A Linearisation Method for Identifying Dependencies in Differential Characteristics

Examining the Intersection of Deterministic Linear Relations and Nonlinear Constraints

Ling Sun

[1] Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University, Jinan, China
[2] School of Cyber Science and Technology, Shandong University, Qingdao, China
[3] Quan Cheng Shandong Laboratory, Jinan, China
lingsun@sdu.edu.cn

Abstract. The analytical perspective employed in the study classifies the theoretical research on dependencies in differential characteristics into two types. By categorising all dependence representations from the value restrictions and the theory of quasidifferential trails, we pinpoint a specific set of nonlinear constraints, which we term linearised nonlinear constraints. We aim to establish a method that utilises value restrictions to identify these constraints, as the current method based on value restrictions is found to be lacking in this area. A linearisation method for searching linearised nonlinear constraints for a given differential characteristic is developed by leveraging linear dependencies between inputs and outputs of active S-boxes. Then, we propose a three-stage evaluation approach to more accurately evaluate differential characteristics with linearised nonlinear constraints. Four differential characteristics of GIFT-64 are analysed using the three-stage evaluation approach, and the exact right key spaces and remaining probabilities are given. According to our results, the right key spaces of the four differential characteristics do not cover the entire key space, and the remaining probabilities are not equivalent to the stated probabilities. Concerning GIFT-128, we find six differential characteristics subject to linearised nonlinear constraints. Besides, inconsistencies are detected in the linear and linearised nonlinear constraints in the characteristics of two differentials employed to initiate the most effective differential attack on GIFT-128. Based on these results, we strongly advise reassessing the differential attacks that rely on these distinguishers. An additional advantage of using the linearisation method and the three-stage evaluation approach is their ability to identify linear and nonlinear constraints in ciphers that utilise the Generalised Feistel Network (GFN). It leads to the first instantiations of linear and nonlinear constraints in the GFN cipher WARP.

Keywords: Differential cryptanalysis · Differential characteristic · Dependency · Linearisation.

1 Introduction

In modern cryptography, differential cryptanalysis is a critical cryptanalytic method initially introduced by Biham and Shamir [8]. In order to facilitate the analysis, it was assumed that all round keys generated by the master key are independent. One can determine the probability of an r-round differential characteristic by multiplying the probabilities of r 1-round differential characteristics. Later, this assumption is incorporated into the Markov cipher theory [23], which serves as a foundational theory for differential cryptanalysis. The target cipher in the differential attack is typically assumed to be a Markov cipher in nearly all later research on differential cryptanalysis.

According to our knowledge, Daemen and Rijmen conducted the initial investigation on the probabilities of the differential characteristic over fixed-keys [17]. They showed that the probability of a differential characteristic over various fixed-keys varied and adhered to a specific distribution for key-alternating ciphers. At nearly the same time, they [16] introduced the concept of plateau characteristics, which are differential characteristics with a probability of either zero or a nonzero constant when the key is fixed at varying values. Their research demonstrates that the probability of the differential characteristic is strongly linked to the key value employed in the cipher. Assuming the independence of round keys can result in errors in cryptanalysis. Consequently, this led to the development of studies on the dependencies in differential characteristics.

The analytical perspective employed in the study can determine the classification of theoretical research on dependencies in differential characteristics. Most previous research [16,27,12,43,26,29] has focused on the value restrictions placed on intermediate cipher states. The exceptional study completed by Beyne and Rijmen [7], which concentrates on the theoretical foundations of differential cryptanalysis, has significantly advanced our understanding of the dependencies.

Despite the divergent perspectives, both explanatory frameworks for dependencies in differential characteristics possess inherent merit. The direct nature of value restrictions on intermediate states leads to the creation of highly obvious linear and nonlinear constraints, facilitating a reasonably straightforward comprehension of these constraints. On the other hand, quasidifferential trails provide profound insight into the fundamental principles of dependencies, and the use of quasidifferential trails enables an extensive and in-depth description of dependencies inside differential characteristics.

By categorising all dependence representations from the value restrictions and the theory of quasidifferential trails, we pinpoint a specific set of nonlinear constraints, which we term *linearised nonlinear constraints*. We aim to establish a method that utilises value restrictions to identify these linearised nonlinear constraints, as the current method based on value restrictions is lacking in this area.

Our Contributions

This study focuses on the linearised nonlinear constraints, which are inherently nonlinear but expressed as linear equations. The findings can be summarised as follows.

Linearisation method for finding linearised nonlinear constraints. We provide theoretical proof that linear dependency between the inputs and outputs of active S-boxes is not rare but rather a regular phenomenon that happens in S-boxes with a differential uniformity of four. Given the differential characteristic of a cryptographic primitive with S-boxes having a differential uniformity of four, we can generate a system of equations that encompasses all internal states and round keys based on the linearisation method. The linearised nonlinear constraints in the given differential characteristics can be obtained by performing Gaussian elimination on these equations. This method enables us to identify a linearised nonlinear constraint for `GIFT-64` [4] that spans eight rounds.

Three-stage evaluation approach for differential characteristics. To achieve a more precise evaluation of the right key space and the remaining probability of differential characteristics that contain linearised nonlinear constraints, a three-stage evaluation approach is proposed. The framework proposed in [33] is employed in the final two stages of the approach, and we introduce three modifications to it to detect potential constraints not identified by the linearisation method. Furthermore, the updated framework allows us to utilise an automatic method to mimic statistical tests, which is a valuable addition to applying automatic methods in cryptanalysis. Our study demonstrates that a simulated statistical test for `GIFT-64`, utilising 2^{57} pairs of plaintexts, can be completed in an average of 158.97 hours. It is considerably more efficient than the conventional statistical test.

Accurate assessment of four differential characteristics for `GIFT-64`. The three-stage evaluation approach is used to analyse four differential characteristics of `GIFT-64` in [48,14,13,41] that have linearised nonlinear constraints. In these characteristics, the longest linearised nonlinear constraint reaches eight rounds. The precise right key spaces and remaining probabilities of these differential characteristics are provided. Our findings indicate that the right key spaces of the four differential characteristics do not cover the entire key space, and the remaining probabilities are not equivalent to the stated probabilities. Thus, we recommend reevaluating the differential attacks that depend on these distinguishers.

Inconsistencies in two differentials for `GIFT-128`. For `GIFT-128`, we found that six out of the eighteen differential characteristics reported in [51,13,25,24,22,52] contain linearised nonlinear constraints. The constraints of the six differential characteristics are explored. Among the six characteristics, the three 20-round differential characteristics proposed by Ji *et al.* [22] are included in the same differential. In [22], this differential is employed to launch a 26-round differential attack against GIFT-128. Our study shows that although the linear constraints of the three differential characteristics are identical, their linearised nonlinear constraints vary. Two 20-round differential characteristics presented by Zong *et al.* [52] also exhibit similar issues. Consequently, it is imperative to carefully reconsider the validity of the differential attack in light of these differentials.

Linear and nonlinear constraints in WARP. Unlike the straightforward approach to locating linear constraints in ciphers that use the Substitution Permutation Network (SPN), detecting linear constraints based on value restrictions in ciphers that employ the Generalised Feistel Network (GFN) is more challenging. Thus, the previous studies based on the value restriction to find linear constraints [16,27,12,43,26] do not concern primitives that utilise the GFN structure. The proposed linearisation method is appropriate for determining linear constraints in GFN ciphers. An instantiation of the linear constraints in GFN ciphers is obtained by applying this method to the differential characteristics of WARP [3]. Additionally, we supply the first instantiation of the nonlinear constraint in GFN ciphers by applying the three-stage evaluation approach.

It is acknowledged that the constraints identified by our methodology can also be determined using the theory of quasidifferential trails [7]. However, because the search for quasidifferential trails is based on mathematical problem solvers, its application to primitives with 8-bit S-boxes may be challenging. Conversely, the linearisation method remains effective for 8-bit S-boxes with a differential uniformity of four. Additionally, the linearisation method and the three-stage evaluation approach possess some additional value, which is elaborated upon in Section 8.

Outline. Section 2 provides an overview of differential cryptanalysis and introduces GIFT, one of the target ciphers, and Section 3 reviews earlier studies on dependencies in differentiable characteristics. In Section 4, we show the newly identified type of nonlinear constraints and describe the linearisation method that enables the detection of these constraints. Section 5 provides a three-stage evaluation approach, which includes the linearisation method and allows for a more precise assessment of the given differential characteristics. The differential characteristics of GIFT are investigated using the three-stage evaluation approach in Section 6. Section 7 considers the differential characteristics of other primitives. Finally, we make a discussion and conclude the paper in Section 8.

2 Preliminaries

This section commences with an overview of the fundamentals of differential cryptanalysis. Then, we describe the general framework of GIFT.

2.1 Differential Cryptanalysis

Differential cryptanalysis [8] looks at how differences spread across a cryptographic function and is predicated on the high likelihood of a particular output difference Δ_{out} occurring given a fixed input difference Δ_{in}. For an n-bit iterated block cipher with vectorial Boolean functions $F_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$ as the round functions ($0 \leqslant i < r$), such an advantageous differential propagation may be discovered round by round. An r-round *differential characteristic* is defined as an $(r+1)$-tuple ($\Delta_{in} = \Delta_0, \Delta_1, \dots, \Delta_r = \Delta_{out}$), where Δ_i represents the n-bit difference after i-round of encryption for every $0 \leqslant i \leqslant r$. A *right pair* is an input pair that satisfies the r-round differential characteristic.

S-boxes are frequently employed components in the construction of iterated block ciphers. The *difference distribution table* (DDT), a $2^s \times 2^s$ table for an s-bit S-box, is used to study the differential characteristics of the S-box. The DDT saves the number of right pairs for the differential characteristic (i, j) of the S-box in the i-th row and the j-th column. The greatest number in the DDT other than the one for trivial propagation $(0, 0)$ is the *differential uniformity* [28] of the S-box.

To simplify the analysis, we commonly assume that the target cipher is a Markov cipher [23]. The differential probability of the r-round differential characteristic may be estimated as

$$\Pr\left(\Delta_0, \Delta_1, \dots, \Delta_r\right) = \prod_{i=0}^{r-1} \Pr\left(\Delta_i, \Delta_{i+1}\right), \tag{1}$$

whereas the probability $\Pr\left(\Delta_i, \Delta_{i+1}\right)$ can be determined by

$$\Pr\left(\Delta_i, \Delta_{i+1}\right) = \frac{\#\{x \in \mathbb{F}_2^n \mid F_i(x) \oplus F_i(x \oplus \Delta_i) = \Delta_{i+1}\}}{2^n}.$$

In essence, using the formula (1) means evaluating the differential propagation across the round functions independently, ignoring the dependencies among different rounds and the dependencies of differential characteristics on the round keys involved.

An r-round *differential* $(\Delta_{in}, \Delta_{out})$ consists of all r-round differential characteristics having the same input and output differences. The probability of the differential is computed as

$$\Pr\left(\Delta_{in}, \Delta_{out}\right) = \sum_{\Delta_1, \Delta_2, \dots, \Delta_{r-1} \in \mathbb{F}_2^n} \Pr\left(\Delta_{in}, \Delta_1, \dots, \Delta_{r-1}, \Delta_{out}\right). \tag{2}$$

The formula (2) is always true. However, when estimating the probability of each differential characteristic, $\Pr\left(\Delta_{in}, \Delta_1, \dots, \Delta_{r-1}, \Delta_{out}\right)$, under the Markov cipher assumption, this assumption also indirectly impacts $\Pr\left(\Delta_{in}, \Delta_{out}\right)$.

2.2 Description of `GIFT`

`GIFT` [4] is a lightweight block cipher that uses the Substitution Permutation Network (SPN). It is available in two versions: `GIFT-64`, which has 28 rounds, and `GIFT-128`, which has 40 rounds.

The cipher operates on a plaintext $b_0\|b_1\|\cdots\|b_{n-1}$ of n bits, where n might be 64 or 128. The cipher additionally receives a 128-bit key as the key state, $K = k[0]\|k[1]\|\cdots\|k[7]$, where $k[i] = k_{16i}\|k_{16i+1}\|\cdots\|k_{16i+15}$ is a 16-bit word for all $0 \leqslant i \leqslant 7$. The GIFT encryption algorithm consists of three processes in each round: **SubCells**, **PermBits**, and **AddRoundKey**.

SubCells The cipher utilises the invertible 4-bit S-box GS from Table 1. The S-box is applied to each nibble of the cipher state.

PermBits The bit permutation in GIFT employs a method known as Bad Output must go to Good Input (BOGI) to address the issue of single active bit transitions across numerous successive rounds in differential and linear characteristics. It transfers bits from bit location i of the cipher state to bit position $P_n(i)$ for all $0 \leqslant i \leqslant n$. Appendix A specifies the bit permutations used in GIFT-64 and GIFT-128.

AddRoundKey This stage entails incorporating the round key and round constants. In the r-th round, an $n/2$-bit round key is generated from the key state, and it is further divided into two s-bit words: $rk^r = U^r\|V^r = u_0^r\|u_1^r\|\cdots\|u_{s-1}^r\|v_0^r\|v_1^r\|\cdots\|v_{s-1}^r$, where $s = 16$ and 32 for GIFT-64 and GIFT-128, respectively.

The combination of U^r and V^r with the cipher state in GIFT-64 is done as

$$b_{4i+2} \leftarrow b_{4i+2} \oplus u_i^r, \quad b_{4i+3} \leftarrow b_{4i+3} \oplus v_i^r, \quad 0 \leqslant i \leqslant 15.$$

In GIFT-128, U^r and V^r are involved in the following manner:

$$b_{4i+1} \leftarrow b_{4i+1} \oplus u_i^r, \quad b_{4i+2} \leftarrow b_{4i+2} \oplus v_i^r, \quad 0 \leqslant i \leqslant 31.$$

Afterwards, XOR operations are performed using round constants. A single bit "1" and a 6-bit round constant $C^r = c_0^r\|c_1^r\|c_2^r\|c_3^r\|c_4^r\|c_5^r$ are XORed into the cipher state at bit positions 0, $n-24$, $n-20$, $n-16$, $n-12$, $n-8$, and $n-4$ for both GIFT versions.

$$\begin{aligned}
&b_0 \leftarrow b_0 \oplus 1,\\
&b_{n-24} \leftarrow b_{n-24} \oplus c_0^r,\ \ b_{n-20} \leftarrow b_{n-20} \oplus c_1^r,\ \ b_{n-16} \leftarrow b_{n-16} \oplus c_2^r,\\
&b_{n-12} \leftarrow b_{n-12} \oplus c_3^r,\ \ b_{n-8} \leftarrow b_{n-8} \oplus c_4^r,\ \ \ \ b_{n-4} \leftarrow b_{n-4} \oplus c_5^r.
\end{aligned}$$

Figure 1 is an illustration of the GIFT-64 round function.

Table 1. Specification of GS in hexadecimal notation.

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

Key schedule Both versions of GIFT follow the same key schedule, with the only difference being the method of extracting the round key. Before the key state update, a round key is first derived from the key state.

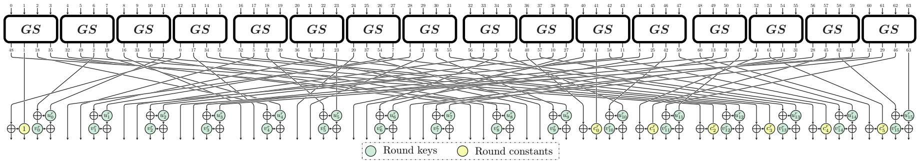


Fig. 1. Round function of `GIFT-64`.

- ▶ The round key rk^r for `GIFT-64` is obtained by extracting two 16-bit words $k[6]$ and $k[7]$ from the key state, which are then concatenated as $rk^r = k[6]\|k[7]$.
- ▶ The round key rk^r for `GIFT-128` is obtained by extracting four 16-bit words $k[2]$, $k[3]$, $k[6]$, and $k[7]$ from the key state, which are then concatenated as $rk^r = k[2]\|k[3]\|k[6]\|k[7]$.

The key state is subsequently modified to

$$k[0]\|k[1]\|\cdots\|k[7] \leftarrow (k[6] \ggg 2)\,\|\,(k[7] \ggg 12)\,\|k[0]\|\cdots\|k[5],$$

where "$\ggg i$" represents a right rotation of i bits inside a 16-bit word.

Round constants Both versions of `GIFT` use identical round constants. An affine 6-bit Linear Feedback Shift Register (LFSR) is used to create the round constants. The six bits of the state $(c_0^{-1}, c_1^{-1}, c_2^{-1}, c_3^{-1}, c_4^{-1}, c_5^{-1})$ are set to zero at the beginning. The state is updated as

$$(c_0^r, c_1^r, c_2^r, c_3^r, c_4^r, c_5^r) \leftarrow (c_1^{r-1}, c_2^{r-1}, c_3^{r-1}, c_4^{r-1}, c_5^{r-1}, c_0^{r-1} \oplus c_1^{r-1} \oplus 1)$$

prior to being utilised in a particular round.

3 Dependencies in Differential Characteristics

The classification of theoretical research on dependencies in differential characteristics can be determined by the analytical perspective employed in the study. The majority of previous research [16,27,12,43,26,29] has focused on the value restrictions placed on intermediate cipher states. In contrast, the unique study by Beyne and Rijmen [7] takes a different approach, concentrating on the theoretical foundations of differential cryptanalysis. This novel perspective effectively captures the essence of the dependencies.

3.1 Dependencies Explained by Value Restrictions

Considering a general round function, we can break it into three parts (as seen in Figure 2): a nonlinear part S, a linear portion L, and a key addition operation. In order to achieve the propagations for S in the specified differential characteristic $(\Delta_0, \Delta_1, \ldots, \Delta_r)$, the input x^i and output y^i of S are limited to subsets of $\mathbb{F}_2^n$ for all $0 \leqslant i < r$. The sets of possible values for x^i and y^i are denoted as $\mathcal{X}^i$ and $\mathcal{Y}^i$, respectively. Daemen and Rijmen [16] have demonstrated that if a differential propagation contains precisely two or four right pairs, the sets of possible input and output values for that differential propagation form affine subspaces. Therefore, if S consists of the parallel application of 4-bit S-boxes, it is probable that $\mathcal{X}^i$ and $\mathcal{Y}^i$ are affine subspaces of $\mathbb{F}_2^n$. The reason is that most commonly seen 4-bit S-boxes have a differential uniformity of 4.

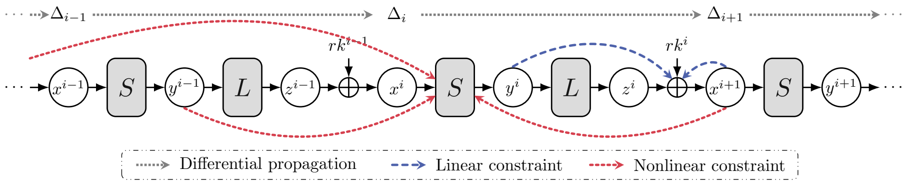


Fig. 2. Illustration for value restrictions in differential characteristics.

Dependencies in differential characteristics arise when compatibility between $\mathcal{X}^i$ and $\mathcal{Y}^i$ is considered. Previous research indicates that the dependencies, explained by value restrictions, can lead to two distinct types of constraints on round keys and round constants, contingent upon incorporating nonlinear components S.

Linear Constraint To guarantee the presence of right pairs in the differential characteristic, the first kind of constraint, as seen in Figure 2, requires that the round key rk^i is a member of the set $L(\mathcal{Y}^i) \oplus \mathcal{X}^{i+1} = \{L(y^i) \oplus x^{i+1} \mid y^i \in \mathcal{Y}^i, x^{i+1} \in \mathcal{X}^{i+1}\}$ for all $0 \leqslant i \leqslant r-1$. This particular constraint is commonly referred to as a *linear constraint* due to its lack of exact involvement of the nonlinear component S. Most earlier studies [16,27,12,43,26] discuss constraints of this type. When $\mathcal{X}^i$ and $\mathcal{Y}^i$ are affine spaces, it is possible to transform the constraints imposed on them into linear equations. Gaussian elimination can be used to find linear constraints.

Nonlinear Constraint Peyrin and Tan [29] are the first to suggest the second type of constraint, which varies from the first in that it involves keys from many rounds. As an example of the nonlinear constraint in Figure 2, the round keys rk^{i-1} and rk^i shall confirm that at least one pair of x and y fulfils $S(x) = y$, where $x \in L(\mathcal{Y}^{i-1}) \oplus rk^{i-1}$ and $y \in L^{-1}(\mathcal{X}^{i+1} \oplus rk^i)$. *Nonlinear constraints* are referred to as such due to the necessity of including nonlinear components S to depict the constraint accurately. The nonlinear constraint can extend beyond a single intermediate round and potentially encompass numerous S-boxes inside the same round. For example, one further nonlinear constraint in Figure 2 may be that when x takes values from set $L(S(L(\mathcal{Y}^{i-2}) \oplus rk^{i-2})) \oplus rk^{i-1}$, and y takes values from set $L^{-1}(\mathcal{X}^{i+1} \oplus rk^i)$, the round keys rk^{i-2}, rk^{i-1}, and rk^i must verify that at least one pair of x and y fulfils $S(x) = y$.

According to Peyrin and Tan's findings [29], the analysis of nonlinear constraints that involve inactive S-boxes is highly complex. Different techniques are used for the two primitives, SKINNY [6] and GIFT [4], that are analysed in their study. The method employed for SKINNY initially locates the position of nonlinear constraints using a top-bottom technique (refer to Algorithm 1 of [29]). Following that, a meticulous examination is carried out on possible round keys and their respective probabilities.

Because of the significant computational expense, the search area for nonlinear constraints in GIFT is limited to three consecutive rounds. Because the key schedule requires GIFT-64 to reuse the same 32 key bits as the round key every four rounds, they divide the rounds into four batches and look for nonlinear constraints in these batches independently, ignoring the 32 key bits that overlap from different batches. The values involved in the t-th batch ($t = 0, 1, 2, 3$) are as follows.

- The output values of the S-boxes in rounds t, $t + 4$, $t + 8$, and so on.
- The inactive S-boxes in rounds $t + 1$, $t + 5$, $t + 9$, and so on.
- The input values of the S-boxes in rounds $t + 2$, $t + 6$, $t + 10$, and so on.

Peyrin and Tan use a framework based on the mathematical problem solver CryptoMiniSat [38] to verify the existence of round keys that prevent the output values of the j-th round from propagating from the inactive S-boxes in the $(j + 1)$-th round to the input values of the S-boxes in the $(j + 2)$-th round. This scenario suggests the presence of a nonlinear constraint in the differential characteristic of the round keys. The batch approach is unsuitable for GIFT-128 due to the large number of key bits involved. The search space for nonlinear constraints in GIFT-128 is limited to each set of three successive rounds separately. Unfortunately, the current batch-based verification technique on GIFT-64 cannot detect nonlinear constraints that extend beyond three rounds.

Peyrin and Tan [29] suggest that when only a subset of keys is possible for the differential characteristics, the most effective way to present the probability of a characteristic is to separately describe the following two pieces of information.

- The dimension of the right key space, which just considers linear constraints without accounting for nonlinear ones.
- The remaining probability of the characteristic that is not influenced by the key.

3.2 Dependencies Explained by Quasidifferential Trails

In contrast to the traditional approach of investigating dependencies from the perspective of value restrictions, Beyne and Rijmen [7] advanced the theoretical foundation of differential cryptanalysis and introduced quasidifferential trails capable of capturing the essence of the dependencies.

Fundamentals of Quasidifferential Trail Theory The *quasidifferential transition matrix* is initially established as an extension of the DDT. It is computed by applying a change-of-basis to the permutation matrices that describe the propagation of probability distributions of pairs through the functions under evaluation. The quasidifferential transition matrix D^{S} of an s-bit S-box S is a matrix with $2^{2\cdot s}$ rows and $2^{2\cdot s}$ columns. In terms of value,

$$D^{\mathsf{S}}[(\Gamma_{out}, \Delta_{out}), (\Gamma_{in}, \Delta_{in})] = \frac{1}{2^s} \sum_{\substack{x \in \mathbb{F}_2^s \\ \mathsf{S}(x) \oplus \mathsf{S}(x \oplus \Delta_{in}) = \Delta_{out}}} (-1)^{\langle \Gamma_{in}, x\rangle \oplus \langle \Gamma_{out}, \mathsf{S}(x)\rangle} \quad (3)$$

for all Γ_{in}, Δ_{in}, Γ_{out}, $\Delta_{out} \in \mathbb{F}_2^s$, where $\langle \cdot, \cdot \rangle$ denotes the inner product. It is evident that when $\Gamma_{in} = \Gamma_{out} = 0^s$, the equation (3) simplifies to the probability of the differential $(\Delta_{in}, \Delta_{out})$, where 0^s denotes the s-bit vector with each bit set to zero. From a formal standpoint, equation (3) may be seen as a correlation matrix [15] of S, given that the input is limited to the set of right pairs for the differential $(\Delta_{in}, \Delta_{out})$. Consequently, the absolute value $|D^{\mathsf{S}}[(\Gamma_{out}, \Delta_{out}), (\Gamma_{in}, \Delta_{in})]|$ never exceeds the probability of the differential.

Quasidifferential transition matrices have similar properties to correlation matrices, resulting in the development of the *quasidifferential trail*. An r-round quasidifferential trail is an $(r+1)$-tuple $[\varpi_0, \varpi_1, \ldots, \varpi_r]$ for the function $F = F_{r-1} \circ \cdots \circ F_1 \circ F_0$, with each element ϖ_i comprising a mask-difference pair $\varpi_i = (\Gamma_i, \Delta_i)$. The *correlation* of the quasidifferential trail is $\prod_{i=0}^{r-1} D^{F_i}[\varpi_{i+1}, \varpi_i]$, where D^{F_i} represents the quasidifferential transition matrix of the round function F_i.

Following the introduction of quasidifferential trails, Beyne and Rijmen proved that the exact probability of a differential characteristic is equal to the sum of the correlations of all quasidifferential trails in the differential characteristic; additionally, the exact probability of a differential is equal to the sum of the correlations of all quasidifferential trails in the differential, as opposed to utilising formulas (1) and (2). Specifically, the probability of the r-round differential characteristic $(\Delta_0, \Delta_1, \ldots, \Delta_r)$ can be calculated as

$$\Pr(\Delta_0, \Delta_1, \ldots, \Delta_r) = \sum_{\substack{\Gamma_0 = \Gamma_r = 0^n \\ \Gamma_1, \ldots, \Gamma_{r-1} \in \mathbb{F}_2^n}} \prod_{i=0}^{r-1} D^{F_i}[(\Gamma_{i+1}, \Delta_{i+1}), (\Gamma_i, \Delta_i)]. \quad (4)$$

The probability of the r-round differential $(\Delta_{in}, \Delta_{out})$ can be computed as

$$\Pr(\Delta_{in}, \Delta_{out}) = \sum_{\substack{\varpi_1, \ldots, \varpi_{r-1} \in \mathbb{F}_2^{2\cdot n} \\ \varpi_0 = (0^n, \Delta_{in}), \varpi_r = (0^n, \Delta_{out})}} \prod_{i=0}^{r-1} D^{F_i}[\varpi_{i+1}, \varpi_i].$$

Therefore, providing a more precise assessment of the probabilities of differential characteristics and differentials is partially transformed into the problem of identifying quasidifferential trails. Multiple methods are offered in [7] for computing the quasidifferential transition matrix for 4-bit and 8-bit S-boxes, bitwise-and operations, and modular additions. Finding quasidifferential trails is converted into a Satisfiability Modulo Theories (SMT) problem, which is then addressed with mathematical problem solvers.

Applying the theory of quasidifferential trails to primitives with 8-bit S-boxes may present a potential issue. The quasidifferential transition matrix of an 8-bit S-box is a $2^{16} \times 2^{16}$ matrix. Handling the DDT of an 8-bit S-box, a $2^8 \times 2^8$ matrix, is already challenging for modern automatic methods [1,2,25,9,40]. It is uncertain whether or not the SMT problem can be solved when a matrix of this magnitude is described. It is also worth noting that all ciphers based on S-boxes studied in [7] have S-box sizes that are strictly smaller than 8-bit.

Quasidifferential Trails and Dependencies in Differential Characteristics The following theorem enables us to clarify dependencies in differential characteristics using quasidifferential trails.

Theorem 1 ([7], Theorem 4.2) *Assume that $(\Delta_0, \Delta_1, \ldots, \Delta_r)$ is an r-round differential characteristic of the function $F = F_{r-1} \circ \cdots \circ F_1 \circ F_0$ with a correlation of p (as a quasidifferential trail); the following conclusions hold.*

(I) *If $[(\Gamma_0, \Delta_0), (\Gamma_1, \Delta_1), \ldots, (\Gamma_r, \Delta_r)]$ is a trail with a correlation of $(-1)^\delta p$, where $\delta \in \{0, 1\}$, then for any trail $[(\Gamma'_0, \Delta_0), (\Gamma'_1, \Delta_1), \ldots, (\Gamma'_r, \Delta_r)]$ with a correlation of q, the correlation of the quasidifferential trail $[(\Gamma_0 \oplus \Gamma'_0, \Delta_0), (\Gamma_1 \oplus \Gamma'_1, \Delta_1), \ldots, (\Gamma_r \oplus \Gamma'_r, \Delta_r)]$ is $(-1)^\delta q$.*

(II) *Suppose the correlations of any number of quasidifferential trails, whose differences follow the differential characteristic $(\Delta_0, \Delta_1, \ldots, \Delta_r)$, and each has a correlation of $\pm p$, sum to zero. In that case, the probability of the differential characteristic $(\Delta_0, \Delta_1, \ldots, \Delta_r)$ is zero.*

Theorem 1 highlights the importance of quasidifferential trails with an absolute correlation equal to the correlation of the associated differential characteristic; these are referred to as *strong quasidifferential trails*. Let $\mathcal{QT}(p)$ denote the set of all strong quasidifferential trails of the differential characteristic $(\Delta_0, \Delta_1, \ldots, \Delta_r)$, and let $\mathcal{QT}(p)|_\Gamma$ be the set

$$\left\{ \Gamma_0 \| \Gamma_1 \| \cdots \| \Gamma_r \in \mathbb{F}_2^{(r+1)n} \;\middle|\; [(\Gamma_0, \Delta_0), (\Gamma_1, \Delta_1), \ldots, (\Gamma_r, \Delta_r)] \in \mathcal{QT}(p) \right\}.$$

Using Theorem 1(I), we can deduce that $\mathcal{QT}(p)|_\Gamma$ forms a linear subspace within the space $\mathbb{F}_2^{(r+1)n}$.

Assuming that the dimension of the linear space $\mathcal{QT}(p)|_\Gamma$ is ι, it is possible to identify a basis for this space that consists of ι vectors, denoted as $\Gamma_0^{(l)} \| \Gamma_1^{(l)} \| \cdots \| \Gamma_r^{(l)}$, $0 \leqslant l < \iota$. The correlation of the strong quasidifferential trail with the concatenation of linear masks being $\Gamma_0^{(l)} \| \Gamma_1^{(l)} \| \cdots \| \Gamma_r^{(l)}$ is denoted by $(-1)^{\delta(l)} p$ for all $0 \leqslant l < \iota$. For any vector $\Gamma_0 \| \Gamma_1 \| \cdots \| \Gamma_r$ in $\mathcal{QT}(p)|_\Gamma$, one may select a_0, a_1, …, and $a_{\iota-1}$ in $\mathbb{F}_2$ such that $\Gamma_0 \| \Gamma_1 \| \cdots \| \Gamma_r = \bigoplus_{l=0}^{\iota-1} a_l \Gamma_0^{(l)} \| \Gamma_1^{(l)} \| \cdots \| \Gamma_r^{(l)}$. According to Theorem 1(I), the correlation of the strong quasidifferential trail with the concatenation of linear masks being $\Gamma_0 \| \Gamma_1 \| \cdots \| \Gamma_r$ is $(-1)^{\bigoplus_{l=0}^{\iota-1} a_l \delta(l)} p$. If there is at least one vector in the basis of $\mathcal{QT}(p)|_\Gamma$ for which $\delta(l) = 1$, then the total correlations of all quasidifferential trails in $\mathcal{QT}(p)$ add to zero. Theorem 1(II) asserts that the probability of the differential characteristic $\Pr(\Delta_0, \Delta_1, \ldots, \Delta_r)$ is zero. Thus, the restrictions $\delta(l) = 0$ for all $0 \leqslant l < \iota$ constitute necessary conditions for the probability of the differential characteristic being nonzero. The requirement for the value of $\delta(l)$ in key-alternating ciphers can be explicitly interpreted as restrictions on round keys.

Given that the round function $F_i(x)$ of key-alternating ciphers may be denoted as $G_i(x) \oplus rk^i$, it follows that

$$D^{F_i}[(\Gamma_{i+1}, \Delta_{i+1}), (\Gamma_i, \Delta_i)] = (-1)^{\langle \Gamma_{i+1}, rk^i \rangle} D^{G_i}[(\Gamma_{i+1}, \Delta_{i+1}), (\Gamma_i, \Delta_i)].$$

Consequently, the probability of the differential characteristic, as calculated in formula (4), can be expressed as

$$\sum_{\substack{\Gamma_0=\Gamma_r=0^n \\ \Gamma_1,\ldots,\Gamma_{r-1}\in\mathbb{F}_2^n}} (-1)^{\langle \Gamma_1 \| \cdots \| \Gamma_{r-1}, rk^0 \| \cdots \| rk^{r-2} \rangle \oplus \varepsilon_{\Gamma_1,\Gamma_2,\ldots,\Gamma_{r-1}}} \left| \prod_{i=0}^{r-1} D^{G_i}[(\Gamma_{i+1}, \Delta_{i+1}), (\Gamma_i, \Delta_i)] \right|,$$

where $(-1)^{\varepsilon_{\Gamma_1,\Gamma_2,\ldots,\Gamma_{r-1}}}$ represents the sign of $\prod_{i=0}^{r-1} D^{G_i}[(\Gamma_{i+1}, \Delta_{i+1}), (\Gamma_i, \Delta_i)]$. The value of $\delta(l)$ for the strong quasidifferential trail associated with the basis vector $\Gamma_0^{(l)} \| \Gamma_1^{(l)} \| \cdots \| \Gamma_r^{(l)}$ can be computed as $\langle \Gamma_1^{(l)} \| \cdots \| \Gamma_{r-1}^{(l)}, rk^0 \| \cdots \| rk^{r-2} \rangle \oplus \varepsilon_{\Gamma_1^{(l)},\Gamma_2^{(l)},\ldots,\Gamma_{r-1}^{(l)}}$, contingent upon the values of the round keys rk^0, rk^1, …, and rk^{r-2}. Hence, the 2^ι quasidifferential trails in $\mathcal{QT}(p)$ impose ι restrictions on the values of the round keys, which are

$$\langle \Gamma_1^{(l)} \| \cdots \| \Gamma_{r-1}^{(l)}, rk^0 \| \cdots \| rk^{r-2} \rangle \oplus \varepsilon_{\Gamma_1^{(l)},\Gamma_2^{(l)},\ldots,\Gamma_{r-1}^{(l)}} = 0, \quad 0 \leqslant l < \iota.$$

These restrictions are referred to as *deterministic linear relations*.

Quasidifferential trails with absolute correlations lower than that of the differential characteristic are generally less significant than strong quasidifferential trails. While the overall correlation of these quasidifferential trails may impact the probability of the differential characteristic, this effect occurs only for a small subset of keys, as it requires the signs of all these quasidifferential trails to align uniformly. The restrictions on round keys derived from these minor quasidifferential trails are referred to as *probabilistic linear relations*.

Although a particular differential characteristic may include several quasidifferential trails, strong quasidifferential trails often exhibit nonzero masks only in the differentially active S-boxes. Strong quasidifferential trails may be seen in many ciphers. One primary factor contributing to this phenomenon is the prevalence of planar S-boxes [16], wherein the input and output values of right pairs consistently form affine subspaces. It is highly likely to identify a nonzero mask $\Gamma_{in} \| \Gamma_{out}$ that maintains constant parity $\langle \Gamma_{in}, x \rangle \oplus \langle \Gamma_{out}, \mathsf{S}(x) \rangle$ when the input x of the planar S-boxes S is restricted to the right pairs of a nontrivial differential propagation. Beyne and Rijmen stated that the plateau characteristics [16] are derived from the propagation of this affine subspace. However, doing so for more than two rounds is difficult.

3.3 Relations Between the Two Types of Explanations

Despite the divergent perspectives, we contend that both explanatory frameworks for dependencies in differential characteristics possess inherent merit. The direct nature of value restrictions on intermediate states leads to the creation of highly obvious linear and nonlinear constraints, facilitating a reasonably straightforward understanding of these constraints. On the other hand, quasidifferential trails provide profound insight into the fundamental principles of dependencies, and the use of quasidifferential trails enables an extensive and in-depth description of dependencies inside differential characteristics, enhancing our understanding of the field.

Using value restrictions allows for representing dependencies in differential characteristics through linear, nonlinear, and unknown constraints[4]. Section 3.2 demonstrates that using quasidifferential trails enables the representation of dependencies as either deterministic or probabilistic linear relations. The following discussion further explores the relationships between these different forms of dependency.

Linear constraints are specific cases of deterministic linear relations. Referring to Figure 2, for the two affine subspaces $\mathcal{Y}^i$ and $\mathcal{X}^{i+1}$, suppose we can identify a nonzero linear mask Γ_{i+1} that ensures the parities $\langle \Gamma_{i+1}, L(y^i) \rangle$ and $\langle \Gamma_{i+1}, x^{i+1} \rangle$ remain constant for all $y^i \in \mathcal{Y}^i$ and $x^{i+1} \in \mathcal{X}^{i+1}$, respectively.

$$[(0^n, \Delta_0), \ldots, (0^n, \Delta_i), (\Gamma_{i+1}, \Delta_{i+1}), (0^n, \Delta_{i+2}) \ldots, (0^n, \Delta_r)] \tag{5}$$

constitutes a strong quasidifferential trail for the differential characteristic $(\Delta_0, \Delta_1, \ldots, \Delta_r)$, where 0^n is the n-bit zero mask. The correlation of this strong quasidifferential trail is

$$(-1)^{\langle \Gamma_{i+1}, rk^i \oplus L(y^i) \oplus x^{i+1} \rangle} \prod_{j=0}^{r-1} D^{L \circ S}[(0^n, \Delta_{j+1}), (0^n, \Delta_j)],$$

for any $y^i \in \mathcal{Y}^i$ and $x^{i+1} \in \mathcal{X}^{i+1}$. Based on the analysis in Section 3.2, a necessary condition for the probability of the differential characteristic being nonzero is that the round key value rk^i must ensure that the correlation of the strong quasidifferential trail matches that of the differential characteristic. The deterministic linear relation derived from the quasidifferential trail in expression (5) should be

$$\langle \Gamma_{i+1}, rk^i \oplus L(y^i) \oplus x^{i+1} \rangle = 0 \text{ for all } y^i \in \mathcal{Y}^i \text{ and } x^{i+1} \in \mathcal{X}^{i+1}.$$

Therefore, the linear constraint $rk^i \in L(\mathcal{Y}^i) \oplus \mathcal{X}^{i+1}$ serves as a sufficient condition for the correlations of all strong quasidifferential trails in expression (5) to be positive. In this sense, linear constraints form a subset of deterministic linear relations.

[4] As Peyrin and Tan [29] noted, it is currently uncertain whether there are any constraints beyond linear and nonlinear constraints. We name these undiscovered constraints as unknown constraints.

Furthermore, suppose we can identify strong quasidifferential trails

$$[(0^n, \Delta_0), \ldots, (0^n, \Delta_{i-1}), (\Gamma_i, \Delta_i), (\Gamma_{i+1}, \Delta_{i+1}), (0^n, \Delta_{i+2}) \ldots, (0^n, \Delta_r)]$$

with nonzero values for Γ_i and Γ_{i+1}. In that case, the deterministic linear relations derived from these trails impose restrictions on round keys rk^{i-1} and rk^i that extend beyond linear constraints. While these constraints are inherently nonlinear by definition, they can be represented in a linear form. More details regarding these specific nonlinear constraints will be discussed in Section 4. Thus, in addition to linear constraints, deterministic linear relations also encompass a subset of nonlinear constraints arising from value restrictions.

In addition to the subset of nonlinear constraints within the deterministic linear relations, the remaining nonlinear constraints should be classified as probabilistic linear relations. If there are any unknown constraints, they must also fall under the category of probabilistic linear relations. See Figure 3 for the relationship among these various representations.

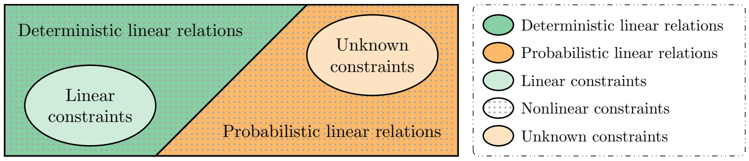

Deterministic linear relations
Unknown constraints
Linear constraints
Probabilistic linear relations
Deterministic linear relations
Probabilistic linear relations
Linear constraints
Nonlinear constraints
Unknown constraints

Fig. 3. Relationship between different dependence representations.

3.4 Verification of Difference-Based Distinguishers

In addition to the theoretical examination of dependencies in differential characteristics, automatic techniques are available to confirm the feasibility of difference-based distinguishers. Sadeghi *et al.* [33] propose a method that utilises Mixed Integer Linear Programming (MILP) to detect incompatible differential characteristics. Figure 4 depicts a schematic representation of the MILP model. The core idea is to simultaneously model the value transitions of the pair of inputs $(x^0, \tilde{x}^0)$ and difference transitions $(\Delta_0, \Delta_1, \ldots, \Delta_r)$ for the target cipher and then link the two by adding the restriction $x^i \oplus \tilde{x}^i = \Delta_i$ for all $0 \leqslant i \leqslant r$. In the model, only the variables for the master key K and input x^0 are free. If the MILP model is infeasible for a specific differential characteristic $(\Delta_0, \Delta_1, \ldots, \Delta_r)$, indicating that the characteristic is invalid for all keys, it is considered incompatible. On the other hand, if the model is feasible, it will yield the right pair and the corresponding key. This approach is utilised to verify the validity of some reported differential characteristics of `SIMECK` [45] and `SPECK` [5]. The MILP model is unlikely to be a suitable method for addressing the fundamental issue of dependencies in difference-based distinguishers, as it cannot explain why a characteristic is impossible or identify the conditions necessary for a key to have the right

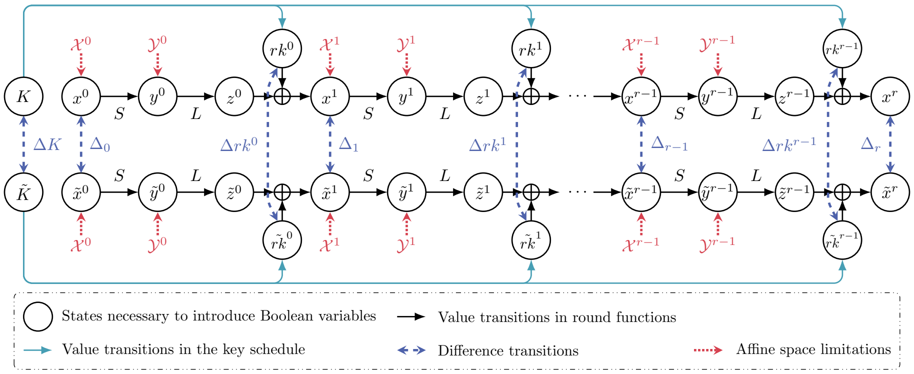


Fig. 4. MILP model in [33] to identify incompatible differential characteristics. Note that the affine space limitations are not included in [33]. The meaning of affine space limitations and the rationale behind their inclusion will be elucidated in Section 5.

pairs. The primary limitation of the procedure in [33] is its failure to account for the nature of the problem.

Peyrin and Tan [29] have developed a Constraint Programming (CP) model designed explicitly for SKINNY. This model can simultaneously search for differential characteristics and test incompatibilities. The CP program can also identify a similar differential characteristic when given an impossible one, which is effective for at least one key.

4 Linearised Nonlinear Constraints: Theory and Solution

Based on the discussion in Section 3.3, linear constraints constitute a subset of deterministic linear relations. Certain ciphers may have nonlinear constraints by definition, yet their representations are linear equations. This section introduces a method that uses value restrictions to identify these particular nonlinear constraints. We acknowledge that the constraints identified by our methodology may also be ascertained using the theory of quasidifferential trails [7]. Nevertheless, we believe our method still has a specific value, which will be discussed in Section 8.

This section provides an example using GIFT-64 to illustrate the particular nonlinear constraint. Next, we demonstrate the technique for identifying these constraints for primitives with S-boxes whose differential uniformity equals 4.

4.1 Nonlinear Constraint Example on GIFT-64

According to Peyrin and Tan [29], the nonlinear constraint may stretch across several rounds. However, the current batch-based verification technique on GIFT-64 cannot detect nonlinear constraints that extend beyond three rounds. In this section, we provide an example displaying the existence of nonlinear constraints on the differential characteristic of GIFT-64 across six rounds.

We select the related-key differential characteristic from [41] as an illustration. Figure 8 of [41] shows that the first to fourth rounds and the thirteenth to sixteenth rounds of the 18-round characteristic have no active S-boxes due to the simplicity of the key schedule. Consequently, the component depicted in Figure 11 of Appendix B—which spans eight rounds and includes an extra adding round key operation at the beginning with zero input and output differences—is a crucial part of the whole characteristic. Notably, although the preceding related-key differential attacks [41,11,10] on `GIFT-64` are all based on this 18-round differential characteristic, the validity of the differential characteristic—more precisely, the dependencies in the differential characteristic—is never taken into account.

Figure 5 highlights a nonlinear constraint in the differential characteristic across six rounds. Due to the propagation of the input difference `0x2` to the output difference `0x5` via the first active S-boxes in the fifth round, the output value $y^5_{48} \| y^5_{49} \| y^5_{50} \| y^5_{51}$ corresponding to this S-box for the right pairs of the differential characteristic must be selected from the set $\{\texttt{0x1}, \texttt{0x3}, \texttt{0x4}, \texttt{0x6}\}$. Therefore, the values of y^5_{49} and y^5_{51} fulfil

$$y^5_{49} \oplus y^5_{51} = 1. \tag{6}$$

Next, y^5_{49} and y^5_{51} will be sent to separate active S-boxes in the following round.

In the sixth round, two active S-boxes exhibit differential propagation $\texttt{0x5} \xrightarrow{GS} \texttt{0x2}$. The two right pairs involved in this propagation satisfy $GS(\texttt{0x8}) = \texttt{0x2}$ and $GS(\texttt{0xd}) = \texttt{0x0}$. Therefore, the values of $x^6_{13} \oplus y^6_{14}$ and $x^6_{47} \oplus y^6_{46}$ are nonzero for the right pairs of the differential characteristic. By substituting the equations $x^6_{13} = y^5_{49}$, $x^6_{47} = y^5_{51} \oplus k_{95}$ and equation (6), we can get the formulas for the values of two output bits of the active S-boxes in the sixth round

$$y^6_{14} = y^5_{51} \text{ and } y^6_{46} = y^5_{51} \oplus k_{95} \oplus 1. \tag{7}$$

Note that the sixth round analysis relies on the observation that when we fix the differential propagation for the S-box, the relationship between the input and output of the active S-boxes becomes linear. We will iteratively use this information to identify the nonlinear constraint spanning numerous rounds.

In the seventh round, two active S-boxes receive the two bits y^6_{14} and y^6_{46} from the sixth round. According to the fixed differential propagation $\texttt{0x2} \xrightarrow{GS} \texttt{0xa}$, the third output bit y^7_{34} of the first active S-box is consistently identical to the third input bit x^7_{34}. Similarly, the fixed differential propagation $\texttt{0x2} \xrightarrow{GS} \texttt{0xe}$ of the second active S-box ensures that the third output bit y^7_{42} is identical to the third input bit x^7_{42}. After applying equation (7), the two output bits y^7_{34} and y^7_{42} of the seventh round for the right pairs may be written as the following linear equations concerning the output bit y^5_{51} of the fifth round

$$y^7_{34} = y^5_{51} \oplus k_{38} \text{ and } y^7_{42} = y^5_{51} \oplus k_{40} \oplus k_{95} \oplus 1.$$

A comparable analysis shows that the two output bits y^8_{27} and y^8_{59} of the active S-boxes in the eighth round are linearly dependent on the value of y^5_{51}, given by the expressions

$$y_{27}^{8} = y_{51}^{5} \oplus k_4 \oplus k_{38} \oplus 1 \text{ and } y_{59}^{8} = y_{51}^{5} \oplus k_{12} \oplus k_{40} \oplus k_{95}.$$

Next, as shown in Figure 5, these two bits are inserted into the second and third active S-boxes during the ninth round. The fixed differential propagation of the active S-boxes establishes linear relationships between x_7^9 and y_4^9, as well as x_{15}^9 and y_{12}^9. These relationships allow us to derive linear expressions for y_4^9 and y_{12}^9

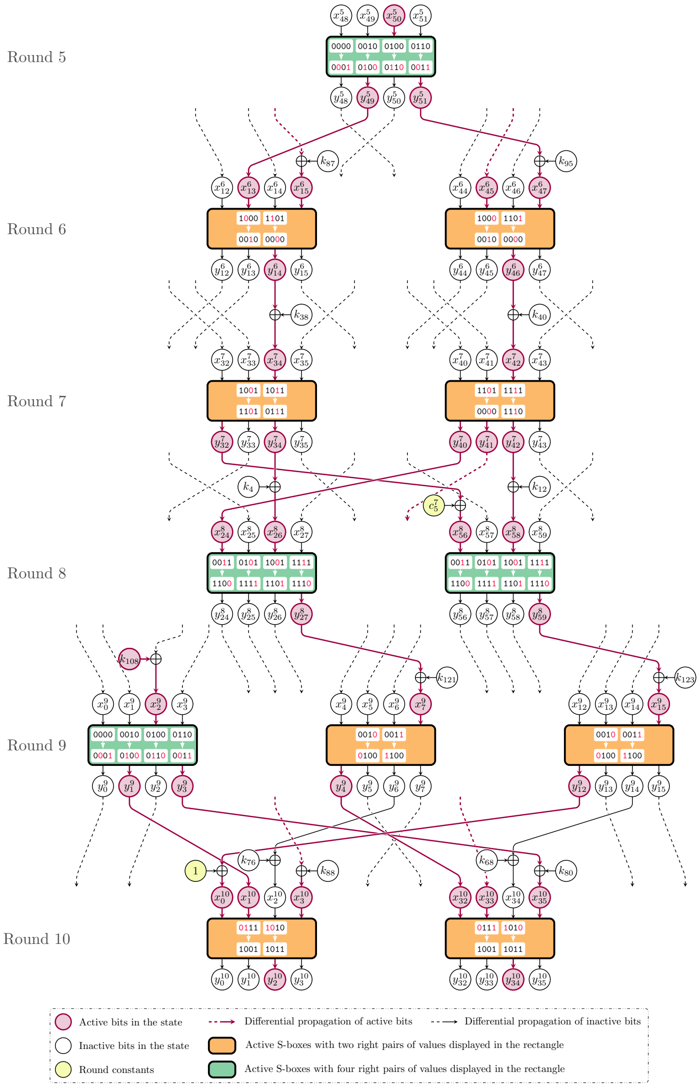

Round 5
Round 6
Round 7
Round 8
Round 9
Round 10
Active bits in the state
Inactive bits in the state
Round constants
Differential propagation of active bits
Differential propagation of inactive bits
Active S-boxes with two right pairs of values displayed in the rectangle
Active S-boxes with four right pairs of values displayed in the rectangle

Fig. 5. Illustration of the nonlinear constraint covering six rounds.

in terms of y^5_{51}, which are

$$y^9_4 = y^5_{51} \oplus k_4 \oplus k_{38} \oplus k_{121} \oplus 1 \text{ and } y^9_{12} = y^5_{51} \oplus k_{12} \oplus k_{40} \oplus k_{95} \oplus k_{123}. \quad (8)$$

Simultaneously, since the first active S-box in the ninth round exhibits a differential propagation of `0x2` $\xrightarrow{GS}$ `0x5`, the data regarding the right pairs associated with this propagation indicates that the two output bits y^9_1 and y^9_3 of the S-box satisfy the equation

$$y^9_1 \oplus y^9_3 = 1. \quad (9)$$

The four output bits y^9_1, y^9_3, y^9_4, and y^9_{12} from the ninth round will be divided into two groups. Each group will be inputted into an active S-box during the tenth round. According to Figure 5, the values y^9_1 and y^9_{12} are inputted into the first active S-box with a differential propagation of `0xd` $\xrightarrow{GS}$ `0x2`. For this propagation to occur, the XORed value of the two input bits x^{10}_0 and x^{10}_1 of this S-box must be nonzero. This connection establishes an equation between y^9_1 and y^9_{12}, expressed as

$$y^9_1 \oplus y^9_{12} = 0. \quad (10)$$

An analogous examination of the second active S-box in the tenth round reveals a linear relation between y^9_3 and y^9_4, expressed as

$$y^9_3 \oplus y^9_4 \oplus k_{80} = 1. \quad (11)$$

By performing an XOR operation on equations (8) - (11), we get a constraint on round keys

$$k_4 \oplus k_{12} \oplus k_{38} \oplus k_{40} \oplus k_{80} \oplus k_{95} \oplus k_{121} \oplus k_{123} = 1 \quad (12)$$

encompassing six rounds of encryption.

Given that the constraint in equation (12) involves S-boxes and keys from many rounds, it is categorised as a nonlinear constraint by definition. Its expression, nonetheless, is a linear one. Interestingly, contrary to what was found in [29], this kind of nonlinear constraint should be considered when estimating the dimension of right key space for a given differential characteristic. It is vital to recognise that this sort of nonlinear constraint, which only incorporates active S-boxes, is just a subtype of nonlinear constraints. We call these particular nonlinear constraints *linearised nonlinear constraints* to distinguish them from the more general nonlinear constraints.

4.2 Linearisation of Active S-Boxes

We have many queries after creating the 6-round nonlinear constraint through value restrictions. For example: Is the linearised nonlinear constraint merely a specific case for the differential characteristic in [41]? Is there a linearised nonlinear constraint in the other differential characteristics of GIFT-64? Does the linearised nonlinear constraint appear in the differential characteristics of other primitives? Before tackling these issues, we must first figure out how to discover linearised nonlinear constraints for given differential characteristics.

Based on the example in Section 4.1, it is evident that one factor contributing to the linearised nonlinear constraint spanning numerous rounds is the linear dependence between the output bits of right pairs for the active S-boxes and the input bits. The following lemma is necessary before establishing this linear dependency in a generic scenario.

Lemma 1. *Let $\{\alpha^0, \alpha^1, \ldots, \alpha^{\varsigma-1}\}$ and $\{\beta^0, \beta^1, \ldots, \beta^{\varsigma-1}\}$ be two sets of linearly independent vectors in the vector space $\mathbb{F}_2^n$ ($n \geqslant 1$ and $\varsigma \leqslant n$). An invertible $n \times n$ matrix M exists such that $M \cdot \alpha^i = \beta^i$ for all $0 \leqslant i < \varsigma$.*

Proof. For the set $\{\alpha^0, \alpha^1, \ldots, \alpha^{\varsigma-1}\}$, which contains ς linearly independent vectors, it is possible to identify $n-\varsigma$ vectors α^{ς}, $\alpha^{\varsigma+1}$, …, α^{n-1} in $\mathbb{F}_2^n$ such that the set $\{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\}$ forms a basis for $\mathbb{F}_2^n$. Similarly, we can select $n-\varsigma$ vectors β^{ς}, $\beta^{\varsigma+1}$, …, β^{n-1} in $\mathbb{F}_2^n$ such that the set $\{\beta^0, \beta^1, \ldots, \beta^{n-1}\}$ constitutes a basis for $\mathbb{F}_2^n$. When these vectors are considered as column vectors, both matrices $M_1 = \left[\begin{array}{c:c:c:c} \alpha^0 & \alpha^1 & \cdots & \alpha^{n-1} \end{array}\right]$ and $M_2 = \left[\begin{array}{c:c:c:c} \beta^0 & \beta^1 & \cdots & \beta^{n-1} \end{array}\right]$, each of dimension $n \times n$, are invertible. The matrix $M \triangleq M_2 \cdot M_1^{-1}$ ensures the validity of the equations $M \cdot \alpha^i = \beta^i$, $0 \leqslant i < \varsigma$.

Using Lemma 1, we can show that linear dependency in the active S-boxes of GIFT-64 is not an exceptional occurrence but a common phenomenon that occurs in S-boxes with a differential uniformity of four.

Proposition 1. *If a vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ ($n > 1$) is invertible and has exactly two right pairs for its differential $(\Delta_{in}, \Delta_{out})$, then an $n \times n$ matrix A and an n-bit vector α exist such that $F(x) = A \cdot x \oplus \alpha$ for all x in the set $\{x \in \mathbb{F}_2^n \mid F(x) \oplus F(x \oplus \Delta_{in}) = \Delta_{out}\}$.*

Proof. Since F is an invertible function and $n > 1$, each possible differential $(\Delta_{in}, \Delta_{out})$ with exactly two right pairs must satisfy the condition that Δ_{in} and Δ_{out} are nonzero vectors. Denote the two right pairs for the differential $(\Delta_{in}, \Delta_{out})$ as x^0 and $x^0 \oplus \Delta_{in}$. We represent $F(x^0)$ as y^0, and $F(x^0 \oplus \Delta_{in})$ is equivalent to $y^0 \oplus \Delta_{out}$. For the two nonzero vectors, Δ_{in} and Δ_{out}, we may obtain an invertible $n \times n$ matrix M by applying Lemma 1, which validates $M \cdot \Delta_{in} = \Delta_{out}$. Then, by assigning $A = M$ and $\alpha = M \cdot x^0 \oplus y^0$, an equivalent equation $A \cdot x \oplus \alpha$ for $F(x)$ confined on the set $\{x^0, x^0 \oplus \Delta_{in}\}$ is found.

Proposition 2. *If a vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ ($n > 2$) is invertible and has exactly four right pairs for its differential $(\Delta_{in}, \Delta_{out})$, then an $n \times n$ matrix A and an n-bit vector α exist such that $F(x) = A \cdot x \oplus \alpha$ for all x in the set $\{x \in \mathbb{F}_2^n \mid F(x) \oplus F(x \oplus \Delta_{in}) = \Delta_{out}\}$.*

Proof. Considering that F is an invertible function and $n > 2$, each differential $(\Delta_{in}, \Delta_{out})$ with precisely four right pairs must satisfy the condition that Δ_{in} and Δ_{out} are nonzero vectors. Denote the inputs of the four right pairs for the differential $(\Delta_{in}, \Delta_{out})$ as x^0, $x^0 \oplus \Delta_{in}$, x^1, and $x^1 \oplus \Delta_{in}$. It can be inferred that $x^0 \neq x^1$ and $x^0 \oplus x^1 \neq \Delta_{in}$. Represent $F(x^0)$ and $F(x^1)$, respectively, as y^0 and y^1. It means $y^0 \oplus \Delta_{out}$ and $y^1 \oplus \Delta_{out}$ can represent $F(x^0 \oplus \Delta_{in})$ and $F(x^1 \oplus \Delta_{in})$. Since F is invertible, it follows that $y^0 \neq y^1$ and $y^0 \oplus y^1 \neq \Delta_{out}$. $\{\Delta_{in}, x^0 \oplus x^1\}$ and $\{\Delta_{out}, y^0 \oplus y^1\}$ are two sets of linearly independent vectors. Lemma 1 allows us to identify an $n \times n$ invertible matrix M such that $M \cdot \Delta_{in} = \Delta_{out}$ and $M \cdot (x^0 \oplus x^1) = y^0 \oplus y^1$. An alternative formula $A \cdot x \oplus \alpha$ is derived to represent the restriction of $F(x)$ on $\{x^0, x^0 \oplus \Delta_{in}, x^1, x^1 \oplus \Delta_{in}\}$ by assigning $A = M$ and $\alpha = M \cdot x^0 \oplus y^0$.

Remark 1. Qiao *et al.* [30] define the affine input subspaces as *linearisation affine subspaces* when the S-box restriction on the affine subspaces corresponds to a linear transformation. They observed that the inputs corresponding to possible differential propagations with a maximum of four right pairs constitute linearisation affine subspaces for the 5-bit S-box of `Keccak` [20]. In addition to providing a theoretical rationale for the finding in [30], Propositions 1 and 2 demonstrate that linearisation affine subspaces are often found as long as the S-box holds differential propagations with two or four right pairs.

4.3 Method for Finding Linearised Nonlinear Constraints

It is now possible to identify linearised nonlinear constraints for primitives with S-boxes. We take the structural primitive in Figure 2 as an illustration.

In this case, we assume that the nonlinear component S comprises S-boxes with a differential uniformity of four. Consequently, for all $0 \leqslant i \leqslant r-1$, the set $\mathcal{X}^i$ consisting of possible values for x^i constitutes affine spaces. It is possible to generate a $\ell^i \times n$ matrix A^i and a ℓ^i-bit vector α^i such that $x^i \in \mathcal{X}^i$ if and only if

$$A^i \cdot x^i = \alpha^i, \quad 0 \leqslant i \leqslant r-1. \tag{13}$$

Using Propositions 1 and 2, the active S-boxes in the nonlinear component S will yield linear connections between certain bits of x^i and y^i. To ensure the existence of at least one right pair for the given differential characteristic, we can create two $\tilde{\ell}^i \times n$ matrices B^i and C^i, as well as a $\tilde{\ell}^i$-bit vector β^i, such that

$$B^i \cdot x^i \oplus C^i \cdot y^i = \beta^i, \quad 0 \leqslant i \leqslant r-1. \tag{14}$$

Aside from that, the value transition in round functions necessitates the satisfaction of the following equations

$$L \cdot y^i \oplus x^{i+1} \oplus rk^i = 0, \quad 0 \leqslant i \leqslant r-2. \tag{15}$$

Combining equations (13) - (15) shows that the vector consisting of $2r+1$ internal states x^0, y^0, x^1, y^1, $\ldots$, x^{r-1}, y^{r-1}, x^r and r round keys rk^0, rk^1, $\ldots$, rk^{r-1}

must satisfy

$$\begin{bmatrix} A^0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ B^0 & C^0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & L & I & 0 & \cdots & 0 & 0 & 0 & I & 0 & \cdots & 0 \\ 0 & 0 & A^1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & B^1 & C^1 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & A^{r-1} & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & B^{r-1} & C^{r-1} & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & L & I & 0 & 0 & \cdots & I \end{bmatrix} \cdot \begin{bmatrix} x^0 \\ y^0 \\ x^1 \\ y^1 \\ \vdots \\ x^{r-1} \\ y^{r-1} \\ x^r \\ rk^0 \\ rk^1 \\ \vdots \\ rk^{r-1} \end{bmatrix} = \begin{bmatrix} \alpha^0 \\ \beta^0 \\ 0 \\ \alpha^1 \\ \beta^1 \\ \vdots \\ \alpha^{r-1} \\ \beta^{r-1} \\ 0 \end{bmatrix}. \quad (16)$$

To simplify the formula, we use the symbol $\vec{x}$ to represent the vector $x^0\|y^0\|\cdots\|x^r$ created by concatenating the $2r+1$ internal states. The dimension of the vector $\vec{x}$, represented as $\dim(\vec{x})$, is equal to $2rn+n$. Similarly, we use the symbol $\vec{k}$ to denote the vector $rk^0\|rk^1\|\cdots\|rk^{r-1}$. We, therefore, have $\dim(\vec{k}) = rn$. After performing Gaussian elimination, equation (16) will be transformed into the following expression

$$\left[\begin{array}{c:c} \multicolumn{2}{c}{M_v} \\ \hdashline 0 & M_k \end{array}\right] \cdot \begin{bmatrix} \vec{x} \\ \hdashline \vec{k} \end{bmatrix} = \begin{bmatrix} \alpha_v \\ \hdashline \alpha_k \end{bmatrix}. \quad (17)$$

In this expression, M_v represents a matrix with each row containing at least one nonzero element among the first $\dim(\vec{x})$ columns, M_k is a binary matrix with $\dim(\vec{k})$ columns, α_v is a column vector with $\dim(\vec{x})$ bits, and α_k is a column vector with $\dim(\vec{k})$ bits. Therefore, the equation

$$M_k \cdot \vec{k} = \alpha_k, \quad (18)$$

derived from equation (17) must have at least one solution for equation (17) to be solvable.

Given that the equations used to determine linear constraints in the given differential characteristic comprise a subset of equation (16), it follows that the constraints derived from equation (18) must encompass the linear constraints that have been previously discussed in the literature [16,27,12,43,26]. In addition, employing the linear dependency between the input and output of active S-boxes, linearised nonlinear constraints may be derived from equation (18) if any such constraints exist.

The linearised nonlinear constraints detection method is initially applied to the 8-round related-key differential characteristic of `GIFT-64` in Appendix B to validate its feasibility. The output consists of eight constraints on the key bits, comprising six linear constraints and two linearised nonlinear constraints. Apart from the linearised nonlinear constraints already established in equation (12), the 8-round differential characteristic exhibits an additional linearised nonlinear constraint covering four rounds, namely

$$k_{12} \oplus k_{88} \oplus k_{122} \oplus k_{123} = 1.$$

See Appendix C for an illustration.

The proposed detection method for linearised nonlinear constraints is effective and highly practical, as demonstrated by its performance on the 8-round differential characteristic for GIFT-64. This strategy allows us to address the concerns presented at the start of Section 4.2. However, the primary objective is not to uncover these linearised nonlinear constraints but to determine how to utilise them to evaluate the specified differential characteristics better. The next part will introduce a methodology for doing this work.

5 Three-Stage Evaluation Approach

In Section 4, we saw the impact of linearised nonlinear constraints on the right key space of the differential characteristic for GIFT-64. These constraints will undoubtedly impact the remaining probability of the differential characteristic. In the next section, we aim to provide a more accurate assessment of the right key spaces and remaining probabilities for differential characteristics incorporating linearised nonlinear constraints. To achieve this goal, we propose a three-stage evaluation approach.

Stage 1: Initial Assessment. The method previously described in [16,27,12,43,26] is employed to search for linear constraints in the given differential characteristics. The linearised nonlinear constraints are then determined using the linearisation method described in Section 4.3. By considering the two sets of constraints, we can make an initial evaluation of the right key space $\mathbb{K}_{\texttt{init}}$ and the remaining probability $p_{\texttt{init}}$ of the differential characteristic.

Example 1. Consider once more the 8-round differential characteristic for GIFT-64. The differential characteristic is subject to six linear and two linearised nonlinear constraints following the initial evaluation, as shown in Table 2. Thus, in the initial assessment, the right key space $\mathbb{K}_{\texttt{init}}$ of the differential characteristic accounts for just 2^{-8} out of the entire key space, resulting in a remaining probability $p_{\texttt{init}}$ of 2^{-42} instead of 2^{-50}.

Stage 2: Detecting Potential Constraints. If the right key space in the initial assessment phase is not empty, we can do the following analysis. The remaining constraints may consist of nonlinear constraints that pertain to inactive S-boxes and unknown constraints, both of which are typically difficult to identify. To

Table 2. Constraints in the 8-round related-key differential characteristic for `GIFT-64`.

Round	5	6	7	8	9	10	11	12
LC	$k_{87} \oplus k_{95} = 0$	-	$k_{30} = 1$	-	$k_{68} = 1$ $k_{76} = 1$ $k_{80} \oplus k_{88} = 1$	-	$k_{17} \oplus k_{25} = 0$	-
LNC	$k_4 \oplus k_{12} \oplus k_{38} \oplus k_{40} \oplus k_{80} \oplus k_{95} \oplus k_{121} \oplus k_{123} = 1$						-	
	-		$k_{12} \oplus k_{88} \oplus k_{122} \oplus k_{123} = 1$				-	

LC: Linear constraints. LNC: Linearised nonlinear constraints.

detect them, we utilise the framework proposed in [33] and implement a sequence of modifications. A minor change to the realisation is that the Boolean satisfiability problem (SAT) approach is used to create the incompatibility detection framework. The primary motivation for using SAT is the handy support for XOR clauses in the SAT solver CryptoMiniSat [38]. It allows us to incorporate Boolean equations represented using XOR operations easily. As seen in Section 4.3, these equations are frequently used to restrict the inputs of active S-boxes to specific affine spaces. The tests are conducted on a desktop computer equipped with Apple M2 Ultra processors, and the stated runtime corresponds to the duration when only a single core is utilised.

Given that the objective is to reveal those unidentified constraints, excluding the impact of the linear and linearised nonlinear constraints that have already been identified is preferable. Therefore, our *initial modification* to the framework in [33] is to fix the key within the framework. Rather than selecting the key randomly, we must choose the key from the initial right key space $\mathbb{K}_{\texttt{init}}$. Doing so eliminates the impact of the previously identified linear and linearised nonlinear constraints.

In general, several keys are selected randomly from $\mathbb{K}_{\texttt{init}}$, and CryptoMiniSat is used to check whether or not each of these keys possesses the right pairs. If some keys do not have the right pairs, it may be inferred that there are undiscovered constraints, as these keys naturally meet the recognised linear and linearised nonlinear constraints. Next, we will strive to grasp them by observing keys missing the right pairs. One recommended approach to discovering them can be found in Section 7.3, which focuses on a specific differential characteristic of `WARP` [3]. Conversely, if the right pairs for each selected key can be identified, it is possible to deduce that the right key space for the characteristic is $\mathbb{K}_{\texttt{init}}$. Given that we only test some keys in $\mathbb{K}_{\texttt{init}}$, the conclusion may be erroneous. To improve precision, we have the flexibility to conduct many tests within the allotted period.

We make the *second modification* when implementing the framework described in [33]. As seen in Figure 4, we incorporate additional conditions to guarantee that internal states fall into distinct affine spaces. Specifically, for every $0 \leqslant i \leqslant r-1$, x^i and $\tilde{x}^i$ belong to $\mathcal{X}^i$, whereas y^i and $\tilde{y}^i$ belong to $\mathcal{Y}^i$. These limitations are considered auxiliary information since they may be deduced from the differences in the internal states. However, we observed in the test that introducing these constraints can speed up the search.

Example 2. We randomly generated 10^6 keys that meet the eight conditions specified in Table 2 for the 8-round differential characteristic of `GIFT-64`. Every individual key gets independent validation, and the test result verifies that all selected keys contain right pairs. The runtime is 5803.47 seconds. Based on this outcome, we can confidently affirm that the initially detected $\mathbb{K}_{\texttt{init}}$ is the right key space for the differential characteristic. The likelihood of undisclosed constraints being present is very low.

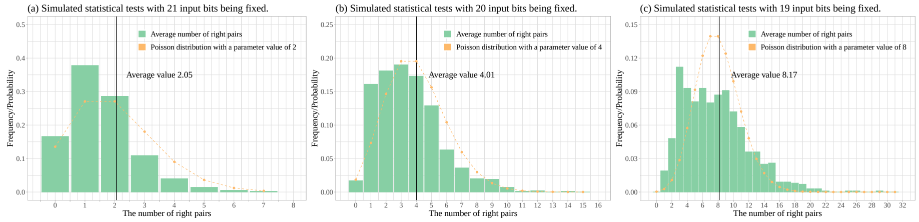
Stage 3: Estimating the Remaining Probability. At this point, the right key space has already been determined. The last step is to evaluate the remaining probability of the differential characteristic. Experimental verification is a reliable method. Nevertheless, statistical testing is sometimes unfeasible due to the generally low probability of the specified differential characteristic. We make the *third modification* to the framework described in [33] to provide a different approach to mimic statistical tests.

The concept involves randomly assigning ψ bits in the input x^0 to ψ randomly generated binary values. These conditions are incorporated into the framework. The key shall remain a fixed value chosen randomly from the right key space. Next, we employ the SAT solver to search for all the right pairs that satisfy the differential characteristic. This approach can be seen as a statistical test using $2^{n-\psi}$ chosen plaintext-ciphertext pairs. However, the result of a single test could contain some inaccuracies since the plaintext-ciphertext pairs are not entirely generated at random. To rectify this defect, we can execute the simulation multiple times. The ψ places and the ψ values associated with these positions may be varied in each test. Once all the tests have been completed, an average number of right pairs ϱ is calculated from the simulation results. The probability of the differential characteristic is approximated as $\varrho/2^{n-\psi}$. Additionally, this simulation can be replicated using several predetermined keys to enhance the outcome's reliability.

Example 3. In continuation of the experiment described in Example 2, the theoretical remaining probability of the 8-round related-key differential characteristic is 2^{-42} due to the absence of any further constraints identified in the second stage. We aim to perform statistical tests using 2^{43} plaintext pairs for 1000 randomly chosen keys from the right key space. As in the previously described method, 21 bits of the input are arbitrarily fixed to arbitrary binary values, and multiple-solution-seeking tasks[5] are executed using the SAT solver. This ap-

[5] We know that specific approximate model counters, including ApproxMC6 [37,36,46] and GANAK [34], can provide approximate model counts for SAT problems. Nevertheless, the majority of these tools lack reliable support for XOR clauses. Consequently, we continue to employ CryptoMiniSat to complete the multiple-solution-seeking work.

proach is iterated 100 times for each fixed key to ensure the randomness of the plaintext pairs. Based on the theoretical remaining probability of 2^{-42}, it may be deduced that the test is anticipated to provide an average of two right pairs. The average number of right pairs in the test across all 1000 keys is 2.05, which closely aligns with the theoretically projected result. Figure 6(a) illustrates the distribution of the average number of right pairs across various keys, which approximately conforms to a Poisson distribution with a parameter value of two. This finding agrees with the conclusion presented by Daemen and Rijmen [17].


(a) Simulated statistical tests with 21 input bits being fixed.

(b) Simulated statistical tests with 20 input bits being fixed.

(c) Simulated statistical tests with 19 input bits being fixed.

Fig. 6. Frequency distributions of the average number of right pairs in the tests.

Figures 6(b) and 6(c) show results with 20 bits and 19 bits randomly fixed in the simulated statistical tests, and the average number of right pairs is around four and eight, respectively. At the same time, both distributions closely resemble Poisson distributions with parameters of four and eight, respectively. Therefore, the three tests demonstrate a consistent statistical pattern regarding the remaining probability of the 8-round related-key differential characteristic for `GIFT-64`. Any of the three outcomes may be used as evidence to demonstrate that the remaining probability is 2^{-42}. Conversely, the three tests have varying runtimes. The test using 21 randomly fixed bits requires around 33363.91 seconds, but the tests involving 20 and 19 fixed bits take approximately 63953.42 seconds and 144684.48 seconds, respectively. This circumstance aligns with our instinctive perception since the test with fewer fixed bits corresponds to a typical statistical test with more plaintext pairs. Considering the consistent performance of these tests, the number of fixed bits ψ is consistently maintained at $n + \log_2(\tilde{p}) - 1$ in the subsequent applications. In this case, $\tilde{p}$ represents the estimated remaining probability derived by integrating the information from the initial two stages. Put another way, we always anticipate that there will be two right pairs on average during the test.

Finally, the test's runtime demonstrates the benefit of using simulated statistical tests with the SAT solver. The time required to complete an actual statistical test with 2^{43} randomly chosen pairs for a single fixed key is approximately 746.89 hours, but employing the simulated statistical test takes only 33.37 seconds. Regrettably, the simulated statistical tests are not always practicable on account of the limited capabilities of the SAT solver. In the following instances, we see that conducting a simulated test for `GIFT-64` is always feasible. However, for primitives with block sizes of 128 bits, the simulated statistical test is only doable in exceptional circumstances. This limitation is comprehensible, as it is nearly impracticable to execute real statistical testing for primitives with extensive states.

6 Evaluation of Differential Characteristics of GIFT

This section focuses on checking the differential characteristics of GIFT. Recall that the method for detecting linearised nonlinear constraints introduced in Section 4.3 is efficient for primitives employing S-boxes with a differential uniformity of four. Due to the S-box of GIFT having a differential uniformity of six, the detection technique for characteristics of GIFT with active S-boxes having six right pairs necessitates specific handling.

We use differential propagation $\texttt{0x4} \xrightarrow{GS} \texttt{0x7}$ as an example; the set of right-pair inputs for this propagation is $\mathcal{B} = \{\texttt{0x0}, \texttt{0x2}, \texttt{0x4}, \texttt{0x6}, \texttt{0x8}, \texttt{0xc}\}$. While $\mathcal{B}$ is not an affine subspace of $\mathbb{F}_2^4$, it may be partitioned into two affine subspaces, $\mathcal{A}_1 = \{\texttt{0x0}, \texttt{0x2}, \texttt{0x4}, \texttt{0x6}\}$ and $\mathcal{A}_2 = \{\texttt{0x0}, \texttt{0x4}, \texttt{0x8}, \texttt{0xc}\}$. Assume that the objective differential characteristic contains an active S-box with propagation $\texttt{0x4} \xrightarrow{GS} \texttt{0x7}$. For the right pair of the differential characteristic, the input value at the input of this S-box must belong to at least one set of $\mathcal{A}_1$ and $\mathcal{A}_2$. We apply the linearisation method twice to the specified differential characteristics. In the first test, we limit the input set for the S-box with propagation $\texttt{0x4} \xrightarrow{GS} \texttt{0x7}$ to the affine space $\mathcal{A}_1$. In the second test, we restrict it to the affine space $\mathcal{A}_2$. If the right key space identified in the initial test is $\mathbb{K}_1$ and the right key space identified in the second test is $\mathbb{K}_2$, then the right key space for the provided differential characteristic should be $\mathbb{K}_1 \cup \mathbb{K}_2$. The calculation of the remaining probability is intricate and needs to be computed separately for the keys in $\mathbb{K}_1 \backslash \mathbb{K}_2$, $\mathbb{K}_2 \backslash \mathbb{K}_1$, and $\mathbb{K}_1 \cap \mathbb{K}_2$.

6.1 Precise Examination of Differential Characteristics of GIFT-64

To determine if there are linearised nonlinear constraints in other differential characteristics of GIFT-64, we examine 24 differential characteristics of GIFT-64 from [48,50,51,14,13,24,22,42,41]. Our investigation reveals that four of these characteristics possess linearised nonlinear constraints. These constraints are present in two differential characteristics in the single-key (SK) setting and two differential characteristics in the related-key (RK) setting. The three-stage evaluation technique described in Section 5 is employed to assess the four differential characteristics. A summary of the test results can be found in Table 3.

Table 4 provides the identified linear and linearised nonlinear constraints for verification purposes. Since the 18-round related-key differential characteristic in [41] has no further constraints beyond those mentioned in Table 2, there is no need to repeat the enumeration. We can confidently conclude that the four differential characteristics have no unknown constraints based on the test results.

It is important to note that the right key spaces of the four differential characteristics do not cover the entire key space, and the remaining probabilities do

Table 3. Test results for four differential characteristics of `GIFT-64`.

Attack	Round	Probability	Stage 1			Stage 2		State 3		Key space	Remaining probability	Ref.
			LCs	LNCs	Max	Keys	Time	Keys	Time			
SK	10	2^{-57}	2	3	5	10^6	8.38h	1000	378.69h	2^{-5}	2^{-52}	[48]
SK	12	2^{-60}	3	1	8	10^5	399.16h	10	1589.74h	2^{-4}	2^{-56}	[14]
RK	12	2^{-37}	1	1	4	10^6	3.12h	20	326.14h	2^{-2}	2^{-35}	[13]
RK	18	2^{-58}	6	2	6	10^6	55.59h	10	130.95h	2^{-8}	2^{-50}	[41]

LCs: The number of linear constraints. LNCs: The number of linearised nonlinear constraints.
Max: Maximum length of linearised nonlinear constraints.
Keys: The number of keys selected from the right key space during Stage 2 or Stage 3 of the verification process.
Time: The cumulative execution time for Stage 2 or Stage 3.
Key space: Ratio of the size of the right key space to the whole key space.
Remaining probability: Remaining probability of the differential characteristic that is not influenced by the key.

not equal the stated probabilities. Therefore, the differential attacks relying on these distinguishers require a reassessment. Notably, the 12-round differential characteristic in [14] contains the longest linearised nonlinear constraint, encompassing eight rounds. Furthermore, the average cost of the simulated statistical test using 2^{57} pairs of plaintexts for a single fixed key is 158.97 hours due to this differential characteristic's very low remaining probability. However, the simulated statistical test utilising the SAT solver is significantly more efficient than the traditional one.

Table 4. Constraints in differential characteristics for `GIFT-64`.

<table>
<tr><th>Ref.</th><th>Round</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th></tr>
<tr><td rowspan="4">[48]</td><td>LC</td><td>-</td><td>-</td><td>-</td><td>$k_{20} \oplus k_{28} = 0$</td><td>-</td><td>-</td><td>-</td><td>$k_{23} \oplus k_{31} = 0$</td><td>-</td><td>-</td><td rowspan="4" colspan="2">-</td></tr>
<tr><td rowspan="3">LNC</td><td>-</td><td colspan="4">$k_{20} \oplus k_{49} \oplus k_{51} \oplus k_{94} = 1$</td><td colspan="5">-</td></tr>
<tr><td>-</td><td colspan="5">$k_{30} \oplus k_{49} \oplus k_{94} \oplus k_{109} \oplus c_5^4 = 1$</td><td colspan="4">-</td></tr>
<tr><td colspan="3">-</td><td colspan="6">$k_{20} \oplus k_{31} \oplus k_{48} \oplus k_{50} \oplus k_{65} \oplus k_{73} \oplus c_3^4 \oplus c_5^4 = 1$</td><td>-</td></tr>
<tr><td rowspan="2">[14]</td><td>LC</td><td>-</td><td>$k_{86} \oplus k_{94} = 0$</td><td>-</td><td>$k_{23} \oplus k_{31} = 0$</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>$k_{86} \oplus k_{94} = 0$</td><td>-</td><td>-</td></tr>
<tr><td>LNC</td><td colspan="3">-</td><td colspan="8">$k_2 \oplus k_{10} \oplus k_{31} \oplus k_{52} \oplus k_{54} \oplus k_{64} \oplus k_{72} \oplus k_{86} \oplus k_{103} \oplus k_{105} \oplus k_{113} \oplus k_{115} = 1$</td><td>-</td></tr>
<tr><td rowspan="2">[13]</td><td>LC</td><td>-</td><td>-</td><td>-</td><td>-</td><td>$k_{112} = 1$</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>LNC</td><td colspan="4">-</td><td colspan="4">$k_{50} \oplus k_{92} \oplus k_{95} \oplus k_{110} \oplus c_4^6 = 1$</td><td colspan="4">-</td></tr>
</table>

LC: Linear constraints. LNC: Linearised nonlinear constraints.

6.2 Evaluation of Differential Characteristics of GIFT-128

Regarding GIFT-128, we check 18 differential characteristics in [51,13,25,24,22,52] and determine that six of these characteristics exhibit linearised nonlinear constraints. A summary of the information regarding these characteristics can be found in Table 5. Because the SAT solver has limited solution capability, detecting potential constraints or conducting simulated statistical tests for these characteristics is not feasible. Due to the possibility of undiscovered constraints, the key space specified in Table 5 is the maximum ratio between the right key space and the whole key space.

Table 5. Detailed test results on the six differential characteristics of GIFT-128.

Round	Probability	LCs	LNCs	Max	Maximum key space	Ref.
18	2^{-109}	6	1	5	0	Table 10 in [51]
20	$2^{-122.415}$	5	2	5	2^{-7}	Trail 2 of Table 11 in [22]
20	$2^{-122.415}$	5	2	5	2^{-7}	Trail 3 of Table 11 in [22]
20	$2^{-123.415}$	5	4	5	2^{-9}	Trail 4 of Table 11 in [22]
20	2^{-124}	6	1	5	2^{-7}	Trail 1 of Table 8 in [52]
20	2^{-124}	6	1	5	2^{-7}	Trail 2 of Table 8 in [52]

LCs: The number of linear constraints. LNCs: The number of linearised nonlinear constraints.
Max: Maximum length of linearised nonlinear constraints.

For verification, the identified linear and linearised nonlinear constraints are presented in Table 6. Peyrin and Tan [29] have determined that the 18-round differential characteristic described in [51] is infeasible. After conducting a reassessment, we find that the differential characteristic is affected by one linearised nonlinear constraint in addition to six linear constraints. This discovery in no way alters the practical impracticability of the differential characteristic. However, it indicates that the linearised nonlinear constraints are not singular instances in GIFT-64.

Due to the identical input and output differences, the three 20-round differential characteristics in [22] are encompassed within the same differential. Ji *et al.* [22] increase the probability of the differential by utilising the clustering effect and then launch a 26-round differential attack against GIFT-128. Our analysis demonstrates that while the linear constraints of the three differential characteristics are the same, their linearised nonlinear constraints differ. Therefore, a comprehensive reevaluation of the validity of the differential attack based on the differential is necessary.

The two 20-round differential characteristics, each with a probability of 2^{-124} in [52], are present in the same differential. According to Zong *et al.* [52], the differential contains six additional characteristics with probabilities below 2^{-124}.

The differential is employed to initiate a 27-round differential attack on `GIFT-128`, which, to our knowledge, is the most effective differential attack on the cipher. Upon analysis, we observe that the linear constraints for the two given differential characteristics in the seventeenth round are distinct, as indicated in Table 6. This observation suggests that the two differential characteristics with the highest probability cannot hold simultaneously for keys even in the right key space. One of the two differential characteristics will be impossible, for instance, if the values of k_4 and k_{92} are set to $k_4 = k_{92} = 1$ or $k_4 = 1$ and $k_{92} = 0$. When the six remaining differential characteristics are considered, the estimation of the right key space and the remaining probability of the differential will become more complicated. Therefore, it is necessary to do a comprehensive reanalysis of the viability of the 27-round differential attack.

Table 6. Constraints in differential characteristics of `GIFT-128`.

<table>
<tr><td colspan="16">Constraints of 18-round differential characteristic in [51]</td></tr>
<tr><td>Ref.</td><td>Round</td><td>0-4</td><td>5</td><td colspan="2">6-9</td><td>10</td><td colspan="3">11-12</td><td>13</td><td>14</td><td>15</td><td>16</td><td colspan="2">17</td></tr>
<tr><td rowspan="3">Table 10</td><td rowspan="2">LC</td><td rowspan="2">-</td><td rowspan="2">$k_4 \oplus k_{26} = 0$</td><td colspan="2" rowspan="2">-</td><td>$k_{96} \oplus k_{114} = 0$</td><td colspan="3" rowspan="2">-</td><td rowspan="2">$k_4 = 1$</td><td colspan="2" rowspan="2">-</td><td>$c_4^{16} = 0$</td><td colspan="2" rowspan="2">-</td></tr>
<tr><td>$k_{110} \oplus k_{112} = 0$</td><td>$0 = 1$</td></tr>
<tr><td>LNC</td><td colspan="4">-</td><td colspan="6">$k_5 \oplus k_9 \oplus k_{110} = 1$</td><td colspan="4">-</td></tr>
<tr><td colspan="16">Constraints of 20-round differential characteristics in [22]</td></tr>
<tr><td>Ref.</td><td>Round</td><td>0-3</td><td>4</td><td>5-6</td><td>7-8</td><td>9</td><td>10</td><td>11</td><td>12-13</td><td>14</td><td>15</td><td colspan="4">16-19</td></tr>
<tr><td rowspan="4">Trail 2 of Table 11</td><td rowspan="2">LC</td><td rowspan="2">-</td><td rowspan="2">$k_{32} \oplus k_{54} = 0$</td><td rowspan="2">-</td><td rowspan="2">-</td><td>$k_4 \oplus k_{16} = 0$</td><td rowspan="2">-</td><td rowspan="2">-</td><td rowspan="2">-</td><td>$k_{104} \oplus k_{112} = 0$</td><td rowspan="2">-</td><td colspan="4" rowspan="2">-</td></tr>
<tr><td>$k_6 \oplus k_{18} = 0$</td><td>$k_{106} \oplus k_{114} = 0$</td></tr>
<tr><td rowspan="2">LNC</td><td>-</td><td colspan="3">$k_{54} \oplus k_{80} \oplus k_{92} = 1$</td><td colspan="10">-</td></tr>
<tr><td colspan="3">-</td><td colspan="3">$k_6 \oplus k_{73} = 0$</td><td colspan="8">-</td></tr>
<tr><td rowspan="4">Trail 3 of Table 11</td><td rowspan="2">LC</td><td rowspan="2">-</td><td rowspan="2">$k_{32} \oplus k_{54} = 0$</td><td rowspan="2">-</td><td rowspan="2">-</td><td>$k_4 \oplus k_{16} = 0$</td><td rowspan="2">-</td><td rowspan="2">-</td><td rowspan="2">-</td><td>$k_{104} \oplus k_{112} = 0$</td><td rowspan="2">-</td><td colspan="4" rowspan="2">-</td></tr>
<tr><td>$k_6 \oplus k_{18} = 0$</td><td>$k_{106} \oplus k_{114} = 0$</td></tr>
<tr><td rowspan="2">LNC</td><td colspan="4">-</td><td colspan="4">$k_{18} \oplus k_{50} \oplus k_{54} = 0$</td><td colspan="6">-</td></tr>
<tr><td colspan="7">-</td><td colspan="3">$k_{35} \oplus k_{114} = 1$</td><td colspan="4">-</td></tr>
<tr><td rowspan="6">Trail 4 of Table 11</td><td rowspan="2">LC</td><td rowspan="2">-</td><td rowspan="2">$k_{32} \oplus k_{54} = 0$</td><td rowspan="2">-</td><td rowspan="2">-</td><td>$k_4 \oplus k_{16} = 0$</td><td rowspan="2">-</td><td rowspan="2">-</td><td rowspan="2">-</td><td>$k_{104} \oplus k_{112} = 0$</td><td rowspan="2">-</td><td colspan="4" rowspan="2">-</td></tr>
<tr><td>$k_6 \oplus k_{18} = 0$</td><td>$k_{106} \oplus k_{114} = 0$</td></tr>
<tr><td rowspan="4">LNC</td><td>-</td><td colspan="3">$k_{54} \oplus k_{80} \oplus k_{92} = 1$</td><td colspan="10">-</td></tr>
<tr><td colspan="3">-</td><td colspan="3">$k_6 \oplus k_{73} = 0$</td><td colspan="8">-</td></tr>
<tr><td colspan="4">-</td><td colspan="4">$k_{18} \oplus k_{50} \oplus k_{54} = 0$</td><td colspan="6">-</td></tr>
<tr><td colspan="7">-</td><td colspan="3">$k_{35} \oplus k_{114} = 1$</td><td colspan="4">-</td></tr>
<tr><td colspan="16">Constraints of 20-round differential characteristics in [52]</td></tr>
<tr><td>Ref.</td><td>Round</td><td>0-3</td><td>4</td><td colspan="2">5-8</td><td>9</td><td colspan="3">10-13</td><td>14</td><td colspan="2">15-16</td><td>17</td><td>18</td><td>19</td></tr>
<tr><td rowspan="3">Trail 1 of Table 8</td><td rowspan="2">LC</td><td rowspan="2">-</td><td rowspan="2">$k_{32} \oplus k_{54} = 0$</td><td colspan="2" rowspan="2">-</td><td>$k_4 \oplus k_{16} = 0$</td><td colspan="3" rowspan="2">-</td><td>$k_{104} \oplus k_{112} = 0$</td><td colspan="2" rowspan="2">-</td><td rowspan="2">$k_{92} = 1$</td><td rowspan="2">-</td><td rowspan="2">-</td></tr>
<tr><td>$k_6 \oplus k_{18} = 0$</td><td>$k_{106} \oplus k_{114} = 0$</td></tr>
<tr><td>LNC</td><td colspan="8">-</td><td colspan="5">$k_2 \oplus k_4 \oplus k_6 \oplus k_{104} = 1$</td><td>-</td></tr>
<tr><td rowspan="3">Trail 2 of Table 8</td><td rowspan="2">LC</td><td rowspan="2">-</td><td rowspan="2">$k_{32} \oplus k_{54} = 0$</td><td colspan="2" rowspan="2">-</td><td>$k_4 \oplus k_{16} = 0$</td><td colspan="3" rowspan="2">-</td><td>$k_{104} \oplus k_{112} = 0$</td><td colspan="2" rowspan="2">-</td><td rowspan="2">$k_4 \oplus k_{92} = 1$</td><td rowspan="2">-</td><td rowspan="2">-</td></tr>
<tr><td>$k_6 \oplus k_{18} = 0$</td><td>$k_{106} \oplus k_{114} = 0$</td></tr>
<tr><td>LNC</td><td colspan="8">-</td><td colspan="5">$k_2 \oplus k_4 \oplus k_6 \oplus k_{104} = 1$</td><td>-</td></tr>
</table>

7 Applications in Other Cryptographic Primitives

Section 6 demonstrates that the linearised nonlinear constraints typically occur in the differential characteristics of GIFT, a cipher built on SPN with a reasonably uncomplicated linear layer. This section will show that linearised nonlinear constraints are also present in the SPN cipher with a relatively complex linear layer. Furthermore, the linearisation method proposed in Section 4.3 can be employed to identify linear constraints in differential characteristics of ciphers that employ the Generalised Feistel Network (GFN). We will utilise SKINNY-64 and WARP as examples.

7.1 Linearised Nonlinear Constraints in SKINNY-64

The SKINNY [6] family of tweakable block ciphers adheres to the TWEAKEY framework [21], which accepts a tweakey input instead of a key. There are two suggested block sizes with $n = 64$ or 128. Given that the 64-bit version, referred to as SKINNY-64, utilises S-boxes with a differential uniformity of four, our main objective is to identify linearised nonlinear constraints inside its differential characteristics. The state of SKINNY-64 can be represented as a 4×4 array, with each cell representing a nibble. The tweakey is available in three sizes: $t = 64$, 128, and 192. The corresponding ciphers are denoted as SKINNY-64-64, SKINNY-64-128, and SKINNY-64-192. The tweakey state is also considered as a collection of 4×4 square arrays. These arrays are designated as $TK1$ when $t = 64$, $TK1$ and $TK2$ when $t = 128$, and $TK1$, $TK2$ and $TK3$ when $t = 192$.

The round function consists of five operations: SubCells (SC), AddConstants (AC), AddRoundTweakey (ART), ShiftRows (SR) and MixColumns (MC). SKINNY-64 deploys an entirely linear tweakey schedule. A permutation P_T is applied to each array of tweakey to interchange the places of each cell. Subsequently, the contents of each cell in the initial two rows of $TK2$ and $TK3$ are refreshed using two LFSRs, namely $\mathtt{LFSR}_2$ and $\mathtt{LFSR}_3$, respectively. An illustration of the round function and tweakey schedule can be found in Appendix D. For further details on the specifications of SKINNY-64, see [6].

In contrast to the frequency of occurrence of linearised nonlinear constraints in differential characteristics of GIFT, the frequency of occurrence of linearised nonlinear constraints in differential characteristics of SKINNY-64 is relatively low. We analysed all (related-key) differential characteristics of SKINNY-64, including those short-round differential characteristics used in boomerang and rectangle attacks, in [47,35,32,18,19,31]. Our analysis reveals that out of all these characteristics, only the 11-round differential characteristic of SKINNY-64-192 in [47] exhibits linearised nonlinear constraints. We provide an example of one of the identified linearised nonlinear constraints in Appendix D.

Remark 2. The 11-round differential characteristic of SKINNY-64-192 in [47] is an infeasible differential characteristic due to the existence of conflicting linear constraints.

7.2 Linear Constraints in WARP

WARP [3] is a cipher that operates on 128-bit blocks and uses a 128-bit key. It is constructed using a 32-branch Type 2 GFN [49]. It employs a straightforward key schedule that initially partitions the master key K into two 64-bit round keys, denoted as $K = K^0 \| K^1$. K^0 and K^1 are also represented as 16 nibbles, namely $K^0 = K^0[0] \| K^0[1] \| \cdots \| K^0[15]$ and $K^1 = K^1[0] \| K^1[1] \| \cdots \| K^1[15]$. The round key $K^{r \bmod 2}$ is used in the r-th round function. The input state X^r of the r-th round is partitioned into 32 nibbles, denoted as $X^r = X^r[0] \| X^r[1] \| \cdots \| X^r[31]$. When examining the state X^r and master key K at the bit level, we represent the i-th bit of X^r and K as X^r_i and K_i, respectively, where $0 \leqslant i \leqslant 127$.

The round function of WARP comprises a 4-bit S-box, XOR operations, and a shuffle operation π that is applied to 32 nibbles. Additionally, it employs round constants based on LFSR. Before applying π in the r-th round, the first and third nibbles of the state are XORed with two 4-bit constants $RC^r[0]$ and $RC^r[1]$. Figure 7 gives an illustration of the round function. See [3] for additional information regarding the cipher.

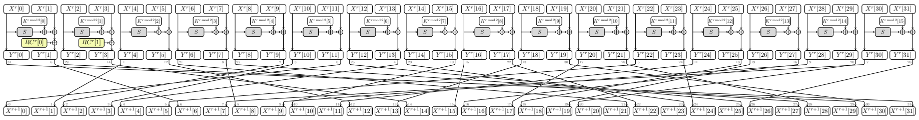

$X^r[0]$ … $X^r[31]$
$K^{r \bmod 2}[0]$ … $K^{r \bmod 2}[15]$
S
$RC^r[0]$
$RC^r[1]$
$Y^r[0]$ … $Y^r[31]$
$X^{r+1}[0]$ … $X^{r+1}[31]$

Fig. 7. Round function of WARP.

Contrary to the direct linkage between the output y^i of the nonlinear component in the i-th round and the input x^{i+1} of the nonlinear component in the $(i+1)$-th round, as seen in Figure 2 for SPN ciphers, GFN ciphers incorporate extra internal states in these linkages. In GFN ciphers, the linear constraint should include input values for nonlinear components in both the $(i-1)$-th and $(i+1)$-th rounds, in addition to the output $y^i[*]$ of the nonlinear component in the i-th round, as illustrated in Figure 8. The actual situation may be more intricate, and linear constraints in GFN ciphers may also encompass numerous rounds. Therefore, the earlier research based on the value restriction to find linear constraints [16,27,12,43,26] does not concern GFN ciphers.

Given that the detection technique presented in Section 4.3 establishes a link between states from several rounds, it may be applied to identify linear constraints in GFN ciphers. We evaluate some differential characteristics of differentials for WARP from 1-round to 20-round in [44]. When the number of rounds exceeds 13, as noted in [44], the number of differential characteristics in the differential increases exceptionally quickly. We exclusively evaluate the differential characteristics of each differential that has the optimised differential probability. Nevertheless, the number of optimal differential characteristics is huge for differentials that span more than 16 rounds. For these differentials, we analyse only 10000 characteristics from all optimal characteristics. The test results suggest that linear constraints are absent in differential characteristics that cover

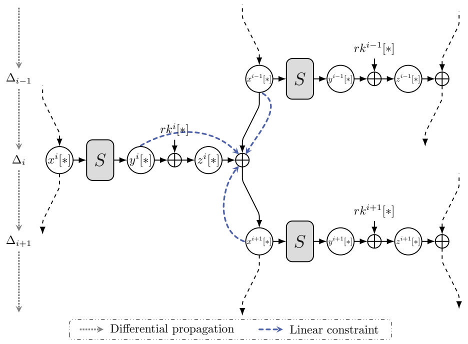


Fig. 8. Visual representation of linear constraints in GFN ciphers.

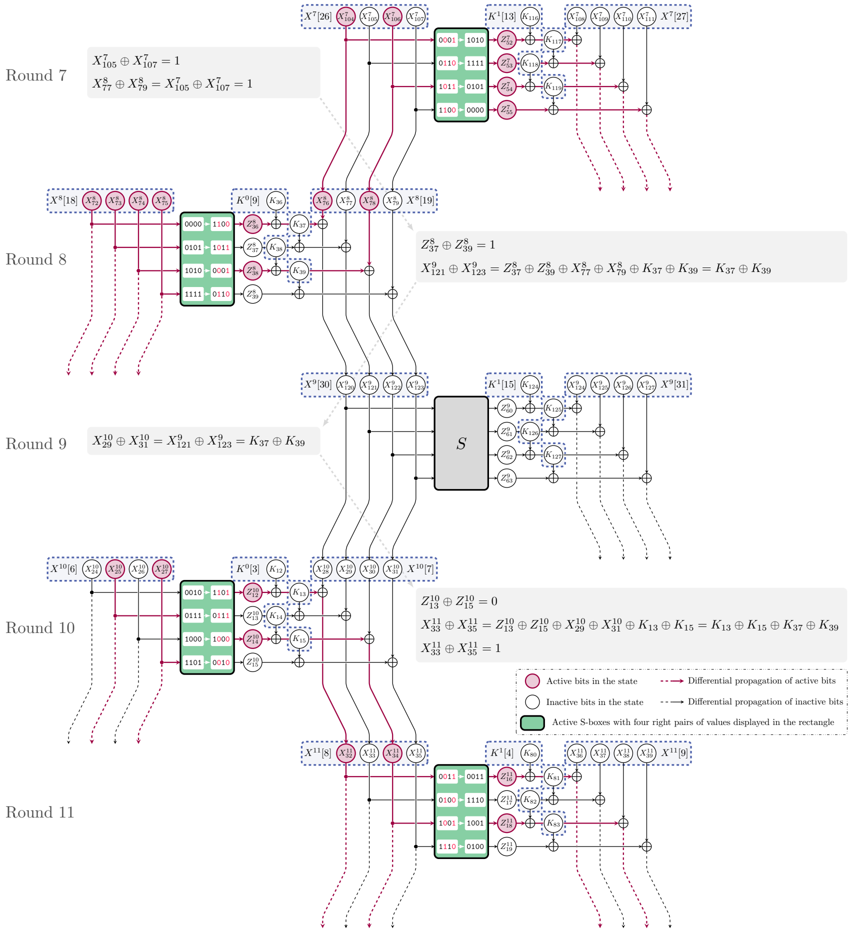
13 or fewer rounds. In contrast, linear constraints are present in all characteristics covering 14 or more rounds. Table 7 summarises test results for differential characteristics with 14 or more rounds.

Table 7. Summary of linear constraints in differential characteristics of `WARP`.

Round	Probability	`#{DC}`	Minimum LCs	`#{DC`$_{\texttt{min}}$`}`	Maximum LCs	`#{DC`$_{\texttt{max}}$`}`
14	2^{-80}	64	1	48	2	16
15	2^{-94}	352	1	32	2	320
16	2^{-104}	2080	4	160	5	1920
17	2^{-114}	10000	5	5938	7	245
18	2^{-122}	10000	4	355	8	218
19	2^{-132}	10000	4	3056	6	2006
20	2^{-140}	10000	10	91	17	12

`#{DC}`: The quantity of examined differential characteristics.
Minimum LCs: The minimum number of linear constraints in differential characteristics.
`#{DC`$_{\texttt{min}}$`}`: The quantity of differential characteristics with the least amount of linear constraints.
Maximum LCs: The maximum number of linear constraints in differential characteristics.
`#{DC`$_{\texttt{max}}$`}`: The quantity of differential characteristics with the greatest amount of linear constraints.

A 17-round differential characteristic with five linear constraints is chosen as an example, and additional details are provided. Appendix E contains more details about the 17-round differential characteristic, and Table 8 lists the associated linear constraints. Four linear constraints encompass three rounds of encryption, and one encompasses five rounds of encryption. The S-boxes involved in the linear constraint $K_{13} \oplus K_{15} \oplus K_{37} \oplus K_{39} = 1$ spanning five rounds are highlighted with blue rectangles in the differential characteristics shown in Figure 16. An explanation of the 5-round linear constraint can be seen in Figure 9.



Round 7
Round 8
Round 9
Round 10
Round 11
S
Active bits in the state
Inactive bits in the state
Differential propagation of active bits
Differential propagation of inactive bits
Active S-boxes with four right pairs of values displayed in the rectangle

$X^7_{105} \oplus X^7_{107} = 1$

$X^8_{77} \oplus X^8_{79} = X^7_{105} \oplus X^7_{107} = 1$

$Z^8_{37} \oplus Z^8_{39} = 1$

$X^9_{121} \oplus X^9_{123} = Z^8_{37} \oplus Z^8_{39} \oplus X^8_{77} \oplus X^8_{79} \oplus K_{37} \oplus K_{39} = K_{37} \oplus K_{39}$

$X^{10}_{29} \oplus X^{10}_{31} = X^9_{121} \oplus X^9_{123} = K_{37} \oplus K_{39}$

$Z^{10}_{13} \oplus Z^{10}_{15} = 0$

$X^{11}_{33} \oplus X^{11}_{35} = Z^{10}_{13} \oplus Z^{10}_{15} \oplus X^{10}_{29} \oplus X^{10}_{31} \oplus K_{13} \oplus K_{15} = K_{13} \oplus K_{15} \oplus K_{37} \oplus K_{39}$

$X^{11}_{33} \oplus X^{11}_{35} = 1$

Fig. 9. Linear constraint covering five rounds.

Table 8. Constraints in the 17-round differential characteristic of `WARP`.

Round	0-6	7	8	9	10	11	12	13	14	15-16
LC	-	$K_{13} \oplus K_{15} \oplus K_{37} \oplus K_{39} = 1$					-			
	-		$K_{89} \oplus K_{91} = 1$		-					
	-			$K_{48} \oplus K_{49} \oplus K_{50} = 1$			-			
	-			$K_{49} \oplus K_{51} = 1$			-			
	-						$K_{109} \oplus K_{111} = 1$			-

7.3 Nonlinear Constraints in WARP

Despite having blocks of the same size, while the number of rounds is fixed, WARP has just half the number of S-boxes compared to GIFT-128. Therefore, we are questioning the possibility of conducting tests on differential characteristics using the SAT solver mentioned in Section 5 for WARP, even though such tests are not practical for GIFT-128. We choose the 17-round characteristic in Figure 16 as our objective.

Considering that the linear constraints in the differential characteristics have already been derived, we generate 1000 keys at random that satisfy the five constraints outlined in Table 8. Each key undergoes individual validation using the SAT solver to see if it has right pairs of differential characteristics. As per the output of the SAT solver, the differential characteristic exhibits right pairs under 149 keys; however, the differential characteristic becomes infeasible for the remaining 851 keys. The test result indicates the presence of extra constraints in the 17-round differential characteristic.

In order to identify these unknown constraints, we select a key $\mathring{k}$ that lacks right pairs. Each of the 128 bits in $\mathring{k}$ is flipped individually, and we employ the SAT solver to validate the 128 transformed keys $\mathring{k}^0$, $\mathring{k}^1$, …, $\mathring{k}^{127}$. We speculate that the ℓ-th bit in the master key may be involved in unknown constraints if a specific modified key $\mathring{k}^\ell$ contains the right pairs. We may continue this process with various keys to find as many unknown constraints as feasible. Once we identify the key bits that may be included in unknown constraints, we observe the differential characteristic to determine the specific locations of these key bits and abstract the corresponding nonlinear constraint. This approach may also be utilised to seek unknown constraints for other primitives.

In this manner, we identify four nonlinear constraints in the 17-round differential characteristic. Due to the presence of inactive S-boxes, these constraints cannot be detected using the approach described in Section 4.3. Figure 10 depicts a nonlinear constraint that spans four rounds of encryption. The right pair of the differential characteristic must satisfy the condition that both $Z^{11}[9]$ and $X^{12}[30]$ should take values from the set $\{\texttt{0x3}, \texttt{0x4}, \texttt{0x9}, \texttt{0xe}\}$. Therefore, the values of $X^{10}[26]$ must be selected from the set $\mathcal{A}_{in} \oplus K^1[9]$, where $\mathcal{A}_{in} = \{\texttt{0x0}, \texttt{0x7}, \texttt{0xa}, \texttt{0xd}\}$, since it can be expressed as $X^{10}[26] = Z^{11}[9] \oplus X^{12}[30] \oplus K^1[9]$. On the other hand, we can confirm that $X^9[8] \in \{\texttt{0x0}, \texttt{0x5}, \texttt{0xa}, \texttt{0xf}\}$ and $X^{11}[16] \in \{\texttt{0x3}, \texttt{0x4}, \texttt{0x9}, \texttt{0xe}\}$. The equation $Z^{10}[13] = X^9[8] \oplus X^{11}[16] \oplus K^0[13]$ ensures that $Z^{10}[13]$ can only have values from $\mathcal{A}_{out} \oplus K^0[13]$, where $\mathcal{A}_{out} = \{\texttt{0x1}, \texttt{0x3}, \texttt{0x4}, \texttt{0x6}, \texttt{0x9}, \texttt{0xb}, \texttt{0xc}, \texttt{0xe}\}$. A nonlinear constraint on $K^0[13] \| K^1[9]$ is that the equation

$$S(x \oplus K^1[9]) = y \oplus K^0[13]$$

must have at least one solution when the values of x and y are taken from $\mathcal{A}_{in}$ and $\mathcal{A}_{out}$, respectively. To the best of our knowledge, we are the first to report nonlinear constraints in a cipher that employs the GFN structure.

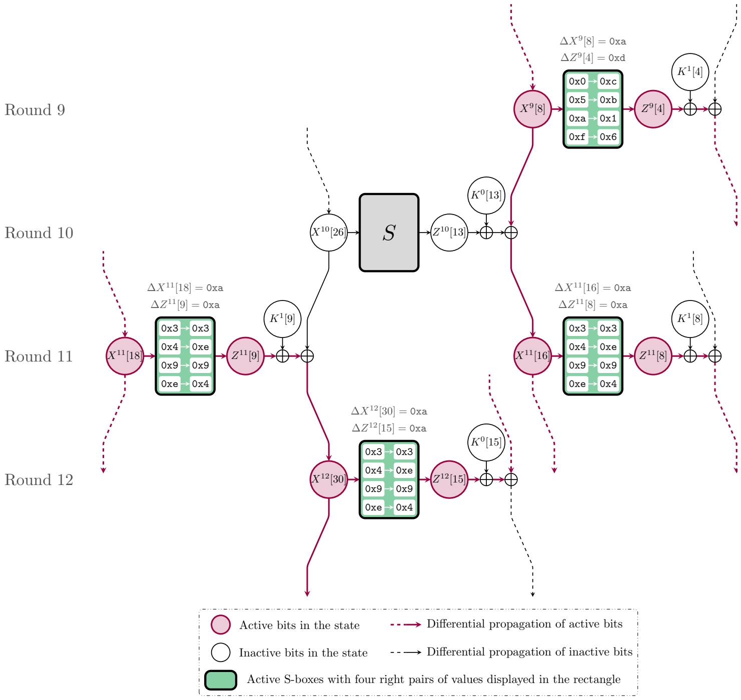

$\Delta X^{9}[8] = \texttt{0xa}$
$\Delta Z^{9}[4] = \texttt{0xd}$
$K^{1}[4]$
Round 9
$X^{9}[8]$
0x0 → 0xc
0x5 → 0xb
0xa → 0x1
0xf → 0x6
$Z^{9}[4]$
$K^{0}[13]$
Round 10
$X^{10}[26]$
S
$Z^{10}[13]$
$\Delta X^{11}[18] = \texttt{0xa}$
$\Delta Z^{11}[9] = \texttt{0xa}$
$K^{1}[9]$
$\Delta X^{11}[16] = \texttt{0xa}$
$\Delta Z^{11}[8] = \texttt{0xa}$
$K^{1}[8]$
Round 11
$X^{11}[18]$
0x3 → 0x3
0x4 → 0xe
0x9 → 0x9
0xe → 0x4
$Z^{11}[9]$
$X^{11}[16]$
0x3 → 0x3
0x4 → 0xe
0x9 → 0x9
0xe → 0x4
$Z^{11}[8]$
$\Delta X^{12}[30] = \texttt{0xa}$
$\Delta Z^{12}[15] = \texttt{0xa}$
$K^{0}[15]$
Round 12
$X^{12}[30]$
0x3 → 0x3
0x4 → 0xe
0x9 → 0x9
0xe → 0x4
$Z^{12}[15]$
Active bits in the state
Differential propagation of active bits
Inactive bits in the state
Differential propagation of inactive bits
Active S-boxes with four right pairs of values displayed in the rectangle

Fig. 10. Nonlinear constraint covering four rounds.

Remark 3. Some nonlinear constraints in the differential characteristics of `WARP` are intricate and nuanced. We do not exclude the possibility of additional uncategorised constraints.

8 Discussion and Conclusion

8.1 Discussion

We acknowledge that the theory of quasidifferential trails [7] is a comprehensive approach to addressing dependencies in differential characteristics, accounting for deterministic and probabilistic linear relations. The linearisation method proposed in Section 4 can only address deterministic linear relations. However, we believe that the unique aspects of our proposed approach, which we will discuss, are of irreplaceable significance.

- As Beyne and Rijmen [7] noted, Plateau characteristics originate from the propagation of affine subspaces made up of the input and output values of right pairs; nonetheless, performing the propagation for more than two rounds is challenging. The linearisation method offers a solution to the propagation of affine subspaces for more than two rounds.

- The linearisation method is intuitive because it uses value restrictions to elucidate dependencies. This intuitive nature makes it an intuitive interpretation of the theory of quasidifferential trails when the concentration is on deterministic linear relations. This intuition will further enhance the prosperity of the theory of quasidifferential trails and contribute to the increased awareness of the dependency issue.
- As stated in Section 3.2, using the quasidifferential trails theory in primitives containing 8-bit S-boxes may provide a possible challenge. Given that the linearisation method does not depend on any mathematical problem solvers, it is practicable to apply it to primitives with 8-bit S-boxes. We employ the linearisation method to identify constraints in the 19-round differential characteristic of SMS4 in [39]. The test results indicate no linearised nonlinear constraint in this differential characteristic, and it takes less than one second to complete.
- In the context of a specific differential characteristic, many quasidifferential trails can exhibit an absolute correlation lower than that of the associated differential characteristic. Analysing probabilistic linear relations arising from these quasidifferential trails can be complicated. In this scenario, the three-stage evaluation approach in Section 5 may serve as an alternative approach.
- Over the last twenty years, we have witnessed the automatic method used to conduct key recovery attacks in cryptanalysis and find various distinguishers. In this work, we suggest a novel application of the automatic method: simulating the statistical test. We believe it has independent interests.

8.2 Conclusion

This work offers a comprehensive overview of prior research on dependencies in differential characteristics. By classifying all dependence representations from the value restrictions and the theory of quasidifferential trails, we identify a specific set of nonlinear constraints and refer to them as linearised nonlinear constraints. We aim to establish a method that utilises value restriction to identify linearised nonlinear constraints, as the previous method is insufficient for this purpose. Leveraging linear dependencies between the inputs and outputs of active S-boxes, a linearisation method is proposed to search for linearised nonlinear constraints for a given differential characteristic. Then, we propose a three-stage evaluation approach based on the linearisation method to better assess differential characteristics with linearised nonlinear constraints. The linearisation method and the three-stage evaluation approach are used to examine four differential characteristics of `GIFT-64` and six differential characteristics of `GIFT-128`. Given the inconsistencies identified in these differential characteristics, we strongly recommend reevaluating the differential attacks that rely on these distinguishers. Determining linear and nonlinear constraints in GFN ciphers is also possible using the newly proposed methods. We examine the differential characteristics of `WARP` as an illustration and present the first-known nonlinear constraint in GFN ciphers.

References

1. Abdelkhalek, A., Sasaki, Y., Todo, Y., Tolba, M., Youssef, A.M.: MILP modeling for (large) s-boxes to optimize probability of differential characteristics. IACR Trans. Symm. Cryptol. **2017**(4), 99–129 (2017). https://doi.org/10.13154/tosc.v2017.i4.99-129
2. Ankele, R., Kölbl, S.: Mind the gap - A closer look at the security of block ciphers against differential cryptanalysis. In: Cid, C., Jacobson Jr:, M.J. (eds.) SAC 2018. LNCS, vol. 11349, pp. 163–190. Springer, Heidelberg (Aug 2019). https://doi.org/10.1007/978-3-030-10970-7_8
3. Banik, S., Bao, Z., Isobe, T., Kubo, H., Liu, F., Minematsu, K., Sakamoto, K., Shibata, N., Shigeri, M.: WARP : Revisiting GFN for lightweight 128-bit block cipher. In: Dunkelman, O., Jr., M.J.J., O'Flynn, C. (eds.) SAC 2020. LNCS, vol. 12804, pp. 535–564. Springer, Heidelberg (Oct 2020). https://doi.org/10.1007/978-3-030-81652-0_21
4. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: A small present - towards reaching the limit of lightweight encryption. In: Fischer, W., Homma, N. (eds.) CHES 2017. LNCS, vol. 10529, pp. 321–345. Springer, Heidelberg (Sep 2017). https://doi.org/10.1007/978-3-319-66787-4_16
5. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404 (2013), https://eprint.iacr.org/2013/404
6. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 123–153. Springer, Heidelberg (Aug 2016). https://doi.org/10.1007/978-3-662-53008-5_5
7. Beyne, T., Rijmen, V.: Differential cryptanalysis in the fixed-key model. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022, Part III. LNCS, vol. 13509, pp. 687–716. Springer, Heidelberg (Aug 2022). https://doi.org/10.1007/978-3-031-15982-4_23
8. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO'90. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (Aug 1991). https://doi.org/10.1007/3-540-38424-3_1
9. Boura, C., Coggia, D.: Efficient MILP modelings for sboxes and linear layers of SPN ciphers. IACR Trans. Symm. Cryptol. **2020**(3), 327–361 (2020). https://doi.org/10.13154/tosc.v2020.i3.327-361
10. 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
11. Canale, F., Naya-Plasencia, M.: Guessing less and better: Improved attacks on GIFT-64. IACR Cryptol. ePrint Arch. p. 354 (2023), https://eprint.iacr.org/2023/354
12. Canteaut, A., Lambooij, E., Neves, S., Rasoolzadeh, S., Sasaki, Y., Stevens, M.: Refined probability of differential characteristics including dependency between

multiple rounds. IACR Trans. Symm. Cryptol. **2017**(2), 203–227 (2017). https://doi.org/10.13154/tosc.v2017.i2.203-227

13. Cao, M., Zhang, W.: Related-key differential cryptanalysis of the reduced-round block cipher GIFT. IEEE Access **7**, 175769–175778 (2019). https://doi.org/10.1109/ACCESS.2019.2957581
14. Chen, H., Zong, R., Dong, X.: Improved differential attacks on GIFT-64. In: Zhou, J., Luo, X., Shen, Q., Xu, Z. (eds.) ICICS 19. LNCS, vol. 11999, pp. 447–462. Springer, Heidelberg (Dec 2019). https://doi.org/10.1007/978-3-030-41579-2_26
15. Daemen, J., Govaerts, R., Vandewalle, J.: Correlation matrices. In: Preneel, B. (ed.) FSE'94. LNCS, vol. 1008, pp. 275–285. Springer, Heidelberg (Dec 1995). https://doi.org/10.1007/3-540-60590-8_21
16. Daemen, J., Rijmen, V.: Plateau characteristics. IET Inf. Secur. **1**(1), 11–17 (2007). https://doi.org/10.1049/IET-IFS:20060099
17. Daemen, J., Rijmen, V.: Probability distributions of correlation and differentials in block ciphers. J. Math. Cryptol. **1**(3), 221–242 (2007). https://doi.org/10.1515/JMC.2007.011
18. Delaune, S., Derbez, P., Huynh, P., Minier, M., Mollimard, V., Prud'homme, C.: Efficient methods to search for best differential characteristics on SKINNY. In: Sako, K., Tippenhauer, N.O. (eds.) ACNS 21, Part II. LNCS, vol. 12727, pp. 184–207. Springer, Heidelberg (Jun 2021). https://doi.org/10.1007/978-3-030-78375-4_8
19. Dong, X., Qin, L., Sun, S., Wang, X.: Key guessing strategies for linear key-schedule algorithms in rectangle attacks. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022, Part III. LNCS, vol. 13277, pp. 3–33. Springer, Heidelberg (May / Jun 2022). https://doi.org/10.1007/978-3-031-07082-2_1
20. Dworkin, M.J.: Sha-3 standard: Permutation-based hash and extendable-output functions (2015)
21. Jean, J., Nikolic, I., Peyrin, T.: Tweaks and keys for block ciphers: The TWEAKEY framework. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part II. LNCS, vol. 8874, pp. 274–288. Springer, Heidelberg (Dec 2014). https://doi.org/10.1007/978-3-662-45608-8_15
22. Ji, F., Zhang, W., Zhou, C., Ding, T.: Improved (related-key) differential cryptanalysis on GIFT. In: Dunkelman, O., Jr., M.J.J., O'Flynn, C. (eds.) SAC 2020. LNCS, vol. 12804, pp. 198–228. Springer, Heidelberg (Oct 2020). https://doi.org/10.1007/978-3-030-81652-0_8
23. Lai, X., Massey, J.L., Murphy, S.: Markov ciphers and differential cryptanalysis. In: Davies, D.W. (ed.) EUROCRYPT'91. LNCS, vol. 547, pp. 17–38. Springer, Heidelberg (Apr 1991). https://doi.org/10.1007/3-540-46416-6_2
24. Li, L., Wu, W., Zheng, Y., Zhang, L.: The relationship between the construction and solution of the MILP models and applications. Cryptology ePrint Archive, Report 2019/049 (2019), https://eprint.iacr.org/2019/049
25. Liu, Y., Liang, H., Li, M., Huang, L., Hu, K., Yang, C., Wang, M.: STP models of optimal differential and linear trail for S-box based ciphers. Cryptology ePrint Archive, Report 2019/025 (2019), https://eprint.iacr.org/2019/025
26. Liu, Y., Zhang, W., Sun, B., Rijmen, V., Liu, G., Li, C., Fu, S., Cao, M.: The phantom of differential characteristics. Des. Codes Cryptogr. **88**(11), 2289–2311 (2020). https://doi.org/10.1007/S10623-020-00782-3
27. Mendel, F., Rijmen, V., Toz, D., Varici, K.: Differential analysis of the LED block cipher. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS,

vol. 7658, pp. 190–207. Springer, Heidelberg (Dec 2012). https://doi.org/10.1007/978-3-642-34961-4_13

28. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) EUROCRYPT'93. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (May 1994). https://doi.org/10.1007/3-540-48285-7_6
29. Peyrin, T., Tan, Q.Q.: Mind your path: On (key) dependencies in differential characteristics. IACR Trans. Symm. Cryptol. **2022**(4), 179–207 (2022). https://doi.org/10.46586/tosc.v2022.i4.179-207
30. Qiao, K., Song, L., Liu, M., Guo, J.: New collision attacks on round-reduced Keccak. In: Coron, J.S., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part III. LNCS, vol. 10212, pp. 216–243. Springer, Heidelberg (Apr / May 2017). https://doi.org/10.1007/978-3-319-56617-7_8
31. Qin, L., Dong, X., Wang, A., Hua, J., Wang, X.: Mind the TWEAKEY schedule: Cryptanalysis on SKINNYe-64-256. In: Agrawal, S., Lin, D. (eds.) ASIACRYPT 2022, Part I. LNCS, vol. 13791, pp. 287–317. Springer, Heidelberg (Dec 2022). https://doi.org/10.1007/978-3-031-22963-3_10
32. Qin, L., Dong, X., Wang, X., Jia, K., Liu, Y.: Automated search oriented to key recovery on ciphers with linear key schedule. IACR Trans. Symm. Cryptol. **2021**(2), 249–291 (2021). https://doi.org/10.46586/tosc.v2021.i2.249-291
33. Sadeghi, S., Rijmen, V., Bagheri, N.: Proposing an milp-based method for the experimental verification of difference-based trails: application to speck, SIMECK. Des. Codes Cryptogr. **89**(9), 2113–2155 (2021). https://doi.org/10.1007/S10623-021-00904-5
34. Sharma, S., Roy, S., Soos, M., Meel, K.S.: GANAK: A scalable probabilistic exact model counter. In: Kraus, S. (ed.) Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence, IJCAI 2019, Macao, China, August 10-16, 2019. pp. 1169–1176. ijcai.org (2019). https://doi.org/10.24963/IJCAI.2019/163
35. Song, L., Qin, X., Hu, L.: Boomerang connectivity table revisited. IACR Trans. Symm. Cryptol. **2019**(1), 118–141 (2019). https://doi.org/10.13154/tosc.v2019.i1.118-141
36. Soos, M., Gocht, S., Meel, K.S.: Tinted, detached, and lazy CNF-XOR solving and its applications to counting and sampling. In: Lahiri, S.K., Wang, C. (eds.) Computer Aided Verification - 32nd International Conference, CAV 2020, Los Angeles, CA, USA, July 21-24, 2020, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12224, pp. 463–484. Springer (2020). https://doi.org/10.1007/978-3-030-53288-8_22
37. Soos, M., Meel, K.S.: BIRD: engineering an efficient CNF-XOR SAT solver and its applications to approximate model counting. In: The Thirty-Third AAAI Conference on Artificial Intelligence, AAAI 2019, The Thirty-First Innovative Applications of Artificial Intelligence Conference, IAAI 2019, The Ninth AAAI Symposium on Educational Advances in Artificial Intelligence, EAAI 2019, Honolulu, Hawaii, USA, January 27 - February 1, 2019. pp. 1592–1599. AAAI Press (2019). https://doi.org/10.1609/AAAI.V33I01.33011592
38. Soos, M., Nohl, K., Castelluccia, C.: Extending SAT solvers to cryptographic problems. In: Kullmann, O. (ed.) Theory and Applications of Satisfiability Testing - SAT 2009, 12th International Conference, SAT 2009, Swansea, UK, June 30 - July 3, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5584, pp. 244–257. Springer (2009). https://doi.org/10.1007/978-3-642-02777-2_24

39. Su, B., Wu, W., Zhang, W.: Differential cryptanalysis of SMS4 block cipher. Cryptology ePrint Archive, Report 2010/062 (2010), https://eprint.iacr.org/2010/062

40. Sun, L., Wang, M.: Sok: Modeling for large s-boxes oriented to differential probabilities and linear correlations. IACR Trans. Symmetric Cryptol. **2023**(1), 111–151 (2023). https://doi.org/10.46586/TOSC.V2023.I1.111-151

41. Sun, L., Wang, W., Wang, M.: Accelerating the search of differential and linear characteristics with the SAT method. IACR Trans. Symm. Cryptol. **2021**(1), 269–315 (2021). https://doi.org/10.46586/tosc.v2021.i1.269-315

42. Sun, L., Wang, W., Wang, M.: Improved attacks on GIFT-64. In: AlTawy, R., Hülsing, A. (eds.) SAC 2021. LNCS, vol. 13203, pp. 246–265. Springer, Heidelberg (Sep / Oct 2022). https://doi.org/10.1007/978-3-030-99277-4_12

43. Sun, L., Wang, W., Wang(66), M.: More accurate differential properties of LED64 and Midori64. IACR Trans. Symm. Cryptol. **2018**(3), 93–123 (2018). https://doi.org/10.13154/tosc.v2018.i3.93-123

44. Teh, J.S., Biryukov, A.: Differential cryptanalysis of WARP. J. Inf. Secur. Appl. **70**, 103316 (2022). https://doi.org/10.1016/J.JISA.2022.103316

45. Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G.: The simeck family of lightweight block ciphers. In: Güneysu, T., Handschuh, H. (eds.) CHES 2015. LNCS, vol. 9293, pp. 307–329. Springer, Heidelberg (Sep 2015). https://doi.org/10.1007/978-3-662-48324-4_16

46. Yang, J., Meel, K.S.: Rounding meets approximate model counting. In: Enea, C., Lal, A. (eds.) Computer Aided Verification - 35th International Conference, CAV 2023, Paris, France, July 17-22, 2023, Proceedings, Part II. Lecture Notes in Computer Science, vol. 13965, pp. 132–162. Springer (2023). https://doi.org/10.1007/978-3-031-37703-7_7

47. Zhang, P., Zhang, W.: Differential cryptanalysis on block cipher skinny with MILP program. Secur. Commun. Networks **2018**, 3780407:1–3780407:11 (2018). https://doi.org/10.1155/2018/3780407

48. Zhao, J., Xu, S., Zhang, Z., Dong, X., Li, Z.: Differential analysis of lightweight block cipher gift. Journal of Cryptologic Research **5**(4), 335–343 (2018). https://doi.org/10.13868/j.cnki.jcr.000244

49. Zheng, Y., Matsumoto, T., Imai, H.: On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In: Brassard, G. (ed.) CRYPTO'89. LNCS, vol. 435, pp. 461–480. Springer, Heidelberg (Aug 1990). https://doi.org/10.1007/0-387-34805-0_42

50. Zhou, C., Zhang, W., Ding, T., Xiang, Z.: Improving the MILP-based security evaluation algorithm against differential/linear cryptanalysis using a divide-and-conquer approach. IACR Trans. Symm. Cryptol. **2019**(4), 438–469 (2019). https://doi.org/10.13154/tosc.v2019.i4.438-469

51. Zhu, B., Dong, X., Yu, H.: MILP-based differential attack on round-reduced GIFT. In: Matsui, M. (ed.) CT-RSA 2019. LNCS, vol. 11405, pp. 372–390. Springer, Heidelberg (Mar 2019). https://doi.org/10.1007/978-3-030-12612-4_19

52. Zong, R., Dong, X., Chen, H., Luo, Y., Wang, S., Li, Z.: Towards key-recovery-attack friendly distinguishers: Application to GIFT-128. IACR Trans. Symm. Cryptol. **2021**(1), 156–184 (2021). https://doi.org/10.46586/tosc.v2021.i1.156-184

A Bit Permutations in GIFT-64 and GIFT-128

Tables 9 and 10 respectively display the bit permutations used in GIFT-64 and GIFT-128.

Table 9. Bit permutation in GIFT-64.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_{64}(i)$	48	1	18	35	32	49	2	19	16	33	50	3	0	17	34	51

i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P_{64}(i)$	52	5	22	39	36	53	6	23	20	37	54	7	4	21	38	55

i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P_{64}(i)$	56	9	26	43	40	57	10	27	24	41	58	11	8	25	42	59

i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P_{64}(i)$	60	13	30	47	44	61	14	31	28	45	62	15	12	29	46	63

B Differential Characteristic in [41]

The component of the 18-round related-key differential characteristic from [41] is depicted in Figure 11.

C 4-Round Linearised Nonlinear Constraint of GIFT-64

Figure 12 displays the segment of differential characteristic that gives rise to the constraint $k_{12} \oplus k_{88} \oplus k_{122} \oplus k_{123} = 1$, encompassing four rounds of encryption.

D Supplementary Materials for SKINNY-64

D.1 Illustration of SKINNY-64

Figure 13 illustrates the round function and tweakey schedule of SKINNY-64.

D.2 One Linearised Nonlinear Constraint for SKINNY-64

We provide an example of one of the linearised nonlinear constraints that have been identified. As illustrated in Figure 14, it is present in the middle three rounds of the differential characteristic, where the cells involved in the linearised nonlinear constraints are circled out with blue rectangles. We will employ X^r and Y^r to represent the states before and after the SC function in the r-th round, as seen in Figure 14. The differences of the states are represented as ΔX^r and

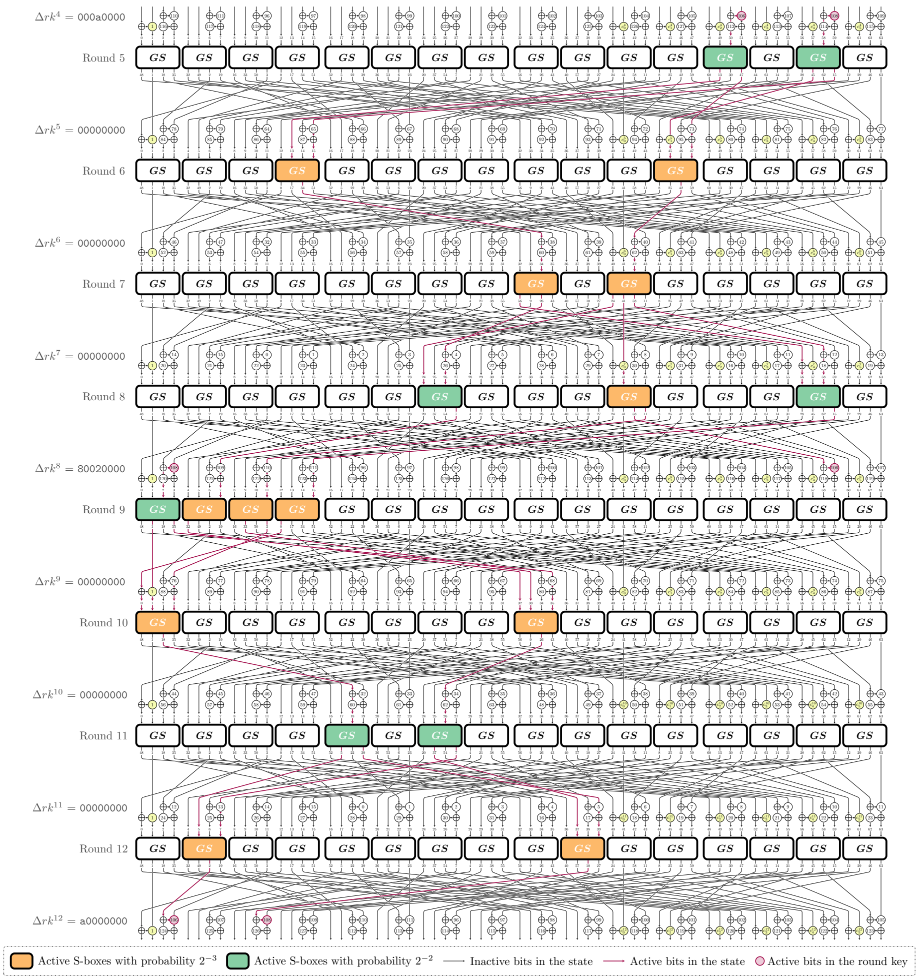


Fig. 11. Partial differential characteristic in [41] with probability 2^{-50}.

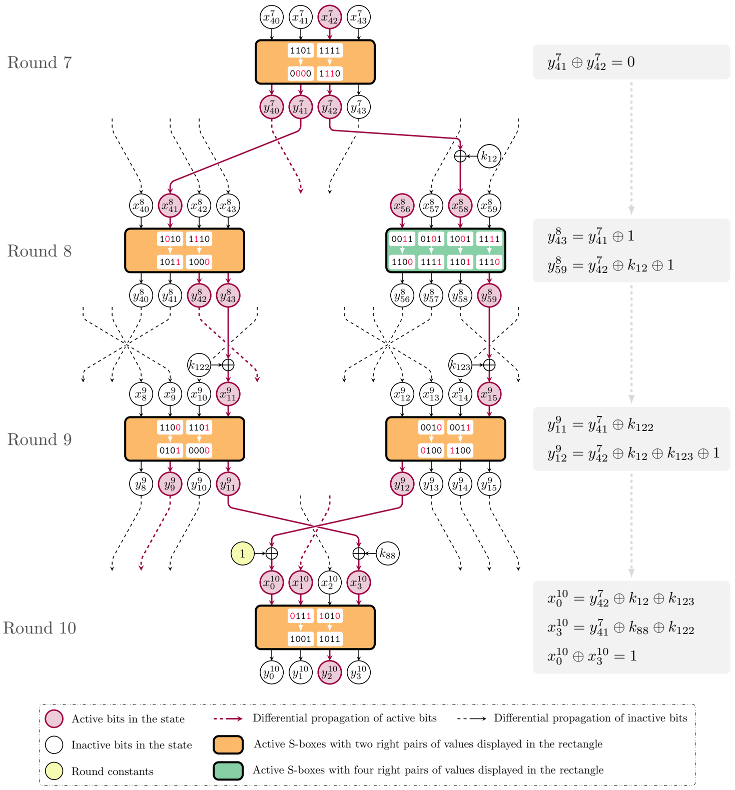

Round 7
Round 8
Round 9
Round 10
$y^7_{41} \oplus y^7_{42} = 0$
$y^8_{43} = y^7_{41} \oplus 1$
$y^8_{59} = y^7_{42} \oplus k_{12} \oplus 1$
$y^9_{11} = y^7_{41} \oplus k_{122}$
$y^9_{12} = y^7_{42} \oplus k_{12} \oplus k_{123} \oplus 1$
$x^{10}_0 = y^7_{42} \oplus k_{12} \oplus k_{123}$
$x^{10}_3 = y^7_{41} \oplus k_{88} \oplus k_{122}$
$x^{10}_0 \oplus x^{10}_3 = 1$
Active bits in the state
Inactive bits in the state
Round constants
Differential propagation of active bits
Differential propagation of inactive bits
Active S-boxes with two right pairs of values displayed in the rectangle
Active S-boxes with four right pairs of values displayed in the rectangle

Fig. 12. Origin of the second nonlinear constraint encompasses four rounds.

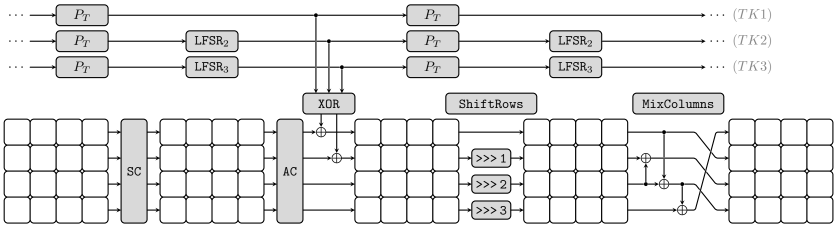


Fig. 13. Round function and tweakey schedule of SKINNY-64.

Table 10. Bit permutation in `GIFT-128`.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_{128}(i)$	96	1	34	67	64	97	2	35	32	65	98	3	0	33	66	99
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P_{128}(i)$	100	5	38	71	68	101	6	39	36	69	102	7	4	37	70	103
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P_{128}(i)$	104	9	42	75	72	105	10	43	40	73	106	11	8	41	74	107
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P_{128}(i)$	108	13	46	79	76	109	14	47	44	77	110	15	12	45	78	111
i	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
$P_{128}(i)$	112	17	50	83	80	113	18	51	48	81	114	19	16	49	82	115
i	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
$P_{128}(i)$	116	21	54	87	84	117	22	55	52	85	118	23	20	53	86	119
i	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
$P_{128}(i)$	120	25	58	91	88	121	26	59	56	89	122	27	24	57	90	123
i	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
$P_{128}(i)$	124	29	62	95	92	125	30	63	60	93	126	31	28	61	94	127

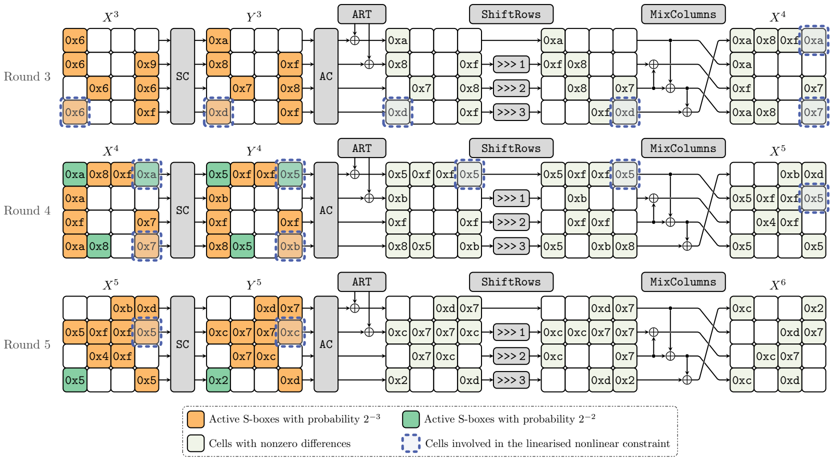

Round 3
Round 4
Round 5
X^3
Y^3
X^4
Y^4
X^5
Y^5
X^6
SC
AC
ART
ShiftRows
MixColumns
>>> 1
>>> 2
>>> 3
Active S-boxes with probability 2^-3
Active S-boxes with probability 2^-2
Cells with nonzero differences
Cells involved in the linearised nonlinear constraint

Fig. 14. Partial differential characteristic of the 11-round differential characteristic for `SKINNY-64-192` in [47].

ΔY^r, respectively. The cell in the i-th row and j-th column of the state X^r is expressed as $X^r[4i+j]$, where $0 \leqslant i, j \leqslant 3$. When examining the state at the level of individual bits, we represent the l-th bit of the state as X_l^r, where $0 \leqslant l \leqslant 63$. For all $0 \leqslant \ell \leqslant 15$, we thus have $X^r[\ell] = X_{4\ell}^r \| X_{4\ell+1}^r \| X_{4\ell+2}^r \| X_{4\ell+3}^r$. To simplify, we will refer to the round tweakey used in the r-th round as rtk^r. The l-th bit of rtk^r will be marked as rtk_l^r, where $0 \leqslant l \leqslant 31$.

Figure 15 provides a more explicit representation of the linearised nonlinear constraint. As the active S-box in the third round transfers the input difference $\Delta X^3[12] = \texttt{0x6}$ to the output difference $\Delta Y^3[12] = \texttt{0xd}$, the output value $Y^3[12]$ for the right pair of the differential characteristic must be chosen from the set $\{\texttt{0x6}, \texttt{0xb}\}$. Hence, the result of the XOR operation on the first three bits of $Y^3[12]$ should always be zero, namely

$$Y_{48}^3 \oplus Y_{49}^3 \oplus Y_{50}^3 = 0. \tag{19}$$

The property of the round function can be employed to derive $X^4[3] \oplus X^4[15] = Y^3[12]$. At the bit level, we have

$$X_{12+i}^4 \oplus X_{60+i}^4 = Y_{48+i}^3 \text{ for all } 0 \leqslant i \leqslant 3. \tag{20}$$

Therefore, $Y^3[12]$ is associated with two active S-boxes in the fourth round. Analysing the active S-box on $X^4[15]$ makes it possible to determine that the XORed value of the first three bits of $X^4[15]$ must adhere to

$$X_{60}^4 \oplus X_{61}^4 \oplus X_{62}^4 = 0. \tag{21}$$

The constraint over the first three bits of the cell $X^4[3]$

$$X_{12}^4 \oplus X_{13}^4 \oplus X_{14}^4 = 0 \tag{22}$$

is obtained by performing an XOR operation on equations (20) - (21).

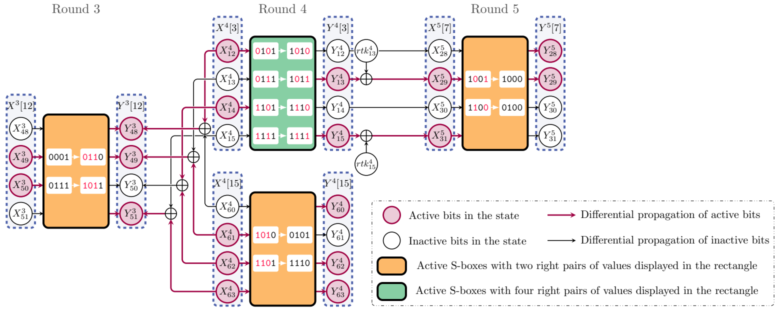

Round 3
Round 4
Round 5
$X^3[12]$
$Y^3[12]$
$X^4[3]$
$Y^4[3]$
$X^4[15]$
$Y^4[15]$
$X^5[7]$
$Y^5[7]$
0001 0110
0111 1011
0101 1010
0111 1011
1101 1110
1111 1111
1010 0101
1101 1110
1001 1000
1100 0100
rtk_{13}^4
rtk_{15}^4
Active bits in the state
Inactive bits in the state
Differential propagation of active bits
Differential propagation of inactive bits
Active S-boxes with two right pairs of values displayed in the rectangle
Active S-boxes with four right pairs of values displayed in the rectangle

Fig. 15. Illustration of a linearised nonlinear constraints for `SKINNY-64-192`.

Subsequently, an examination of the active S-box on $X^4[3]$ indicates that the input value of the right pair should be selected from the set $\{\texttt{0x5}, \texttt{0x7}, \texttt{0xd}, \texttt{0xf}\}$

for the differential propagation from $\Delta X^4[3] = \texttt{0xa}$ to $\Delta Y^4[3] = \texttt{0x5}$ to occur. That is, the second bit X^4_{13} of $X^4[3]$ should always be one. By including this restriction in equation (22), we deduce

$$X^4_{12} \oplus X^4_{14} = 1. \tag{23}$$

In addition, it is possible to generate two linear equations

$$Y^4_{13} = X^4_{12} \text{ and } Y^4_{15} = X^4_{14} \tag{24}$$

relating specific bits of the input $X^4[3]$ to the output $Y^4[3]$. Next, the two bits Y^4_{13} and Y^4_{15} will transmit to X^5_{29} and X^5_{31} in the subsequent round, possibly establishing linear equations using these bits

$$X^5_{29} = Y^4_{13} \oplus rtk^4_{13} \text{ and } X^5_{31} = Y^4_{15} \oplus rtk^4_{15}. \tag{25}$$

By examining the input of the active S-box in the fifth round using differential propagation $\texttt{0x5} \rightarrow \texttt{0xc}$, it can be determined that the equation

$$X^5_{29} \oplus X^5_{31} = 1 \tag{26}$$

should be validated by the two bits of $X^5[7]$. A constraint on the round tweakey

$$rtk^4_{13} \oplus rtk^4_{15} = 0 \tag{27}$$

can be extracted by performing an XOR operation on equations (23) - (26).

Remark 4. While constraint (27) only pertains to the round tweakey in the fourth round, it is a nonlinear constraint since it relies on the active S-boxes from three rounds. In contrast, the linear constraints only rely on the active S-boxes from two consecutive rounds. Furthermore, the nonlinear constraint being illustrated is distinct from the one presented in [29], which incorporates inactive S-boxes (refer to Figure 6 of [29]).

E 17-Round Differential Characteristic of WARP

Figure 16 displays the 17-round differential characteristic.

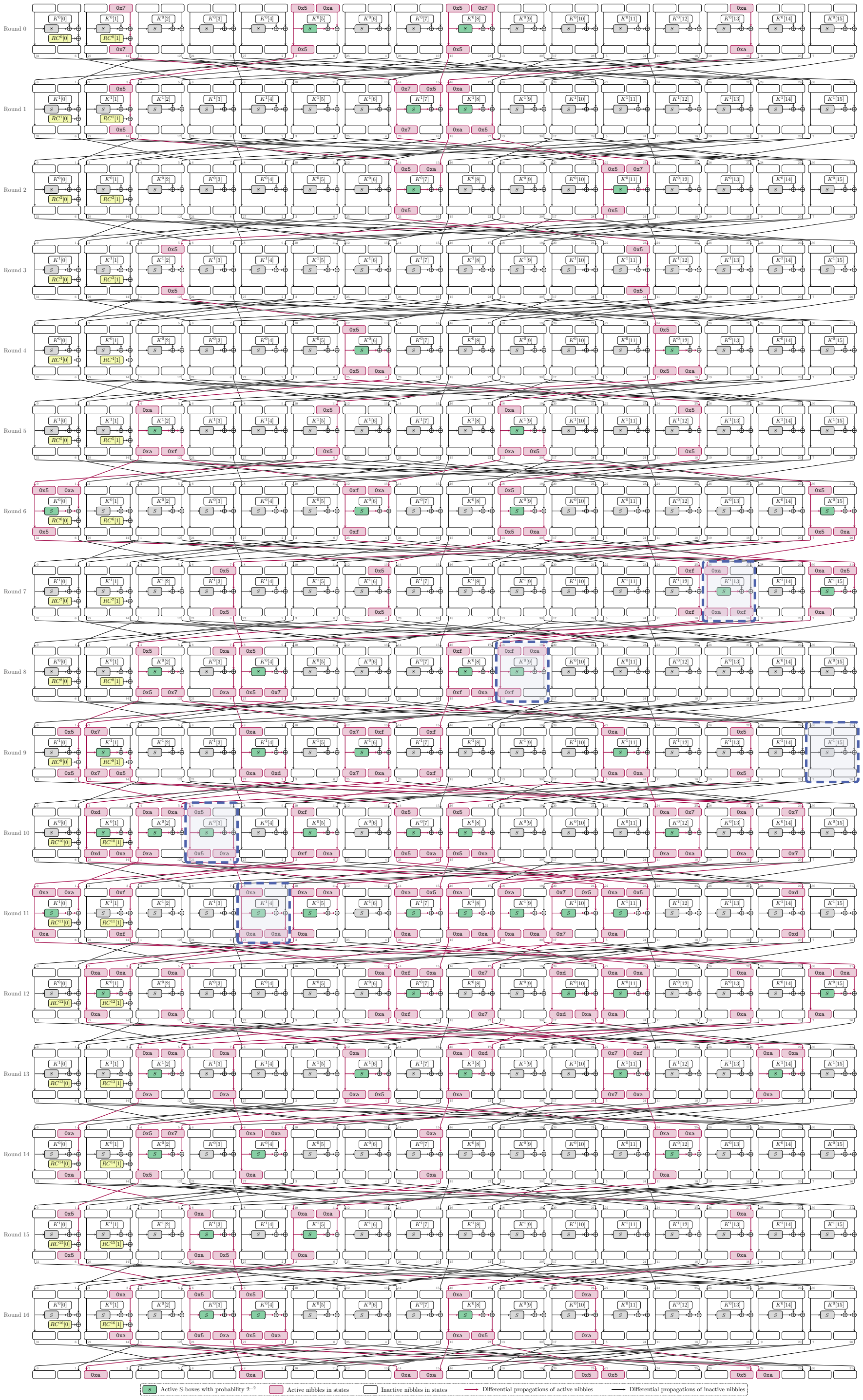

Round 0
Round 1
Round 2
Round 3
Round 4
Round 5
Round 6
Round 7
Round 8
Round 9
Round 10
Round 11
Round 12
Round 13
Round 14
Round 15
Round 16
S Active S-boxes with probability 2^{-2}
Active nibbles in states
Inactive nibbles in states
Differential propagations of active nibbles
Differential propagations of inactive nibbles

Fig. 16. 17-round differential characteristic of WARP with a probability of 2^{-114}.