshaw. Printcipher: A block cipher for ic-printing. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings*, volume 6225 of *Lecture Notes in Computer Science*, pages 16–32. Springer, 2010.

[LGS17] Guozhen Liu, Mohona Ghosh, and Ling Song. Security Analysis of SKINNY under Related-Tweakey Settings. *IACR Trans. Symmetric Cryptol.*, 2017(3):37–72, 2017.

[MA19] AmirHossein E. Moghaddam and Zahra Ahmadian. New automatic search method for truncated-differential characteristics: Application to midori, skinny and craft. Cryptology ePrint Archive, Report 2019/126, 2019. https://eprint.iacr.org/2019/126.

[Mur11] Sean Murphy. The Return of the Cryptographic Boomerang. *IEEE Trans. Information Theory*, 57(4):2517–2521, 2011.

[SQH19] Ling Song, Xianrui Qin, and Lei Hu. Boomerang connectivity table revisited. application to SKINNY and AES. *IACR Trans. Symmetric Cryptol.*, 2019(1):118–141, 2019.

[Wag99] David A. Wagner. The Boomerang Attack. In Lars R. Knudsen, editor, *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 1999.

[WP19] Haoyang Wang and Thomas Peyrin. Boomerang switch in multiple rounds. application to AES variants and deoxys. *IACR Trans. Symmetric Cryptol.*, 2019(1):142–169, 2019.

[ZDM+20] Boxin Zhao, Xiaoyang Dong, Willi Meier, Keting Jia, and Gaoli Wang. Generalized related-key rectangle attacks on block ciphers with linear key schedule: applications to skinny and gift. *Designs, Codes and Cryptography*, pages 1–24, 2020.

A $\mathtt{DBCT}^{\vdash}$, and $\mathtt{DBCT}^{\dashv}$ Algorithms

B Probability Matrix of E_m^{7r}

Algorithm 2: Building $\mathtt{DBCT}^{\vdash}$

Input: S-box S

Initialize an empty table $\mathtt{DBCT}^{\vdash}$ with $2^n \times 2^n \times 2^n$ entries;
for $\Delta_1 = 0 \to 2^n - 1$ **do**
    for $\nabla_3 = 0 \to 2^n - 1$ **do**
        for $\Delta_2 = 0 \to 2^n - 1$ **do**
            $num = 0$;
            if $\mathtt{DDT}(\Delta_1, \Delta_2) > 0$ *and* $\mathtt{BCT}(\Delta_2, \nabla_3) > 0$ **then**
                for $\nabla = 0 \to 2^n - 1$ **do**
                    $\mathcal{Y}^{\cap}_{\mathtt{DDT}} = \mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \cap (\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \oplus \nabla)$;
                    if $\mathcal{Y}^{\cap}_{\mathtt{DDT}} \neq \emptyset$ **then**
                        $num \mathrel{+}= \mathtt{DDT}(\Delta_1, \Delta_2) \cdot \mathtt{BDT}(\Delta_2, \nabla_3, \nabla) \cdot \frac{\#\mathcal{Y}^{\cap}_{\mathtt{DDT}}}{\#\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta_2)}$;
                    end
                end
            end
            $\mathtt{DBCT}^{\vdash}(\Delta_1, \Delta_2, \nabla_3) = num$;
        end
    end
end

Algorithm 3: Building $\mathtt{DBCT}^{\dashv}$

Input: S-box S

Initialize an empty table $\mathtt{DBCT}^{\dashv}$ with $2^n \times 2^n \times 2^n$ entries;
for $\Delta_1 = 0 \to 2^n - 1$ **do**
    for $\nabla_3 = 0 \to 2^n - 1$ **do**
        for $\nabla_2 = 0 \to 2^n - 1$ **do**
            $num = 0$;
            if $\mathtt{DDT}(\nabla_2, \nabla_3) > 0$ *and* $\mathtt{BCT}(\Delta_1, \nabla_2) > 0$ **then**
                for $\Delta = 0 \to 2^n - 1$ **do**
                    $\mathcal{X}^{\cap}_{\mathtt{DDT}} = \mathcal{X}_{\mathtt{DDT}}(\nabla_2, \nabla_3) \cap (\mathcal{X}_{\mathtt{DDT}}(\nabla_2, \nabla_3) \oplus \Delta)$;
                    if $\mathcal{X}^{\cap}_{\mathtt{DDT}} \neq \emptyset$ **then**
                        $num \mathrel{+}= \mathtt{DDT}(\nabla_2, \nabla_3) \cdot \mathtt{DBT}(\Delta_1, \Delta, \nabla_2) \cdot \frac{\#\mathcal{X}^{\cap}_{\mathtt{DDT}}}{\#\mathcal{X}_{\mathtt{DDT}}(\nabla_2, \nabla_3)}$;
                    end
                end
            end
            $\mathtt{DBCT}^{\dashv}(\Delta_1, \nabla_2, \nabla_3) = num$;
        end
    end
end

$$
R^{7r} = \begin{pmatrix}
2^{-14.07} & 2^{-13.45} & 2^{-14.38} & 2^{-14.07} & 2^{-13.67} & 2^{-14.35} & 2^{-14.20} & 2^{-14.36} & 2^{-14.07} & 2^{-13.58} & 2^{-14.38} & 2^{-14.07} & 2^{-13.99} & 2^{-14.36} & 2^{-14.01} \\
2^{-13.45} & 2^{-13.42} & 2^{-14.28} & 2^{-13.45} & 2^{-14.07} & 2^{-14.28} & 2^{-13.97} & 2^{-14.24} & 2^{-13.45} & 2^{-13.83} & 2^{-14.28} & 2^{-13.45} & 2^{-14.29} & 2^{-14.28} & 2^{-14.30} \\
2^{-14.38} & 2^{-14.28} & 2^{-14.35} & 2^{-14.35} & 2^{-13.33} & 2^{-14.30} & 2^{-13.53} & 2^{-14.81} & 2^{-14.36} & 2^{-12.68} & 2^{-14.33} & 2^{-14.38} & 2^{-13.31} & 2^{-14.33} & 2^{-13.23} \\
2^{-14.07} & 2^{-13.45} & 2^{-14.35} & 2^{-14.07} & 2^{-13.67} & 2^{-14.38} & 2^{-14.20} & 2^{-14.36} & 2^{-14.07} & 2^{-13.58} & 2^{-14.36} & 2^{-14.07} & 2^{-13.99} & 2^{-14.38} & 2^{-14.01} \\
2^{-13.67} & 2^{-14.07} & 2^{-13.33} & 2^{-13.67} & 2^{-12.05} & 2^{-13.33} & 2^{-12.27} & 2^{-14.27} & 2^{-13.67} & 2^{-11.26} & 2^{-13.33} & 2^{-13.67} & 2^{-11.97} & 2^{-13.33} & 2^{-11.86} \\
2^{-14.35} & 2^{-14.28} & 2^{-14.30} & 2^{-14.38} & 2^{-13.33} & 2^{-14.35} & 2^{-13.53} & 2^{-14.81} & 2^{-14.38} & 2^{-12.68} & 2^{-14.33} & 2^{-14.36} & 2^{-13.31} & 2^{-14.33} & 2^{-13.23} \\
2^{-14.20} & 2^{-13.97} & 2^{-13.53} & 2^{-14.20} & 2^{-12.27} & 2^{-13.53} & 2^{-12.49} & 2^{-14.34} & 2^{-14.20} & 2^{-11.46} & 2^{-13.53} & 2^{-14.20} & 2^{-12.24} & 2^{-13.53} & 2^{-12.07} \\
2^{-14.36} & 2^{-14.24} & 2^{-14.81} & 2^{-14.36} & 2^{-14.27} & 2^{-14.81} & 2^{-14.34} & 2^{-14.97} & 2^{-14.36} & 2^{-13.84} & 2^{-14.81} & 2^{-14.36} & 2^{-14.37} & 2^{-14.81} & 2^{-14.35} \\
2^{-14.07} & 2^{-13.45} & 2^{-14.36} & 2^{-14.07} & 2^{-13.67} & 2^{-14.38} & 2^{-14.20} & 2^{-14.36} & 2^{-14.07} & 2^{-13.58} & 2^{-14.35} & 2^{-14.07} & 2^{-13.99} & 2^{-14.38} & 2^{-14.01} \\
2^{-13.58} & 2^{-13.83} & 2^{-12.68} & 2^{-13.58} & 2^{-11.26} & 2^{-12.68} & 2^{-11.46} & 2^{-13.84} & 2^{-13.58} & \mathbf{2^{-10.39}} & 2^{-12.68} & 2^{-13.58} & 2^{-11.18} & 2^{-12.68} & 2^{-11.03} \\
2^{-14.38} & 2^{-14.28} & 2^{-14.33} & 2^{-14.36} & 2^{-13.33} & 2^{-14.33} & 2^{-13.53} & 2^{-14.81} & 2^{-14.35} & 2^{-12.68} & 2^{-14.30} & 2^{-14.38} & 2^{-13.31} & 2^{-14.35} & 2^{-13.23} \\
2^{-14.07} & 2^{-13.45} & 2^{-14.38} & 2^{-14.07} & 2^{-13.67} & 2^{-14.36} & 2^{-14.20} & 2^{-14.36} & 2^{-14.07} & 2^{-13.58} & 2^{-14.38} & 2^{-14.07} & 2^{-13.99} & 2^{-14.35} & 2^{-14.01} \\
2^{-13.99} & 2^{-14.29} & 2^{-13.31} & 2^{-13.99} & 2^{-11.97} & 2^{-13.31} & 2^{-12.24} & 2^{-14.37} & 2^{-13.99} & 2^{-11.18} & 2^{-13.31} & 2^{-13.99} & 2^{-11.89} & 2^{-13.31} & 2^{-11.78} \\
2^{-14.36} & 2^{-14.28} & 2^{-14.33} & 2^{-14.38} & 2^{-13.33} & 2^{-14.33} & 2^{-13.53} & 2^{-14.81} & 2^{-14.38} & 2^{-12.68} & 2^{-14.35} & 2^{-14.35} & 2^{-13.31} & 2^{-14.30} & 2^{-13.23} \\
2^{-14.01} & 2^{-14.30} & 2^{-13.23} & 2^{-14.01} & 2^{-11.86} & 2^{-13.23} & 2^{-12.07} & 2^{-14.35} & 2^{-14.01} & 2^{-11.03} & 2^{-13.23} & 2^{-14.01} & 2^{-11.78} & 2^{-13.23} & 2^{-11.66}
\end{pmatrix}
$$

$$
R^{7r}_e = \begin{pmatrix}
2^{-13.90} & 2^{-12.99} & 2^{-14.18} & 2^{-13.86} & 2^{-13.48} & 2^{-14.18} & 2^{-13.92} & 2^{-14.04} & 2^{-13.86} & 2^{-13.41} & 2^{-14.25} & 2^{-13.90} & 2^{-13.83} & 2^{-14.18} & 2^{-13.80} \\
2^{-12.98} & 2^{-12.43} & 2^{-13.68} & 2^{-13.01} & 2^{-13.35} & 2^{-13.64} & 2^{-13.42} & 2^{-13.48} & 2^{-13.02} & 2^{-13.21} & 2^{-13.66} & 2^{-12.99} & 2^{-13.60} & 2^{-13.65} & 2^{-13.58} \\
2^{-14.20} & 2^{-13.66} & 2^{-14.26} & 2^{-14.17} & 2^{-13.20} & 2^{-14.21} & 2^{-13.34} & 2^{-14.33} & 2^{-14.17} & 2^{-12.56} & 2^{-14.21} & 2^{-14.24} & 2^{-13.20} & 2^{-14.22} & 2^{-13.06} \\
2^{-13.90} & 2^{-13.00} & 2^{-14.18} & 2^{-13.89} & 2^{-13.49} & 2^{-14.23} & 2^{-13.94} & 2^{-14.06} & 2^{-13.88} & 2^{-13.43} & 2^{-14.19} & 2^{-13.85} & 2^{-13.79} & 2^{-14.20} & 2^{-13.76} \\
2^{-13.49} & 2^{-13.31} & 2^{-13.18} & 2^{-13.50} & 2^{-11.96} & 2^{-13.20} & 2^{-12.06} & 2^{-13.69} & 2^{-13.45} & 2^{-11.10} & 2^{-13.19} & 2^{-13.47} & 2^{-11.84} & 2^{-13.22} & 2^{-11.69} \\
2^{-14.16} & 2^{-13.63} & 2^{-14.17} & 2^{-14.22} & 2^{-13.21} & 2^{-14.24} & 2^{-13.33} & 2^{-14.34} & 2^{-14.19} & 2^{-12.56} & 2^{-14.27} & 2^{-14.17} & 2^{-13.20} & 2^{-14.20} & 2^{-13.06} \\
2^{-13.96} & 2^{-13.40} & 2^{-13.34} & 2^{-13.97} & 2^{-12.04} & 2^{-13.33} & 2^{-12.07} & 2^{-13.81} & 2^{-13.97} & 2^{-11.12} & 2^{-13.33} & 2^{-13.97} & 2^{-11.98} & 2^{-13.34} & 2^{-11.67} \\
2^{-14.07} & 2^{-13.53} & 2^{-14.35} & 2^{-14.03} & 2^{-13.67} & 2^{-14.34} & 2^{-13.76} & 2^{-14.39} & 2^{-14.03} & 2^{-13.22} & 2^{-14.37} & 2^{-14.04} & 2^{-13.80} & 2^{-14.35} & 2^{-13.69} \\
2^{-13.87} & 2^{-12.99} & 2^{-14.17} & 2^{-13.87} & 2^{-13.51} & 2^{-14.22} & 2^{-13.97} & 2^{-14.00} & 2^{-13.93} & 2^{-13.39} & 2^{-14.20} & 2^{-13.85} & 2^{-13.87} & 2^{-14.21} & 2^{-13.79} \\
2^{-13.41} & 2^{-13.24} & 2^{-12.56} & 2^{-13.39} & 2^{-11.11} & 2^{-12.53} & 2^{-11.11} & 2^{-13.22} & 2^{-13.41} & \mathbf{2^{-10.11}} & 2^{-12.58} & 2^{-13.39} & 2^{-11.02} & 2^{-12.55} & 2^{-10.72} \\
2^{-14.23} & 2^{-13.66} & 2^{-14.19} & 2^{-14.14} & 2^{-13.23} & 2^{-14.19} & 2^{-13.32} & 2^{-14.33} & 2^{-14.14} & 2^{-12.58} & 2^{-14.20} & 2^{-14.16} & 2^{-13.23} & 2^{-14.22} & 2^{-13.06} \\
2^{-13.86} & 2^{-12.98} & 2^{-14.21} & 2^{-13.85} & 2^{-13.48} & 2^{-14.17} & 2^{-13.97} & 2^{-14.02} & 2^{-13.86} & 2^{-13.39} & 2^{-14.22} & 2^{-13.87} & 2^{-13.84} & 2^{-14.18} & 2^{-13.81} \\
2^{-13.83} & 2^{-13.61} & 2^{-13.17} & 2^{-13.82} & 2^{-11.87} & 2^{-13.20} & 2^{-11.99} & 2^{-13.78} & 2^{-13.84} & 2^{-11.03} & 2^{-13.18} & 2^{-13.83} & 2^{-11.76} & 2^{-13.21} & 2^{-11.56} \\
2^{-14.18} & 2^{-13.69} & 2^{-14.19} & 2^{-14.19} & 2^{-13.21} & 2^{-14.27} & 2^{-13.31} & 2^{-14.36} & 2^{-14.21} & 2^{-12.53} & 2^{-14.23} & 2^{-14.16} & 2^{-13.23} & 2^{-14.20} & 2^{-13.03} \\
2^{-13.82} & 2^{-13.59} & 2^{-13.08} & 2^{-13.79} & 2^{-11.68} & 2^{-13.07} & 2^{-11.70} & 2^{-13.65} & 2^{-13.78} & 2^{-10.73} & 2^{-13.05} & 2^{-13.78} & 2^{-11.56} & 2^{-13.07} & 2^{-11.32}
\end{pmatrix}
$$

C Relation Between New and The Previous Sbox Tables

$$\mathtt{DBCT}^{\vdash}(\Delta_1, \Delta_2, \nabla_3) = \sum_{\nabla_2} \mathtt{DBT}(\Delta_1, \nabla_2, \Delta_2).\mathtt{BDT}(\Delta_2, \nabla_3, \nabla_2).$$

$$\mathtt{DBCT}^{\dashv}(\Delta_1, \nabla_2, \nabla_3) = \sum_{\Delta_2} \mathtt{DBT}(\Delta_1, \nabla_2, \Delta_2).\mathtt{BDT}(\Delta_2, \nabla_3, \nabla_2).$$

$$\mathtt{DBCT}(\Delta_1, \nabla_3) = \sum_{\Delta_2} \mathtt{DBCT}^{\vdash}(\Delta_1, \Delta_2, \nabla_3) = \sum_{\nabla_2} \mathtt{DBCT}^{\dashv}(\Delta_1, \nabla_2, \nabla_3).$$

$$\mathtt{DBT}^{\star}(\Delta_1, \Delta_1, \nabla_2, \Delta_2) = \mathtt{DBT}(\Delta_1, \nabla_2, \Delta_2).$$

$$\mathtt{BDT}^{\star}(\Delta_1, \nabla_2, \nabla_2, \nabla_1) = \mathtt{BDT}(\Delta_1, \nabla_2, \nabla_1).$$

D Reformulating the Probability Calculation of 7-round Boomerang Distinguisher of CRAFT

In this section we re-evaluate the probability of the 7-round boomerang distinguisher of CRAFT, using the previous boomerang connectivity tables.

$$\begin{aligned}\mathtt{DBT}_{\mathtt{tot}} = &\mathtt{DBT}(A'_5, b_9, B_9).\mathtt{BDT}(B_9, c_5, b_9)\\ &.\mathtt{DBT}(B_9, c_{12}, C_{12}).\mathtt{BDT}(C_{12}, d_1, c_{12})\\ &.\mathtt{DBT}(E'_1, f'_{12}, F_{12}).\mathtt{BDT}(F_{12}, g'_9, f'_{12})\\ &.\mathtt{DBT}(F'_5, g'_9, G_9).\mathtt{BDT}(G_9, h_5, g'_9).\end{aligned}$$

$$\begin{aligned}\Pr_{\text{total}} = &\Pr(d_1 \xleftarrow{2\ \mathtt{DDT}} f'_{12}) \cdot \Pr(c_5 \xleftarrow{3\ \mathtt{DDT}} f'_{12}) \cdot \\ &\Pr(C_{12} \xrightarrow{2\ \mathtt{DDT}} E'_1) \cdot \Pr(C_{12} \xrightarrow{3\ \mathtt{DDT}} F'_5).\end{aligned}$$

$$R^{7r}[A'_5, h_5] = 2^{-8.n}.\sum_{b_9}\sum_{B_9}\sum_{c_5}\sum_{c_{12}}\sum_{C_{12}}\sum_{d_1}\sum_{E'_1}\sum_{f'_{12}}\sum_{F_{12}}\sum_{g'_9}\sum_{F'_5}\sum_{G_9} \mathtt{DBT}_{\mathtt{tot}}.\Pr_{\mathtt{tot}}.$$

In order to reduce the complexity of evaluating the above formula, we can divide the formula to some smaller pieces, and evaluate the smaller parts at first, as follows.

$$\begin{aligned}
M_1(A'_5, B_9, c_5) &= \sum_{b_9} \mathtt{DBT}(A'_5, b_9, B_9).\mathtt{BDT}(B_9, c_5, b_9),\\
M_2(B_9, C_{12}, d_1) &= \sum_{c_{12}} \mathtt{DBT}(B_9, c_{12}, C_{12}).\mathtt{BDT}(C_{12}, d_1, c_{12}),\\
M_3(E'_1, f'_{12}, g'_9) &= \sum_{F_{12}} \mathtt{DBT}(E'_1, f'_{12}, F_{12}).\mathtt{BDT}(F_{12}, g'_9, f'_{12}),\\
M_4(F'_5, g'_9, h_5) &= \sum_{G_9} \mathtt{DBT}(F'_5, g'_9, G_9).\mathtt{BDT}(G_9, h_5, g'_9),\\
M_{12}(A'_5, c_5, C_{12}, d_1) &= \sum_{B_9} M_1(A'_5, B_9, c_5).M_2(B_9, C_{12}, d_1),\\
M_{34}(E'_1, f'_{12}, F'_5, h_5) &= \sum_{g'_9} M_3(E'_1, f'_{12}, g'_9).M_4(F'_5, g'_9, h_5).
\end{aligned}$$

After evaluating the above tables, the probability is obtained according to the following formula:

$$R^{7r}[A'_5, h_5] = 2^{-8.n}.\sum_{c_5}\sum_{C_{12}}\sum_{d_1}\sum_{E'_1}\sum_{f'_{12}}\sum_{F'_5} M_{12}(A'_5, c_5, C_{12}, d_1).M_{34}(E'_1, f'_{12}, F'_5, h_5).\mathtt{Pr_{tot}}.$$

E A More Efficient Formula to Compute $R^{7r}[i, j, k, l]$

A more efficient, and simplified formula, for computing the four dimensional matrix $R^{7r}[i, j, k, l]$, can be obtain as follows.

$$\begin{aligned}
M_1(A_{51}, A_{52}, B_9, c_5) &= \sum_{b_9} \mathtt{DBT}^\star(A_{51}, A_{52}, b_9, B_9).\mathtt{BDT}(B_9, c_5, b_9),\\
M_2(B_9, C_{12}, d_1) &= \sum_{c_{12}} \mathtt{DBT}(B_9, c_{12}, C_{12}).\mathtt{BDT}(C_{12}, d_1, c_{12}),\\
M_3(E'_1, f'_{12}, g'_9) &= \sum_{F_{12}} \mathtt{DBT}(E'_1, f'_{12}, F_{12}).\mathtt{BDT}(F_{12}, g'_9, f'_{12}),\\
M_4(F'_5, g'_9, h_{51}, h_{52}) &= \sum_{G_9} \mathtt{DBT}(F'_5, g'_9, G_9).\mathtt{BDT}^\star(G_9, h_{51}, h_{52}, g'_9),\\
M_{12}(A_{51}, A_{52}, c_5, C_{12}, d_1) &= \sum_{B_9} M_1(A_{51}, A_{52}, B_9, c_5).M_2(B_9, C_{12}, d_1),\\
M_{34}(E'_1, f'_{12}, F'_5, h_{51}, h_{52}) &= \sum_{g'_9} M_3(E'_1, f'_{12}, g'_9).M_4(F'_5, g'_9, h_{51}, h_{52}).
\end{aligned}$$

After constructing the above tables, $R^{7r}[i, j, k, l]$, can be obtained according to the following formula:

$$\begin{aligned}
R^{7r}[i, j, k, l] = 2^{-8.n}.\sum_{c_5}\sum_{C_{12}}\sum_{d_1}\sum_{E'_1}\sum_{f'_{12}}\sum_{F'_5} & M_{12}(A_{51} = i, A_{52} = j, c_5, C_{12}, d_1)\\
& .M_{34}(E'_1, f'_{12}, F'_5, h_{51} = k, h_{52} = l)\\
& .\mathtt{Pr_{tot}},
\end{aligned}$$

where $\mathtt{Pr_{tot}}$, is calculated as follows.

$$\begin{aligned}
\mathtt{Pr}_{\text{total}} = & \Pr(d_1 \xleftarrow{2\ \mathtt{DDT}} f'_{12}) \cdot \Pr(c_5 \xleftarrow{3\ \mathtt{DDT}} f'_{12}) \cdot\\
& \Pr(C_{12} \xrightarrow{2\ \mathtt{DDT}} E'_1) \cdot \Pr(C_{12} \xrightarrow{3\ \mathtt{DDT}} F'_5).
\end{aligned}$$