Impossible Boomerang Attacks Revisited

Applications to Deoxys-BC, Joltik-BC and SKINNY

Jianing Zhang, Haoyang Wang\(^{(es)}\) and Deng Tang

Shanghai Jiao Tong University, Shanghai, China

\{zhangjn,haoyang.wang,dengtang\}@sjtu.edu.cn

Abstract. The impossible boomerang (IB) attack was first introduced by Lu in his doctoral thesis and subsequently published at DCC in 2011. The IB attack is a variant of the impossible differential (ID) attack by incorporating the idea of the boomerang attack. In this paper, we revisit the IB attack, and introduce the incompatibility of two characteristics in boomerang to the construction of an IB distinguisher. With our methodology, all the constructions of IB distinguisher are represented in a unified manner. Moreover, we show that the related-(twea)key IB distinguishers possess more freedom than the ones of ID so that it can cover more rounds.

We also propose a new tool based on Mixed-Integer Quadratically-Constrained Programming (MIQCP) to search for IB attacks. To illustrate the power of the IB attack, we mount attacks against three tweakable block ciphers: Deoxys-BC, Joltik-BC and SKINNY. For Deoxys-BC, we propose a related-tweakey IB attack on 14-round Deoxys-BC-384, which improves the best previous related-tweakey ID attack by 2 rounds, and we improve the data complexity of the best previous related-tweakey ID attack on 10-round Deoxys-BC-256. For Joltik-BC, we propose the best attacks against 10-round Joltik-BC-128 and 14-round Joltik-BC-192 with related-tweakey IB attack. For SKINNY-\(n\)-3\(n\), we propose a 27-round related-tweakey IB attack, which improves both the time and the memory complexities of the best previous ID attack. We also propose the first related-tweakey IB attack on 28-round SKINNY-\(n\)-3\(n\), which improves the previous best ID attack by one round.

Keywords: Impossible Boomerang Attack · MIQCP · Deoxys-BC · Joltik-BC · SKINNY

1 Introduction

Differential cryptanalysis, one of the most important attacks on block ciphers, was first introduced by Biham and Shamir in 1990 [BS91], and has since been widely studied. The idea is to study the propagation of differences inside an iterated block cipher and construct a high-probability differential. An adversary can use this high-probability differential to recover (part of) the key bits. Built upon the foundation of differential attacks, various derivative cryptanalytic methods have been developed, with impossible differential attacks [BBS99a] and boomerang attacks [Wag99] being representative examples.

The impossible differential (ID) attack was first proposed independently by Knudsen [Knu98] and Biham [BBS99a]. Unlike traditional differential cryptanalysis, the impossible differential attack uses a differential with a probability of 0. The adversary can use this impossible differential to eliminate wrong key bits. Since its introduction, the impossible differential attack has gained widespread attention and has effectively targeted some block ciphers. The most significant step of the impossible differential attack is to construct a distinguisher that covers as many rounds as possible, and the typical way is...
to use the *miss-in-the-middle* technique [BBS99b]. In the miss-in-the-middle technique, cryptanalysts try to track the propagation of input and output differences from the encryption and decryption directions, respectively. If there is a contradiction at certain points in between, then an impossible differential has been identified.

The boomerang attack was first introduced by Wagner [Wag99], sharing some similarities with the impossible differential attack in that it involves cascading two characteristics. In the boomerang attack, two short high-probability characteristics are combined to form a longer distinguisher, aiming to achieve a better attack.

At INDOCRYPT 2003, Kim *et al.* [KHS+03] proposed the first computer-aided tool for searching impossible differentials called the $\mathcal{U}$-method. Later, some improved methods such as the WW-method [WW12] and the UID-method [LLWG14] were introduced by Wu *et al.* in 2012 and Luo *et al.* in 2014, respectively. Mixed-integer linear programming (MILP) was introduced to search characteristics by Mouha *et al.* in 2011 [MWGP11], and later was refined by Sun *et al.* in 2014 [SHW+14]. Based on the feasibility of the model, Cui *et al.* [CJF+16] was the first to apply MILP to the search for impossible differential distinguishers. At CRYPTO 2016, Derbez and Fouque [DF16] developed a new Generalized Demirci-Seçuk search algorithm for a large class of block ciphers and applied the algorithm to search for impossible differential attacks. At EUROCRYPT 2017, Sasaki *et al.* [ST17] applied MILP to block ciphers with 8-bit S-boxes and tried to find contradictions from linear layers. In recent works, [ARS+22, HPW22, CLH+23] all use the solvability of the MILP/SMT problems to determine IDs. In [HSE23], Hadipour *et al.* proposed a generic CP-based model to find full impossible differential attacks without using the infeasibility.

For the automatic searching tools for the boomerang attack and its variants, Cid *et al.* [CHP+17] in 2017 firstly introduced MILP to characterize the ladder switch in the boomerang distinguishers for Deoxys-BC. Later, Zhao *et al.* [ZDJ19] used the MILP method to search for boomerang distinguishers of Deoxys-BC including BDT effect. Delaune *et al.* [DDV20] described a new MILP model to search for truncated boomerang characteristics and a CP model to instantiate the truncated boomerang characteristics for SKINNY with the effects of DDT, BCT, UBCT, etc. At EUROCRYPT 2022 [DQSW22], Dong *et al.* managed to search rectangle distinguishers by proposing a new key guessing strategy with MILP and CP models. In [DEFN22], Derbez *et al.* extended the MILP model to search for a complete boomerang attack, which is applied to the attack on AES-192.

Building upon the foundations of the impossible differential attack and the boomerang attack, we think it is an interesting idea to combine them together, with the name *impossible boomerang attack*. The impossible boomerang (IB) attack was firstly proposed by Lu in his doctoral thesis [Lu08] and subsequently published in [Lu11]. In [Lu08, Lu11], the author introduced the definition and extended its application to the related-key scenario. With this new technique, Lu proposed several single-key attacks on 6-round AES-128 and 7-round AES-192/AES-256, and related-key attacks on 8-round AES-192 and 9-round AES-256. In [CY09], Choy and Yap adapted the $\mathcal{U}$-method [KHS+03] to align with the impossible boomerang attack and computed the maximum length of impossible boomerang distinguishers for ciphers with MARS-like [BCD+98]/RC6-like [RRSY98] structure.

**Our Contributions.** In this work, we revisit the impossible boomerang attack, providing a systematic overview of the contradiction conditions, a comparison with the impossible differential attack, and the key recovery process under the related-key setting. Based on Mixed-Integer Quadratically-Constrained Programming (MIQCP), we propose a new automatic searching tool for impossible boomerang attacks and successfully apply it to three block ciphers: Deoxys-BC, Joltik-BC and SKINNY. The main results are summarized in Tables 1 and 2.
We revisit the impossible boomerang attack proposed in \cite{Lu11}. There is a lack of an impossible differential attack against some attacks listed in Table 1: \cite{Deoxys-128-384}. All the attacks listed below are under related-(twea)key settings.

<table>
<thead>
<tr>
<th>Cipher</th>
<th>#R</th>
<th>Key Size</th>
<th>Tweak Size</th>
<th>Attack</th>
<th>#K</th>
<th>Data</th>
<th>Time</th>
<th>Memory</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joltik-BC-128</td>
<td>10</td>
<td>&gt; 109</td>
<td>&lt; 19</td>
<td>ID</td>
<td>2</td>
<td>20</td>
<td>2100.7</td>
<td>2104</td>
<td>[ZD18]</td>
</tr>
<tr>
<td>Joltik-BC-192</td>
<td>11</td>
<td>= 128</td>
<td>= 64</td>
<td>MITM</td>
<td>2</td>
<td>0.5</td>
<td>2123</td>
<td>2141</td>
<td>[LC21]</td>
</tr>
<tr>
<td>Deoxys-BC-256</td>
<td>13</td>
<td>= 128</td>
<td>= 64</td>
<td>IB</td>
<td>4</td>
<td>2.7</td>
<td>2135.8</td>
<td>2144</td>
<td>Section 4.3</td>
</tr>
<tr>
<td>Deoxys-BC-384</td>
<td>14</td>
<td>&gt; 183</td>
<td>&lt; 9</td>
<td>IB</td>
<td>4</td>
<td>2.6</td>
<td>2173.5</td>
<td>2182</td>
<td>Section 4.4</td>
</tr>
<tr>
<td>Deoxys-BC-192</td>
<td>9</td>
<td>= 128</td>
<td>= 128</td>
<td>ID</td>
<td>2</td>
<td>2118</td>
<td>2190</td>
<td>2182</td>
<td>[MMS18]</td>
</tr>
<tr>
<td>Deoxys-BC-256</td>
<td>10</td>
<td>&gt; 186</td>
<td>&lt; 70</td>
<td>IB</td>
<td>4</td>
<td>2132.5</td>
<td>2186.46</td>
<td>2181.6</td>
<td>Section 4.3</td>
</tr>
<tr>
<td>Deoxys-BC-384</td>
<td>11</td>
<td>&gt; 222</td>
<td>&lt; 34</td>
<td>Rect.</td>
<td>4</td>
<td>2126.78</td>
<td>2222.49</td>
<td>2128</td>
<td>[SZY*22]</td>
</tr>
<tr>
<td>Deoxys-BC-192</td>
<td>12</td>
<td>&gt; 329</td>
<td>&lt; 55</td>
<td>ID</td>
<td>2</td>
<td>2135.5</td>
<td>2190.5</td>
<td>2192</td>
<td>Appendix C</td>
</tr>
<tr>
<td>Deoxys-BC-256</td>
<td>13</td>
<td>= 256</td>
<td>= 128</td>
<td>IB</td>
<td>4</td>
<td>2133.6</td>
<td>2163.6</td>
<td>2162</td>
<td>Section 4.4</td>
</tr>
<tr>
<td>Deoxys-BC-384</td>
<td>14</td>
<td>&gt; 368</td>
<td>&lt; 16</td>
<td>IB</td>
<td>4</td>
<td>2130.9</td>
<td>2190</td>
<td>2120</td>
<td>Section 4.5</td>
</tr>
<tr>
<td>Deoxys-BC-192</td>
<td>15</td>
<td>&gt; 374</td>
<td>&lt; 13</td>
<td>Rect.</td>
<td>4</td>
<td>2115</td>
<td>2171.7</td>
<td>2128</td>
<td>[SYC^+24]</td>
</tr>
<tr>
<td>SKINNY-64-192</td>
<td>27</td>
<td>&gt; 189</td>
<td>&lt; 6</td>
<td>ID</td>
<td>2</td>
<td>283</td>
<td>2189</td>
<td>2184</td>
<td>\cite{LGS17}</td>
</tr>
<tr>
<td>SKINNY-128-256</td>
<td>27</td>
<td>&gt; 189</td>
<td>&lt; 6</td>
<td>ID</td>
<td>2</td>
<td>283</td>
<td>2189</td>
<td>2184</td>
<td>\cite{LGS17}</td>
</tr>
<tr>
<td>SKINNY-128-384</td>
<td>27</td>
<td>&gt; 357</td>
<td>&lt; 22</td>
<td>IB</td>
<td>4</td>
<td>2130.8</td>
<td>2230.8</td>
<td>2232</td>
<td>[HSE23]</td>
</tr>
<tr>
<td>SKINNY-128-192</td>
<td>31</td>
<td>&gt; 187</td>
<td>&lt; 15</td>
<td>Rect.</td>
<td>4</td>
<td>2115</td>
<td>2171.7</td>
<td>2128</td>
<td>[DQS22]</td>
</tr>
<tr>
<td>SKINNY-128-256</td>
<td>27</td>
<td>&gt; 357</td>
<td>&lt; 22</td>
<td>IB</td>
<td>4</td>
<td>2130.8</td>
<td>2230.8</td>
<td>2232</td>
<td>[HSE23]</td>
</tr>
<tr>
<td>SKINNY-128-384</td>
<td>27</td>
<td>&gt; 357</td>
<td>&lt; 22</td>
<td>IB</td>
<td>4</td>
<td>2130.8</td>
<td>2230.8</td>
<td>2232</td>
<td>[HSE23]</td>
</tr>
</tbody>
</table>

Some attacks listed are beyond full-codebook attacks. For an introduction to beyond full-codebook attacks and the computation of the corresponding data complexity, please refer to the remark in Section 3.4.2. The preceding column "#K" refers to the number of related keys used in the attack.

We revisit the impossible boomerang attack proposed in \cite{Lu11} and introduce the applicable Generalized Boomerang Framework (GBF). For the impossible boomerang, we introduce the generation of contradictions and its advantages over the impossible differential, and then give two key recovery methods. In addition, we propose a MIQCP-based tool to search for complete impossible boomerang attacks.

For Deoxys-BC, we provide a related-tweakey impossible boomerang attack against 10-round Deoxys-BC-256 and a related-tweakey impossible boomerang attack against 14-round Deoxys-BC-384. As a demonstration of the effectiveness of the impossible boomerang attack, our attack against 14-round Deoxys-BC-384 surpasses the previous best related-tweakey impossible differential attack by two rounds. The distinguishers used in our attacks can cover 1 or 2 more rounds than the previous related-tweakey impossible distinguishers.

For Joltik-BC-128, we propose an improved 10-round related-tweakey impossible
Table 2: Summary of cryptanalytic distinguishers.

<table>
<thead>
<tr>
<th>Cipher</th>
<th>#Rounds</th>
<th>Distinguisher</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joltik-BC-128</td>
<td>6</td>
<td>ID</td>
<td>[CLH]</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>IB</td>
<td>Table 8</td>
</tr>
<tr>
<td>Joltik-BC-192</td>
<td>7</td>
<td>ID</td>
<td>[CLH]</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>IB</td>
<td>Table 9</td>
</tr>
<tr>
<td>Deoxys-BC-256</td>
<td>6</td>
<td>ID</td>
<td>[ZDW]</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>IB</td>
<td>Table 6</td>
</tr>
<tr>
<td>Deoxys-BC-384</td>
<td>7</td>
<td>ID</td>
<td>Appendix C</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>IB</td>
<td>Table 7</td>
</tr>
<tr>
<td>SKINNY-64-192</td>
<td>16</td>
<td>ID</td>
<td>[LGS]</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>ID</td>
<td>Figure 15</td>
</tr>
<tr>
<td>SKINNY-128-384</td>
<td>16</td>
<td>ID</td>
<td>[LGS]</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>ID</td>
<td>[HSE]</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>IB</td>
<td>Figures 14 and 16 †</td>
</tr>
</tbody>
</table>

† The distinguisher shown in Figure 16 has been proved to be wrong in [BL].

boomerang attack compared to the previous best attack. For Joltik-BC-192, we present the best related-tweakey attack against 14-round Joltik-BC-192. The distinguishers used in our attacks can cover 1 or 2 more rounds than the previous related-tweakey impossible distinguishers.

- For SKINNY-n-3n, we present a 27-round related-tweakey impossible boomerang attack, with improved time and memory complexity compared to the previous best related-tweakey impossible attack. We also provide the first 28-round related-tweakey impossible boomerang attack, which extends one more round than the previous best related-tweakey impossible attack.

Organization. In Section 2, we give a brief description of boomerang attacks, sandwich attacks, boomerang connectivity table (BCT) and MIQCP, followed by the notations used in this work. In Section 3, we revisit the impossible boomerang attack, then describe a new automatic search tool, and propose two key recovery methods for impossible boomerang attacks. We introduce the new cryptanalytic results on Joltik-BC and Deoxys-BC in Section 4. The new cryptanalytic results on SKINNY-n-3n are provided in Section 5. Finally, Section 6 concludes this paper.

2 Preliminaries

2.1 Boomerang Attacks

The boomerang attack [Wag99] is an extension of the traditional differential cryptanalysis proposed by Wagner, which allows the adversary to use two short characteristics of high probability to construct a long one.

The boomerang attack regards the targeted cipher \( E : \{0, 1\}^n \times \{0, 1\}^k \rightarrow \{0, 1\}^n \) as a cascade of two sub-ciphers \( E = E_1 \circ E_0 \), where there are two short differentials \( \alpha \rightarrow \beta \).
and $\gamma \rightarrow \delta$ with probability $p$ and $q$ for $E_0$ and $E_1$, respectively, as depicted in Figure 1. The probability of the boomerang distinguisher is

$$\Pr[E^{-1}(E(P) \oplus \delta) \oplus E^{-1}(E(P \oplus \alpha) \oplus \delta) = \alpha] = p^2 q^2.$$  

The boomerang attack is an adaptive chosen plaintext and ciphertext attack, with the following process:

- Encrypt pair of plaintexts $(p_1, p_2)$ s.t. $p_1 \oplus p_2 = \alpha$ into $(c_1, c_2)$ respectively.
- Get $p_3, p_4$ by decrypting $c_3 = c_1 \oplus \delta$ and $c_4 = c_2 \oplus \delta$ respectively.
- Check whether $p_3 \oplus p_4 = \alpha$.

### 2.2 Sandwich Attacks and Boomerang Connectivity Table

In [DKS10], Dunkelman et al. proposed the sandwich attack (see in Figure 2) to exploit the dependence between two differentials of the boomerang distinguisher, which divides a cipher $E$ into three sub-ciphers: $E = E_1 \circ E_m \circ E_0$. The probability of the sandwich distinguisher is

$$\Pr[E^{-1}(E(P) \oplus \delta) \oplus E^{-1}(E(P \oplus \alpha) \oplus \delta) = \alpha] = \tilde{p}^2 \tilde{q}^2 r,$$

where $\tilde{p}$ (resp. $\tilde{q}$) is the probability of the differential of $E_0$ ($E_1$), and $r$ is the probability of generating a right quartet for $E_m$.

In [CHP+18], Cid et al. proposed a tool, named Boomerang Connectivity Table (BCT), to calculate $r$ when $E_m$ is composed of a single S-box layer. The BCT well captures the previous observations including incompatibility [Mur11], the S-box switch and the ladder switch [BK09], and gives more new insights into the boomerang switch. Later, the methods describing multi-round transitions of the boomerang have been proposed by many works [WP19, SQH19, DDV20, HBS21]. These works indicate that a thorough investigation on the construction of the middle layer can lead to a better boomerang attack. Here, we provide the definition of the BCT.

**Definition 1 ([CHP+18])**. Let $S$ be an $n$-bit bijective S-box, and $\Delta_i, \nabla_o \in \mathbb{F}_2^n$. The BCT of $S$ is given by a $2^n \times 2^n$ table, in which the entry for $(\Delta_i, \nabla_o)$ is given by:

$$\text{BCT} (\Delta_i, \nabla_o) = \# \{ x \in \mathbb{F}_2^n | S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla_o) = \Delta_i \}.$$  

---

**Figure 1**: Boomerang attack  
**Figure 2**: Sandwich attack
2.3 Mixed-Integer Quadratically-Constrained Programming

Mixed-Integer Programming (MIP) is a category of mathematical optimization problems that includes Mixed-Integer Linear Programming (MILP), Mixed-Integer Quadratic Programming (MIQP), Mixed-Integer Quadratically-Constrained Programming (MIQCP), etc. These problems were initially applied in the field of Operations Research. Recently, their applications in cryptanalysis have been extensively studied, especially the MILP problem. Our new model employs MIQCP, which involves quadratic constraints and quadratic objective functions. MIQCP has been previously used to model the differential-linear attack in [BGG+23] and [LJC23]. We use the Gurobi solver$^1$ to solve the MIQCP model in this paper. Here, we provide the mathematical definition of MIQCP.

**Definition 2 ([BS12]).** A Mixed-Integer Quadratically-Constrained Programming (MIQCP) is a problem, where the objective function and constraints can both include linear and quadratic terms, and some or all the decision variables are integer variables. The mathematical definition can be expressed as follows:

$$\begin{align*}
\text{min or max} \quad & x^T C x + c^T x \\
\text{s.t.} \quad & x^T A_k x + a_k^T x \leq b_k \quad \forall k = 1, \ldots, m \\
& x \in \mathbb{R}^n : \quad l \leq x \leq u \\
& x_i \in \mathbb{Z} \quad \forall i \in I, I \subseteq N := \{1, \ldots, n\}
\end{align*}$$

where $(C, c) \in S^n \times \mathbb{R}^n$, $(A_k, a_k, b_k) \in S^n \times \mathbb{R}^n \times \mathbb{R}$ for all $k = 1, \ldots, m$, $(l, u) \in (\mathbb{R} \cup \{-\infty\})^n \times (\mathbb{R} \cup \{+\infty\})^n$ and $S^n$ is the set of all $n \times n$ symmetric matrices.

It is worth noting that the distinction between MIQCP and MIQP lies in the types of constraints and objective function. MIQP can only use linear constraints and a quadratic objective function. MIQCP must include quadratic constraints, and the objective function does not matter.

2.4 Notations

The following notations are followed throughout the rest of the paper.

- $STK_r$: Subtweakey of round $r$
- $cSTK_r$: Equivalent subtweakey of round $r$
- $X_r$: Internal state before SubBytes (resp. SubCells) in round $r$ for Deoxys-BC (resp. SKINNY)
- $Y_r$: Internal state before ShiftRows (resp. AddRoundTweakey) in round $r$ for Deoxys-BC (resp. SKINNY)
- $Z_r$: Internal state before MixColumns (resp. ShiftRows) in round $r$ for Deoxys-BC (resp. SKINNY)
- $W_r$: Internal state after MixColumns (resp. ShiftRows) in round $r$ for Deoxys-BC (resp. SKINNY)
- $\Delta X$: Difference of a state $X$ in the upper trail
- $\nabla X$: Difference of a state $X$ in the lower trail
- $X_r[i]$: $i$-th cell of a state $X$ in round $r$
- $X_r[i, \ldots, k]$: $i$-th cell, ..., $k$-th cell of a state $X$ in round $r$

$^1$Gurobi: www.gurobi.com
3 Revisiting the Impossible Boomerang Attack

3.1 Definition of the Impossible Boomerang Distinguisher

The impossible boomerang attack was first introduced by Lu in [Lu08, Lu11], and the definition is given as follows.

**Definition 3.** Suppose \( E : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n \) is a block cipher and \( K \in \{0,1\}^k \) is a key for \( E \). If there exist a quartet \((\alpha, \alpha', \delta, \delta') \in \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n \) satisfying
\[
\forall X \in \mathbb{F}_2^n, \quad \Pr[E^{-1}_K(E_K(X) \oplus \delta) \oplus E^{-1}_K(E_K(X \oplus \alpha) \oplus \delta') = \alpha'] = 0,
\]
then \((\alpha, \alpha', \delta, \delta')\) is called an impossible boomerang distinguisher, written \((\alpha, \alpha') \nrightarrow (\delta, \delta')\).

The paper [Lu11] also describes how to construct an impossible boomerang distinguisher. Specifically, the distinguisher consists of four characteristics of probability 1:
- \( \alpha \rightarrow \beta \) with probability 1 and \( \alpha' \rightarrow \beta' \) with probability 1 for \( E_0 \);
- \( \delta \rightarrow \gamma \) with probability 1 and \( \delta' \rightarrow \gamma' \) with probability 1 for \( E_1^{-1} \),
where \( \beta, \beta', \gamma, \gamma' \) satisfy the condition \( \beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0 \). The distinguisher is depicted in Figure 3.

Figure 3: Impossible Boomerang Distinguisher in [Lu11]

Figure 4: Difference transition in the single S-box layer

3.2 Generalized Boomerang Framework

As we can see from Definition 3, the impossible boomerang distinguisher allows two symmetric characteristics used in \( E_0 \) to be different, as well as the ones in \( E_1 \). The same idea has been briefly mentioned in [HBS21]. In this paper, to capture this unusual construction of boomerang distinguishers, we propose the **Generalized Boomerang Framework** (GBF). Similar to the traditional boomerang attack, the GBF divides the targeted cipher as two sub-ciphers \( E = E_1 \circ E_0 \), but there are two differentials \( \alpha \xrightarrow{p_1} \beta, \alpha' \xrightarrow{p_2} \beta' \) for \( E_0 \) and two differentials \( \gamma \xrightarrow{q_1} \delta, \gamma' \xrightarrow{q_2} \delta' \) for \( E_1 \). The traditional boomerang is the GBF under the conditions where \( \alpha = \alpha', \beta = \beta', \gamma = \gamma' \), and \( \delta = \delta' \). In GBF, structures excluding traditional boomerangs are referred to as asymmetric boomerangs. The probability of the generalized boomerang distinguisher is \( p_1p_2q_1q_2 \). Similarly, we can also generalize the sandwich distinguisher.

The BCT can also be extended to the GBF, which was first proposed in [LWL22] and named the **Generalized Boomerang Connectivity Table** (GBCT).
Definition 4 ([LWL22]). Let $S$ be an $n$-bit bijective S-box, and $\Delta_i, \Delta'_i, \nabla_o, \nabla'_o \in \mathbb{F}_2^n$. The GBCT of $S$ is given by a four-dimensional table, in which the entry for $(\Delta_i, \Delta'_i, \nabla_o, \nabla'_o)$ is given by:

$$\text{GBCT}(\Delta_i, \Delta'_i, \nabla_o, \nabla'_o) = \#\{x \in \mathbb{F}_2^n | S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla'_o) = \Delta'_i\}.$$

Other generalized tables for multiple rounds in GBF are listed in Appendix A.

3.3 Construct Impossible Boomerang Attacks

The core step for the impossible boomerang attack is to find a boomerang distinguisher that never returns back. One direction is to utilize four distinct characteristics such that their XORed difference is nonzero, as described in Section 3.1. However, a limitation of this direction is that it ignores the dependence of the two sub-ciphers, which has been extensively studied in recent years since the introduction of the BCT. Even earlier, Murphy [Mur11] pointed out that the incompatibility of two characteristics could lead to a boomerang distinguisher of probability 0. Thus, an intuitive idea for constructing an impossible boomerang distinguisher is to explore the incompatibility between the middle layer $E_m$ using advanced tools like BCT, GBCT, etc. The principle of generating an impossible boomerang distinguisher is as follows.

Proposition 1. A boomerang distinguisher is impossible as long as the probability of generating a right quartet for $E_m$ is zero.

It is easy to see that this proposition covers the impossible case described in Section 3.1. More importantly, it reveals the construction of an impossible boomerang distinguisher through the incompatibility of multiple rounds, which could possibly lead to a longer distinguisher.

Similar to impossible differentials, we adopt the miss-in-the-middle approach to search impossible boomerangs: For a cipher $E = E_1 \circ E_m \circ E_0$, we can find two forward characteristics (same or different) and two backward characteristics (same or different) both with probability one in order to make the difference transition through the middle layer $E_m$ with probability zero. There are many studies on the switching probability of the middle layer, and therefore a natural idea for constructing impossible boomerang distinguishers is to consider the switching probability of certain cells in $E_m$ using the techniques such as BCT, GBCT, etc., which can be easily modeled by MIQCP (discussed in Section 3.3.3).

In this work, we searched for IB attacks on both traditional boomerangs and asymmetric ones, and found that the attacks based on traditional boomerangs are more effective, so the rest of the paper will focus on traditional boomerangs.

3.3.1 Impossible Boomerangs vs Impossible Differentials

As another cryptanalytic technique using distinguishers with probability zero, impossible differentials have been extensively studied. Then, an interesting discussion would arise from comparing impossible boomerangs with impossible differentials.

For single-key setting, it has been proven in [SLG+16] that the upper bounds for the length of impossible differentials depend on the linear layer. The same approach can be applied to the impossible boomerangs. Related-key attacks [Bih94] allow the attacker uses weaknesses of the encryption function and of the key schedule algorithm to derive information on the unknown keys. In related-key impossible differentials, two related keys are involved ($K_a$ and $K_b = K_a \oplus \Delta K$), while related-key impossible boomerangs could involve four related keys ($K_a$, $K_b = K_a \oplus \Delta K$, $K_c = K_a \oplus \nabla K$, $K_d = K_a \oplus \nabla K \oplus \Delta K$). Compared to the single-key impossible boomerang in Definition 3, the related-key impossible boomerang with the traditional boomerang structure can be defined as

$$\forall X \in \mathbb{F}_2^n, \ Pr[E_{K_c}^{-1}(E_{K_a}(X) \oplus \delta) \oplus E_{K_d}^{-1}(E_{K_a}(X \oplus \alpha) \oplus \delta) = \alpha] = 0.$$
This fact allows the adversary to have more freedom to choose key differences for the upper and lower trails independently in the case of the impossible boomerang attack, which is illustrated in Figure 5.

![Related-key impossible differential](image1)

![Related-key impossible boomerang](image2)

**Figure 5:** Impossible Differential vs Impossible Boomerang (related-key setting)

Therefore, related-key impossible boomerangs are expected to cover more rounds compared to related-key impossible differentials. For example, we refer to our attack on Deoxys-BC-384. Specifically, we provide a 9-round related-tweakey impossible boomerang distinguisher and a 7-round related-tweakey impossible differential distinguisher in Table 7 and Figure 13, respectively. The reason that the impossible boomerang is better lies in the fact that the subtweakey difference cancellation (Proposition 2) is only applied once in the impossible differential, whereas in the case of the impossible boomerang, this cancellation is utilized twice (in Round 3-4 and Round 9-10).

### 3.3.2 Contradictions through Multiple Rounds

In addition to applying the BCT to find incompatibility of a single S-box layer, we can also construct an impossible boomerang distinguisher through incompatibility of multiple rounds. **Double Boomerang Connectivity Table (DBCT)** [HBS21] is a technique to evaluate the boomerang switch through multiple rounds. Similar to the constraints on cells in a single S-box layer, we can apply quadratic constraints on the propagation of active cells through multiple rounds. The distinguisher in Figure 16 is an example of using the DBCT technique.

![DBCT of S-box](image3)

**Figure 6:** DBCT of S-box

**Definition 5 ([WP19, DDV20]).** Let $S$ be an $n$-bit S-box, and $\Delta_i, \Delta_o, \nabla_i, \nabla_o \in \mathbb{F}_2^n$. The Upper BCT (UBCT) and the Lower BCT (LBCT) of $S$ are three-dimensional tables defined as

\[
\text{UBCT}(\Delta_i, \Delta_o, \nabla_i) = \# \left\{ x \in \mathbb{F}_2^n \mid S(x) \oplus S(x \oplus \Delta_i) = \Delta_o \right\},
\]

\[
\text{LBCT}(\Delta_o, \nabla_i, \nabla_o) = \# \left\{ x \in \mathbb{F}_2^n \mid S(x) \oplus S(x \oplus \nabla_i) = \nabla_o \right\}.
\]
Definition 6 ([HBS21, YSS+22]). Let $S$ be an $n$-bit S-box, and $\Delta_i, \Delta_o, \nabla_i, \nabla_o \in \mathbb{F}_2^n$. The DBCT of $S$ is a $2^n \times 2^n$ table, in which the entry for $(\Delta_i, \nabla_o)$ is given by:

$$\text{DBCT}(\Delta_i, \nabla_o) = \sum_{\Delta_o, \nabla_i} \text{UBCT}(\Delta_i, \Delta_o, \nabla_i) \cdot \text{LBCT}(\Delta_o, \nabla_i, \nabla_o).$$

The Attempt to Build Impossibilities Using The DBCT. In the ToSC version of our paper, we attempted to give an example of constructing an impossible boomerang distinguisher of SKINNY using the contradiction through multiple rounds as shown in Figure 7, but it was later proved to be wrong in [BL24]. The complete 18-round distinguisher is shown in Figure 16. The contradiction was assumed to occur in consecutive three rounds: Round 13 to 15. For $\Delta X_{13}[2]$, its difference 0x05 is equal to $\Delta Z_{12}[2]$, which comes from $\Delta STK_{12}[2] = 0x05$ of ART in Round 12. For $\nabla Z_{14}[6]$, its difference $\alpha$ is equal to $\nabla X_{15}[7]$ due to the linear transformations SR and MC. And $\nabla X_{15}[7]$ is derived from the operation SC on the known difference $\nabla Y_{15}[7] = 0x04$ in Round 15. Therefore, it seems that we can use $\text{DBCT}(0x05, \alpha) = 0$ for $\forall \alpha$ s.t. $\text{DDT}(\alpha, 0x04) \neq 0$ to construct the contradiction. However, we show below that this is not an impossible distinguisher.

Limits of The DBCT. In [BCL+24], Bonnetain et al. introduced the limitations of using DBCT in identifying multi-round contradictions in IB. The DBCT only considers the case of equal differences in the middle between the two S-boxes, ignoring those $(\Delta_o, \nabla_i, \nabla'_i, \Delta'_o)$ with $\Delta_o \neq \Delta'_o$ and $\nabla_i \neq \nabla'_i$.

In [BL24], Bonnetain and Lallemand provided a counterexample of Figure 7, thereby proving the flaw in the distinguisher shown in Figure 16. The counterexample is shown in Table 3. For a detailed description of the usage of DBCT, please refer to [BCL+24, BL24].

3.3.3 MIQCP-based Search Tool for Impossible Boomerang Attacks

In this section, we describe a MIQCP-based search tool for impossible boomerang attacks. Differing from the previous search for distinguishers, the quadratic constraints make it easier for us to search for complete attacks. In the following, we will use the round function of Deoxys-BC to describe the constraints of the MIQCP model. We use this model to search for the truncated attack and instantiate it after running the model.

Variables. We assign three attributes to each byte of the internal states and the sub-twekeys: $z$, $k$, and $d$, indicating whether it has a zero difference, whether it has a known difference value, and whether it belongs to the distinguisher, respectively. For attributes $z$ and $k$, if $z = 1$, it means that the byte is zero difference (corresponding to the white
Table 3: An counterexample of an actual quartet for Figure 7 provided by [BL24] (Treat the 2nd, 5th, 8th and 15th cells in $X_{13}$ as a 32-bit word (red boxes in Figure 7).)

<table>
<thead>
<tr>
<th></th>
<th>$x^1$</th>
<th>$x^2$</th>
<th>$x^3$</th>
<th>$x^4$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td>0xa7ed0098</td>
<td>0xb8ed009d</td>
<td>0xa0690090</td>
<td>0xbf690095</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td>0x8e521bd8</td>
<td>0xab523ac8</td>
<td>0xeb7d4b8c</td>
<td>0xce7d6a9c</td>
</tr>
<tr>
<td><strong>Middle key+constant</strong></td>
<td>0x000028862</td>
<td>0x000028962</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\Delta X_{13}$</td>
<td>(0x1f000005,0x1f000005)</td>
<td>(0xf000005,0xf000005)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>After Sbox layer</td>
<td>0x7d000026</td>
<td>0x5d000006</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\nabla Y_{14}$</td>
<td>(0x652f 50 54, 0x652f 50 54)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Squares in the following figures): if $z = 0, k = 1$, it means the byte is nonzero known difference (corresponding to the green and pink squares in the following figures); if $z = k = 0$, it means the byte is unknown difference (corresponding to the gray squares in the following figures). For attribute $d$, if $d = 1$, it implies that the byte belongs to the distinguisher; if $d = 0$, it implies that the byte belongs to the key recovery phase.

Based on the notations introduced in Section 2.4, we use $\Delta X_r[i]$ to represent the attribute $z$ of the difference $\Delta X_r[i]$, and so on. There are some intuitive constraints: for any byte $a$, we have $a^z \leq a^k$. Let $a \xrightarrow{T} b$, where $S$ is an S-box and $a, b$ are the input and output differences of $S$, we have $a^z = b^z$. Additionally, the number of rounds $R$ for a complete attack and the number of rounds $r_m$ for the middle layer $E_m$ need to be fixed before running the model. Thus, for the plaintext and ciphertext in the complete attack, we have $\Delta\text{plaintext}[i]^d = \nabla\text{ciphertext}[i]^d = 0$ and $\nabla X_r[i]^d = \Delta X_r[i]^d = 1$.

**New Constraints with Quadratic Terms.** For attribute $d$, it indicates whether the byte is in the distinguisher or in the key recovery phase. We use the notation $T$ to represent a transformation in the round function and let $a \xrightarrow{T} b$, where $a$ and $b$ are the input and output differences of the transformation $T$, respectively. For the upper trail of $E_0$, there are three possibilities:

$$a^d = 1 \xrightarrow{T} b^d = 1 \quad a^d = 0 \xrightarrow{T} b^d = 1 \quad a^d = 0 \xrightarrow{T} b^d = 0$$

and for the lower trail of $E_1$, there are also three possibilities:

$$a^d = 0 \xrightarrow{T} b^d = 0 \quad a^d = 1 \xrightarrow{T} b^d = 1 \quad a^d = 1 \xrightarrow{T} b^d = 0$$

Suppose that $L_1$ and $L_2$ respectively represent linear inequalities for the transformation $T$ within the distinguisher and the key recovery phase. Then we can use $a^d \cdot L_1 + (1-a^d) \cdot L_2$ as the quadratic terms to describe the transformation $T$. The description of the SubBytes operation in the following text will serve as an example explaining the quadratic term. These quadratic constraints make our model a MIQCP model rather than a MIQP one. Since all variables in this model are binary, it is undeniable that the constraints in this model can be rewritten as linear ones. In [DEFN22], the authors used linear constraints with the same variable $d$ to search for complete boomerang attacks. We fine-tuned their model to adapt to IB attacks and our experiments show that for IB attack MIQCP is more efficient than linear constraints, the rewritten linear inequalities would be more complex and redundant.
SubBytes With the miss-in-the-middle technique, we aim to search for two characteristics with probability 1. When the input difference of S-box takes a nonzero known value, the output difference becomes unknown. For the upper trail of $E_0$, the constraints would be described as:

$$\Delta X_r[i]^d - \Delta Y_r[i]^d \leq 0 \quad (1)$$

$$\Delta X_r[i]^d \cdot (\Delta X_r[i]^k - \Delta Y_r[i]^k + 1) + (1 - \Delta X_r[i]^d) \cdot (\Delta Y_r[i]^k - \Delta X_r[i]^k + 1) \geq 1 \quad (2)$$

$$\Delta X_r[i]^d \cdot (\Delta Y_r[i]^k - \Delta Y_r[i]^e + 1) + (1 - \Delta X_r[i]^d) \cdot (\Delta X_r[i]^k - \Delta X_r[i]^e + 1) = 1 \quad (3)$$

The linear inequality (1) can be intuitively derived from the three possibilities mentioned above for $E_0$. For inequalities (2) and (3), only one additive term will work, corresponding to the propagation in the distinguisher or in the key recovery phase. For instance, when $\Delta X_r[i]^d = 1$, both (2) and (3) will only activate the first term, constraining the difference propagation in the distinguisher: zero input difference ($z = 1, k = 1$) to zero output difference ($z = 1, k = 1$), nonzero known difference ($z = 0, k = 1$) to unknown output difference ($z = 0, k = 0$), and unknown input difference ($z = 0, k = 0$) to unknown output difference ($z = 0, k = 0$).

The constraints for the lower trail of $E_1$ are symmetric:

$$\nabla X_r[i]^d - \nabla Y_r[i]^d \geq 0 \quad (4)$$

$$\nabla Y_r[i]^d \cdot (\nabla Y_r[i]^k - \nabla X_r[i]^k + 1) + (1 - \nabla Y_r[i]^d) \cdot (\nabla X_r[i]^k - \nabla Y_r[i]^k + 1) \geq 1 \quad (5)$$

$$\nabla Y_r[i]^d \cdot (\nabla X_r[i]^k - \nabla X_r[i]^e + 1) + (1 - \nabla Y_r[i]^d) \cdot (\nabla Y_r[i]^k - \nabla X_r[i]^e + 1) = 1 \quad (6)$$

ShiftRows The ShiftRows operation preserves the values of all attributes of the variable.

MixColumns For the constraints for MixColumns, we use some linear constraints on the MDS matrix proposed in [DEFN22]. Let $(b_1, b_2, b_3, b_4) = MC(a_1, a_2, a_3, a_4)$, then we have

$$a_1^u + a_2^u + a_3^u + a_4^u + b_1^u + b_2^u + b_3^u + b_4^u \in \{0, 1, 2, 3, 8\}$$

This could be translated into linear constraints by adding extra dummy variables $e_{u,i}$ and $e'_{u,i}$ corresponding to each $u$ and $i$:

$$\sum_{j=0}^{3} \Delta Z_r[i + j]^u + \sum_{j=0}^{3} \Delta W_r[i + j]^u \leq 8 - 5e_{u,i}, \text{ for } u \in \{z, k, d\}, i \in \{0, 4, 8, 12\} \quad (4)$$

$$\sum_{j=0}^{3} \Delta Z_r[i + j]^u + \sum_{j=0}^{3} \Delta W_r[i + j]^u \geq 8 - 8e_{u,i}, \text{ for } u \in \{z, k, d\}, i \in \{0, 4, 8, 12\} \quad (5)$$

$$\sum_{j=0}^{3} \nabla Z_r[i + j]^u + \sum_{j=0}^{3} \nabla W_r[i + j]^u \leq 8 - 5e'_{u,i}, \text{ for } u \in \{z, k, d\}, i \in \{0, 4, 8, 12\} \quad (6)$$

$$\sum_{j=0}^{3} \nabla Z_r[i + j]^u + \sum_{j=0}^{3} \nabla W_r[i + j]^u \geq 8 - 8e'_{u,i}, \text{ for } u \in \{z, k, d\}, i \in \{0, 4, 8, 12\} \quad (7)$$

$$4\Delta Z_r[i]^d \leq \sum_{j=0}^{3} \Delta W_r[4i/4 + j]^d \quad (8)$$

$$4\nabla W_r[i]^d \leq \sum_{j=0}^{3} \nabla Z_r[4i/4 + j]^d \quad (9)$$

Besides, we introduce the following quadratic constraints to more accurately describe the difference propagation of MixColumns operation by adding two dummy variables $e_u$
\[ \Delta Z_r[i]^d \cdot \sum_{j=0}^{3} \Delta W_r[i/4] + j]^k + (1 - \Delta Z_r[i]^d) \cdot \sum_{j=0}^{3} \Delta Z_r[i/4] + j]^k = 4 - 4e_u \quad (10) \]

\[ \nabla W_r[i]^d \cdot \sum_{j=0}^{3} \nabla Z_r[i/4] + j]^k + (1 - \nabla W_r[i]^d) \cdot \sum_{j=0}^{3} \nabla W_r[i/4] + j]^k = 4 - 4e_l \quad (11) \]

Specifically, inequalities (4)-(9) provide a rough characterization of the MDS-type MixColumns and cannot eliminate cases such as \( \text{MC} \) (the green color stands for nonzero known difference and the gray color stands for unknown difference). The problem can be solved with inequalities (10) and (11).

**AddRoundTweakey** For the primary XOR operation within the AddRoundTweakey, expressed as \( a \oplus b = c \), we treat it as an ordered operation to exclude the possible case \( a[z = 0, k = 0] \oplus b[z = 0, k = 0] = c[z = 0, k = 1] \) that is feasible under the previous constraint: \( a^u + b^u + c^u \neq 2, u \in \{z, k\} \).

Table 4: Possible values for \( a \oplus b = c \)

<table>
<thead>
<tr>
<th>( (a^z, a^k) )</th>
<th>( (b^z, b^k) )</th>
<th>( (c^z, c^k) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1, 1)</td>
<td>(1, 1)</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>(1, 1)</td>
<td>(0, 1)</td>
<td>(0, 1)</td>
</tr>
<tr>
<td>(0, 1)</td>
<td>(1, 1)</td>
<td>(0, 1)</td>
</tr>
<tr>
<td>(0, 1)</td>
<td>(0, 1)</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>(1, 1)</td>
<td>(0, 0)</td>
<td>(0, 0)</td>
</tr>
<tr>
<td>(0, 0)</td>
<td>(1, 1)</td>
<td>(0, 0)</td>
</tr>
<tr>
<td>(0, 1)</td>
<td>(0, 0)</td>
<td>(0, 0)</td>
</tr>
<tr>
<td>(0, 0)</td>
<td>(0, 1)</td>
<td>(0, 0)</td>
</tr>
<tr>
<td>(0, 0)</td>
<td>(0, 0)</td>
<td>(0, 0)</td>
</tr>
</tbody>
</table>

Considering the attributes \( z \) and \( k \) of bytes \( a, b \) and \( c \), there are a total of 10 possibilities (shown in Table 4). We have the following inequality constraints for these cases:

\[
\begin{align*}
& a^k - a^z + b^z - b^u + c^u - c^k \geq 0 \\
& a^z - b^z + b^k - c^z \geq 0 \\
& a^k - a^z + b^z - c^z \geq 0 \\
& c^k - a^k - b^k \geq 0 \\
& a^k - c^k \geq 0 \\
& b^k - c^k \geq 0
\end{align*}
\]

**Construct Contradiction** The distinguisher retrieved by the model is based on the contradiction we constructed rather than automatically captured by the model in previous works. For the \( r_m \)-th round \( E_m \) which is composed of a single S-box layer, there exists at least one byte whose input and output differences are both nonzero known values:

\[
\sum_{r=0}^{15} (\Delta X_{r_m}[i]^k - \Delta X_{r_m}[i]^z) \cdot (\nabla Y_{r_m}[i]^k - \nabla Y_{r_m}[i]^z) \geq 1. \quad (12)
\]

After running the MIQCP model, we use BCT and tweakey schedule to obtain specific instantiation that satisfy the truncated characteristics. Inequality (12) can provide a very
simple example comparing linear constraints with quadratic constraints. If we rewrite it as a linear constraint

\[ \Delta X_{r_m}[i]^k - \Delta X_{r_m}[i]^z + \nabla Y_{r_m}[i]^k - \nabla Y_{r_m}[i]^z = 2, \]

and then need to run the model 16 times for \( i \) ranging from 0 to 15.

As for the contradictions through multiple rounds, it is necessary to analyze the round function of the cipher to construct contradictions. It is possible that the model needs to be run multiple times to obtain the final result. Thanks to the efficiency of our model, the overall time takes a few minutes even when multiple iterations are required (single execution requiring only several seconds on Intel(R) Xeon(R) Gold 5220R CPU @ 2.20GHz).

Taking Figure 7 as an example, we use the following constraints to construct the contradiction:

\[
(\Delta X_{r_m}[2]^k - \Delta X_{r_m}[2]^z) \cdot (3 - \nabla Y_{r_m+2}[7]^z - \nabla Y_{r_m+2}[11]^z - \nabla Y_{r_m+2}[15]^z) = 1
\]

\[ \nabla Y_{r_m+2}[7]^k + \nabla Y_{r_m+2}[11]^k + \nabla Y_{r_m+2}[15]^k = 3 \]

**Objective Function.** Generally, both the beginning and the end of an impossible boomerang have very few active bytes. We aim to activate as few bytes as possible during the key recovery phase, thus reducing the number of bytes with unknown difference \( k = 0 \) of plaintext and ciphertext, and consequently lowering the complexity. Thus, we have the following objective function and ask the solver for the maximum value:

\[
\sum_{i=0}^{15} (\Delta \text{plaintext}[i]^k + \nabla \text{ciphertext}[i]^k),
\]

in which the plaintext and ciphertext refer to the actual ones in a complete attack.

**Advantages and Limitations.** Previously, most automatic tools focused on searching for impossible differential distinguishers. Those tools were designed by specifying a set of input differences and a set of output differences in the model and asking the solver to iterate through all input and output differences in the given sets. If the solver outputs an error code with "infeasible", it implies the detection of an impossible differential. The advantage of this method is that it can detect impossible differentials with arbitrary types of contradictions. However, the search space is large, and it is time-consuming.

In our new model, we no longer need to specify the sets of input and output differences. Instead, we use quadratic constraints to construct contradictions in \( E_{r_m} \) and describe the propagation of differences during the distinguisher and key recovery phase. This significantly reduces the search space compared to previous models, allowing results to be obtained in seconds. The limitation of the new model is that it cannot capture all types of contradictions like the previous model. We need to sequentially describe contradictions to run the model for several times. The model cannot promise the optimal results for IB attacks because there has not been a thorough study on the types of contradictions yet.

### 3.4 Key Recovery Attacks under Related-Key Setting

The impossible boomerang combines the concepts of impossible differentials and boomerangs. Therefore, we propose two approaches for its key recovery attack: the impossible differential style and the boomerang style. In the following, we will introduce the two methods, both under the related-key setting with the targeted cipher having linear key schedule. The introduction follows the procedures and notations from the previous works [BNS14, BLNS18, ZDJ19].

As illustrated in Figure 8, assume that there is an impossible boomerang distinguisher \((\alpha, \gamma) \rightarrow (\delta, \delta)\). We denote the targeted cipher as \( E = E_f \circ E_{dist} \circ E_b \), where \( E_{dist} \) denotes the rounds covered by the impossible boomerang distinguisher, and \( E_b \) and \( E_f \) denote the rounds added at the beginning and at the end of the distinguisher, respectively. We denote by \( K \) the size of master key, by \( s \) the size of S-box, by \( r_b \) (resp. \( r_f \)) the dimension
of vector space $\mathcal{I}$ (resp. $\mathcal{O}$). Let $k_{in}$ (resp. $k_{out}$) denotes the number of subkey bits involved in $E_b$ (resp. $E_f$), $c_{in}$ (resp. $c_{out}$) denotes the number of bit-conditions that have to be verified during $E_b$ (resp. $E_f$).

The goal of the key recovery attack is to discard the keys that allow the differentials $\mathcal{I} \rightarrow \alpha$ and $\mathcal{O} \rightarrow \delta$ at the same time at the both sides of the boomerang.

### 3.4.1 Impossible Differential Style

Construct a structure of $2^r$ plaintexts, and each can combine $2^2rb$ plaintext pairs. In total, $2^{2N+4r_b}$ plaintext quartets can be constructed if $2^N$ structures are prepared. After filtration on the ciphertext side, $Q = 2^{2N+4r_b-2(n-r_f)}$ quartets will remain. For a given key, the probability that a quartet satisfying the differences $\mathcal{I}$ and $\mathcal{O}$ verifies all the bit-conditions in $E_b$ and $E_f$ is $2^{-2(c_{in}+c_{out})}$. Thus we have

$$2^\alpha \geq 2^{k_{in} \cup k_{out} | (1 - 2^{-2(c_{in}+c_{out})})^Q},$$

where $\alpha$ denotes the number of subkey bits need to be exhaustively searched of the $K = |k_{in} \cup k_{out}|$ subkey bits after incorrect keys are rejected.

**Data Complexity.** The formula above could be rewritten as:

$$Q \geq 2^{2(c_{in}+c_{out})} \cdot \frac{\mathcal{K} - \alpha}{\log_2 \epsilon}.$$

Thus, the data complexity of the attack is $D = 2^{N+r_b+2}$.

**Time Complexity.** As for the key recovery phase, we could adopt the early abort technique [LKKD08], which is popular in impossible differential cryptanalysis. Similar to impossible differential attack, the time complexity of impossible boomerang attacks consists of three terms. The first term is the time of preparing $Q = 2^{2N+4r_b-2(n-r_f)}$ quartets, denoted by $C_Q$. The second is the time of guessing all candidate keys $k_{in} \cup k_{out}$ and the cost can be approximated by $C_G = \left( Q + 2^K \frac{Q}{2^{2(c_{in}+c_{out})}} \right) C'_E$, where $C'_E$ is the ratio of the cost for one partial encryption to the full encryption. Finally, the last term is the cost for brute force, including the remaining key candidates after the sieving and the subkey bits not involved in key recovery procedure, given by $C_B = 2^{K-K+\alpha}$. Considering
the cost of one encryption as \( C_E \), we have a total time complexity

\[
T = (C_Q + C_G + C_R)C_E
\]

\[
= \left( C_Q + \left( Q + 2^K \frac{Q}{2^2r_{\text{out}} + 1}\right) \right) C_E + 2^{K-K+\alpha} C_E.
\]

Memory Complexity. The memory complexity \( M \) of this attack is bounded by \( Q + 2^K \).

3.4.2 Boomerang Style

1. Construct \( 2^N \) structures of \( 2^r \) plaintexts each, each of them taking all the possible values of \( r \) active bits.

2. For each structure, query the ciphertexts corresponding to \( 2^r \) plaintexts under four related keys: \( K_1, K_2 = K_1 \oplus \Delta K, K_3 = K_1 \oplus \nabla K, K_4 = K_1 \oplus \Delta K \oplus \Delta K \), respectively. We denote by \( S_i \) the plaintext-ciphertext sets encrypted by \( K_i \), where \( i \in \{1, 2, 3, 4\} \), and insert \( S_1 \) and \( S_4 \) into hash tables \( H_1 \) and \( H_2 \) indexed by the \( r \) bits of plaintexts.

3. Guess \(|k_i|\) subkey bits involved in \( E_b\):

(a) For each structure, partially encrypt \( P_1 \in S_1 \) to the beginning of the distinguisher. XOR the obtained state with \( \alpha \), then decrypt it to produce the plaintext and search for a collision in \( H_1 \) to find \( P_2 \). It is expected for one collision for each \( P_1 \). Conduct the same operation to the set \( S_3 \) to find expected pairs \((P_3, P_4)\). Two new sets can be obtained:

\[
L_1 = \{(P_1, C_1, P_2, C_2) : (P_1, C_1) \in S_1, (P_2, C_2) \in S_2, E_{bK_1}(P_1) \oplus E_{bK_2}(P_2) = \alpha\},
\]

\[
L_2 = \{(P_3, C_3, P_4, C_4) : (P_3, C_3) \in S_3, (P_4, C_4) \in S_4, E_{bK_3}(P_3) \oplus E_{bK_4}(P_4) = \alpha\}.
\]

(b) The sizes of \( L_1 \) and \( L_2 \) are both \( 2^N \cdot 2^r \). Insert \( L_1 \) into a hash table \( H_3 \) indexed by \( n - r_f \) bits of \( C_1 \) and \( n - r_f \) bits of \( C_2 \). For each element \((P_3, C_3, P_4, C_4)\) of \( L_2 \), we lookup the hash table \( H_3 \) to find the corresponding \((P_1, C_1, P_2, C_2)\) satisfying \( C_1 \oplus C_3 \in \mathcal{O} \) and \( C_2 \oplus C_4 \in \mathcal{O} \). Finally, there are \( Q = 2^{2N+2r_n-2(n-r_f)} \) quartets can be constructed.

(c) Guess the \(|k_{\text{out}}|\) subkey bits involved in \( E_f \) and eliminate the candidate keys which satisfy the differential \( \mathcal{O} \rightarrow \delta \). As this is a type of impossible attacks, we employ the widely-used technique of early abort to eliminate incorrect keys, as commonly done in impossible differential attacks.

4. Exhaustively search the remaining key candidates and the unknown \( K - \left| k_{\text{in}} \cup k_{\text{out}} \right| \) subkey bits.

Complexity. The average number of quartets \( Q \) required to be left with at most \( 2^a \) key candidates is given by the formula:

\[
2^a \geq 2^{2|k_{\text{in}} \cup k_{\text{out}}|}(1 - 2^{-2c_{\text{out}}})Q.
\]

The data complexity is \( D = 2^{N+r_n} \cdot 2^{a+1} \) chosen plaintexts and do \( 2^{2k_{\text{in}}}(2 \cdot 2^N + 2^{N+r_n}) = 3 \cdot 2^{k_{\text{in}}+N+r_n} \) table lookups to prepare quartets. The total time complexity, including data collection, key guessing and brute force, is

\[
T = \left( 2^{N+r_n+2} + 2^{k_{\text{in}}}(2 \cdot 2^N + 2^{N+r_n}) + Q + 2^K \frac{Q}{2^{c_{\text{out}}}} \right) C_E + 2^{K-K+\alpha} C_E,
\]

where \( C_E' \) is the ratio of the cost of partial encryption to the full encryption, \( K = |k_{\text{in}} \cup k_{\text{out}}| \) denotes the targeted key space, and \( C_E \) denotes the cost of one encryption. The memory complexity \( M \) is bounded by \( 4 \cdot 2^N \cdot 2^r + 2^N \cdot 2^r + Q + 2^K = 5 \cdot 2^{N+r} + Q + 2^K \).
Beyond Full-Codebook. For the block cipher with block size $n$, an attack against it that requires $D > 2^n$ plaintexts/ciphertexts is known as a beyond full-codebook attack. Recall that a tweakable block cipher takes as input an $n$-bit plaintext and a $t$-bit tweak, it is reasonable to assume that an attacker may have available an amount of data $D \gg 2^n$ to carry out an attack, as long as $D \leq 2^{n+t}$. Ciphers adopting the TWEAKEY framework [JNP14], such as Deoxys-BC and SKINNY, offer further flexibility in setting the limit of data resources available for an attack. The construction allows one to add a tweak of (almost) any length to a key-alternating block cipher and/or to extend the key space of the block cipher to (almost) any size. This provides cryptanalysts with a potentially optimal strategy to attack the ciphers: select the key size $k$ as large as possible, which results on a higher security claim, as long as the size of the tweak $t$ is large enough to supply the required data to run the attack. In fact, the beyond full-codebook attacks are considered to be realistic and effective against real-world tweakable block ciphers, and have been applied in previous works [BHT16, ABC$^+17$, CHP$^+17$, ZDW19].

Suppose the tweak size is $t$, the tweak size is $h$, the number of related keys used in the attack is $r_k$, we have two natural constraints for the related-tweak impossible boomerang attack: (1) the data complexity under each related key $D' = \frac{D}{2^t} = 2^{N+t}r_k$ should be less than $2^{n+t}$, and the total data complexity $D$ should be less than $2^{n+t+\log_2 r_k}$; (2) the time complexity $T$ should be less than $2^{h-t}$.

4 Applications to Deoxys-BC and Joltik-BC

4.1 Description of Deoxys-BC

Deoxys [JNPS16] is an authenticated encryption scheme selected as one of the finalists for the CAESAR competition. As its internal primitive, Deoxys-BC is a 128-bit block cipher conforming to the TWEAKEY framework [JNP14]. Deoxys-BC has two versions according to different tweak sizes: for Deoxys-BC-256 the tweak size is 256 bits, while for Deoxys-BC-384 it is 384 bits.

Deoxys-BC is an AES-like design, it adopts an iterative substitution-permutation network (SPN) that transforms the internal states through a round function similar to that of AES. Deoxys-BC-256 has 14 rounds, while Deoxys-BC-384 has 16 rounds. The ordering of the internal state and the tweak state is represented by a $4 \times 4$ matrix:

$$
\begin{bmatrix}
0 & 4 & 8 & 12 \\
1 & 5 & 9 & 13 \\
2 & 6 & 10 & 14 \\
3 & 7 & 11 & 15
\end{bmatrix}
$$

Each round function consists of the four transformations in the order specified below:

- **AddRoundTweakey (ART):** XOR the 128-bit round subtweakey to the internal state.
- **SubBytes (SB):** Apply the 8-bit AES S-box $S$ to the 16 bytes of the internal state.
- **ShiftRows (SR):** Rotate the 4-byte $i$-th row left by $i$ positions, $i = 0, 1, 2, 3$.
- **MixColumns (MC):** Multiply the internal state by the $4 \times 4$ MDS matrix of AES.

At the end of the last round, a final AddRoundTweakey operation is applied to the internal state to produce the ciphertext.

**Tweakey Schedule.** Different from the key schedule of AES, Deoxys-BC used a linear tweakey schedule under the TWEAKEY framework. We denote the concatenation of the key $K$ and the tweak $T$ as $KT$, i.e. $KT = K||T$. For Deoxys-BC-256, the size of $KT$ is 256 bits with the first (most significant) 128 bits denoted as $W_1$, the second $W_2$, while the 384 bits tweakey of Deoxys-BC-384 is divided into $W_1$, $W_2$ and $W_3$ per 128 bits sequentially. For Deoxys-BC-256, a subtweakey of $i$-th round is defined as $STK_i = TK_i^1 \oplus TK_i^2 \oplus RC_i$, while for the case of Deoxys-BC-384 it is defined as $STK_i = TK_i^1 \oplus TK_i^2 \oplus TK_i^3 \oplus RC_i$. 


For the byte permutation \( Joltik \) oriented design, the TWEAKEY function and conforms to the consecutive subtweakeys. For \( Joltik \) algorithm, initialized with \( TK = \{Tk_1, Tk_2, Tk_3\} \) and \( TK = \{Tk_1, Tk_2, Tk_3\} \), the subtweakey difference of the first round is defined as

\[
TK_{i+1}^1 = h(TK_i^1), TK_{i+1}^2 = h(LFSR_2(TK_i^2)), TK_{i+1}^3 = h(LFSR_3(TK_i^3)),
\]

where the byte permutation \( h \) is defined as:

\[
\begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
1 & 6 & 11 & 12 & 5 & 10 & 15 & 0 & 9 & 14 & 3 & 4 & 13 & 2 & 7 & 8
\end{pmatrix}.
\]

The \( LFSR_2 \) and \( LFSR_3 \) functions are the application of an LFSR to each of the 16 bytes of a tweak block word. The two LFSRs used are given in Table 5.

**Table 5:** Two LFSRs used in Deoxys-BC tweak schedule

<table>
<thead>
<tr>
<th>LFSR2</th>
<th>( x_7 \parallel x_6 \parallel x_5 \parallel x_4 \parallel x_3 \parallel x_2 \parallel x_1 \parallel x_0 ) \rightarrow ( x_6 \parallel x_5 \parallel x_4 \parallel x_3 \parallel x_2 \parallel x_1 \parallel x_0 \parallel x_7 \oplus x_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>LFSR3</td>
<td>( x_7 \parallel x_6 \parallel x_5 \parallel x_4 \parallel x_3 \parallel x_2 \parallel x_1 \parallel x_0 ) \rightarrow ( x_0 \oplus x_6 \parallel x_7 \parallel x_6 \parallel x_5 \parallel x_4 \parallel x_3 \parallel x_2 \parallel x_1 )</td>
</tr>
</tbody>
</table>

Additionally, for the specifics of round constants \( RC_i \), please refer to [JNPS16]. Figure 9 illustrates an instantiation of the TWEAKEY framework for Deoxys-BC-256, the one for Deoxys-BC-384 is similar.

**Proposition 2** (Subtweakey Difference Cancellation [JNPS16]). For Deoxys-BC-256, suppose that a single cell of \( TK^1 \) and \( TK^2 \) are active. Let \( a_1 \) and \( a_2 \) be differences of the active cell, respectively. Thus, the subtweakey difference of the first round is \( a_2 \oplus a_3 \), and in the \( i \)-th round, the subtweakey difference is \( a_2 \oplus LFSR^2_2(a_1) \). Since \( a_1 \) and \( a_2 \) are both nonzero differences, \( a_2 \oplus LFSR^2_2(a_1) = 0 \) can happen only once over 15 consecutive subtweakeys. For Deoxys-BC-384, suppose that a single cell of \( TK^1 \), \( TK^2 \) and \( TK^3 \) are active. Let \( a_1 \), \( a_2 \) and \( a_3 \) be differences of the active cell, respectively. Thus, the sub-}

tweakey difference of the first round is \( a_1 \oplus a_2 \oplus a_3 \), and in the \( i \)-th round, the subtweakey difference is \( a_1 \oplus LFSR^2_3(a_2) \oplus LFSR^2_3(a_3) \). Since \( a_1 \), \( a_2 \) and \( a_3 \) are both nonzero differences, the cancellation \( a_1 \oplus LFSR^2_3(a_2) \oplus LFSR^2_3(a_3) \) can happen twice for 15 consecutive subtweakeys.

### 4.2 Description of Joltik-BC

Joltik-BC is a lightweight ad-hoc tweakable block cipher of the authenticated encryption scheme Joltik [JNP15]. Similar to Deoxys-BC, Joltik-BC uses an AES-like round function and conforms to the TWEAKEY framework. Adopting a lightweight and hardware-oriented design, Joltik-BC has a 64-bit state, and it has two versions Joltik-BC-128 and Joltik-BC-192 according to different tweak sizes. The number of rounds is 24 for...
Joltik-BC-128 and 32 for Joltik-BC-192. Joltik-BC uses a 4-bit S-box and an involutory MDS matrix, and the subtweakey update function in the tweakey schedule is a bit different from Deoxys-BC. For a more detailed specification of Joltik-BC, please refer to [JNP15]. The tweakey schedules of Joltik-BC family also have the property explained in Proposition 2.

4.3 Related-Tweakey Impossible Boomerang Attack on 10-Round Deoxys-BC-256 and 10-Round Joltik-BC-128

For all the attacks in this paper, we omit the MixColumns in the last round as it is a linear operation. Due to the similarities in the round function and tweakey schedule of Deoxys-BC and Joltik-BC, we can mount a 10-round related-tweakey impossible boomerang attack on these two ciphers. We prefix 1 round at the beginning and append 2 rounds at the end of a 7-round distinguisher to mount the attack, as shown in Figure 10. The distinguishers for Deoxys-BC-256 and Joltik-BC-128 are listed in Table 6 and Table 8, respectively. We denote the cell size as $c$, with $c = 4$ for Joltik-BC-128 and $c = 8$ for Deoxys-BC-256. The key recovery part follows the impossible differential style, as proposed in Section 3.4.1, and the attack begins by constructing quartets on the plaintext side.

Data Collection. Prepare a structure $S$ of size $2^{2c}$ by traversing the 2 gray cells $\Delta P[6, 11]$ of the plaintext and fixing the remaining 14 cells to constants. Then, prepare another structure $S'$ by XORing the difference to each element of $S$. We can obtain $2^{4c}$ ordered pairs $(P_1, P_2)$ from the two structures, each XORed difference conforms to
\[ \Delta P. \] For \( 2^n \) structures, we can construct \((2^{n+4c})^2 = 2^{2n+8c}\) ordered plaintext quartets \((P_1, P_2, P_3, P_4)\). Encrypt \(P_1, P_2, P_3, P_4\) with \(K_1, K_2 = K_1 \oplus \Delta K, K_3 = K_1 \oplus \nabla K, K_4 = K_1 \oplus \Delta K \oplus \nabla K\), and get the corresponding ciphertext quartets \((C_1, C_2, C_3, C_4)\). Then filter the ciphertext quartets according to the 7 known differences of \(\nabla C\). Finally, there are \(2^{2n+8c-12c} = 2^{2n-6c}\) ciphertext quartets remaining.

**Guess-and-Filter.** We make use of the \(2^{2n-6c}\) quartets to eliminate wrong key bits, and then exhaust the remaining key bits to recover the full key. The procedure of the tweakey recovery phase is briefly described in Algorithm 1.

---

**Algorithm 1:** Guess-and-Filter Phase of Related-Tweakey Impossible Boomerang Attacks on 10-round Deoxys-BC-256 and Joltik-BC-128

1. for \(2^c\) guesses of \(STK_0[6]\) do
2. \hspace{1em} for \(2^{2n-6c}\) remaining quartets do
3. \hspace{2em} Filter with known \(\Delta Z_0[14]\);
4. \hspace{2em} Obtain \(2^{2n-8c}\) remaining quartets;
5. \hspace{1em} for \(2^c\) guesses of \(STK_0[11]\) do
6. \hspace{2em} for \(2^{2n-8c}\) remaining quartets do
7. \hspace{3em} Filter with known \(\Delta Z_0[15]\);
8. \hspace{3em} Obtain \(2^{2n-10c}\) remaining quartets;
9. \hspace{2em} for \(2^c\) guesses of \(STK_{10}[12]\) do
10. \hspace{3em} for \(2^{2n-10c}\) remaining quartets do
11. \hspace{4em} Filter with known \(\nabla X_9[12]\);
12. \hspace{4em} Obtain \(2^{2n-12c}\) remaining quartets;
13. \hspace{3em} for \(2^c\) guesses of \(STK_{10}[1, 4, 11, 14]\) do
14. \hspace{4em} for \(2^{2n-12c}\) remaining quartets do
15. \hspace{5em} Filter with known \(\nabla eW_8[5-7]\);
16. \hspace{5em} Obtain \(2^{2n-18c}\) remaining quartets;
17. \hspace{3em} for \(2^c\) guesses of \(STK_{10}[2, 5, 8, 15]\) do
18. \hspace{4em} for \(2^{2n-18c}\) remaining quartets do
19. \hspace{5em} Filter with known \(\nabla eW_8[8, 10, 11]\);
20. \hspace{5em} Obtain \(2^{2n-24c}\) remaining quartets;
21. \hspace{3em} for \(2^c\) guesses of \(eSTK_9[4]\) do
22. \hspace{4em} for \(2^{2n-24c}\) remaining quartets do
23. \hspace{5em} Filter with known \(\nabla X_8[4]\);
24. \hspace{5em} Obtain \(2^{2n-26c}\) remaining quartets;
25. \hspace{3em} for \(2^c\) guesses of \(eSTK_9[13]\) do
26. \hspace{4em} for \(2^{2n-26c}\) remaining quartets do
27. \hspace{5em} Use the known \(\nabla X_8[13]\) to filter out the wrong subtweakeys.

1. Guess \(2^c\) possible values of \(STK_0[6]\) and partially encrypt \((P_1, P_2, P_3, P_4)\) for one round, then use the known difference cell \(\Delta Z_0[14]\) to filter the quartets. There are about \(2^{2n-6c} \cdot 2^{-2c} = 2^{2n-8c}\) remaining quartets. The time complexity of this step is \(2^c : 2^{2n-6c+2} \cdot \frac{1}{10^{10}} \approx 2^{2n-5c-5.32}\).
2. Guess \(2^c\) possible values of \(STK_0[11]\) and partially encrypt \((P_1, P_2, P_3, P_4)\) for one round, then use the known difference cell \(\Delta Z_0[15]\) to filter the quartets. There are
about $2^{2n-10c}$ remaining quartets. The time complexity of this step is $2^{2c} \cdot 2^{2n-8c+2} \cdot \frac{1}{16^{10}} \approx 2^{2n-6c-5.32}$.

3. Guess $2^c$ possible values of $STK_{10}[12]$ and partially decrypt $(C_1, C_2, C_3, C_4)$ for one round. Use the known difference cell $X_5[12]$ to filter quartets and about $2^{2n-12c}$ quartets left. The time complexity of this step is $2^{2c} \cdot 2^{2n-10c+2} \cdot \frac{1}{16^{10}} \approx 2^{2n-7c-5.32}$.

4. Guess $2^4$ possible values of $STK_{10}[1, 4, 11, 14]$. Use the three cells $W_5[5-7]$ with zero difference from the operations of SB and MC in Round 9 to filter quartets and about $2^{2n-18c}$ quartets left. The time complexity of this step is $2^{7c} \cdot 2^{2n-12c+2} \cdot \frac{1}{16^{10}} \approx 2^{2n-5c-5.32}$.

5. Guess $2^{4c}$ possible values of $STK_{10}[2, 5, 8, 15]$. Use the three cells $W_5[8, 10, 11]$ with known difference value from the operations of SB and MC in Round 9 to filter quartets and about $2^{2n-24c}$ quartets left. The time complexity of this step is $2^{13c} \cdot 2^{2n-18c+2} \cdot \frac{1}{16^{10}} \approx 2^{2n-7c-5.32}$.

6. Guess $2^c$ possible values of $eSTK_9[4]^4$. Use the known $X_4[4]$ to filter quartets and keep only $2^{2n-26c}$ quartets remaining. The time complexity of this step is $2^{13c} \cdot 2^{2n-24c+2} \cdot \frac{1}{16^{10}} \approx 2^{2n-12c-5.32}$.

7. Guess $2^c$ possible values of $eSTK_{13}[13]$. Use the known $X_3[13]$ to filter out wrong candidate subtweakeys. The time complexity of this step is $2^{13c} \cdot 2^{2n-26c+2} \cdot \frac{1}{16^{10}} \approx 2^{2n-13c-5.32}$.

**Complexity.** In this attack, we have $2^n = 2^{13c} \cdot (1 - 2^{-22c})^{2^{2n-6c}}$. For Joltik-BC-128, $c = 4$, we choose $\alpha = 15$, $n \approx 58.3$, thus the time complexity of the attack is approximately $2^{2n-5c-5.32} + 2^{2n-6c-5.32} + 2^{2n-5c-3.32} + 2^{128-13c+15} \approx 2^{93.8}$, the data complexity is $2^{98.3}$ and the memory complexity is $2^{92.6}$. For Deoxys-BC-256, $c = 8$, we choose $\alpha = 30$, $n \approx 114.8$, thus the time complexity of the attack is approximately $2^{2n-5c-5.32} + 2^{2n-5c-3.32} + 2^{256-13c+30} \approx 2^{186.6}$, the data complexity is $2^{132.5}$ and the memory complexity is $2^{181.6}$.

### 4.4 Related-Tweakey Impossible Boomerang Attack on 13-Round

**Deoxys-BC-384 and 13-Round Joltik-BC-192**

The 13-round related-tweakey impossible boomerang attack against Deoxys-BC-384 and Joltik-BC-192 is based on a 9-round distinguisher each, which are listed in Table 7 and Table 9, respectively. We prefix two rounds at the beginning and append two rounds at the end of the distinguisher to mount the attacks, as shown in Figure 11. The key recovery part follows the boomerang style, as proposed in Section 3.4.2, and the attacks begin by constructing quartets on the ciphertext side.

**Data Collection.** Prepare a structure $S$ of size $2^{5c}$ by traversing the 6 gray cells $C[2, 3, 5, 8, 9, 15]$ of the ciphertext and fixing the other 10 cells to constants. For the ciphertexts in $S$, we query the corresponding plaintext under two related tweakeys $K_1$ and $K_2 = K_1 \oplus \Delta K$ and denote the plaintext-ciphertext sets by $S_1$ and $S_2$. Then, prepare another structure $S'$ by XORing the difference $\square$ to each element of $S$. We can also get two plaintext-ciphertext sets $S_3$ and $S_4$ under the related tweakeys $K_3 = K_1 \oplus \nabla K$ and $K_4 = K_1 \oplus \Delta K \oplus \nabla K$. Then, we insert $S_3$ and $S_4$ into hash tables $H_1$ and $H_2$ indexed by the 6 gray cells $C[2, 3, 5, 8, 9, 15]$.

For $K_1$, we guess $2^{8c}$ possible values of 6 cells $STK_{13}[2, 3, 5, 8, 9, 15]$ and 2 cells $eSTK_{12}[2, 8]$. For each guess, partially decrypt the ciphertexts $C_1 \in S_1$ under the key $K_1$ to the position at $X_{11}$, then XOR the decrypted states with the fixed difference $\nabla X_{11}$, after that partially encrypt the XORed states to get the ciphertexts using the known subtweakey $STK_r$. Its equivalent subtweakey is defined as $eSTK_r = SR^{-1} \circ MC^{-1}(STK_r)$.

---

\footnote{For the $r$-th round subtweakey $STK_r$, its equivalent subtweakey is defined as $eSTK_r = SR^{-1} \circ MC^{-1}(STK_r)$.}
For each of the cells of $K_3$, finally lookup the hash table $H_1$ to find collisions indexed by the 6 cells $C[2, 3, 5, 8, 9, 15]$. The expected number of collisions is $2^{6c}$, and we store all the corresponding plaintext-ciphertext pairs into a set $L_1 = \{(P_1, C_1, P_3, C_3) : (P_1, C_1) \in S_1, (P_3, C_3) \in S_3, E^{-1}_{f_{K_3}}(C_1) \oplus E^{-1}_{f_{K_3}}(C_3) = \nabla X_{11}\}$.

Similarly, we can get another set $L_2$:

$$L_2 = \{(P_2, C_2, P_4, C_4) : (P_2, C_2) \in S_2, (P_4, C_4) \in S_4, E^{-1}_{f_{K_3}}(C_2) \oplus E^{-1}_{f_{K_3}}(C_4) = \nabla X_{11}\}.$$  

Then, we insert $L_1$ in a hash table $H_3$ indexed by 12 cells $P_3[0, 2, 7, 8, 13, 15]$ and $P_4[0, 2, 7, 8, 13, 15]$. For each element $(P_2, C_2, P_4, C_4)$ of $L_2$, we find the corresponding $(P_3, C_1, P_3, C_3)$ satisfying $P_1 \oplus P_2 \in \Delta P$ and $P_3 \oplus P_4 \in \Delta P$. There are about $2^{6c+n} \cdot 2^{6c+n} = 2^{12c} = 2^n$ quartets constructed using $2^n$ structures. In total, we do $2^{8c} \cdot (2 \cdot 2^{6c+n} + 2^{6c+n}) = 3 \cdot 2^{14c+n}$ table lookups and $2^{n+6c+2} + 2^{8c} \cdot 2^{n+6c} \cdot \frac{8}{16} \approx 2^{2n+14c-3.7}$ encryptions to prepare quartets.

**Guess-and-Filter.** For each of the $2^{8c}$ guesses in the data collection phase, we use the $2^{2n}$ quartets to eliminate wrong key bits, and then exhaust the remaining key bits to recover the full key:

1. For each of the $2^{2n}$ quartets, we guess $2^c$ possible values of $STK_0[5]$ and partially encrypt $(P_1, P_2, P_3, P_4)$ for one round. Use the known $\Delta Z_0[1]$ to filter quartets and about $2^{2n-2c}$ quartets left. The time complexity of this step is $2^{10c} \cdot 2^{2n-2c} \cdot \frac{1}{16} \approx 2^{2n+8c-5.7}$.

2. Guess $2^c$ possible values of $STK_0[10]$ and partially encrypt $(P_1, P_2, P_3, P_4)$ for one round. Use the known $\Delta Z_0[2]$ to filter quartets and about $2^{2n-4c}$ quartets left. The time complexity of this step is $2^{10c} \cdot 2^{2n-4c} \cdot \frac{1}{16} \approx 2^{2n+4c-5.7}$.
3. Guess $2^c$ possible values of $STK_0[3, 4, 9, 14]$ and partially encrypt $(P_1, P_2, P_3, P_4)$ for one round. Use the known $\Delta W_0[7]$ after the MC operation in Round 0 to filter quartets and about $2^{2n-8c}$ quartets left. The time complexity of this step is $2^{14c} \cdot 2^{2n-4c+2} \cdot \frac{1}{16 \cdot 13} \approx 2^{2n+10c-3.7}$.

4. Guess $2^c$ possible values of $STK_1[4]$ and use known difference $\Delta Z_1[4]$ to filter quartets. There are about $2^{2n-8c}$ remaining quartets. Then, guess $2^c$ possible values of $STK_1[5]$, use $\Delta Z_1[1]$ to filter quartets and $2^{2n-10c}$ quartets will remain. For the remaining $2^{2n-10}$ quartets, guess $2^c$ possible values of $STK_1[6]$ and use $\Delta Z_1[14]$ to filter the quartets. There are about $2^{2n-12c}$ remaining quartets that meet the above conditions. The time complexity of this step is $2^{13c} \cdot 2^{2n-6c+2} \cdot \frac{1}{16 \cdot 13} + 2^{16c} \cdot 2^{2n-8c+2} \cdot \frac{1}{16 \cdot 13} \approx 2^{2n+9c-5.7}$.

5. Guess $2^c$ possible values of $STK_0[1, 6, 11, 12]$ and partially encrypt $(P_1, P_2, P_3, P_4)$ for one round. Use the known $\Delta W_0[13]$ after the MC operation in Round 0 to filter quartets and about $2^{2n-14c}$ quartets left. The time complexity of this step is $2^{21c} \cdot 2^{2n-12c+2} \cdot \frac{1}{16 \cdot 13} \approx 2^{2n+9c-3.7}$.

6. Guess $2^c$ possible values of $STK_1[12]$ and partially encrypt the remaining quartets. Use the condition of known $\Delta Z_1[12]$ to filter quartets and about $2^{2n-16c}$ quartets will remain. The time complexity of this step is $2^{22c} \cdot 2^{2n-14c+2} \cdot \frac{1}{16 \cdot 13} \approx 2^{2n+8c-5.7}$.

7. Guess $2^c$ possible values of $STK_1[14]$. Use the condition of known $\Delta Z_1[6]$ to filter quartets and about $2^{2n-18c}$ quartets will remain. The time complexity of this step is $2^{23c} \cdot 2^{2n-16c+2} \cdot \frac{1}{16 \cdot 13} \approx 2^{2n+7c-5.7}$.

8. Guess $2^c$ possible values of $STK_1[15]$. Use the condition of known $\Delta Z_1[3]$ to filter out wrong subtweakeys. The time complexity of this step is $2^{24c} \cdot 2^{2n-18c+2} \cdot \frac{1}{16 \cdot 13} \approx 2^{2n+6c-5.7}$.

**Complexity.** We reduce all the guessed subtweakey bits to the master tweakey and find that all the 16 cells in the master tweakey have been derived. In the guess-and-filter phase, we have $2^n = 2^{24c} \cdot (1 - 2^{-20c})^{2^n}$. For Joltik-BC-192 with $c = 4$, we choose $\alpha = 20, n \approx 42.9$, thus the time complexity of the whole attack is $2^n = 2^{14c} = 2^{2n+10c-3.7} + 2^{192-24c+\alpha} \approx 2^{242.3}$, the data complexity is $2^{6c+n+2} = 2^{68.9}$ and the memory complexity is $2^{96}$. For Deoxys-BC-384 with $c = 8$, we choose $\alpha = 50, n \approx 83.3$, thus the time complexity of the whole attack is approximately $2^{n+14c-3.7} + 2^{2n+10c-3.7} + 2^{384-24c+\alpha} \approx 2^{243.5}$, the data complexity is $2^{6c+n+2} = 2^{133.3}$ and the memory complexity is $2^{192}$.

### 4.5 Related-Tweakey Impossible Boomerang Attack on 14-Round

**Deoxys-BC-384 and 14-Round Joltik-BC-192**

The 13-round attack can be directly extended to a 14-round attack by appending one round to the last round, which makes the states in the final round fully active.

At the data collection phase, we need to guess the full $STK_{14}$, compared to the 13-round attack. We prepare a structure of ciphertexts of size $2^n$, and then by guessing $2^{8c+16c}$ possible values of the subtweakeys $STK_{12}, STK_{13}$ and $STK_{14}$, we can obtain the set $L_1$ and $L_2$ of size $2^{2n-16c}$ for each guess. Then $2^{2(2^n-16c) \cdot 2-12c} = 2^{24x-44c}$ quartets can be constructed. The time complexity of data collection is $2^{24c} \cdot 2 \cdot 2^c \cdot \frac{24}{16 \cdot 13} = 2^{x+24c-22.2}$. The guess-and-filter phase follows exactly the same as the 13-round attack in Section 4.4. Finally, we have $2^n = 2^{40c} \cdot (1 - 2^{-20c})^{2^{x+44c}}$.

For Joltik-BC-192, $c = 4$, we choose $\alpha = 150, n \approx 64.7$, thus the time complexity of the whole attack is $2^{+24c-2.22} + 2^{4x-18c-3.7} + 2^{192-40c+\alpha} \approx 2^{183.65}$, the data complexity is $2^{x+2} = 2^{96.7}$ and the memory complexity is $2^{106}$. For Deoxys-BC-384, $c = 8$, we choose $\alpha = 300, x \approx 128.9$, thus the time complexity of the whole attack is approximately $2^{368}$, the data complexity is $2^{130.9}$ and the memory complexity is $2^{220}$. 

5 Applications to SKINNY

5.1 Related-Tweakey Impossible Boomerang Attacks on 27-Round SKINNY-\(n-3n\)

In this section, we provide a 27-round related-tweakey impossible boomerang attack against SKINNY-\(n-3n\), the specification of SKINNY is given in Appendix E. Though the last round of SKINNY completes the full round function, we omit the SR and MC operations in the last round as they are linear operations. The impossible boomerang distinguishers used in this attack are depicted in Figure 14 and Figure 15. We prefix 4 rounds at the beginning and append 5 rounds at the end of the 18-round distinguisher (\(\Delta Y_4 \rightarrow \nabla X_{22}\)) to mount a 27-round related-tweakey impossible boomerang attack, as shown in Figure 12. The subtweakey bits involved in \(E_b\) and \(E_f\) are listed in Table 10. The guess-and-filter part follows the boomerang style (introduced in Section 3.4.2) and the attack begins by constructing quartets on the ciphertext side.

![18-Round Distinguisher for SKINNY-\(n-3n\)](image)

**Figure 12:** The related-tweakey impossible boomerang attack against 27-round SKINNY-\(n-3n\)

**Data Collection.** We prepare a set of ciphertexts of size \(2^x\), and then by guessing \(2^{24c}\) possible values of \(STK_{26}[0 - 7], STK_{25}[0 - 7], STK_{24}[1, 2, 3, 4, 5, 7], STK_{23}[3, 7]\), we can obtain two sets \(L_1\) and \(L_2\) of size \(2^{2x-16c}\) for each guess. Then, \(2^{2(2x-16c)} = 2^{4x-32c}\) quartets satisfying \(\nabla C \rightarrow \nabla X_{22}\) can be constructed. Because of the equivalent representation of the first key \(eSTK_0 = MC \circ SR(STK_0)\) in the first round, we can filter the quartets obtained by \(\Delta c W_0\) and about \(2^{4x-32c-29c} = 2^{4x-59c}\) quartets will remain. In total, \(2^{24c} \cdot 2^{2x+24c+1} + 2^{2x+8c}\) table lookups and \(2^{24c} \cdot 2^{2x} \cdot \frac{48}{16^{27}} = 2^{x+24c-17}\) encryptions are needed in this phase.
**Guess-and-Filter.** For each of the $2^{24c}$ guesses in the data collection phase, we use the $2^{4x-50c}$ quartets to discard wrong key bits, and then exhaust the remaining key bits to recover the full key.

1. **Satisfying Round 1:**
   - (a) Guess $2^{2c}$ possible values of $\epsilon STK_0[2, 8]$. Use the condition $\Delta W_1[2] = \Delta W_1[10]$ from the MC operation in round 1 to filter the quartets, and about $2^{4x-50c-2c} = 2^{4x-52c}$ quartets will remain. The time complexity of this step is $2^{26c} \cdot 2^{4x-50c+2}$, $\frac{2}{2^{7/16}} = 2^{4x-24c-5.75}$.
   - (b) Guess $2^c$ possible values of $\epsilon STK_0[5]$. Use the condition $\Delta W_1[6] = \Delta W_1[10]$ from the MC operation in round 1 to filter the quartets, and about $2^{4x-54c}$ quartets will remain. The time complexity of this step is $2^{27c} \cdot 2^{4x-52c+2}$, $\frac{2}{2^{7/16}} = 2^{4x-25c-5.75}$.
   - (c) Guess $2^{2c}$ possible values of $\epsilon STK_0[7, 10]$. Use the condition $\Delta W_1[4] = \Delta W_1[8]$ from the MC operation in round 1 to filter the quartets, and about $2^{4x-56c}$ quartets will remain. The time complexity of this step is $2^{28c} \cdot 2^{4x-54c+2}$, $\frac{2}{2^{7/16}} = 2^{4x-25c-5.75}$.

2. **Satisfying Round 2:**
   - (a) Guess $2^{2c}$ possible values of $\epsilon STK_0[0], STK_1[0]$. Use the condition $\Delta Y_2[0] = \Delta STK_0[0]$ to filter the quartets and about $2^{4x-58c}$ quartets will remain. The time complexity of this step is $2^{31c} \cdot 2^{4x-56c+2}$, $\frac{2}{2^{7/16}} = 2^{4x-25c-5.75}$.
   - (b) Guess $2^{2c}$ possible values of $\epsilon STK_0[11], STK_1[4]$. Use the condition $\Delta W_2[11] = \Delta W_2[15]$ from the MC operation in round 1 to filter the quartets, and about $2^{4x-60c}$ quartets will remain. The time complexity of this step is $2^{33c} \cdot 2^{4x-58c+2}$, $\frac{2}{2^{7/16}} = 2^{4x-26c-5.75}$.
   - (c) Guess $2^c$ possible values of $STK_1[2]$. Use the condition $\Delta W_2[7] = \Delta W_2[11]$ from the MC operation in round 1 to filter the quartets, and about $2^{4x-62c}$ quartets will remain. The time complexity of this step is $2^{34c} \cdot 2^{4x-60c+2}$, $\frac{2}{2^{7/16}} = 2^{4x-26c-6.75}$.

3. **Satisfying Round 4:** Guess $2^{6c}$ possible values of $\epsilon STK_0[9], STK_1[3, 5, 7], STK_2[3]$ and $STK_3[2]$. (For the involved subtweak key cell $STK_2[2]$, we can uniquely determine its value in the tweakey schedule by the previously guessed values of $STK_2[3], STK_2[5]$ and $\epsilon STK_0[0]$. The same principle applies to another cell, $STK_2[7]$.) Use the known $\Delta Y_3[2]$ of the beginning of the distinguisher to filter out wrong subtweak keys. The time complexity of this step is $2^{40c} \cdot 2^{4x-62c+2}$, $\frac{6}{2^{7/16}} = 2^{4x-22c-4.17}$.

**Complexity.** We have $2^x = 2^{40c} \cdot (1 - 2^{-14c}) 2^{4x-50c}$. When $c = 4$, $a = 130$, we choose $x \approx 65.1$. In total, the time complexity of this attack is $2^{x + 24c - 2.17} + 2^{4x - 22c - 4.17} + 2^{48c - 40c + a} \approx 2^{68.23}$. The data complexity is $2^{67.1}$ ciphertex, the memory complexity is $2^{160}$. When $c = 8$, $a = 265$, we choose $x \approx 129.3$, thus the time complexity of this attack is $2^{337}$. The data complexity is $2^{313.3}$ ciphertex and the memory complexity is $2^{320}$.

### 5.2 Related-Tweakey Impossible Boomerang Attacks on 28-Round SKINNY-$n$-3n

The 27-round attack can be directly extended to 28-round attack by appending one round to the last round. The overall procedure of the attack is similar to Section 5.1.

**Data Collection.** We prepare a set of ciphertexs of size $2^x$, and then by guessing $2^{32c}$ possible values of $STK_{27}[0-7], STK_{26}[0-7], STK_{25}[0-7], STK_{24}[1, 2, 3, 4, 5, 7]$ and $STK_{23}[3, 7]$, we can obtain the sets $L_1$ and $L_2$ of size $2^{2x-16c}$ for eeach guess. Then, we can construct $2^{2(2x-16c)} = 2^{4x-32c}$ quartets satisfying $\nabla C \rightarrow \nabla X_{22}$. After filtering with
\[ \Delta cW_0, \text{about } 2^{32c} \cdot 2^{-16c} = 2^{4x-50c} \] quartets will remain. In total, \[ 2^{32c}(2 \cdot 2^x + 2^{x-16c}) = 2^x + 32c+1 + 2^x + 16c \] table lookups are needed in this phase. The time complexity of this step is \[ 2^{32c} \cdot 2 \cdot 2^x \cdot \frac{32}{16} = 2^{4x-32c-2.8} \] approximately.

**Guess-and-Filter.** For each of the \( 2^{32c} \) guesses in the data collection phase, we use the \( 2^{4x-50c} \) quartets obtained to recover subtweakes.

1. **Round 1:** Guess \( 2^{32c} \) possible values of \( eSTK_0[2,8] \). Use the condition \( \Delta W_1[2] = \Delta W_1[10] \) to filter the quartets and about \( 2^{4x-50c-2c} = 2^{4x-52c} \) quartets will remain. The time complexity of this step is \( 2^{34c} \cdot 2^{4x-50c+2} \cdot \frac{2}{28} = 2^{4x-16c-5.8} \).

2. **Round 1:** Guess \( 2^c \) possible values of \( eSTK_0[5] \). Use the condition \( \Delta W_1[6] = \Delta W_1[10] \) to filter the quartets and about \( 2^{4x-54c} \) quartets will remain. The time complexity of this step is \( 2^{15c} \cdot 2^{4x-54c+2} \cdot \frac{1}{28} = 2^{4x-17c-6.8} \).

3. **Round 1:** Guess \( 2^{32c} \) possible values of \( eSTK_0[7,10] \). Use the condition \( \Delta W_1[4] = \Delta W_1[8] \) to filter the quartets and about \( 2^{4x-56c} \) quartets will remain. The time complexity of this step is \( 2^{37c} \cdot 2^{4x-56c+2} \cdot \frac{2}{28} = 2^{4x-16c-5.8} \).

4. **Round 2:** Guess \( 2^{32c} \) possible values of \( eSTK_0[0], STK_1[0] \). Use the known value of \( \Delta V_2[0] \) to filter the quartets and about \( 2^{4x-56c} \) quartets will remain. The time complexity of this step is \( 2^{38c} \cdot 2^{4x-56c+2} \cdot \frac{2}{28} = 2^{4x-17c-5.8} \).

5. **Round 2:** Guess \( 2^c \) possible values of \( eSTK_0[11] \). Use the condition \( \Delta W_2[11] = \Delta W_2[15] \) to filter the quartets and about \( 2^{4x-60c} \) quartets will remain. The time complexity of this step is \( 2^{16c} \cdot 2^{4x-60c+2} \cdot \frac{1}{28} = 2^{4x-19c-6.8} \).

6. **Round 2:** Guess \( 2^{32c} \) possible values of \( STK_1[2] \). Use the condition \( \Delta W_2[7] = \Delta W_2[11] \) to filter the quartets and about \( 2^{4x-62c} \) quartets will remain. The time complexity of this step is \( 2^{46c} \cdot 2^{4x-62c+2} \cdot \frac{5}{28} = 2^{4x-16c-4.22} \).

**Complexity.** We have \( 2^c = 2^{46c} \cdot (1 - 2^{-14c})^{4x-50c} \). When \( c = 4, \alpha = 180 \), we choose \( x \approx 64.37 \), thus the time complexity of this attack is \( 2^{x+32c-2.8} + 2^{4x-16c-5.8} + 2^{4x-16c-4.22} + 2^{48c-46c+10} \approx 2^{190.8} \) approximately. The data complexity is \( 2^{206.37} \) ciphertexts and the memory complexity is \( 2^{184} \). When \( c = 8, \alpha = 365 \), we choose \( x \approx 128.26 \), thus the time complexity of this attack is \( 2^{182.8} \) approximately. The data complexity is \( 2^{130.26} \) ciphertexts and the memory complexity is \( 2^{168} \).

6 Conclusions

In this paper, we revisit the impossible boomerang attack. We introduce a systematic overview of the generation of impossible boomerang distinguishers, analyze the advantages of impossible boomerang attacks over impossible differential attacks, and propose two key recovery methods for impossible boomerang attacks. Based on MIQCP, we propose an automatic tool for searching complete impossible boomerang attacks and successfully apply it to three tweakable block ciphers: Deoxys-BC, Joltik-BC and SKINNY. In particular, the results for Deoxys-BC-384, Joltik-BC-128, Joltik-BC-192, SKINNY-64-192 and SKINNY-128-384 have all improved the best previous related-tweakey impossible differential attacks, demonstrating the power of the impossible boomerang attack. Our cryptanalytic results show that the impossible boomerang attack needs more attention in the design and analysis of block ciphers. In addition, the MIQCP tool has the potential to be extended for modeling other cryptanalytic methods, due to the convenience provided by the quadratic constraints in describing block ciphers.
Acknowledgments

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper. The authors would also like to thank the authors of [BL24] for their valuable feedback. This work was supported by the National Natural Science Foundation of China (Grants No. 62302293 and 62272303).

References


A Cryptanalytic Tables in Generalized Boomerang Framework

For the previously extended techniques for $E_m$ with multiple rounds, all of them can be generalized to be applicable in GBF:

**Definition 7** (Generalized Upper BCT (GUBCT)). Let $S$ be an $n$-bit bijective S-box, and $\Delta_i, \Delta'_i, \Delta_o, \Delta'_o, \nabla_i, \nabla'_i, \nabla_o, \nabla'_o \in \mathbb{F}_2^n$. The GUBCT of $S$ is a six-dimensional table, in which the entry for $(\Delta_i, \Delta'_i, \Delta_o, \Delta'_o, \nabla_i, \nabla'_i)$ is given by:

\[
\text{GUBCT}(\Delta_i, \Delta'_i, \Delta_o, \Delta'_o, \nabla_i, \nabla'_i) = \# \left\{ x \in \mathbb{F}_2^n \middle| \begin{array}{l}
S(x) \oplus S(x \oplus \Delta_i) = \Delta_o \\
S(x) \oplus \nabla_o \oplus S(x \oplus \Delta_i) \oplus \nabla'_o = \Delta'_o \\
S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla'_o) = \Delta'_i
\end{array} \right\}.
\]

**Definition 8** (Generalized Lower BCT (GLBCT)). Let $S$ be an $n$-bit bijective S-box, and $\Delta_i, \Delta'_i, \nabla_i, \nabla'_i, \nabla_o, \nabla'_o \in \mathbb{F}_2^n$. The GLBCT of $S$ is a six-dimensional table, in which the entry for $(\Delta_i, \Delta'_i, \nabla_i, \nabla'_i, \nabla_o, \nabla'_o)$ is given by:

\[
\text{GLBCT}(\Delta_i, \Delta'_i, \nabla_i, \nabla'_i, \nabla_o, \nabla'_o) = \# \left\{ x \in \mathbb{F}_2^n \middle| \begin{array}{l}
x \oplus S^{-1}(S(x) \oplus \nabla_o) = \nabla_i \\
x \oplus \Delta_i \oplus x \oplus \nabla_i \oplus \Delta'_i = \nabla'_i \\
S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla'_o) = \Delta'_i
\end{array} \right\}.
\]

**Definition 9** (Generalized Extended BCT (GEBCT)). Let $S$ be an $n$-bit bijective S-box, and $\Delta_i, \Delta'_i, \Delta_o, \Delta'_o, \nabla_i, \nabla'_i, \nabla_o, \nabla'_o \in \mathbb{F}_2^n$. The GEBCT of $S$ is a eight-dimensional table, in which the entry for $(\Delta_i, \Delta'_i, \Delta_o, \Delta'_o, \nabla_i, \nabla'_i, \nabla_o, \nabla'_o)$ is given by:

\[
\text{GEBCT}(\Delta_i, \Delta'_i, \Delta_o, \Delta'_o, \nabla_i, \nabla'_i, \nabla_o, \nabla'_o) = \#
\begin{bmatrix}
S(x) \oplus S(x \oplus \Delta_i) = \Delta_o \\
S(x) \oplus \nabla_o \oplus S(x \oplus \Delta_i) \oplus \nabla'_o = \Delta'_o \\
x \oplus S^{-1}(S(x) \oplus \nabla_o) = \nabla_i \\
x \oplus \Delta_i \oplus x \oplus \nabla_i \oplus \Delta'_i = \nabla'_i \\
S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla'_o) = \Delta'_i
\end{bmatrix}.
\]

**Definition 10** (Generalized Double BCT (GDBCT)). Let $S$ be an $n$-bit bijective S-box, and $\Delta_i, \Delta'_i, \nabla_o, \nabla'_o \in \mathbb{F}_2^n$. The GDBCT of $S$ is a four-dimensional table, in which the entry for $(\Delta_i, \Delta'_i, \nabla_o, \nabla'_o)$ is given by:

\[
\text{GDBCT}(\Delta_i, \Delta'_i, \nabla_o, \nabla'_o) = \sum_{\Delta_o, \Delta'_o, \nabla_i, \nabla'_i} \text{GUBCT}(\Delta_i, \Delta'_i, \Delta_o, \Delta'_o, \nabla_i, \nabla'_i) \cdot \text{GLBCT}(\Delta_o, \Delta'_o, \nabla_i, \nabla'_i, \nabla_o, \nabla'_o).
\]

The GBC consists of the following two apparent properties:

**Property 1** (Commutativity).

\[
\text{GBC}(\Delta_i, \Delta'_i, \nabla_o, \nabla'_o) = \text{GBC}(\Delta'_i, \Delta_i, \nabla_o, \nabla'_o) = \text{GBC}(\Delta_i, \Delta'_i, \nabla_o, \nabla'_o) = \text{GBC}(\Delta'_i, \Delta_i, \nabla_o, \nabla'_o)
\]

**Property 2** (Symmetry).

\[
\text{GBC}(\Delta_i, \Delta'_i, \nabla_o, \nabla'_o) = \text{BCT}(\Delta_i, \nabla_o)
\]

Similar to GBC, the properties of commutativity and symmetry are equally applicable to the generalized tables above. Under the condition of identical opposite differentials, they can be transformed into UBC, LBC, and so forth.
B Related-Tweakey Impossible Boomerang Distinguishers for Deoxys-BC

Table 6: The 7-round related-tweakey impossible boomerang distinguisher for Deoxys-BC-256 (Contradiction: 15-th byte in Round 4, BCT(2c, 2c) = 0)

<table>
<thead>
<tr>
<th>R</th>
<th>( \Delta STK )</th>
<th>( \Delta X )</th>
<th>( \Delta Y )</th>
<th>( \Delta W )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>00 00 00 6a</td>
</tr>
<tr>
<td></td>
<td>00 00 00 6a</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
</tr>
</tbody>
</table>
Table 7: The 9-round related-tweakey impossible boomerang distinguisher for Deoxys-BC-384 (Contradiction: 15-th byte in Round 6, $\text{BCT}(4f, 4f) = 0$)

- $\Delta TK_{i}^{1}$: $\text{cb c5 bc 00 00 00 00 00 00 00 00 00 00 00 00 00 00}$
- $\Delta TK_{i}^{2}$: $\text{17 48 4d 60 00 00 00 00 e2 00 00 00 00 00 00 00 00}$
- $\Delta TK_{i}^{3}$: $\text{95 34 bc 00 00 00 00 00 00 00 00 00 00 00 00 00 00}$
- $\nabla TK_{i}^{1}$: $\text{00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00}$
- $\nabla TK_{i}^{2}$: $\text{00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00}$
- $\nabla TK_{i}^{3}$: $\text{00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00}$

<table>
<thead>
<tr>
<th>R</th>
<th>$\Delta STK$</th>
<th>$\Delta X$</th>
<th>$\Delta Y$</th>
<th>$\Delta W$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$71 \text{ e1 00 26}$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
</tr>
<tr>
<td>2</td>
<td>$13 00 00 98$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
</tr>
<tr>
<td>3</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
</tr>
<tr>
<td>4</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
</tr>
<tr>
<td>5</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
</tr>
<tr>
<td>6</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
</tr>
<tr>
<td>7</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
</tr>
<tr>
<td>8</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
</tr>
<tr>
<td>9</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
</tr>
<tr>
<td>10</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
</tr>
<tr>
<td>11</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
<td>$00 00 00 00$</td>
</tr>
</tbody>
</table>
C Related-Tweakey Impossible Differential Attack against 12-Round Deoxys-BC-384

We mount a 12-round related-tweakey impossible differential attack on Deoxys-BC-384 by prefixing 2 rounds at the beginning and appending 3 rounds at the end of a 7-round distinguisher ($\Delta W_1 \rightarrow \Delta X_0$), shown in Figure 13.

Data Collection. Construct $2^n$ structures that each of them traverses all $2^{36}$ possible values of $\Delta P[1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14]$, then we get $2^{192}$ plaintext pairs for each structure. Encrypt the plaintexts under two related tweakeys ($K_A, K_B$), choose the pairs satisfying ciphertext differences and $2^{192+n}$ pairs would remain.

Guess-and-Filter For each of the remaining pairs:
1. Guess $2^{32}$ possible values of $STK_0[3, 4, 9, 14]$ and partially encrypt $(P_A, P_B)$ for one round, then check whether $W_{A,0}[5] \oplus W_{B,0}[5] = W_{A,0}[6] \oplus W_{B,0}[6] = W_{A,0}[7] \oplus W_{B,0}[7] = 0$. Keep only $2^{192+n} \cdot 2^{-24} = 2^{168+n}$ pairs that meet above condition remain. Time complexity of this step is $2^{n+192+1} \cdot 2^{32} \cdot \frac{1}{64} = 2^{n+199.4}$.
2. Guess $2^{32}$ possible values of $STK_0[2, 7, 8, 13]$ and partially encrypt $(P_A, P_B)$ for one round, then check whether $W_{A,0}[8] \oplus W_{B,0}[8] = W_{A,0}[11] \oplus W_{B,0}[11] = 0$, $W_{A,0}[10] \oplus W_{B,0}[10] = \Delta STK_1[10]$. Keep only $2^{168+n} \cdot 2^{-24} = 2^{144+n}$ pairs that meet above conditions remain. Time complexity of this step is $2^{n+168+1} \cdot 2^{64} \cdot \frac{1}{128} = 2^{n+227.4}$.
3. Guess $2^{32}$ possible values of $STK_0[1, 6, 11, 12]$ and partially encrypt $(P_A, P_B)$ for one round, then check whether $W_{A,0}[12] \oplus W_{B,0}[12] = W_{A,0}[13] \oplus W_{B,0}[13] = 0, W_{A,0}[15] \oplus W_{B,0}[15] = \Delta STK_1[15]$. Keep only $2^{144+n} \cdot 2^{-24} = 2^{120+n}$ pairs that
meet above conditions remain. Time complexity of this step is $2^{n+144+1} \cdot 2^{96} \cdot \frac{4}{16} = 2^{n+235.4}$.

4. Guess $2^8$ possible values of $STK_1[4]$ and partially encrypt for one round, then check whether $Z_{A,1}[4] \oplus Z_{B,1}[4] = \Delta Z_1[4]$. Keep only $2^{120+n} \cdot 2^{-8} = 2^{112+n}$ pairs that meet above condition remain. Time complexity of this step is $2^{n+120+1} \cdot 2^{112} \cdot \frac{1}{16} = 2^{217.4+n}$.

5. Guess $2^8$ possible values of $STK_1[9]$ and partially encrypt for one round, then check whether $Z_{A,1}[5] \oplus Z_{B,1}[5] = \Delta Z_1[5]$. Keep only $2^{112+n} \cdot 2^{-8} = 2^{104+n}$ pairs that meet above conditions remain. Time complexity of this step is $2^{n+112+1} \cdot 2^{104} \cdot \frac{1}{16} = 2^{217.4+n}$.

6. Guess $2^8$ possible values of $STK_1[14]$ and partially encrypt for one round, then check whether $Z_{A,1}[6] \oplus Z_{B,1}[6] = \Delta Z_1[6]$. Keep only $2^{104+n} \cdot 2^{-8} = 2^{96+n}$ pairs that meet above condition remain. Time complexity of this step is $2^{n+104+1} \cdot 2^{96} \cdot \frac{1}{16} = 2^{217.4+n}$.

7. Guess $2^{32}$ possible values of $STK_{12}[1, 4, 11, 14]$ and partially decrypt for one round, then check whether $eW_{A,10}[4 - 6] \oplus eW_{B,10}[4 - 6] = \Delta eW_{10}[4 - 6]$. Keep only $2^{32+n} \cdot 2^{-24} = 2^{22+n}$ pairs that meet above condition remain. Time complexity of this step is $2^{n+32+1} \cdot 2^{212} \cdot \frac{4}{16} = 2^{243.4+n}$.

8. Guess $2^{32}$ possible values of $STK_{12}[2, 5, 8, 15]$ and partially decrypt for one round, then check whether $eW_{A,10}[8, 9, 11] \oplus eW_{B,10}[8, 9, 11] = \Delta eW_{10}[8, 9, 11]$. Keep only $2^{22+n} \cdot 2^{-24} = 2^{48+n}$ pairs that meet above condition remain. Time complexity of this step is $2^{n+72+1} \cdot 2^{184} \cdot \frac{4}{16} = 2^{251.4+n}$.

9. Guess $2^{32}$ possible values of $STK_{12}[0, 7, 10, 13]$ and partially decrypt for one round, then check whether $eW_{A,10}[2, 3] \oplus eW_{B,10}[2, 3] = \Delta eW_{10}[2, 3]$. Keep only $2^{32+n} \cdot 2^{-16} = 2^{24+n}$ pairs that meet above condition remain. Time complexity of this step is $2^{n+32+1} \cdot 2^{216} \cdot \frac{1}{16} = 2^{259.4+n}$.

10. Guess $2^{32}$ possible values of $STK_{12}[3, 6, 9, 12]$ and partially decrypt for one round, then check whether $eW_{A,10}[12, 15] \oplus eW_{B,10}[12, 15] = \Delta eW_{10}[12, 15]$. Keep only $2^{24+n} \cdot 2^{-16} = 2^{16+n}$ pairs that meet above condition remain. Time complexity of this step is $2^{n+32+1} \cdot 2^{224} \cdot \frac{1}{16} = 2^{275.4+n}$.

11. Guess $2^8$ possible values of $cSTK_{11}[5]$ and partially decrypt for one round, then check whether $X_{A,10}[5] \oplus X_{B,10}[5] = \Delta X_{10}[5]$. Keep only $2^{16+n} \cdot 2^{-8} = 2^{8+n}$ pairs that meet above conditions remain. Time complexity of this step is $2^{n+16+1} \cdot 2^{8} \cdot \frac{1}{16} = 2^{265.4+n}$.

12. Guess $2^8$ possible values of $cSTK_{11}[6]$ and partially decrypt for one round, then check whether $X_{A,10}[6] \oplus X_{B,10}[6] = \Delta X_{10}[6]$. Keep only $2^{8+n} \cdot 2^{-8} = 2^n$ pairs that meet above condition remain. Time complexity of this step is $2^{n+8+1} \cdot 2^{6} \cdot \frac{1}{16} = 2^{265.4+n}$.

13. Guess $2^{32}$ possible values of $cSTK_{11}[0 - 3]$ and partially decrypt for one round, then check whether $eW_{A,9}[0 - 1] \oplus eW_{B,9}[0 - 1] = \Delta eW_{9}[0 - 1]$. Keep only $2^n \cdot 2^{-16} = 2^{n-16}$ pairs that meet above condition remain. Time complexity of this step is $2^{n+1} \cdot 2^{206} \cdot \frac{4}{16} = 2^{201.4+n}$.

14. Guess $2^8$ possible values of $cSTK_{10}[10]$ and partially decrypt for one round, then check whether $X_{A,9}[10] \oplus X_{B,9}[10] = \Delta X_{9}[10]$. Keep only $2^{n-16} \cdot 2^{-8} = 2^{n-24}$ pairs that meet above condition remain. Time complexity of this step is $2^{n-16+1} \cdot 2^{204} \cdot \frac{1}{16} = 2^{281.4+n}$.

15. Guess $2^8$ possible values of $cSTK_{10}[15]$ and partially decrypt for one round, then use the condition $X_{A,9}[15] \oplus X_{B,9}[15] = \Delta X_{9}[15]$ to filter out wrong tweakkey bits. Time complexity of this step is $2^{n-24+1} \cdot 2^{312} \cdot \frac{1}{16} = 2^{281.4+n}$.

**Complexity.** In this attack, we have $2^n = 2^{312} \cdot (1 - 2^{-28}) ^ {2^{102+n}}$. We choose $\alpha = 200$, $n \approx 38.3$, thus the time complexity of the whole attack is $2^{201.4+n} \approx 2^{229.7}$ approximately. The
data complexity is $2^{135.3}$ and the memory complexity is $2^{312}$. 
D Related-Tweakey Impossible Boomerang Distinguishers for Joltik-BC

Table 8: The 7-round related-tweakey impossible boomerang distinguisher for Joltik-BC-128 (Contradiction: 15-th byte in Round 4, BCT(8, 8) = 0)

<table>
<thead>
<tr>
<th>R</th>
<th>(\Delta STK)</th>
<th>(\Delta X)</th>
<th>(\Delta Y)</th>
<th>(\Delta W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0 0 0 1</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>1</td>
<td>0 0 0 1 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>2</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>3</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>4</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>5</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>6</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>7</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>8</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
</tbody>
</table>
### Table 9: The 9-round related-tweakey impossible boomerang distinguisher for Joltik-BC-192 (Contradiction: 15-th byte in Round 6, BCT(6,9) = 0)

<table>
<thead>
<tr>
<th>R</th>
<th>ASFK</th>
<th>AX</th>
<th>AY</th>
<th>AW</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8c05</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>2</td>
<td>f009</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>3</td>
<td>020d</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>4</td>
<td>0b00</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>5</td>
<td>0c20</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>6</td>
<td>0e09</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>7</td>
<td>0016</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>8</td>
<td>0a00</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>9</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>10</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>11</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
</tbody>
</table>

\[ \Delta T K_1: \text{f} d 9 0 0 a 0 b 0 f 6 0 5 0 8 \]
\[ \Delta T K_2: \text{f} d 9 0 0 a 0 b 0 f 6 0 5 0 8 \]
\[ \Delta T K_3: \text{f} c b 0 0 4 0 1 0 6 d 0 2 0 e \]
\[ \nabla T K_1: 0 0 0 0 1 0 9 0 0 0 0 0 0 \]
\[ \nabla T K_2: 0 0 0 0 0 a 0 5 0 0 0 0 0 0 \]
\[ \nabla T K_3: 0 0 0 0 e 0 7 0 0 0 0 0 0 \]
E Description of SKINNY

SKINNY is a tweakable block cipher family following the TWEAKEY framework, first proposed in [BJK+16]. SKINNY family has 6 versions, denoted by SKINNY-\( n\)-\( t\): \( n \in \{64, 128\} \) is the block size and \( t \in \{n, 2n, 3n\} \) is the tweakey size. The cell size \( c \) is 4 for SKINNY-64 and 8 for SKINNY-128. The number \( r \) of rounds is 32 for SKINNY-64-64, 36 for SKINNY-64-128, 40 for SKINNY-64-192 and SKINNY-128-128, 48 for SKINNY-128-256 and 56 for SKINNY-128-384. The ordering of the internal state and the tweakey state is represented by a \( 4 \times 4 \) matrix:

\[
\begin{bmatrix}
0 & 1 & 2 & 3 \\
4 & 5 & 6 & 7 \\
8 & 9 & 10 & 11 \\
12 & 13 & 14 & 15
\end{bmatrix}
\]

The SKINNY round function applies five transformations: SubCells (SC), AddConstants (AC), AddRoundTweakey (ART), ShiftRows (SR), MixColumns (MC):

- **SubCells (SC)**: Apply a 4-bit (resp. 8-bit) S-box on each cell for SKINNY-64 (resp. SKINNY-128).
- **AddConstants (AC)**: XOR the round constant to the internal state,
- **AddRoundTweakey (ART)**: XOR the first and second rows of subtweakey with the corresponding cells in the internal state,
- **ShiftRows (SR)**: Rotate the 4-cell \( i \)-th row right by \( i \) positions, \( i = 0, 1, 2, 3 \),
- **MixColumns (MC)**: Multiply the internal state by a binary matrix \( M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \).

We denote the internal states in the \( r \)-th round as follows:

\[ X_r \xrightarrow{SC} Y_r \xrightarrow{ART} Z_r \xrightarrow{SR} W_r \xrightarrow{MC} X_{r+1}. \]

Similar to Deoxys-BC, the tweakey schedule of SKINNY is a linear algorithm and satisfies the property explained in Proposition 2. It divides the master tweakey into \( z \) tweakey arrays \( (TK_1, \ldots, TK_2) \) with \( n \)-bit length each, where \( z = \frac{t}{n} \in \{1, 2, 3\} \). \( TK_1 \), \( TK_2 \) and \( TK_3 \) follow three independent update functions. The subtweakey used in \( r \)-th round \( STK_r \) is generated from:

- \( STK_r = TK_1 \) when \( z = 1 \),
- \( STK_r = TK_1 \oplus TK_2 \) when \( z = 2 \),
- \( STK_r = TK_1 \oplus TK_2 \oplus TK_3 \) when \( z = 3 \),

where \( TK_1, TK_2, TK_3 \) denote the tweakey arrays in round \( r \) and are generated as follows. First, a permutation \( h \) is applied to each tweakey array as \( TK_{z+1}[i] \leftarrow TK_{z}[h[i]] \). Next, each cell of the first and second rows of \( TK_2 \) and \( TK_3 \) are individually updated with an LFSR. For more details about SKINNY, please refer to [BJK+16].
F Related-Tweakey Impossible Boomerang Distinguishers for SKINNY-\(n\)-3\(n\)

![Diagram](image.png)

**Figure 14:** The 18-round related-tweakey impossible boomerang distinguisher for SKINNY-128-384 with BCT effect (Contradiction: 7-th cell in Round 13, BCT(11, 11) = 0)
Figure 15: The 18-round related-tweakey impossible boomerang distinguisher for SKINNY-64-192 with BCT effect (Contradiction: 7-th cell in Round 13, BCT(5,5) = 0)
Figure 16: The 18-round related-tweakey impossible boomerang distinguisher for SKINNY-128-384 with DBCT effect
Subtweakey cells involved in $E_b$ and $E_f$ of the attack against 27-round SKINNY-$n$-3n

Table 10: Subtweakey cells involved in $E_b$ and $E_f$ of the attack against 27-round SKINNY-$n$-3n

<table>
<thead>
<tr>
<th>Filter</th>
<th>Involved Subtweakey Cells</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_b$</td>
<td></td>
</tr>
<tr>
<td>$\Delta W_1[2] = \Delta W_1[10]$</td>
<td>$eSTK_0[2, 8]$</td>
</tr>
<tr>
<td>$\Delta W_1[6] = \Delta W_1[10]$</td>
<td>$eSTK_0[5, 8]$</td>
</tr>
<tr>
<td>$\Delta W_1[4] = \Delta W_1[8]$</td>
<td>$eSTK_0[7, 10]$</td>
</tr>
<tr>
<td>$\Delta Y_2[0]$</td>
<td>$eSTK_0[0, 10, 13]$, $STK_1[0]$</td>
</tr>
<tr>
<td>$\Delta W_2[11] = \Delta W_2[15]$</td>
<td>$eSTK_0[0, 4, 10, 11]$, $STK_1[0, 4]$</td>
</tr>
<tr>
<td>$\nabla X_{25}[1] = \nabla X_{25}[13]$</td>
<td>$STK_{25}[1]$</td>
</tr>
<tr>
<td>$\nabla X_{25}[5] \oplus \nabla X_{25}[9] = \nabla X_{25}[13]$</td>
<td>$STK_{25}[5]$</td>
</tr>
<tr>
<td>$\nabla X_{25}[6] = \nabla X_{25}[14]$</td>
<td>$STK_{25}[6]$</td>
</tr>
<tr>
<td>$\nabla X_{25}[7] \oplus \nabla X_{25}[11] = \nabla X_{25}[15]$</td>
<td>$STK_{25}[7]$</td>
</tr>
<tr>
<td>$\nabla X_{25}[3] = \nabla X_{25}[15]$</td>
<td>$STK_{25}[3]$</td>
</tr>
<tr>
<td>$\nabla X_{24}[11]$</td>
<td>$STK_{25}[5]$</td>
</tr>
<tr>
<td>$\nabla X_{24}[9] = \nabla X_{24}[13]$</td>
<td>$STK_{25}[0, 7]$</td>
</tr>
<tr>
<td>$\nabla X_{24}[1] = \nabla X_{24}[13]$</td>
<td>$STK_{25}[0, 5]$, $STK_{24}[1]$</td>
</tr>
<tr>
<td>$\nabla X_{24}[7] = \nabla X_{24}[15]$</td>
<td>$STK_{25}[2, 4]$, $STK_{24}[7]$</td>
</tr>
<tr>
<td>$\nabla X_{24}[3] = \nabla X_{24}[15]$</td>
<td>$STK_{25}[2, 7]$, $STK_{24}[3]$</td>
</tr>
<tr>
<td>$\nabla X_{23}[11] = \nabla X_{23}[15]$</td>
<td>$STK_{25}[0, 1, 6]$, $STK_{24}[2, 5]$</td>
</tr>
<tr>
<td>$\nabla X_{23}[3] = \nabla X_{23}[15]$</td>
<td>$STK_{25}[1, 4, 6]$, $STK_{24}[2, 7]$, $STK_{23}[3]$</td>
</tr>
<tr>
<td>$\nabla X_{22}[9]$</td>
<td>$STK_{25}[1, 3, 5, 6]$, $STK_{24}[2, 4]$, $STK_{23}[7]$</td>
</tr>
<tr>
<td>$\nabla X_{20}[9]$</td>
<td>$STK_{26}[0 – 7]$</td>
</tr>
</tbody>
</table>