Quasidifferential Saves Infeasible Differential

Improved Weak-Key Key-Recovery Attacks on Round-Reduced GIFT

Chengcheng Chang[1,2], Meiqin Wang[2,1,3], Wei Wang[2,1,3] and Kai Hu[2,1,3(✉)]

[1] School of Cyber Science and Technology, Shandong University, Qingdao 266237, Shandong, China
{chengcheng.chang}@mail.sdu.edu.cn
[2] Quancheng Laboratory, Jinan 250103, China
{mqwang,weiwangsdu,kai.hu}@sdu.edu.cn
[3] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Qingdao 266237, Shandong, China

Abstract. `GIFT`, including `GIFT`-64 and `GIFT`-128, is a family of lightweight block ciphers with outstanding implementation performance and high security, which is a popular underlying primitive chosen by many AEADs such as `SUNDAE-GIFT`. Currently, differential cryptanalysis is the best key-recovery attack on both ciphers, but they have stuck at 21 and 27 rounds for `GIFT`-64 and `GIFT`-128, respectively. Recently, Beyne and Rijmen proposed the quasidifferential transition matrix for differential cryptanalysis at CRYPTO 2022 and showed that the fixed-key probability of a differential (characteristic) can be expressed as the sum of correlations of all quasidifferential trails corresponding to this differential (characteristic). As pointed out by Beyne and Rijmen in their paper, the quasidifferential methodology is useful in identifying weak-key differential attacks.

In this paper, we apply Beyne and Rijmen's method to `GIFT`. Some differential characteristics with small (average) probabilities can have much larger probabilities when weak-key conditions hold. Improved weak-key differential attacks on `GIFT`-64 and `GIFT`-128 are thus obtained. For `GIFT`-64, the probability of a 13-round differential is improved from $2^{-62.06}$ to $2^{-57.82}$ with 4 bits of weak-key conditions, then an improved differential key-recovery attack on 21-round `GIFT`-64 is obtained with $2^{117.42}/2^{64}$ time/data complexities; the probability of a 13-round multiple differential (containing 33 characteristics) is improved from $2^{-58.96}$ to $2^{-55.67}$ with 4 bits of weak-key conditions, then an improved multiple differential key-recovery attack on 21-round `GIFT`-64 is obtained with $2^{123.27}/2^{64}$ time/data complexities. For `GIFT`-128, the probability of a 20-round differential is improved from $2^{-121.83}$ to $2^{-114.77}$ with 6 bits of weak-key conditions; the probability of a 21-round multiple differential (containing 2 differentials) is improved from $2^{-128.38}$ to $2^{-122.77}$ with 4 bits of weak-key conditions. Improved (multiple) differential weak-key key-recovery attacks are obtained for 27 and 28 rounds of `GIFT`-128 with $2^{115.77}/2^{115.77}$ and $2^{123.77}/2^{123.77}$ time/data complexities, respectively. As far as we know, this is the first time that a (weak-key) key-recovery attack can reach 28 rounds of `GIFT`-128.

Additionally, as an independent interest, we perform the first differential attack on `SUNDAE-GIFT`. The differential used in this attack is checked with quasidifferential trails, thus the probability is reliable. Our attack is nonce-respecting and has significantly better complexities than the currently best attack.

Keywords: Quasidifferential · Differential · Weak-Key · GIFT.

1   Introduction

Differential cryptanalysis is one of the most fundamental methods to analyze the security of block ciphers, which was proposed by Biham and Shamir [6] at CRYPTO 1990 to attack the block cipher DES. The core concept of the differential attack is to construct the probabilistic transition from an input difference to an output difference for iterated ciphers. This involves choosing plaintext pairs that satisfy the input difference, tracing the difference transitions of the iterated block cipher throughout the multi-round encryption process, and finding high-probability differentials over a large number of rounds. The differential transition that traces the large number of rounds is usually converted to tracing intermediate differences, the calculation of the differential probability of long rounds can be estimated heuristically as the product of multiple probabilities of intermediate differences, and Lai et al. [14] showed that it yields the correct value of the *key-averaged probability* for *Markov ciphers*. In addition, Lai et al. introduced an additional assumption, which is called the *hypothesis of stochastic equivalence*, to deal with the problem that the actual probability may be different from *key-averaged probability*, which is caused by the fixed-key throughout a differential attack. This assumption states that the probability for each key is close to the average probability.

At CRYPTO 2022, Beyne and Rijmen [5] proposed the quasidifferential transition matrix in differential cryptanalysis, and established the connection between the correlation matrix in linear cryptanalysis [11] and the quasidifferential transition matrix in differential cryptanalysis. The quasidifferential transition matrix satisfies similar properties to the correlation matrix in linear cryptanalysis. One such property is that the fixed-key probability of a differential can be expressed as the sum of the correlations of all its quasidifferential trails, without any assumption. Given one differential (characteristic), correlations of its corresponding quasifferentials are heavily affected by keys. Thus, differential probability in different key spaces can be analyzed relatively more easily now. It is not surprising that in some key spaces, the differential probability would be significantly larger than others.

`GIFT` [4] is a lightweight block cipher with two versions: `GIFT`-64 and `GIFT`-128. The outstanding implementation performance and high security make `GIFT` be a popular underlying primitive for many Authenticated Encryptions with Associated Data (AEADs) such as `SUNDAE-GIFT` [2], `GIFT-COFB` [3], and `HyENA` [9]. In the security evaluation of `GIFT`, differential cryptanalysis is currently the most effective attack compared with other attacks. At CT-RSA 2019, Zhu et al. [24]

proposed the first third-party cryptanalysis on `GIFT`, which includes a 19-round attack on `GIFT`-64 and a 22-round attack on `GIFT`-128, respectively. Sasaki et al. [17] improved the meet-in-the-middle (MitM) attack on 15-round `GIFT`-64. The 20-round and 21-round differential attacks on `GIFT`-64 were proposed by Chen et al. [10] at ICISC 2019 using the full codebook. Chen et al. [10] also performed the 20-round differential key-recovery attack on `GIFT`-64 without the full codebook. Li et al. [15] proposed the 26-round differential attack on `GIFT`-128, and the 26-round attack is improved by Ji et al. [13] at SAC 2021. At FSE 2021, Zong et al. [26] proposed the key-recovery-attack friendly distinguishers, gave a 27-round differential key-recovery attack and a 22-round linear key-recovery attack on `GIFT`-128, respectively. For the linear cryptanalysis of `GIFT`, Sun et al. [20] proposed a 19-round linear attack on `GIFT`-64 at SAC 2021, and a 24-round linear attack on `GIFT`-128 at FSE 2021 [21]. After that, Sun et al. [22] gave a 25-round linear attack on `GIFT`-128 at FSE 2022, and improved the 25-round linear attack to increase the success probability by using more data and higher time complexity. Antonio Flórez-Gutiérrez et al. [12] further improved the complexity and success probability of the 25-round linear key-recovery attack on `GIFT`-128 at EUROCRYPT 2024. In addition, Wang et al. [23] proposed the differential-linear attacks on 18-round `GIFT`-64 and on 19-round `GIFT`-128 at CIC 2024. All the above attacks are under the single-key setting. In the relate-key setting, Liu et al. [16] proposed a 21-round boomerang attack on `GIFT`-128, and Ji et al. [13] proposed a 23-round rectangle attack on `GIFT`-128 at SAC 2021.

Although extensive cryptanalysis from the community has been applied to `GIFT`, the security of `GIFT` is still strong. All attacks stuck at 21 and 27 rounds for `GIFT`-64 and `GIFT`-128 in the single-key setting, respectively. Considering the importance of `GIFT` (as mentioned, `GIFT`-128 is the underlying primitive of three NIST LWC candidates), a better evaluation on `GIFT`'s security is always warranted, even in the extreme scenarios such as under the weak-key settings.

On the other hand, Beyne and Rijmen's quasidifferential approach has been successfully applied to `RECTANGLE`, `KNOT`, `SPECK`, and `SIMON`, and new weak-key attacks are presented. However, few works tried to extend their attacks to more ciphers, to the best of our knowledge. In this paper, we aim to bridge the gap by studying how to utilize the quasidifferential method to analyze the security of `GIFT`.

Our contributions. This paper applies Beyne and Rijmen's quasidifferential approach [5] to `GIFT`, studying the differential attacks in the weak-key setting. Some differential characteristics with small probabilities that are infeasible in a normal differential attack can be used now in a weak-key setting, by putting some weak-key conditions. The best attacks on `GIFT`-64 and `GIFT`-128 are provided, in terms of the complexity or the number of rounds.

Concretely, by diving deep into the linear key-schedule of `GIFT`, we extract linear equations for round-key bits, based on the signs of correlations of quasidifferential trails, and convert them to equations for master-key bits. Then the weak-key space of master-key bits is obtained, and the probability of the differ-

Table 1. Summary of the attack results on GIFT-64, GIFT-128 and SUNDAE-GIFT, respectively. SK stands for single-key setting. RK stands for related-key setting.

Algorithm	Attack Type	Rounds	Scenario	# Keys	Time	Data	Memory	P_S	Reference
GIFT-64	Boomerang	23	RK‡	2^{128}	$2^{126.60}$	$2^{63.30}$	-	-	[16]
	Rectangle	24	RK‡	2^{128}	$2^{106.00}$	$2^{63.78}$	$2^{64.10}$	-	[13]
	Rectangle	25	RK‡	2^{128}	$2^{120.92}$	$2^{63.78}$	$2^{64.10}$	-	[13]
	Differential	26	RK‡	2^{128}	$2^{123.23}$	$2^{60.96}$	$2^{102.86}$	-	[19]
	Differential	26	RK‡	2^{128}	$2^{115.96}$	$2^{60.96}$	$2^{102.86}$	-	[8]
	Differential-Linear	18	SK	2^{128}	$2^{124.61}$	$2^{61.57}$	-	-	[23]
	Linear	19	SK	2^{128}	$2^{127.11}$	$2^{62.96}$	2^{60}	60%	[20]
	Differential	19	SK	2^{128}	2^{112}	2^{63}	2^{80}	-	[24]
	Multiple Differential	20	SK	2^{128}	$2^{112.68}$	2^{62}	2^{112}	-	[10]
	Differential	20	SK	2^{128}	$2^{101.68}$	2^{64}	2^{96}	-	[10]
	Multiple Differential	**21**	**SK**	$\mathbf{2^{124}}$	$\mathbf{2^{123.27}}$	$\mathbf{2^{64}}$	$\mathbf{2^{112}}$	**99.9%**	**Sect. 5.1**
	Differential	21	SK	2^{128}	$2^{121.66†}$	2^{64}	2^{96}	51.60%†	[10]
	Differential	**21**	**SK**	$\mathbf{2^{124}}$	$\mathbf{2^{117.42}}$	$\mathbf{2^{64}}$	$\mathbf{2^{96}}$	**81.06%**	**Sect. 5.1**
	Differential	**21**	**SK**	$\mathbf{2^{124}}$	$\mathbf{2^{120.60}}$	$\mathbf{2^{64}}$	$\mathbf{2^{96}}$	**99.41%**	**Sect. 5.1**
GIFT-128	Boomerang	21	RK‡	2^{128}	$2^{126.6}$	$2^{126.6}$	$2^{126.6}$	-	[16]
	Rectangle	23	RK‡	2^{128}	$2^{126.89}$	$2^{121.31}$	$2^{121.63}$	-	[13]
	Differential-Linear	19	SK	2^{128}	$2^{121.53}$	$2^{122.51}$	-	-	[23]
	Differential	22	SK	2^{128}	2^{120}	2^{120}	2^{86}	-	[25]
	Linear	22	SK	2^{128}	2^{117}	2^{117}	2^{78}	-	[26]
	Linear	24	SK	2^{128}	$2^{124.45}$	$2^{122.55}$	2^{105}	80.01%	[21]
	Linear	25	SK	2^{128}	$2^{126.77}$	$2^{124.75}$	2^{96}	50%	[22]
	Linear	25	SK	2^{128}	$2^{127.77}$	$2^{125.75}$	2^{96}	75%	[22]
	Linear	25	SK	2^{128}	$2^{124.61}$	$2^{123.02}$	2^{112}	80%	[12]
	Differential	26	SK	2^{128}	$2^{124.415}$	2^{109}	$2^{124.415}$	-	[15]
	Differential	26	SK	2^{128}	$2^{123.245}$	$2^{123.245}$	2^{109}	-	[13]
	Differential	27	SK	2^{128}	$2^{124.83}$	$2^{123.53}$	2^{80}	-	[26]
	Differential	**27**	**SK**	$\mathbf{2^{122}}$	$\mathbf{2^{115.77}}$	$\mathbf{2^{115.77}}$	$\mathbf{2^{92}}$	**99.9%**	**Sect. 5.2**
	Multiple Differential	**28**	**SK**	$\mathbf{2^{124}}$	$\mathbf{2^{123.77}}$	$\mathbf{2^{123.77}}$	$\mathbf{2^{96}}$	**86.5%**	**Sect. 5.2**
SUNDAE-GIFT	Linear	16	Nonce-respecting	2^{128}	$2^{91.20}$	$2^{60.00}$	2^{96}	-	[26]
	Linear	17	Nonce-respecting	2^{128}	$2^{123.38}$	$2^{61.51}$	2^{49}	80.01%	[21]
	Differential	**17**	**Nonce-respecting**	$\mathbf{2^{128}}$	$\mathbf{2^{75.37}}$	$\mathbf{2^{62.5}}$	$\mathbf{2^{66}}$	**99.9%**	**Sect. 6**

† The 21-round differential key-recovery attack on GIFT-64 presented by [10] with $2^{107.61}/2^{64}/2^{96}$ time/data/memory complexities, which is the combination of the 1-round attack and the 20-round attack, is not accurate, we reevaluate the complexities and success probability by the successive 21-round attack.

‡ Note that there is no security claim of GIFT under the related-key setting, the results under the related-key setting are shown in grey.

ential characteristic in this weak-key space is improved. Furthermore, in order to use the *differential* to amplify the probability, we introduce a method to derive the best weak-key conditions from all the characteristics of the differential. These analyses are based on a reasonable assumption that the exact probability of a differential characteristic can be approximated by the sum of correlations of those trails whose absolute correlation is equal to the average probability of the characteristic. We have done experiments on GIFT-64 and GIFT-128 to verify the

validity of the assumption, and the experimental results are exactly consistent with our assumption.

After applying the quasidifferential cryptanalysis to GIFT, we present improved (multiple) differential attacks on GIFT-64 and GIFT-128 in the weak-key settings, respectively. For GIFT-64, the probability of a 13-round differential is improved from $2^{-62.06}$ to $2^{-57.82}$ with 4-bit conditions of master-key, which can mount a 21-round differential attack with $2^{117.42}/2^{64}$ time/data complexities. The probability of a 13-round multiple differential of GIFT-64 is improved from $2^{-58.96}$ to $2^{-55.67}$ with 4-bit conditions of master-key, which can boost the multiple differential attack on GIFT-64 from 20-round to 21-round with $2^{123.27}/2^{64}$ time/data complexities. For GIFT-128, the probability of a 20-round differential is improved from $2^{-121.83}$ to $2^{-114.77}$ with 6-bit conditions of master-key, and the probability of a 21-round multiple differential is improved from $2^{-128.38}$ to $2^{-122.77}$ with 4-bit conditions of master-key. The 27-round and the first 28-round improved (multiple) differential attacks on GIFT-128 are obtained with $2^{115.77}/2^{115.77}$ and $2^{123.77}/2^{123.77}$ time/data complexities, respectively.

Finally, an 11-round differential characteristic whose probability is 2^{-60} without conditions of master-key can be utilized to launch the first differential attack on 17-round SUNDAE-GIFT with $2^{75.37}/2^{62.5}$ time/data complexities. The related results and our attacks are summarized in Table 1.

All source code and results of this paper are provided at https://github.com/ccc53021/quasidifferential-gift.

Outline. In Sect. 2, we briefly describe the differential cryptanalysis, linear cryptanalysis, and quasidifferential proposed in [5], define some notations, recall the description of GIFT. In Sect. 3, we revisit and discuss the roles of the keys in the exact probability of a characteristic. In Sect. 4, we introduce how to apply the quasidifferential cryptanalysis to GIFT, derive weak-key differential (characteristic) distinguishers, and make some experiments on GIFT. Sect. 5 presents the weak-key (multiple) differential attacks on GIFT-64 and GIFT-128, respectively, and the attack on SUNDAE-GIFT is given in Sect. 6. Sect. 7 concludes this paper.

2 Preliminaries and Related Works

In this section, we first recall the differential cryptanalysis and linear cryptanalysis, and introduce the quasidifferential proposed by Beyne and Rijmen [5], which shows that the fixed-key probability of a differential can be expressed as the sum of the correlations of its quasidifferential trails. In addition, we define the notations used in this paper and briefly review the description of GIFT and SUNDAE-GIFT with GIFT-128 as an underlying primitive.

2.1 Review of Differential Cryptanalysis in Fixed-Key Model

Differential Cryptanalysis. Differential cryptanalysis [6] is used to analyze the propagation of differences through the function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, and find a differ-

ential with high probability to attack the cipher. The target of the adversary is to find a differential $(a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ that maximizes the number of solutions x to the difference equation

$$\mathsf{F}(x \oplus a) \oplus \mathsf{F}(x) = b. \tag{1}$$

The difference distribution table of F, denoted as DDT^F, is a $2^n \times 2^m$ table with rows and columns indexed by input and output differences. The corresponding entries are equal to the number of solutions x for a particular differential (a, b):

$$\mathsf{DDT}^\mathsf{F}_{(a,b)} = \left|\{x \in \mathbb{F}_2^n | \mathsf{F}(x \oplus a) \oplus \mathsf{F}(x) = b\}\right|. \tag{2}$$

Differential cryptanalysis typically focuses on functions F structured as compositions $\mathsf{F} = \mathsf{F}_r \circ \mathsf{F}_{r-1} \circ \cdots \circ \mathsf{F}_1$, where individual functions F_i exhibit differentials with relatively high probability, making them more suitable for analysis. Thus, it is possible to estimate the probability of differential (a_1, a_{r+1}) based on *characteristics*. A characteristic is a sequence $(a_1, a_2, \ldots, a_{r+1})$ of compatible differences between intermediate inputs and outputs through each F_i. The estimation of characteristic probabilities frequently relies on the assumption of independence among intermediate differentials:

$$\Pr[\wedge_{i=1}^r \mathsf{F}_i(x_i \oplus a_i) \oplus \mathsf{F}_i(x_i) = a_{i+1}] \approx \prod_{i=1}^r \Pr[\mathsf{F}_i(x_i \oplus a_i) \oplus \mathsf{F}_i(x_i) = a_{i+1}]. \tag{3}$$

When functions $\mathsf{F}_1, \ldots, \mathsf{F}_r$ are dependent on keys $k_1, \ldots, k_r$, the heuristic proposed in Eq. (3) can be justified by applying the *Markov cipher* assumption [14]. Specifically, it has been demonstrated that if all round keys are uniformly random and independent, the *key-averaged probability* of a characteristic aligns with the product of intermediate key-averaged probabilities.

Quasidifferential. Beyne and Rijmen [5] proposed the quasidifferential framework by introducing the quasidifferential transition matrices as a differential analog of correlation matrices [11] to achieve a more complete understanding of differential cryptanalysis.

Definition 1 (Quasidifferential basis [5]). *Let n be a positive integer. For any $u, a \in \mathbb{F}_2^n$, the function $\beta_{u,a} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{R}$ is defined by*

$$\beta_{u,a}(x, y) = \chi_u(x)\delta_a(x + y). \tag{4}$$

The set of all $\beta_{u,a}$ is called the quasidifferential basis for $\mathbb{R}[\mathbb{F}_2^n \times \mathbb{F}_2^n]$.

The functions δ_x such that $\delta_x(y) = 1$ if $y = x$ and zero elsewhere, and the functions χ_x such that $\chi_u(x) = (-1)^{u^\mathsf{T} x}$ with $u \in \mathbb{F}_2^n$. The functions $\beta_{u,a}$ are not only linearly independent but also orthogonal. Similar to the Fourier transformation, Beyne and Rijmen define the change-of-basis operator $\mathcal{Q}_n : \mathbb{R}[\mathbb{F}_2^n \times \mathbb{F}_2^n] \to \mathbb{R}[\mathbb{F}_2^n \times \mathbb{F}_2^n]$ by $(\mathcal{Q}_n f)(u, a) = \langle \beta_{u,a}, f \rangle$. The definition of the *quasidifferential*

transition matrix using the change-of-basis operator $\mathscr{Q}_n$ and the transition matrix for pairs of values is in Definition 2. The Kronecker (or tensor) product $T^{\mathsf{F}} \otimes T^{\mathsf{F}}$ is defined as a $2^{2m} \times 2^{2n}$ matrix with coordinates

$$(T^{\mathsf{F}} \otimes T^{\mathsf{F}})_{(y_1,y_2),(x_1,x_2)} = T^{\mathsf{F}}_{y_1,x_1} T^{\mathsf{F}}_{y_2,x_2} = \delta_{y_1}(\mathsf{F}(x_1))\delta_{y_2}(\mathsf{F}(x_2)). \qquad (5)$$

Definition 2 (Quasidifferential transition matrix [5]). *Let n and m be two positive integers and $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ a function. The quasidifferential transition matrix D^{F} is defined as the matrix-representation of $T^{\mathsf{F}} \otimes T^{\mathsf{F}}$ with respect to the quasidifferential basis defined in Definition 1. That is, $D^{\mathsf{F}} = \mathscr{Q}_m(T^{\mathsf{F}} \otimes T^{\mathsf{F}})\mathscr{Q}_n^{-1}$.*

As described in [5], the coordinates of D^{F} are pairs $(u, a) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ and $(v, b) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$. By the orthogonality of the quasidifferential basis, it holds that $\mathscr{Q}_n^{-1} = \mathscr{Q}_n^{\mathsf{T}}/2^n$ and consequently

$$
\begin{aligned}
D^{\mathsf{F}}_{(v,b),(u,a)} &= \langle \delta_{(v,b)}, \mathscr{Q}_n(T^{\mathsf{F}} \otimes T^{\mathsf{F}})\mathscr{Q}_n^{\mathsf{T}}\delta_{(u,a)}\rangle/2^n = \langle \beta_{v,b}, (T^{\mathsf{F}} \otimes T^{\mathsf{F}})\beta_{u,a}\rangle/2^n \\
&= \frac{1}{2^n} \sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \chi_u(x)\chi_v(\mathsf{F}(x))\delta_a(x+y)\delta_b(\mathsf{F}(x)+\mathsf{F}(y)) \\
&= \frac{1}{2^n} \sum_{\substack{x\in\mathbb{F}_2^n \\ \mathsf{F}(x+a)=\mathsf{F}(x)+b}} (-1)^{u^{\mathsf{T}}x+v^{\mathsf{T}}\mathsf{F}(x)}.
\end{aligned}
\qquad (6)
$$

For $u = v = 0$, Eq. (6) reduces to the probability of the differential with input difference a and output difference b, that is, $D^{\mathsf{F}}_{(0,b),(0,a)} = 2^{-n}\mathsf{DDT}^{\mathsf{F}}_{(a,b)}$. For $a = b = 0$, the coordinates of the correlation matrix of F can be obtained. In particularly, $D^{\mathsf{F}}_{(v,0),(u,0)} = C^{\mathsf{F}}_{v,u}$. Overall, the coordinates of D^{F} express the correlations of probabilistic linear relations ("linear approximations") between the input and output values of the right pairs.

Motivated by the notion of *linear trails*, Beyne and Rijmen propose the definition of *quasidifferential trails* in Definition 3, and show that exact expression for the probabilities of differentials can be given in terms of the correlations of quasidifferential trails in Theorem 1. For key-alternating ciphers, the expressions are shown in Theorem 2.

Definition 3 ([5]). *A quasidifferential trail for a function $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_1$ is a sequence $\omega_1, \ldots, \omega_{r+1}$ of mask-difference pairs $\omega_i = (u_i, a_i)$. The correlation of this quasidifferential trail is defined as $\prod_{i=1}^r D^{\mathsf{F}_i}_{\omega_{i+1},\omega_i}$.*

Theorem 1 ([5]). *Let $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function such that $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_1$. The probability of a characteristic with differences $a_1, \ldots, a_{r+1}$ is equal to the sum of the correlations of all quasidifferential trails with the same intermediate differences:*

$$\Pr[\wedge_{i=1}^r \mathsf{F}_i(x_i + a_i) = \mathsf{F}_i(x_i) + a_{i+1}] = \sum_{u_2,\cdots,u_r} \prod_{i=1}^r D^{\mathsf{F}_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)}, \qquad (7)$$

with $u_1 = u_{r+1} = 0$, $x_i = \mathsf{F}_{i-1}(x_{i-1})$ for $i = 2, \ldots, r$ and x_1 uniform random on $\mathbb{F}_2^n$.

Table 2. Notations used in describing the attacks on GIFT.

X_i	the input state of the round i
$X_i[j]$	the j-th bit of the state X_i, $j = 0, \ldots, 127$, $X_i[127]$ is the most significant bit of X_i
$X_i[j \cdots k]$	the j-th bit, $\ldots$, k-th bit of the state X_i
$X_i[j_{n-1} \sim j_0]$	consecutive n bits from j_{n-1}-th to j_0-th bit of the state X_i
X_i^S	the state after the operation SubCells of round i
X_i^P	the state after the operation PermBits of round i
X_{i+1}	the state after the operation AddRoundKeys of round i
ΔX	the difference in state X
RK_i	the round key of the round i
$RK_i[j]$	the j-th bit of the i-th round key RK_i
k_i	the 16-bit word of the master key, $i = 0, \ldots 7$
k_i^j	the j-th bit of a 16-bit word k_i of the master-key
$\ggg$	circular right shift
P	the plaintext
C	the ciphertext
T	the tag of the output of encryption for SUNDAE-GIFT
RK_i'	is equal to PermBits$^{-1}(RK_i)$
$X_i'^P$	is equal to X_{i+1}

Theorem 2 ([5]). *Let* $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_1$ *with* $\mathsf{F}_i(x) = \mathsf{G}_i(x) + k_i$. *If* $\boldsymbol{k} = (\boldsymbol{k}_1, \ldots, \boldsymbol{k}_r)$ *is a uniform random variable on a set* $\mathcal{K}$, *then*

$$\Pr[\mathsf{F}(x + a) = \mathsf{F}(x) + b] = \sum_{\substack{u_2, \ldots, u_r \\ a_2, \ldots, a_r \\ (u_2, \ldots, u_r) \perp \mathcal{K}}} \prod_{i=1}^r D^{\mathsf{G}_i}_{(u_{i+1}, a_{i+1}), (u_i, a_i)}, \qquad (8)$$

where $u_1 = u_{r+1} = 0$ *and the probability is over a uniform random* x *and over the keys* $\boldsymbol{k}_1, \ldots, \boldsymbol{k}_r$. *In particular, for* $\mathcal{K} = \mathbb{F}_2^n$, *only quasidifferential trails with zero masks contribute to the key-averaged probability of the differential.*

2.2 Description of GIFT Family

GIFT. To describe the attacks on GIFT, notations in Table 2 are used. Proposed by Banik et al. at CHES 2017 [4], GIFT has two versions: GIFT-64 and GIFT-128. GIFT adopts an SPN structure, with a 64-bit input for GIFT-64 and a 128-bit input for GIFT-128, both using a 128-bit key. The round numbers for GIFT-64 and GIFT-128 are 28 and 40, respectively. The function for each round is the same for both versions, composed of three operations: SubCells, PermBits, and AddRoundKey.

SubCells. Both versions of GIFT use the same invertible 4-bit S-box GS. The S-box is applied to every nibble of the internal state and is given in Appendix A, Table 9.

PermBits. The bit permutation maps bits from bit position i of the internal state to bit position $P(i)$: $b_{P(i)} \leftarrow b_i, i \in \{0, 1, \ldots, 63\}$ for GIFT-64, and $i \in \{0, 1, \ldots, 127\}$ for GIFT-128. Two tables of bit permutation used in GIFT-64 and GIFT-128 are given in Appendix A, Table 10 and Table 11, respectively.

AddRoundKey. For `GIFT`-64, the 32-bit round key $RK = U||V = u_{15} \cdots u_0||v_{15} \cdots v_0$, and is XORed with the internal state in the following way:

$$b_{4i+1} \leftarrow b_{4i+1} \oplus u_i, \ b_{4i} \leftarrow b_{4i} \oplus v_i, \ i \in \{0, 1, \cdots, 15\}.$$

For `GIFT`-128, the 64-bit round key $RK = U||V = u_{31} \cdots u_0||v_{31} \cdots v_0$, and is XORed with the internal state in the following way:

$$b_{4i+2} \leftarrow b_{4i+2} \oplus u_i, \ b_{4i+1} \leftarrow b_{4i+1} \oplus v_i, \ i \in \{0, 1, \ldots, 31\}.$$

AddRoundConstants. The round constants are given in Appendix A, Table 12.

Key Schedule. The 128-bit master key is initialized as $k_7||k_6|| \cdots ||k_1||k_0$, where k_i is 16-bit. For `GIFT`-64, two 16-bit words of the key state are extracted as the round key $RK = U||V$. $U \leftarrow k_1$, $V \leftarrow k_0$. For `GIFT`-128, four 16-bit words of the key state are extracted as the round key $RK = U||V$. $U \leftarrow k_5||k_4$, $V \leftarrow k_1||k_0$.

The key state is then updated as follows:

$$k_7||k_6 \cdots ||k_1||k_0 \leftarrow (k_1 \ggg 2)||(k_0 \ggg 12)|| \cdots ||k_3||k_2.$$

SUNDAE-GIFT. `SUNDAE-GIFT` is based on the mode of operation `SUNDAE` [1] at ToSC 2019, and the underlying block cipher is `GIFT`-128. The encryption algorithm takes as input an encryption key $K \in \{0, 1\}^{128}$, an associated data $A \in \{0, 1\}^*$, and a message $M \in \{0, 1\}^{128}$. A nonce N with fixed length for variants is prepended on and regarded as a part of the associated data A. The output of the encryption is a ciphertext $C \in \{0, 1\}^{|M|}$ and a tag $T \in \{0, 1\}^{128}$. The operation "$\times$" denotes the multiplication by 2 or 4 depending on the length of the last blocks of A and M.

3   Revisiting and Discussion on the Weak-Key Conditions with Quasidifferential Approach [5]

This section provides a brief description of how to use the quasidifferential to derive the weak-key conditions for a *key-alternating cipher*, as given in [5]. We also discuss the assumptions implicitly used in this approach.

In the normal differential cryptanalysis, an r-round differential characteristic of a function $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_1$ with $\mathsf{F}_i = \mathsf{G}_i + k_i$ is a sequence

$$\varepsilon = \{a_1, a_2, \ldots, a_{r+1}\},$$

where a_i is the input differences of the i-th round. In the quasidifferential cryptanalysis, according to Beyne and Rijmen [5], an r-round quasidifferential trail corresponding to the above characteristic ε is the following sequence,

$$t = \{(u_1, a_1), (u_2, a_2), \ldots, (u_{r+1}, a_{r+1})\},$$

where (u_i, a_i) is the input mask-difference pair of the i-th round.

The correlation of a quasidifferential trail can be calculated by the quasidifferential transition matrix D^{G_i} of G_i, which is

$$cor = \prod_{i=1}^{r}(-1)^{u_{i+1}^{\mathsf{T}}k_i} D^{\mathsf{G}_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)}$$

Let $c = \prod_{i=1}^{r} D^{\mathsf{G}_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)}$, we have

$$cor = (-1)^{\mathcal{K}} \cdot c = (-1)^{\mathcal{K}} \cdot (-1)^b \cdot |c|, \tag{9}$$

where $\mathcal{K} = \sum_{i=1}^{r} u_{i+1}^{\mathsf{T}}k_i$, $|c|$ is the absolute value of c, and b represents the sign of c, i.e., when $b = 1$, $c < 0$, otherwise, $c > 0$.

It is easy to check, the correlation $cor > 0$ under a condition $\mathcal{K} = b$, and $cor < 0$ under a condition $\mathcal{K} = b + 1$. According to Theorem 1, given a differential characteristic ε with *key-averaged probability*, denoted by p_{avg}, the exact probability of ε, denoted by p, is equal to the sum of correlations of all its corresponding quasidifferential trails. By Eq. (9),

$$p = \sum_i cor_i = \sum_i (-1)^{\mathcal{K}_i} \cdot c_i = \sum_i (-1)^{\mathcal{K}_i} \cdot (-1)^{b_i} \cdot |c_i|. \tag{10}$$

Unfortunately, the number of quasidifferential trails is too enormous to exhaust, thus, we actually cannot collect all quasidifferential trails, so we can only approximate the exact p by considering a fraction of the trails. For example, in [5], Beyne and Rijmen consider the quasidifferential trails with $|c| = p_{avg}$ for the analysis of KNOT and RECTANGLE, and $|c| = 2^0 \cdot p_{avg}$ to $|c| = 2^{-4} \cdot p_{avg}$ for the analysis of SPECK-32.

This paper follows a similar strategy in that we only consider those trails that have a significant contribution to the exact p. Divide all quasidifferential trails corresponding to ε into two parts according to $|c| = p_{avg}$ and $|c| < p_{avg}$, we have

$$p = p_{|c|=p_{avg}} + p_{|c|<p_{avg}} = \sum_{i,|c_i|=p_{avg}} (-1)^{\mathcal{K}_i} \cdot (-1)^{b_i} \cdot |c_i| + \sum_{j,|c_j|<p_{avg}} (-1)^{\mathcal{K}_j} \cdot (-1)^{b_j} \cdot |c_j|. \tag{11}$$

Assumption 1 *The probability of a differential characteristic ε whose average probability is p_{avg} is dominated by those quasidifferential trails with $|c| = p_{avg}$.*

Based on the Assumption 1, we approximate that

$$p \approx p_{|c|=p_{avg}} = \sum_{i,|c_i|=p_{avg}} (-1)^{\mathcal{K}_i} \cdot (-1)^{b_i} \cdot |c_i|. \tag{12}$$

Remark. Assumption 1 is intuitive. However, it is similar to the cases in the traditional differential and linear cryptanalysis, where dominating trails are used to approximate the real probabilities or correlations. For our applications in this paper, we have done experiments to verify Assumption 1 on GIFT-64 and GIFT-128 in Sect. 4.4, the experimental results are exactly consistent with our assumption, showing that Assumption 1 works well.

4   Derive Weak-Key Distinguishers of `GIFT`

In this section, we introduce how to apply the quasidifferential cryptanalysis and derive weak-key distinguishers for `GIFT`. In Sect. 3, we have revisited the roles of the keys in the exact probability of a differential characteristic. In our analysis of `GIFT`, we tend to use the differential (multiple differential characteristics sharing the same input and output differences) to amplify the probability. Therefore, the method in Sect. 3 cannot be trivially used as needs to handle more quasidifferential trails simultaneously. In Sect. 4.1, we introduce a method how to obtain the weak-key conditions for a differential and choose a good weak-key space. In Sect. 4.2 and 4.3, we obtain the weak-key distinguishers on `GIFT`-64 and `GIFT`-128, respectively. Finally, we verify Assumption 1 experimentally on `GIFT`-64 and `GIFT`-128 in Sect. 4.4, respectively, the experimental results are consistent with our assumption.

4.1   Obtain a Good Weak-Key Space for a Differential

According to Sect. 3, if a characteristic with p_{avg} has m quasidifferential trails satisfying $|c| = p_{avg}$, then $p \leq m \cdot |c|$ (under Assumption 1). The "=" case holds only if we can add m conditions such that

$$\mathcal{K}_i = b_i, \quad i = 1, \ldots, m.$$

Each condition above corresponds to an equation of keys, thus the m conditions lead to a weak-key space. Furthermore, there might be redundancy among the m conditions, i.e., the rank of the m conditions might be smaller than m, which we denote by ℓ. Thus, the size of this weak-key space is of size $2^{n-\ell}$ (n is the length of the key). When a key falls into this weak-key space, $p = m \cdot p_{avg}$.

As mentioned, we want to use the differential to enhance our attack. If a differential contains d differential characteristics, denoted by $\varepsilon_1, \ldots, \varepsilon_d$, respectively. According to Theorem 2 and Eq. (12), the probability p of this differential can be expressed as

$$p = \sum_{i=1}^{d} p_{\varepsilon_i} = \sum_{i=1}^{d} \sum_{\substack{j \\ |c_j^i| = p_{avg}^i}} (-1)^{\mathcal{K}_j^i} \cdot (-1)^{b_j^i} \cdot |c_j^i|. \tag{13}$$

For each characteristic ε_i above, suppose its average probability is p_{avg}^i, $i = 1, \ldots, d$. By applying ℓ_i equations to the keys, we can make the probability of ε_i be maximum, i.e., $m_i \cdot p_{avg}^i$. The corresponding weak-key space is denoted by W_i.

Not all W_i are compatible. A good weak-key space should satisfy two points: (a) the number of key conditions should be as small as possible; (b) the probability of the differential in this weak-key space should be as large as possible. To choose a good weak-key space, we choose the W_i with the maximum $\log_2(p) - \ell_i$. The algorithm procedure pseudo-code is shown in Appendix B, Algorithm 1.

4.2   Weak-Key Distinguishers for `GIFT-64`

In this subsection, we automate the search for quasidifferential trails following [5], and obtain weak-key conditions for distinguishers of `GIFT-64` according to the discussion in Sect. 4.1. The probability of the 13-round differential of `GIFT-64` in [10], which is used to launch the known best published 21-round differential attack on `GIFT-64`, is improved from $2^{-62.06}$ to $2^{-57.82}$ with 4-bit conditions of master-key, and is close to zero in some fraction of master-key. The probability of a 13-round multiple differentials of `GIFT-64`, which has the same input difference patterns and same output difference, is improved from $2^{-58.96}$ to $2^{-55.67}$ with 4-bit conditions of master-key. The details of the analysis are as follows.

The 13-round differential of `GIFT-64`. For the dominant characteristic with average probability $p_{avg} = 2^{-64}$, denoted by ε_1, of the 13-round differential of `GIFT-64` presented in [10], we search and find 64 quasidifferential trails with $|c| = p_{avg}$ corresponding to ε_1. Take one of 64 trails, denoted by t_1, corresponding to ε_1 as an example. The ε_1 and t_1 are both listed in Table 3. The function for each round is $\mathsf{F}_i = \mathsf{G}_i + rk_i$ for $i = 1, \dots, r$, where G_i is the `PermBits ∘ SubCells` operation, and rk_i is the `AddRoundKey` operation. According to Eq. (9), we have the correlation for t_1 is that

$$cor_1 = (-1)^{\sum_{i=1}^{r} u_{i+1}^{\mathsf{T}} rk_i} \cdot (-1)^{\sum_{i=1}^{r} b_i} \cdot \prod_{i=1}^{r} |D^{\mathsf{G}_i}_{(u_{i+1}, a_{i+1}), (u_i, a_i)}| = (-1)^{\mathcal{K}_1} \cdot (-1)^0 \cdot 2^{-64},$$
$$(14)$$

where $\mathcal{K}_1 = rk_1^0 + rk_1^{16} + rk_3^2 + rk_3^{17} + rk_5^0 + rk_5^{16} + rk_7^2 + rk_7^{17} + rk_9^0 + rk_9^{16} + rk_{11}^2 + rk_{11}^{17}$. Thus, a weak-key condition $\mathcal{K}_1 = 0$ for t_1 is obtained to ensure that $cor_1 > 0$. After performing a similar analysis for the other 63 trails, a total of 64 conditions are obtained.

It is easy to convert the 64 conditions about round-key bits into conditions about master-key bits as the linear key-schedule of `GIFT`. We get 4-bit conditions of the master-key after the Gaussian elimination of the 64 conditions. Suppose that four rounds are added before the 13-round distinguisher to launch the key-recovery attack, we get a weak-key space with 4-bit conditions of master-key, denoted by W_1:

$$k_0^4 + k_0^{12} = 0, k_4^5 + k_4^{13} = 0, k_0^0 + k_0^8 = 0, k_4^1 + k_4^9 = 0. \qquad (15)$$

The size of the weak-key space W_1 is $2^{128-4} = 2^{124}$. In the weak-key space W_1, the probability of characteristic ε_1 is increased from 2^{-64} to $2^6 \cdot 2^{-64} = 2^{-58}$, and the probability of the differential $\texttt{0x0000000000000202} \xrightarrow{13\text{-}r} \texttt{0x0000000500000005}$ is improved from $2^{-62.06}$ to $2^{-57.82}$ after applying Algorithm 1.

The 13-round multiple differentials of `GIFT-64`. According to the 13-round multiple differentials in [10], we search for all 13-round characteristics with $p_{avg} \geq 2^{-64}$ satisfying the output difference $\texttt{0x0000000000001010}$, and find

Table 3. A quasidifferential trail t_1 corresponding to a differential characteristic ε_1.

r	a_r, SubCell(a_r) in ε_1, t_1	p^r_{avg}	u_r, SubCell(u_r) in t_1	$c_r = D^{G_r}_{(u_{r+1},a_{r+1}),(u_r,a_r)}$	$(-1)^{u^\mathsf{T}_{r+1}rk_r}$	b_r
1	0x0000000000000202 0x0000000000000505	2^{-4}	0x0000000000000000 0x0000000000000505	$D^{G_1}_{(5,5),(0,2)}D^{G_1}_{(5,5),(0,2)}=2^{-4}$	$(-1)^{rk^0_1+rk^{16}_1}$	0
2	0x0000000500000005 0x0000000200000002	2^{-6}	0x0000000500000005 0x0000000000000000	$D^{G_2}_{(0,2),(5,5)}D^{G_2}_{(0,2),(5,5)}=2^{-6}$		0
3	0x0000000002020000 0x0000000005050000	2^{-4}	0x0000000000000000 0x0000000005050000	$D^{G_3}_{(5,5),(0,2)}D^{G_3}_{(5,5),(0,2)}=2^{-4}$	$(-1)^{rk^2_3+rk^{17}_3}$	0
4	0x0000005000000050 0x0000002000000020	2^{-6}	0x0000005000000050 0x0000000000000000	$D^{G_4}_{(0,2),(5,5)}D^{G_4}_{(0,2),(5,5)}=2^{-6}$		0
5	0x0000000000000202 0x0000000000000505	2^{-4}	0x0000000000000000 0x0000000000000505	$D^{G_5}_{(5,5),(0,2)}D^{5_1}_{(5,5),(0,2)}=2^{-4}$	$(-1)^{rk^0_5+rk^{16}_5}$	0
6	0x0000000500000005 0x0000000200000002	2^{-6}	0x0000000500000005 0x0000000000000000	$D^{G_6}_{(0,2),(5,5)}D^{G_6}_{(0,2),(5,5)}=2^{-6}$		0
7	0x0000000002020000 0x0000000005050000	2^{-4}	0x0000000000000000 0x0000000005050000	$D^{G_7}_{(5,5),(0,2)}D^{G_7}_{(5,5),(0,2)}=2^{-4}$	$(-1)^{rk^2_7+rk^{17}_7}$	0
8	0x0000005000000050 0x0000002000000020	2^{-6}	0x0000005000000050 0x0000000000000000	$D^{G_8}_{(0,2),(5,5)}D^{G_8}_{(0,2),(5,5)}=2^{-6}$		0
9	0x0000000000000202 0x0000000000000505	2^{-4}	0x0000000000000000 0x0000000000000505	$D^{G_9}_{(5,5),(0,2)}D^{G_9}_{(5,5),(0,2)}=2^{-4}$	$(-1)^{rk^0_9+rk^{16}_9}$	0
10	0x0000000500000005 0x0000000200000002	2^{-6}	0x0000000500000005 0x0000000000000000	$D^{G_{10}}_{(0,2),(5,5)}D^{G_{10}}_{(0,2),(5,5)}=2^{-6}$		0
11	0x0000000002020000 0x0000000005050000	2^{-4}	0x0000000000000000 0x0000000005050000	$D^{G_{11}}_{(5,5),(0,2)}D^{G_{11}}_{(5,5),(0,2)}=2^{-4}$	$(-1)^{rk^2_{11}+rk^{17}_{11}}$	0
12	0x0000005000000050 0x0000002000000020	2^{-6}	0x0000005000000050 0x0000000000000000	$D^{G_{12}}_{(0,2),(5,5)}D^{G_{12}}_{(0,2),(5,5)}=2^{-6}$		0
13	0x0000000000000202 0x0000000000000505	2^{-4}	0x0000000000000000 0x0000000000000000	$D^{G_{13}}_{(0,5),(0,2)}D^{G_{13}}_{(0,5),(0,2)}=2^{-4}$		0

196 characteristics with $p_{avg} = 2^{-64}$. Furthermore, we find 33 of the 196 characteristics having the same input difference patterns and the same weak-key space, which are listed in Appendix C, Table 13. Suppose that three rounds are added before the 13-round multiple differential distinguisher to launch the key-recovery attack, we get a weak-key space with 4-bit conditions of master-key, denoted by W_2:

$$k^1_2 + k^9_2 = 0, k^5_2 + k^{13}_2 = 0, k^0_6 + k^8_6 = 0, k^4_6 + k^{12}_6 = 0. \tag{16}$$

The size of W_2 is 2^{124}. In W_2, the probability of the 13-round multiple differentials, which contains 33 characteristics, is improved from $2^{-58.96}$ to $2^{-55.67}$.

4.3   Weak-Key Distinguishers for `GIFT-128`

Similarly, we find that for `GIFT`-128, the probability of the 20-round differential (presented in [26]) is improved from $2^{-121.83}$ to $2^{-114.77}$ with 6-bit conditions of master-key, and the probability of a 21-round multiple differentials of `GIFT`-128 is improved from $2^{-128.38}$ to $2^{-122.77}$ with 4-bit conditions of master-key.

The 20-round differentials of `GIFT-128`. For the 8 20-round differentials proposed in [26] (Table 7), which are used to launch the known best published 27-round differential attack on `GIFT`-128, a similar analysis is performed to obtain the weak-key spaces and probabilities. We find that the probability of differential 2 (0x00000000000000000000000000000a0 $\xrightarrow{20\text{-}r}$ 0x0000000000000000200000 0210000001), which contains 8 characteristics, is improved from $2^{-121.83}$ to $2^{-114.77}$ with 6-bit conditions of master-key. The size of the weak-key space is 2^{122}. The details are listed in Appendix D, Table 16. Suppose that four rounds are added before the 20-round distinguisher to launch the key-recovery attack, we get a weak-key space with 6-bit conditions of master-key, denoted by W_3:

$$k_0^9 + k_1^7 = 0, k_0^{11} + k_1^9 = 0, k_4^5 + k_5^1 = 0, k_6^9 + k_7^{11} = 0, k_6^{11} + k_7^{13} = 0, k_2^{15} = 1. \quad (17)$$

The 21-round differentials of `GIFT-128`. We search for 21-round differentials that satisfy only one active S-box in the input difference, the output difference ΔOUT satisfies $\Delta OUT[127 \sim 64] = 0$ or $\Delta OUT[63 \sim 0] = 0$, and find 18 21-round differentials, which are listed in Appendix E, Table 19. Similarly, the quasidifferential trails for these differentials are searched, and the weak-key conditions for each differential are obtained. After that, we find 2 (differential 9 and 10 in Table 19) of the 18 differentials having the same input difference with the same 4-bit conditions of master-key. The details are listed in Appendix E, Table 20. Suppose that four rounds are added before the 21-round multiple differential distinguisher to launch the key-recovery attack, we get a weak-key space with 4-bit conditions of master-key, denoted by W_4:

$$k_4^4 + k_5^0 = 0, k_6^8 + k_7^{10} = 0, k_6^{10} + k_7^{12} = 0, k_2^1 = 1. \quad (18)$$

The size of W_4 is 2^{124}, and the probability of the 21-round multiple differentials, which contains 2 differentials, is improved from $2^{-128.38}$ to $2^{-122.77}$ in W_4.

4.4   Experiments

In Sect. 3 Assumption 1, we suppose that quasidifferential trails satisfying $|c| = p_{avg}$ are dominant for the probability of a characteristic. However, take the characteristic ε_1 in Table 3 as an example, when $\frac{|c|}{p_{avg}} \leq 2^{-6}$, a large number of quasidifferential trails exist. The number of quasidifferential trails of ε_1 from $\frac{|c|}{p_{avg}} = 2^0$ to $\frac{|c|}{p_{avg}} = 2^{-9}$ are listed in Table 4. To verify the effect of quasidifferential trails with $|c| < p_{avg}$ on the probability of characteristic can be ignored, we have done experimental verification on `GIFT`-64 and `GIFT`-128, respectively.

Table 4. The numbers of trails (denoted by # t) from $\frac{|c|}{p_{avg}} = 2^0$ to $\frac{|c|}{p_{avg}} = 2^{-9}$.

$-\log_2 \frac{|c|}{p_{avg}}$	0	1	2	3	4	5	6	7	8	9
# t	64	0	0	0	0	0	1024	0	1536	≥ 5856

Table 5. Experimental results of `GIFT`-64.

			Cases of key in the encryption					
$round$	p_{avg}	$pairs_{exp}$	Random round-key		Random master-key		Fixed master-key	
			$pairs_{right}$	p_{exp}	$pairs_{right}$	p_{exp}	$pairs_{right}$	p_{exp}
1 to 4	2^{-20}	2^{25}	3325	$2^{-19.95}$	3385	$2^{-19.92}$	12786	$2^{-18.00}$
5 to 8	2^{-20}	2^{25}	3252	$2^{-19.98}$	3564	$2^{-19.84}$	12668	$2^{-18.01}$
9 to 13	2^{-24}	2^{29}	3204	$2^{-24.00}$	2842	$2^{-24.17}$	12805	$2^{-22.00}$

Experiments on `GIFT`-64. The 13-round characteristic ε_1 (listed in Table 3) is divided into two consecutive 4-rounds and one consecutive 5-round to experiment with the probability in the weak-key space W_1.

For each consecutive round, we conduct experiments under three cases: (1) round-key bits of each round are randomly generated, corresponding to the *key-averaged probability* for *Markov ciphers*; (2) the 128-bit master-key used in the key-schedule is randomly generated, corresponding to the key space of size 2^{128}; (3) the 128-bit master-key used in the key-schedule satisfies 4-bit conditions of W_1 (Eq. (15)), corresponding to the weak-key space of size 2^{124}.

In each case, 100 times are performed. Each time, plaintext pairs satisfying the input difference are randomly generated, the number of corresponding consecutive rounds is encrypted, and the number of right pairs (satisfying all intermediate differences) is counted. The experimental results are listed in Table 5. $pairs_{exp}$ represents the number of randomly generated plaintext pairs in each time. $pairs_{right}$ represents the number of right pairs counted by 100 times, and $p_{exp} = \frac{pairs_{right}}{pairs_{exp}}$.

From the results in Table 5, the probabilities p_{exp} of case (3) in the weak-key space W_1 are much higher than case (2). The experimental probability of the characteristic ε_1 can be expressed as the product of two consecutive 4-rounds and one consecutive 5-round, i.e., $p \approx 2^{-58.01}$, which is close to 2^{-58} and exactly consistent with Assumption 1.

The numbers of right pairs of each experiment for three cases are shown in Fig. 1. In each subfigure, the lower triangles in yellow, the squares in blue, and the stars in red represent case (1), case (2), and case (3), respectively. It shows that the number of right pairs of case (2) is zero for some fraction of keys.

Experiments on `GIFT`-128. We also perform the experiments for six consecutive 2-rounds for the two dominant 21-round characteristics, which are listed in Ap-

(a) round 1 to 4

(b) round 5 to 8

(c) round 9 to 13
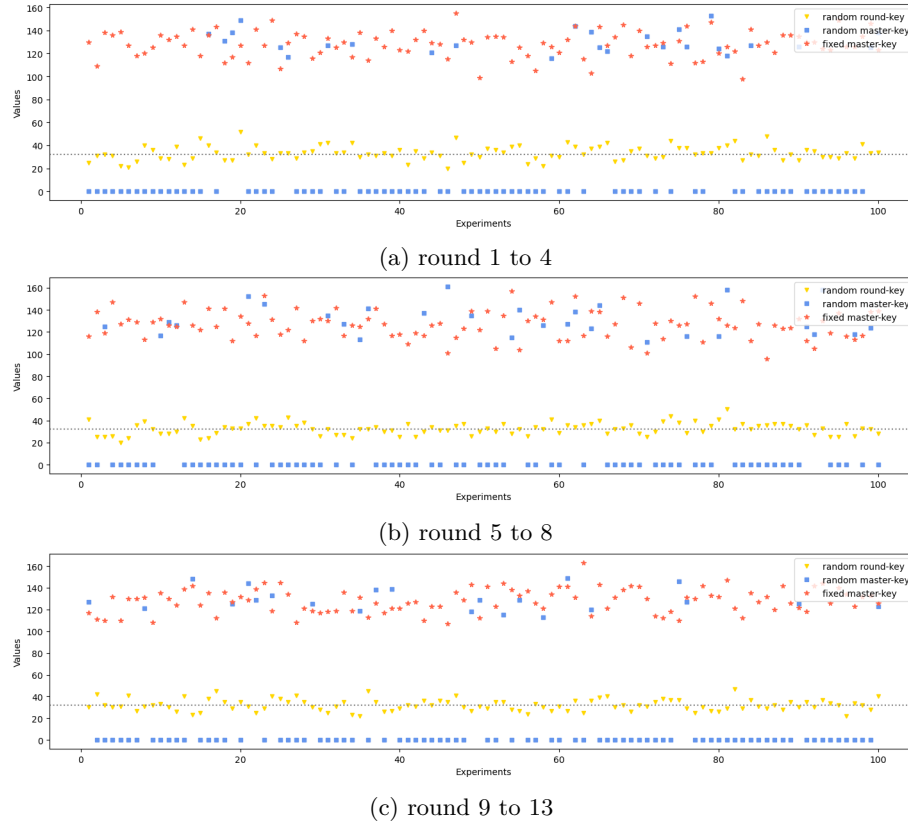
Fig. 1. Numbers of right pairs of 100 times for three cases of the key of `GIFT`-64.

Table 6. Experimental results of `GIFT`-128.

$round$	p_{avg}	$pairs_{exp}$	Cases of key in the encryption					
			Random round-key		Random master-key		Fixed master-key	
			$pairs_{right}$	p_{exp}	$pairs_{right}$	p_{exp}	$pairs_{right}$	p_{exp}
5 to 6	2^{-19}	2^{25}	6468	$2^{-18.99}$	7238	$2^{-18.81}$	12690	$2^{-18.00}$
8 to 9	2^{-9}	2^{15}	12854	$2^{-8.00}$	12698	$2^{-8.00}$	12696	$2^{-8.00}$
10 to 11	2^{-21}	2^{25}	1525	$2^{-21.07}$	1098	$2^{-21.54}$	6394	$2^{-19.00}$
13 to 14	2^{-9}	2^{15}	12704	$2^{-8.00}$	12916	$2^{-7.98}$	12608	$2^{-8.00}$
16 to 17	2^{-20}	2^{25}	3233	$2^{-19.98}$	3432	$2^{-19.90}$	6340	$2^{-19.01}$
19 to 20	2^{-9}	2^{15}	9577	$2^{-8.42}$	9578	$2^{-8.42}$	9687	$2^{-8.40}$

pendix E, Table 21, to verify that the probability in the weak-key space W_4. The results are listed in Table 6, showing that Assumption 1 is reasonable.

5   Improved Weak-Key Key-Recovery Attacks on `GIFT`

In this section, we mount and reevaluate the attacks on `GIFT`-64, and `GIFT`-128, by the differentials in the weak-key spaces proposed in Sect. 4, respectively.

5.1   Weak-Key Key-Recovery Attacks on `GIFT`-64

The 21-round differential attack on `GIFT`-64. By adding four rounds before and four rounds after the 13-round differential distinguisher, which is presented in Sect. 4.2 with probability $2^{-57.82}$ in the weak-key space W_1, we launch a 21-round weak-key key-recovery attack on `GIFT`-64. The key-recovery process is shown in Fig. 2.

   To facilitate representation and simplify the process, we perform an equivalent substitution for the `AddRoundkey` operation in the bottom of the distinguisher, and move it before the `PermBits` operation. The RK' is equals to the inverse of `PermBits` of RK, i.e., $RK' = \texttt{PermBits}^{-1}(RK)$. Additionally, according to the key schedule of `GIFT`-64, the round key RK_i and RK_j involve the same 32-bit master key when $i \equiv j \bmod 4$.

Data collection. `GIFT`'s structure allows us to freely extend one round because there is no whitening key at the beginning. Specifically, the structure can be constructed at X_1^P, while the plaintext P can be obtained by applying the inverse operation of `PermBits` ($\texttt{PermBits}^{-1}$) and `SubCell` ($\texttt{SubCell}^{-1}$) to X_1^P. Then encrypt the plaintext and obtain the corresponding ciphertext. By iterating all 64-bit in X_1^P, i.e., 2^{64} plaintexts, we can generate about $\binom{2^{64}}{2} \approx 2^{127}$ plaintext pairs.

Key Recovery Phase. Suppose that after data collection, we have 2^n plaintext pairs and corresponding ciphertext pairs. The corresponding bits of the master-key that need to be guessed during the key-recovery phase are listed in Table 7. The time complexity of each step with initial 2^n pairs is listed in Table 8. The detailed analysis of guessing keys and filtering to get the right pairs is given below. ? represents one bit of undetermined difference.

1). Guess 32-bit of RK_1: Guess 2-bit value of $RK_1[1,0]$, make the `SubCell` operation on the first S-box, remain the pairs satisfying

$$\texttt{SubCell}(X_1^P[3 \sim 0] \oplus RK_1[1,0]) \oplus \texttt{SubCell}(X_1^P[3 \sim 0] \oplus RK_1[1,0]) = 00?0,$$

and about $2^n \times 2^{-3}$ pairs left. Similarly, for the other 30-bit value of RK_1, i.e., $RK_1[31 \sim 2]$, guess each 2-bit RK_1 and perform a 3-bit filtering, around the right candidate pairs remain. The similar procedures are performed 16 times in total. Step 1) guesses 32-bit RK_1 in total, and about 2^{n-48} pairs left.

Table 7. Involved keys in the 21-round differential attack on `GIFT`-64 of the 13-round differential. The keys in blue represent the bits that do not repeat the guess.

RK_1	$k_1^{15}k_0^{15}$	$k_1^{14}k_0^{14}$	$k_1^{13}k_0^{13}$	$k_1^{12}k_0^{12}$	$k_1^{11}k_0^{11}$	$k_1^{10}k_0^{10}$	$k_1^9k_0^9$	$k_1^8k_0^8$	$k_1^7k_0^7$	$k_1^6k_0^6$	$k_1^5k_0^5$	$k_1^4k_0^4$	$k_1^3k_0^3$	$k_1^2k_0^2$	$k_1^1k_0^1$	$k_1^0k_0^0$
RK_2									$k_3^7k_2^7$	$k_3^6k_2^6$	$k_3^5k_2^5$	$k_3^4k_2^4$				
RK_3							$k_5^9k_4^9$							$k_5^1k_4^1$		
RK_4																
RK'_{18}							$k_3^{14}k_2^2$									$k_3^{12}k_2^0$
RK'_{19}		$k_5^7k_4^{11}$		$k_5^{15}k_4^3$		$k_5^6k_4^{10}$		$k_5^{14}k_4^2$		$k_5^5k_4^9$		$k_5^{13}k_4^1$		$k_5^4k_4^8$		$k_5^{12}k_4^0$
RK'_{20}	$k_7^3k_6^7$	$k_7^7k_6^{11}$	$k_7^{11}k_6^{15}$	$k_7^{15}k_6^3$	$k_7^2k_6^6$	$k_7^6k_6^{10}$	$k_7^{10}k_6^{14}$	$k_7^{14}k_6^2$	$k_7^1k_6^5$	$k_7^5k_6^9$	$k_7^{39}k_6^{13}$	$k_7^{13}k_6^1$	$k_7^9k_6^4$	$k_7^4k_6^8$	$k_7^8k_6^{12}$	$k_7^{12}k_6^0$
RK'_{21}	$k_1^5k_0^3$	$k_1^9k_0^7$	$k_1^{13}k_0^{11}$	$k_1^1k_0^{15}$	$k_1^4k_0^2$	$k_1^8k_0^6$	$k_1^{12}k_0^{10}$	$k_1^0k_0^{14}$	$k_1^3k_0^1$	$k_1^7k_0^5$	$k_1^{11}k_0^9$	$k_1^{15}k_0^{13}$	$k_1^2k_0^0$	$k_1^6k_0^4$	$k_1^{10}k_0^8$	$k_1^{14}k_0^{12}$

2). Guess 8-bit of RK_2: Guess 2-bit value of $RK_2[9,8]$, make `SubCell` on the 5-th S-box, remain the pairs satisfying

$$\texttt{SubCell}(X_2^P[18 \sim 15]\oplus RK_2[9,8])\oplus\texttt{SubCell}(X_2^P[18 \sim 15]\oplus RK_2[9,8]) = 010?,$$

and about $2^{n-48} \times 2^{-3}$ pairs left. Guess $RK_2[13,12]$, and perform a similar 3-bit filtering. Guess $RK_2[11,10]$, make `SubCell` on the 6-th S-box, and discard the pairs that do not satisfy $\Delta X_3^S[23 \sim 20] =?0?0$. Then a 2-bit filtering is performed. Similarly, guess $RK_{15,14}$ and perform a 2-bit filtering. Step 2) guess 8-bit RK_2 in total, and about 2^{n-58} pairs left.

3). Guess 4-bit RK_3: For each of the 2 active S-boxes in ΔX_3^P, guess the corresponding 2-bit RK_3, make `SubCell`, and perform a 3-bit filtering. Step 3) guesses 4-bit RK_3 in total, and about 2^{n-64} pairs left.

4). Guess 32-bit RK'_{21}: Note that all 32-bit subkeys of RK'_{21} are already guessed in Step 1), thus, for each of the 16 active S-boxes in $\Delta X'^P_{21}$, make `SubCell`$^{-1}$ on the corresponding S-box. Step 4) does not perform the filtering, and about 2^{n-64} pairs left.

5). Guess 32-bit RK'_{20}: Guess 2-bit $RK'_{20}[1,0]$, make `SubCell`$^{-1}$, remain the pairs satisfying

$$\texttt{SubCell}^{-1}(X'^P_{20}[3 \sim 0]\oplus RK'_{20}[1,0])\oplus\texttt{SubCell}^{-1}(X'^P_{20}[3 \sim 0]\oplus RK'_{20}[1,0]) = 0?0?,$$

and about $2^{n-64} \times 2^{-2}$ pairs left. For the other 15 active S-boxes in $\Delta X'^P_{20}$, 2-bit filtering is performed for each 2-bit RK'_{20} is guessed. The similar procedures are performed 16 times, and 32 bits RK'_{20} are guessed in Step 5) in total. After this step, there are about 2^{n-96} pairs left.

6). Guess 16-bit RK'_{19}: Similarly, for each one of 8 active S-boxes in $\Delta X'^P_{19}$, guess the corresponding 2-bit RK'_{19}, make `SubCell`$^{-1}$, and perform a 3-bit filtering. Step 6) guesses 16-bit RK'_{19}, and about 2^{n-120} pairs left.

7). Guess 4-bit RK'_{18}: Guess $RK'_{18}[1,0]$ and $RK'_{18}[17,16]$, make `SubCell`$^{-1}$, perform a 8-bit filtering in total. Step 7) guesses 4-bit RK'_{18}, and about 2^{n-128} pairs left.

Complexity and Success Probability. For the right key guesses, there are about $2^{n-64-57.82}$ pairs left, while for the wrong key guesses, about 2^{n-128} pairs left. We set $n = 121.82$ to ensure that at least one pair is remained for the right key

Fig. 2. 21-Round differential attack on `GIFT`-64. Each square represents one bit. The squares in white stand for the values of difference bits are '0'. The squares in green stand for the values of difference bits are '1'. The squares in grey stand for the values of difference bits that are indeterminate. The squares in orange stand for the bits of key are need to be guessed. The squares in blue stand for the bits of key that are omitted.
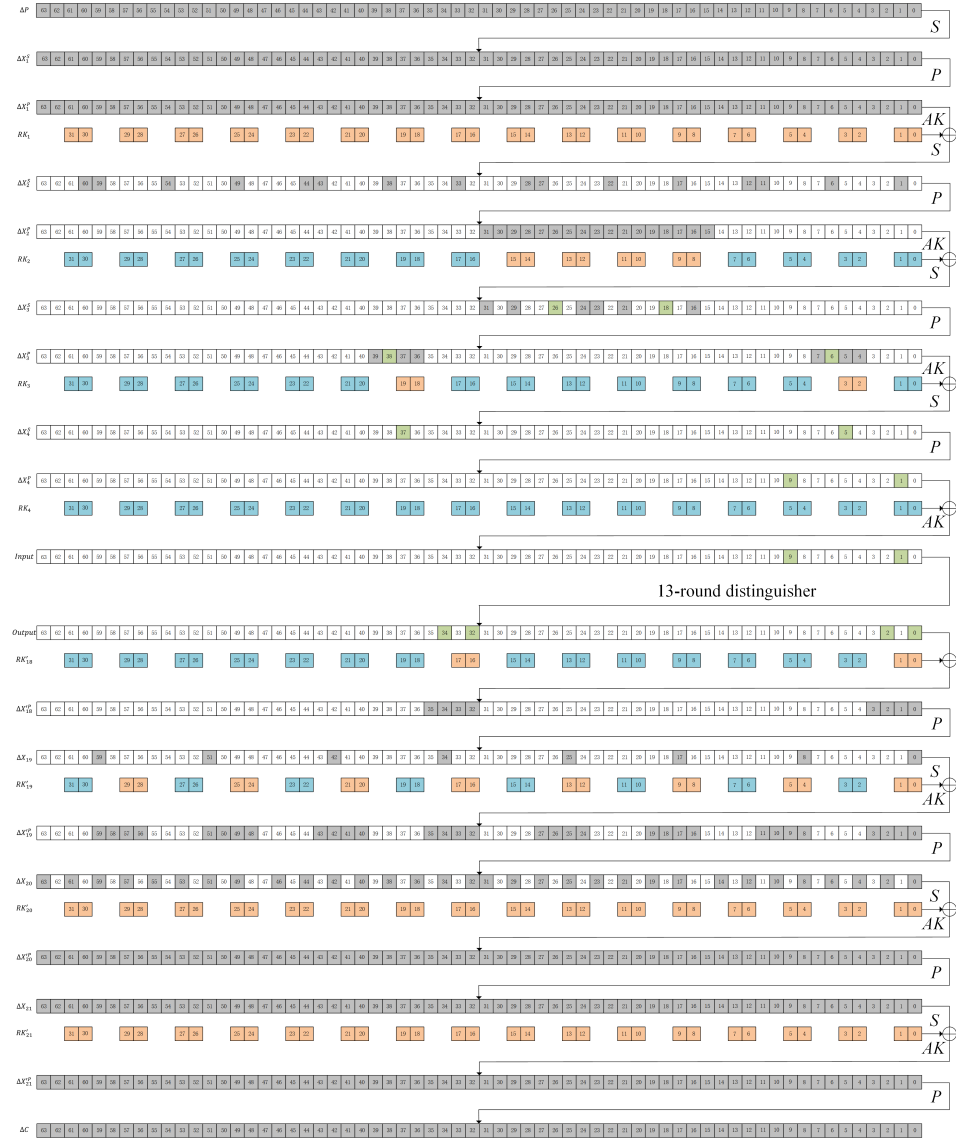
Table 8. Time complexity of the 21-round differential attack on `GIFT-64` in each step.

Step	RK	# Key	Time(S-box operations)	Filtering probability	# Remaining pairs
1.	RK_1	2^{32}	$2 \times 2^n \times 2^3$	$2^{-3 \times 16}$	2^{n-48}
2.	RK_2	2^8	$2 \times 2^{32} \times 2^{n-48} \times 2^3$	$2^{-3 \times 2 - 2 \times 2}$	2^{n-58}
3.	RK_3	2^4	$2 \times 2^{40} \times 2^{n-58} \times 2^3$	$2^{-3 \times 2}$	2^{n-64}
4.	RK'_{21}	-	$2 \times 2^{44} \times 2^{n-64} \times 16$	-	2^{n-64}
5.	RK'_{20}	2^{32}	$2 \times 2^{44} \times 2^{n-64} \times 2^6$	$2^{-2 \times 16}$	2^{n-96}
6.	RK'_{19}	2^{16}	$2 \times 2^{76} \times 2^{n-96} \times 2^3$	$2^{-3 \times 8}$	2^{n-120}
7.	RK'_{18}	2^4	$2 \times 2^{92} \times 2^{n-120} \times 2^{2.32}$	$2^{-4 \times 2}$	2^{n-128}

guesses, while about $2^{-6.18}$ pairs are remained for the wrong key guesses. Therefore, the data complexity is about 2^{64} chosen-plaintexts, the time complexity is dominated by Step 1), and about $2^{125.82} \cdot \frac{1}{16} \cdot \frac{1}{21} \approx 2^{117.42}$ 21-round operations, the memory complexity is about 2^{96}-bit. We use the formula presented by Selçuk in [18] to evaluate the success probability P_S:

$$P_S = \Phi\left(\frac{\sqrt{\mu S_N} - \Phi^{-1}(1 - 2^{-a})}{\sqrt{S_N + 1}}\right), \qquad (19)$$

where p is the probability of the differential, N is the plaintext-ciphertext pairs, $\mu = pN$, S_N is the signal-to-noise, and a is an a-bit or higher advantage. We have $S_N = 2^{6.18}$. For $n = 121.82$, $\mu = 1$, $a = 5$, $P_S \approx 81.06\%$. For $n = 125$, $\mu = 2^{3.18}$, $a = 15$, $P_S \approx 99.41\%$, and time complexity is about $2^{120.6}$ 21-round operations.

Remark. The calculation of the time complexity of the 21-round differential attack proposed in [10], which is the combination of the 1-round attack and the 20-round, is not accurate, we reevaluate the time complexity utilizing their 13-round differential with average probability $2^{-62.06}$ based on the above analysis. Then $S_N = \frac{2^{n-64-62.06}}{2^{n-128}} = 2^{1.94}$. For $n = 126.06$ to ensure that at least one right pair left, $\mu = 1$, $P_S \approx 51.60\%$ for $a = 5$, and the time complexity is about $2^{121.66}$ 21-round operations. Our attack improves the success probability and complexity in the weak-key space W_1 compared to [10].

The 21-round multiple differential attack on `GIFT-64`. Based on the 13-round multiple differentials proposed in Sect. 4.2 with probability $2^{-55.67}$ in the weak-key space W_2, we add three rounds before and five rounds after the distinguisher to mount the 21-round multiple differential attack on `GIFT`-64 in Appendix C. Thanks to increasing the probability of the 13-round multiple differential distinguisher in the weak-key space W_2, it allows us to boost the multiple differential attack on `GIFT`-64 from 20 to 21 rounds.

Complexity and Success Probability. The data complexity is 2^{64} chosen-plaintexts, the time complexity is about $2^{123.27}$ 21-round operations, the memory complexity is about 2^{112}-bit, and the success probability is about 99.9%.

5.2   Weak-Key Key Recovery Attacks on `GIFT-128`

The 27-round differential attack on `GIFT-128`. Using the 20-round differential with probability $2^{-114.77}$ in the weak-key space W_3, which is presented in Sect. 4.3, we launch the differential attack on 27-round `GIFT-128` by adding four rounds before and three rounds after the distinguisher in Appendix D.

Complexity and Success Probability. The data complexity is about $2^{115.77}$ chosen-plaintexts, the time complexity is about $2^{110.85}$ 27-round operations, the memory complexity is about 2^{92}-bit, and the success probability is about 99.9%. Compared to the 27-round differential attack in [26], the complexity is reduced by about $2^{3.06}$ in a weak-key setting.

The 28-round differential attack on `GIFT-128`. Similarly, by adding four rounds before and three rounds after, the first 28-round multiple differential attack on `GIFT`-128 is launched based on the 21-round multiple differentials with probability $2^{-122.77}$ in the weak-key space W_4, which is proposed in Sect. 4.3. The details of the attack are presented in Appendix E.

Complexity and Success Probability. The data complexity is about $2^{123.77}$ chosen-plaintexts, the time complexity is about $2^{123.77}$ 28-round operations, the memory complexity is about 2^{96}-bit, and the success probability is about 86.5%.

6   Distinguisher and Attack on `SUNDAE-GIFT`

We attack the initialization phase without plaintext data of version `SUNDAE-GIFT`-96 of `SUNDAE-GIFT` family with a 96-bit nonce, which is the primary member satisfying the requirements set by NIST. Our restriction for searching distinguishers is that the difference of the plaintext is only active in the high 96 bits by adding a certain number of rounds before the distinguisher. Then we find two 11-round differential characteristics, which are listed in Appendix F, Table 25 with average probability 2^{-60}, can be utilized to launch a 17-round differential attack by adding three rounds before and three rounds after the distinguisher. Similarly, we search for quasidifferential trails satisfying $|c| = p_{avg}$ and find only one quasidifferential trail with all-zero masks for each characteristic, thus, there are no weak-key conditions for these two characteristics.

The first 17-round differential attack on `SUNDAE-GIFT` utilizing the 11-round differential characteristic with probability 2^{-60} is proposed in Appendix F.

Complexity and Success Probability : The data complexity is about $2^{62.5}$ chosen-plaintexts, the time complexity is about $2^{75.37}$ 17-round operations, the memory complexity is about 2^{66}-bit, and the success probability is about 99.9%.

7   Conclusion

In this paper, we continue the work on the quasidifferential transition matrix in differential cryptanalysis proposed by Beyne and Rijmen at CRYPTO 2022 and apply their approach to `GIFT`. By holding some conditions of master-key, the probabilities of some differential characteristics with small probabilities can be improved in a weak-key setting. Then the weak-key (multiple) differential key-recovery attacks on `GIFT` are obtained based on the weak-key distinguishers. For `GIFT`-64, the multiple differential attack can be boosted from 20 to 21 rounds, and the 21-round differential attack can be improved in terms of complexity. For `GIFT`-128, the complexity of the 27-round differential attack can be improved, and the first 28-round (multiple) differential attack is obtained. Finally, after checking the 11-round differential characteristic with quasidifferential trails, we mount the first differential attack on the 17-round `SUNDAE-GIFT`.

References

1. Banik, S., Bogdanov, A., Luykx, A., Tischhauser, E.: Sundae: Small universal deterministic authenticated encryption for the internet of things. IACR Transactions on Symmetric Cryptology **2018**(3), 135 (Sep 2018), `https://tosc.iacr.org/index.php/ToSC/article/view/7296`
2. Banik, S., Bogdanov, A., Peyrin, T., Sasaki, Y., Tischhauser, S.M.E., Todo, Y.: Sundae-gift. Submission to Round, 1, 2019
3. Banik, S., Chakraborti, A., Inoue, A., Iwata, T., Minematsu, K., Nandi, M., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: Gift-cofb. Cryptology ePrint Archive, Paper 2020/738 (2020), `https://eprint.iacr.org/2020/738`
4. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: Gift: A small present. In: Fischer, W., Homma, N. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2017. pp. 321–345. Springer International Publishing, Cham (2017)
5. Beyne, T., Rijmen, V.: Differential cryptanalysis in the fixed-key model. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13509, pp. 687–716. Springer (2022), `https://doi.org/10.1007/978-3-031-15982-4_23`

6. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds.) Advances in Cryptology-CRYPTO' 90. pp. 2–21. Springer Berlin Heidelberg, Berlin, Heidelberg (1991)

7. Blondeau, C., Gérard, B.: Multiple differential cryptanalysis: Theory and practice. In: Joux, A. (ed.) Fast Software Encryption. pp. 35–54. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)

8. Boura, C., David, N., Derbez, P., Boissier, R.H., Naya-Plasencia, M.: A generic algorithm for efficient key recovery in differential attacks - and its associated tool. In: Joye, M., Leander, G. (eds.) Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part I. Lecture Notes in Computer Science, vol. 14651, pp. 217–248. Springer (2024). `https://doi.org/10.1007/978-3-031-58716-0_8`, `https://doi.org/10.1007/978-3-031-58716-0_8`

9. Chakraborti, A., Datta, N., Jha, A., Nandi, M.: Hyena. Submission to the NIST Lightweight Cryptography project, 2019

10. Chen, H., Zong, R., Dong, X.: Improved differential attacks on GIFT-64. In: Zhou, J., Luo, X., Shen, Q., Xu, Z. (eds.) Information and Communications Security - 21st International Conference, ICICS 2019, Beijing, China, December 15-17, 2019, Revised Selected Papers. Lecture Notes in Computer Science, vol. 11999, pp. 447–462. Springer (2019), `https://doi.org/10.1007/978-3-030-41579-2_26`

11. Daemen, J., Govaerts, R., Vandewalle, J.: Correlation matrices. In: Preneel, B. (ed.) Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings. Lecture Notes in Computer Science, vol. 1008, pp. 275–285. Springer (1994), `https://doi.org/10.1007/3-540-60590-8_21`

12. Flórez-Gutiérrez, A., Todo, Y.: Improving linear key recovery attacks using walsh spectrum puncturing. In: Joye, M., Leander, G. (eds.) Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part I. Lecture Notes in Computer Science, vol. 14651, pp. 187–216. Springer (2024), `https://doi.org/10.1007/978-3-031-58716-0_7`

13. 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.) Selected Areas in Cryptography. pp. 198–228. Springer International Publishing, Cham (2021)

14. Lai, X., Massey, J.L., Murphy, S.: Markov ciphers and differential cryptanalysis. In: Davies, D.W. (ed.) Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings. Lecture Notes in Computer Science, vol. 547, pp. 17–38. Springer (1991), `https://doi.org/10.1007/3-540-46416-6_2`

15. Li, L., Wu, W., Zheng, Y., Zhang, L.: The relationship between the construction and solution of the milp models and applications. Cryptology ePrint Archive, Paper 2019/049 (2019), `https://eprint.iacr.org/2019/049`

16. Liu, Y., Sasaki, Y.: Related-key boomerang attacks on gift with automated trail search including bct effect. Cryptology ePrint Archive, Paper 2019/669 (2019). `https://doi.org/10.1007/978-3-030-21548-4`

17. Sasaki, Y.: Integer linear programming for three-subset meet-in-the-middle attacks: Application to GIFT. In: Inomata, A., Yasuda, K. (eds.) Advances in Information and Computer Security - 13th International Workshop on Security, IWSEC 2018, Sendai, Japan, September 3-5, 2018, Proceedings. Lecture Notes in Computer Science, vol. 11049, pp. 227–243. Springer (2018), `https://doi.org/10.1007/978-3-319-97916-8_15`

18. Selçuk, A.A.: On probability of success in linear and differential cryptanalysis. J Cryptol 21, 131147 (2008) **2008**, `https://doi.org/10.1007/s00145-007-9013-7`
19. Sun, 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), `https://doi.org/10.46586/tosc.v2021.i1.269-315`
20. Sun, L., Wang, W., Wang, M.: Improved attacks on GIFT-64. In: AlTawy, R., Hülsing, A. (eds.) Selected Areas in Cryptography - 28th International Conference, SAC 2021, Virtual Event, September 29 - October 1, 2021, Revised Selected Papers. Lecture Notes in Computer Science, vol. 13203, pp. 246–265. Springer (2021), `https://doi.org/10.1007/978-3-030-99277-4_12`
21. Sun, L., Wang, W., Wang, M.: Linear cryptanalyses of three aeads with gift-128 as underlying primitives. IACR Transactions on Symmetric Cryptology **2021**(2), 199221 (Jun 2021), `https://tosc.iacr.org/index.php/ToSC/article/view/8909`
22. Sun, L., Wang, W., Wang, M.: Addendum to linear cryptanalyses of three aeads with GIFT-128 as underlying primitives. IACR Trans. Symmetric Cryptol. **2022**(1), 212–219 (2022), `https://doi.org/10.46586/tosc.v2022.i1.212-219`
23. Wang, S., Liu, M., Hou, S., Lin, D.: Differential-linear cryptanalysis of GIFT family and gift-based ciphers. IACR Commun. Cryptol. **1**(1), 13 (2024), `https://doi.org/10.62056/a6n5txol7`
24. Zhu, B., Dong, X., Yu, H.: Milp-based differential attack on round-reduced GIFT. In: Matsui, M. (ed.) Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11405, pp. 372–390. Springer (2019), `https://doi.org/10.1007/978-3-030-12612-4_19`
25. Zhu, B., Dong, X., Yu, H.: Milp-based differential attack on round-reduced gift. In: Matsui, M. (ed.) Topics in Cryptology – CT-RSA 2019. pp. 372–390. Springer International Publishing, Cham (2019)
26. Zong, R., Dong, X., Chen, H., Luo, Y., Wang, S., Li, Z.: Towards key-recovery-attack friendly distinguishers: Application to gift-128. IACR Transactions on Symmetric Cryptology **2021**(1), 156184 (Mar 2021), `https://tosc.iacr.org/index.php/ToSC/article/view/8836`

A Tables of GIFT

Table 9. 4-bit invertible S-box in GIFT.

x	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
$GS(x)$	0x1	0xa	0x4	0xc	0x6	0xf	0x3	0x9	0x2	0xd	0xb	0x7	0x5	0x0	0x8	0xe

Table 10. Bit permutation of GIFT-64.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_{64}(i)$	0	17	34	51	48	1	18	35	32	49	2	19	16	33	50	3
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P_{64}(i)$	4	21	38	55	52	5	22	39	36	53	6	23	20	37	54	7
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P_{64}(i)$	8	25	42	59	56	9	26	43	40	57	10	27	24	41	58	11
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P_{64}(i)$	12	29	46	63	60	13	30	47	44	61	14	31	28	45	62	15

Table 11. Bit permutation of GIFT-128.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_{64}(i)$	0	33	66	99	96	1	34	67	64	97	2	35	32	65	98	3
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P_{64}(i)$	4	37	70	103	100	5	38	71	68	101	6	39	36	69	102	7
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P_{64}(i)$	8	41	74	107	104	9	42	75	72	105	10	43	40	73	106	11
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P_{64}(i)$	12	45	78	111	108	13	46	79	76	109	14	47	44	77	110	15
i	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
$P_{64}(i)$	16	49	82	115	112	17	50	83	80	113	18	51	48	81	114	19
i	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
$P_{64}(i)$	20	53	86	119	116	21	54	87	84	117	22	55	52	85	118	23
i	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
$P_{64}(i)$	24	57	90	123	120	25	58	91	88	121	26	59	56	89	122	27
i	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
$P_{64}(i)$	28	61	94	127	124	29	62	95	92	125	30	63	60	93	126	31

Table 12. The values of the round constants in `GIFT`.

Rounds	Constants
$1-16$	01,03,07,0F,1F,3E,3D,3B,37,2F,1E,3C,39,33,27,0E
$17-32$	1D,3A,35,2B,16,2C,18,30,21,02,05,0B,17,2E,1C,38
$33-48$	31,23,06,0D,1B,36,2D,1A,34,29,12,24,08,11,22,04

B   Algorithm for Obtain a Good Weak-Key Space and Probability for a Differential

---

Algorithm 1 Obtain a good weak-key space and probability p for a differential.

Require: A given r-round differential, which contains d differential characteristics, denoted as
$\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_d$, respectively;
Ensure: A weak-key space, and the probability p of the differential in this weak-key space;
1: Initialize an empty set $\mathcal{S}$;
2: Initializes two linear systems M_c^i and M_a^i as empty;
3: **for** $i = 1, 2, \cdots, d$ **do**
4:     $p^i = 0$;
5:     ε_i is a differential characteristic with average probability p_{avg}^i in the differential;
6:     Search for all quasidifferential trails of ε_i that satisfy $|c_i| = p_{avg}^i$, and denoted as t_i;
7:     $len(t_i)$ represents the number of trails;
8:     **for** $j = 1, 2, \cdots, len(t_i)$ **do**
9:         $cor_j^i = (-1)^{\mathcal{K}_j^i + b_j^i} \cdot |c_j^i|$ is the correlation of the j-th trail $t_i[j]$;
10:         $lb_j^i : \mathcal{K}_j^i$ is a linear combination of round-key bits, which is derived by $\mathcal{K}_j^i$;
11:         $M_c^i = M_c^i \cup \{lb_j^i\}$;
12:         $le_j^i : \mathcal{K}_j^i = b_j^i$ is a linear equation of round-key bits, which is derived by $cor_j^i > 0$;
13:         $M_a^i = M_a^i \cup \{le_j^i\}$;
14:
15:     **if** $rank(M_c^i) = rank(M_a^i)$ and $len(t_i) > 2^{M_a^i}$ **then**
16:         $\ell_i = rank(M_a^{'i})$ and $M_a^{'i}$ is M_a^i after Gaussian elimination;
17:         W_i with ℓ_i linear equations is a valid weak-key space;
18:         $p^i = p^i + len(t_i) \cdot p_{avg}^i$;
19:         **for** $i' = 1, \cdots, d$ and $i' \neq i$ **do**
20:             $\varepsilon_{i'}$ is a characteristic with average probability $p_{avg}^{i'}$;
21:             Search for all quasidifferential trails of $\varepsilon_{i'}$ satisfying $|c_{i'}| = p_{avg}^{i'}$, and denoted as $t_{i'}$;
22:             **for** $j = 1, 2, \cdots, len(t_{i'})$ **do**
23:                 **if** $\mathcal{K}_j^{i'}$ is a linear combination of ℓ_i equations and the value is $v_j^{i'}$ **then**
24:                     $p^i = p^i + (-1)^{v_j^{i'} + b_j^{i'}}$
25:             $\mathcal{S} = \mathcal{S} \cup (log_2(p^i) - \ell_i)$;
26:     **else**
27:         break
28: Take the maximum value in set $\mathcal{S}$, suppose that the corresponding index of characteristic is i;
29: W_i is chosen as the weak-key space for the differential;
30: p^i is the probability of the differential in the weak-key space W_i;

C   Multiple Differential Attack on 21-Round `GIFT-64`

For the 13-round multiple differentials (33 characteristics are listed in Table 13) presented in Sect. 4.2 with probability $2^{-55.67}$ in the weak-key space W_2,

Table 13. 13-Round characteristics of `GIFT`-64 that have the common output difference 0x0000000000001010, both with $p_{avg} = 2^{-64}$. # t represents the number of quasidifferential trails satisfying $|c| = p_{avg}$ corresponding to each characteristic.

# t	Index	Input difference	Index	Input difference	Index	Input difference
	1	0x000000f0000000f0	2	0x000000c0000000c0	3	0x000000c0000000f0
	4	0x000000c0000000d0	5	0x000000d0000000f0	6	0x000000f0000000e0
16	7	0x000000c0000000e0	8	0x000000e0000000c0	9	0x000000e0000000f0
	10	0x000000e0000000d0	11	0x000000d0000000e0	12	0x000000d0000000c0
	13	0x000000f0000000d0	14	0x000000d0000000d0	15	0x000000f0000000c0
	16	0x000000e0000000e0				
	1	0x000000c0000000c0	2	0x000000c0000000d0	3	0x000000c0000000f0
	4	0x000000e0000000c0	5	0x000000d0000000c0	6	0x000000c0000000e0
4	7	0x000000f0000000c0	8	0x000000d0000000e0	9	0x000000e0000000d0
	10	0x000000e0000000f0	11	0x000000f0000000d0	12	0x000000d0000000d0
	13	0x000000e0000000e0	14	0x000000f0000000e0	15	0x000000d0000000f0
	16	0x000000f0000000f0				
1	1	0x000000f0000000d0				

Table 14. Involved master-keys in the 21-round key-recovery attack on `GIFT`-64 of the 13-round multiple differential distinguisher. The keys in blue represent the bits that do not repeat the guess.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
RK_1	$k_1^{15}k_0^{15}$	$k_1^{14}k_0^{14}$	$k_1^{13}k_0^{13}$	$k_1^{12}k_0^{12}$	$k_1^{11}k_0^{11}$	$k_1^{10}k_0^{10}$	$k_1^9k_0^9$	$k_1^8k_0^8$	$k_1^7k_0^7$	$k_1^6k_0^6$	$k_1^5k_0^5$	$k_1^4k_0^4$	$k_1^3k_0^3$	$k_1^2k_0^2$	$k_1^1k_0^1$	$k_1^0k_0^0$
RK_2									$k_3^7k_2^7$	$k_3^6k_2^6$	$k_3^5k_2^5$	$k_3^4k_2^4$				
RK_3																
RK'_{17}													$k_1^0k_0^4$		$k_1^8k_0^{12}$	
RK'_{18}			$k_3^{15}k_2^3$					$k_3^{14}k_2^2$				$k_3^{13}k_2^1$				$k_3^{12}k_2^0$
RK'_{19}	$k_5^3k_4^7$	$k_5^7k_4^{11}$	$k_5^{11}k_4^{15}$	$k_5^{15}k_4^3$	$k_5^2k_4^6$	$k_5^6k_4^{10}$	$k_5^{10}k_4^{14}$	$k_5^{14}k_4^2$	$k_5^1k_4^5$	$k_5^5k_4^9$	$k_5^9k_4^{13}$	$k_5^{13}k_4^1$	$k_5^0k_4^4$	$k_5^4k_4^8$	$k_5^8k_4^{12}$	$k_5^{12}k_4^0$
RK'_{20}	$k_7^3k_6^7$	$k_7^7k_6^{11}$	$k_7^{11}k_6^{15}$	$k_7^{15}k_6^3$	$k_7^2k_6^6$	$k_7^6k_6^{10}$	$k_7^{10}k_6^{14}$	$k_7^{14}k_6^2$	$k_7^1k_6^5$	$k_7^5k_6^9$	$k_7^9k_6^{13}$	$k_7^{13}k_6^1$	$k_7^0k_6^4$	$k_7^4k_6^8$	$k_7^8k_6^{12}$	$k_7^{12}k_6^0$
RK'_{21}	$k_1^5k_0^3$	$k_1^9k_0^7$	$k_1^{13}k_0^{11}$	$k_1^1k_0^{15}$	$k_1^4k_0^2$	$k_1^8k_0^6$	$k_1^{12}k_0^{10}$	$k_1^0k_0^{14}$	$k_1^3k_0^1$	$k_1^7k_0^5$	$k_1^{11}k_0^9$	$k_1^{15}k_0^{13}$	$k_1^2k_0^0$	$k_1^6k_0^4$	$k_1^{10}k_0^8$	$k_1^{14}k_0^{12}$

Table 15. Time complexity of the 21-round multiple differential attack on `GIFT-64` in each step.

Step	RK	# Key	Time(S-box operations)	Filtering probability	# Remaining pairs
1.	RK_1	2^{32}	$2 \times 2^n \times 2^3$	$2^{-3\times16}$	2^{n-48}
2.	RK_2	2^8	$2 \times 2^{32} \times 2^{n-48} \times 2^4$	$2^{-4\times4}$	2^{n-64}
3.	RK'_{21}	-	$2 \times 2^{40} \times 2^{n-64} \times 16$	-	2^{n-64}
4.	RK'_{20}	2^{32}	$2 \times 2^{40} \times 2^{n-64} \times 2^{32.41}$	-	2^{n-64}
5.	RK'_{19}	2^{32}	$2 \times 2^{72} \times 2^{n-64} \times 2^3$	$2^{-3\times16}$	2^{n-112}
6.	RK'_{18}	2^8	$2 \times 2^{104} \times 2^{n-112} \times 2^4$	$2^{-2\times4}$	2^{n-120}
7.	RK'_{17}	-	$2 \times 2^{112} \times 2^{n-120} \times 2^{0.08}$	$2^{-4\times2}$	2^{n-128}

we mount the 21-round multiple differential attack on `GIFT`-64 by adding three rounds before and five rounds after the distinguisher. The master-keys involved in the key-recovery attack are listed in Table 14. The time complexity of each step with initial 2^n pairs is listed in Table 15.

Complexity and Success Probability. For the right key guesses, there are about $2^{n-64-55.67}$ pairs left, while for the wrong key guesses, about $2^{n-128} \cdot 33$ pairs left. We set $n = 119.67$ to expect that at least one pair remains for the right key guesses, while about $2^{-3.28}$ pairs remain for the wrong key guesses. Therefore, the data complexity is about 2^{64} chosen-plaintexts, the time complexity is dominated by Step 5), and about $2^{131.67} \cdot \frac{1}{16} \cdot \frac{1}{21} \approx 2^{123.27}$ 21-round operations, the memory complexity is about 2^{112}-bit.

We use the following formula proposed by Blondeau et al. [7] to evaluate the success probability P_S:

$$P_S \approx 1 - G_*[G^{-1}(1 - \frac{l-1}{2^{n_k} - 2}) - \frac{1}{N_s}], \tag{20}$$

where n_k is the number of key candidates, l is the size of the list to keep, G is defined by $G^{-1}(y) = min\{x|G(x) \geq y\}$, and N_s is the number of samples. Please refer to [7] for more details of the functions G, G_*, and the analysis. For $n_k = 112$, $l = 2^{91}$, and $N_s = 2^{64}$, the success probability $P_S \approx 99.9\%$.

D   Differential Cryptanalysis of 27-Round `GIFT-128`

For the 20-round differentials (weak-key space and details are listed in Table 16) presented in Sect. 4.3 with probability $2^{-114.77}$ in the weak-key space W_3, which has input difference 0x00000000000000000000000 00000a0 and output difference 0x00000000000000002000000210000001, we launch the 27-round differential attack on `GIFT`-128. The master-keys involved in the key-recovery attack are listed in Table 17. The time complexity of each step with initial 2^n pairs is listed in Table 18. Suppose that there are 2^n pairs to perform the attack.

Complexity and Success Probability. For the right key guesses, there are about $2^{n-64-114.77}$ pairs left, while for the wrong key guesses, about $2^{n-64-128}$ pairs left. We set $n = 178.77$ to expect that at least one pair remains for the right key guesses, while about $2^{-13.23}$ pairs remain for the wrong key guesses. One structure contains 2^{64} plaintexts, and can generate 2^{127} pairs, thus, about $2^{178.77-127} = 2^{51.77}$ structures are required. Therefore, the data complexity is about $2^{51.77+64} = 2^{115.77}$ chosen-plaintexts, the time complexity is about $2^{120.61} \cdot \frac{1}{32} \cdot \frac{1}{27} \approx 2^{110.85}$ 27-round operations, the memory complexity is about 2^{92}-bit.

We use the formula in Eq. (19) to evaluate the success probability P_S. When S_N is very large, $P_S \approx \Phi(\sqrt{\mu})$. For $S_N = 2^{13.23}$, $\mu = pN = 2^{-114.77} \cdot 2^{178.77}$, P_S is about 99.9%.

E   Multiple Differential Attack on 28-Round `GIFT-128`

For the 21-round multiple differentials (2 differentials listed in Table 20) proposed in Sect. 4.3 with probability $2^{-122.77}$ in the weak-key space W_4, the 28-round key-

Table 16. The details of the 20-round differential of `GIFT-128` proposed in [26] (Table 7), differential 2. $\#\ t$ is the number of quasidifferential trails, and $\#\ valid\ t$ is the number of valid quasidifferential trails in the weak-key space W_3.

differential index	characteristic index	p_{avg}	$\#\ t$	$\#\ valid\ t$	p	weak-key space
	1	2^{-124}	256	256		
	2	2^{-124}	256	128		$k_0^9 + k_1^7 = 0$
	3	2^{-125}	512	128		$k_0^{11} + k_1^9 = 0$
2	4	2^{-125}	512	64	$2^{-114.77}$	$k_4^5 + k_5^1 = 0$
	5	2^{-125}	512	64		$k_6^9 + k_7^{11} = 0$
	6	2^{-125}	512	128		$k_6^{11} + k_7^{13} = 0$
	7	2^{-126}	1024	64		$k_2^{15} = 1$
	8	2^{-126}	1024	32		

Table 17. Involved mater-keys in the 27-round differential key-recovery attack on `GIFT` 128. The keys in blue represent the bits that will not repeat the guess.

RK_1	$k_5^{15}k_1^{15}$	$k_5^{14}k_1^{14}$	$k_5^{13}k_1^{13}$	$k_5^{12}k_1^{12}$	$k_5^{11}k_1^{11}$	$k_5^{10}k_1^{10}$	$k_5^9k_1^9$	$k_5^8k_1^8$	$k_5^7k_1^7$	$k_5^6k_1^6$	$k_5^5k_1^5$	$k_5^4k_1^4$	$k_5^3k_1^3$	$k_5^2k_1^2$	$k_5^1k_1^1$	$k_5^0k_1^0$
RK_2	$k_7^{15}k_3^{15}$	$k_7^{14}k_3^{14}$	$k_7^{13}k_3^{13}$	$k_7^{12}k_3^{12}$					$k_7^7k_3^7$	$k_7^6k_3^6$	$k_7^5k_3^5$	$k_7^4k_3^4$				
RK_3								$k_0^3k_4^7$		$k_0^1k_4^5$						
RK_4																
RK'_{25}	$k_5^7k_1^{15}$					$k_5^{14}k_0^2$ $k_5^5k_1^{13}$										$k_5^{12}k_0^0$
RK'_{26}			$k_7^{10}k_3^2$ $k_6^{14}k_3^{10}$ $k_6^6k_2^{14}$ $k_7^2k_2^6$ / $k_7^6k_3^{14}$ $k_6^{10}k_3^6$ $k_6^2k_2^{10}$ $k_7^{14}k_2^2$										$k_7^8k_3^0$ $k_6^{12}k_3^8$ $k_6^4k_2^{12}$ $k_7^0k_2^4$ / $k_7^4k_3^{12}$ $k_6^8k_3^4$ $k_6^0k_2^8$ $k_7^{12}k_2^0$			
RK'_{27}	$k_0^{11}k_5^{11}$ $k_0^7k_5^7$	$k_1^5k_4^7$ $k_1^1k_4^3$	$k_0^{10}k_5^{10}$ $k_0^6k_5^6$	$k_1^4k_4^6$ $k_1^0k_4^2$	$k_0^9k_5^9$ $k_0^5k_5^5$	$k_1^3k_4^5$ $k_1^{15}k_4^1$	$k_0^8k_5^8$ $k_0^4k_5^4$	$k_1^2k_4^4$ $k_1^{14}k_4^0$								

Table 18. The time complexity and filtering probability of the 20-round differential to attack 27-round `GIFT`-128 in each step with 2^n pairs.

Step	RK	# Key	Time(S-box operations)	Filtering probability	Remaining pairs
1.	RK_1	2^{32}	$2^{n-64+5.32}$	$2^{-3\times 2-2\times 14} = 2^{-34}$	2^{n-98}
2.	RK_2	2^{16}	$2^{n-64+1.99}$	$2^{-3\times 7-2} = 2^{-23}$	2^{n-121}
3.	RK_3	2^4	$2^{n-64-5.91}$	$2^{-4-3} = 2^{-7}$	2^{n-128}
4.	RK'_{27}	2^{14}	$2^{n-64-6.09}$	-	2^{n-128}
5.	RK'_{26}	2^{24}	$2^{n-64+3.73}$	$2^{-3\times 16} = 2^{-48}$	2^{n-176}
6.	RK'_{25}	2^2	$2^{n-64-20.9}$	$2^{-4\times 4} = 2^{-16}$	2^{n-192}

Table 19. The 18 21-round differentials of `GIFT`-128.

differential	Input difference	Output difference	Pr
1	0x000000000000000000000000000000a0	0x00000000000000002000000210000001	$2^{-128.64}$
2	0x000000000000000000000000000000a0	0x00000000000000000000002200000011	$2^{-128.64}$
3	0x000000000000000000000000000000a0	0x00000000000000000000004100000028	$2^{-128.59}$
4	0x000000000000000000000000000000a0	0x00000014000000820000000000000000	$2^{-128.59}$
5	0x00000000000000000000000000000a00	0x00000000000000000022000000110000	$2^{-128.64}$
6	0x00000000000000000000000000000a00	0x00000000000000000002200000011000	$2^{-128.64}$
7	0x00000000000000000000000000000a00	0x00044000000220000000000000000000	$2^{-129.64}$
8	0x00000000000000000000000000000a00	0x00000000000000008020000000100000	$2^{-130.75}$
9	0x00000000000000000000000000000a00	0x00140000008200000000000000000000	$2^{-128.59}$
10	0x00000000000000000000000000000a00	0x0050040000a020000000000000000000	$2^{-131.29}$
11	0x0000000000000000000000000a000000	0x00000000000000000000002200000011	$2^{-128.64}$
12	0x0000000000000000000000000a000000	0x00000000000000000000000408000002	$2^{-129.64}$
13	0x0000000000000000000000000a000000	0x00000000000000000000001008000080	$2^{-130.75}$
14	0x000000000000000000000000a0000000	0x00000000000000000022000000110000	$2^{-128.64}$
15	0x000000000000000000000000a0000000	0x00000000000000000020200000100100	$2^{-128.64}$
16	0x000000000000000000000000a0000000	0x00400400002002000000000000000000	$2^{-129.64}$
17	0x000000000000000000000000a0000000	0x00410000002800000000000000000000	$2^{-128.59}$
18	0x000000000000000000000000a0000000	0x00010400000802000000000000000000	$2^{-130.75}$

recovery attack on `GIFT`-128 is launched by adding four rounds before and three rounds after the distinguisher. The master-keys involved in the key-recovery attack are listed in Table 22 and Table 23. The time complexity of each step with initial 2^n pairs is listed in Table 24.

Complexity and Success Probability. For the right key guesses, there are about $2^{n-64-122.77}$ pairs left, while for the wrong key guesses, about $2^{n-64-128} \cdot 2$ pairs left. We set $n = 186.77$ to expect that at least one pair remains for the right key guesses, while about $2^{-4.23}$ pairs remain for the wrong key guesses. One structure contains 2^{64} plaintexts, and can generate 2^{127} pairs, thus, about $2^{186.77-127} = 2^{59.77}$ structures are required. Therefore, the data complexity is about $2^{59.77+64} = 2^{123.77}$ chosen-plaintexts, the time complexity is about $2^{128.07} \cdot \frac{1}{32} \cdot \frac{1}{28} \approx 2^{118.27}$ 28-round operations, the memory complexity is about 2^{96}-bit.

We use the formula in Eq. (20) to evaluate the success probability P_S. For $n_k = 96$, $l = 2^{91}$, and $N_s = 2^{123.77}$, the success probability $P_S \approx 86.5\%$.

Note that the time complexity of the attack is dominated by encrypting plaintexts, so the time complexity of guessing the key reduced by the weak-key space is negligible.

F   Differential Cryptanalysis of 17-Round `SUNDAE-GIFT`

For `SUNDAE-GIFT`-96, we target the initial phase without plaintext data in Fig. 3, and only one associated data block, which is the 96-bit nonce after padding. We observe that the initial block IV is a constant, therefore, the $E_K(IV)$ is determined by the K. We treat $E_K(IV)$ as a 128-bit whitening key based on

Table 20. The details of the two 21-round differentials of GIFT-128 in Table 19, differential 9 and 10, respectively. $\# t$ is the number of quasidifferential trails, and $\# valid\ t$ is the number of the valid quasidifferential trails in the weak-key space W_4.

differential index	characteristic index	p_{avg}	$\# t$	$\# valid\ t$	p	weak-key space
	1	2^{-130}	64	64		
	2	2^{-131}	128	32		
	3	2^{-131}	128	32		
	4	2^{-132}	256	16		
	5	2^{-133}	256	68		
9	6	2^{-134}	512	34	$2^{-123.11}$	
	7	2^{-134}	512	64		
	8	2^{-134}	512	34		$k_4^4 + k_5^0 = 0$
	9	2^{-135}	1024	32		$k_6^8 + k_7^{10} = 0$
	10	2^{-135}	1024	32		$k_6^{10} + k_7^{12} = 0$
	11	2^{-135}	1024	17		$k_2^1 = 1$
	1	2^{-133}	128	128		
	2	2^{-134}	128	64		
	3	2^{-134}	256	64		
10	4	2^{-134}	256	64	$2^{-125.04}$	
	5	2^{-135}	256	32		
	6	2^{-135}	256	32		
	7	2^{-135}	512	32		

Table 21. Two primary 21-round differential characteristics of `GIFT`-128. One is in differential 9 characteristic 1 with average probability 2^{-130}, the other is in differential 10 characteristic 1 with average probability 2^{-133} in Table 20, respectively.

r	ΔX_r of differential 9 characteristic 1	p_{avg}	ΔX_r of differential 10 characteristic 1	p_{avg}
1	0x0000000000000000000000000000000a00	2^{-0}	0x0000000000000000000000000000000a00	2^{-0}
2	0x0000000000000001000000000000000000	2^{-2}	0x0000000000000001000000000000000000	2^{-2}
3	0x0008000000000000000000000000000000	2^{-5}	0x0008000000000000000000000000000000	2^{-5}
4	0x0000000000000000200000010000000000	2^{-7}	0x0000000000000000200000010000000000	2^{-7}
5	0x0000040400000202000000000000000000	2^{-12}	0x0000040400000202000000000000000000	2^{-12}
6	0x0505000000000000505000000000000000	2^{-20}	0x0505000000000000505000000000000000	2^{-20}
7	0x000000000000000a000a00000000000000	2^{-32}	0x000000000000000a000a00000000000000	2^{-32}
8	0x0000000000000000000000110000000000	2^{-36}	0x0000000000000000000000110000000000	2^{-36}
9	0x0000000000000000000008000000000800	2^{-42}	0x0000000000000000000008000000000800	2^{-42}
10	0x0000020200000101000000000000000000	2^{-46}	0x0000020200000101000000000000000000	2^{-46}
11	0x0000000005050000000000000005050000	2^{-56}	0x0000000005050000000000000005050000	2^{-56}
12	0x000000000000000000a000a00000000000	2^{-68}	0x000000000000000000a000a00000000000	2^{-68}
13	0x0000011000000000000000000000000000	2^{-72}	0x0000011000000000000000000000000000	2^{-72}
14	0x0000000000000000080000000c000000	2^{-78}	0x0000000000000000080000000c000000	2^{-78}
15	0x0000020200000100000000000000000000	2^{-82}	0x0000020200000100000000000000000000	2^{-82}
16	0x050400000a0200000000000000000000	2^{-90}	0x050400000a0200000000000000000000	2^{-90}
17	0x0000000005050000000000000050100000	2^{-99}	0x0000000005050000000000000050100000	2^{-99}
18	0x0000000000a000a00000000000000000	2^{-111}	0x0000000000a000a00000000000000000	2^{-111}
19	0x0011000000000000000000000000000000	2^{-115}	0x0011000000000000000000000000000000	2^{-115}
20	0x00000000c000000060000000000000000	2^{-121}	0x80000000c0000000000000000000000000	2^{-121}
21	0x0000000000202000000000000000000000	2^{-125}	0x0000000002020000010000000000000000	2^{-125}
22	0x0014000000820000000000000000000000	2^{-130}	0x0050400000a020000000000000000000000	2^{-133}

Table 22. Involved keys in the 28-round multiple differential key-recovery attack on `GIFT`-128 of the 21-round differential 9 in Table 20.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16
RK_1	$k_5^{15}k_1^{15}$	$k_5^{14}k_1^{14}$	$k_5^{13}k_1^{13}$	$k_5^{12}k_1^{12}$	$k_5^{11}k_1^{11}$	$k_5^{10}k_1^{10}$	$k_5^9k_1^9$	$k_5^8k_1^8$	$k_5^7k_1^7$	$k_5^6k_1^6$	$k_5^5k_1^5$	$k_5^4k_1^4$	$k_5^3k_1^3$	$k_5^2k_1^2$	$k_5^1k_1^1$	$k_5^0k_1^0$
RK_2	$k_6^{15}k_2^{15}$	$k_6^{14}k_2^{14}$	$k_6^{13}k_2^{13}$	$k_6^{12}k_2^{12}$					$k_6^7k_2^7$	$k_6^6k_2^6$	$k_6^5k_2^5$	$k_6^4k_2^4$				
RK_3					$k_0^7k_4^{11}$		$k_0^5k_4^9$									
RK_4																
RK'_{26}			$k_7^9k_3^9$	$k_7^8k_3^8$								$k_7^1k_3^1$	$k_7^0k_3^0$			
RK'_{27}	$k_1^{13}k_5^{11}$		$k_1^{11}k_5^9$						$k_1^5k_5^3$	$k_1^3k_5^1$						
	$k_0^3k_4^7$		$k_0^1k_4^5$						$k_0^{11}k_4^{15}$	$k_0^9k_4^{13}$						
RK'_{28}	$k_3^{13}k_7^{11}$		$k_3^{11}k_7^9$		$k_3^9k_7^7$		$k_3^7k_7^5$		$k_3^5k_7^3$		$k_3^3k_7^1$		$k_3^1k_7^{15}$		$k_3^{15}k_7^{13}$	
	$k_2^3k_6^7$		$k_2^1k_6^5$		$k_2^{15}k_6^3$		$k_2^{13}k_6^1$		$k_2^{11}k_6^{15}$		$k_2^9k_6^{13}$		$k_2^7k_6^{11}$		$k_2^5k_6^9$	

Table 23. Involved keys in the 28-round differential key recovery attack on GIFT-128 of the 21-round differential 10 in Table 20.

RK																
RK_1	$k_5^{15}k_1^{15}$	$k_5^{14}k_1^{14}$	$k_5^{13}k_1^{13}$	$k_5^{12}k_1^{12}$	$k_5^{11}k_1^{11}$	$k_5^{10}k_1^{10}$	$k_5^9k_1^9$	$k_5^8k_1^8$	$k_5^7k_1^7$	$k_5^6k_1^6$	$k_5^5k_1^5$	$k_5^4k_1^4$	$k_5^3k_1^3$	$k_5^2k_1^2$	$k_5^1k_1^1$	$k_5^0k_1^0$
RK_2	$k_6^{15}k_2^{15}$	$k_6^{14}k_2^{14}$	$k_6^{13}k_2^{13}$	$k_6^{12}k_2^{12}$					$k_6^7k_2^7$	$k_6^6k_2^6$	$k_6^5k_2^5$	$k_6^4k_2^4$				
RK_3				$k_0^7k_4^{11}$		$k_0^5k_4^9$										
RK_4																
RK'_{26}			$k_7^9k_3^9$		$k_7^7k_3^7$						$k_7^1k_3^1$		$k_7^{15}k_3^{15}$			
RK'_{27}	$k_1^{13}k_5^{11}$	$k_1^{12}k_5^{10}$	$k_1^{11}k_5^9$	$k_1^{10}k_5^8$					$k_1^5k_5^3$	$k_1^4k_5^2$	$k_1^3k_5^1$	$k_1^2k_5^0$				
	$k_0^3k_4^7$	$k_0^2k_4^6$	$k_0^1k_4^5$	$k_0^0k_4^4$					$k_0^{11}k_4^{15}$	$k_0^{10}k_4^{14}$	$k_0^9k_4^{13}$	$k_0^8k_4^{12}$				
RK'_{28}	$k_3^{13}k_7^{11}$		$k_3^{11}k_7^9$		$k_3^9k_7^7$		$k_3^7k_7^5$		$k_3^5k_7^3$		$k_3^3k_7^1$		$k_3^1k_7^{15}$		$k_3^{15}k_7^{13}$	
	$k_2^3k_6^7$		$k_2^1k_6^5$		$k_2^{15}k_6^3$		$k_2^{13}k_6^1$		$k_2^{11}k_6^{15}$		$k_2^9k_6^{13}$		$k_2^7k_6^{11}$		$k_2^5k_6^9$	

Table 24. The time complexity and filtering probability of 21-round differential to attack 28-round GIFT-128 in each step with 2^n pairs.

Step	RK	# Key	Time(S-box operations)	Filtering probability	Remaining pairs
1.	RK_1	2^{32}	$2^{n-64+5.3}$	$2^{-2\times3-14\times2}=2^{-34}$	2^{n-34}
2.	RK_2	2^{16}	$2^{n-64-1.95}$	$2^{-7\times3-6-4\times3-8\times2}=2^{-55}$	2^{n-89}
	RK'_{28}	2^{24}			
3.	RK_3	2^4	$2^{n-64-13.68}$	$2^{-4-3-5\times2-3\times3}=2^{-26}$	2^{n-115}
	RK'_{27}	2^8			
4.	RK_4	-	$2^{n-64-26.68}$	$2^{-4-2-3-4}=2^{-13}$	2^{n-128}
	RK'_{26}	2^4			

Table 25. Two 11-round differential characteristics of `SUNDAE-GIFT`.

r	ΔX_r in differential characteristic 1	p	ΔX_r in differential characteristic 2	p
1	0x00000000000000000000000000000a00	2^{-0}	0x00000000000000000000000000000e00	2^{-0}
2	0x00000000000000010000000000000000	2^{-2}	0x00000000000000010000000000000000	2^{-2}
3	0x00080000000000000000000000000000	2^{-5}	0x00080000000000000000000000000000	2^{-5}
4	0x00000000000000002000000010000000	2^{-7}	0x00000000000000002000000010000000	2^{-7}
5	0x00004040000020200000000000000000	2^{-12}	0x00004040000020200000000000000000	2^{-12}
6	0x05050000000000000505000000000000	2^{-20}	0x05050000000000000505000000000000	2^{-20}
7	0x0000000000000000a000a00000000000	2^{-32}	0x0000000000000000a000a00000000000	2^{-32}
8	0x00000000000000000000110000000000	2^{-36}	0x00000000000000000000110000000000	2^{-36}
9	0x00000060000000000000090000000000	2^{-42}	0x00000060000000000000090000000000	2^{-42}
10	0x02000000000001000000000000000000	2^{-47}	0x02000000000001000000000000000000	2^{-47}
11	0x00000000010000000008000040000000	2^{-52}	0x00000000010000000008000040000000	2^{-52}
12	0x00000000000000000000201000801080	2^{-60}	0x00000000000000000000201000801080	2^{-60}

Fig. 3. `SUNDAE-GIFT` encryption without plaintext data.
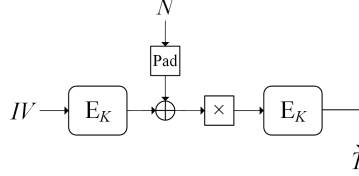
the structure that there is no whitening key at the beginning of `GIFT`, and write it as IK. In addition, the multiplication "$\times$" is a linear operation, the order of operation "$\times$" and $(pad(N) \oplus IK)$ can be swapped, we have $\times(pad(N) \oplus IK) = \times(pad(N)) \oplus \times(IK))$, where $pad(N)$ is a 128-bit state after padding, i.e., $pad(N) = N||0^{32}$. The $\times(pad(N))$ and $\times(IK)$ are denoted by $G(N)$ and IK', respectively.

According to the differential attack in Fig. 4. The structures are constructed in $G(N)$ by choosing nonce. One structure has a 64-bit traversal value and 64-bit constant and can generate about 2^{127} pairs. Before performing the subsequent key recovery, the partial value of the IK' needs to be recovered. For a 4-bit S-box, we make a precomputation table to record solutions by traversing all input pairs with given input difference and output difference. The 4-bit IK' corresponding to an S-box can be squeezed out by precomputation-table lookup. For the `GIFT`'s 4-bit S-box, the average number of solutions is $\frac{78 \times 2 + 18 \times 4 + 2 \times 6}{78 + 18 + 2} \approx 2.4$ according to the difference distribution table (DDT). As a result, there are about $2.4^{16} \approx 2^{20.16}$ possible values for the $IK'[127 \sim 64]$. After that, the key recovery attack can be performed by guessing key and filtering pairs for each possible value of $IK'[127 \sim 64]$, and the procedure is similar to the 21-round differential attack on `GIFT`-64, which is omitted.

Table 26. Involved keys in the 17-round differential key-recovery attack on `SUNDAE-GIFT` of the 11-round differential characteristic 1 in Table 25. The keys in blue represent the bits that do not repeat the guess.

RK_1	$k_4^{15}k_0^{15}$ $k_4^{14}k_0^{14}$ $k_4^{13}k_0^{13}$ $k_4^{12}k_0^{12}$				$k_4^7k_0^7$ $k_4^6k_0^6$ $k_4^5k_0^5$ $k_4^4k_0^4$			
RK_2		$k_7^{10}k_3^{10}$		$k_7^8k_3^8$				
RK_3								
RK'_{15}		$k_1^2k_5^8$	$k_0^{10}k_4^6$		$k_0^9k_4^5$	$k_1^0k_5^6$	$k_0^8k_4^4$	
RK'_{16}			$k_2^6k_7^4$ $k_2^{14}k_6^{10}$ $k_3^{14}k_6^2$				$k_2^4k_7^2$ $k_2^{12}k_6^8$ $k_3^{12}k_6^0$	
			$k_2^2k_7^0$ $k_2^{10}k_6^6$ $k_3^{10}k_6^{14}$				$k_2^0k_7^{14}$ $k_2^8k_6^4$ $k_3^8k_6^{12}$	
RK'_{17}	$k_4^7k_1^7$	$k_5^{15}k_0^{15}$	$k_4^6k_1^6$	$k_5^{14}k_0^{14}$	$k_4^5k_1^5$	$k_5^{13}k_0^{13}$	$k_4^4k_1^4$	$k_5^{12}k_0^{12}$
	$k_4^3k_1^3$	$k_5^{11}k_0^{11}$	$k_4^2k_1^2$	$k_5^{10}k_0^{10}$	$k_4^1k_1^1$	$k_5^9k_0^9$	$k_4^0k_1^0$	$k_5^8k_0^8$

Table 27. The time complexity and filtering probability of the 11-round differential characteristic to attack 17-round `SUNDAE-GIFT` in each step with 2^{n-64} pairs. The 64-bit IK' in step 1. yields about $2^{20.16}$ possible values.

Step	RK	# Key	Time(S-box operations)	Filtering probability	Remaining pairs
1.	K'	2^{64}	$2^{n-64+20.16}$	-	2^{n-64}
2.	RK_1	2^{16}	$2^{n-64+24.16}$	$2^{-7\times3-2}=2^{-23}$	2^{n-87}
3.	RK_2	2^4	$2^{n-64+16.48}$	$2^{-4-3}=2^{-7}$	2^{n-94}
4.	RK'_{17}	2^8	$2^{n-64+15.16}$	$2^{-8\times1}=2^{-8}$	2^{n-102}
		2^{16}	$2^{n-64+21.16}$	$2^{-8\times1}=2^{-8}$	2^{n-110}
5.	RK'_{16}	2^{22}	$2^{n-64+20.89}$	$2^{-4\times2-3\times4-2\times6}=2^{-32}$	2^{n-142}
6.	RK'_{15}	2^1	$2^{n-64+9.25}$	$2^{-4\times3-2\times2}=2^{-16}$	2^{n-158}

The keys involved in the key recovery attack are listed in Table 26. Suppose that there are 2^n pairs to perform the attack. The time complexity details of each step with 2^{n-64} pairs satisfying the pattern of 64 inactive bits in ΔT are listed in Table 27.

Complexity and Success Probability. For the right key guesses, there are about $2^{n-64-60} = 2^{n-124}$ pairs will be left, while for the wrong key guesses, about $2^{n-64-94} = 2^{n-158}$ pairs will be left. We set $n = 124$, that is, about $2^{62.5}$ nonce are required. Thus, the data complexity is about $2^{62.5}$ chosen-nonces, the time complexity is about $2^{84.46}\cdot\frac{1}{32}\cdot\frac{1}{17} \approx 2^{75.37}$ 17-round encryptions, and the memory complexity is about 2^{66}-bit.

We use the formula in Eq. (19) to evaluate the success probability P_S. When S_N is very large, $P_S \approx \Phi(\sqrt{\mu})$. For $S_N = 2^{43}$, $\mu = pN = 2^{-60}\cdot 2^{124}$, P_S is about 99.9%.

Fig. 4. 17-round differential attack on `SUNDAE-GIFT`.