# A Note on the use of the Double Boomerang Connectivity Table (DBCT) for Spotting Impossibilities

Xavier Bonnetain and Virginie Lallemand

Université de Lorraine, CNRS, Inria, LORIA, Nancy, France

**Abstract.** In this short note we examine one of the impossible boomerang distinguishers of Skinny-128-384 provided by Zhang, Wang and Tang at ToSC 2024 Issue 2 and disprove it. The issue arises from the use of the Double Boomerang Connectivity Table (DBCT) as a tool to establish that a boomerang switch over 2 rounds has probability zero, whereas the DBCT only covers specific cases of difference propagation, missing a large set of events that might make the connection possible. We study in details the specific instance provided by Zhang *et al.* and display one example of a returning quartet that contradicts the impossibility.

**Keywords:** Cryptanalysis · Boomerang · DBCT

## 1 Results by Zhang, Wang and Tang

In their article published in ToSC 2024 [ZWT24], Zhang, Wang and Tang revisit the impossible boomerang attack of Lu [Lu08, Lu11] by showing how to build distinguishers based on other types of contradictions. They decompose the cipher $E$ under study as $E = E_1 \circ E_m \circ E_0$ and propose to find two probability-one forward characteristics for $E_0$ and two probability-one backward characteristics for $E_1$ such that connecting them in $E_m$ is impossible. They propose to rely on recent advances such as the (G)BCT [CHP$^+$18, LWL22] to build this miss-connection.

The authors also detail the functioning of the key recovery of these types of attacks and explain how to search for impossible boomerang attacks with a Mixed-Integer Quadratically-Constrained Programming (MIQCP) model. They detail several applications on the recent ciphers Deoxys-BC, Joltik-BC and SKINNY. We do not detail all these results here but focus on one specific contribution of the article, namely the 18-round related-tweakey impossible boomerang distinguisher of SKINNY-128-384 relying on a DBCT contradiction.

### 1.1 Brief Reminder on Boomerang Distinguishers

A boomerang distinguisher [Wag99] corresponds to the observation of the following relation which is satisfied more often for the cipher $E$ than for a random permutation:

$$E^{-1}(E(M) \oplus \delta) \oplus E^{-1}(E(M \oplus \alpha) \oplus \delta) = \alpha. \tag{1}$$

Building such a distinguisher is usually done by following the sandwich construction [DKS10]. It first splits the cipher into $E = E_1 \circ E_m \circ E_0$ and searches 2 differentials, one over $E_0$ of probability $p$ and one over $E_1$ of probability $q$. The probability of Equation (1) is then approximated by $p^2q^2r$, where r is the probability of connecting the two

E-mail: xavier.bonnetain@loria.fr (Xavier Bonnetain), virginie.lallemand@loria.fr (Virginie Lallemand)

Date of this document: 2024-07-30.

top differentials to the two bottom differentials. The size and position of $E_m$ should be chosen so that $E_m$ covers all the middle rounds where the top and bottom trails interact with each other.

When $E$ is an SPN cipher and when $E_m$ covers only one round, the probability $r$ of connecting two top differentials ending with the same difference to two bottom differentials starting with the same difference can be derived from the Boomerang Connectivity Table (BCT) [CHP+18] which covers one Sbox at a time:

**Definition 1** (BCT [CHP+18])**.** Let $S$ be a bijective Sbox of $\mathbb{F}_2^s$ and let $\Delta X_i, \nabla Y_i$ be two elements of $\mathbb{F}_2^s$. The Boomerang Connectivity Table (BCT) of $S$ is defined by:

$$\mathrm{BCT}(\Delta X_i, \nabla Y_i) = \#\{x \in \mathbb{F}_2^s \mid S^{-1}(S(x) \oplus \nabla Y_i) \oplus S^{-1}(S(x \oplus \Delta X_i) \oplus \nabla Y_i) = \Delta X_i\}.$$

Following works studied the case of other cipher types and larger middle parts $E_m$. The so-called DBCT (for "Double Boomerang Connectivity Table"), first introduced in [HBS21] and later analyzed in depth in [YSS+22], is a table that studies two SPN rounds at once and which is defined as follows:

**Definition 2** (DBCT [HBS21, YSS+22])**.** Let $S$ be a bijective Sbox of $\mathbb{F}_2^s$ and let $\Delta X_i, \Delta Y_i, \nabla Y_i, \nabla Y_{i+1}$ be elements of $\mathbb{F}_2^s$. The Double Boomerang Connectivity Table (DBCT) of $S$ is defined by:

$$\mathrm{DBCT}(\Delta X_i, \nabla Y_{i+1}) = \sum_{\Delta Y_i, \nabla Y_i} \mathrm{UBCT}(\Delta X_i, \Delta Y_i, \nabla Y_i) \times \mathrm{LBCT}(\Delta Y_i, \nabla Y_i, \nabla Y_{i+1}).$$

Where the UBCT and LBCT are given as (see Figure 1):

**Definition 3** (UBCT and LBCT [WP19, SQH19, DDV20])**.** Let $S$ be a bijective Sbox of $\mathbb{F}_2^s$. The Upper Boomerang Connectivity Table (UBCT) and the Lower Boomerang Connectivity Table (LBCT) of $S$ are defined by:

$$\begin{aligned}\mathrm{UBCT}(\Delta X_i, \Delta Y_i, \nabla Y_i) = \#\{x \in \mathbb{F}_2^s \mid\ & S^{-1}(S(x) \oplus \nabla Y_i) \oplus S^{-1}(S(x \oplus \Delta X_i) \oplus \nabla Y_i) = \Delta X_i, \\ & S(x) \oplus S(x \oplus \Delta X_i) = \Delta Y_i\} \text{ where } \Delta X_i, \Delta Y_i, \nabla Y_i \in \mathbb{F}_2^s.\end{aligned}$$

$$\begin{aligned}\mathrm{LBCT}(\Delta X_i, \nabla X_i, \nabla Y_i) = \#\{x \in \mathbb{F}_2^s \mid\ & S^{-1}(S(x) \oplus \nabla Y_i) \oplus S^{-1}(S(x \oplus \Delta X_i) \oplus \nabla Y_i) = \Delta X_i, \\ & S(x) \oplus S(x \oplus \nabla X_i) = \nabla Y_i\} \text{ where } \Delta X_i, \nabla X_i, \nabla Y_i \in \mathbb{F}_2^s.\end{aligned}$$

The article by Yang and co-authors [YSS+22] also covered the case where a linear layer is in between of the two Sboxes considered in the initial definition, as detailed below.

**Definition 4** (General case of the DBCT [YSS+22])**.** Let $S$ be an Sbox layer and $M$ be a linear layer. The Double Boomerang Connectivity Table (DBCT) of $S \circ M \circ S$ is defined by:

$$\mathrm{DBCT}(\Delta X_i, \nabla Y_{i+1}) = \sum_{\substack{\Delta X_{i+1} = M(\Delta Y_i) \\ \nabla X_{i+1} = M(\nabla Y_i)}} \mathrm{UBCT}(\Delta X_i, \Delta Y_i, \nabla Y_i) \times \mathrm{LBCT}(\Delta X_{i+1}, \nabla X_{i+1}, \nabla Y_{i+1}).$$

## 1.2 Claim of Impossibility of Zhang, Wang and Tang

The related-tweakey impossible boomerang distinguisher proposed by Zhang *et al.* is copied in Figure 2. The authors explain that the contradiction happens in three consecutive rounds, namely round 13 to round 15, in which the following relation is verified:

$$\forall \alpha \in \mathbb{F}_2^8, \mathrm{DDT}(\alpha, \texttt{0x04}) \neq 0 \Rightarrow \mathrm{DBCT}(\texttt{0x05}, \alpha) = 0.$$

This is what defines the contradiction they rely on to affirm that the boomerang distinguisher is of probability 0.

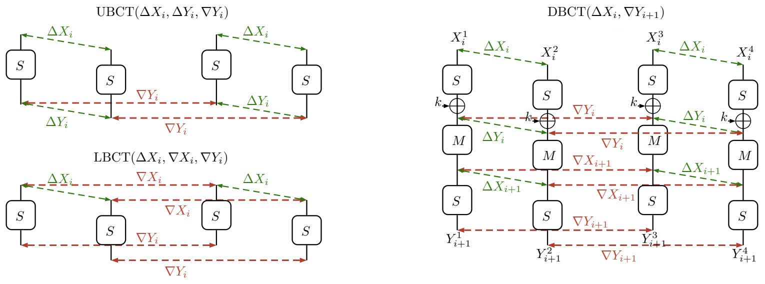


**Figure 1:** Parameters of the UBCT, of the LBCT and of the general case of the DBCT.

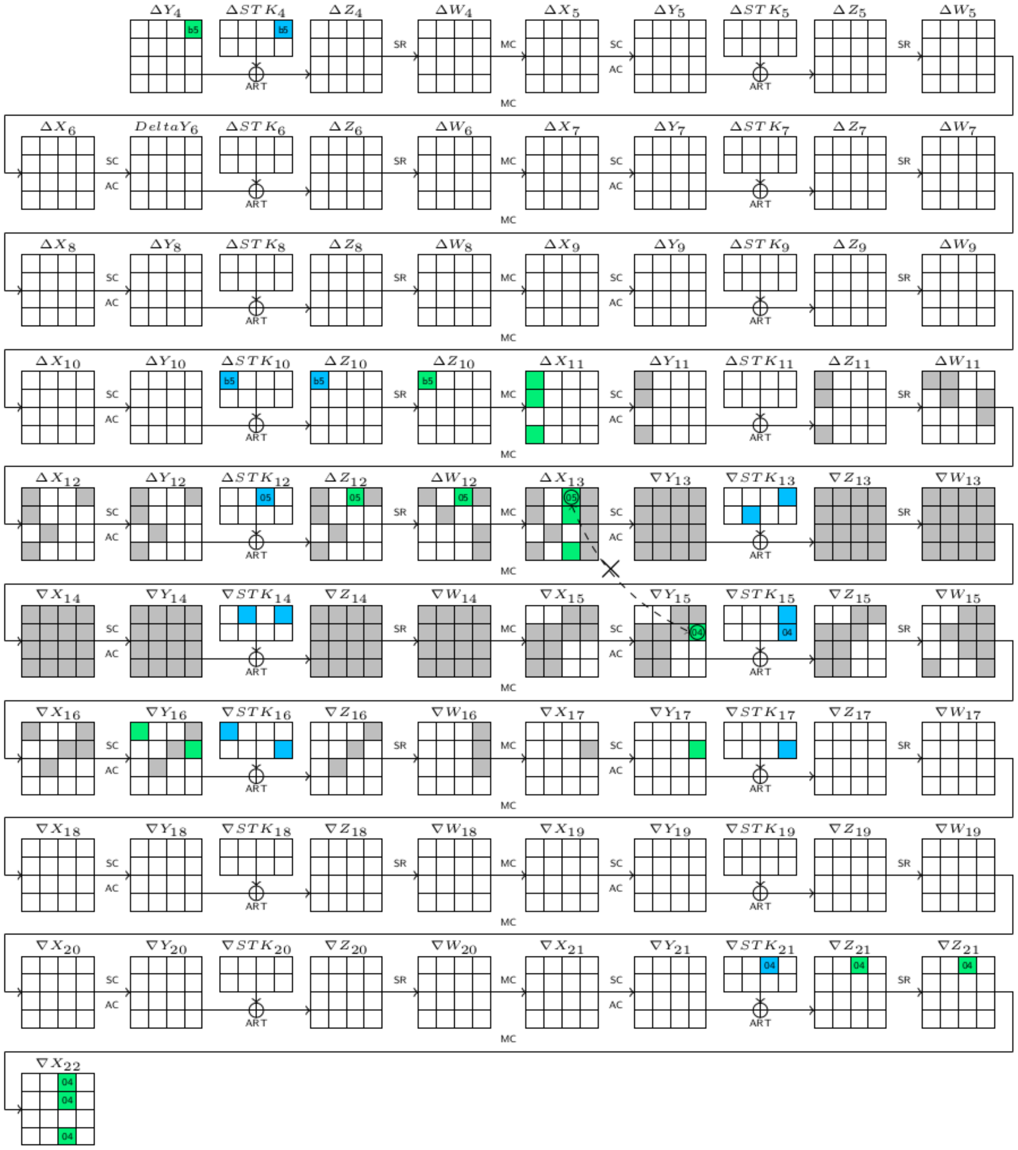
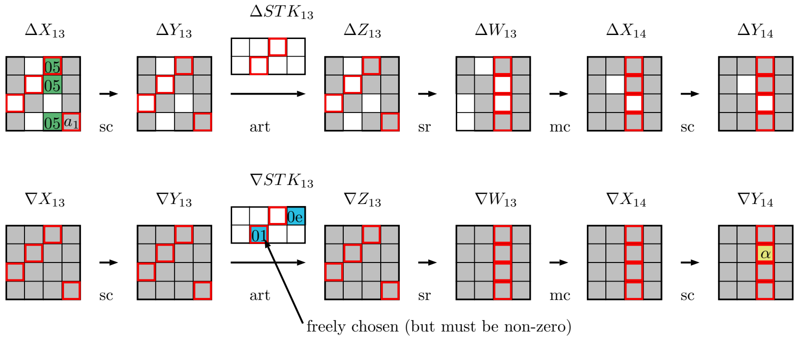


**Figure 2:** Screenshot of the 18-round related-tweakey impossible boomerang distinguisher relying on a DBCT contradiction of SKINNY-128-384 presented in [ZWT24].

# 2 Disproving the Impossibility

## 2.1 Details of the Configuration used in [ZWT24]

Figure 3 gives a close-up of the 2 rounds where the DBCT coefficient of value 0 appears. Given the structure of SKINNY [BJK+16][1], the probability of the 2-round boomerang switch is given by the product of the probability of the 4 2-round boomerang switches over each of the 32-bit Super-Sboxes (as they are independent one from the others). The specific Super-Sbox that is expected to have a boomerang switch probability of zero is highlighted in red.



freely chosen (but must be non-zero)

**Figure 3:** Close-up of the two rounds with a null DBCT used in the distinguisher of Zhang *et al.* [ZWT24]. The difference $\alpha$ is such that $\mathrm{DDT}(\alpha, \texttt{0x04}) \neq 0$.

## 2.2 Limits of the DBCT

The underlying assumption of the impossibility claimed in [ZWT24] is that if the DBCT coefficient is 0, then the corresponding 2-round boomerang is impossible. This is unfortunately not correct.

As can be seen on the right in Figure 1, the DBCT only takes into account quartets with equal differences on facing sides (the differences $\Delta Y_i$ and $\nabla Y_i$ appear twice). Thus, many transitions are not seen by the DBCT, which implies that by itself, having $\mathrm{DBCT}(\alpha, \beta) = 0$ is not a strong enough ground to build an impossible boomerang distinguisher.

To correctly evaluate the two-round switching probability, one must either use the DBCT* [WSW+23] (covering the cases where the input and output differences are the same on facing sides, but where all the possibilities are included for the middle differences) or the GDBCT [ZWT24] (covering the most generic case where even the input and output differences have no specific structure).

Another possibility would be to first prove that it is impossible to have middle differences that are not the same on facing sides to justify that the DBCT does compute the correct value. Such an example can be found in a research work simultaneous to the one of Zhang *et al.* and that relies on the properties of the middle linear layer $M$ [BCL+24].

In addition to the previous arguments, note that there is no reason for the two facing cells in line 2, column 3 to have the same "$\alpha$" difference in $\nabla Y_{14}$ in Figure 3.

## 2.3 Finding Actual Quartets

The previous remarks stress that the DBCT might not cover all the possible difference transitions over 2 rounds but they do not prove that the 2-round connection is possible in

[1] We refer the reader to the specification of SKINNY [BJK+16] for details on the round function.

**Table 1:** A quartet of columns encrypted with 2 rounds of SKINNY (SB-ARK-MC-SB), with $\alpha =$ `0x50` on both sides.

| | $x^1$ | $x^2$ | $x^3$ | $x^4$ |
|---|---|---|---|---|
| Input | `0xa7ed0098` | `0xb8ed009d` | `0xa0690090` | `0xbf690095` |
| Output | `0x8e521bd8` | `0xab523ac8` | `0xeb7d4b8c` | `0xce7d6a9c` |
| Middle key+constant | `0x00028862` | | `0x00028962` | |
| | $(x^1, x^2)$ | | $(x^3, x^4)$ | |
| Input difference $(\Delta X_{13})$ | `0x1f000005` | | `0x1f000005` | |
| After Sbox layer | `0x7d000026` | | `0x5d000006` | |
| | $(x^1, x^3)$ | | $(x^2, x^4)$ | |
| Output difference $(\nabla Y_{14})$ | $\texttt{0x652f}\underbrace{\texttt{50}}_{\alpha}\texttt{54}$ | | $\texttt{0x652f}\underbrace{\texttt{50}}_{\alpha}\texttt{54}$ | |

the given configuration. To prove it, we exhibit a returning Super-Sbox quartet, that we found experimentally.

We wrote a program in C language searching for quartets of 32-bit states that are consistent with the configuration represented in Figure 3. The program starts by picking a random key and brute-forces the possibilities. As the problem constraints are quite loose, we enforced some additional conditions, both to simplify the search and to obtain nicer solutions:

- The input difference in the last cell ($a_1$ in Figure 3) is fixed to an arbitrary value, `0x1f`, on both sides,
- the output differences after two rounds ($\nabla Y_{14}$ in Figure 3) is enforced to be the same on both sides.

An example of such quartet is given in Table 1. We can see that the differences of the quartet after the first Sbox layer are not identical on both sides, which is why it is not covered by the DBCT. The detail of the value evolution and of the difference propagation of this quartet is given in Figure 4 and Figure 5, respectively.

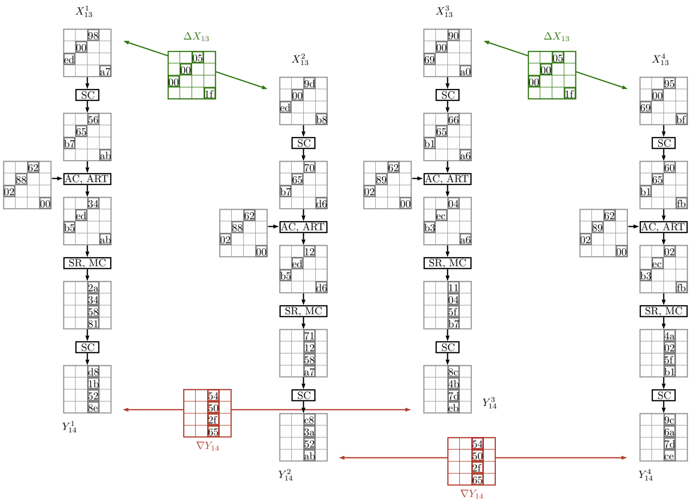


**Figure 4:** Example hexadecimal values of a Super-Sbox satisfying the trail depicted in Figure 3. ($\alpha =$ `0x50` and we can check that DDT(`0x50`, `0x04`) $= 64 \neq 0$ as required.)

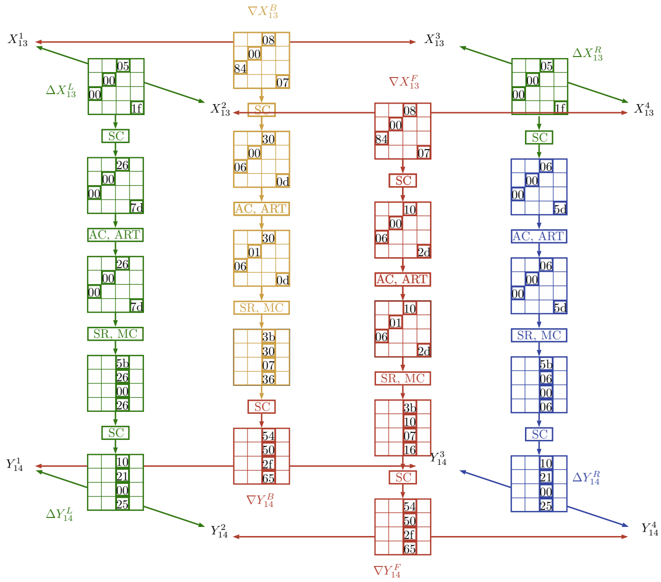


**Figure 5:** Evolution of the difference of the quartet detailed in Figure 4.

## Conclusion

In view of the observations made in this note we would like to reiterate the cautionary statement (already made in [BCL+24]) that the DBCT is a dangerous tool that does not capture the actual probability of a 2-round boomerang. Thus, it might lead to errors and do not allow as-is to conclude in an impossibility. The table that must be used is the DBCT* introduced in [WSW+23] (or its extensions like the GDBCT [ZWT24]) and that takes into account every possible middle transition.

We reached out to the authors of [ZWT24] and they confirmed our findings.

## Acknowledgments

The authors would like to thank the authors of [ZWT24] for their valuable feedback.

This work has been partially supported by the French Agence Nationale de la Recherche through the OREO project under Contract ANR-22-CE39-0015, and through the France 2030 program under grant agreement No. ANR-22-PECY-0010 CRYPTANALYSE.

## References

[BCL+24] Xavier Bonnetain, Margarita Cordero, Virginie Lallemand, Marine Minier, and María Naya-Plasencia. On impossible boomerang attacks: Application to simon and skinnyee. *IACR Transactions on Symmetric Cryptology*, 2024(2):222–253, Jun. 2024. URL: https://tosc.iacr.org/index.php/ToSC/article/view/11629, doi:10.46586/tosc.v2024.i2.222-253.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, Heidelberg, August 2016. doi:10.1007/978-3-662-53008-5_5.

[CHP+18] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 683–714. Springer, Heidelberg, April / May 2018. doi:10.1007/978-3-319-78375-8_22.

[DDV20] Stéphanie Delaune, Patrick Derbez, and Mathieu Vavrille. Catching the fastest boomerangs application to SKINNY. *IACR Transactions on Symmetric Cryptology*, 2020(4):104–129, 2020. doi:10.46586/tosc.v2020.i4.104-129.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 393–410. Springer, Heidelberg, August 2010. doi:10.1007/978-3-642-14623-7_21.

[HBS21] Hosein Hadipour, Nasour Bagheri, and Ling Song. Improved rectangle attacks on SKINNY and CRAFT. *IACR Transactions on Symmetric Cryptology*, 2021(2):140–198, 2021. doi:10.46586/tosc.v2021.i2.140-198.

[Lu08] Jiqiang Lu. *Cryptanalysis of block ciphers*. PhD thesis, University of London UK, 2008.

[Lu11] Jiqiang Lu. The (related-key) impossible boomerang attack and its application to the AES block cipher. *Des. Codes Cryptogr.*, 60(2):123–143, 2011. doi:10.1007/s10623-010-9421-9.

[LWL22] Chenmeng Li, Baofeng Wu, and Dongdai Lin. Generalized boomerang connectivity table and improved cryptanalysis of GIFT. In Yi Deng and Moti Yung, editors, *Information Security and Cryptology - 18th International Conference, Inscrypt 2022, Beijing, China, December 11-13, 2022, Revised Selected Papers*, volume 13837 of *Lecture Notes in Computer Science*, pages 213–233. Springer, 2022. doi:10.1007/978-3-031-26553-2_11.

[SQH19] Ling Song, Xianrui Qin, and Lei Hu. Boomerang connectivity table revisited. *IACR Transactions on Symmetric Cryptology*, 2019(1):118–141, 2019. doi:10.13154/tosc.v2019.i1.118-141.

[Wag99] David Wagner. The boomerang attack. In Lars R. Knudsen, editor, *Fast Software Encryption – FSE'99*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, Heidelberg, March 1999. doi:10.1007/3-540-48519-8_12.

[WP19] Haoyang Wang and Thomas Peyrin. Boomerang switch in multiple rounds. *IACR Transactions on Symmetric Cryptology*, 2019(1):142–169, 2019. doi:10.13154/tosc.v2019.i1.142-169.

[WSW+23] Libo Wang, Ling Song, Baofeng Wu, Mostafizar Rahman, and Takanori Isobe. Revisiting the boomerang attack from a perspective of 3-differential. *IEEE Transactions on Information Theory*, 2023. doi:10.1109/TIT.2023.3324738.

[YSS+22] Qianqian Yang, Ling Song, Siwei Sun, Danping Shi, and Lei Hu. New properties of the double boomerang connectivity table. *IACR Transactions on Symmetric Cryptology*, 2022(4):208–242, 2022. doi:10.46586/tosc.v2022.i4.208-242.

[ZWT24] Jianing Zhang, Haoyang Wang, and Deng Tang. Impossible boomerang attacks revisited: Applications to deoxys-bc, joltik-bc and skinny. *IACR Transactions on Symmetric Cryptology*, 2024(2):254–295, Jun. 2024. URL: https://tosc.iacr.org/index.php/ToSC/article/view/11631, doi:10.46586/tosc.v2024.i2.254-295.