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 that regard the target cipher E as a composition of 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., $E = E_1 \circ E_m \circ E_0$, 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 accurately evaluate the probabilities of the best SKINNY's boomerang distinguishers. 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 in terms of probability and number of rounds. More precisely, we propose related-tweakey boomerang distinguishers for up to 19, 21, 23, and 25 rounds of SKINNY-64-128, SKINNY-128-256, SKINNY-64-192, and SKINNY-128-384 respectively, which improve the previous boomerang distinguishers of these variants of SKINNY by 1, 2, 1, and 1 round respectively. Based on the improved boomerang distinguishers for SKINNY, we provide related-tweakey rectangle attacks on 23 rounds of SKINNY-64-128, 24 rounds of SKINNY-128-256, 29 rounds of SKINNY-64-192, and 30 rounds of SKINNY-128-384. It worth noting that our improved related-tweakey rectangle attacks on SKINNY-64-192, SKINNY-128-256 and SKINNY-128-384 can be directly applied for the same number of rounds of ForkSkinny-64-192, ForkSkinny-128-256 and ForkSkinny-128-384 respectively. CRAFT is another SKINNY-like tweakable block cipher for which we provide the security analysis against rectangle attack for the first time. As a result, we provide a 14-round boomerang distinguisher for CRAFT in the single-tweak model based on which we propose a single-tweak rectangle attack on 18 rounds of this cipher. Moreover, following the previous research regarding the evaluation of switching in multiple rounds of boomerang distinguishers, we also introduce new tools called *Double Boomerang Connectivity Table* (DBCT), $\mathtt{BDT}^{\dashv}$, and $\mathtt{DBT}^{\vDash}$ to evaluate the boomerang switch through the multiple rounds more accurately.

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

IACR Transactions on Symmetric Cryptology Vol. 0, No.0, pp.1—49, DOI:XXXXXXXX

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 at first, and then using the novel key recovery attack introduced in [ZDM+20], we conduct key recovery attacks, on reduced `SKINNY` under the related-tweakey setting.

`CRAFT` is among the recent tweakable block ciphers, proposed at FSE 2019 by Beierle *et al.*. 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. [GSS+20], is the latest work on the security analysis of `CRAFT` which exploits the special properties of `CRAFT` to provide weak-tweakey truncated differential distinguishers of `CRAFT` in the single-key model, where they introduced a related tweak 15-round differential characteristic with probability of 2^{-54}, which can be extended to 19-round key-recovery attack. However, to the best of our knowledge, there is no publicly reported security evaluation of `CRAFT` against the boomerang attack. Hence, we are motivated to present the first security analysis of this cipher against the boomerang attack.

Our contribution

Applying a heuristic approach to search for boomerang distinguishers, in which we consider the ladder switch effect, we significantly improve the best previous boomerang distinguishers of `SKINNY`-n-$2n$ and `SKINNY`-n-$3n$ [LGS17a, SQH19] for $n \in \{64, 128\}$. For instance, while the best published boomerang distinguisher for 18 rounds of `SKINNY`-128-256 [LGS17a, 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 [LGS17a, 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 $2^{-107.86}$ [LGS17a, SQH19][2], we introduce a new boomerang dsitinguisher for the same number of rounds of SKINNY-128-384 with probability $2^{-87.39}$, which can be extended to provide a boomerang distinguisher for 25 rounds of this variant with probability $2^{-116.59}$. 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 9, summarizes our results for boomerang distinguishers of SKINNY.

To demonstrate the usefulness of our searching strategy for boomerang distinguishers, we also applied it on CRAFT, and provided 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 in single-tweak model, 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 in the single-tweak model is $2^{-49.79}$, we present a single-tweak 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. As another example, while the best previous distinguisher for 9 rounds of the cipher in single-tweak model has the probability of $2^{-40.20}$, the boomerang distinguisher for the same number for rounds has the probability of $2^{-14.76}$. We also introduce a 14-round single-tweak boomerang distinguisher for CRAFT.

Based on the provided boomerang distinguishers, we also mounted related-tweakey rectangle attacks on SKINNY-n-$2n$, and SKINNY-n-$3n$, for $n \in \{64, 128\}$ and CRAFT. As a result, in the term of the number of attacked rounds by key recovery, to the best of our knowledge, we could improve the best previous attacks on SKINNY-64-192, SKINNY-128-256, and SKINNY-128-384 respectively by 2, 1 and 2 rounds, respectively by attacking 29, 24 and 30 rounds of those variants. We also presented the first key recovery attack on 18 rounds of CRAFT in the single-tweak model. Table 1, summarizes our key recovery attacks on SKINNY's variants and CRAFT.

Furthermore, we have introduced some new tools to formulate the dependency between the upper and lower differential trails of boomerang distinguishers, including DBCT, $\texttt{DBCT}^{\vdash}$ and $\texttt{DBCT}^{\dashv}$. We also introduce new variants of DBT and BDT including $\texttt{DBT}^{\vDash}$ and $\texttt{BDT}^{=\!\!|}$ which are useful to consider the clustering effect in boomerang cryptanalysis.

Outline.

The rest of the paper is organized as follows: in Section 2, we present the required preliminaries for boomerang and rectangle attacks. Section 3, is dedicated to introduce new tools for boomerang cryptanalysis, and Section 4, describes our method to search for boomerang distinguishers. In Section 5, after giving a brief description of CRAFT, we propose boomerang distinguisher for up to 14 rounds of CRAFT, where we apply our new tools to model the dependency between the upper and lower differentials over up to 7 rounds of CRAFT. Next, in Section 6, after giving a brief description of SKINNY, we introduce

[1] The best previous boomerang distinguisher for SKINNY-128-256, is an 18-round distinguisher proposed in [LGS17a, 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 [LGS17a, SQH19], which can be extended up to 24 rounds with probability $2^{-107.86}$.

Table 1: Summary of results of the key recovery attacks on the variants of SKINNY and CRAFT.

Scheme	#rounds	Data	Memory	Time	Attack	P_s	Reference
SKINNY-64-128	23	$2^{60.54}$	$2^{60.9}$	$2^{120.7}$	Rectangle	0.977	This
SKINNY-64-192	29	$2^{62.92}$	2^{80}	$2^{181.7}$	Rectangle	0.977	This
SKINNY-128-256	24	$2^{125.21}$	$2^{125.54}$	$2^{209.85}$	Rectangle	0.977	This
SKINNY-128-384	30	$2^{125.29}$	$2^{125.8}$	$2^{361.68}$	Rectangle	0.977	This
CRAFT	18	$2^{60.9}$	2^{84}	$2^{101.7}$	Rectangle	0.977	This
SKINNY-64-128	23	$2^{62.47}$	2^{124}	$2^{125.91}$	Impossible	1	[LGS17a]
SKINNY-64-192	27	$2^{63.5}$	2^{80}	$2^{165.5}$	Rectangle	0.916	[LGS17a]
SKINNY-128-256	23	$2^{124.47}$	2^{248}	$2^{251.47}$	Impossible	1	[LGS17a]
SKINNY-128-384	28	2^{122}	$2^{122.32}$	$2^{315.25}$	Rectangle	0.8315	[ZDM+20]

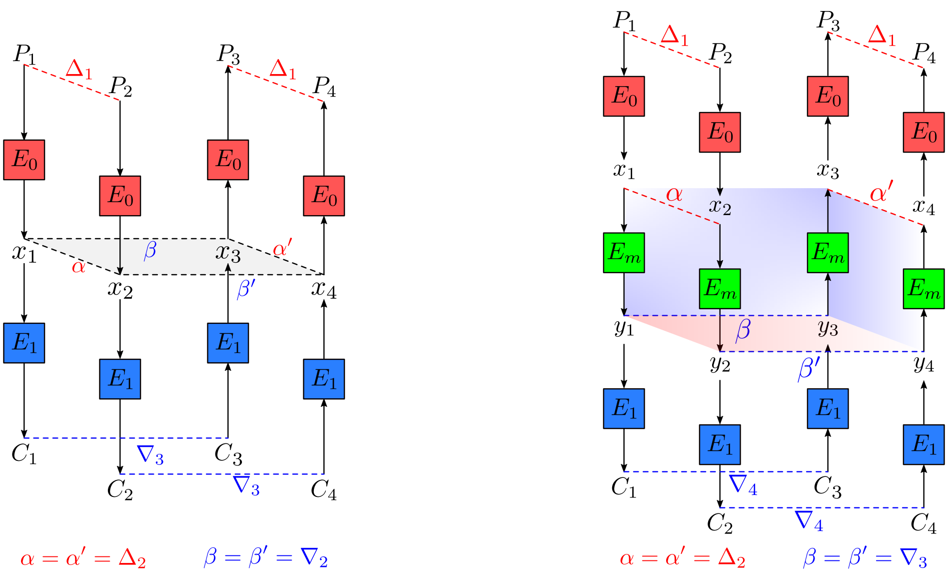

Figure 1: Basic boomerang attack (left) and Sandwich attack (right)

new boomerang distinguishers for SKINNY-n-$2n$ and SKINNY-n-$2n$. Lastly, based on the proposed boomerang distinguishers, we mount key recovery attacks against reduced CRAFT and SKINNY, in Section 7, and conclude the paper in Section 8.

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 Figure 1(left). 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 $C_2 \leftarrow E(P_2)$.
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 $C_1 \oplus C_3 = C_2 \oplus C_4 = \nabla_3$. Under the assumption that the two differentials $\Delta_1 \to \Delta_2$ and $\nabla_2 \to \nabla_3$, in Figure 1(left) are independent, the probability of generating a right quartet is p^2q^2.

In practical cases, the two differentials 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 1(right), the sandwich attack regards E as the composition of three sub-ciphers E_0, E_m and E_1, where the middle part E_m specifically handles the dependency. Let r be the probability of generating a right quartet for E_m in Figure 1(right), when its input and output differences are fixed differences Δ_2, and ∇_3, respectively, i.e.:

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

Furthermore, let $e_\alpha, e_{\alpha'}, e_\beta$, and $e_{\beta'}$, denote the events $x_1 \oplus x_2 = \alpha, x_3 \oplus x_4 = \alpha', y_1 \oplus y_3 = \beta$, and $y_2 \oplus y_4 = \beta'$, respectively. Then, for the probability of the whole boomerang distinguisher in Figure 1(right), we have:

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

where $e_{\alpha,\alpha',\beta,\beta'}$, denote the condition $(x_1 \oplus x_2 = \alpha) \wedge (y_1 \oplus y_3 = \beta) \wedge (y_2 \oplus y_4 = \beta') \wedge (x_3 \oplus x_4 = \alpha')$. Assuming that e_α, e_β, and $e_{\beta'}$, are three independent events, and $p_\alpha = \Pr(\Delta_1 \xrightarrow{E_0} \alpha)$, and $q_\beta = \Pr(\beta \xrightarrow{E_1} \nabla_4)$, for $\alpha, \beta \in \mathbb{F}_2^n$, we have:

$$\Pr\left(P_3 \oplus P_4 = \Delta_1\right) = \sum_{\alpha,\alpha',\beta,\beta'} p_\alpha.p_{\alpha'}. \Pr(e_{\alpha'} | e_\alpha, e_\beta, e_{\beta'}).q_\beta.q_{\beta'} \geq \sum_{\alpha,\beta} p_\alpha^2.r.q_\beta^2 \geq p^2q^2r,$$

where $p = \Pr(\Delta_1 \xrightarrow{E_0} \Delta_2)$, and $q = \Pr(\nabla_3 \xrightarrow{E_1} \nabla_4)$, for fixed differences $\Delta_2, \nabla_3 \in \mathbb{F}_2^n$ in Figure 1(right). Hence, p^2q^2r, 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 2. 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.

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

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

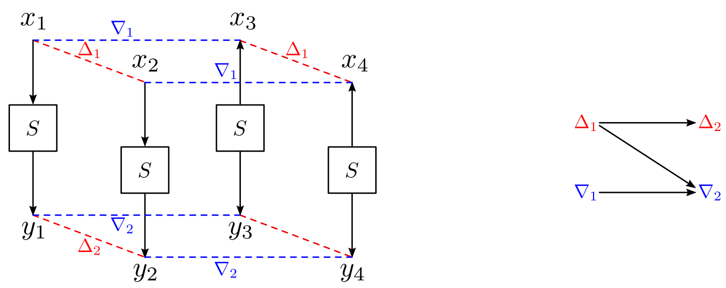

Figure 2: Differences of an S-box on four facets

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 difference boomerang table (DBT) of S is a three-dimensional table defined by

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

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

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

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

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

3 New Tools for Boomerang Cryptanalysis

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 3 (middle) shows the differences of such two S-boxes, where '$*$' stands for any possible difference, Δ_1 and ∇_3 are known.

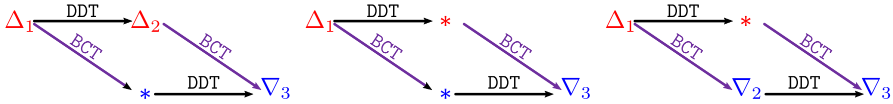

Figure 3: Differences of $\mathtt{DBCT}^{\vdash}$ (left), `DBCT` (middle) and $\mathtt{DBCT}^{\dashv}$ (right)

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           $\mathcal{Y}_{\mathtt{DDT}}^{\cap} = \mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta) \cap (\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta) \oplus \nabla)$;
9   **if** $\mathcal{Y}_{\mathtt{DDT}}^{\cap} \neq \emptyset$ **then**
10             $num \mathrel{+}= \mathtt{DDT}(\Delta_1, \Delta) \cdot \mathtt{BDT}(\Delta, \nabla_3, \nabla) \cdot \frac{\#\mathcal{Y}_{\mathtt{DDT}}^{\cap}}{\#\mathcal{Y}_{\mathtt{DDT}}(\Delta_1, \Delta)}$;
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}.

Additionally, we introduce two variants of `DBCT`, *i.e.*, $\mathtt{DBCT}^{\vdash}$ and $\mathtt{DBCT}^{\dashv}$ as shown in Figure 3, where the differential of one S-box is fixed. Moreover, $\mathtt{DBCT}^{\vdash}(\Delta_1, \Delta_2, \nabla_3), \mathtt{DBCT}^{\dashv}(\Delta_1,$

$\nabla_2, \nabla_3)$ can be precomputed by adapting algorithm 1, as shown in algorithm 2 and algorithm 3 in the appendix.

We also introduce new tables to consider the clustering effect in the middle part of boomerang distinguishers. As it's illustrated in Figure 4, the differences in the same positions at two faces of boomerang distinguisher should not necessarily be the same, particularly in the middle part. For instance, Δ_2^0 and Δ'^0_2 in Figure 4 denote the differences in the same position of cipher during the encryption and decryption respectively, which can take different values in two faces of boomerang distinguisher. ∇_3^0 and ∇'^0_3 in Figure 4, can be different in the same way. Accordingly, we define $\mathtt{DBT}^{\vDash}$ and $\mathtt{BDT}^{\dashv}$ similar to $\mathtt{DBT}$

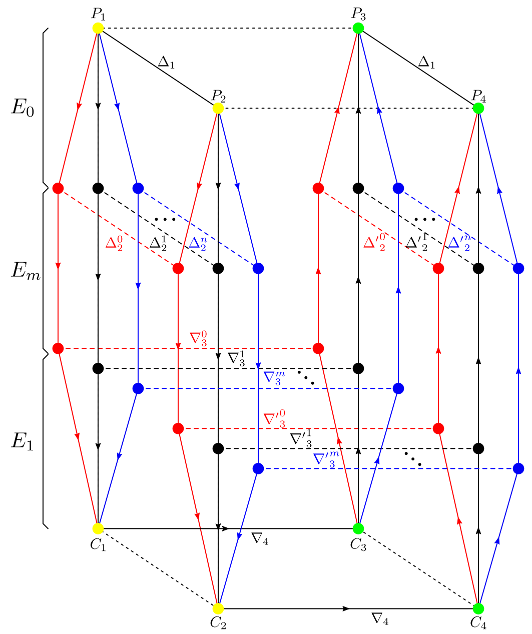

Figure 4: Cluster of sandwich distinguishers

and $\mathtt{BDT}$ respectively as follows:

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

$\mathtt{BCT}^{\vDash}$ and $\mathtt{BCT}^{\dashv}$, can also be defined as follows as the two alternatives of $\mathtt{BCT}$, where the input or the output differences are not the same in two faces of boomerang distinguisher respectively:

$$\mathtt{BCT}^{\vDash}(\Delta_1, \Delta'_1, \nabla_2) := \#\{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus \nabla_2) \oplus S^{-1}(S(x \oplus \Delta_1) \oplus \nabla_2) \ = \Delta'_1\}.$$
$$\mathtt{BCT}^{\dashv}(\Delta_1, \nabla_2, \nabla'_2) := \#\{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus \nabla_2) \oplus S^{-1}(S(x \oplus \Delta_1) \oplus \nabla'_2) \ = \Delta_1\}.$$

4 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 S-boxes 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 5 where the first r_0 and last r_1 rounds are represented in red and blue and denoted by E_0 and E_1 respectively. Moreover, the middle r_m rounds where the first $r_0 + r_m$ and last $r_1 + r_m$ rounds overlap is illustrated in green and denoted by E_m. Firstly, we generate a word-oriented MILP model consisting of constraints corresponding to truncated differential characteristics for the first $r_0 + r_m$ and for the last $r_1 + r_m$ rounds based on the independent binary variables respectively.

Let $u_0, \dots, u_{t-1}$ denote the activeness of S-boxes in last r_m rounds of $E_m \circ E_0$ and $l_0, \dots, l_{t-1}$ denote the activeness of S-boxes in first r_m rounds of $E_1 \circ E_m$, such that u_i and l_i correspond to the same S-box's position for all $0 \le i \le t-1$. In order to model the switching effect in r-round middle part E_m, we introduce t new binary variables $s_0, \dots, s_{t-1}$ linking u_i and l_i for all $0 \le i \le t-1$ as follows:

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

In other words $s_i = 1$ if and only of $u_i = l_i = 1$. Let binary variables $\tilde{u}_0, \dots, \tilde{u}_{m-1}$ and $\tilde{l}_0, \dots, \tilde{l}_{n-1}$ denote the activity of S-boxes in the first r_0 and last r_1 rounds respectively. Assuming that w_0, w_1 and w are positive integers, the objective is to minimize:

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

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 the probability of the boomerang distinguisher, w_0, w_1 and w, are chosen such that $w_0 = w_1 \ge w$.

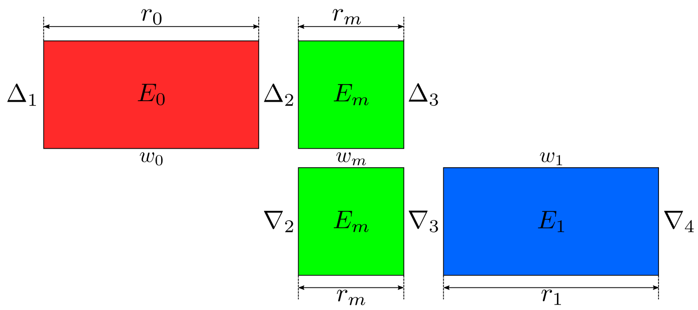

Figure 5: Main parameters of our word-oriented MILP tool to search for boomerang distinguishers

2. At the second step, based on the discovered truncated differential characteristics for E_0 and 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 E_0 and E_1. Then, by fixing the input and output differences of actual differential paths for E_0 and E_1, and taking into account the clustering effect, we compute the differential effects for E_0 and E_1, which are represented by p and q

respectively. Note that, there might not exist an actual differential characteristic instantiating the discovered truncated differential characteristic. 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 distinguisher 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 the upper and lower differential paths respectively, then the compatibility of the upper and lower differential paths is checked by experimentally evaluation of 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. To correctly evaluate the size of E_m, where contains the 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 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 E_0 and 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.

5 Boomerang Distinguishers for Reduced-Round `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. Table 2, summarizes our results on boomerang distinguishers of `CRAFT`, and Table 3, briefly describes the notations we use through this section.

5.1 A Brief Description of `CRAFT`

`CRAFT` is a lightweight tweakable block cipher which has been introduced in FSE 2018 by Beierle *et al.* [BLMR19]. 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

Table 2: Summary of our results and the other known single-tweak attacks on CRAFT. ST, stands for single-tweak, and the 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. The probabilities highlighted in red have been verified experimentally.

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	$\mathbf{1}$	Section 5
	7	$\mathbf{2^{-4}}$	
	8	$\mathbf{2^{-8}}$	
	9	$\mathbf{2^{-14.76}}$	
	10	$\mathbf{2^{-19.83}}$	
	11	$\mathbf{2^{-24.90}}$	
	12	$\mathbf{2^{-34.89}}$	
	13	$2^{-44.89}$	
	14	$2^{-55.85}$	

Table 3: 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 $(i = 0, 1, 2, 3)$
X_i	The internal state before the Mix-Columns (MC) in round i
Y_i	The internal state after the MixColumn (MC) in round i
Z_i	The internal state before the PermuteNibbles (PN) in round i
W_i	The internal state before the S-boxes (SB) in round i
$S_i[j]$	j^{th} cell of a state S, in round i, where $0 \leq j \leq 15$
ΔS	Forward difference in a state S
∇S	Backward difference in a state S
$\mathtt{Y}$	Hexadecimal representation of an arbitrary value $Y \in \mathbb{F}_2^4$, where we are using typewriter style

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 $0 \leq i \leq 30$, $\mathcal{R}_i = SB \circ PN \circ ATK_i \circ ARC_i \circ MC$.

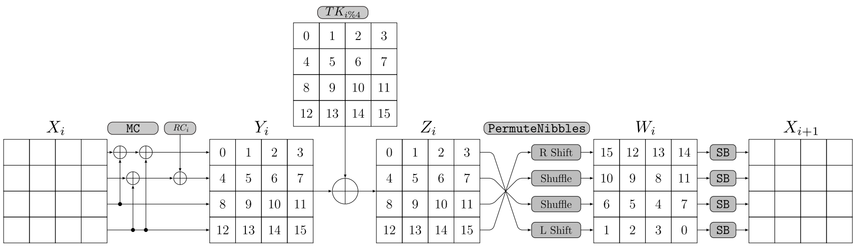

Figure 6: A round of CRAFT

The MC layer is the multiplication of internal state by a 4×4 involutory binary matrix. 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 $\mathcal{R}_i$, $TK_{i\%4}$ 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 layer in which a 4-bit S-box which has been borrowed from MIDORI [BBI+15] is applied on each nibble. One can refer to [BLMR19], to see more details about CRAFT's specification.

5.2 Boomerang Distinguishers for 6 to 8 Rounds of CRAFT

Applying our searching method for boomerang distinguishers of CRAFT, we discovered that up to 6 rounds of this cipher can be distinguished from a random permutation using a boomerang distinguisher with probability one. For instance, let the input and output differences of 6-round boomerang distinguisher of CRAFT are chosen as follows:

$$\Delta X_0 = \texttt{000}\gamma\ \texttt{0000}\ \texttt{000}\gamma\ \texttt{0000},\ \nabla X_6 = \texttt{0000}\ \texttt{0000}\ \texttt{0}\delta\texttt{000}\ \texttt{0000},$$

where $\delta, \gamma \in \mathbb{F}_2^4 \setminus \{0\}$. Rounds 2 to 7 of Figure 7, represents the forward and backward propagation of ΔX_0, and ∇X_6 over 6 rounds of CRAFT respectively, where yellow and green squares denote the nonzero and any differences respectively. It can be seen that there is not any interaction between the active S-boxes of upper and lower differential trails over the rounds 2 to 7 in Figure 7. Therefore, due to the switching effect, the boomerang returns with probability 1.

Next, by extending the discovered 6-round boomerang distinguisher one round backward, we construct a 7-round boomerang distinguisher, which covers rounds 1 to 7 of Figure 7. Table 4, specifies the input and output differences of our 7-round boomerang distinguisher for CRAFT.

Table 4: Specification of boomerang distinguisher for 7 rounds of `CRAFT`

$r_0 = 0, r_m = 7, r_1 = 0, p = 1,\ q = 1,\ r = 2^{-4},\ p^2.q^2.r = 2^{-4}$			
ΔX_0	`00A0 00AA 0000 00A0`	∇X_7	`0000 0000 0A00 0000`

As it can be seen in Figure 7, the upper differential path depends on whether $\gamma = \gamma'$, and there are still some nonzero upper and lower crossing differences even after 7 rounds which reveals that there is dependency between the upper and lower differential paths throughout rounds 1 to 7 in Figure 7. Let r_1, and r_2 be the probability of boomerang distinguisher when $\gamma = \gamma'$, and $\gamma \neq \gamma'$ respectively. Consequently, the probability of the provided 7-round boomerang distinguisher is $r = r_1.\Pr(\gamma = \gamma') + r_2.\Pr(\gamma \neq \gamma')$.

If $\gamma = \gamma'$, as illustrated in Figure 7, the upper and lower differential trails have only one active S-box in common. Let γ, and β denote the output differences of the common active S-box in upper and lower differential paths respectively. The red frames in Figure 7, represent the propagation of difference β, to show where this difference is originated from. As it is visible, the difference β has not been affected by the upper differential path. On the other hand, β is almost uniformly distributed. In conclusion, $r_1 = \sum_{\gamma \in \{\texttt{5,A,D,F}\}} \left(\frac{\texttt{DDT(A,}\gamma\texttt{)}}{2^4}\right)^2 = \sum_{\gamma \in \{\texttt{5,A,D,F}\}} (2^{-2})^2 = 2^{-2}$, and , $r_1.\Pr(\gamma = \gamma') = 2^{-2}.2^{-2} = 2^{-4}$. Due to the fact that $0 \leq r_2.\Pr(\gamma \neq \gamma') \leq 1$, we can conclude that $r \geq 2^{-4}$. According to the experimental evaluation, $r = 2^{-3.97}$, which validates the provided lower bound and also confirms that r_2, contributes less in the total probability r in comparison to r_1.

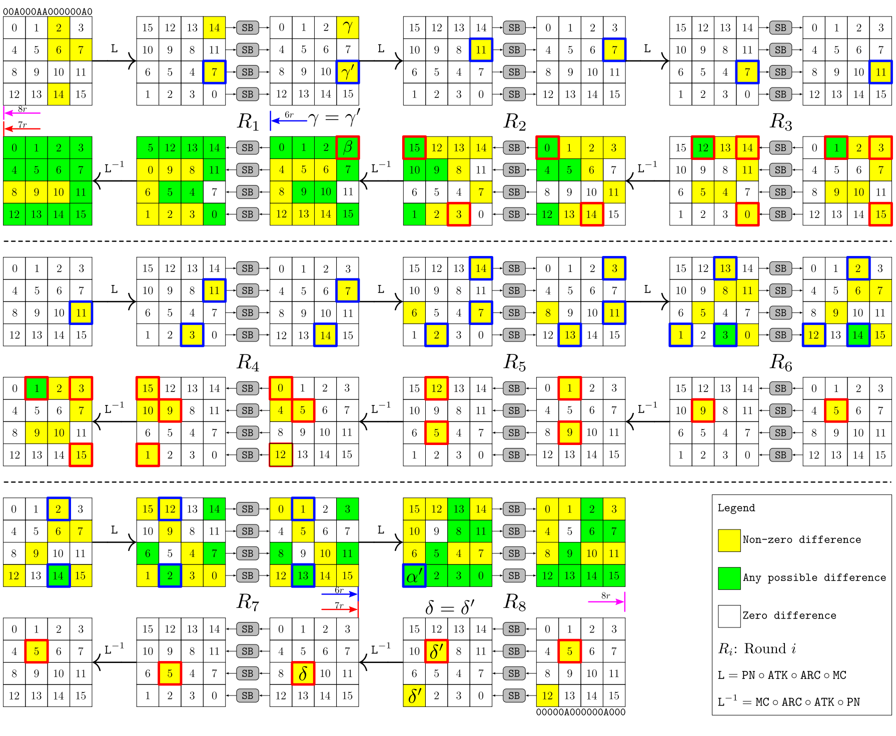

Figure 7: Boomerang Distinguishers for 6 to 8 Rounds of `CRAFT`

Table 5: Specification of the boomerang distinguisher for 8 rounds of `CRAFT`

$r_0 = 0, r_m = 8, r_1 = 0, p = 1,\ q = 1,\ r = 2^{-8},\ p^2.q^2.r = 2^{-8}$			
ΔX_0	`00A0 00AA 0000 00A0`	∇X_8	`0000 0A00 0000 A000`

By extending the discovered 7-round boomerang distinguisher one round forwards, we construct an 8-round boomerang distinguisher whose specification is provided by Table 5. Figure 7, represents the propagation of the input/output differences, in our 8-round boomerang distinguisher. As illustrated, the propagation of the input difference depends on whether $(\gamma = \gamma') \wedge (\delta = \delta')$. In the Figure 7, it is supposed that $(\gamma = \gamma') \wedge (\delta = \delta')$. It can be seen that nonzero differences exist even after 8 rounds in both forward and backward propagation of input and output differences respectively, which means the whole of these 8 rounds contain dependency.

Let r_1, and r_2 be the probability of the 8-round boomerang distinguisher, when $(\gamma = \gamma') \wedge (\delta = \delta')$, and $(\gamma \neq \gamma') \vee (\delta \neq \delta')$ respectively. Hence, the entire probability of the 8-round 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:

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

On the other hand, the upper, and lower differential trails in Figure 7, have only two active cells in common, and there is not any interaction between other active cells in upper and lower differential trails, and the lower crossing difference β is almost uniformly distributed. The red frames depict where the difference β is originated from. It can be seen that it has not been affected by the upper differential trail. The upper crossing difference α', is also uniformly distributed, and as it's depicted by blue frames, it is also independent of the lower differential trail. Therefore, the probability of that the boomerang returns when $(\gamma = \gamma') \wedge (\delta = \delta')$ is:

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

Besides, $\Pr(\gamma = \gamma') = \Pr(\delta = \delta') = 2^{-2}$. Consequently, $r \geq 2^{-8}$. The experimental evaluation show that the boomerang returns with probability $r = 2^{-7.92}$ which confirms the provided lower bound and also show that the total probability r, is almost determined by r_1.

5.3 Probability of The Middle Part in Boomerang Distinguishers for 9 to 14 Rounds of CRAFT

During the search for boomerang distinguishers covering 9 to 14 rounds of CRAFT, we observed that many boomerang distinguishers for these number of rounds have a common active pattern in the 7-round middle part. In other words, there are many boomerang distinguishers for 9 to 14 rounds of CRAFT that can be constructed by extending a 7-round boomerang distinguisher, such that the dependency between the upper and lower differential trails doesn't exist outside the 7-round middle part. Therefore, for the sake of simplicity, we chose a 7-round middle part and then constructed the boomerang distinguishers for 9 to 14 rounds based on it. Figure 9, shows the 7-round boomerang distinguisher with the following input/output differences, which is expandable to construct 9-/10-/11-/12-/13-/14-round boomerang distinguishers of CRAFT.

$$\Delta X_0 = \mathtt{0000\ 0A00\ 0000\ 0000}, \ \nabla X_7 = \mathtt{0000\ 0A00\ 0000\ 0000}.$$

Next, let us calculate the probability of this 7-round boomerang distinguisher. In Figure 9, 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 9). 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 9, 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 $\texttt{DBCT}$, *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 9 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 (A_5, h_5) is:

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

If $(A_5, h_5) = (\texttt{A}, \texttt{A})$, then $r = 2^{-10.39}$. Using Equation 2, we evaluated r, for all $(A_5, h_5) \in \{(i, j) | 1 \leq i \leq 15, 1 \leq j \leq 15\}$, and arranged the results into a 15×15 matrix which is denoted by $R^{7r} = [r]_{i,j}$, where $r_{i,j}$ is the value of r, when $(A_5, h_5) = (i, j)$. R^{7r} is represented in Appendix B. We carried out out experiments on the 7-round boomerang

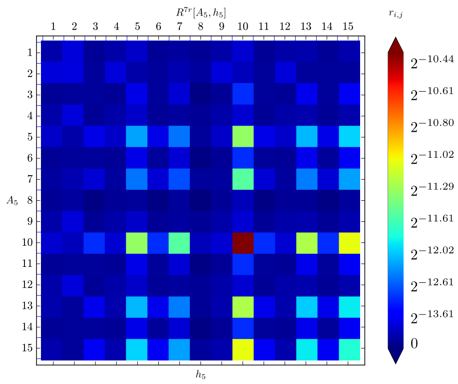

Figure 8: A visual representation of probability matrix R^{7r}

distinguisher in Figure 9, and arranged the experimental probabilities in matrix R^{7r}_e which is displayed in Appendix B. Comparing the theoretical and the empirical probabilities for all $(i, j) \in \mathbb{F}_2^4 \times \mathbb{F}_2^4$, we verified the correctness of the derived formula. Figure 8, visualizes the matrix R^{7r}. It is visible that the maximum value of $r_{i,j}$, is obtained when $(i, j) = (\texttt{A}, \texttt{A})$. In the next sections we extend the 7-round boomerang distinguisher E^{7r}_m, to construct longer boomerang distinguisher up to 14 rounds of $\texttt{CRAFT}$.

5.4 Boomerang Distinguishers for 9 to 14 Rounds of CRAFT

9-Round Boomerang Distinguisher

In order to construct a 9-round boomerang distinguisher for $\texttt{CRAFT}$, we extend the 7-round distinguisher E^{7r}_m in Subsection 5.3, by one round in both directions. Accordingly, as

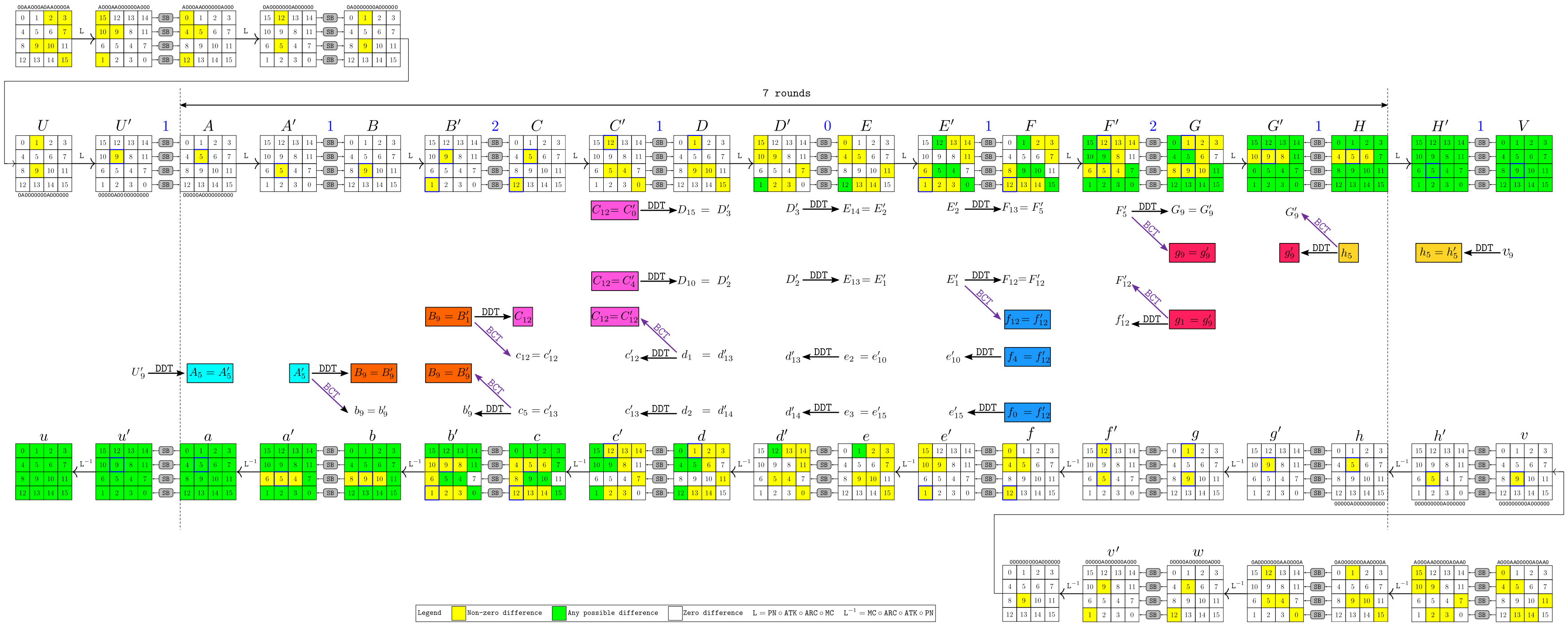

Figure 9: A 7-round E_m where two $\mathtt{DBCT}^{\vdash}$ and two $\mathtt{DBCT}^{\dashv}$ are involved

represented in Figure 9, the input and output differences of the 9-round distinguisher are chosen as follows:

$$\Delta X_0 = \texttt{0A00 0000 0A00 0000},\ \nabla X_9 = \texttt{0000 0000 0A00 0000},$$

to maximize the differential effect for the extended parts which are included in E_0, and E_1. Given that the lower and the upper crossing differences in E_m^{7r}, can be seen as uniform after 7 rounds, we consider the extended parts including the one round ahead and the one round behind, as E_0 and E_1 respectively. Let $\Delta X_1^i = \texttt{0000 0}i\texttt{00 0000 0000}$, and $\nabla X_8^j = \texttt{0000 0}j\texttt{00 0000 0000}$, denote the input and output differences of the 7-round middle part E_m, respectively, where $i, j \in \mathbb{F}_2^4 \setminus \{0\}$. Besides, let $p_i = \Pr(\Delta X_0 \xrightarrow{E_0^{1r}} \Delta X_1^i)$, and $q_j = \Pr(\nabla X_8^j \xrightarrow{E_1^{1r}} \nabla X_9)$. If $(i, j) = (10, 10)$, then $p_i^2 q_j^2 R_{10,10}^{7r} = 2^{-18.39}$, where R^{7r}, is the matrix defined in Subsection 5.3. Taking into account the clustering effect, $p_{bm}^{9r} = \sum_{i=1}^{15} \sum_{j=1}^{15} p_i^2 q_j^2 R_{i,j}^{7r} = 2^{-15.43}$, gives a more accurate lower bound for the probability of the 9-round boomerang distinguisher. However, according to the experimental evaluation, $p_{bm}^{9r} = 2^{-14.50}$. The main reason for this gap between the theoretical bound, and the empirical approximation of p_{bm}^{9r}, is assuming that the differences are equal in two sides of boomerang distinguisher, whereas they can take different values indeed.

More precisely, the differences at positions A_5, and h_5, can take different values in two faces of boomerang. Accordingly, using the $\texttt{DBT}^{\vDash}$ and $\texttt{BDT}^{\dashv}$, we provide a more accurate theoretical bound for the probability of 9-round boomerang distinguisher as follows:

$$p_{bm}^{9r}(U_9', v_9) = 2^{-12\cdot n} \sum_{A_{51}} \sum_{A_{52}} \sum_{b_9} \sum_{B_9} \sum_{c_5} \sum_{c_{12}} \sum_{C_{12}} \sum_{d_1} \sum_{E_1'} \sum_{f_{12}'} \sum_{F_{12}} \sum_{g_9'} \sum_{F_5'} \sum_{G_9} \sum_{h_{51}} \sum_{h_{52}} \texttt{BCT}_{tot}.\texttt{Pr}_{tot}, \tag{3}$$

where $n = 4$, and (A_{51}, A_{52}) and (h_{51}, h_{52}), denote the differences at position A_5 and h_5 in two faces of boomerang distinguisher respectively, and $\texttt{BCT}_{tot}$, and $\texttt{Pr}_{tot}$ are defined as follows:

$$\begin{aligned}
\texttt{BCT}_{tot} = {} & \texttt{DDT}(U_9', A_{51}).\texttt{DDT}(U_9', A_{52}).\texttt{DBT}^{\vDash}(A_{51}, A_{52}, b_9, B_9) \\
& .\texttt{BDT}(B_9, c_5, b_9).\texttt{DBT}(B_9, c_{12}, C_{12}).\texttt{BDT}(C_{12}, d_1, c_{12}) \\
& .\texttt{DBT}(E_1', f_{12}', F_{12}).\texttt{BDT}(F_{12}, g_9', f_{12}').\texttt{DBT}(F_5', g_9', G_9) \\
& .\texttt{BDT}^{\dashv}(G_9, h_{51}, h_{52}, g_9').\texttt{DDT}(h_{51}, v_9).\texttt{DDT}(h_{52}, v_9), \\
\texttt{Pr}_{tot} = {} & \Pr(d_1 \xleftarrow{2\ \texttt{DDT}} cyan) \cdot \Pr(c_5 \xleftarrow{3\ \texttt{DDT}} cyan) \cdot \\
& \Pr(orchid \xrightarrow{2\ \texttt{DDT}} E_1') \cdot \Pr(orchid \xrightarrow{3\ \texttt{DDT}} F_5').
\end{aligned}$$

Evaluation of $p_{bm}^{9r}(U_9', v_9)$, when $(U_9', v_9) = (\texttt{A}, \texttt{A})$, yields $p_{bm}^{9r} = 2^{-14.76}$, which is too close to the experimental value of p_{bm}^{9r}. One can see that, the experimental values of p_{bm}^{9r} and the theoretical value which is obtained using Equation 3, are also close for other values of $(U_9', v_9) \in (\mathbb{F}_2^n \setminus \{0\}, \mathbb{F}_2^n \setminus \{0\})$. It confirms our assumption that there is no dependency out of the 7-round middle part, as Equation 3 has been derived based on the assumption that the upper and lower crossing differences H_5 and a_5, are both uniformly distributed.

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 S-box tables $\texttt{DBT}^{\vDash}$, and $\texttt{BDT}^{\dashv}$. Let A_{51}, and A_{52}, be the differences in two sides of boomerang at position A_5. Similarly h_{51}, and h_{52}, denote the differences in two sides of boomerang at position h_5. To obtain a more accurate bound for the boomerang distinguishers that are constructed by extending our 7-round boomerang distinguisher, we define the 4-dimensional matrix

$R^{7r}_{i,j,k,l}$, as follows:

$$R^{7r}[i,j,k,l] = 2^{-8\cdot n}\sum_{b_9}\sum_{B_9}\sum_{c_5}\sum_{c_{12}}\sum_{C_{12}}\sum_{d_1}\sum_{E'_1}\sum_{f'_{12}}\sum_{F_{12}}\sum_{g'_9}\sum_{f'_{12}}\sum_{F'_5}\sum_{G_9}\mathtt{DBT}^{\vDash}(A_{51},A_{52},b_9,B_9)$$
$$.\mathtt{BDT}(B_9,c_5,b_9).\mathtt{DBT}(B_9,c_{12},C_{12}).\mathtt{BDT}(C_{12},d_1,c_{12})$$
$$.\mathtt{DBT}(E'_1,f'_{12},F_{12}).\mathtt{BDT}(F_{12},g'_9,f'_{12}).\mathtt{DBT}(F'_5,g'_9,G_9)$$
$$.\mathtt{BDT}^{\dashv}(G_9,h_{51},h_{52},g'_9).\mathtt{Pr_{tot}}, \tag{4}$$

where $n = 4, A_{51} = i, A_{52} = j, h_{51} = k$, and $h_{52} = l$. Hereafter, we use this matrix to provide a lower bound for the probability of the extended distinguishers based on E^{7r}_m.

10-Round Boomerang Distinguisher

As illustrated in Figure 9, if the 7-round boomerang distinguisher E^{7r}_m, is extended two rounds forwards, and one round backward, a 10-round boomerang distinguisher is constructed with the following input and output differences:

$$\Delta X_0 = \mathtt{0A00\ 0000\ 0A00\ 0000},\ \nabla X_{10} = \mathtt{0000\ 0A00\ 0000\ A000}.$$

Let E^{1r}_0 and E^{2r}_1, depict the extended parts corresponding to one round ahead and two rounds behind respectively. Furthermore, we consider rounds 2 to 8 as E_m. Let $p_i = \Pr(\Delta X_0 \xrightarrow{E^{1r}_0} \Delta X^i_1)$, and $q_j = \Pr(\nabla X^j_8 \xrightarrow{E^{2r}_1} \nabla X_{10})$, where $\Delta X^i_1 = \mathtt{0000\ 0}i\mathtt{00\ 0000\ 0000}$, and $\nabla X^j_8 = \mathtt{0000\ 0}j\mathtt{00\ 0000\ 0000}$, for $i,j \in \mathbb{F}^4_2 \setminus \{0\}$. Then, a lower bound for the probability of our 10-round boomerang distinguisher is:

$$p^{10r}_{bm} = \sum_{i=1}^{15}\sum_{j=1}^{15}\sum_{k=1}^{15}\sum_{l=1}^{15} p_i p_j q_k q_l R^{7r}_{i,j,k,l} = 2^{-19.83}.$$

However, based on the experimental evaluation, $p^{10r}_{bm} = 2^{-18.17}$. Although it validates our theoretical bound, there is still a gap between the theoretical bound and the empirical value of p^{10r}_{bm}, which is originated from the assumption $v'_1 = v'_9$, for the lower differential trail in Figure 9. As it can be seen in Figure 9, it is supposed that $v'_1 = v'_9$, whereas the differences v'_1 and v'_9, should not necessarily be the same in the 10-round boomerang distinguisher. Given that the output differences of active S-boxes in the last round of the 10-round boomerang distinguisher are equal to A, the input differences, i.e. v'_1 and v'_9, can take an arbitrary value from $\{\mathtt{5},\mathtt{A},\mathtt{D},\mathtt{F}\}$. As a result, in theoretical evaluation of p^{10r}_{bm}, we have considered only 4 possible cases out of 16 possible cases for $v' = \mathtt{0000\ 0}v'_9\mathtt{00\ 0000\ }v'_1\mathtt{000}$. Hence, applying the theoretical formulas provided for the 7-round middle part E^{7r}_m, i.e. Equation 2 and Equation 4, to compute the probability of longer boomerang distinguishers, only gives a lower bound for the probability of boomerang distinguisher covering more than 9 rounds.

One may construct a 10-round boomerang distinguisher by extending the 7-round boomerang distinguisher E^{7r}_m, two rounds backward, and one round forwards. However, as it can be seen in Figure 9, due to the symmetry between the upper and lower differential trails, the total probability of this distinguisher, is the same as the probability of the 10-round distinguisher which is constructed by extending the 7-round boomerang distinguisher one round backward and two rounds forwards.

11-Round Boomerang Distinguisher

The 11-round boomerang distinguisher for CRAFT, can be constructed by extending the 7-round boomerang distinguisher E^{7r}_m, two rounds forwards and backward. As it can be seen in Figure 9, the input and output differences of this 11-round boomerang distinguisher, are as follows:

$$\Delta X_0 = \texttt{A000 AA00 0000 A000}, \ \nabla X_{11} = \texttt{0000 0A00 0000 A000}.$$

Let E_0^{2r} and E_1^{2r}, denote the extended parts ahead and behind respectively, and E_m includes the 7-round at the middle. Assuming that the input/output differences of E_m are $\Delta X_2^i = \texttt{0000 0}i\texttt{00 0000 0000}$, and $\nabla X_9^j = \texttt{0000 0}j\texttt{00 0000 0000}$, respectively, and $p_i = \Pr(\Delta X_0 \xrightarrow{E_0^{2r}} \Delta X_2^i)$, and $q_j = \Pr(\nabla X_9^j \xrightarrow{E_1^{2r}} \nabla X_{11})$, for all $i, j \in \mathbb{F}_2^4$, a lower bound for the probability of the 11-round boomerang distinguisher is:

$$p_{bm}^{11} = \sum_{i=1}^{15} \sum_{j=1}^{15} \sum_{k=1}^{15} \sum_{l=1}^{15} p_i p_j q_k q_l R_{i,j,k,l}^{7r} = 2^{-24.90}.$$

However, according to the experimental evaluations $p_{bm}^{11r} = 2^{-22.44}$. To find the reason of this gap between the theoretical bound and the experimental approximation, note that in Figure 9, it is supposed that $U_1 = U_9$, whereas U_1 and U_9 can take different values. In addition it is supposed that that $v_1' = v_9'$, while v_1' and v_9' should not necessarily be the same.

12-Round Boomerang Distinguisher

One can extend the 7-round boomerang distinguisher E_m^{7r}, 3 rounds backward and 2 rounds forwards to obtain a 12-round boomerang distinguisher for CRAFT. The input/output differences of the 12-round boomerang distinguisher are shown in Table 6, and the input and output differences of the 7-round middle part are assumed to be $\Delta X_3^i = \texttt{0000 0}i\texttt{00 0000 0000}$, and $\nabla X_{10}^j = \texttt{0000 0}j\texttt{00 0000 0000}$, respectively, where $i, j \in \mathbb{F}_2^4 \setminus \{0\}$. Assuming that $p_i = \Pr(\Delta X_0 \xrightarrow{E_0^{3r}} \Delta X_3^i)$, and $q_j = \Pr(\nabla X_{10}^j \xrightarrow{E_1^{2r}} \nabla X_{12})$, a lower bound for the probability of the 12-round boomerang distinguisher is $\sum_{i=1}^{15} \sum_{j=1}^{15} p_i^2 . q_j^2 . R_{i,j}^{7r} = 2^{-35.49}$.

Taking into account that the input and output differences of the middle part should not necessarily be the same in two sides of boomerang distinguisher, the following formula gives a more accurate lower bound for the probability of 12-round boomerang distinguisher:

$$\sum_{i=1}^{15} \sum_{j=1}^{15} \sum_{k=1}^{15} \sum_{l=1}^{15} p_i . p_j . q_k . q_l . R_{i,j,k,l}^{7r} = 2^{-34.89}.$$

According to the experimental evaluations, the probability of that the boomerang returns, is $2^{-32.11}$, which validates the provided lower bound. Table 6, provides a right quartet for the 12-round boomerang distinguisher.

Table 6: The input/output differences, plus a right quartet for 12-round boomerang distinguisher

k	1e97469ac59c9ea9fe87e344887e3ee5		
t	c1bd0a3437864c1f		
ΔX_0	00aa000a0aa0000a	∇X_{12}	00000a000000a000
p_1	7f39ad1a3683588f	c_1	bb6372ede46edf5e
p_2	7f93ad103c235885	c_2	67da6cd68f591770
p_3	4329c595f6d51b67	c_3	bb6378ede46e7f5e
p_4	4383c59ffc751b6d	c_4	67da66d68f59b770

13-Round Boomerang Distinguisher

We construct a 13-round boomerang distinguisher by appending 3 rounds before and after the 7-round boomerang distinguisher E_m^{7r}, in Subsection 5.3. Assuming that, the input and output differences of the 7-round middle part are $\Delta X_3^i = \texttt{0000 0}i\texttt{00 0000 0000}$, and $\nabla X_{10}^j = \texttt{0000 0}j\texttt{00 0000 0000}$, respectively where $i, j \in \mathbb{F}_2^4 \setminus \{0\}$, the following input and output differences for the 13-round boomerang distinguisher, yield the best differential effects for the first and last three rounds:

$$\Delta X_0 = \texttt{00AA 000A 0AA0 000A}, \ \nabla X_{13} = \texttt{0A00 0000 0AA0 000A}.$$

Let $p_i = \Pr(\Delta X_0 \xrightarrow{E_0^{3r}} \Delta X_3^i)$, and $q_j = \Pr(\nabla X_{10}^j \xrightarrow{E_1^{3r}} \nabla X_{13})$. Taking into account that ΔX_3^i, and ∇X_3^j have not to be identical in two faces of boomerang distinguisher, a lower bound for the probability of the 13-round boomerang distinguisher is:

$$\sum_{i=1}^{15}\sum_{j=1}^{15}\sum_{k=1}^{15}\sum_{l=1}^{15} p_i p_j q_k q_l R_{i,j,k,l}^{7r} = 2^{-44.89},$$

where $R_{i,j,k,l}^{7r}$, is the matrix derived from Equation 4. We expect that the probability of the 13-round boomerang distinguisher to be greater than $2^{-44.89}$, since we have not considered all possible differential trails for the given input/output differences in our estimation.

14-Round Boomerang Distinguisher

Lastly, we show that the 7-round boomerang distinguisher in Subsection 5.3 can be extended to construct a 14-round boomerang distinguisher. To do so, we append 3 rounds before, and 4 rounds after the 7-round boomerang distinguisher E_m^{7r}. For all $i, j \in \mathbb{F}_2^4 \setminus \{0\}$, let $\Delta X_3^i = \texttt{0000 0}i\texttt{00 0000 0000}$, $\nabla X_{10}^j = \texttt{0000 0}j\texttt{00 0000 0000}$, be the input and output differences of E_m which is composed of rounds 4 to 10. It can be seen that the best differential effect for the first 3 rounds E_0^{3r}, last 4 rounds E_1^{4r}, are obtained when the input and output differences of the 14-round boomerang distinguisher are chosen as follows:

$$\Delta X_0 = \texttt{00AA 000A 0AA0 000A}, \ \nabla X_{14} = \texttt{A000 AA00 000A 0AA0}.$$

Therefore, assuming that $p_i = \Pr(\Delta_1 \xrightarrow{E_0^{3r}} \Delta_2^i)$, and $q_j = \Pr(\nabla_3^j \xrightarrow{E_1^{4r}} \nabla_4)$, for all $i, j \in \mathbb{F}_2^4 \setminus \{0\}$, a lower bound for the probability of the 14-round boomerang distinguisher is:

$$\sum_{i=1}^{15}\sum_{j=1}^{15}\sum_{k=1}^{15}\sum_{l=1}^{15} p_i p_j q_k q_l R_{i,j,k,l}^{7r} = 2^{-60.33}.$$

Similar to the previous cases, we expect that the boomerang returns with a probability higher than what is estimated above as we have not considered the entire clustering effect inside the boomerang distinguisher.

5.5 A Dedicated Boomerang Distinguisher for 14 Rounds of CRAFT

In the previous sections, we showed that there exist boomerang distinguishers for up to 14 rounds of CRAFT. However, for convenience, we used a common middle part to construct the boomerang distinguishers covering 9 to 14 rounds of CRAFT. Thus, it may be possible to find a better distinguisher in terms of probability if we search for a dedicated boomerang distinguisher for each case. Here, we provide a dedicated boomerang distinguisher with higher probability for 14 rounds of CRAFT. Table 7, describes the specification of a dedicated boomerang distinguisher for 14 rounds of CRAFT, and Figure 10, illustrates three different parts of this distinguisher, i.e., E_0, E_1 and E_m.

As shown in Figure 10, the upper and lower differential paths are strongly interrelated and there are many common active S-boxes in the middle part. Hence, to avoid the complicated formulas we switch to the experimental approach to provide a lower bound for the probability of this boomerang distinguisher. Let consider the 8-round middle part including rounds 4 to 11 as E_m. As it can be seen in Figure 10, there exist only one active cell in both input and output differences of E_m. On the other hand, each of the input and output differences can take different values in two faces of boomerang. Consequently, there are in total $15^4 = 50625$ possible combinations for the input/output differences of E_m in two sides of boomerang distinguisher. However, due to the restricted computing power, we let the differences in active input and output cells of E_m, to be different in two sides of boomerang only if they are taken from $S = \{\mathtt{5}, \mathtt{7}, \mathtt{A}, \mathtt{D}, \mathtt{F}\}$, otherwise, we assume that they are the same in two faces of boomerang. Thus, we consider only $5^4 + 10^2 = 725$ cases out of 50625 possible combinations for the input/output differences of E_m. Let $\Delta X_3^i = \mathtt{0000\ 00}i\mathtt{0\ 0000\ 0000}$, and $\nabla X_{11}^j = \mathtt{0000}\ j\mathtt{000\ 0000\ 0000}$, for all $i, j \in \mathbb{F}_2^4 \setminus \{0\}$. For each of 725 possible combinations, the input and output differences of E_m in two sides of boomerang are fixed, and the probability of that the boomerang returns is experimentally evaluated. Then, for all $i, j, k, l \in S$, the results are arranged into:

$$R_{i,j,k,l}^{8r} := \Pr\{E_m^{-1}\left(E_m(x) \oplus \nabla X_{11}^k\right) \oplus E_m^{-1}\left(E_m\left(x \oplus \Delta X_3^i\right) \oplus \nabla X_{11}^l\right) = \Delta X_3^j\},$$

and for all $i, j \in \mathbb{F}_2^4 \setminus S \cup \{0\}$, the results are stored into $R_{i,j}$, such that:

$$R_{i,j}^{8r} := \Pr\{E_m^{-1}\left(E_m(x) \oplus \nabla X_{11}^j\right) \oplus E_m^{-1}\left(E_m\left(x \oplus \Delta X_3^i\right) \oplus \nabla X_{11}^j\right) = \Delta X_3^i\}.$$

Next, we show that the dependency doesn't exist outside E_m. To this end, we firstly assume that the lower and upper crossing differences are uniformly distributed outside E_m. Based on this assumption, the following formula:

$$\sum_{i \in S} \sum_{j \in S} \sum_{k \in S} \sum_{l \in S} p_i p_j q_k q_l R_{i,j,k,l}^{8r} = 2^{-25.65},$$

where $p_i = \Pr(\Delta X_2 \xrightarrow{E_0^{1r}} \Delta X_3^i)$, and $q_j = \Pr(\nabla X_{11}^j \xrightarrow{E_1^{1r}} \nabla X_{12})$, for all $i, j \in \mathbb{F}_2^4 \setminus \{0\}$, and $\Delta X_2 = \mathtt{A000\ 0000\ A000\ 0000}$, and $\nabla X_{12} = \mathtt{0000\ A000\ 0000\ 0000}$, must give the same value as the experimental probability of the 10-round boomerang distinguisher that is constructed by appending one round before and after the E_m, in Figure 10. It can be seen that the experimental probability of the 10-round boomerang distinguisher composing of rounds 3 to 12 in Figure 10 is $2^{-25.65}$, which confirms our assumption. Consequently, a lower bound for the probability of the 14-round boomerang distinguisher is:

$$\sum_{i,j,k,l \in S} p_i . p_j . q_k . q_l . R_{i,j,k,l}^{8r} + \sum_{i,j \in \mathbb{F}_2^4 \setminus S \cup \{0\}} p_i^2 . q_j^2 . R_{i,j}^{8r} = 2^{-55.85} + 2^{-66.70} = 2^{-55.85},$$

where $p_i = \Pr(\Delta X_0 \xrightarrow{E_0^{3r}} \Delta X_3^m)$, and $q_j = \Pr(\nabla X_{11}^n \xrightarrow{E_1^{3r}} \nabla X_{14})$, for all $i, j \in \mathbb{F}_2^4 \setminus \{0\}$. It is visible that the total probability is almost determined by the first term.

Table 7: Specification of a dedicated boomerang distinguisher for 14 rounds of CRAFT

$r_0 = 3, r_m = 8, r_1 = 3,\ \sum p_i p_j . q_k . q_l . R_{i,j,k,l}^{8r} = 2^{-55.80};\ \delta, \gamma \in \mathbb{F}_2^4 \setminus \{0\}$			
ΔX_0	00AA 00A0 A00A 00A0	ΔX_3	0000 00δ0 0000 0000
∇X_{11}	0000 γ000 0000 0000	∇X_{14}	00A0 0000 0AA0 A000

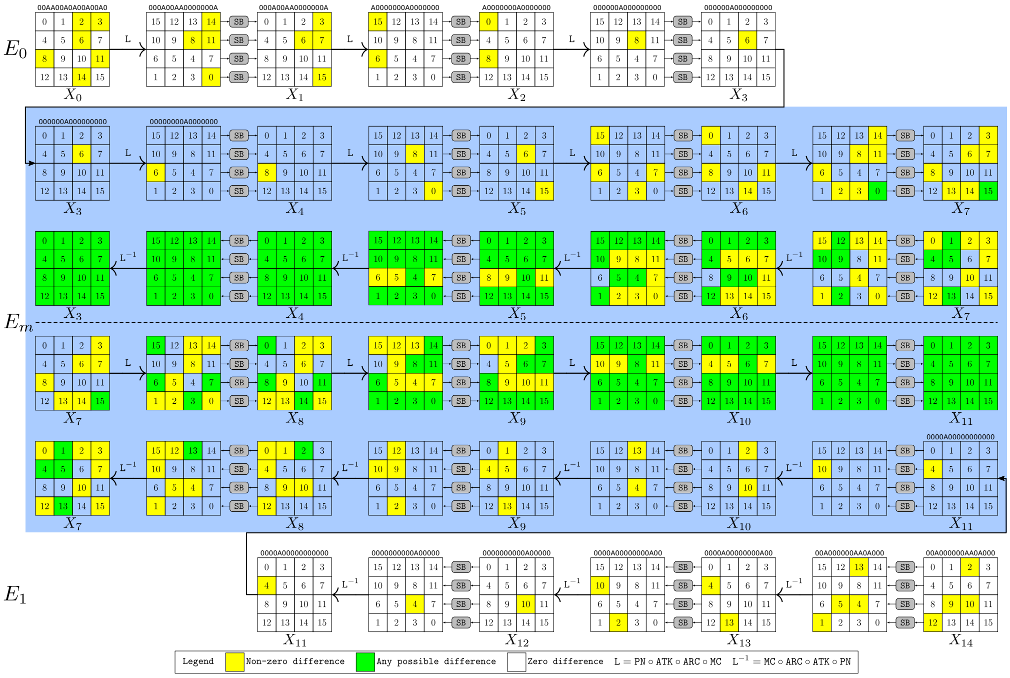

Figure 10: A dedicated boomerang distinguisher for 14 rounds of `CRAFT` with the form $3 + 8 + 3$

5.6 Boomerang Distinguishers of `CRAFT` in the Related-Tweak Model

We have investigated the boomerang behavior of `CRAFT` in related-tweak model also. In contrast to the single tweak model where the boomerang distinguishers have significant advantages against the basic differential distinguishers, the outcome was not promising in terms of number of rounds compared to the current best differential distinguishers in the related tweak model. It shows that boomerang attack is less efficient than the basic differential attack for `CRFAT` in the related tweak model. It worth noting, we expected this behavior and it is not surprising. More precisely, on the one hand the differences that are introduced by the tweakey schedule accelerate the diffusion of uniformly distributed differences which reduces the number of rounds that can be covered by the middle part. On the other hand, the clustering effect in the related tweak model, is weaker in compare with the single tweak model for `CRAFT`. Hence, the outcome was not promising in this model compared to the previous related tweak differential cryptanalysis [BLMR19].

6 Boomerang Distinguishers for Reduced-Round `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`. Table 8, briefly describes the notations we use through this section of the paper.

6.1 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

Table 8: Notations for `SKINNY`.

$TK1_i$	Tweakey state $TK1$ in round i. $TK2_i$ and $TK3_i$ are defined similarly
TK_i	i^{th} round tweakey. This is equal to the result of XORing the first and the second rows of $TK1_i$ and $TK2_i$ for `SKINNY`-n-$2n$ and $TK1_i$,$TK2_i$ and $TK3_i$ for `SKINNY`-n-$3n$
X_i	Internal state before SC in round i
Y_i	Internal state before ART in round i
Z_i	Internal state before SR in round i
W_i	Internal state before MC in round i
$S_i[j]$	j^{th} cell of a state S, in round i, where $0 \leq j \leq 15$
ΔS	Forward difference in a state S
∇S	Backward difference in a state S
`Y`	Hexadecimal representation of arbitrary value $Y \in \mathbb{F}_2^4$, where we are using typewriter style.

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 into a 4×4 array, where $I_i \in \mathbb{F}_2^4$ (or $\mathbb{F}_2^8$).

As illustrated in Figure 11, 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`) where some round-dependent constants are XORed to the first column of the the cipher internal state. Then, in AddRoundTweakey (`ART`), as represented in Figure 11, the first and second rows of the tweakey state are XORed with 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 the MixColumns (`MC`) layer, each column of the internal state is multiplied by 4×4 binary matrix. The tweakey state of `SKINNY` can contain both key and tweak materials

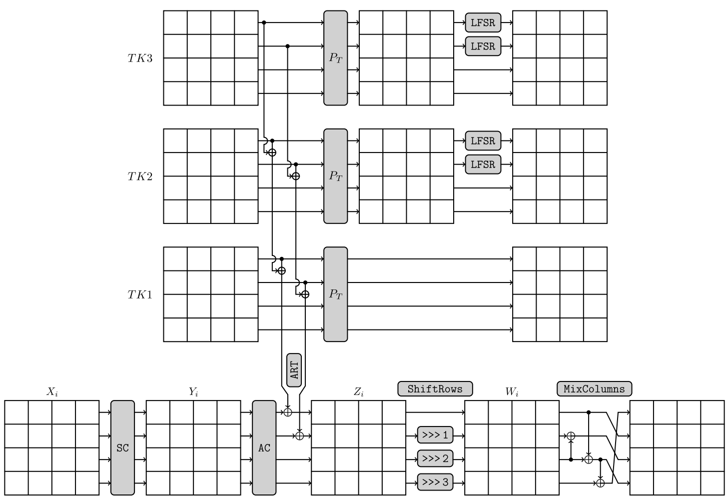

Figure 11: The round function and tweakey schedule of `SKINNY`

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 $TK1, TK2$, and $TK3$ when $z = 3$. Let $TKi[j]$ represents the j'th cell of TKi for $i \in \{1, 2, 3\}$. 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].

Table 9: Summary of our results in comparison to the best previous results in [SQH19], for boomerang distinguishers of SKINNY. The probabilities highlighted in red have been verified experimentally. The Roman numbers represent the corresponding distinguisher in our paper. The probabilities denoted by †, correspond to the distinguishers that can be obtained by extending the distinguishers proposed in [SQH19].

Version	n	#Rounds	Probability: Our Distinguisher	Probability: [SQH19]
SKINNY-n-$2n$	64	17	$\mathbf{2^{-26.54}}$ (II)	$2^{-29.78}$
		18	$\mathbf{2^{-37.90}}$ (II)	$2^{-45.14}$†
		19	$\mathbf{2^{-51.08}}$ (II)	$2^{-65.62}$†
	128	18	$\mathbf{2^{-40.87}}$ (II)	$2^{-77.83}$
		19	$\mathbf{2^{-58.33}}$ (II)	$2^{-97.53}$†
		20	$\mathbf{2^{-85.31}}$ (I)	$2^{-128.65}$†
		21	$\mathbf{2^{-114.07}}$ (II)	$2^{-171.77}$†
SKINNY-n-$3n$	64	22	$\mathbf{2^{-40.67}}$ (I)	$2^{-42.98}$
		23	$\mathbf{2^{-55.85}}$ (I)	$2^{-67.36}$†
	128	22	$\mathbf{2^{-40.57}}$ (I)	$2^{-48.30}$
		23	$\mathbf{2^{-56.47}}$ (I)	$2^{-75.86}$†
		24	$\mathbf{2^{-87.39}}$ (I)	$2^{-107.86}$†
		25	$\mathbf{2^{-116.59}}$ (I)	$2^{-141.66}$†

In [LGS17a], Liu *et al.*, provided related tweakey rectangle attacks against SKINNY. After that, in EUROCRYPT 2018, Cid *et al.* introduced the BCT in [CHP+18], and applied it to accurately evaluate the probability of generating the right quartet for two middle rounds of boomerang distinguishers proposed in [LGS17a]. 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 [LGS17a] are much higher than previously evaluated. To the best of our knowledge, the results of Song *et al.* 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 remarkably better than the best previous boomerang distinguishers of SKINNY in terms of probability and number of rounds. Table 9, summarizes our results on boomerang distinguishers for SKINNY-n-$2n$ and SKINNY-n-$3n$, where they are compared with the best previous ones.

Firstly, we investigated the best previous boomerang distinguishers in [SQH19], to see how many rounds they can be extended. To this end, by keeping the middle part and the tweakey's difference of the proposed distinguishers unchanged, we extend them some rounds forwards and backward. Then, by fixing the input and output differences of E_m, we look for the best differential trails covering the extended E_0 and E_1. After that, taking into account the clustering effect, we compute p and q. In conclusion, given that r is known, we compute the total probability using p^2q^2r formula. The summary of our results concerning this search is given in Table 15. As it can be seen, the best previous boomerang distinguishers of SKINNY-64-128, SKINNY-128-256 and SKINNY-128-384, proposed in [SQH19] and [LGS17c], can be extended up to 18, 19, and 24 rounds respectively, whereas the best previous boomerang distinguisher for 22 rounds of SKINNY-64-192, can not be extended for a higher number of rounds at all.

Based on the results in [SQH19], where it is proved that the upper and lower differential paths in boomerang distinguishers of SKINNY can be dependent up to 6 rounds, we searched for the boomerang distinguisher of SKINNY taking into account the 6-round middle part as E_m. Given that the boomerang distinguishers for 8-bit versions of SKINNY, cover more number of rounds [SGSL18], in comparison to the 4-bit versions, and 8-bit S-boxes are heavy for MILP/SAT solvers, applying our searching method on 8-bit versions of SKINNY is more time-consuming. Accordingly, we applied a dedicated method to find boomerang distinguishers for SKINNY to speed up the search. Due to the structural similarity between 4-bit and 8-bit versions of SKINNY, our idea is to use the discovered boomerang distinguishers for 4-bit versions, in discovering boomerang distinguishers for 8-bit versions. Once a boomerang distinguisher is discovered for 18 rounds of SKINNY-64-128, we use the middle part of the discovered boomerang distinguisher to find a boomerang distinguisher for 18 rounds of SKINNY-128-256, as well as a 22 rounds of SKINNY-128-256. To do so, we divide 18 (and 22) rounds of SKINNY-128-256 (and SKINNY-128-384) into three parts such that E_m includes the 6-round middle part. Then, we look for the best differential trails for the first and last parts, i.e., E_0 and E_1 satisfying the active pattern of the input and output in the discovered E_m. The discovered boomerang distinguishers for 22 rounds of SKINNY-64-192 can be used to discover boomerang distinguishers for 22 rounds of SKINNY-128-384 in the same way. As a result, the discovered boomerang distinguishers have a common active pattern in the middle part.

Throughout applying our searching method for boomerang distinguishers on SKINNY, we observed that a suitable boomerang distinguisher for 18 rounds of SKINNY-64-128 and SKINNY-128-256, can be extended up to 19 and 21 rounds of these variants respectively. Besides, we observed that a suitable boomerang distinguisher for 22 rounds of SKINNY-64-192 and SKINNY-128-384 can be extended up to 23 and 25 rounds respectively. Among all of the discovered boomerang distinguishers using our dedicated searching method, we picked the two best ones that are called the boomerang distinguisher I, and boomerang distinguisher II, which are presented in the next sections.

6.2 Boomerang Distinguisher I for SKINNY

In this section we present the details of boomerang distinguisher I, for different variants of SKINNY. This distinguisher is constructed using our dedicated method to search for boomerang distinguishers of SKINNY, where we first discover a suitable boomerang distinguisher for 18 rounds of SKINNY-64-128, and then use it's middle part to discover boomerang distinguishers for other variants of SKINNY. That's is why the active pattern in the middle part of boomerang distinguisher I, is the same for all variants of SKINNY. We first focus on the boomerang distinguisher I, for SKINNY-64-128 and SKINNY-128-256.

Boomerang Distinguisher I for SKINNY-64-128 and SKINNY-128-256

Table 10, describes the specification of the boomerang distinguisher I for 18 rounds of SKINNY-64-128, and Figure 12, represents the upper and lower differential trails of this boomerang distinguisher, where the yellow squares stand for active cells, and green squares represents any differences in Figure 12. Hex numbers at the top of the state squares are exact differences specified by the differential trails. The horizontal dashed lines in Figure 12, separate E_0, E_m and E_1. It can be seen that each one of E_0, E_1 and E_m

includes 6 rounds, such that the middle part E_m, is composed of rounds R_7 to R_{12}, over which the upper and lower differential trails are extended with probability 1 towards each other.

Table 10: Specification of boomerang distinguisher I for 18 rounds of SKINNY-64-128

$r_0 = 6, r_m = 6, r_1 = 6, p = 2^{-2.41},\ q = 2^{-8},\ r = 2^{-19.16},\ p^2.q^2.r = 2^{-39.98}$			
$\Delta TK1$	00000000C0000000	$\Delta TK2$	00000000F0000000
ΔX_0	0000000000000008	ΔX_6	0000000000040000
$\nabla TK1$	0000000000004000	$\nabla TK2$	0000000000007000
∇X_{12}	0000000000000000	∇X_{18}	0454000404070404

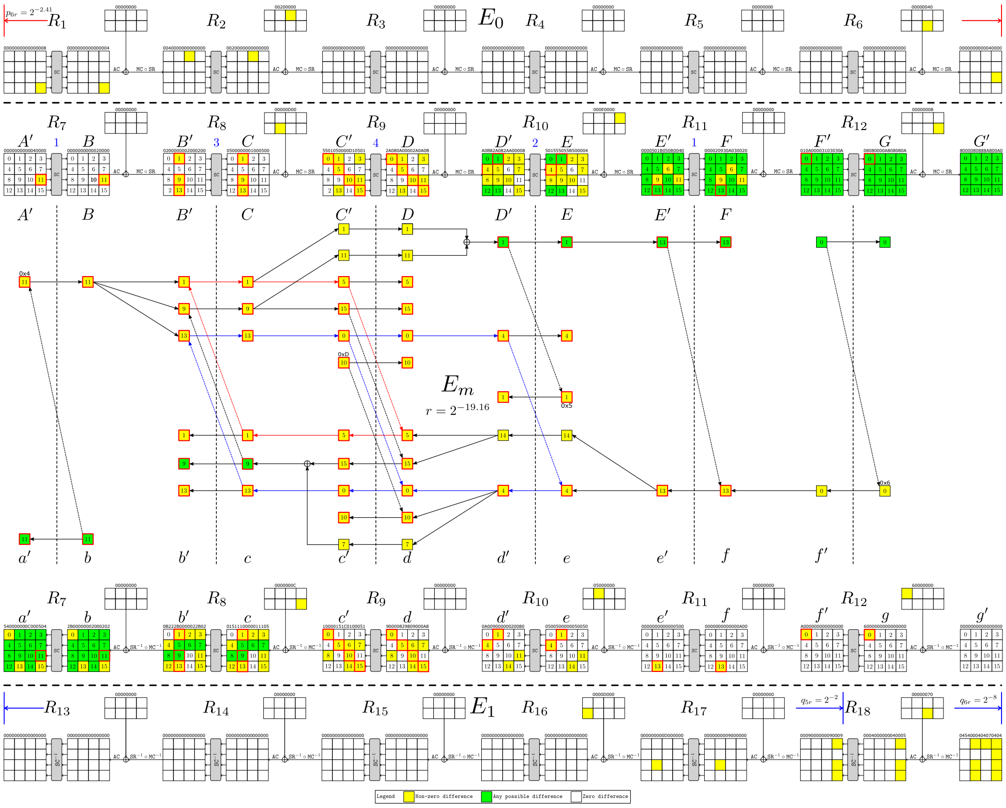

Figure 12: Boomerang distinguisher I for 18 rounds of SKINNY-64-128 with the form 6 + 6 + 6

Next we compute the probability of the middle part E_m, where assumed to include the dependency between the upper and lower differential trails. As illustrated in Figure 12, most of the common active S-boxes between the upper and lower differential trails, appear in rounds R_8 to R_{10}. Hence, we start with computing the probability for intermediate rounds consisting of rounds R_8 to R_{10}. It can be seen that c'_9 and D'_1, in lower and upper differential trails respectively, are almost uniformly distributed. On the other hand, due to the weak diffusion of the linear layer, the difference d'_1 in lower differential trail, doesn't diffuse to more cells. In addition, d'_1, should not necessarily take an identical value in two sides of boomerang. Consequently, assuming that $d'_{1,1}$ and $d'_{1,2}$, denote the different values of difference d'_1, in two sides of boomerang, and c'_9 and D'_1 are uniformly distributed, the probability of the 3-round middle part including rounds R_8 to R_{10} can be computed as follows:

$$p_m^{3r} = 2^{-13\cdot n}. \sum_{d'_{14}} \sum_{C_9} \sum_{d'_4} \sum_{C_{13}} \sum_{d'_{1,1}} \sum_{d'_{1,2}} \mathtt{DBCT}(B_{11}, d'_{14}).\mathtt{DDT}^2(B_{11}, C_9).$$
$$\mathtt{DBCT}^{\vdash}(B_{11}, C_{13}, d'_4).\mathtt{BCT}(C_9, d'_{14}).$$
$$\mathtt{DBCT}^{\dashv}(C_{13}, d'_4, e'_{13}).\mathtt{BCT}(C'_{10}, d'_4).$$
$$\mathtt{DDT}(d'_{1,1}, e_1).\mathtt{DDT}(d'_{1,2}, e_1).\mathtt{DDT}(d'_{14}, e'_{13}) = 2^{-11.55},$$

where $n = 4, B_{11} = \mathtt{2}, C'_{10} = \mathtt{D}$, and $e_1 = e'_{13} = \mathtt{5}$. Experimental value of p_m^{3r} is $2^{-11.70}$, which is too close the the provided theoretical value. Next, we append round R_{11}, and provide a formula to theoretically evaluate the probability for the 4-round intermediate part including rounds R_8, R_9, R_{10}, and R_{11}. To this end, note that the difference e'_{13} has not to be identical in two faces of boomerang. Thus, assuming that $e'_{13,1}$ and $e'_{13,2}$ represents the differences at position e'_{13}, in two sides of boomerang, we have:

$$p_m^{4r} = 2^{-15\cdot n} \sum_{d'_{14}} \sum_{C_9} \sum_{d'_4} \sum_{C_{13}} \sum_{d'_{1,1}} \sum_{d'_{1,2}} \sum_{e'_{13,1}} \sum_{e'_{13,2}} \sum_{D'_4} \mathtt{DBCT}(B_{11}, d'_{14}).\mathtt{DDT}^2(B_{11}, C_9).\mathtt{BCT}(C_9, d'_{14})$$
$$.\mathtt{BCT}(C'_{10}, d'_4).\mathtt{DBCT}^{\vdash}(B_{11}, C_{13}, d'_4).\mathtt{DDT}(C_{13}, D'_4).\mathtt{BDT}^{\dashv}(D'_4, e'_{13,1}, e'_{13,2}, d'_4).$$
$$.\mathtt{DDT}(d'_{1,1}, e_1).\mathtt{DDT}(d'_{1,2}, e_1)(\mathtt{DDT}(d'_{14}, e'_{13,1}) + \mathtt{DDT}(d'_{14}, e'_{13,2})) = 2^{-13.73},$$

where $n = 4, B_{11} = \mathtt{2}, C'_{10} = \mathtt{D}, e_1 = \mathtt{5}$, and $f_{13} = \mathtt{2}$. Based on the experimental evaluations, $p_m^{4r} = 2^{-13.89}$ which is too close to the provided theoretical value. It should be noted that, providing an accurate formula for high number of rounds in which the clustering effect in the middle part can be considered, is not only complicated, but also evaluating such a formula in our boomerang distinguishers is a computationally hard problem, especially for 8-bit versions of SKINNY. In conclusion, to avoid the complicated formulas, and with the aim of providing a more accurate bound, we switch to the experimental approach.

As illustrated in Figure 12, the lower crossing differences after 6 rounds are not enough random, as there are still nonzero differences in state a'. On the other hand, four rounds ahead and four rounds behind the 6-round E_m, are fully passive, and we can be sure that the dependency doesn't exist out of the 6-round middle part, as after propagating the lower and upper differential trails by four more rounds forwards and backward, the crossing differences can be seen as perfectly uniform. Note that the input and output differences of E_m in Figure 12, are imposed by the tweakey differences. Given that, the tweakey schedule is linear, and the master tweakey's difference is fixed, the only possible combination for the input/output differences of E_m in Figure 12, is $\Delta X_6 = \mathtt{0000000000040000}$, $\nabla X_{12} = \mathtt{0000000000000000}$. Therefore, by fixing the input/output differences of E_m, by ΔX_6, and ∇X_{12} respectively, we can simply evaluate the experimental probability of the 6-round middle part.

According to the experimental evaluation, the probability of intermediate E_m with 6 rounds in Figure 12, is $2^{-19.16}$. Then, for the full 18-round distinguisher, taking into account the clustering effect, the probability of the first and last 6 rounds can be simply calculated using automatic methods based on MILP/SAT, which are $p = 2^{-2.41}$ and $q = 2^{-8}$ respectively. In conclusion, a lower bound for the probability of full 18-round boomerang distinguisher I for SKINNY-64-128 is $p^2q^2r = 2^{-39.98}$. We experimentally verified the correctness of this bound, and Table 20, provides a right quartet for this distinguisher.

The boomerang distinguisher I for 18 rounds of SKINNY-64-128 can be extended one round backward, to construct a 19-round boomerang distinguisher, whose specification is provided in Table 11, which improves the previous results by one round. Also, as it can be seen in Figure 12, removing the last round of 18-round boomerang distinguisher I for SKINNY-64-128, results in a 17-round boomerang distinguisher with probability $2^{-27.98}$,

Table 11: Specification of boomerang distinguisher I for 19 rounds of SKINNY-64-128

$r_0 = 7, r_m = 6, r_1 = 6, p = 2^{-9},\ q = 2^{-8},\ r = 2^{-19.10},\ p^2.q^2.r = 2^{-53.10}$			
$\Delta TK1$	C000000000000000	$\Delta TK2$	F000000000000000
ΔX_0	2000001001001000	ΔX_7	0000000000040000
$\nabla TK1$	0000400000000000	$\nabla TK2$	0000700000000000
∇X_{13}	0000000000000000	∇X_{19}	0454000404070404

which is better than the 17-round boomerang distinguisher proposed in [LGS17c], in terms of probability.

As mentioned before, to find a boomerang distinguisher for 18 rounds of SKINNY-128-256, we divide it into three 6-round parts, and then look for the best differential trails for E_0 and E_1, satisfying the input/output active pattern of the discovered E_m in boomerang distinguisher I for SKINNY-64-128. Due to the structural similarity between the SKINNY-64-128 and SKINNY-128-256, we found an 18-round boomerang distinguisher for SKINNY-128-256, with exactly the same active pattern as 18-round boomerang distinguisher I for SKINNY-64-128, where, the large block size of SKINNY-128-256, let us extend the discovered boomerang distinguisher I for SKINNY-128-256, up to 21 rounds of this cipher, which improves the previous distinguisher by two rounds. The specification of boomerang distinguisher I for 18 to 21 rounds of SKINNY-128-256 are described in Table 16.

Boomerang Distinguisher I for SKINNY-64-192 and SKINNY-128-384

Table 12, describes the specification of boomerang distinguisher I for 22 rounds of SKINNY-64-192, and Figure 13, illustrates the upper and lower differential trails of this distinguisher. E_0 and E_1 are composed of the first and last 8 rounds respectively, and the 6-round middle part has been considered as E_m. It can be seen that the active pattern in the middle part of this distinguisher is exactly the same as the active pattern of the middle part in boomerang distinguisher I for SKINNY-64-128.

Next, we show that E_m in Figure 13, contains entire dependency between the upper and lower differential trails. The propagation of lower differences with probability 1 over the E_m in Figure 13, shows that there are still non-zero differences even after 6 rounds. Hence, the upper and lower differential trails are dependent in E_m. On the other hand, 6 rounds before and after E_m, are totally passive, and the upper and lower crossing differences are uniformly distributed after 6 rounds propagation in forward and backward directions respectively. Consequently, E_m, contains entire dependency between the upper and lower differential trails in Figure 13. Given that the input/output differences of the middle part E_m are induced from the tweakey differences, and therefore are fixed, we experimentally evaluate the probability of the middle part, for the fixed input/output differences shown in Figure 13. Then, taking into account the clustering effect, we compute p and q which are given in Table 12. Lastly using the p^2q^2r formula we provide a lower bound for the probability of boomerang distinguisher. We also experimentally verified the correctness of the constructed distinguisher. Table 21, provide a right quartet satisfying the boomerang distinguisher I for SKINNY-64-192.

Table 12: Specification of boomerang distinguisher I for 22 rounds of SKINNY-64-192. $\Delta TK = \Delta TK1||\Delta TK2||\Delta TK3$, and $\nabla TK = \nabla TK1||\nabla TK2||\nabla TK3$

$r_0 = 8, r_m = 6, r_1 = 8, p = 2^{-2.41},\ q = 2^{-7},\ r = 2^{-21.85},\ p^2.q^2.r = 2^{-40.67}$			
ΔTK	0000000007000000 0000000003000000 000000000B000000		
ΔX_0	0000000000000100	ΔX_8	0000000000040000
∇TK	0000000000200000 0000000000300000 0000000000D00000		
∇X_{14}	0000000000000000	∇X_{22}	5605060000450605

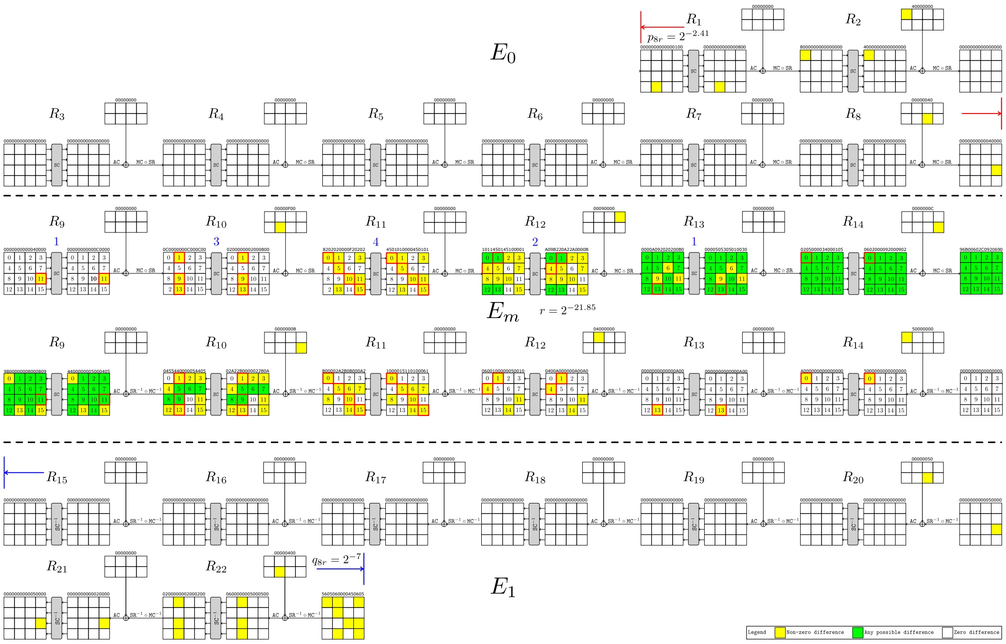

Figure 13: Boomerang distinguisher I for 12 rounds of SKINNY-64-192 with the form 8 + 6 + 8

Boomerang distinguisher I for SKINNY-64-192, can be extended one round backward, which results in a 23-round boomerang distinguisher whose specification is given by Table 13, whereas the best previous boomerang distinguisher for 22 rounds of SKINNY-64-192 in [LGS17c], can't be extended for 23 rounds of this version.

Table 13: Specification of boomerang distinguisher I for 23 rounds of SKINNY-64-192

$r_0 = 9, r_m = 6, r_1 = 8, p = 2^{-10},\ q = 2^{-7},\ r = 2^{-21.85},\ p^2.q^2.r = 2^{-55.85}$			
ΔTK = 0700000000000000 0300000000000000 0B00000000000000			
ΔX_0	0900200000020020	ΔX_9	0000000000040000
∇TK = 0020000000000000 0030000000000000 00D0000000000000			
∇X_{15}	0000000000000000	∇X_{23}	5605060000450605

In the same way, we also found a boomerang distinguisher for 22 rounds of SKINNY-128-384 with exactly the same active pattern as the active pattern of boomerang distinguisher I for 22 rounds of SKINNY-64-192. The large block size of SKINNY-128-384, allows us to extend the discovered boomerang distinguisher I for 22 rounds of SKINNY-128-384, up to 25 rounds of this cipher, whereas the best previous boomerang distinguisher of this variant in [LGS17c], can be extended up to 24 rounds. Table 17, describes the specifications of boomerang distinguisher I for 22 to 25 rounds of SKINNY-128-384. Thanks to the high probability of boomerang distinguisher I for 22 rounds of SKINNY-128-384, we could experimentally verify it, and Table 22, represents one of the right quartets that were discovered during our experiments.

6.3 Boomerang Distinguisher II for SKINNY-64-128 and SKINNY-128-256

Throughout our search for boomerang distinguishers of SKINNY, we discovered a boomerang distinguisher which was a little better than boomerang distinguisher I for SKINNY-64-128, and SKINNY-128-256, in terms of probability, which is introduced here as boomerang distinguisher II for these variants of SKINNY. Due to our strategy to search for boomerang distinguishers of SKINNY, the active pattern of the middle part in boomerang distinguisher II, is also the same for 18 rounds of SKINNY-64-128, and SKINNY-128-256. Therefore, we represent both of them in Figure 14.

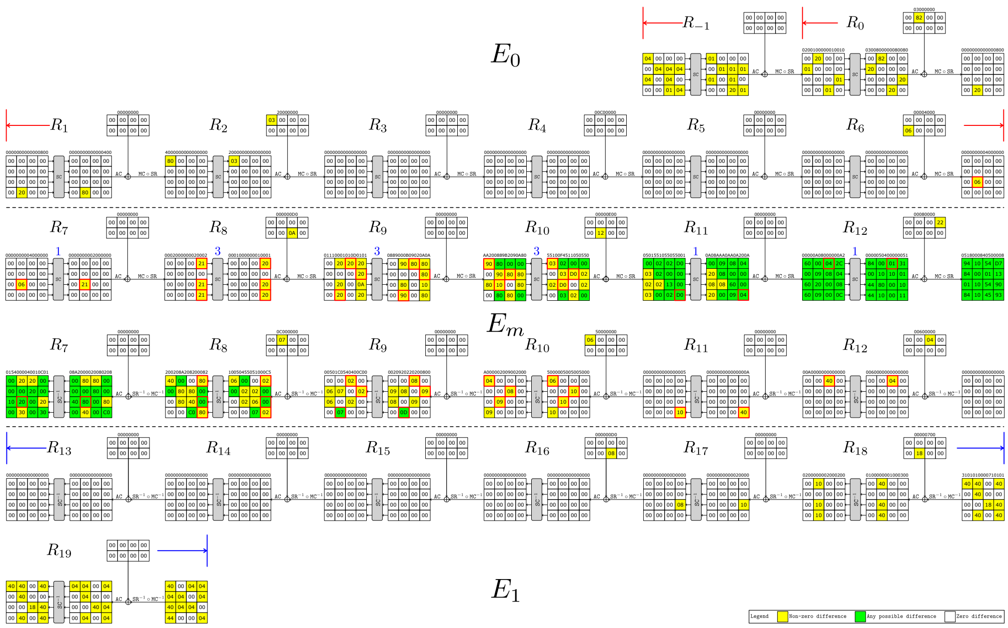

Figure 14: Boomerang distinguisher II for 18 and 19 rounds of SKINNY-64-128, and 18 to 21 rounds of SKINNY-128-256

In Figure 14, the hex numbers inside the squares represent the exact differences of upper and lower differential trails in boomerang distinguisher II for SKINNY-128-256, whereas the hex number at the top of the state arrays represent the exact difference of upper and lower differential trails in boomerang distinguisher II for SKINNY-64-128. As illustrated in Figure 14, four rounds before and after E_m, are fully passive, which shows E_m contains entire dependency between the upper and lower differential trails. A lower bound can be computed for the probability of this distinguisher as before. As it is shown in Figure 14, the 18-round boomerang distinguisher II for SKINNY-64-128, can be extended one round backward to construct a 19-round boomerang distinguisher for this variant os SKINNY. Similarly, the boomerang distinguisher II for SKINNY-128-256, can be extended up to 21 rounds of this variant. The full specification of boomerang distinguisher II for SKINNY-64-128 and SKINNY-128-256 are given in Table 18, and Table 19, respectively.We experimentally verified the correctness of boomerang distinguisher II for 18 rounds of SKINNY-128-256 and Table 23, represents one of the right quartets discovered in during our experiments. It worth noting that the boomerang distinguisher II for 18 rounds of SKINNY-128-256 is the first practical boomerang distinguisher for 18 rounds of SKINNY-128-256, that can be verified practically without consuming too much computing power.

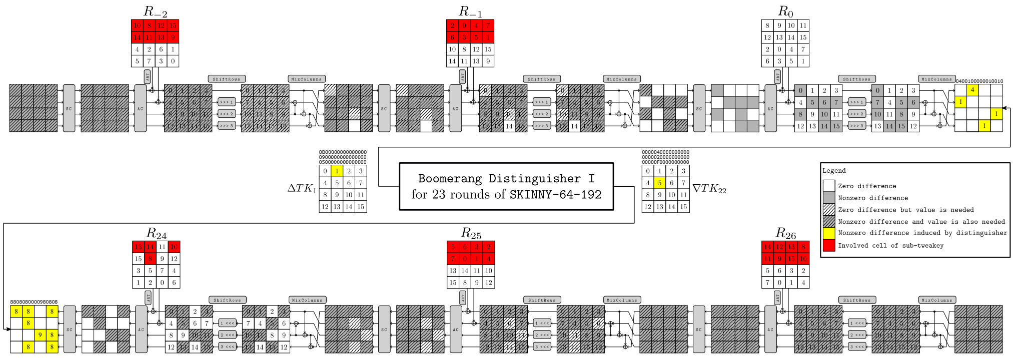

Figure 15: A 29-round key recovery attack against SKINNY-64-192

7 Rectangle Attacks on SKINNY and CRAFT

In this section, based on the new distinguishers introduced in the previous section for SKINNY, i.e. distinguisher I/II, and the best boomerang distinguisher covering 14 rounds of CRAFT, i.e. Figure 10, we present improved related tweakey rectangle attacks on SKINNY's variants and CRAFT. Through the attack, we follow the generalized framework for key recovery which has been recently proposed by Zhao *et al.* [ZDM+20]. We also use the same notations as much as possible. Hence, the number of bits in each cell are denoted by c, and r_b denotes the number of unknown bits in the difference of input pairs when we backtrack the trail from the input difference of the boomerang distinguisher in backward direction under related key difference ΔK for n_b round(s), where the number of involved bits of the sub-tweakeys are denoted by m_b. Similarly, we can define r_f and m_f for propagation of the output of the boomerang distinguisher in forward direction under the related keys difference ∇K for n_f round(s). To have s quartets satisfy the distinguisher, we should design y structures that for each structure we assign all possible values to the unknown cells of the plaintexts (r_b bits) and we also should satisfy $y = \sqrt{s}.2^{n/2-r_b}/\sqrt{p^2.r.q^2}$. We define $M = y.2^{r_b}$ as the number of messages that are queried under each related-key. Through the attacks on SKINNY's variants, we use the bellow properties of SKINNY [ZDM+20, SMB18]:

- Given that the round-tweak is XORed with internal state after the SC layer and also AC, SR and MC layers are linear, we can do key recovery at Y_0 by defining $\Delta Y_0 = \mathtt{SR}^{-1} \circ \mathtt{MC}^{-1}(\Delta_1) \oplus \Delta TK_0$, where Δ_1 is the difference at the input of the boomerang distinguisher (see Figure 15). Hence, it does not necessary to guess this round's sub-tweakey.
- Similarly we can start the key recovery attack at Z_{-n_b+1}, by defining the equivalent tweakey ETK by using $ETK = MC \circ SR(TK_{r_b-1})$.
- Given the ciphertext C, we can decrypt MC and SR layers of the last round. Hence, we use $\mathtt{SR}^{-1} \circ \mathtt{MC}^{-1}(C)$ for the key recovery attack. For the last two rows that are not affected by the sub-tweakey, we can also invert SC layer also.

Besides we recall the bellow lemma from [ABC+17, LGS17c]:

Lemma 1. *For the SKINNY's S-box, the equation $S(x + \Delta_i) + S(x) = \Delta_o$ has one solution x on average for $\Delta_i, \Delta_o \neq 0$.*

7.1 Related Tweakey Rectangle Attack on SKINNY-64-192

Following Figure 15, we prefix three rounds at the beginning and three rounds at the end of the distinguisher I for SKINNY-64-192, which includes 23 rounds, to conduct a related-tweakey boomerang attack on 29 rounds of the cipher. In this process $r_b = 13 \times 4$, $m_b = 16 \times 4$, $r_f = 16 \times 4$ and $m_f = 20 \times 4$. We should satisfy $y = \sqrt{s}.2^{n/2-r_b}/\sqrt{p^2.r.q^2}$ which is $y = 2.2^{32-52}/\sqrt{2^{-55.85}} = 2^{8.92}$ for $s = 4$ and $M = y.2^{r_b} = 2^{60.92}$. The attack procedure is as follows:

1. In data collection, we construct y structures at Y_{-2}, each structure include 2^{rb} possible values for the unknown cells to achieve $M = y.2^{r_b}$ different plaintexts. Next, each plaintext (P) is encrypted under four related tweaks TK^1, $TK^2 = \Delta TK \oplus TK^1$, $TK^3 = \nabla TK \oplus TK^1$ and $TK^4 = \Delta TK \oplus TK^3$ to receive (C_1, C_2, C_3, C_4). Then, (P, C_1), (P, C_2), (P, C_3) and (P, C_4) are respectively stored in four separate lists as L_1, L_2, L_3 and L_4, where L_2 and L_4 are stored in hash tables H_1 and H_2 respectively, indexed by the r_b bits of plaintexts.

2. Guess a value for the m_b bits of the sub-tweakeys of TK^1 that are involved in E_b and do as follows:

   (a) We create two sets S_1 and S_2 and for each pair $(P_1, C_1) \in L_1$, using the guessed bits of TK^1 we partially encrypt it up to Y_0, XOR it with the intermediate difference at Y_0, i.e. ΔY_0, decrypt it partially using $TK^2 = TK^1 \oplus \Delta TK$ to achieve P_2 and find related $(P_2, C_2) \in H_1$ and store $(P_1, C_1), (P_2, C_2)$ in the set S_1. We do a similar approach for $P_3 \in L_3$ and $P_4 \in L_4/H_2$ and store the related pairs $(P_3, C_3), (P_4, C_4)$ in the set S_2. It is clear:

   $$\{((P_1, C_1), (P_2, C_2)) \in S_1 :(P_1, C_1) \in L_1, (P_2, C_2) \in L_2, \\ E_{bTK^1}(P_1) \oplus E_{bTK^2}(P_2) = \Delta Y_0\}$$

   and

   $$\{((P_3, C_3), (P_4, C_4)) \in S_2 :(P_3, C_3) \in L_3, (P_4, C_4) \in L_4, \\ E_{bTK^3}(P_3) \oplus E_{bK^4}(P_4) = \Delta Y_0\}$$

   Hence, the size of each set is $M = y.2^{r_b} = 2^{60.92}$.

   (b) Assuming the known cells at the output difference includes $n - r_f$ bits, while we are propagating from ∇_1 as the output difference of the distinguisher toward the ciphertext, we use those $n - r_f$ bits of C_1 and $n - r_f$ bits of C_2 to put S_1 to hash table H_3. Next, for any $((P_3, C_3), (P_4, C_4)) \in S_2$ we try to find an entry $((P_1, C_1), (P_2, C_2)) \in H_3$ such that (C_1, C_3) and (C_2, C_4) collide in $n - r_f$ known bits. We remove any entry in S_2/H_3 that does not collide at all. The remaining quartets will be about $M^2.2^{-2(n-r_f)}$. However, in this case $n - r_f = 0$ and the remaining quartets will be $(2^{60.92})^2.2^{2.(0)} = 2^{121.85}$.

   (c) We then initialize a list of 2^{m_f} counters, i.e. 2^{80}, each of them corresponds to a choice for the active m_f bits of sub-tweakeys of the last two rounds.

   (d) For each surviving quartets from Step 2b, we do the key recovery step by step as follows:

      i. It is possible to partially decrypt the ciphertext pairs (C_1, C_3), and determine their Z_{26}. Since the last two rows of Z_{26} are not affected by TK_{26}, we can also determine $X_{26}[8] \sim X_{26}[15]$. Given that $\Delta X_{26}[1] = \Delta X_{26}[5] = \Delta X_{26}[13]$ and we know $\Delta Y_{26}[1]$ and $\Delta Y_{26}[5]$, so on average we achieve one solutions for each of $TK[12]$ and $TK[9]$. Besides, $\Delta X_{26}[7] = \Delta X_{26}[11] \oplus \Delta X_{26}[15]$ and we know $\Delta Y_{26}[7]$. Therefore on average we achieve one solutions for $TK[10]$.

ii. Next, we partially decrypt the ciphertext pairs (C_2, C_4), and in a similar approach we determine the candidates for $TK[9]$,$TK[10]$ and $TK[12]$ and determine whether they are matched with the retrieved values in the previous steps. It happens with the probability of 2^{-12} and about $2^{-12}.2^{121.85} = 2^{109.85}$ quartets are remaining.

iii. Given $TK[12]$ and $TK[9]$ we can decrypt the second column of Y_{26} and determine $\Delta Y_{25}[1]$, $\Delta Y_{25}[4]$, $\Delta Y_{25}[11]$ and $\Delta Y_{25}[14]$ for any quartets.

iv. Next, we guess $TK[14]$ and partially decrypt the first column of Y_{26} and determine $Y_{25}[13]$ for any quartets.

v. For any right pair of (C_1, C_3) and (C_2, C_4), we should have $\Delta X_{25}[13] = \Delta X_{25}[1]$. Hence, given that we have $Y_{25}[13]$ and $\Delta Y_{25}[1]$ for any (C_1, C_3) and (C_2, C_4) we can determine $\Delta X_{25}[1]$. Given $\Delta X_{25}[1]$ and $\Delta Y_{25}[1]$ we should receive identical solution for $TK[6]$, for both (C_1, C_3) and (C_2, C_4) of any quartet. Therefor the remaining quartets will be $2^4.2^{109.85}.2^{-4} = 2^{109.85}$.

vi. Given $TK[10]$ we can partially decrypt the last column of Y_{26} and determine $\Delta Y_{25}[3]$, $\Delta Y_{25}[6]$ and $Y_{25}[9]$ for any quartets.

vii. Next, we guess $TK[15]$ and partially decrypt the rest of the third column of Y_{26} and determine $\Delta Y_{25}[2]$, $\Delta Y_{25}[5]$ and $Y_{25}[8]$ for any quartets.

viii. For any right pair of (C_1, C_3) and (C_2, C_4), we should have $\Delta X_{25}[5] = \Delta X_{25}[9]$. Hence, given that we have $Y_{25}[9]$ and $\Delta Y_{25}[5]$ for any (C_1, C_3) and (C_2, C_4) we can determine $\Delta X_{25}[9]$ and $\Delta X_{25}[5]$. Given $\Delta X_{25}[5]$ and $\Delta Y_{25}[5]$ we should receive identical solution for $TK[0]$, for both (C_1, C_3) and (C_2, C_4) of any quartet. Therefor the remaining quartets will be $2^4.2^{109.85}.2^{-4} = 2^{109.85}$.

ix. Next, we guess $TK[8]$ and partially decrypt the last column of Y_{26} and determine $Y_{25}[12]$ for any quartets.

x. For any right pair of (C_1, C_3) and (C_2, C_4), we should have $\Delta X_{25}[4] = \Delta X_{25}[8] \oplus \Delta X_{25}[12]$. Hence, given that we have $Y_{25}[12]$, $Y_{25}[8]$ and $\Delta Y_{25}[4]$ for any (C_1, C_3) and (C_2, C_4) we can determine $\Delta X_{25}[4]$. Given $\Delta X_{25}[4]$ and $\Delta Y_{25}[4]$ we should receive identical solution for $TK[7]$, for both (C_1, C_3) and (C_2, C_4) of any quartet. Therefor the remaining quartets will be $2^4.2^{109.85}.2^{-4} = 2^{109.85}$.

xi. Next, we guess $TK[13]$ and partially decrypt the third column of Y_{26} to determine $Y_{25}[15]$ and $X_{25}[15]$ for any quartets.

xii. For any right pair of (C_1, C_3) and (C_2, C_4), we should have $\Delta X_{25}[15] = \Delta X_{25}[3]$. Hence, given that we have $X_{25}[15]$ and $\Delta Y_{25}[3]$ for any (C_1, C_3) and (C_2, C_4) we should receive identical solution for $TK[2]$, for both (C_1, C_3) and (C_2, C_4) of any quartet. Therefor the remaining quartets will be $2^4.2^{109.85}.2^{-4} = 2^{109.85}$.

xiii. Similarly, we guess $TK[11]$ and partially decrypt the last first column of Y_{26} to determine $\Delta Y_{25}[0]$, $\Delta Y_{25}[7]$ and $Y_{25}[10]$ for any quartets.

xiv. For any right pair of (C_1, C_3) and (C_2, C_4), we should have $\Delta X_{25}[15] = \Delta X_{25}[7]$. Hence, given that we have $X_{25}[15]$ and $\Delta Y_{25}[7]$ for any (C_1, C_3) and (C_2, C_4) we should receive identical solution for $TK[4]$, for both (C_1, C_3) and (C_2, C_4) of any quartet. Therefor the remaining quartets will be $2^4.2^{109.85}.2^{-4} = 2^{109.85}$.

xv. Then we partially decrypt the second column of Z_{25} of (C_1, C_3) to determine the value and differences at $Z_{24}[1]$, $Z_{24}[4]$,$Z_{24}[11]$ and $Z_{24}[14]$. Given that we have the difference value at $X_{24}[1]$ we achieve one solution for each of $TK[14]$. We also know the expected difference of $X_{24}[11]$ and a wrong key will remain with the probability of 2^{-4}. Hence, about $2^{-4}.2^{109.85} = 2^{105.85}$ quartets are remaining.

xvi. We also partially decrypt the second column of Z_{25} of (C_2, C_4) to determine the value and differences at $Z_{24}[1]$, $Z_{24}[4]$,$Z_{24}[11]$ and $Z_{24}[14]$ and determine whether the differences at $X_{24}[1]$ and $X_{24}[11]$ are satisfied. Hence, about $2^{-8}.2^{105.85} = 2^{97.85}$ quartets are remaining.

xvii. We then partially decrypt the last column of Z_{25} of (C_1, C_3) to determine the values and differences at $Z_{24}[3]$, $Z_{24}[6]$,$Z_{24}[9]$ and $Z_{24}[12]$. Given that we have the difference value at $X_{24}[3]$ we achieve one solution for $TK[10]$.

xviii. Next, we partially decrypt the last column of Z_{25} of $(C_2, C4)$ to determine the values and differences at $Z_{24}[3]$, $Z_{24}[6]$,$Z_{24}[9]$ and $Z_{24}[12]$ and determine whether the differences at $X_{24}[3]$ is satisfied. Hence, about $2^{-4}.2^{97.85} = 2^{93.85}$ quartets are remaining.

xix. We guess $TK[5]$ and partially decrypt the first column of Z_{25} of (C_1, C_3) to determine the value and differences at $Z_{24}[0]$, $Z_{24}[7]$,$Z_{24}[10]$ and $Z_{24}[13]$. Given that we have the difference values at $X_{24}[0]$ we achieve one solution for $TK[13]$. Besides, we have the difference at $X_{24}[10]$ and $X_{24}[13]$ the probability of mapping the values of $X_{24}[10]$ and $X_{24}[13]$ for (C_1, C_2) to that differences will happen with the probability of 2^{-8}. Hence, about $2^4.2^{93.85}.2^{-8} = 2^{89.85}$ quartets are remaining.

xx. Then, we partially decrypt the first column of Z_{25} of (C_2, C_4) to determine the values and differences at $Z_{24}[0]$, $Z_{24}[7]$,$Z_{24}[10]$ and $Z_{24}[13]$ and determine whether the differences at $X_{24}[0]$, $X_{24}[7]$, $X_{24}[10]$and $X_{24}[13]$ are satisfied. Hence, about $2^{-12}.2^{89.85} = 2^{77.85}$ quartets are remaining.

xxi. We guess $TK[3]$ and $TK[1]$ and partially decrypt the third column of Z_{25} of (C_1, C_3) to determine the value and differences at $Z_{24}[2]$, $Z_{24}[5]$,$Z_{24}[8]$ and $Z_{24}[15]$. Given that we have the difference values at $X_{24}[5]$ we achieve one solution for $TK[8]$ and since also we have the difference at $X_{24}[15]$ the probability of mapping the values of $X_{24}[15]$ for (C_1, C_2) to that differences will happen with the probability of 2^{-4}. Hence, about $2^8.2^{77.85}.2^{-4} = 2^{81.85}$ quartets are remaining.

xxii. Then, we partially decrypt the third column of Z_{25} of (C_2, C_4) to determine the values and differences at $Z_{24}[2]$, $Z_{24}[5]$,$Z_{24}[8]$ and $Z_{24}[15]$ and determine whether the differences at $X_{24}[2]$, $X_{24}[5]$, $X_{24}[8]$and $X_{24}[15]$ are satisfied. Hence, about $2^{-8}.2^{81.85} = 2^{73.85}$ quartets are remaining, to be used to count for the 80-bit sub-tweakeys involved in the forward part.

xxiii. We select the first $2^{m_f - h}$ candidates for the m_f bits of the sub-tweakeys and do exhaustive search for the remaining $192 - m_b - h = 108$ bits of the master key based on each candidate, when $h = 20$.

xxiv. Go to item 2 if there is not the correct key.

Given that $m_b = 64$ the amount of table look-ups are $3 \times 2^{m_b} \times M = 2^{126.51}$, to create the lists. To do the first filtering at Steps 2(d)i and 2(d)ii, we should do one round decryption for the survived quartets that are $2^{121.85}$ quartets and costs $2^{121.85} \times \frac{1}{29} = 2^{117.68}$ and should be repeated for any guess of m_b, leads to $2^{181.68}$. Next, through Steps 2(d)iii to 2(d)xiv we should do one round encryption which costs $2^{113.85} \times \frac{1}{29} = 2^{109.68}$ and should be repeated for any guess of m_b, leads to $2^{173.68}$. We should do another round decryption for the survived quartets at Step 2(d)xiv through the rest of the attack, that are $2^{109.85}$ quartets, and costs $2^{109.85} \times \frac{1}{29} = 2^{104.99}$ and again should be repeated for any guess of m_b, leads to $2^{168.99}$. It is the dominant complexity of the rest of the attack up to the Step 2(d)xxii. In item 2(d)xxiii, the complexity is $2^{m_b} 2^{192 - m_b - h} = 2^{172}$, for $h = 20$. Hence, the total time complexity will be almost $2^{181.7}$. The data complexity of the attack is $4 \times M = 2^{62.92}$

chosen plaintexts. The memory complexity is $4 \times M + M + 2^{m_f} = 5 \times 2^{60.92} + 2^{80} \approx 2^{80}$. The signal/noise ratio is $S_N = \frac{p^2.r.q^2}{2^{-n}} = \frac{2^{-55.85}}{2^{-64}} = 2^{8.15}$ is the success probability is $P_s = 0.976$.

A similar attack can be conducted on other variants of SKINNY also. Based on the parameter-set that is depicted in Table 14, a summary of the key recovery attacks has been presented in Table 1. Following this we achieved the bellow results:

1. We prefix two rounds at the beginning and two rounds at the end of the distinguisher II for SKINNY-64-128, which includes 19 rounds, to conduct a related-tweakey boomerang attack on 22 rounds of the cipher. In this process $r_b = 8 \times 4 = 32$, $m_b = 8 \times 4 = 32$, $r_f = 13 \times 4$ and $m_f = 12 \times 4$. We should satisfy $y = 2^{26.54}$ for $s = 4$ and it results $M = 2^{58.54}$. Given that $m_b = 32$ the amount of table look-ups are $2^{92.12}$, to create the lists. To do the first filtering, based on the ciphertexts, we should inverse the last round's MC-layer which costs less than $2^{56.01}$. We should also do one round decryption for the survived quartets that are $2^{93.08}$ quartets and costs $2^{32} \times 2^{93.08} \times \frac{1}{23} = 2^{120.56}$. In item 2(d)xxiii, the complexity is $2^{m_b} 2^{128-m_b-h} = 2^{88}$, for $h = 40$. Given that the complexity of the other steps are negligible, the time complexity will be approximately $4M + 2^{120.56} + 2^{88} \approx 2^{120.7}$. The data complexity of the attack is $2^{60.54}$ chosen plaintexts. The memory complexity is $5 \times 2^{58.54} + 2^{48} \approx 2^{60.9}$. The signal/noise ratio is $2^{12.92}$ and the success probability is $P_s = 0.977$.

2. We extend the 21-round boomerang distinguisher I against SKINNY-128-256 to 24 rounds key recovery attack. It worth noting that distinguisher II has better probability but distinguisher I provides lower total complexity in key recovery, based on our analysis. Through the attack, we prefix a round at the beginning and two rounds at the end of the distinguisher I for SKINNY-128-256, which includes 21 rounds, to conduct a related-tweakey boomerang attack on 24 rounds of the cipher. In this process $r_b = 0$, $m_b = 0$, $r_f = 14 \times 8$ and $m_f = 13 \times 8$. In this attack, we have $y = 2^{123.21}$ for $s = 4$ and $M = 2^{123.21}$. Given that $m_b = 0$ the amount of table look-ups are $2^{124.8}$, to create the lists. To do the first filtering, based on the ciphertexts, we should inverse the last round's MC-layer and a cell of SC-layer which costs less than $2^{120.63}$. We should also do one round decryption for the survived quartets that are $2^{214.43}$ quartets and costs $2^{209.84}$. In item 2(d)xxiii, the complexity is 2^{168} for $h = 88$. Given that the complexity of the other steps are negligible, the time complexity will be approximately $4M + 2^{209.84} + 2^{168} \approx 2^{209.85}$. The data complexity of the attack is $2^{125.21}$ chosen plaintexts. The memory complexity is $5 \times 2^{123.21} + 2^{104} = 2^{125.54}$. The signal/noise ratio is $2^{11.57}$, the success probability is $P_s = 0.977$.

3. We prefix three rounds at the beginning and two rounds at the end of the distinguisher Ifor SKINNY-128-384, which includes 25 rounds, to conduct a related-tweakey boomerang attack on 30 rounds of the cipher. In this process $r_b = 13 \times 8$, $m_b = 15 \times 8$, $r_f = 16 \times 8$ and $m_f = 15 \times 8$. We should satisfy $y = 2^{19.29}$ for $s = 4$ and $M = 2^{123.29}$. Given that $m_b = 120$ the amount of table look-ups are $2^{244.88}$, to create the lists. We should also inverse the last round's MC-layer and a cell of SC-layer which costs less than $2^{120.43}$. We should also do one round decryption for the survived quartets that are $2^{246.59}$ quartets and costs $2^{120} \times 2^{246.59} \times \frac{1}{30} = 2^{361.68}$. In item 2(d)xxiii, the complexity is 2^{280}, for $h = 104$. Given that the complexity of the other steps are negligible, the time complexity will be approximately $4M + 2^{361.68} + 2^{280} \approx 2^{361.68}$. The data complexity of the attack is $2^{125.29}$ chosen plaintexts and the memory complexity is $2^{125.8}$. The signal/noise ratio is $S_N = \frac{p^2.r.q^2}{2^{-n}} = \frac{2^{-116.59}}{2^{-128}} = 2^{11.41}$ and the success probability is $P_s = 0.977$.

Table 14: Summary of the used parameters through our recovery attacks on the variants of SKINNY and CRAFT, where D, nD, n_b and n_f respectively denote the used distinguisher,number of rounds of the used distinguisher, backward appended rounds and forward appended rounds.

Scheme	D	nD	n_b	n_f	r_b	m_b	r_f	m_f	$q^2.r.q^2$	M	h
SKINNY-64-128	Table 18	19	2	2	32	32	52	48	$2^{51.08}$	$2^{58.54}$	40
SKINNY-64-192	Table 13	23	3	3	52	64	64	80	$2^{55.85}$	$2^{60.92}$	20
SKINNY-128-256	Table 16	21	1	2	0	0	112	104	$2^{116.43}$	$2^{123.21}$	88
SKINNY-128-384	Table 17	25	3	2	104	120	128	120	$2^{116.59}$	$2^{123.29}$	104
CRAFT	Figure 10	14	1	3	24	24	44	84	$2^{55.8}$	$2^{60.9}$	72

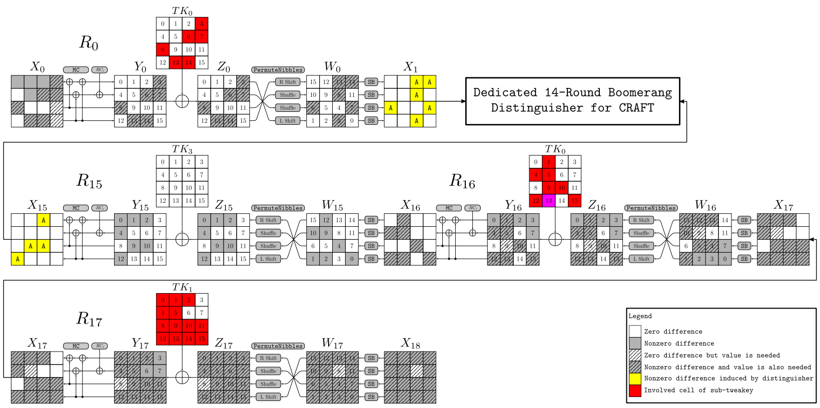

Figure 16: A 18-round key recovery attack against CRAFT

7.2 Single-Tweak Rectangle Attack on CRAFT

In this section we use the best boomerang distinguisher covering 14 rounds of CRAFT, i.e. Figure 10, to provide a key-recovery attack on 18 rounds of the cipher in single-tweak model as it is depicted in Figure 16. To have s quartets satisfy the distinguisher, we should design y structures that for each structure we assign all possible values to the unknown cells and we also should satisfy $y = \sqrt{s} \cdot 2^{n/2-r_b}/\sqrt{p^2.r.q^2}$ and we also define $M = y.2^{r_b}$ as the number of messages that are queried under each related-key. Through the attack, given that the round-tweak is XORed with the internal state after the MC layer, we can ignore this layer in the first round while we are constructing the structures and based the structures on Y_i of the first round (the state after MC layer). Besides, given the ciphertexts, it is possible to decrypt the last round's SB and PN layers. Besides, the MC layer is linear and we can filter the ciphertexts at the X_i of the last round. In addition, we can verify the difference of at the output of the distinguisher at W_i of the first round in the forward direction. Hence, it does not necessary to guess this round's sub-tweakey.

Following Figure 16, we prefix a round at the beginning and three rounds at the end of the dedicated distinguisher for CRAFT, which includes 14 rounds, to conduct a related-tweakey boomerang attack on 18 rounds of the cipher. In this process $r_b = 24$ bits, $m_b = 24$ bits, $r_f = 44$ bits and $m_f = 84$ bits. However, m_f and m_b have 4 bits overlap ($TK_0[13]$ which we highlighted it in purple) and the effective value of $m_f = 80$ bits. In this attack, we have $y = 2.2^{32-24}/\sqrt{2^{-58.8}} = 2^{36.9}$ for $s = 4$ and $M = y.2^{r_b} = 2^{60.9}$. The attack procedure is as follows:

1. In data collection, we construct $y = 2^{24.9}$ structures at Y_0, each structure include 2^{rb} possible values for the unknown cells to achieve $M = y.2^{r_b} = 2^{60.9}$ different plaintexts. Next, each plaintext (P) is encrypted under tweaks TK to receive the

ciphertext C. Then, (P, C) is stored in a list L_1 and also stored in a hash table H_1, indexed by the r_b bits of plaintexts.

2. Guess a value for the m_b bits of the sub-tweakeys that are involved in E_b and do as follows:

   (a) For each pair $(P_1, C_2) \in L_1$, using the guessed sub-tweakeys, we partially encrypt it up to X_1, XOR it with the intermediate difference at X_1, i.e. Δ_1, decrypt it partially using the guessed sub-tweakeys to achieve P_2 and find related $(P_2, C_2) \in H_1$ and store $(P_1, C_1), (P_2, C_2)$ in a set S_1. It is clear: $\forall\ ((P_1, C_1), (P_2, C_2)) \in S_1 : (P_1, C_1) \in L_1, (P_2, C_2) \in L_2, E_{bTK}(P_1) \oplus E_{bTK}(P_2) = \Delta_1$. Hence, the size of the set is $M = y.2^{r_b} = 2^{60.9}$.

   (b) Assuming the known cells at the output difference includes $n - r_f = 20$ bits, while we are propagating from ∇_1 toward the ciphertext, we use those $n - r_f$ bits of C_1 and $n - r_f$ bits of C_2 to put S_1 to hash table H_2. Next, for any $((P_1, C_1), (P_2, C_2)) \in S_1$ we try to find a different entry $((P_3, C_3), (P_4, C_4)) \in H_2$ such that (C_1, C_3) and (C_2, C_4) collide in $n - r_f$ known bits. We remove any entry in S_1/H_2 that does not collide at all. The remaining quartets will be $M^2.2^{-2(n-r_f)}$, i.e. $(2^{60.9})^2.2^{2.(-20)} = 2^{81.8}$.

   (c) We then initialize a list of 2^{m_f} counters, i.e. 2^{80}, each corresponds to a choice for the active m_f bits of sub-tweakeys of the last two rounds.

   (d) For each surviving quartets from Step 2b, we do the key recovery step by step as follows:

      i. For any right pair (C_1, C_3), the differences should satisfy $Y_{16}[3] = Y_{16}[7] = Y_{16}[15]$, $Y_{16}[2] = Y_{16}[10]$ and $Y_{16}[0] = Y_{16}[12]$ and also respectively $Z_{16}[3] = Z_{16}[7] = Z_{16}[15]$, $Z_{16}[2] = Z_{16}[10]$ and $Z_{16}[0] = Z_{16}[12]$.

      ii. We guess $TK_1[11]$ and $TK_1[14]$, partially decrypt $Z_{17}[11]$ and $Z_{17}[14]$ to determine whether $Z_{16}[7] = Z_{16}[3]$ for both (C_1, C_2) and (C_2, C_4). Hence, about $2^8.2^{81.8}.2^{-8} = 2^{81.8}$ quartets are remaining.

      iii. We guess $TK_1[4]$, $TK_1[12]$ and $TK_1[13]$, partially decrypt $Z_{17}[4]$ and $Z_{17}[13]$ to determine whether $Z_{16}[2] = Z_{16}[10]$ for both (C_1, C_2) and (C_2, C_4). Hence, about $2^{12}.2^{81.8}.2^{-8} = 2^{85.8}$ quartets are remaining.

      iv. Given $TK_1[4]$ and $TK_1[12]$ from the previous step, we guess $TK_1[0]$ and $TK_1[8]$ and partially decrypt the firs column of Z_{17} to determine $Z_{16}[1]$, $Z_{16}[6]$, $Z_{16}[10]$ and $Z_{16}[15]$. Next we determine whether $Z_{16}[3] = Z_{16}[15]$ for both (C_1, C_2) and (C_2, C_4). Hence, about $2^8.2^{85.8}.2^{-8} = 2^{85.8}$ quartets are remaining.

      v. Given $Z_{16}[15]$, we guess $TK_0[15]$ to determine whether $W_{15}[15] = 0xA$ for both (C_1, C_2) and (C_2, C_4). Hence, about $2^4.2^{85.8}.2^{-8} = 2^{81.8}$ quartets are remaining.

      vi. Given $Z_{16}[10]$, we guess $TK_0[10]$ to determine whether $W_{15}[10] = 0xA$ for both (C_1, C_2) and (C_2, C_4). Hence, about $2^4.2^{81.8}.2^{-8} = 2^{77.8}$ quartets are remaining.

      vii. Given $TK_1[13]$, we guess $TK_1[1]$ and $TK_1[9]$ to determine $Z_{16}[12]$ and guess $TK_1[15]$ to determine $Z_{16}[0]$. Next, we verify whether $Z_{16}[0] = Z_{16}[12]$ is satisfied for both both (C_1, C_2) and (C_2, C_4). Hence, about $2^{12}.2^{77.8}.2^{-8} = 2^{81.8}$ quartets are remaining.

      viii. Given $Z_{16}[12]$, we guess $TK_0[12]$ to determine whether $W_{15}[12] = 0xA$ for both (C_1, C_2) and (C_2, C_4). Hence, about $2^4.2^{81.8}.2^{-8} = 2^{77.8}$ quartets are remaining.

ix. Given $TK_1[14]$, we guess $TK_1[2]$ and $TK_1[10]$ to determine $Z_{16}[4]$ and $Z_{16}[13]$. We know $TK_0[13]$ from m_b and we can determine $W_{15}[13]$ and verify whether $W_{15}[13] = 0xA$ for both (C_1, C_2) and (C_2, C_4). Hence, about $2^8.2^{77.8}.2^{-8} = 2^{77.8}$ quartets are remaining.

x. Given $Z_{16}[4]$, $Z_{16}[12]$ and $TK_0[12]$, we guess $TK_0[4]$ to determine whether $W_{15}[4] = 0xA$ for both (C_1, C_2) and (C_2, C_4). Hence, about $2^4.2^{77.8}.2^{-8} = 2^{73.8}$ quartets are remaining.

xi. Given $Z_{16}[5]$, $Z_{16}[13]$ and $TK_0[13]$, we guess $TK_0[5]$ to determine whether $W_{15}[5] = 0xA$ for both (C_1, C_2) and (C_2, C_4). Hence, about $2^4.2^{73.8}.2^{-8} = 2^{69.8}$ quartets are remaining.

xii. Given $TK_1[13]$, we guess $TK_1[5]$ to determine $Z_{16}[9]$ and about $2^4.2^{69.8}.2^{-8} = 2^{73.8}$ quartets are remaining.

xiii. Given $Z_{16}[1]$, $Z_{16}[9]$, $Z_{16}[13]$ and $TK_0[13]$, we guess $TK_0[1]$ and $TK_0[9]$ to determine whether $W_{15}[1] = 0xA$ for both (C_1, C_2) and (C_2, C_4). Hence, about $2^8.2^{73.8}.2^{-8} = 2^{73.8}$ quartets are remaining, to be used to count for the 80-bit sub-tweakeys involved in forward part.

xiv. We select the first $2^{m_f - h}$ candidates for the m_f bits of the sub-tweakeys and do exhaustive search for the remaining $128 - m_b - h = 32$ bits of the master key based on each candidate, for $h = 72$.

xv. Go to item 2 if there is not the correct key.

Given that $m_b = 24$ the amount of table look-ups are $3 \times M = 2^{86.48}$, to create the lists. To do the first filtering, based on the ciphertexts, we should inverse the last round's MC-layer which costs less than $2 \times M \times \frac{1}{18} = 2^{57.81}$. We should also do a one round decryption for the survived quartets that are $2^{81.8}$ quartets and costs $2^{24} \times 2^{81.8} \times \frac{1}{18} = 2^{101.63}$. In item 2(d)xiv, the complexity is $2^{m_b} 2^{128 - m_b - h} = 2^{56}$ for $h = 72$. The complexity of the Step item 2(d)ii to Step item 2(d)xiii is less than $2^8.2^{85.8}.\frac{2}{18} = 2^{90.63}$. Hence, the time complexity will be approximately $4M + 2^{101.63} + 2^{56} + 2^{90.63} \approx 2^{101.7}$. The data complexity of the attack is $M = 2^{60.09}$ chosen plaintexts. The memory complexity is $4 \times M + 2^{m_f} = 4 \times 2^{60.09} + 2^{84} \approx 2^{84}$. The signal/noise ratio is $S_N = 2^{8.2}$ and the success probability is $P_s = 0.976$.

8 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`)), $\mathtt{DBT}^{\vDash}$, and $\mathtt{BDT}^{\dashv}$. We also applied a more advanced method to search for boomerang distinguishers. We employed this technique and provided the first security analysis of `CRAFT` against the boomerang attack in the single-tweak model, 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 the single-tweak model, for the same number of rounds. In addition, based on the 14-round boomerang distinguisher for `CRAFT`, we provided a single-tweak rectangle attack on 18 rounds of this cipher. We also applied our heuristic approach to search for boomerang distinguishers of `SKINNY` in the related-tweakey model, and we could considerably improve the best previous boomerang distinguishers of `SKINNY`-n-$2n$ and `SKINNY`-n-$3n$ for $n \in \{64, 128\}$, and thanks to the improved boomerang distinguishers, we could improve the best previous attacks on `SKINNY-64-192`, `SKINNY-128-256`, and `SKINNY-128-384`, in the related-tweakey setting. It worth noting that, our improved related-tweakey rectangle attacks on `SKINNY-64-192`, SKINNY-128-256 and SKINNY-128-384, can be directly applied for the same number of rounds of ForkSkinny-64-192, ForkSkinny-128-256, and ForkSkinny-128-384.

Acknowledgments

The experimental verifications were accomplished on the HPC cluster of Jinan University[4] and also on NRTC's infrastructure[5], jointly. The first author would like to thank Amir Hossein Firouzian for his kind help throughout the experimental verification of the results.

References

[ABC+17] Ralph Ankele, Subhadeep Banik, Avik Chakraborti, Eik List, Florian Mendel, Siang Meng Sim, and Gaoli Wang. Related-key impossible-differential attack on reduced-round skinny. In *International Conference on Applied Cryptography and Network Security*, pages 208–228. Springer, 2017.

[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.

[4] https://english.jnu.edu.cn/
[5] https://www.nrtc.science/

[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.

[GSS+20] Hao Guo, Siwei Sun, Danping Shi, Ling Sun, Yao Sun, Lei Hu, and Meiqin Wang. Differential attacks on craft exploiting the involutory s-boxes and tweak additions. *IACR Transactions on Symmetric Cryptology*, pages 119–151, 2020.

[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.

[LGS17a] Guozhen Liu, Mohona Ghosh, and Ling Song. Security Analysis of SKINNY under Related-Tweakey Settings. *IACR Trans. Symmetric Cryptol.*, 2017(3):37–72, 2017.

[LGS17b] Guozhen Liu, Mohona Ghosh, and Ling Song. Security Analysis of SKINNY under Related-Tweakey Settings. *IACR Transactions on Symmetric Cryptology*, 2017(3):37–72, Sep. 2017.

[LGS17c] Guozhen Liu, Mohona Ghosh, and Ling Song. Security analysis of skinny under related-tweakey settings (long paper). *IACR Transactions on Symmetric Cryptology*, 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.

[SGSL18] Ling Song, Jian Guo, Danping Shi, and San Ling. New MILP Modeling: Improved Conditional Cube Attacks on Keccak-Based Constructions. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part II*, volume 11273 of *Lecture Notes in Computer Science*, pages 65–95. Springer, 2018.

[SMB18] Sadegh Sadeghi, Tahereh Mohammadi, and Nasour Bagheri. Cryptanalysis of reduced round SKINNY block cipher. *IACR Trans. Symmetric Cryptol.*, 2018(3):124–162, 2018.

[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*, 88(6):1103–1126, 2020.

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

This section, describes algorithm 2, and algorithm 3.

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

```
Input: S-box S
Initialize an empty table DBCT^⊢ with 2^n × 2^n × 2^n entries;
for Δ_1 = 0 → 2^n − 1 do
    for ∇_3 = 0 → 2^n − 1 do
        for Δ_2 = 0 → 2^n − 1 do
            num = 0;
            if DDT(Δ_1, Δ_2) > 0 and BCT(Δ_2, ∇_3) > 0 then
                for ∇ = 0 → 2^n − 1 do
                    Y^∩_DDT = Y_DDT(Δ_1, Δ_2) ∩ (Y_DDT(Δ_1, Δ_2) ⊕ ∇);
                    if Y^∩_DDT ≠ ∅ then
                        num += DDT(Δ_1, Δ_2) · BDT(Δ_2, ∇_3, ∇) · #Y^∩_DDT / #Y_DDT(Δ_1, Δ_2);
                    end
                end
            end
            DBCT^⊢(Δ_1, Δ_2, ∇_3) = num;
        end
    end
end
```

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

```
Input: S-box S
Initialize an empty table DBCT^⊣ with 2^n × 2^n × 2^n entries;
for Δ_1 = 0 → 2^n − 1 do
    for ∇_3 = 0 → 2^n − 1 do
        for ∇_2 = 0 → 2^n − 1 do
            num = 0;
            if DDT(∇_2, ∇_3) > 0 and BCT(Δ_1, ∇_2) > 0 then
                for Δ = 0 → 2^n − 1 do
                    X^∩_DDT = X_DDT(∇_2, ∇_3) ∩ (X_DDT(∇_2, ∇_3) ⊕ Δ);
                    if X^∩_DDT ≠ ∅ then
                        num += DDT(∇_2, ∇_3) · DBT(Δ_1, Δ, ∇_2) · #X^∩_DDT / #X_DDT(∇_2, ∇_3);
                    end
                end
            end
            DBCT^⊣(Δ_1, ∇_2, ∇_3) = num;
        end
    end
end
```

B Probability Matrix of E_m^{7r}

$$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_e^{7r} = \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 S-box Tables

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

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

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

$$\texttt{DBT}^{\vDash}(\Delta_1, \Delta_1, \nabla_2, \Delta_2) = \texttt{DBT}(\Delta_1, \nabla_2, \Delta_2).$$

$$\texttt{BDT}^{\Dashv}(\Delta_1, \nabla_2, \nabla_2, \nabla_1) = \texttt{BDT}(\Delta_1, \nabla_2, \nabla_1).$$

D The Specification of Boomerang Distinguishers

Table 15: Specification of boomerang distinguishers for SKINNY proposed by [LGS17b] and [SQH19]. The probabilities denoted by †, correspond to the distinguishers that are obtained by extending the distinguishers proposed in [LGS17b] and [SQH19].

Version	n	#Rounds	E_0		E_m		E_1		p^2q^2r
			r_0	p	r_m	r	r_1	q	
n-$2n$	64	17	6	$2^{-2.41}$	6	$2^{-12.96}$	5	2^{-6}	$2^{-29.78}$
		18	7	$2^{-10.09}$	6	$2^{-12.96}$	5	2^{-6}	$2^{-45.14}$†
		19	7	$2^{-10.09}$	6	$2^{-12.96}$	6	$2^{-16.24}$	$2^{-65.62}$†
	128	18	7	$2^{-25.19}$	5	$2^{-11.45}$	6	2^{-8}	$2^{-77.83}$
		19	8	$2^{-35.04}$	5	$2^{-11.45}$	6	2^{-8}	$2^{-97.53}$†
		20	8	$2^{-35.04}$	5	$2^{-11.45}$	7	$2^{-23.56}$	$2^{-128.65}$†
		21	9	$2^{-56.60}$	5	$2^{-11.45}$	7	$2^{-23.56}$	$2^{-171.77}$†
n-$2n$	64	22	9	$2^{-9.83}$	5	$2^{-10.50}$	8	$2^{-6.41}$	$2^{-42.98}$
		23	10	$2^{-22.02}$	5	$2^{-10.50}$	8	$2^{-6.41}$	$2^{-67.36}$†
	128	22	9	$2^{-11.51}$	5	$2^{-9.88}$	8	$2^{-7.70}$	$2^{-48.30}$
		23	10	$2^{-25.30}$	5	$2^{-9.88}$	8	$2^{-7.70}$	$2^{-75.88}$†
		24	10	$2^{-25.30}$	5	$2^{-9.88}$	9	$2^{-23.70}$	$2^{-107.88}$†
		25	11	$2^{-42.20}$	5	$2^{-9.88}$	9	$2^{-23.70}$	$2^{-141.68}$†

Table 16: Specification of boomerang distinguisher I for 18, 19, 20 and 21 rounds of SKINNY-128-256

18: $r_0 = 6, r_m = 6, r_1 = 6, p = 2^{-3.68},\ q = 2^{-8},\ r = 2^{-19.15},\ p^2.q^2.r = 2^{-42.51}$	
$\Delta TK1 =$ 0000000000000000f000000000000000 $\Delta TK2 =$ 0000000000000000fc00000000000000	
ΔX_0 00000000000000000000000000000080	ΔX_6 00000000000000000000001000000000
$\nabla TK1 =$ 000000000000000000000000fc000000 $\nabla TK2 =$ 00000000000000000000000067000000	
∇X_{12} 00000000000000000000000000000000	∇X_{18} 00202020000000200020000c00200020
19: $r_0 = 7, r_m = 6, r_1 = 6, p = 2^{-11.68},\ q = 2^{-8},\ r = 2^{-19.15},\ p^2.q^2.r = 2^{-58.51}$	
$\Delta TK1 =$ f0000000000000000000000000000000 $\Delta TK2 =$ fc000000000000000000000000000000	
ΔX_0 02000000000020000020000020000000	ΔX_7 00000000000000000000001000000000
$\nabla TK1 =$ 00000000fc0000000000000000000000 $\nabla TK2 =$ 00000000670000000000000000000000	
∇X_{13} 00000000000000000000000000000000	∇X_{19} 00202020000000200020000c00200020
20: $r_0 = 8, r_m = 6, r_1 = 6, p = 2^{-25.08},\ q = 2^{-8},\ r = 2^{-19.15},\ p^2.q^2.r = 2^{-85.31}$	
$\Delta TK1 =$ 000000000000000000f0000000000000 $\Delta TK2 =$ 000000000000000000fe000000000000	
ΔX_0 00000100010100010100010000d50000	ΔX_8 00000000000000000000001000000000
$\nabla TK1 =$ 00000000000000000000fc0000000000 $\nabla TK2 =$ 00000000000000000000330000000000	
∇X_{14} 00000000000000000000000000000000	∇X_{20} 00202020000000200020000c00200020
21: $r_0 = 8, r_m = 6, r_1 = 7, p = 2^{-25.08},\ q = 2^{-23.56},\ r = 2^{-19.15},\ p^2.q^2.r = 2^{-116.43}$	
$\Delta TK1 =$ 000000000000000000f0000000000000 $\Delta TK2 =$ 000000000000000000fe000000000000	
ΔX_0 00000100010100010100010000d50000	ΔX_8 00000000000000000000001000000000
$\nabla TK1 =$ 00000000000000000000fc0000000000 $\nabla TK2 =$ 00000000000000000000330000000000	
∇X_{14} 00000000000000000000000000000000	∇X_{21} 80910000008080808011008000918000

Table 17: Specification of boomerang distinguisher I for 22 to 25 rounds of SKINNY-128-384

22: $r_0 = 8, r_m = 6, r_1 = 8, p = 2^{-3},\ q = 2^{-7},\ r = 2^{-20.57},\ p^2.q^2.r = 2^{-40.57}$	
$\Delta TK1 =$ 0000000000000000002a000000000000 $\Delta TK2 =$ 00000000000000000079000000000000 $\Delta TK3 =$ 00000000000000000033000000000000	
ΔX_0 00000000000000000000000000080000	∇X_8 00000000000000000000004000000000
$\nabla TK1 =$ 00000000000000000000540000000000 $\nabla TK2 =$ 000000000000000000000f0000000000 $\nabla TK3 =$ 00000000000000000000f80000000000	
∇X_{14} 00000000000000000000000000000000	∇X_{22} 10100010001000000000071000100010
23: $r_0 = 9, r_m = 6, r_1 = 8, p = 2^{-10.95},\ q = 2^{-7},\ r = 2^{-20.57},\ p^2.q^2.r = 2^{-56.47}$	
$\Delta TK1 =$ 002a0000000000000000000000000000 $\Delta TK2 =$ 00790000000000000000000000000000 $\Delta TK3 =$ 00330000000000000000000000000000	
ΔX_0 00110000020000000000000200000200	ΔX_9 00000000000000000000004000000000
$\nabla TK1 =$ 00005400000000000000000000000000 $\nabla TK2 =$ 00000f00000000000000000000000000 $\nabla TK3 =$ 0000f800000000000000000000000000	
∇X_{15} 00000000000000000000000000000000	∇X_{23} 10100010001000000000071000100010
24: $r_0 = 10, r_m = 6, r_1 = 8, p = 2^{-26.41},\ q = 2^{-7},\ r = 2^{-20.57},\ p^2.q^2.r = 2^{-87.39}$	
$\Delta TK1 =$ 0000000000000000000000000000002a $\Delta TK2 =$ 0000000000000000000000000000003c $\Delta TK3 =$ 00000000000000000000000000000067	
ΔX_0 80000000008080808000800000000c80	ΔX_{10} 00000000000000000000004000000000
$\nabla TK1 =$ 00000000000000005400000000000000 $\nabla TK2 =$ 00000000000000008700000000000000 $\nabla TK3 =$ 0000000000000000f000000000000000	
∇X_{16} 00000000000000000000000000000000	∇X_{24} 10100010001000000000071000100010
25: $r_0 = 10, r_m = 6, r_1 = 9, p = 2^{-26.41},\ q = 2^{-21.60},\ r = 2^{-20.57},\ p^2.q^2.r = 2^{-116.59}$	
$\Delta TK1 =$ 0000000000000000000000000000002a $\Delta TK2 =$ 0000000000000000000000000000003c $\Delta TK3 =$ 00000000000000000000000000000067	
ΔX_0 80000000008080808000800000000c80	ΔX_{10} 00000000000000000000004000000000
$\nabla TK1 =$ 00000000000000005400000000000000 $\nabla TK2 =$ 00000000000000008700000000000000 $\nabla TK3 =$ 0000000000000000f000000000000000	
∇X_{16} 00000000000000000000000000000000	∇X_{25} 08104040505000400840400058100040

Table 18: Specification of boomerang distinguisher II for 18 and 19 rounds of SKINNY-64-128

$18: r_0 = 6, r_m = 6, r_1 = 6, p = 2^{-2.41},\ q = 2^{-7.68},\ r = 2^{-17.72},\ p^2.q^2.r = 2^{-37.90}$			
$\Delta TK1$	000000000C000000	$\Delta TK2$	000000000F000000
ΔX_0	0000000000000800	ΔX_6	0000000004000000
$\nabla TK1$	0000000000000040	$\nabla TK2$	0000000000000070
∇X_{12}	0000000000000000	∇X_{18}	3101010000710101
$19: r_0 = 7, r_m = 6, r_1 = 6, p = 2^{-9},\ q = 2^{-7.68},\ r = 2^{-17.72},\ p^2.q^2.r = 2^{-51.08}$			
$\Delta TK1$	0C00000000000000	$\Delta TK2$	0F00000000000000
ΔX_0	0200100000010010	ΔX_7	0000000004000000
$\nabla TK1$	0000004000000000	$\nabla TK2$	0000007000000000
∇X_{13}	0000000000000000	∇X_{19}	3101010000710101

Table 19: Specification of boomerang distinguisher II for 18, 19, 20 and 21 rounds of SKINNY-128-256

$18: r_0 = 6, r_m = 6, r_1 = 6, p = 2^{-3},\ q = 2^{-7.29},\ r = 2^{-20.19},\ p^2.q^2.r = 2^{-40.77}$	
$\Delta TK1 =$ 00000000000000000002000000000000 $\Delta TK2 =$ 00000000000000000008000000000000	
ΔX_0 00000000000000000000000000200000	ΔX_6 00000000000000000006000000000000
$\nabla TK1 =$ 0000000000000000000000000000f800 $\nabla TK2 =$ 0000000000000000000000000000cf00	
∇X_{12} 00000000000000000000000000000000	∇X_{18} 40400040004000000000184000400040
$19: r_0 = 7, r_m = 6, r_1 = 6, p = 2^{-11.78},\ q = 2^{-7.29},\ r = 2^{-20.19},\ p^2.q^2.r = 2^{-58.33}$	
$\Delta TK1 =$ 00020000000000000000000000000000 $\Delta TK2 =$ 00800000000000000000000000000000	
ΔX_0 00200000010000000000000100000100	ΔX_7 00000000000000000006000000000000
$\nabla TK1 =$ 00000000000f80000000000000000000 $\nabla TK2 =$ 00000000000cf0000000000000000000	
∇X_{13} 00000000000000000000000000000000	∇X_{19} 40400040004000000000184000400040
$20: r_0 = 8, r_m = 6, r_1 = 6, p = 2^{-27.32},\ q = 2^{-7.29},\ r = 2^{-20.19},\ p^2.q^2.r = 2^{-89.41}$	
$\Delta TK1 =$ 00000000000000000000000000000002 $\Delta TK2 =$ 00000000000000000000000000000040	
ΔX_0 04000000000404040400040000000104	ΔX_8 00000000000000000006000000000000
$\nabla TK1 =$ 000000000000000000000000f8000000 $\nabla TK2 =$ 00000000000000000000000067000000	
∇X_{14} 00000000000000000000000000000000	∇X_{20} 40400040004000000000184000400040
$21: r_0 = 8, r_m = 6, r_1 = 7, p = 2^{-27.32},\ q = 2^{-19.62},\ r = 2^{-20.19},\ p^2.q^2.r = 2^{-114.07}$	
$\Delta TK1 =$ 00000000000000000000000000000002 $\Delta TK2 =$ 00000000000000000000000000000040	
ΔX_0 04000000000404040400040000000104	ΔX_8 00000000000000000006000000000000
$\nabla TK1 =$ 000000000000000000000000f8000000 $\nabla TK2 =$ 00000000000000000000000067000000	
∇X_{14} 00000000000000000000000000000000	∇X_{21} 40000404040400044004040044000004

Table 20: A right quartet satisfying the boomerang distinguisher I for 18 rounds of SKINNY-64-128

k_1	3494d8c130c487bd 6e42d1c2f71ef823		
k_2	3494d8c1f0c487bd 6e42d1c2071ef823		
k_3	3494d8c130c4c7bd 6e42d1c2f71e8823		
k_4	3494d8c1f0c4c7bd 6e42d1c2071e8823		
p_1	98adaabd5cfff8a7	c_1	8323a64a80b77a4f
p_2	98adaabd5cfff8af	c_2	ed42621b9cf1fa1c
p_3	c3e70c62cf12e3eb	c_3	8777a64e84b07e4b
p_4	c3e70c62cf12e3e3	c_4	e916621f98f6fe18

Table 21: A right quartet satisfying boomerang distinguisher I for 22 rounds of SKINNY-64-192

k_1	15c9a8301861cb0dc1ecf6b8409489b635f08b1c4c019d55		
k_2	15c9a8301f61cb0dc1ecf6b8439489b635f08b1c47019d55		
k_3	15c9a8301841cb0dc1ecf6b840a489b635f08b1c4cd19d55		
k_4	15c9a8301f41cb0dc1ecf6b843a489b635f08b1c47d19d55		
p_1	54d75682eeeba6b7	c_1	a91de693d94c08f9
p_2	54d75682eeeba7b7	c_2	0a4c8579b44ae917
p_3	c74561c99f7f6a94	c_3	ff18e093d9090efc
p_4	c74561c99f7f6b94	c_4	5c498379b40fef12

Table 22: A right quartet satisfying boomerang distinguisher I for 22 rounds of SKINNY-128-384

k_1		k_2	
2c2c5fc838b8a48195e627dd67da0590 0ffb5fb4094b88996352a459dacc8706 f9e6ce319e72b23359da10c0b41550c3		2c2c5fc838b8a48195cc27dd67da0590 0ffb5fb4094b8899632ba459dacc8706 f9e6ce319e72b23359e910c0b41550c3	
k_3		k_4	
2c2c5fc838b8a48195e673dd67da0590 0ffb5fb4094b88996352ab59dacc8706 f9e6ce319e72b23359dae8c0b41550c3		2c2c5fc838b8a48195cc73dd67da0590 0ffb5fb4094b8899632bab59dacc8706 f9e6ce319e72b23359e9e8c0b41550c3	
p_1	8b68483d7e54a1140cb4ad56f5cfacc9	c_1	23820cc9011c130afeac8b879c7967aa
p_2	8b68483d7e54a1140cb4ad56f5c7acc9	c_2	8325b6082c46116050ed125f66cb9f15
p_3	9442ed20a6934b4c50925ffcf0d0526e	c_3	33920cd9010c130afeac8c979c6967ba
p_4	9442ed20a6934b4c50925ffcf0d8526e	c_4	9335b6182c56116050ed154f66db9f05

Table 23: A right quartet satisfying boomerang distinguisher II for 18 rounds of SKINNY-128-256

k_1	a733ade942312ce0503c3e528aa0c417cb47c7dad8bcefbc3f8131b6375d98de		
k_2	a733ade942312ce0503e3e528aa0c417cb47c7dad8bcefbc3f0131b6375d98de		
k_3	a733ade942312ce0503c3e528aa03c17cb47c7dad8bcefbc3f8131b6375d57de		
k_4	a733ade942312ce0503e3e528aa03c17cb47c7dad8bcefbc3f0131b6375d57de		
p_1	8d9a13adfc4d3d8046145385edc26a21	c_1	eb871cd1bbd5c3de4503f64d3b6fdb11
p_2	8d9a13adfc4d3d8046145385ede26a21	c_2	eb9d9bdfaaeded28d773172b082e82de
p_3	91b30cc8898c0324631b80319a5745de	c_3	abc71c91bb95c3de4503ee0d3b2fdb51
p_4	91b30cc8898c0324631b80319a7745de	c_4	abdd9b9faaaded28d7730f6b086e829e