Generalized Boomerang Connectivity Table and Improved Cryptanalysis of GIFT

Chenmeng Li[1,2], Baofeng Wu[1,2(✉)], and Dongdai Lin[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
{lichenmeng,wubaofeng,ddlin}@iie.ac.cn
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract. Boomerang connectivity table (BCT), an essential tool in boomerang attack, gives a unified description of the probability in the middle round of a boomerang distinguisher. However, it suffers the drawback that the asymmetric relationship between the upper and lower differentials in the middle round is ignored. To make up for this deficiency, we propose the generalized boomerang connectivity table (GBCT), which characterizes all combinations of upper and lower differentials to provide a more precise probability in the middle round. We first study the cryptographic properties of GBCT and introduce its variants applied in multiple rounds and Feistel structure. Then, we provide an automatic search algorithm to increase the probability of the boomerang distinguisher by adding thorough considerations that more trails can be included, which is applicable to all S-box based ciphers. Finally, we increase the probabilities of the 20-round GIFT-64 distinguisher from $2^{-58.557}$ to $2^{-57.43}$ and the 19-round GIFT-128 distinguisher from $2^{-109.626}$ to $2^{-108.349}$, both of which are the highest so far. Applying the key recovery attack proposed by Dong et al. at Eurocrypt 2022 on the new distinguisher, we achieve the lowest complexities of the attack on GIFT-64 and the best rectangle attack on GIFT-128.

Keywords: Rectangle attack · Automatic search algorithm · BCT · GIFT

1 Introduction

Differential cryptanalysis, proposed by Biham and Shamir [4] in 1990, is one of the most effective and widely used methods to attack many cryptographic primitives. However, it is often hard to find differential characteristics with high probabilities as the rounds of a cipher increase. In 1999, Wagner [21] proposed boomerang attack to replace one bad long differential trail with two good short

Y. Deng and M. Yung (Eds.): Inscrypt 2022, LNCS 13837, pp. 213–233, 2023.
https://doi.org/10.1007/978-3-031-26553-2_11

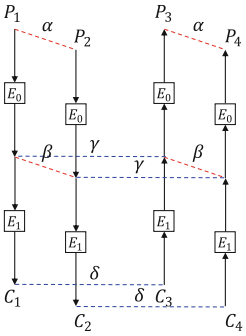

Fig. 1. The boomerang attack

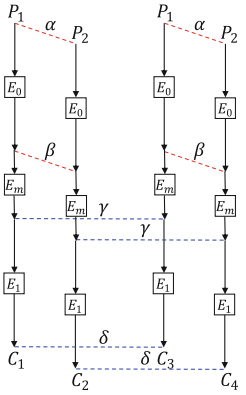

Fig. 2. The sandwich attack

differential trails. This attack makes it possible to conquer more rounds, and indicates that the security of a cipher cannot be guaranteed only by the non-existence of differentials with high probability.

In a boomerang attack, the target cipher E is decomposed into two parts as $E = E_1 \circ E_0$, where E_0 has a differential trail $\alpha \to \beta$ and E_1 has a differential trail $\gamma \to \delta$. Compositing the two sub-ciphers in a swerving way admits a boomerang distinguisher as long as $\beta \neq \gamma$, see Fig. 1. Under the independence assumption of E_0 and E_1, the probability of this distinguisher should be p^2q^2. However, it requires an adaptive chosen-plaintext/ciphertext scenario, which is not applicable to most key recovery settings. Then, the rectangle attack [3], a chosen-plaintext attack, is proposed to not only overcome this issue but also increase the probability of the distinguisher. It actually covers all possible differential trails $\alpha \to \beta_i$ for E_0 and $\gamma_j \to \delta$ for E_1 in the framework of a boomerang attack, thus increases the probability of the distinguisher to $2^{-n}\hat{p}^2\hat{q}^2$, where $\hat{p} = \sqrt{\sum_i \Pr^2(\alpha \to \beta_i)}$ and $\hat{q} = \sqrt{\sum_j \Pr^2(\gamma_j \to \delta)}$. To perform a rectangle attack, one needs to sieve right quarters (x, y, z, w) with $x \oplus y = z \oplus w = \alpha$ according to this probability.

It was noticed later that the independence assumption was invalid. To reveal this phenomenon, Biryukov and Khovratovich [5] proposed the boomerang switch to connect two differentials with a strong dependency. The observations were depicted in the framework of sandwich attack [13], which decomposes the cipher as $E = E_1 \circ E_m \circ E_0$, where the middle part E_m is the connection of the upper trail $\alpha \to \beta$ and the lower trail $\gamma \to \delta$, see Fig. 2. Then, E_m can be regarded as a small boomerang distinguisher with probability r, where

$$r = \Pr[E_m^{-1}(E_m(x) \oplus \gamma) \oplus E_m^{-1}(E(x \oplus \beta) \oplus \gamma) = \beta].$$

Thus, the probability of the whole boomerang distinguisher is $\hat{p}^2\hat{q}^2r$. Besides, Murphy [18] has pointed out that there may be incompatibility when connecting two independently chosen differential trails, which will result in an invalid

boomerang distinguisher. Since the dependency between these two differential trails has a great impact on the probability of a boomerang distinguisher, at Eurocrypt 2018, Cid et al. [10] captured the above observations in a unified table called boomerang connectivity table (BCT) when E_m is a single S-box layer. A new switch method named generalized switch was also depicted by the BCT.

As automatic tools has been widely used in searching for cryptographic distinguishers, it is natural to consider integrating BCTs with automatic tools to search for good distinguishers. There are mainly three automatic search tools in cryptanalysis, namely MILP (mixed integer linear programming), SAT/SMT (satisfiabality module theory) and Matsui's algorithm. Liu and Sasaki [17] gave the first generic model of BCT to search for related-key boomerang distinguishers with SMT. Later, Ji et al. [16] proposed an automatic search algorithm by improving Matsui's algorithm to search for the clustering of related-key differential trails utilized in the related-key boomerang distinguisher for GIFT-64 and GIFT-128, obtaining the best result up to now.

GIFT [2] is a lightweight block cipher with SPN structure. Because of its excellent performance in both hardware and software implementations, GIFT has been chosen as primitives in the design of many ciphers, such as GIFT-COFB [1], HYENA [8], LOCTUS-AEAD and LOCUS-AEAD [7], all of which are submitted to NIST's Lightweight Cryptography Project, with GIFT-COFB being selected as one of the ten finalists. Studying the security of GIFT is therefore crucial and imperative.

Our Contributions. The main contributions of this paper are summarized below.

1. **We propose a generalized boomerang connectivity table (GBCT).** The GBCT, which can be viewed as a generalized version of BCT, receives four distinct differences as input to determine the number of quartets that meet these four differences. Additionally, we study the cryptographic properties of GBCT and give some variants of GBCT applied in multiple rounds and Feistel structure.
2. **We provide a new search algorithm for boomerang distinguishers with considerations that more trails can be included, and increase the probability of distinguishers for GIFT.**
   By adding three additional factors to the algorithm in [16], a better automatic search algorithm for boomerang distinguishers is obtained. Firstly, we relax the condition of input/output differences from optimal to suboptimal to get a better clustering effect. Secondly, we modify their method of searching for differential trails to search for differentials within a probability range. Lastly, we incorporate GBCT to ensure the compatibility of E_0 and E_1. Using the new algorithm, we improved the probabilities of distinguishers for GIFT-64 and GIFT-128, which increase from $2^{-58.557}$ to $2^{-57.43}$ and from $2^{-109.626}$ to $2^{-108.349}$ respectively.

Table 1. Summary of the cryptanalytic results on GIFT

Rounds	Approach	Setting	Time	Data	Memory	Ref.
GIFT-64						
23	Boomerang	RK	$2^{126.60}$	$2^{63.3}$	–	[17]
25	Rectangle	RK	$2^{120.92}$	$2^{63.78}$	$2^{64.10}$	[16]
26	Differential	RK	$2^{123.23}$	$2^{60.96}$	$2^{120.86}$	[20]
26	Rectangle	RK	$2^{122.78}$	$2^{63.78}$	$2^{63.78}$	[12]
26	Rectangle	RK	$2^{121.75}$	$2^{62.715}$	$2^{62.715}$	Section 5
GIFT-128						
22	Boomerang	RK	$2^{112.63}$	$2^{112.63}$	2^{52}	[16]
23	Rectangle	RK	$2^{126.89}$	$2^{121.31}$	$2^{121.63}$	[16]
23	Rectangle	RK	$2^{125.175}$	$2^{120.175}$	$2^{120.175}$	Section 5
23	Differential	SK	2^{120}	2^{120}	2^{86}	[23]
26	Differential	SK	$2^{125.75}$	$2^{120.25}$	$2^{120.25}$	[16]

3. **We decrease the complexity of the attack on GIFT-64/GIFT-128 under the key recovery framework proposed by Dong et al.**
We apply the key recovery attack proposed by Dong et al. on the distinguishers and achieve a lower complexity than previous attacks. The data and time complexity drop from $2^{63.78}$ to $2^{62.72}$ and from $2^{122.78}$ to $2^{121.75}$ when attacking the 26-round GIFT-64. When attacking 23-round GIFT-128, the data and time complexity decrease from $2^{121.31}$ to $2^{120.175}$ and from $2^{126.89}$ to $2^{124.25}$ respectively. The current cryptanalytic results on GIFT are summarized in Table 1.

Outline. The rest of the paper is organized as follows. In Sect. 2, we give a brief overview of some previous work. In Sect. 3, we introduce the generalized boomerang connectivity table and study properties and variants of it. In Sect. 4, we outline the strategies for searching for a rectangle distinguisher, and give a new search algorithm. In Sect. 5, we provide the complexity analysis of the 26/23-round attacks on GIFT-64/GIFT-128. Section 6 concludes the paper.

2 Background and Previous Work

In this section, we give some preliminaries. First, we introduce some tables used to connect two sub-ciphers, such as BCT, BDT, EBCT (Figs. 3 and 4). Secondly, we give a brief introduction of some concepts necessary to search for a rectangle distinguisher, including the automatic search tool and the clustering effect. Finally, we recall the latest advances in key recovery attacks given in [12].

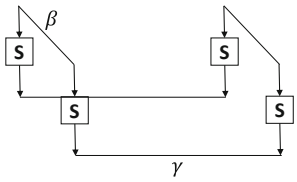

Fig. 3. Structure of BCT

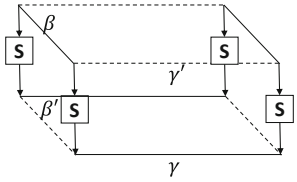

Fig. 4. Structures of BDT and EBCT

2.1 BCT, BDT, EBCT

BCT is the first unified tool for evaluating dependencies between E_0 and E_1, but only applicable when E_m is a single S-box layer. For $\beta,\ \gamma \in \mathbb{F}_2^n$, define

$$BCT(\beta,\gamma) = \#\{x \in \mathbb{F}_2^n \mid S^{-1}(S(x) \oplus \gamma) \oplus S^{-1}(S(x \oplus \beta) \oplus \gamma) = \beta\}.$$

Song et al. [19] noticed that dependencies could affect more rounds. Meanwhile, some practical experiments [9,17] showed that a higher probability could be achieved when E_m contained two rounds. It is reasonable to believe that the more rounds E_m contains, the more accurate the probability will be. Then, how to employ BCT in more rounds received much attention in the following research. Wang et al. [22] proposed a systematic analysis of the boomerang switching effect in multiple rounds and gave the boomerang difference table (BDT), renamed as UBCT in [11]. And its variant called BDT' is also denoted by D_{BCT} in [19] and renamed as LBCT in [11]. Its entry for $(\beta,\beta',\gamma) \in (\mathbb{F}_2^n)^3$ is computed by

$$BDT(\beta,\beta',\gamma) = \#\left\{x \in \mathbb{F}_2^n \;\middle|\; \begin{array}{l} S(x) \oplus S(x \oplus \beta) = \beta', \\ S^{-1}(S(x) \oplus \gamma) \oplus S^{-1}(S(x \oplus \beta) \oplus \gamma) = \beta \end{array}\right\}.$$

After that, Delaune et al. [11] provided a new table to connect two differentials in more than two rounds, called extended boomerang connectivity table (EBCT), where for $(\beta,\beta',\gamma,\gamma') \in (\mathbb{F}_2^n)^4$,

$$EBCT(\beta,\beta',\gamma',\gamma) = \#\left\{x \in \mathbb{F}_2^n \;\middle|\; \begin{array}{l} S(x) \oplus S(x \oplus \beta) = \beta',\ S(x) \oplus S(x \oplus \gamma') = \gamma, \\ S^{-1}(S(x) \oplus \gamma) \oplus S^{-1}(S(x \oplus \beta) \oplus \gamma) = \beta \end{array}\right\}.$$

Besides, Hadipour et al. [14] introduced a new tool to model the dependency in more rounds called double boomerang connectivity table (DBCT) and used it for automatic searching for boomerang distinguishers.

2.2 Automatic Tools Modeling BCT

Because of its efficiency and simplicity, automatic tools have become crucial techniques for cryptanalysis in recent years. The effect of many commonly used attacks can be improved with the help of automatic tools, not only in searching for distinguishers but also in key recovery attacks. In this paper, we propose an

algorithm to search for boomerang distinguishers with the automatic tool SMT. Here we give a brief introduction to it.

SMT is refereed to the problem of determining whether a mathematical formula is satisfiable. In cryptanalysis, one can use languages (e.g., SMTLIB2, CVC or BTOR) to model the property of components of a cipher, such as propagation of a differential and its probability, as an SMT problem, and obtain a desired solution (e.g., a differential trail with high probability) by SMT solvers. For example, in [17] the authors modelled the DDT and BCT with boolean constraints of an S-box. Following is an example of the description of BCT.

Example 1. Given boomerang propagations $(2 \rightarrow 5)$ and $(2 \rightarrow 6)$ of a 4×4 S-box with $BCT(2,5) = BCT(2,6) = 4$, we can model them with the logic expression $(x = 2) \wedge ((y = 5) \vee (y = 6))$. It is true when $x = 2$ and $y = 5$ or 6. Meanwhile, the probability is depicted by $w_4 = ((x = 2) \wedge (y = 5) \vee (x = 2) \wedge (y = 6))$, which means $w_4 = 1$ when the expression in the RHS is true, and the probability is obviously $4 \cdot w_4/16$.

2.3 Clustering Effect in Boomerang Distinguishers

When utilizing a boomerang distinguisher, two essential factors are the input and output differences and the probability of the boomerang trail. Except for the input and output differences, the specific value of the differentials in the middle rounds is no longer important. We use $\hat{r}$ to denote the probability of getting a right quartet that follows an exact boomerang trail. The actual probability r is composed of the probabilities $\hat{r}$ corresponding to all possible intermediate differences and hence r is always greater than or equal to any single $\hat{r}$. Ji et al. gave a definition of the clustering of the related-key differential trails utilized in an R-round related-key boomerang distinguisher and proposed an automatic search algorithm for boomerang distinguishers, which exploits the concept of clustering effect to make the probability improved [16].

2.4 Key-Recovery Algorithms for Rectangle Attacks

Much research has been done on the key recovery algorithm for the rectangle attacks. The first rectangle attack [3] was proposed by Biham et al. in 2001, and was applied to Serpent in the single-key setting. Later, numerous research have been done to reduce the complexity of the attacks. For ciphers with linear key schedules, Dong et al. recently built a new key recovery attack model, with which the ratio of right quartets greatly soared. They found the right quartets must satisfy some nonlinear relations, which could be exploited to filter the wrong ones, so as to increase the proportion of the right quartets and decrease the attack complexity. The key recovery attack on GIFT-64 with their algorithm is the best so far. Afterwards, Dong et al. [12] made some modifications on their algorithm to give a unified and generic key recovery algorithm, which achieved the optimal complexity by selecting different parameters. In order to better illustrate the advantage of the new distinguisher, we use the same attack in [12]

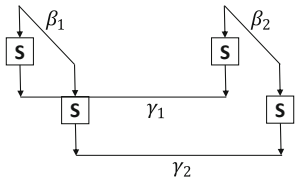

Fig. 5. Structure of GBCT

to launch on GIFT. Symbols used in the complexity analysis in Sect. 5 of our attack are the same to theirs as well.

3 Generalized Boomerang Connectivity Table

In this section, we give a generalized boomerang connectivity table (GBCT), which looses the limitation of the symmetric connections to be arbitrary. After that, some cryptographic properties of GBCT are exhibited. In addition, we present some variants of GBCT for multiple rounds and Feistel structure. Finally, the benefits of GBCT are illustrated by some applications.

3.1 Introduction to GBCT

The idea for generalizing the BCT is natural, that is, instead of considering symmetric differences in two directions of the connection part of two sub-ciphers, we take all possible values in four directions in to consideration, see Fig. 5. When loosing the limitation of the symmetric input and output differences to be arbitrary, all possible connections of two sub-ciphers E_0 and E_1 are covered. Thus, a more precise probability of a boomerang distinguisher can be obtained with GBCT. This idea was mentioned in the [14] with no formal description given.

Definition 1. *Let S be a permutation over $\mathbb{F}_2^n$ and $\beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathbb{F}_2^n$. The generalized boomerang connectivity table of S is a four-dimensional table, in which the entry for $(\beta_1, \beta_2; \gamma_1, \gamma_2)$ is computed by*

$$GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2) = \#\{x \in \mathbb{F}_2^n | S^{-1}(S(x) \oplus \gamma_1) \oplus S^{-1}(S(x \oplus \beta_1) \oplus \gamma_2) = \beta_2\}.$$

It is easy to see that GBCT can also be represented as

$$GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2) = \# \left\{ (x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \;\middle|\; \begin{array}{l} S(x) \oplus S(y) = \gamma_1, \\ S(x \oplus \beta_1) \oplus S(y \oplus \beta_2) = \gamma_2 \end{array} \right\}.$$

The probability for an S-box with a given quarter of differences $(\beta_1, \beta_2; \gamma_1, \gamma_2)$ is $p = \frac{1}{2^n} \times GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2)$. The time complexity for generating the GBCT for an n-bit S-box is $O(2^{4n})$.

In the following, we explain why GBCT can gain more solutions than BCT with the S-box of GIFT as an example.

Example 2. Given an input difference $\beta = 8$, and two output differences $\gamma_1 = 8$, $\gamma_2 = c$, the value of GBCT, DDT, and BCT are $GBCT(8,8;8,c) = 16$, $DDT(8,8) = DDT(8,c) = 0$, $BCT(8,8) = BCT(8,c) = 0$, respectively.

By looking up the DDT, we can find $\{\gamma_1' : DDT(\gamma_1', 8) = 2\} = \{\gamma_2' : DDT(\gamma_2', c) = 2\} = \{1,3,5,7,9,b,c,e\}$, and the solution for each input difference is shown in the following table.

γ_1'	1	3	5	7	9	b	c	e
(x_1, x_1')	$(2,3)$	(d,e)	$(9,c)$	$(0,7)$	$(1,8)$	$(4,f)$	$(6,a)$	$(5,b)$
γ_2'	1	3	5	7	9	b	c	e
(x_2, x_2')	(a,b)	$(5,6)$	$(1,4)$	$(8,f)$	$(9,0)$	$(c,7)$	$(2,e)$	$(3,d)$

It is clear that $(x_1, x_1') \oplus (x_2, x_2') = (8,8)$ always holds when $\gamma_1' = \gamma_2'$. That means if (x_1, x_1') and (x_2, x_2') are the solutions of two faces of a boomerang structure, we can use a difference $\beta_1 = \beta_2 = 8$ to connect the differential trails on both sides to get a boomerang trail. Due to the symmetry of solutions, we can obtain 16 solutions in total.

Example 3. Given two input differences $\beta_1 = 1$, $\beta_2 = 7$ and an output difference $\gamma = 5$, the value of GBCT, DDT, and BCT are $GBCT(1,7;5,5) = 10$, $DDT(1,5) = DDT(7,5) = 2$, $BCT(1,5) = BCT(7,5) = 2$, respectively. By looking up the DDT, we can find $\{\gamma' : DDT(\gamma', 5) = 2 \text{ or } 4\} = \{1,2,3,4,5,7\}$. Solutions of $DDT(\gamma', 5) > 0$ are given below.

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

Let $\beta_1 = 1$ and $\beta_2 = 7$, we can get $(x \oplus \beta_1, x' \oplus \beta_2)$ as follows.

(x, x')	$(c,d)(d,c)$	$(0,2)(2,0)$	$(4,6)(6,4)$	$(8,b)(b,8)$	$(1,5)(5,1)$	$(3,7)(7,3)$	$(a,f)(f,a)$	$(9,e)(e,9)$
$(x \oplus \beta_1, x' \oplus \beta_2)$	$(d,a)(c,b)$	$(1,5)(3,7)$	$(5,1)(7,3)$	$(9,c)(a,f)$	$(0,2)(4,6)$	$(2,0)(6,4)$	$(b,8)(e,d)$	$(8,9)(f,e)$

When x and x' are shifted by $\beta_1 = 1$ and $\beta_2 = 7$ respectively, there are 10 solutions whose output differences are 5. A boomerang trail can be obtained by connecting the differential trails on both sides of a boomerang structure with differences $\beta_1 = 1$ and $\beta_2 = 7$.

It can be concluded from the above examples that for a boomerang structure, (x_1, x_1') and (x_2, x_2') are solutions to differential trails $\gamma_1' \to \gamma_1$ and $\gamma_2' \to \gamma_2$ respectively on both sides of the structure, then $GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2) > 0$ as long as there exists two differences β_1 and β_2 such that $(x_2 \oplus \beta_1, x_2' \oplus \beta_2) = (x_1, x_1')$.

3.2 Properties of GBCT

In the following we give some basic properties of GBCT and its links with other tables, most of which can be deduced directly from the definition, so some proofs are omitted here.

Proposition 1. *(Symmetry of GBCT)*

$$\begin{aligned}&GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2)\\ &= GBCT(\beta_2, \beta_1; \gamma_1, \gamma_2) = GBCT(\beta_1, \beta_2; \gamma_2, \gamma_1) = GBCT(\beta_2, \beta_1; \gamma_2, \gamma_1).\end{aligned}$$

Proposition 2. *(Telations with DDT and BCT)*

$$\begin{aligned}&GBCT(\beta, \beta; \gamma, \gamma) = BCT(\beta; \gamma), \quad GBCT(\beta_2, \beta_1; 0, \gamma_2) = DDT(\beta_1 \oplus \beta_2; \gamma_2),\\ &GBCT(0, \beta_2; \gamma_1, \gamma_2) = DDT(\beta_2; \gamma_1 \oplus \gamma_2).\end{aligned}$$

Proposition 3. *(Summation formula I)*

$$\begin{aligned}\sum_{\beta_1} GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2) &= \sum_{\beta_2} GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2) = 2^n,\\ \sum_{\gamma_1} GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2) &= \sum_{\gamma_2} GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2) = 2^n.\end{aligned}$$

Proposition 4. *(Summation formula II)*

$$\sum_{\beta_1, \beta_2} GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2) = \sum_{\gamma_1, \gamma_2} GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2) = 2^{2n}.$$

Proposition 5.

$$GBCT_{S^{-1}}(\gamma_1, \gamma_2; \beta_1, \beta_2) = GBCT_S(\beta_1, \beta_2; \gamma_1, \gamma_2).$$

Proposition 6.

$$\begin{aligned}&GBCT(\beta_1, \beta_2; \gamma_1, \gamma_2)\\ &= CDDT(\beta_1, \gamma_2; \beta_2, \gamma_1) + \sum_{\alpha \neq 0, \beta_2} \#\left(\bigcup_{\alpha, \gamma_1} \cap \left(\bigcup_{\alpha \oplus \gamma_1 \oplus \gamma_2, \gamma_2} \oplus \beta_1\right)\right),\end{aligned}$$

where $\bigcup_{a,b} := \{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus a) = b\}$ *and the cross-DDT of* S *is*

$$CDDT(\beta_1, \gamma_2; \beta_2, \gamma_1) = \#\left\{x \in \mathbb{F}_2^n \;\middle|\; \begin{array}{l} S(x) \oplus S(x \oplus \beta_1) = \gamma_2,\\ S(x) \oplus S(x \oplus \beta_2) = \gamma_1 \end{array}\right\}.$$

Proposition 7.

$$GBCT(\beta_1,\beta_2;\gamma_1,\gamma_2) = \frac{1}{2^{4n}} \cdot \sum_{a,b,c,d} (-1)^{a\cdot\gamma_1 \oplus b\cdot\gamma_2 \oplus c\cdot\beta_1 \oplus d\cdot\beta_2} \cdot W_F(c,a) \cdot W_F(c,b) \cdot W_F(d,a) \cdot W_F(d,b).$$

where $W_F(u,v) := \sum_x (-1)^{ux\oplus vF(x)}$.

Proof. We have

$$\begin{aligned}
&GBCT(\beta_1,\beta_2;\gamma_1,\gamma_2)\\
&= \#\{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n | F(x)\oplus F(y) = \gamma_1,\ F(x\oplus\beta_1)\oplus F(y\oplus\beta_2) = \gamma_2\}\\
&= \frac{1}{2^{2n}} \sum_{x,y}\sum_{a,b} (-1)^{a(F(x)\oplus F(y)\oplus\gamma_1)} (-1)^{b(F(x\oplus\beta_1)\oplus F(y\oplus\beta_2)\oplus\gamma_2)}\\
&= \frac{1}{2^{2n}} \sum_{a,b} (-1)^{a\gamma_1\oplus b\gamma_2} \sum_{x,y} (-1)^{a\cdot F(x)\oplus b\cdot F(x\oplus\beta_1)} (-1)^{a\cdot F(y)\oplus b\cdot F(y\oplus\beta_2)}\\
&= \frac{1}{2^{2n}} \sum_{a,b} (-1)^{a\gamma_1\oplus b\gamma_2} C_{\beta_1}(a,b) C_{\beta_2}(a,b),
\end{aligned}$$

where

$$\begin{aligned}
C_\beta(a,b) &= \sum_x (-1)^{a\cdot F(x)\oplus b\cdot F(x\oplus\beta)}\\
&= \frac{1}{2^n} \sum_w (-1)^{w(x\oplus y)} \sum_{x,y} (-1)^{a\cdot F(x)\oplus F(y\oplus\beta)}\\
&= \frac{1}{2^n} \sum_w (-1)^{w\cdot z} \sum_{x,z} (-1)^{a\cdot F(x)\oplus b\cdot F(x\oplus z\oplus\beta)}\\
&= \frac{1}{2^n} \sum_{w,x,z} (-1)^{[a\cdot F(x)\oplus w\cdot x]\oplus[b\cdot F(x\oplus z\oplus\beta)\oplus w(x\oplus z\oplus\beta)]\oplus w\cdot\beta}\\
&= \frac{1}{2^n} \sum_w (-1)^{w\cdot\beta} W_F(w,a)\cdot W_F(w,b).
\end{aligned}$$

Proposition 8. *Let* F, G *be two permutations of* $\mathbb{F}_2^n$ *with* $G = F \circ L$ *for an invertible affine transformation* L *of* $\mathbb{F}_2^n$. *Then we have*

$$g_G(a_1,a_2;b_1,b_2) = g_F(L_1(a_1), L_1(a_2), L_2^{-1}(b_1), L_2^{-1}(b_2)).$$

for all $a,b \in \mathbb{F}_2^n$, *where* $g_F(a_1,a_2;b_1,b_2) = GBCT(a_1,a_2;b_1,b_2)$ *for* F.

3.3 Variants of GBCT

GBCT in Multi-rounds. Just as how Wang et al. extend BCT to be used in two-round E_m, GBCT can also be converted with the same idea to be applied in two rounds. We introduce the generalized boomerang differential table (GBDT) (Fig. 6).

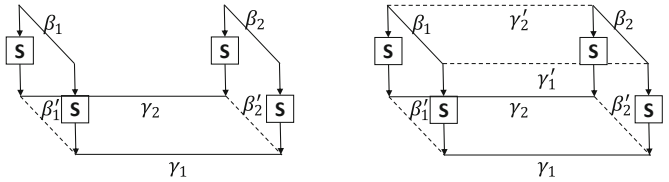

Fig. 6. Structures of GBDT (left) and GBET (right)

Definition 2. *Let S be a permutation over $\mathbb{F}_2^n$ and $\beta_1, \beta_2, \gamma_1, \gamma_2, \beta'_1, \beta'_2 \in \mathbb{F}_2^n$. The generalized boomerang differential table (GBDT) of S is a 6-dimensional table, in which the entry for $(\beta_1, \beta_2; \gamma_1, \gamma_2; \beta'_1, \beta'_2)$ is computed by*

$$GBDT(\beta_1, \beta_2; \gamma_1, \gamma_2; \beta'_1, \beta'_2) = \#\left\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \;\middle|\; \begin{array}{l} S(x) \oplus S(y) = \gamma_1, S(x \oplus \beta_1) \oplus S(y \oplus \beta_2) = \gamma_2, \\ S(x) \oplus S(x \oplus \beta_1) = \beta'_1, S(x) \oplus S(x \oplus \beta_2) = \beta'_2 \end{array}\right\}.$$

GBDT and BDT shares some properties, most of which can be easily obtained from the definition, so it is not proved here. Refer interested readers to [22] for more details.

Next, we use the same notations as in [22] to show how to calculate the probability with GBDT. The probability of a two-round E_m is the product of the two probabilities $r = p_1 p_2$, where

$$p_1 = \prod_{(\Delta_1, \Delta_2; \nabla''_1, \nabla''_2; \Delta'_1, \Delta'_2) \in L_1} GBDT(\Delta_1, \Delta_2; \nabla''_1, \nabla''_2; \Delta'_1, \Delta'_2)/2^n,$$

$$p_2 = \prod_{(\nabla_1, \nabla_2; \Delta''_1, \Delta''_2; \nabla'_1, \nabla'_2) \in L_2} GBDT(\nabla_1, \nabla_2; \Delta''_1, \Delta''_2; \nabla'_1, \nabla'_2)/2^n.$$

When E_m covers more rounds, we can borrow the idea of EBCT [11] to give the definition of GBET.

Definition 3. *Let S be a permutation over $\mathbb{F}_2^n$ and $\beta_1, \beta_2, \gamma_1, \gamma_2, \beta'_1, \beta'_2, \gamma'_1, \gamma'_2 \in \mathbb{F}_2^n$. The generalized boomerang extended table (GBET) of S is a 8-dimensional table, in which the entry for $(\beta_1, \beta_2; \gamma_1, \gamma_2; \beta'_1, \beta'_2; \gamma'_1, \gamma'_2)$ is computed by*

$$GBET(\beta_1, \beta_2; \gamma_1, \gamma_2; \beta'_1, \beta'_2; \gamma'_1, \gamma'_2) = \#\left\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \;\middle|\; \begin{array}{l} x \oplus y = \gamma'_1, (x \oplus \beta_1) \oplus (y \oplus \beta_2) = \gamma'_2, \\ S(x) \oplus S(x \oplus \beta_1) = \beta'_1, S(y) \oplus S(y \oplus \beta_2) = \beta'_2, \\ S(x) \oplus S(y) = \gamma_1, S(x \oplus \beta_1) \oplus S(y \oplus \beta_2) = \gamma_2 \end{array}\right\}.$$

When E_m covers more rounds, the probability is $r = \prod_i p_i$, where

$$p_i = \prod_{(\Delta_1, \Delta_2; \nabla_1, \nabla_2; \nabla'_1, \nabla'_2; \Delta'_1, \Delta'_2) \in L_i} GBDT(\Delta_1, \Delta_2; \nabla_1, \nabla_2; \nabla'_1, \nabla'_2; \Delta'_1, \Delta'_2)/2^n,$$

and L_i has the same meaning as the previous one.

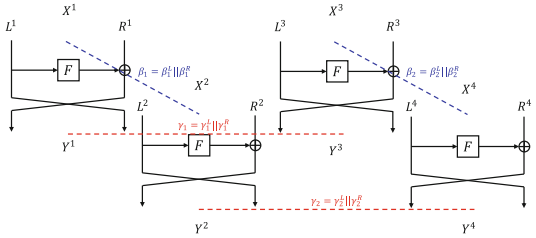

Fig. 7. The GBCT in a Feistel structure

Put GBCT into a Feistel Structure. The FBCT was proposed as a counterpart of BCT for Feistel structures and its properties have also been studied in [6,15]. Similar to BCT, GBCT is also applicable into Feistel structures. Here we take a generic Feistel structure as example, as shown in Fig. 7. Denote the output after one round of $X^i = L^i||R^i, i = 1, ..., 4$ as $Y^i = G^i||L^i, i = 1, ..., 4$. Assume that $X^1 \oplus X^2 = \beta_1 = \beta_1^L||\beta_1^R$, $Y^1 \oplus Y^3 = \gamma_1 = \gamma_1^L||\gamma_1^R$ and $Y^2 \oplus Y^4 = \gamma_2 = \gamma_2^L||\gamma_2^R$. Now, we check whether $X^3 \oplus X^4 = \beta_2 = \beta_2^L||\beta_2^R$:

$$
\begin{aligned}
\beta_2^L &= L^3 \oplus L^4 = L^1 \oplus \gamma_1^R \oplus L^2 \oplus \gamma_2^R = \beta_1^L \oplus \gamma_1^R \oplus \gamma_2^R, \\
\beta_2^R &= R^3 \oplus R^4 = F(L^3) \oplus G^3 \oplus F(L^4) \oplus G^4 \\
&= R^1 \oplus R^2 \oplus \gamma_1^L \oplus \gamma_2^L \oplus F(L^1) \oplus F(L^1 \oplus \gamma_1^R) \oplus F(L^2) \oplus F(L^2 \oplus \gamma_2^R) \\
&= \beta_1^R \oplus \gamma_1^L \oplus \gamma_2^L \oplus F(L^1) \oplus F(L^1 \oplus \gamma_1^R) \oplus F(L^1 \oplus \beta_1^L) \oplus F(L^1 \oplus \beta_1^L \oplus \gamma_2^R).
\end{aligned}
$$

If $X^3 \oplus X^4 = \beta_2$, then β_2 should satisfy $\beta_2^L = \beta_1^L \oplus \gamma_1^R \oplus \gamma_2^R$ and $\beta_2^R = \beta_1^R \oplus \gamma_1^L \oplus \gamma_2^L \oplus F(L^1) \oplus F(L^1 \oplus \gamma_1^R) \oplus F(L^1 \oplus \beta_1^L) \oplus F(L^1 \oplus \beta_1^L \oplus \gamma_2^R)$.

We degenerate the F function to the S-box layer. For each S-box, the input difference deduced from $\beta_i^L, i = 1, 2$ and $\gamma_i^R, i = 1, 2$ are denoted as $\Delta_i^L, i = 1, 2$ and $\Delta_i^R, i = 1, 2$. The output differences are denoted as $\nabla_i, i = 1, 2$ which are deduced from $\beta_i^R \oplus \gamma_i^L$. Then, the definition of FGBCT for each S-box is given below:

Definition 4. *Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $\Delta_1^L, \Delta_1^R, \Delta_2^L, \Delta_2^R, \nabla_1, \nabla_2 \in \mathbb{F}_2^n$. The FGBCT of S is given by a 6-dimensional table, in which the entry for the $(\Delta_1^L, \Delta_1^R; \Delta_2^L, \Delta_2^R; \nabla_1, \nabla_2)$ position is given by*

$$
\begin{aligned}
&FGBCT(\Delta_1^L, \Delta_1^R; \Delta_2^L, \Delta_2^R; \nabla_1, \nabla_2) \\
&= \#\left\{ x \in \mathbb{F}_2^n \;\middle|\; \begin{array}{l} S(x) \oplus S(x \oplus \Delta_1^L) \oplus S(x \oplus \Delta_1^R) \oplus S(x \oplus \Delta_1^L \oplus \Delta_2^R) \oplus \nabla_1 \oplus \nabla_2 = 0, \\ \Delta_1^L \oplus \Delta_2^L \oplus \Delta_1^R \oplus \Delta_2^R = 0 \end{array} \right\}.
\end{aligned}
$$

Then, the probability of a boomerang for a Feistel structure with an S-box is given by $2^{-n} \cdot FGBCT(\Delta_1^L, \Delta_1^R; \Delta_2^L, \Delta_2^R; \nabla_1, \nabla_2)$.

Similarly, we give the definition of FGBDT and FGBET used in multi-round E_m. Symbols in the definitions are shown in the Fig. 8.

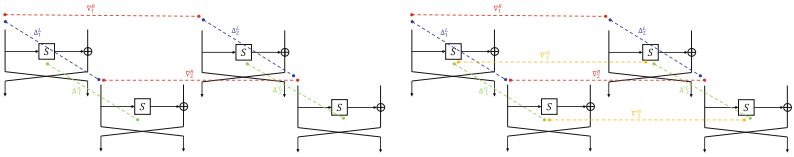

Fig. 8. Structures of FGBDT and FGBET

Definition 5. *Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$, and the differences $\Delta_1^L, \Delta_1^R, \Delta_2^L, \Delta_2^R, \nabla_1, \nabla_2, {\Delta'_1}^L, {\Delta'_2}^L \in \mathbb{F}_2^n$. The FGBDT of S is given by a 8-dimensional table, in which the entry for the $(\Delta_1^L, \Delta_1^R; \Delta_2^L, \Delta_2^R; \nabla_1, \nabla_2; {\Delta'_1}^L, {\Delta'_2}^L)$ position is given by*

$$
\begin{aligned}
&FGBDT(\Delta_1^L, \Delta_1^R; \Delta_2^L, \Delta_2^R; \nabla_1, \nabla_2; {\Delta'_1}^L, {\Delta'_2}^L) \\
&= \#\left\{ x \in \mathbb{F}_2^n \;\middle|\; \begin{array}{l} S(x) \oplus S(x \oplus \Delta_1^L) \oplus S(x \oplus \Delta_1^R) \oplus S(x \oplus \Delta_1^L \oplus \Delta_2^R) \oplus \nabla_1 \oplus \nabla_2 = 0, \\ \Delta_1^L \oplus \Delta_2^L \oplus \Delta_1^R \oplus \Delta_2^R = 0, \\ S(x) \oplus S(x \oplus \Delta_1^L) = {\Delta'_1}^L, S(x) \oplus S(x \oplus \Delta_2^L) = {\Delta'_2}^L \end{array} \right\}.
\end{aligned}
$$

Definition 6. *Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$, and the differences $\Delta_1^L, \Delta_1^R, \Delta_2^L, \Delta_2^R, \nabla_1, \nabla_2, {\Delta'_1}^L, {\Delta'_2}^L, {\Delta'_1}^R, {\Delta'_2}^R \in \mathbb{F}_2^n$. The FGBET of S is given by a 10-dimensional table, in which the entry for the $(\Delta_1^L, \Delta_1^R; \Delta_2^L, \Delta_2^R; \nabla_1, \nabla_2; {\Delta'_1}^L, {\Delta'_2}^L; {\Delta'_1}^R, {\Delta'_2}^R)$ position is given by*

$$
\begin{aligned}
&FGBET(\Delta_1^L, \Delta_1^R; \Delta_2^L, \Delta_2^R; \nabla_1, \nabla_2; {\Delta'_1}^L, {\Delta'_2}^L; {\Delta'_1}^R, {\Delta'_2}^R) \\
&= \#\left\{ x \in \mathbb{F}_2^n \;\middle|\; \begin{array}{l} S(x) \oplus S(x \oplus \Delta_1^L) \oplus S(x \oplus \Delta_1^R) \oplus S(x \oplus \Delta_1^L \oplus \Delta_2^R) \oplus \nabla_1 \oplus \nabla_2 = 0, \\ \Delta_1^L \oplus \Delta_2^L \oplus \Delta_1^R \oplus \Delta_2^R = 0, \\ S(x) \oplus S(x \oplus \Delta_1^L) = {\Delta'_1}^L, S(x) \oplus S(x \oplus \Delta_2^L) = {\Delta'_2}^L, \\ S(x) \oplus S(x \oplus \nabla_1^R) = {\nabla'_1}^R, S(x) \oplus S(x \oplus \nabla_2^R) = {\nabla'_2}^R \end{array} \right\}.
\end{aligned}
$$

3.4 The Advantages of GBCT

The probability of a boomerang distinguisher with BCT in one-round E_m is calculated in [16] as

$$\hat{p}^2\hat{q}^2 = \frac{1}{2^n}\sum_{i,j} p_i^2 \cdot q_j^2 \cdot BCT(\beta_i, \gamma_j).$$

For each boomerang trail $\alpha \to \beta_i \to \gamma_j \to \delta$, if the value of $BCT(\beta_i, \gamma_j)$ is 0, even if the value of $p_i^2 \cdot q_j^2$ is high enough, the trail is still in vain. Yet, BCT is limited to connecting β and γ that are symmetric in two faces of E_m, leaving out a large number of asymmetric combinations, which can be completed by GBCT.

In order to illustrate that GBCT can completely describe all combinations of β and γ, we list the distribution of GBCTs of some 4-bit S-boxes used in cryptographic primitives in Table 2, where the blue font represents the corresponding value of BCT. It turns out that GBCT can provide some probabilities that BCT cannot. The following example illustrates a boomerang trail that is incompatible when connecting E_0 and E_1 via BCT but effective with GBCT.

Table 2. GBCTs of 4-bit S-boxes from Sage's `Cryptography` package; see https://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/sboxes.html

S-boxs	Prob.									
	1	0.63	0.5	0.44	0.38	0.31	0.25	0.19	0.13	0.06
GIFT	34(32)	6(2)	48(12)	0	278(6)	24	2426(30)	0	16212(72)	15424
PRESENT	33(33)	0	108(8)	0	60(12)	40	2856(36)	0	16172(60)	16096
SKINNY_4	37(33)	0	116(16)	0	64(0)	96	3028(32)	0	16040(72)	16440
Elephant	35(33)	0	112(12)	0	64(8)	64	2900(32)	0	16140(64)	16184
KNOT	33(33)	0	108(8)	0	60(6)	40	2856(36)	1240	16172(60)	16096
Spook	37(33)	0	116(16)	0	64(0)	96	3028(32)	840	16040(72)	16440
GOST_1	34(32)	6(2)	48(12)	0	278(6)	24	2426(30)	1736	16212(72)	15424
LBlock_0	37(33)	10(0)	116(16)	0	64(0)	96	3028(32)	840	16040(72)	16440
SERPENT_S0	35(33)	0	112(12)	0	64(8)	64	2900(32)	1128	16104(64)	16184
KLEIN	31(31)	4(4)	0	16	62(14)	0	1807(23)	2512	16184(72)	17384
Midori_Sb0	33(33)	0	108(8)	0	60(12)	40	2856(36)	1240	16172(60)	16096
Piccolo	37(33)	0	116(16)	0	64(0)	96	3028(32)	840	16040(72)	16440
Pride	37(33)	0	116(16)	0	64(0)	96	3028(32)	840	16040(72)	16440
PRINCE	31(31)	1(1)	2(2)	0	75(11)	60	1824(28)	2380	15970(78)	17888
Rectangle	33(33)	0	108(8)	0	60(12)	40	2856(36)	1240	16172(60)	16096
TWINE	31(31)	0	0	0	30(30)	0	1455(15)	2280	17940(60)	16320
BLAKE_1	31(31)	0	75(7)	4	90(14)	114	2056(40)	2756	14990(66)	16680
Iceberg_S0	31(31)	4(4)	0	16	62(14)	0	1807(23)	2512	16184(72)	17384
Kuznyechik_nu0	31(31)	0	0	0	166(14)	80	1275(27)	2608	16732(84)	17256
Serpent_type_S0	33(33)	0	108(8)	0	60(12)	40	2856(36)	1240	16172(60)	16096
Golden_S0	31(31)	1(1)	13(5)	0	58(14)	148	1980(28)	2508	15525(69)	17344

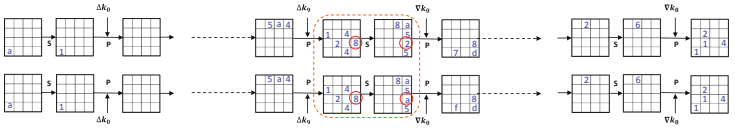

Fig. 9. 20-round boomerang trail with GBCT

Example 4. A 20-round boomerang trail of GIFT-64 with GBCT is shown in Fig. 9. The trail is obtained by connecting two 10-round related-key differential trails in E_0 and two 9-round related-key differential trails in E_1 with GBCT. And two key differences are

$$\Delta iniK = 0x0004000000000800000000000000010,$$
$$\nabla iniK = 0x2000000000000000800000002000800$$

The probability of this distinguisher is $p^2q^2r = 2^{-21\cdot2} \cdot 2^{-15\cdot2} \cdot 2^{-1} = 2^{-73}$ when connected with GBCT, but 0 when connected with BCT.

4 New Search Algorithm for a Boomerang Distinguisher

The instance in Example 4 illustrates the effectiveness of using GBCT as the connection in a boomerang trail. Then, we consider to construct a generic model of the GBCT with automatic the search tool SMT, and search for boomerang distinguishers.

4.1 Strategies in the Search Algorithm

In [16], Ji et al. proposed an automatic search algorithm to boost the probability of a related-key boomerang distinguisher by taking the cluster effect into account, which has the best performance in searching for boomerang distinguishers. Making some improvements on the base of the algorithm, we obtain a new search algorithm performing better. With the new algorithm, we get boomerang distinguishers with higher probabilities for GIFT-64 and GIFT-128. The details of the distinguishers will be given in the next subsection.

Here gives the strategy to search for a rectangle distinguisher. Firstly, we find that when searching for the 10-round differential trails the optimal probability is $2^{-19.83}$, rather than $2^{-20.415}$ searched in [16]. The details of the optimal differentials are listed in Table 6 in Appendix A. Taking the probability range $bw = 4$, and choosing the optimal α, we discover that it has only 263 output differences β_i and a total of 308 trails can be obtained, which is smaller than the quantity of that with the suboptimal α, who has 2944 distinct β_i and a total of 5728 trails. Thus, to get a better cluster effect, we should select α and δ with more β and γ in the first phase. In addition, replacing the probability of each differential trail with the probability of differential is a better way to approximate the real probability. Thirdly, the completeness of the connections in E_m should be ensured to form more valid boomerang trails. Finally, an improved boomerang distinguisher search Algorithm 1 is proposed in light of the aforementioned factors. And the search algorithm in single-key setting can be obtained likewise. Symbols used in Algorithm 1 is explained in Table 3.

Table 3. Symbols in Algorithm 1

$P(\cdot)$, $K(\cdot)$	PermBits operation, AddRoundKey operation
ΔX_i, ΔY_i	the differential value of X_i, Y_i in round i
$\Delta iniK_i$, $\nabla iniK_j$	the master key difference of differential trails in E_0, E_1
$W(l)$	the weight of the differential trail l
B_R, $\bar{B}_R$	the weight of the R-round optimal, sub-optimal trails
B_{c_R}	the upper bound of B_R
bw, $\bar{bw}$	$bw = B_{c_R} - B_R$, $\bar{bw} \geq bw$

Algorithm 1: The search algorithm for related-key boomerang distinguishers

Input: R_0, R_1; bw, $\bar{bw}$
Output: Pd; ΔY_1^i, $\Delta iniK_i$; $\Delta X^j_{R_1-1}$, $\nabla iniK_j$

Phase 1: Determine all the distinct $\Delta Y_1^i, \Delta iniK_i$ and $\Delta X^j_{R_1-1}, \nabla iniK_j$ with minimal and sub minimal weight
Search for the R_0-round related-key differential trails with B_{R_0} and $\bar{B}_{R_0}$ for E_0 with SMT.
$\Delta Y_1^i, \Delta iniK_i$ and $B^i_{R_0}$, $1 \le i \le m \leftarrow$ first-round output difference, the master key difference and weight of each R_0-round trail.
Search for the R_1-round related-key differential trails with B_{R_1} and $\bar{B}_{R_1}$ for E_1 with SMT.
$\Delta X^j_{R_1-1}, \nabla iniK_j$ and $B^j_{R_1}$, $1 \le j \le n \leftarrow$ last-round input difference, the master key difference and weight of each R_1-round trail.
Phase 2: Search for all the clusters in E_0 and E_1
for *each* $\Delta Y_1^i, \Delta iniK_i, B^i_{R_0}, 1 \le i \le m$ **do**
    $\beta_i^u = K \circ P(\Delta Y^i_{R_0}), 1 \le u \le s \leftarrow$ all distinct output differences of E_0 within the probability range $(B^i_{R_0} + bw)$ searched with SMT.
    for *each* $\beta_i^u, 1 \le u \le s$ **do**
        $l_i^{u_1}, ..., l_i^{u_g} \leftarrow$ all the trails under the probability range $(B^i_{R_0} + \bar{bw})$ searched with SMT.
        $B^{i_{u_d}}_{R_0} \leftarrow W(l_i^{u_d}), 1 \le d \le g$
        $p_i^u = \sum_{1 \le d \le g} 2^{-B^{i_{u_d}}_{R_0}} \leftarrow$ the approximate probability of $(\Delta Y_1^i, \beta_i^u)$.
    end
end
for *each* $\Delta X^j_{R_1-1}, \nabla iniK_j, \bar{B}_{R_1}, 1 \le j \le n$ **do**
    $\gamma_j^v = P^{-1} \circ K^{-1}(\Delta X_1), 1 \le v \le t \leftarrow$ all distinct input differences of E_1 within the probability range $(B^j_{R_1} + bw)$ searched with SMT.
    for *each* $\gamma_j^v, 1 \le v \le t$ **do**
        $l_j^{v_1}, ..., l_j^{v_h} \leftarrow$ all the trails under the probability range $(B^j_{R_1} + \bar{bw})$.
        $B^{i_{v_e}}_{R_1} \leftarrow W(l_j^{v_e}), 1 \le e \le h$
        $q_j^v = \sum_{1 \le h \le e} 2^{-B^{i_{v_e}}_{R_1}} \leftarrow$ the approximate probability of $(\gamma_j^v, \Delta X^j_{R_1-1})$.
    end
end
Phase 3: Determine the boomerang distinguisher with highest probability
for *each* $(\Delta Y_1^i, \Delta X^j_{R_1-1})$, *and all* $\beta_i^u, \beta_i^{u'}, 1 \le u, u' \le s$, $\gamma_j^v, \gamma_j^{v'}, 1 \le v, v' \le t$ **do**
    $r(\beta_i^u, \beta_i^{u'}, \gamma_j^v, \gamma_j^{v'}) = \frac{1}{2^n} GBCT(\beta_i^u, \beta_i^{u'}, \gamma_j^v, \gamma_j^{v'})$
    $P_{i,j} \leftarrow \sum_{u,u',v,v'} p_i^u \cdot p_i^{u'} \cdot q_j^v \cdot q_j^{v'} \cdot r(\beta_i^u, \beta_i^{u'}, \gamma_j^v, \gamma_j^{v'})$
end
$Pd \leftarrow \max_{i,j}\{P_{i,j}\}$

4.2 The Improved Distinguisher with GBCT for GIFT

Here, we give the details of the new distinguisher of GIFT-64 and GIFT-128.

Choosing $R_0 = 10$ for E_0, $R_1 = 9$ for E_1, $R_m = 1$ for E_m and $bw = \bar{bw} = 4$ to search for a 20-round GIFT-64 distinguisher. The experimental result indicates that the probability of the new distinguisher is optimal with the α and δ used in [16]. But, in Phase 2, we get 376 differentials trails with 376 distinct γ_j more than 312 differentials trails searched in [16]. In phase 3, we found a total of 5520 boomerang trails that were left out as BCT could not connect. Finally, the probability of the 20-round distinguisher found in [16] is increased to $2^{-57.43}$.

For GIFT-128, we chose $R_0 = 9$ for E_0, $R_1 = 9$ for E_1, $R_m = 1$ for E_m and $bw = \bar{bw} = 4$. In phase 1, we got 10184 distinct β. All the β and γ can form $(10184 \times 2944)^2$ possible boomerang trails, which leads to an excessive calculating complexity. So we select the top 200 β and 450 γ with high probability to connect by GBCT$(\beta^i, \beta^j; \gamma^s, \gamma^t)$, and the remaining are still connected by BCT(β, γ). Finally, 2782 trails ignored under BCT connection are obtained, and the probabilities of these trails are accumulated to obtain the probability of the distinguisher of $2^{-108.349}$.

All the parameters of the 20/19-round related-key rectangle distinguisher for GIFT-64/128 are shown in Table 4 and Table 5.

Table 4. The specifications of the 20-round related-key rectangle distinguisher for GIFT-64

$R_0 = 10, R_m = 1, R_1 = 9; B_{c_{R0}} = 24.415, B_{c_{R1}} = 17.415; \hat{p}^2\hat{q}^2 = 2^{-57.43}$		
E_0	α_1	$\Delta iniK_0$
	0000 0000 0000 a000	0004 0000 0000 0800 0000 0000 0000 0010
E_1	δ_1	$\nabla iniK_1$
	0400 0000 0120 1000	2000 0000 0000 0000 0800 0000 0200 0800

Table 5. The specifications of the 19-round related-key rectangle distinguisher for GIFT-128

$R_0 = 9, R_m = 1, R_1 = 9; B_{c_{R0}} = 34, B_{c_{R1}} = 34; \hat{p}^2\hat{q}^2 = 2^{108.349}$		
E_0	α_1	$\Delta iniK_0$
	0000 0000 0000 00a0 0000 0000 6000 0000;	8000 0000 0000 0000 0000 0000 0002 0000
E_1	δ_1	$\nabla iniK_1$
	0020 0000 0000 0000 0000 0040 0000 2020;	000 0000 0000 0000 0002 0000 0002 0000

5 Rectangle Attacks on GIFT-64 and GIFT-128 with Reduced Complexities

Since the new distinguishers for GIFT-64 and GIFT-128 improve only the probability while using the same input-output differences as in [16], Dong's key recovery algorithm can be directly applied with it. Here, we only give the complexity

analysis of the attack and will not dwell on the details of the key recovery process. Interested readers are referred to [12,16].

Complexity Analysis of Key-Recovery Attack on GIFT-64

The target key bits are 68 with 30 bits in E_b and 38 bits in E_f. We first guess $m_b + m'_f = 60$ bits subkey to construct quartet candidates. Then eliminate the wrong quartets in a guess and filter procedure to determine the remaining 8 bits. Finally, guess the remaining $128 - h$ bit keys to check the full key.

- Data complexity: we need to prepare $4 \cdot D = 4 \cdot y \cdot 2^{r_b} = \sqrt{s} \cdot 2^{n/2+2}/\hat{p}\hat{q} = \sqrt{s} \cdot 2^{62.715}$ data.
- Memory complexity: we need $4 \cdot D + 2^{68-x} = \sqrt{s} \cdot 2^{62.715} + 2^{68-x}$ memory to store the data and key counters.
- Time complexity: Firstly, we need $T_1 = \sqrt{s} \cdot 2^{m_b+m'_f+n/2+1}/\hat{p}\hat{q} = \sqrt{s} \cdot 2^{121.715}$ to generate quartet candidates. Then, the time complexity of filtering wrong quartets is $T_2 = (s \cdot 2^{m_b+m'_f-n+2r_f-2h_f}/\hat{p}^2\hat{q}^2) \cdot \varepsilon = s \cdot 2^{83.43} \cdot \varepsilon$. Finally, we need $T_3 = 2^{128-h}$ for an exhaustive search.

To balance the above complexity, we choose $x = 8$, $h = 20$ and $s = 1$ in order to achieve a success probability of 69.45%. At last, we have a time complexity of $2^{121.715}$ for 26-round encryptions, a data complexity of $2^{62.715}$ and a memory complexity of $2^{62.715}$.

Complexity Analysis of Key-Recovery Attack on GIFT-128

The target key bits is 39 with 6 bits in E_b and 33 bits in E_f. We repeat the same process as the attack on GIFT-64 for GIFT-128 with $m_b + m'_f = 6 + 0 = 6$.

- Data complexity: we need to prepare $4 \cdot D = \sqrt{s} \cdot 2^{120.175}$ data.
- Memory complexity: we need $4 \cdot D + 2^{68-x} = \sqrt{s} \cdot 2^{120.175} + 2^{39}$ memory to store the data and key counters.
- Time complexity: Firstly, we need $T_1 = \sqrt{s} \cdot 2^{m_b+m'_f+n/2+1}/\hat{p}\hat{q} = \sqrt{s} \cdot 2^{125.175}$ to generate quartet candidates. Then, the time complexity of filtering wrong quartets is $T_2 = (s \cdot 2^{m_b+m'_f-n+2r_f-2h_f}/\hat{p}^2\hat{q}^2) \cdot \varepsilon = s \cdot 2^{90.5} \cdot \varepsilon$. Finally, we need $T_3 = 2^{128-h}$ for an exhaustive search.

To balance the above complexity, We choose $h = 20$ and $s = 1$ in order to achieve a good success probability of 84.00%. At last, we have a time complexity of $2^{125.175}$ 23-round encryptions, a data complexity of $2^{120.175}$ and a memory complexity of $2^{120.175}$.

6 Conclusion and Future Discussion

In this paper, we propose the GBCT to complement the leaky part that can not be evaluated by BCT, so as to obtain a more accurate distinguisher probability. Then, an automatic search algorithm applicable to all S-box-based block ciphers is provided to obtain a rectangle distinguisher with higher probability. Utilizing

the algorithm, we achieve the optimal probability of distinguishers for 20/19-round GIFT-64/128, and therefore the lowest data and time complexities of the related-key rectangle attacks on GIFT-64/128 up to now.

There are still some unfinished work to be investigated in the future. More variables introduced by GBCT are very constrained for the MILP model when $E_m > 1$. In addition, the search algorithm is only applicable to ciphers with S-boxes as the nonlinear layers. In the future, we will extend the research to fully assess the probability in E_m, not only when $E_m > 1$, but also for ciphers with nonlinear components like modular additions or bit-wise AND operations.

Acknowledgement. This work was supported by the National Natural Science Foundation of China (Grant No. 61872359, No. 61936008 and No. 61972393) and the Climbing Program from Institute of Information Engineering CAS (Grant No. E1Z0041112).

A 10-Round Optimal (Related-Key) Differentials for GIFT-64

Table 6. Input and Output differences of 10-round related-key differential trails with weight 19.8 of GIFT-64

i	input differences α_i	master key differences $\Delta iniK$
1	0000 0000 0000 6002 0000 0000 0000 6004	000C 0000 0000 0000 0040 0000 0000 0011
2	0000 0000 6002 0000 0000 0000 6004 0000	00C0 0000 0000 0000 0004 0000 0000 0022
3	0000 6002 0000 0000 0000 6004 0000 0000	0C00 0000 0000 0000 4000 0000 0000 0044
4	6002 0000 0000 0000 6004 0000 0000 0000	C000 0000 0000 0000 0400 0000 0000 0088

i	output differences δ_i	master key differences $\nabla iniK$
1	0800 0400 0220 0310	000C 0000 0000 0000 0040 0000 0000 0011
2	0310 0800 0400 0220	00C0 0000 0000 0000 0004 0000 0000 0022
3	0220 0310 0800 0400	0C00 0000 0000 0000 4000 0000 0000 0044
4	0400 0220 0310 0800	C000 0000 0000 0000 0400 0000 0000 0088

References

1. Banik, S., et al.: GIFT-COFB. Cryptology ePrint Archive, Paper 2020/738 (2020)
2. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Yu., Sim, S.M., Todo, Y.: GIFT: a small present - towards reaching the limit of lightweight encryption. In: Fischer, W., Homma, N. (eds.) CHES 2017. LNCS, vol. 10529, pp. 321–345. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66787-4_16
3. Biham, E., Dunkelman, O., Keller, N.: The rectangle attack—rectangling the serpent. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 340–357. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44987-6_21
4. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
5. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1–18. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10366-7_1
6. Boukerrou, H., Huynh, P., Lallemand, V., Mandal, B., Minier, M.: On the feistel counterpart of the boomerang connectivity table: introduction and analysis of the FBCT. IACR Trans. Symmetric Cryptol. **2020**(1), 331–362 (2020)
7. Chakraborti, A., Datta, N., Jha, A., Lopez, C.M., CINVESTAV, Sasaki, Y.: LOTUS-AEAD and LOCUS-AEAD. Submission to the NIST Lightweight Cryptography project (2019)
8. Chakraborti, A., Datta, N., Jha, A., Nandi, M.: HYENA. Submission to the NIST Lightweight Cryptography project (2019)
9. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: A Security Analysis of Deoxys and its Internal Tweakable Block Ciphers. IACR Trans. Symmetric Cryptol. **3**, 73–107 (2017)
10. Cid, C., Huang, T., Peyrin, T., Sasaki, Yu., Song, L.: Boomerang connectivity table: a new cryptanalysis tool. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10821, pp. 683–714. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78375-8_22
11. Delaune, S., Derbez, P., Vavrille, M.: Catching the fastest boomerangs application to SKINNY. IACR Trans. Symmetric Cryptol. **2020**(4), 104–129 (2020)
12. Dong, X., Qin, L., Sun, S., Wang, X.: Key guessing strategies for linear key-schedule algorithms in rectangle attacks. IACR Cryptol. ePrint Arch., p. 856 (2021)
13. Dunkelman, O., Keller, N., Shamir, A.: A practical-time related-key attack on the Kasumi cryptosystem used in GSM and 3G telephony. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 393–410. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_21
14. Hadipour, H., Bagheri, N., Song, L.: Improved rectangle attacks on SKINNY and CRAFT. IACR Trans. Symmetric Cryptol. **2021**(2), 140–198 (2021)
15. Hadipour, H., Nageler, M., Eichlseder, M.: Throwing boomerangs into feistel structures: application to CLEFIA, WARP, LBlock, LBlock-s and TWINE. Cryptology ePrint Archive, Paper 2022/745 (2022)
16. Ji, F., Zhang, W., Zhou, C., Ding, T.: Improved (related-key) differential cryptanalysis on GIFT. In: Dunkelman, O., Jacobson, Jr., M.J., O'Flynn, C. (eds.) SAC 2020. LNCS, vol. 12804, pp. 198–228. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-81652-0_8
17. Liu, Y., Sasaki, Yu.: Related-key boomerang attacks on GIFT with automated trail search including BCT Effect. In: Jang-Jaccard, J., Guo, F. (eds.) ACISP 2019. LNCS, vol. 11547, pp. 555–572. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-21548-4_30

18. Murphy, S.: The return of the cryptographic boomerang. IEEE Trans. Inf. Theory **57**(4), 2517–2521 (2011)
19. Song, L., Qin, X., Hu, L.: Boomerang connectivity table revisited. Application to SKINNY and AES. IACR Trans. Symmetric Cryptol. **2019**(1), 118–141 (2019)
20. Su, L., Wang, W., Wang, M.: Accelerating the search of differential and linear characteristics with the SAT method. IACR Trans. Symmetric Cryptol. **2021**(1), 269–315 (2021)
21. Wagner, D.: The boomerang attack. In: Knudsen, L. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48519-8_12
22. Wang, H., Peyrin, T.: Boomerang switch in multiple rounds. Application to AES variants and deoxys. IACR Trans. Symmetric Cryptol. **2019**(1), 142–169 (2019)
23. Zhu, B., Dong, X., Yu, H.: MILP-based differential attack on round-reduced GIFT. IACR Cryptol. ePrint Arch. **2018**, 390 (2018)