Hindawi
IET Information Security
Volume 2023, Article ID 5323380, 14 pages
https://doi.org/10.1049/2023/5323380

Research Article

SAT-Based Security Evaluation for WARP against Linear Cryptanalysis

Jiali Shi, Guoqiang Liu, and Chao Li

College of Science, National University of Defense Technology, Changsha, China

Correspondence should be addressed to Guoqiang Liu; liuguoqiang87@hotmail.com

Received 2 September 2023; Revised 30 October 2023; Accepted 10 November 2023; Published 6 December 2023

Academic Editor: Qichun Wang

WARP, an efficient lightweight block cipher presented by Banik et al., offers a viable alternative to AES with its 128-bit block and a 128-bit key. It adopts a 32-nibble type-II generalized Feistel network (GFN) structure, incorporating a nibble permutation optimized for both security and efficiency. Notably, WARP has achieved the lowest hardware implementation among 128-bit block ciphers. Its bit-serial encryption-only circuit is only 763 gate equivalents (GEs). Consequently, WARP has received significant attention since its inception. The designers evaluated the number of active Sboxes for linear trails in WARP to establish its security. To further investigate WARP's resistance against linear attacks, we employed an automated model to analyze the optimal linear trails/hulls of WARP. To achieve this, the problem will be transformed into a Boolean satisfiability problem (SAT). The constraints in conjunctive normal form (CNF) are used to describe the mask propagation of WARP and invoke the SAT solver to find valid solutions. The results allowed us to obtain the optimal correlation of the initial 21-round linear trails for WARP. Furthermore, by enumerating the linear trails within a linear hull, the distribution of linear trails is revealed, and the probability of the linear hull is improved to be more accurate. This work extends the linear distinguisher from 18 to 21 rounds. Additionally, the first independent analysis of WARP's linear properties is presented, offering a more precise evaluation of its resistance against linear cryptanalysis.

1. Introduction

1.1. Background. Linear cryptanalysis, as presented by Matsui [1], stands as a prominent method employed in the analysis of symmetric-key ciphers. By identifying linear trails with high correlation, it becomes possible to conduct attacks more efficiently, achieving a lower complexity compared to brute-force searching. Consequently, resistance to linear cryptanalysis emerges as a critical aspect to be considered by both designers and potential attackers.

The development of search methods for differential [2, 3] and linear trails is closely intertwined. This is because the propagation of difference pairs and linear masks in branching and XOR operations exhibit a dual nature [4]. Matsui's branch-and-bound method, initially introduced at EUROCRYPT 1994 for searching differential trails with optimal probability, is also commonly employed for searching linear trails with optimal correlation. Although this method is powerful, it demands strong programming skills. In recent years, the automated models like mixed integer linear programming (MILP) [5, 6], constraint programming (CP) [7], satisfiability modulo theories (SMT) [8], and Boolean satisfiability problem (SAT) [9, 10] have exhibited remarkable performance in discovering various distinguishers in cryptanalysis. However, for long trails or ciphers with 128-bit block, these models still struggle to return solutions within a reasonable time. By integrating the strengths of both approaches, researchers have made significant progress in improving the efficiency of trail search algorithms, as demonstrated in works such as those by Sun et al. [10] and Zhang et al. [11].

It is crucial for symmetric-key cryptography to prioritize resistance against distinguishing attacks as a fundamental security requirement. WARP with a 128-bit block was specifically designed for efficient hardware implementation [12]. It has undergone a preliminary security evaluation, encompassing a range of attacks such as the differential, linear, impossible differential, and integral attacks. Regarding impossible differentials cryptanalysis, the designers obtained a 21-round

Table 1: Summary of distinguishers in the single key scenarios for WARP.

Approach	Rounds	Probability	Data	References
Linear distinguisher	18	2^{-122}	-	[12]
	18	$2^{-109.08}$	-	Section 5
	19	$2^{-120.01}$	-	Section 5
	20	$2^{-127.27}$	-	Section 5
Differential distinguisher	18	2^{-122}	-	[19]
	18	$2^{-104.62}$	-	[18]
	19	$2^{-118.07}$	-	[18]
	19	$2^{-116.92}$	-	[20]
	20	$2^{-122.71}$	-	[18]
Impossible differential distinguisher	21	-	-	[12, 21]
Zero-correlation distinguisher	21	-	-	[14, 15]
Integral distinguisher	20	-	2^{124}	[12]
	24	-	2^{127}	[14]
Boomerang distinguisher	23	$2^{120.6}$	-	[22]

Bold values refers to the new results obtained in this article, and explanations have been added in the paper.

impossible differential distinguisher using the approach outlined in a study by Sasaki and Todo [13]. Independently, other researchers discovered a 21-round zero-correlation distinguisher [14, 15]. For integral attacks, the designers found a 20-round integral distinguisher utilizing the MILP model provided in a study by Xiang et al. [16], and a 24-round generalized integral distinguisher was subsequently proposed by observing the properties of WARP's construction [14]. Additionally, an extension of the model led to the discovery of a 23-round boomerang distinguisher [17]. To assess security against differential and linear attacks, designers employed a MILP-based automated model [5] to obtain lower bounds for the number of active Sboxes. In the presence of the clustering effect, a 20-round differential distinguisher was identified in a study by Teh and Biryukov [18]. However, until now, no investigation has been conducted to explore actual linear distinguisher in WARP. This gap in research leaves room for further exploration of WARP.

1.2. Contribution. In this paper, the main objective is to identify distinguishers, which are instrumental in understanding the structural properties and the security of the underlying components in WARP. The analysis in this paper has yielded several important findings and results, which are summarized as follows:

(1) Using the constructed SAT model, we have successfully validated the lower bounds for the number of active Sboxes required for the initial 19 rounds of linear trails in WARP, as stated in the design documentation. Furthermore, the lower bound for the number of active Sboxes in the 20-, 21-, and 22-round linear trails is determined to be 70, 75, and 79, respectively.
(2) We have successfully identified the first 21-round linear trails with optimal correlation, which align with the upper bound estimated using the lower bound for the number of active Sboxes. Notably, the findings reveal that the 18-round linear trails in WARP have the optimal correlation 2^{-61}, indicating that WARP is not able to withstand the linear trail-based distinguishing attack.
(3) Moreover, the 20-round linear trail with optimal probability 2^{-140} is obtained. With the help of the automated model, 186,856 trails are found to contribute to the same 20-round linear hull, and the probability of the 20-round linear hull is improved from 2^{-140} to $2^{-127.27}$, which is lower than 2^{-128}, thereby extending the distinguishers from 18 to 20 rounds. As far as our knowledge goes, these results represent the current optimal linear distinguishers for WARP. Table 1 shows a comprehensive overview of the single-key distinguishers for WARP, and the bold information is the result obtained in this paper.

1.3. Organization. This paper is structured as follows. We present the necessary definitions related to linear cryptanalysis and provide a concise overview of WARP in Section 2. Section 3 outlines the SAT model employed in the search for linear trails in WARP. The identification of linear trails with lower bounds for the number of active Sboxes and optimal correlations is presented in Section 4. Section 5 focuses on the discovery of optimal linear distinguishers for WARP. Finally, a summary of this work can be found in Section 6.

2. Preliminaries

Let us begin by introducing the notations that will be utilized throughout this paper. Subsequently, a concise overview of the concepts related to linear cryptanalysis will be presented. Moving forward, we provide a detailed description of the WARP specification, which is the primary focus of our study.

2.1. Notions. To maintain consistency and clarity, we employ specific notations to analyze and discuss the linear cryptanalysis of WARP. The meanings of these notations are summarized in Table 2.

Table 2: Notations.

Symbol	Meaning
Γ_{in}	Input mask
Γ_{out}	Output mask
$\overline{a}$	Bitwise NOT of a
$a\|\|b$	Binary concatenation of a and b
$a \oplus b$	Binary exclusive OR (XOR) of a and b
$a \wedge b$	Bitwise AND of a and b
$a \vee b$	Bitwise OR of a and b
$a \cdot b$	The inner product of a and b

2.2. Linear Cryptanalysis. Linear cryptanalysis is widely recognized as a powerful technique for analyzing symmetric-key primitives, especially block ciphers [1]. It has gained widespread recognition and has been extensively applied in the field, with several extensions proposed over time. In the subsequent sections, we introduce a collection of definitions and notations, which will be consistently employed in this paper. These definitions and notations aim to facilitate our discussions and analysis.

Definition 1. Let $E_K(X)$ denotes an iterative block cipher, where X represents the input and K denotes the master key. The round function of the block cipher is recorded as $f(X, K)$. For a given pair of linear masks $(\Gamma_{\text{in}}, \Gamma_{\text{out}})$, we can express the linear approximation expression of $f(X, K)$ as $\Gamma_{\text{in}} \cdot X \oplus \Gamma_{\text{out}} \cdot f(X, K)$. Similarly, for the block cipher $E_K(X)$, the linear approximation expression is given by $\Gamma_{\text{in}} \cdot X \oplus \Gamma_{\text{out}} \cdot E_K(X)$.

Linear cryptanalysis is a well-known method utilized for analyzing block ciphers. Its primary goal is to distinguish a block cipher from a random permutation by discovering a probabilistic linear approximation expression that establishes a correlation between the plaintext and ciphertext. This technique serves as the foundation for key recovery attacks.

For block cipher, by analyzing the biases and correlations of the linear approximation expressions, cryptanalysts can identify potential distinguishers to exploit the linear trails. In linear cryptanalysis, let Γ_{in} denotes the mask of the input X and Γ_{out} represents the mask of the output $f(X)$. The probability of the linear approximation expression $\Gamma_{\text{in}} \cdot X \oplus \Gamma_{\text{out}} \cdot f(X) = 0$ is represented as $p(\Gamma_{\text{in}}, \Gamma_{\text{out}}) = Pr\{\Gamma_{\text{in}} \cdot X \oplus \Gamma_{\text{out}} \cdot f(X) = 0\}$. The bias of this expression quantifies the deviation from a balanced distribution and is defined as the difference between the probability of the expression holding and the ideal probability $1/2$. The linear approximation bias is given by $\varepsilon(\Gamma_{\text{in}}, \Gamma_{\text{out}}) = p(\Gamma_{\text{in}}, \Gamma_{\text{out}}) - 1/2$, and it ranges from $-1/2$ to $1/2$. The correlation measures the strength of the linear relationship between the input and output masks. It is calculated as follows:

$$Cor(\Gamma_{\text{in}}, \Gamma_{\text{out}}) = 2 \cdot p(\Gamma_{\text{in}}, \Gamma_{\text{out}}) - 1, \tag{1}$$

where $Cor_{(\Gamma_{\text{in}}, \Gamma_{\text{out}})} \in [-1, 1]$. Usually, in the distinguish phase, linear cryptanalysis mainly focuses on linear trails with optimal correlation.

Definition 2. For a block cipher, a r-round linear trail $(\Gamma^0, \Gamma^1, \ldots, \Gamma^{r-1})$ is concatenated linear approximations (Γ^i, Γ^{i+1}) of a single round $f^i(X, K)$, where $0 \le i \le r - 1$.

Definition 3. (The correlation of the linear trail [23]) Given a r-round linear trail $(\Gamma^0, \Gamma^1, \ldots, \Gamma^{r-1})$, its correlation is computed by taking the product of the individual correlations along the trail, i.e.:

$$Cor(\Gamma^0, \ldots, \Gamma^{r-1}) = \prod_{i=0}^{r-1} Cor(\Gamma^i, \Gamma^{i+1}). \tag{2}$$

When constructing a distinguisher, the adversary's primary concern is the probability of the linear hull rather than individual intermediate masks. Consequently, the adversary aims to gather all trails having the same masks $\Gamma_{\text{in}}, \Gamma_{\text{out}}$. By collecting a larger number of trails, the adversary can obtain a more accurate estimation of probability associated with the specific linear hull.

Definition 4. (Linear hull [24]) A linear hull $(\Gamma_{\text{in}}, \Gamma_{\text{out}})$ is a construct utilized in linear cryptanalysis that consists of a collection of linear trails. These trails share identical masks for both the masks $(\Gamma_{\text{in}}, \Gamma_{\text{out}})$. Essentially, a linear hull represents a specific linear approximation $(\Gamma_{\text{in}}, \Gamma_{\text{out}})$ for a given block cipher.

Definition 5. The potential of a linear hull $(\Gamma_{\text{in}}, \Gamma_{\text{out}})$ is measured by the average linear probability (ALP) over the key space K. This measure, denoted as $ALP(\Gamma_{\text{in}}, \Gamma_{\text{out}})$, is defined as the average of the squared correlations between the input and output masks $\Gamma_{\text{in}}, \Gamma_{\text{out}}$, considering all possible keys k in K, i.e.:

$$ALP(\Gamma_{\text{in}}, \Gamma_{\text{out}}) = \frac{1}{|K|} \sum_{k \in K} Cor(\Gamma_{\text{in}}, \Gamma_{\text{out}})^2. \tag{3}$$

2.3. Description of `WARP`. `WARP` is a lightweight block cipher with the aim of achieving 128-bit security while keeping the implementation footprint small [12]. It applies the type-II generalized Feistel network (GFN) [25] structure, which is a well-known construction in the field of symmetric-key cryptography. It takes a 128-bit plaintext denoted as M and the 128-bit master key written as K as inputs. Through a series of 41 encryption rounds, `WARP` transforms the plaintext into a 128-bit ciphertext represented as C.

2.3.1. Round Function. For `WARP`, the internal state in the rth round operates on 32 nibbles denoted as $X_i^r = X_0^r || X_1^r || \ldots || X_{31}^r$, where $0 \le r \le 40$, and each $X_i^r \in \{0, 1\}^4$ denotes the ith nibble. The round key is expressed as 16 nibbles $k^r = k_0^r || k_1^r || \ldots || k_{15}^r$, where $k_j^r \in \{0, 1\}^4$, $0 \le j \le 15$. The round function of `WARP`, as shown in Figure 1, employs 4-bit Sbox operations, nibble XOR operations, and shuffle operations applied to the 32 nibbles. These operations are performed as follows.

Sbox: To fulfill the design objectives of `WARP`, such as a compact circuit, low path delay, and efficient energy

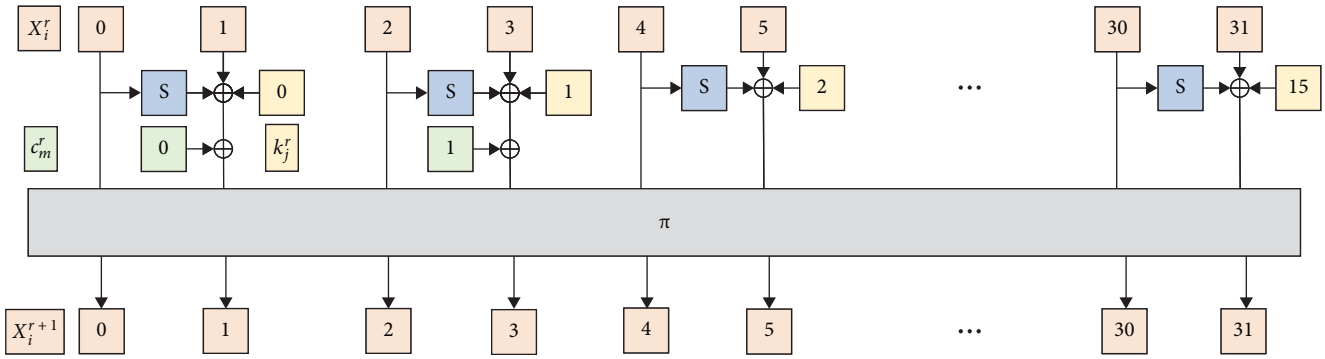

FIGURE 1: Round function of WARP.

TABLE 3: 4-bit Sbox.

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

TABLE 4: The shuffle operation.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\pi(x)$	31	6	29	14	1	12	21	8	27	2	3	0	25	4	23	10
x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$\pi(x)$	15	22	13	30	17	28	5	24	11	18	19	16	9	20	7	26

utilization. WARP utilizes the 4-bit Sbox from MIDORI [26]. The Sbox is defined by the values, as shown in Table 3.

Add round key: XOR operation is performed bitwise between the 16 nibbles S_{i-1}^r of the Sbox output, the 16 nibbles of the even branches X_i^r, and the 16 nibbles round key k_j^r, where $i \bmod 2 = 1$ and $j = \frac{i-1}{2}$.

Add round constant: The round constants, represented by 2 nibbles $c_0^r \| c_1^r$, are XOR-ed with the first and third nibbles of the intermediate state.

Shuffle operation: WARP employs a 32-branch permutation that exhibits strong diffusion properties and resistance against major attacks. The input state, composed of 32 nibbles, is represented as $Y^r = Y_0^r \| Y_1^r \| \| \ldots \| Y_{31}^r$. The output state is obtained by applying the permutation π such that $X_{\pi(i)}^{r+1} = Y_i^r$, where $0 \le i \le 31$. The specific permutation π is shown in Table 4. It is worth mentioning that the permutation operation π is not performed in the final round.

The paper does not specifically investigate the influence of adding the round constants on the attack's validity, and it does not delve into the discussion of the key schedule. Banik et al. [12] showed a more comprehensive understanding of WARP and its specific details.

3. SAT-Based Model to Search Linear Trail for WARP

As far as cryptanalysis is concerned, many problems such as the search for linear trails can be reformulated as systems of equations, and SAT solvers are commonly employed to solve equation-based problems. In this section, the SAT-based automated model introduced in a study by Sun et al. [10] is utilized to assess the resistance of WARP against linear attacks. This systematic approach allows us to efficiently identify the optimal linear trails for WARP.

3.1. Boolean Satisfiability Problem. The algebraic normal form (ANF) is a commonly employed representation in cryptography for describing symmetric ciphers. By converting ANF equations with Boolean variables into the conjunctive normal form (CNF), SAT solvers can be effectively employed since CNF serves as their standard input format. This transformation enables the utilization of SAT solvers to analyze and solve cryptographic problems based on equations. In CNF, the Boolean function is represented as a conjunction of clauses $\bigwedge_{i=0}^{n} \bigvee_{j=0}^{m_i} C_{ij}$, where each clause $\bigvee_{j=0}^{m_i} C_{ij}$ consists of a disjunction of literals. This form is equivalent to the product-of-sum representation of Boolean functions, where the function is expressed as a conjunction of terms, and each term is a disjunction of literals. Russell and Norvig [27] postulated a more detailed information on CNF and its relation to Boolean functions.

Cook [28] established that the SAT is a computationally challenging problem that has been proven to be nondeterministic polynomial (NP) complete. This means that finding a satisfying assignment for a given set of Boolean clauses is computationally challenging. However, despite its theoretical complexity, modern SAT solvers have made significant advancements and can effectively handle problems with millions of variables. The solver, Cryptominisat5 [29], is an example of a universal and efficient SAT solver. It is specifically designed to handle large-scale SAT instances and offers support for XOR and Gaussian elimination techniques. This solver employs advanced algorithms and heuristics to improve performance and optimize the search for satisfying assignments. With the capabilities of SAT solvers like Cryptominisat5, it is possible to tackle complex cryptanalysis problems by formulating them as SAT instances and utilizing the solver's efficient solving techniques.

Table 5: Linear approximation table (LAT) of WARP Sbox.

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	2	4	2	−2	0	2	0	−2	0	2	0	4	−2	0	−2
0x2	0	4	0	0	4	0	0	0	−4	0	0	0	0	4	0	0
0x3	0	2	0	2	−2	0	2	4	2	−4	−2	0	0	2	0	2
0x4	0	−2	4	−2	2	0	−2	0	−2	−4	−2	0	0	−2	0	2
0x5	0	0	0	0	0	0	0	0	0	0	−4	−4	0	0	4	−4
0x6	0	2	0	2	−2	0	2	−4	−2	0	−2	0	−4	−2	0	2
0x7	0	0	0	4	0	0	−4	0	0	0	0	−4	0	0	−4	0
0x8	0	−2	−4	2	−2	0	−2	0	−4	−2	0	2	2	0	2	0
0x9	0	0	0	−4	−4	0	0	0	−2	2	−2	−2	2	2	−2	2
0xa	0	2	0	−2	−2	−4	−2	0	0	−2	4	−2	−2	0	2	0
0xb	0	0	0	0	0	−4	0	−4	2	−2	−2	2	2	2	−2	−2
0xc	0	4	0	0	0	0	−4	0	2	2	−2	2	2	−2	2	2
0xd	0	−2	4	2	−2	0	−2	0	0	2	0	2	−2	4	2	0
0xe	0	0	0	0	0	4	0	−4	2	−2	2	−2	2	2	2	2
0xf	0	−2	0	2	2	−4	2	0	0	2	0	−2	2	0	2	4

Each entry represents $LAT(\Gamma_{in}, \Gamma_{out}) = \#\{x \in \mathbb{F}_2^4 | x \bullet \Gamma_{in} = S(x) \bullet \Gamma_{out} - 8\}$.

3.2. SAT Models for the Linear Approximation of WARP. When utilizing SAT solvers to search for linear trails, it is necessary to translate this problem into a set of clauses that capture the linear propagation properties within WARP. By the findings in a study by Sun et al. [4], the linear propagation of the XOR operation is equivalent to the differences propagation for the XOR operation. Next, we will present a concise overview of the SAT models employed for some fundamental operations used in WARP. However, for a more comprehensive understanding, we recommend referring to [9, 10, 30] for detailed information.

3.2.1. Three-Fork Branching. Consider the XOR operation, where Γ_0 represents the input mask and Γ_1 and Γ_2 denote the two output masks. The nontrivial propagation is valid if and only if the masks Γ_0, Γ_1, and Γ_2 satisfy all the conditions outlined as follows:

$$\begin{cases} \Gamma_1 \vee \Gamma_2 \vee \overline{\Gamma_0} = 1, \\ \Gamma_1 \vee \overline{\Gamma_2} \vee \Gamma_0 = 1, \\ \overline{\Gamma_1} \vee \Gamma_2 \vee \Gamma_0 = 1, \\ \overline{\Gamma_1} \vee \overline{\Gamma_2} \vee \overline{\Gamma_0} = 1. \end{cases} \tag{4}$$

3.2.2. XOR. The propagation of the two input masks Γ_0 and Γ_1, along with the output mask Γ_2, should fulfill all the conditions described as follows:

$$\begin{cases} \Gamma_2 \vee \overline{\Gamma_0} = 1, \\ \overline{\Gamma_2} \vee \Gamma_0 = 1, \\ \Gamma_2 \vee \overline{\Gamma_1} = 1, \\ \overline{\Gamma_2} \vee \Gamma_1 = 1. \end{cases} \tag{5}$$

3.2.3. Sbox. The linear propagation of Sbox is often characterized using a linear approximation table (LAT). The input mask of the Sbox is denoted as $\Gamma_{\text{in}} = \Gamma_0 \| \Gamma_1 || \Gamma_2 \| \Gamma_3$ and the output mask is written as $\Gamma_{\text{out}} = \Gamma_4 \| \Gamma_5 || \Gamma_6 \| \Gamma_7$, then, Table 5 shows LAT of Sbox, which includes values of $0, \pm 2, \pm 4, 8$. The corresponding absolute correlations of the linear approximation fall within the range $\{0, 2^{-2}, 2^{-1}, 1\}$. Two Boolean variables c_0 and c_1 are used to encode the correlation of the linear propagation for the Sbox. To describe the correlation for valid linear propagation, $Cor(\Gamma_{\text{in}}, \Gamma_{\text{out}})$ and $c_0 \| c_1$ follow the following rule as follows:

$$c_0 \| c_1 = \begin{cases} 01, & \text{if } Cor(\Gamma_{\text{in}}, \Gamma_{\text{out}}) = 2^{-1}, \\ 11, & \text{if } Cor(\Gamma_{\text{in}}, \Gamma_{\text{out}}) = 2^{-2}, \\ 00, & \text{if } Cor(\Gamma_{\text{in}}, \Gamma_{\text{out}}) = 1. \end{cases} \tag{6}$$

Note that $c_0 + c_1$ represents the opposite number of the binary logarithm of $Cor(\Gamma_{in}, \Gamma_{out})$, i.e., $-\log_2(|Cor(\Gamma_{in}, \Gamma_{out})|) = c_0 + c_1$. To capture the valid linear propagation with correlation $2^{-(c_0+c_1)}$, we define a 10-bit Boolean function $g(\Gamma_{in} \| \Gamma_{out} || c_0 \| c_1)$ as follows:

$$g(\Gamma_{\text{in}} \| \Gamma_{\text{out}} \| c_0 \| c_1) = \begin{cases} 1, & \text{if } \Gamma_{\text{in}} \to \Gamma_{\text{out}} \text{ is a valid propagation with} \\ & -\log_2(|Cor(\Gamma_{\text{in}}, \Gamma_{\text{out}})|) = c_0 + c_1, \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Following that, the constraint conditions are reduced using Logic Friday (https://web.archive.org/web/20131022021257/http:/www.sontrak.com/), and the results showed that the nontrivial linear mask propagations with correlation for WARP's Sbox can be described by 53 clauses, as shown in Table 6. Similarly, a Boolean variable w is utilized to indicate

Table 6: The constraints used to describe the nontrivial mask propagations with correlation for Sbox.

No.	Clause	No.	Clause	No.	Clause
1	$y_3 \vee y_2 \vee y_0 \vee \overline{c_1} = 1$	19	$x_3 \vee x_2 \vee x_0 \vee \overline{c_1} = 1$	37	$y_3 \vee \overline{y_2} \vee \overline{y_0} \vee \overline{c_1} = 1$
2	$x_3 \vee \overline{x_2} \vee \overline{x_0} \vee \overline{c_1} = 1$	20	$\overline{x_3} \vee x_2 \vee \overline{x_0} \vee y_3 \vee \overline{c_1} = 1$	38	$\overline{x_3} \vee \overline{x_2} \vee x_0 \vee y_3 \vee \overline{c_1} = 1$
3	$x_3 \vee \overline{y_3} \vee y_2 \vee \overline{y_0} \vee \overline{c_1} = 1$	21	$x_3 \vee \overline{y_3} \vee \overline{y_2} \vee y_0 \vee \overline{c_1} = 1$	39	$x_2 \vee x_0 \vee y_2 \vee y_0 \vee \overline{c_1} = 1$
4	$\overline{x_2} \vee \overline{x_0} \vee \overline{y_2} \vee \overline{y_0} \vee \overline{c_1} = 1$	22	$\overline{y_3} \vee c_0 = 1$	40	$\overline{x_2} \vee y_3 \vee y_1 \vee y_0 \vee c_1 = 1$
5	$\overline{y_2} \vee c_0 = 1$	23	$x_3 \vee x_1 \vee y_3 \vee y_1 \vee c_1 \vee \overline{c_0} = 1$	41	$x_1 \vee x_0 \vee \overline{y_2} \vee y_1 \vee c_1 = 1$
6	$x_2 \vee x_1 \vee y_1 \vee \overline{y_0} \vee c_1 = 1$	24	$\overline{x_2} \vee \overline{x_1} \vee y_2 \vee y_0 \vee c_1 = 1$	42	$x_2 \vee \overline{x_0} \vee \overline{y_3} \vee \overline{y_1} \vee c_1 = 1$
7	$x_1 \vee x_0 \vee \overline{y_3} \vee \overline{y_1} \vee c_1 = 1$	25	$x_2 \vee x_0 \vee \overline{y_2} \vee \overline{y_1} \vee c_1 = 1$	43	$\overline{x_3} \vee \overline{x_1} \vee \overline{y_3} \vee y_1 \vee c_1 = 1$
8	$\overline{x_3} \vee \overline{x_1} \vee y_2 \vee \overline{y_0} \vee c_1 = 1$	26	$\overline{x_3} \vee \overline{x_1} \vee \overline{y_2} \vee y_0 \vee c_1 = 1$	44	$x_1 \vee \overline{x_0} \vee y_2 \vee y_1 \vee c_1 = 1$
9	$\overline{y_0} \vee c_0 = 1$	27	$x_2 \vee \overline{x_1} \vee \overline{x_0} \vee y_0 \vee c_1 = 1$	45	$x_0 \vee y_2 \vee \overline{y_1} \vee \overline{y_0} \vee c_1 = 1$
10	$\overline{x_2} \vee x_1 \vee y_3 \vee \overline{y_1} \vee \overline{y_0} \vee c_1 = 1$	28	$x_3 \vee \overline{x_2} \vee \overline{x_1} \vee y_1 \vee \overline{y_0} \vee c_1 = 1$	46	$\overline{x_3} \vee \overline{x_0} \vee \overline{y_3} \vee y_0 \vee c_1 = 1$
11	$\overline{x_3} \vee x_1 \vee \overline{x_0} \vee \overline{y_2} \vee \overline{y_1} \vee c_1 = 1$	29	$\overline{x_3} \vee y_3 \vee y_2 \vee y_1 \vee y_0 = 1$	47	$\overline{x_1} \vee y_3 \vee y_2 \vee y_0 = 1$
12	$x_3 \vee x_2 \vee \overline{x_0} \vee y_3 \vee y_2 \vee \overline{y_0} \vee c_1 = 1$	30	$x_3 \vee \overline{x_2} \vee \overline{x_0} \vee y_1 = 1$	48	$x_3 \vee x_2 \vee x_0 \vee \overline{y_1} = 1$
13	$x_3 \vee \overline{x_1} \vee \overline{x_0} \vee \overline{y_3} \vee \overline{y_2} \vee \overline{y_0} \vee c_1 = 1$	31	$\overline{x_1} \vee x_0 \vee \overline{y_3} \vee y_2 \vee \overline{y_0} \vee c_1 = 1$	49	$\overline{x_3} \vee \overline{y_3} \vee y_2 \vee \overline{y_0} \vee c_1 = 1$
14	$\overline{x_3} \vee \overline{x_2} \vee x_0 \vee y_2 \vee y_0 \vee c_1 = 1$	32	$x_0 \vee \overline{y_3} \vee \overline{y_2} \vee \overline{y_1} \vee c_1 = 1$	50	$x_3 \vee \overline{x_2} \vee x_1 \vee \overline{x_0} \vee y_3 = 1$
15	$x_1 \vee \overline{x_0} \vee y_3 \vee \overline{y_2} \vee \overline{y_1} \vee c_1 = 1$	33	$x_3 \vee y_3 \vee \overline{y_2} \vee y_1 \vee \overline{y_0} = 1$	51	$x_3 \vee x_0 \vee \overline{y_2} \vee \overline{y_1} \vee y_0 \vee c_1 = 1$
16	$x_3 \vee x_1 \vee y_2 \vee y_1 \vee y_0 \vee c_1 \vee \overline{c_0} = 1$	34	$\overline{x_3} \vee x_2 \vee \overline{x_0} \vee \overline{y_1} \vee y_0 \vee c_1 = 1$	52	$\overline{x_2} \vee \overline{x_0} \vee y_3 \vee \overline{y_2} \vee \overline{y_1} \vee \overline{y_0} = 1$
17	$\overline{x_2} \vee x_1 \vee \overline{x_0} \vee y_3 \vee \overline{y_0} \vee c_1 = 1$	35	$\overline{x_2} \vee \overline{x_0} \vee y_2 \vee y_0 \vee \overline{c_1} = 1$	53	$x_2 \vee x_0 \vee \overline{y_2} \vee \overline{y_0} \vee \overline{c_1} = 1$
18	$x_2 \vee x_0 \vee \overline{y_3} \vee \overline{y_2} \vee y_0 \vee c_1 = 1$	36	$\overline{y_1} \vee c_0 = 1$		

Table 7: The constraints used to describe the nontrivial mask propagations for the activeness of Sbox.

No.	Clause	No.	Clause	No.	Clause
1	$x_3 \vee y_3 \vee \overline{y_2} \vee y_1 \vee \overline{y_0} = 1$	15	$x_3 \vee \overline{x_2} \vee x_1 \vee \overline{x_0} \vee y_3 = 1$	28	$x_3 \vee x_2 \vee x_0 \vee \overline{y_1} = 1$
2	$\overline{x_1} \vee y_3 \vee y_2 \vee y_0 = 1$	16	$x_3 \vee x_0 \vee \overline{y_3} \vee y_2 \vee \overline{y_1} \vee \overline{y_0} = 1$	29	$\overline{x_3} \vee \overline{x_2} \vee \overline{x_1} \vee x_0 \vee y_3 \vee y_2 = 1$
3	$x_3 \vee x_2 \vee \overline{y_3} \vee \overline{y_2} \vee \overline{y_1} \vee y_0 = 1$	17	$x_3 \vee x_2 \vee \overline{y_3} \vee y_2 \vee \overline{y_1} \vee \overline{y_0} = 1$	30	$\overline{x_3} \vee x_2 \vee \overline{x_1} \vee \overline{x_0} \vee y_3 \vee y_2 = 1$
4	$x_1 \vee y_3 \vee \overline{y_2} \vee \overline{y_0} = 1$	18	$x_3 \vee x_0 \vee \overline{y_3} \vee \overline{y_2} \vee \overline{y_1} \vee y_0 = 1$	31	$\overline{x_3} \vee x_2 \vee \overline{x_1} \vee \overline{x_0} \vee y_3 \vee y_0 = 1$
5	$\overline{x_3} \vee \overline{x_2} \vee \overline{x_1} \vee x_0 \vee y_3 \vee y_0 = 1$	19	$x_3 \vee \overline{x_2} \vee \overline{x_0} \vee y_1 = 1$	32	$x_3 \vee \overline{x_2} \vee \overline{x_1} \vee \overline{x_0} \vee \overline{y_2} \vee \overline{y_0} = 1$
6	$\overline{x_2} \vee \overline{x_0} \vee y_3 \vee \overline{y_2} \vee \overline{y_1} \vee \overline{y_0} = 1$	20	$x_2 \vee x_1 \vee x_0 \vee \overline{y_3} \vee y_2 \vee \overline{y_1} \vee y_0 = 1$	33	$\overline{x_3} \vee x_2 \vee \overline{x_1} \vee x_0 \vee y_2 \vee y_1 \vee y_0 = 1$
7	$\overline{x_3} \vee x_2 \vee x_0 \vee \overline{y_3} \vee \overline{y_2} \vee \overline{y_0} = 1$	21	$\overline{x_3} \vee \overline{x_2} \vee \overline{x_0} \vee \overline{y_3} \vee y_2 \vee y_0 = 1$	34	$x_2 \vee x_0 \vee \overline{y_2} \vee \overline{y_1} \vee \overline{y_0} = 1$
8	$\overline{x_2} \vee \overline{x_1} \vee \overline{x_0} \vee y_2 \vee y_0 = 1$	22	$\overline{x_3} \vee \overline{x_2} \vee x_1 \vee \overline{x_0} \vee \overline{y_2} \vee \overline{y_1} \vee \overline{y_0} = 1$	35	$\overline{x_2} \vee \overline{x_1} \vee \overline{x_0} \vee \overline{y_3} \vee \overline{y_2} \vee y_1 \vee \overline{y_0} = 1$
9	$\overline{y_0} \vee w = 1$	23	$\overline{y_2} \vee w = 1$	36	$\overline{y_3} \vee w = 1$
10	$y_3 \vee y_2 \vee y_1 \vee y_0 \vee \overline{w} = 1$	24	$\overline{x_0} \vee w = 1$	37	$x_3 \vee x_2 \vee x_1 \vee x_0 \vee \overline{w} = 1$
11	$\overline{x_3} \vee \overline{x_2} \vee x_0 \vee y_3 \vee y_1 \vee y_0 = 1$	25	$\overline{x_3} \vee \overline{x_2} \vee x_0 \vee y_3 \vee y_2 \vee \overline{y_1} = 1$	38	$\overline{x_3} \vee w = 1$
12	$\overline{x_2} \vee w = 1$	26	$\overline{x_3} \vee x_2 \vee \overline{x_0} \vee y_3 \vee \overline{y_1} \vee y_0 = 1$	39	$x_3 \vee \overline{x_1} \vee x_0 \vee \overline{y_3} \vee y_2 \vee \overline{y_0} = 1$
13	$x_3 \vee x_2 \vee \overline{x_1} \vee \overline{y_3} \vee \overline{y_2} \vee y_0 = 1$	27	$\overline{x_3} \vee x_2 \vee \overline{x_0} \vee y_3 \vee y_2 \vee y_1 = 1$	40	$x_3 \vee x_1 \vee x_0 \vee \overline{y_3} \vee \overline{y_2} \vee y_0 = 1$
14	$x_3 \vee x_2 \vee x_1 \vee \overline{y_3} \vee y_2 \vee \overline{y_0} = 1$				

the activeness of the Sbox. If the input and output masks of Sbox are nonzero, it is called an active Sbox, then $w = 1$. Conversely, when $w = 0$, it denotes an inactive Sbox. As a result, 40 clauses, as shown in Table 7, are used to describe the valid linear mask propagations of the WARP's Sbox. These clauses capture the conditions under which the linear propagation holds for the Sbox.

3.3. Modeling the Objective Function. When analyzing primitives that rely on Sboxes as fundamental components, automated searches for linear trails aim to achieve the following two kinds of objectives:

(1) The first kind of objective is to minimize the number of active Sboxes in the trails. To achieve this, auxiliary variables $w^{(i,j)}$ are introduced for each Sbox in each round, where $0 \le i \le r-1$ and $0 \le j \le 31$. The number of active Sboxes is limited at most ξ, where ξ is a positive integer; the objective function is defined as follows:

$$\sum_{i=0}^{r-1} \sum_{j=0}^{31} w^{(i,j)} \le \xi. \tag{8}$$

(2) The second kind of objective is to discover linear trails with optimal correlation. To achieve this, auxiliary variables $c_0^{(i,j)}$ and $c_1^{(i,j)}$ are introduced for each Sbox in each round, where $0 \le i \le r-1$ and $0 \le j \le 31$. The objective is to find linear trails with correlation no more than $2^{-\tau}$, i.e., $2^{-\tau} \le 2^{-(c_0^{(i,j)} + c_1^{(i,j)})}$, where τ is a positive integer. The objective function indicates the opposite number of the binary logarithm of the correlation, that is:

Input: r-round, predefined threshold of the correlation $2^{-\tau}$ (the number of active Sboxes ϵ),
$Flag = 0$ ($Flag = 1$).
Output: If $Flag = 0$ ($Flag = 1$), return a linear trail with optimal correlation (lower bound for the number of active Sboxes).
1: /*Step 1: Construct the SAT model.*/
2: For $t = 0$ to r do
3: For $i = 0$ to 32 do
4: Add the constraints in Equation (4) to describe the mask propagations of three-fork branching.
5: If $i \bmod 2 = 0$:
6: If $flag = 0$:
7: Add the constraints in Table 6 to describe the mask propagations of Sbox with correlations.
8: If $flag = 1$:
9: Add the constraints in Table 7 to describe the mask propagations of the activeness of Sbox.
10: Add the constaints in Equation (5) to describe the mask propagations of XOR operation and π operation.
11: /* Step 2: Find a linear trail.*/
12: If $Flag = 0$ then
13: $m = \tau$, set the objective function to Equation (9).
14: If $Flag = 1$ then
15: $m = \epsilon$, set the objective function to Equation (8).
16: For $v = 0$ to m do
17: Add the constraints to describe the objective function.
18: Invoke the solver to solve the model.
19: If solver finds a solution then
20: Return the r-round linear trail.
21: Else
22: $v++$.

Algorithm 1: The SAT model for searching the linear trails with optimal correlation/lower bound for the number of active Sboxes of WARP

$$\sum_{i=0}^{r-1}\sum_{j=0}^{31}\left(c_0^{(i,j)} + c_1^{(i,j)}\right) \le \tau. \tag{9}$$

Indeed, the objective functions mentioned in Equations (8) and (9) can be expressed as cardinality constraints of the form $\sum_{i=0}^{n-1} x_i \le \eta$, where η is a nonnegative integer. The sequential encoding method proposed in a study by Sinz [31] can be employed to convert these constraints into Boolean expressions [9, 10, 30, 32]. When $\eta = 0$, the constraint is simply $\overline{x_i} = 1$ for $0 \le i \le n-1$, which is trivial. However, for $\eta > 0$, additional Boolean variables $\mu_{i,j}$ are introduced to construct the following clauses, where $0 \le i \le n-2$ and $0 \le j \le \eta - 1$.

$$\begin{cases} \overline{x_0} \vee \mu_{0,0} = 1, & , \\ \overline{\mu_{0,j}} = 1, & \text{if } 1 \le j \le \eta - 1, \\ \overline{x_i} \vee \mu_{i,0} = 1, & \text{if } 1 \le i \le n-2, \\ \overline{\mu_{i-1,0}} \vee \mu_{i,0} = 1, & \text{if } 1 \le i \le n-2, \\ \overline{x_i} \vee \overline{\mu_{i-1,j-1}} \vee \mu_{i,j} = 1, & \text{if } 1 \le j \le \eta - 1, 1 \le i \le n-2, \\ \overline{\mu_{i-1,j}} \vee \mu_{i,j} = 1, & \text{if } 1 \le j \le \eta - 1, 1 \le i \le n-2, \\ \overline{x_i} \vee \overline{\mu_{i-1,\eta-1}} = 1, & \text{if } 1 \le i \le n-2, \\ x_{n-1} \vee \overline{\mu_{n-2,\eta-1}} = 1. \end{cases} \tag{10}$$

Algorithm 1 explains the process of searching for the r-round linear trails. The search model mainly consists of two steps: constructing the linear mask propagations of the r-round function for WARP and setting the corresponding objective function based on the threshold. The objective function of linear analysis is generally in these two forms, as shown in Equation (8) or Equation (9). Invoke the solver to solve the search model. If the model has a solution, it indicates that the model has a feasible solution. For example, when searching for the r-round linear trails with the optimal correlation $2^{-\tau}$, if the objective function in Equation (9) is set to $\tau - 1$ and the model has no solution, and the objective function in Equation (9) is set to τ and the model has a solution, it is considered that the solver has found a r-round linear trail with the optimal correlation of $2^{-\tau}$.

3.4. Modeling the Conditions for Branch-and-Bound Method with Sequential Encoding Method. The branch-and-bound method is a popular approach that finds applications in solving integer programming problems. It is an effective method for systematically exploring the solution space and identifying the optimal solutions. In the context of cryptanalysis, the branch-and-bound method has been successfully utilized to search for optimal solutions, such as differential trails with optimal probabilities [33]. The core concept behind the branch-and-bound method is to break down the solution space into smaller subsets by employing branching techniques.

Table 8: The minimum number of active linear Sboxes.

Round	1	2	3	4	5	6	7	8	9	10	11
#Sbox	0	1	2	3	4	6	8	11	14	17	22
Round	12	13	14	15	16	17	18	19	**20**	**21**	**22**
#Sbox	28	34	40	47	52	57	61	66	**70**	**75**	**79**

Bold values refers to the new results obtained in this paper, and explanations have been added in the paper.

By iteratively branching and calculating bounds, the algorithm progressively narrows down the search space until an optimal solution is found.

In the context of cryptanalysis, let's consider a scenario where we have an initial correlation estimate $Cor_{ini}(R)$ for R-round trails. The information about the optimal correlation $Cor_{opt}(i)$ of the i-round linear trails is known, where $1 \le i \le R-1$. Assuming that the linear trails $(\Gamma^0, \Gamma^1, \ldots, \Gamma^r)$ of the first r rounds have been obtained, the correlation of each round is expressed as $Cor(\Gamma^i, \Gamma^{i+1})$, where $1 \le r \le R$ and $0 \le i \le r$. The question is whether this partial trail has the potential to extend and become a better R-round trail. We can determine this by checking this equation as follows:

$$\prod_{i=0}^{r-1} Cor(\Gamma^i, \Gamma^{i+1}) \cdot Cor_{opt}(R-r) \geqslant Cor_{ini}(R). \tag{11}$$

This condition serves as a criterion for pruning. If a partial trail does not meet this condition, it is unnecessary to explore it further as it cannot lead to a better solution. By pruning such partial trails, the search space is pruned, reducing the computational effort required. The branch-and-bound method, combined with the pruning condition, allows for an efficient search for optimal linear trails in cryptanalysis.

The following equations are utilized to describe the bounding conditions in the branch-and-bound method:

$$\sum_{\gamma=e_1}^{e_2} x_\gamma \le m, e_1 \geqslant 0, e_2 \le n-1, m \le \eta, \tag{12}$$

where n is the total number of Boolean variables represented as x_γ. Referring to the method described in a study by Sun et al. [10], the Equation (12) can be encoded into three cases according to the values of e_1 and e_2. These cases are as follows:

$$\begin{cases} \overline{x_\gamma} \vee \overline{\mu_{\gamma-1,m-1}} = 1, 1 \le \gamma \le e_2, & \text{if } e_1 = 0, e_2 \le n-1, \\ \mu_{e_1-1,\gamma} \vee \overline{\mu_{e_2,\gamma+m}} = 1, 0 \le \gamma \le \eta - m - 1, & \text{if } e_1 > 0, e_2 \le n-1, \\ \left.\begin{array}{l} \mu_{e_1-1,\gamma} \vee \overline{\mu_{n-2,\gamma+m}} = 1, 0 \le \gamma \le \eta - m - 1 \\ \mu_{e_1-1,\gamma} \vee \overline{x_{n-1}} \vee \overline{\mu_{n-2,\gamma+m-1}}, 0 \le \gamma \le \eta - m \end{array}\right\}, & \text{if } e_1 > 0, e_2 = n-1. \end{cases} \tag{13}$$

The number of clauses in the three cases is as follows: e_2 clauses for the first case, $\eta - m$ clauses for the second case, and $2(\eta - m) + 1$ clauses for the third case. By encoding the conditions in these cases into clauses, the branch-and-bound method can be applied effectively in cryptanalysis to explore and prune partial trails.

4. Linear Trails of WARP

In this section, with a primary focus on identifying optimal linear trails, the findings from applying the SAT model to WARP are presented. The goal is to uncover trails that either have the minimum number of active Sboxes or optimal correlations.

4.1. Linear Trail with Minimum Number of Active Sboxes. Through the utilization of the SAT model, we have made significant progress in identifying the optimal linear trail in WARP that requires the minimum number of active Sboxes. It is worth noting that the designer of WARP initially provided the minimum number of active Sboxes for linear trails up to 19 rounds [12]. However, this approach has enabled us to extend this analysis and determine the minimum number of active Sboxes for linear trails up to 22 rounds.

Table 8 shows the comprehensive summary of the minimum number of active Sboxes for the linear trails of round-reduced WARP. These findings confirm the results presented in the referenced work. Specifically, the results marked with bold information indicate that the minimum number of active Sboxes of the 20-round, 21-round, and 22-round linear trails are 70, 75, and 79, respectively. Additionally, the 18-round linear trail with 61 active Sboxes is shown in Table 9. This further contributes to the understanding of the cryptographic and analysis of WARP.

4.2. Linear Trail with Optimal Correlation for WARP. To derive the constraints for the linear approximation of WARP, we begin by setting the objective function to describe the optimal correlation for the r-round linear trails. Through analysis, the optimal correlations of the linear trails up to the first 21 rounds are successfully determined. The results show that the optimal correlation of linear trails can reach the upper bound of the active Sbox estimation. More specifically, for r-round linear trail, if the lower bound of the active Sbox is m, the trails with correlation 2^{-m} can be discovered, where $0 \le r \le 20$ and $0 \le m \le 75$.

Generally, there is a focus on finding linear trails with input and output masks characterized by lower hamming weight. This preference stems from their potential advantages in terms of key recovery, such as involving fewer keys or extending to more rounds. However, it has been observed that linear trails, without additional constraints, may exhibit high hamming weights according to research findings [9, 20]. To address this, the cardinality constraints introduced are used to limit their hamming weights and obtain trails with

Table 9: The 18-round linear trial with 61 active Sboxes for WARP.

Round	Mask	#Sboxes
0	0x0000 0081 0000 0000 1018 0000 2800 2000	0
1	0x0000 0000 1200 0001 0080 0000 0000 0080	3
2	0x0020 0008 0010 0800 0000 000c 0000 0000	5
3	0x0001 8800 8000 0000 0000 0800 c100 0200	8
4	0x0000 0000 0801 8010 0410 2000 0008 8400	13
5	0x1084 0000 0000 0108 8202 4041 0802 0000	18
6	0x0000 1000 0082 0140 2481 0024 1200 0021	26
7	0x2100 1400 0000 0000 0020 0044 4410 0010	33
8	0x0800 0011 0000 4200 0041 0000 4000 0000	37
9	0x0000 2080 1004 0000 0000 0000 0000 0014	41
10	0x4202 0000 0000 0000 0000 0800 0041 0000	43
11	0x0000 0020 0000 0020 1400 0000 0000 8800	47
12	0x0000 0000 0000 0000 0000 8242 0000 0000	49
13	0x0000 0000 0000 0000 0000 0000 2000 2000	51
14	0x0000 0000 0202 0000 0000 0000 0000 0000	51
15	0x2028 0000 0000 0000 0000 0000 0008 0000	53
16	0x0000 0000 0000 0080 8002 0000 0000 0002	55
17	0x0000 0008 0000 0808 0000 0008 0020 0020	57
18	0x0000 8202 8080 0000 0002 0202 8200 0000	61

Table 10: 18-round linear trial with optimal correlation 2^{-61}.

Round	Mask	$Cor_{(\Gamma_{in}^{18}, \Gamma_{out}^{18})}$
0	0xa05a 0000 a500 5000 0000 00aa 0000 0000	1
1	0x0050 0000 0000 00a0 0000 0000 a500 000a	2^{-3}
2	0x0000 0005 0000 0000 0050 000a 00a0 0500	2^{-5}
3	0x0000 0a00 5f00 0500 000a 5e00 a000 0000	2^{-8}
4	0x0af0 5000 000a a500 0000 0000 0a0a e0a0	2^{-13}
5	0xa50a 50aa 0e0a 0000 a0aa 0000 0000 0f0a	2^{-18}
6	0xa5e5 005a a500 00aa 0000 f000 00a5 0aa0	2^{-26}
7	0x0050 005a a5a0 0050 5f00 af00 0000 0000	2^{-33}
8	0x005a 0000 a000 0000 0500 00f5 0000 f500	2^{-37}
9	0x0000 0000 0000 00aa 0000 5050 500a 0000	2^{-41}
10	0x0000 0500 00a5 0000 a505 0000 0000 0000	2^{-43}
11	0x5e00 0000 0000 5b00 0000 0050 0000 0050	2^{-47}
12	0x0000 b5e5 0000 0000 0000 0000 0000 0000	2^{-49}
13	0x0000 0000 5000 5000 0000 0000 0000 0000	2^{-51}
14	0x0000 0000 0000 0000 0000 0000 0505 0000	2^{-51}
15	0x0000 0000 000b 0000 505e 0000 0000 0000	2^{-53}
16	0xb007 0000 0000 0005 0000 0000 0000 00e0	2^{-55}
17	0x0000 000e 0050 0070 0000 000a 0000 060b	2^{-57}
18	0x0005 0a05 ec00 0000 0000 6507 a0b0 0000	2^{-61}

the lowest hamming weight. Due to the fact that the WARP is nibble based, the main focus here is on nibble-oriented activity. The process resembles the search for optimal trails and involves a series of steps as follows:

(1) Within the framework of the model for discovering trails with optimal correlation, we incorporate additional constraints that describe the activeness of the input and output masks for trails. The activeness of a nibble is represented by constraints with Boolean variables. For a nibble mask written as $\Gamma_0 \| \Gamma_1 \| \Gamma_2 \| \Gamma_3$, introduce a Boolean variable to indicate its activeness. When the nibble mask is nonzero, i.e., $\Gamma_0 \| \Gamma_1 \| \Gamma_2 \| \Gamma_3 \neq 0$, then the nibble is called an active nibble, represented by $a = 1$, and in other cases, it is called an inactive nibble, denoted as $a = 0$. The constraints can be formulated as follows:

$$\begin{cases} \overline{\Gamma_0} \vee a & = 1, \\ \overline{\Gamma_1} \vee a & = 1, \\ \overline{\Gamma_2} \vee a & = 1, \\ \overline{\Gamma_3} \vee a & = 1, \\ \Gamma_0 \vee \Gamma_1 \vee \Gamma_2 \vee \Gamma_3 \vee \overline{a} & = 1. \end{cases} \tag{14}$$

(2) Add an objective function to limit the active nibbles for the input and output masks of trails.
(3) Start by setting an initial number of the input and output mask nibbles of the obtained optimal trials.
(4) Query whether there is a solution that satisfies this target value.
(5) Reduce the number of the input and output mask nibbles for linear trails, iterating the process until no solution is obtained.

By employing this approach, the linear trails with the optimal correlation and the fewest active input and output mask nibbles can be identified.

The minimum active input and output masks of linear trails with optimal correlation are denoted as N_c^r, and that of differential trails are denoted as N_d^r. The analysis of the results reveals an observation: $N_c^r = N_d^r$. This equivalence holds for the first 20 rounds of both differential and linear trails, i.e., $N_c^r = N_d^r$ for $1 \leq r \leq 20$. Detailed results are shown in Table 3 in a study by Shi et al. [20]. For instance, the optimal correlations of the 18-, 19-, and 20-round linear trails are 2^{-61}, 2^{-66}, and 2^{-70}, respectively. The specific details of these trails are shown in Tables 10–12, respectively.

5. Improved Linear Distinguishers of WARP

Modern block ciphers are specifically designed to provide resistance against linear cryptanalysis, and their security is often supported by provable limitations on the correlation of linear trails. While many automated tools focus on searching for linear trails, the exploration of linear hulls is equally important. This is due to the intentional design of modern block ciphers to mitigate the presence of dominant trails, thereby enhancing their resistance against linear cryptanalysis. However, by employing advanced automated tools capable of searching for linear hulls, we can analyze multiple trails within a single linear hull. By identifying these trails contributed to a hull, the optimal linear hulls for WARP are successfully discovered.

Table 11: 19-round linear trial with optimal correlation 2^{-66}.

Round	Mask	$Cor_{(\Gamma_{in}^{19}, \Gamma_{out}^{19})}$
0	0xa000 005a 00f0 00aa 0000 0000 5000 005f	1
1	0x000f 0000 a0a5 0000 0000 0000 00f0 00a	2^{-3}
2	0x5000 0005 0000 00f0 000f 0000 00aa 0500	2^{-6}
3	0x0000 0000 5f00 0500 a000 5a0f 0000 00f5	2^{-10}
4	0x00f0 5500 0000 000a 0000 0000 ff50 a000	2^{-15}
5	0x0f00 0000 0aa0 5000 00f5 000a 0000 0f00	2^{-18}
6	0x00aa 0af0 0f00 0000 0000 f000 a505 005f	2^{-23}
7	0x05f0 0000 0000 a0a0 5f5a 0f00 00f5 0000	2^{-29}
8	0x0000 0050 0000 0f0a 5f00 00fa 0a00 ffaa	2^{-34}
9	0x0000 f500 00aa 0000 00a0 f5f5 a5a0 0000	2^{-41}
10	0xa500 0000 0000 5a00 005a 0000 5000 5000	2^{-46}
11	0x0000 a050 0505 0000 0000 0000 0000 00a5	2^{-49}
12	0x5a5f 0000 0000 0000 0000 0500 005f 0000	2^{-52}
13	0x0000 00a0 0000 00f0 ff00 0000 0000 5a00	2^{-56}
14	0x0000 0000 0000 0000 0000 aaff 0000 0000	2^{-58}
15	0x0000 0000 0000 0000 0000 0000 f000 a000	2^{-60}
16	0x0000 0000 0a0f 0000 0000 0000 0000 0000	2^{-60}
17	0xf0a5 0000 0000 0000 0000 0000 000a 0000	2^{-62}
18	0x0000 0000 0000 0050 a00a 0000 0000 000f	2^{-64}
19	0x0000 0005 0000 0a0a 0000 0005 00f0 00a0	2^{-66}

Table 12: 20-round linear trial with optimal correlation 2^{-70}.

Round	Mask	$Cor_{(\Gamma_{in}^{20}, \Gamma_{out}^{20})}$
0	0x5000 00aa 0050 00b5 0000 0000 f000 00a5	1
1	0x0005 0000 a05f 0000 0000 0000 0050 0005	2^{-3}
2	0xf000 000f 0000 0050 0005 0000 005a 0f00	2^{-6}
3	0x0000 0000 ff00 0f00 a000 f505 0000 005f	2^{-10}
4	0x00f0 fa00 0000 000a 0000 0000 5ff0 5000	2^{-15}
5	0x0500 0000 05a0 a000 00ff 0005 0000 0f00	2^{-18}
6	0x005a 0f50 0f00 0000 0000 f000 5a0a 00ff	2^{-23}
7	0x05f0 0000 0000 f0a0 afaa 0500 00f5 0000	2^{-29}
8	0x0000 0050 0000 0f05 5f00 00fa 0f00 5faa	2^{-34}
9	0x0000 f500 005f 0000 00f0 f5ff a5a0 0000	2^{-41}
10	0xf500 0000 0000 5f00 005a 0000 f000 5000	2^{-46}
11	0x0000 f050 050f 0000 0000 0000 0000 00a5	2^{-49}
12	0xff55 0000 0000 0000 0000 0500 005a 0000	2^{-52}
13	0x0000 00f0 0000 0050 aa00 0000 0000 5f00	2^{-56}
14	0x0000 0000 0000 0000 0000 ffa5 0000 0000	2^{-58}
15	0x0000 0000 0000 0000 0000 0000 5000 f000	2^{-60}
16	0x0000 0000 0f05 0000 0000 0000 0000 0000	2^{-60}
17	0x50ff 0000 0000 0000 0000 0000 0005 0000	2^{-62}
18	0x0000 0000 0000 00f0 500a 0000 0000 0005	2^{-64}
19	0x0000 000a 0000 0a05 0000 000f 0050 00a0	2^{-66}
20	0x0000 a50a a050 0000 0005 0a0a fa00 0000	2^{-70}

The estimation of probability for linear hulls $(\Gamma_{in}, \Gamma_{out})$ often relies on the dominant linear trails. However, the research findings in a study by Teh and Biryukov [18] and Shi et al. [20] indicate a notable distinction between the probabilities of differential trails and differentials in WARP. This phenomenon arises due to the multiple trails being present in a differential and similarly, the linear hull may also contain multiple linear trails. Consequently, further investigation into the linear analysis of WARP is required to enhance the estimation of linear hull's probability $ALP(\Gamma_{in}, \Gamma_{out})$. The approach involves enumeration of the linear trails to improve the accuracy of the probability estimation.

The Cryptominisat5 solver [29] is employed to achieve the automated search of linear hulls. This solver is specifically designed to handle XOR operations and solve XOR equation systems using Gaussian elimination. The process involves finding multiple solutions while keeping the input and output masks fixed. However, directly outputting all solutions using the solver may lead to duplicate solutions. To ensure correctness and efficiency, we follow the approach outlined in a study by Kölbl et al. [8] and Liu et al. [9], which involves enumerating multiple solutions step by step.

(1) Step 1: Incorporate the SAT-based model used for searching linear trails.
(2) Step 2: Introduce constraints that fix the input and output masks Γ_{in} and Γ_{out}.
(3) Step 3: Execute the Cryptominisat5 solver to find a solution representing trail t belonging to the linear hull $(\Gamma_{in}, \Gamma_{out})$.
(4) Step 4: Add a new clause describing the obtained solution to the current CNF model to exclude the trail t.
(5) Step 5: Reiterate the process by asking the solver to find a new solution. Repeat steps 3 and 4 until the solver returns unsatisfiable, indicating that all possible solutions within the linear hull have been enumerated.

As shown in Table 13 we present the linear hulls with a clustering effect for the first 20 rounds of WARP. The "$Cor_{(\Gamma_{in}, \Gamma_{out})}$" column represents the optimal correlation of the dominant trails within each linear hull. The "#Trails" column indicates the number of trails searched for within the linear hull. Then, the averaged linear probability of the linear hull is calculated by utilizing these trails. Upon analyzing the findings, as shown in Table 13, it is evident that the linear hulls of the first 9 rounds have only one dominant differential trail, indicating a limited clustering effect. The number of active Sboxes for short trails is relatively small. However, starting from the 10th round, multiple trails appear within the linear hulls. The number of trails within the 13-round linear hulls increases significantly, with the longest-round linear hulls exhibiting the most prominent clustering effect. For instance, the 28,527, 149,447, and 186,856 trails improve the ALP of the 18-round, 19-round, and 20-round linear hulls from 2^{-122}, 2^{-132}, and 2^{-140} to $2^{-109.08}$, $2^{-120.01}$, and $2^{-127.27}$, respectively. We further analyze the distribution of the trails within the linear hulls from 10 to 20 rounds, as shown in Table 14. For example, considering the 13-round linear hull with the given input and output masks as follows:

TABLE 13: The probability of the linear distinguishers with clustering effect for WARP.

Round	Mask	$Cor_{(\Gamma_{in}^r, \Gamma_{out}^r)}$	#Trails	ALP
1	$\Gamma_{in}^1 = 0x0000\ 8000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$ $\Gamma_{out}^1 = 0x0800\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$	2^{-0}	1	2^{-0}
2	$\Gamma_{in}^2 = 0x0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0028$ $\Gamma_{out}^2 = 0x0000\ 0000\ 0000\ 0000\ 0008\ 0000\ 0000\ 0000$	2^{-1}	1	2^{-2}
3	$\Gamma_{in}^3 = 0x0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0020$ $\Gamma_{out}^3 = 0x0000\ 0000\ 0000\ 0000\ 0200\ 0000\ 0002\ 1000$	2^{-2}	1	2^{-4}
4	$\Gamma_{in}^4 = 0x0000\ 1000\ 0012\ 0000\ 0000\ 0000\ 0000\ 0000$ $\Gamma_{out}^4 = 0x0000\ 0000\ 0000\ 0000\ 0200\ 0000\ 0000\ 1000$	2^{-3}	1	2^{-6}
5	$\Gamma_{in}^5 = 0x0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 8240\ 0000$ $\Gamma_{out}^5 = 0x0000\ 0000\ 0000\ 0000\ 0100\ 0000\ 0004\ 2000$	2^{-4}	1	2^{-8}
6	$\Gamma_{in}^6 = 0x8800\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0080$ $\Gamma_{out}^6 = 0x0000\ 4002\ 0080\ 0000\ 0000\ 0002\ 0900\ 0000$	2^{-6}	1	2^{-12}
7	$\Gamma_{in}^7 = 0x0076\ 0000\ 0000\ 0000\ 0000\ c000\ 00c6\ 0000$ $\Gamma_{out}^7 = 0x0000\ 000c\ 0200\ 0000\ 0000\ 100c\ 0060\ 0000$	2^{-8}	1	2^{-16}
8	$\Gamma_{in}^8 = 0x0000\ 0000\ 0000\ 2000\ 0000\ 0024\ 0000\ 0088$ $\Gamma_{out}^8 = 0x0020\ 0800\ 0020\ 0408\ 0000\ 0004\ 0001\ 0020$	2^{-11}	1	2^{-22}
9	$\Gamma_{in}^9 = 0x0088\ 4200\ 0000\ 0000\ 8080\ 0028\ 0000\ 0000$ $\Gamma_{out}^9 = 0x0101\ 0100\ 0000\ 2000\ 8008\ 0000\ c000\ 0800$	2^{-14}	1	2^{-28}
10	$\Gamma_{in}^{10} = 0x8010\ 0000\ 0000\ 0012\ 0088\ 8200\ 0000\ 1000$ $\Gamma_{out}^{10} = 0x0010\ 0200\ 1000\ 0000\ 0202\ 0200\ 400c\ 0000$	2^{-17}	7	$2^{-33.54}$
11	$\Gamma_{in}^{11} = 0x4080\ 0000\ 0000\ 0028\ 0039\ 2800\ 0000\ 8000$ $\Gamma_{out}^{11} = 0x0200\ 0000\ 0002\ d802\ 8c08\ 0040\ 0002\ 1280$	2^{-7}	7	$2^{-43.54}$
12	$\Gamma_{in}^{12} = 0x4000\ 3900\ 4210\ 8200\ 0039\ 0040\ 3982\ 0000$ $\Gamma_{out}^{12} = 0x4902\ 0040\ 0009\ 3940\ 0900\ 0000\ 0009\ 3202$	2^{-28}	3	$2^{-55.83}$
13	$\Gamma_{in}^{13} = 0x24a8\ 0000\ 00c1\ 0088\ 0000\ 0820\ 8024\ 0000$ $\Gamma_{out}^{13} = 0x0010\ 4209\ 0200\ 0802\ 0200\ 1000\ 020c\ 0080$	2^{-34}	1,800	$2^{-65.74}$
14	$\Gamma_{in}^{14} = 0x0082\ 2080\ 1008\ 1021\ 0800\ 0000\ 2000\ 0000$ $\Gamma_{out}^{14} = 0x0020\ 8808\ 0800\ 0802\ 0400\ 8000\ 0808\ 0080$	2^{-40}	8,782	$2^{-75.81}$
15	$\Gamma_{in}^{15} = 0xf000\ 505f\ 5000\ a000\ 5fa5\ aa00\ 5aa0\ 5f00$ $\Gamma_{out}^{15} = 0x0500\ a000\ 0a0a\ 00a0\ 00a0\ a505\ 0a00\ 0a05$	2^{-47}	18,700	$2^{-85.12}$
16	$\Gamma_{in}^{16} = 0xaa00\ aa00\ a5a0\ 5000\ 0000\ 5000\ 0000\ 005b$ $\Gamma_{out}^{16} = 0x0005\ 0a0a\ aa00\ 0000\ 0000\ aa0a\ a0a0\ 0000$	2^{-52}	16,111	$2^{-94.38}$
17	$\Gamma_{in}^{17} = 0xf0f5\ 0000\ ff00\ a000\ 0000\ 00f5\ 0000\ 0000$ $\Gamma_{out}^{17} = 0x0000\ 000f\ 00f0\ 00f0\ 0000\ 0005\ 0000\ 050f$	2^{-57}	31,460	$2^{-101.85}$
18	$\Gamma_{in}^{18} = 0xa05a\ 0000\ a500\ 5000\ 0000\ 00aa\ 0000\ 0000$ $\Gamma_{out}^{18} = 0x0005\ 0a05\ ec00\ 0000\ 0000\ 6507\ a0b0\ 0000$	2^{-61}	28,527	$2^{-109.08}$
19	$\Gamma_{in}^{19} = 0xa000\ 005a\ 00f0\ 00aa\ 0000\ 0000\ 5000\ 005f$ $\Gamma_{out}^{19} = 0x0000\ 0005\ 0000\ 0a0a\ 0000\ 0005\ 00f0\ 00a0$	2^{-66}	149,447	$2^{-120.01}$
20	$\Gamma_{in}^{20} = 0x5000\ 00aa\ 0050\ 00b5\ 0000\ 0000\ f000\ 00a5$ $\Gamma_{out}^{20} = 0x0000\ a50a\ a050\ 0000\ 0005\ 0a0a\ fa00\ 0000$	2^{-70}	186,856	$2^{-127.27}$

$$\begin{cases} \Gamma_{in}^{13} = 0x24a8\ 0000\ 00c1\ 0088\ 0000\ 0820\ 8024\ 0000, \\ \Gamma_{out}^{13} = 0x0010\ 4209\ 0200\ 0802\ 0200\ 1000\ 020c\ 0080. \end{cases} \quad (15)$$

It is found that one trail with correlation 2^{-34} and 664 trails with correlation 2^{-42}. A total of 1800 trails are found to improve the ALP of this 13-round linear hull. The symbols "$*$" in Table 14 indicates not all linear trails with fixed correlation within the linear hull have been found. For example, for the 20-round linear hull with the given input and output masks:

$$\begin{cases} \Gamma_{in}^{20} = 0x5000\ 00aa\ 0050\ 00b5\ 0000\ 0000\ f000\ 00a5, \\ \Gamma_{out}^{20} = 0x0000\ a50a\ a050\ 0000\ 0005\ 0a0a\ fa00\ 0000. \end{cases} \quad (16)$$

Table 14: The distribution of the linear trials belonging to the linear hull for WARP.

Linear hull		Distribution of linear trails								
$(\Gamma_{in}^{10}, \Gamma_{out}^{10})$	$Cor_{(\Gamma_{in}^{10}, \Gamma_{out}^{10})}$	2^{-17}	2^{-18}	2^{-19}	2^{-20}					
	#Trails	1	1	1	4					
$(\Gamma_{in}^{11}, \Gamma_{out}^{11})$	$Cor_{(\Gamma_{in}^{11}, \Gamma_{out}^{11})}$	2^{-22}	2^{-23}	2^{-24}	2^{-25}					
	#Trails	1	1	1	4					
$(\Gamma_{in}^{12}, \Gamma_{out}^{12})$	$Cor_{(\Gamma_{in}^{12}, \Gamma_{out}^{12})}$	2^{-28}	2^{-29}	2^{-30}						
	#Trails	1	0	2						
$(\Gamma_{in}^{13}, \Gamma_{out}^{13})$	$Cor_{(\Gamma_{in}^{13}, \Gamma_{out}^{13})}$	2^{-34}	2^{-35}	2^{-36}	2^{-37}	2^{-38}	2^{-39}	2^{-40}	2^{-41}	2^{-42}
	#Trails	1	6	16	38	100	192	289	494	664
$(\Gamma_{in}^{14}, \Gamma_{out}^{14})$	$Cor_{(\Gamma_{in}^{14}, \Gamma_{out}^{14})}$	2^{-40}	2^{-41}	2^{-42}	2^{-43}	2^{-44}	2^{-45}	2^{-46}	2^{-47}	
	#Trails	1	12	61	271	828	2,179	2, 707*	2, 723*	
$(\Gamma_{in}^{15}, \Gamma_{out}^{15})$	$Cor_{(\Gamma_{in}^{15}, \Gamma_{out}^{15})}$	2^{-47}	2^{-48}	2^{-49}	2^{-50}	2^{-51}	2^{-52}			
	#Trails	168	488	1,072	5,563*	5,912*	5,497*			
$(\Gamma_{in}^{16}, \Gamma_{out}^{16})$	$Cor_{(\Gamma_{in}^{16}, \Gamma_{out}^{16})}$	2^{-52}	2^{-53}	2^{-54}	2^{-55}	2^{-56}				
	#Trails	102	1,124	4,788*	5,449*	4,648*				
$(\Gamma_{in}^{17}, \Gamma_{out}^{17})$	$Cor_{(\Gamma_{in}^{17}, \Gamma_{out}^{17})}$	2^{-57}	2^{-58}	2^{-59}	2^{-60}	2^{-61}	2^{-62}	2^{-63}		
	#Trails	2,579	6,151*	5,124*	5,045*	4,356*	3,769*	4,436		
$(\Gamma_{in}^{18}, \Gamma_{out}^{18})$	$Cor_{(\Gamma_{in}^{18}, \Gamma_{out}^{18})}$	2^{-61}	2^{-62}	2^{-63}	2^{-64}	2^{-65}	2^{-66}	2^{-67}		
	#Trails	6,437	3,900	3,628*	4,165*	4,437*	2,946*	3,014*		
$(\Gamma_{in}^{19}, \Gamma_{out}^{19})$	$Cor_{(\Gamma_{in}^{19}, \Gamma_{out}^{19})}$	2^{-66}	2^{-67}	2^{-68}	2^{-69}	2^{-70}				
	#Trails	300	2,690	32094	54,885	59,478				
$(\Gamma_{in}^{20}, \Gamma_{out}^{20})$	$Cor_{(\Gamma_{in}^{20}, \Gamma_{out}^{20})}$	2^{-70}	2^{-71}	2^{-72}	2^{-73}	2^{-74}	2^{-75}	2^{-76}		
	#Trails	296	5,281	64,342*	63,144*	37,475*	4,876*	11,442*		

The asterisk "*" indicates not all linear trails with fixed correlation within the linear hull have been found.

The results show that there are at least 64,242 trails within the linear hull with a fixed correlation 2^{-72}. These findings provide insights into the clustering effect and distribution of trails within linear hulls for different rounds of WARP.

6. Conclusion

This paper presents a comprehensive investigation into the linear cryptanalysis of WARP. The analysis covers a thorough examination of the cipher's behavior for the first 19 rounds, along with a validation of the lower bound on the number of active Sboxes as stated in the design documentation. Notably, the complexity of finding linear trails escalates as the number of rounds increased, especially considering its 128-bit block size. We leverage the power of the SAT model to efficiently identify optimal linear trails. It was discovered that the correlation of the 18-round linear trails was 2^{-61}. Additionally, recognizing that a linear hull can consist of multiple trails, the researchers found that the probability of the 20-round linear hull improved from 2^{-140} to $2^{-127.27}$. This is the current optimal linear distinguisher for WARP. These findings contribute to the understanding of the vulnerabilities and resistance of WARP against linear cryptanalysis. The next step of the research will further explore the cryptographic properties of WARP or use other attack methods such as differential attacks and meet-in-the-middle attacks to improve the attack results of WARP that provide a more comprehensive security evaluation for WARP.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study is supported by the National Natural Science Foundation of China (grant nos. 61702537 and 62172427).

References

[1] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology — EUROCRYPT '93*, T. Helleseth, Ed., vol. 765 of *Lecture Notes in Computer Science*, pp. 386–397, Springer, Berlin, Heidelberg, 1993.

[2] E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryptosystems," in *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, A. Menezes and S. A. Vanstone, Eds., vol. 537 of *Lecture Notes in Computer Science*, pp. 2–21, Springer, Santa Barbara, California, USA, 1990.

[3] X. Dong and Y. Shen, *Cryptanalysis of Reduced-Round Midori64 Block Cipher*, IACR Cryptology ePrint Archive, 676, 2016.

[4] B. Sun, Z. Liu, V. Rijmen et al., "Links among impossible differential, integral and zero correlation linear cryptanalysis," in *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, R. Gennaro and M. Robshaw, Eds., vol. 9215 of *Lecture Notes in Computer Science*, pp. 95–115, Springer, Santa Barbara, CA, USA, 2015.

[5] N. Mouha, Q. Wang, D. Gu, and B. Preneel, "Differential and linear cryptanalysis using mixed-integer linear programming,"

in *Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers*, C. Wu, M. Yung, and D. Lin, Eds., vol. 7537 of *Lecture Notes in Computer Science*, pp. 57–76, Springer, Beijing, China, 2011.

[6] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song, "Automatic security evaluation and (related-key) differential characteristic search: Application to simon, present, lblock, DES(L) and other bit-oriented block ciphers," in *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, P. Sarkar and T. Iwata, Eds., vol. 8873 of *Lecture Notes in Computer Science*, pp. 158–178, Springer, Kaoshiung, Taiwan, R.O.C, 2014.

[7] S. Sun, D. Gerault, P. Lafourcade et al., "Analysis of aes, skinny, and others with constraint programming," *IACR Transactions on Symmetric Cryptology*, vol. 2017, no. 1, pp. 281–306, 2017.

[8] S. Kölbl, G. Leander, and T. Tiessen, "Observations on the SIMON block cipher family," in *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I, volume 9215 of Lecture Notes in Computer Science*, R. Gennaro and M. Robshaw, Eds., vol. 9215 of *Lecture Notes in Computer Science*, pp. 161–185, Springer, Santa Barbara, CA, USA, 2015.

[9] Y. Liu, Q. Wang, and V. Rijmen, "Automatic search of linear trails in ARX with applications to SPECK and chaskey," in *Applied Cryptography and Network Security - 14th International Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings*, M. Manulis, A.-R. Sadeghi, and S. A. Schneider, Eds., vol. 9696 of *Lecture Notes in Computer Science*, pp. 485–499, Springer, Guildford, UK, 2016.

[10] L. Sun, W. Wang, and M. Wang, "Accelerating the search of differential and linear characteristics with the SAT method," *IACR Transactions on Symmetric Cryptology*, vol. 2021, no. 1, pp. 269–315, 2021.

[11] Y. Zhang, S. Sun, J. Cai, and L. Hu, "Speeding up MILP aided differential characteristic search with matsui's strategy," in *Information Security - 21st International Conference, ISC 2018, Guildford, UK, September 9-12, 2018, Proceedings*, L. Chen, M. Manulis, and S. A. Schneider, Eds., vol. 11060 of *Lecture Notes in Computer Science*, pp. 101–115, Springer, Guildford, UK, 2018.

[12] S. Banik, Z. Bao, T. Isobe et al., "Revisiting GFN for lightweight 128-bit block cipher," in *Selected Areas in Cryptography - SAC 2020 - 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers*, O. Dunkelman, M. J. Jacobson, and C. O'Flynn, Eds., vol. 12804 of *Lecture Notes in Computer Science*, pp. 535–564, Springer, Halifax, NS, Canada (Virtual Event), 2020.

[13] Y. Sasaki and Y. Todo, "New impossible differential search tool from design and cryptanalysis aspects - revealing structural properties of several ciphers," in *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III*, J.-S. Coron and J. B. Nielsen, Eds., vol. 10212 of *Lecture Notes in Computer Science*, pp. 185–215, NTT Secure Platform Laboratories, 2017.

[14] H. Hadipour and M. Eichlseder, "Integral cryptanalysis of WARP based on monomial prediction," *IACR Transactions on Symmetric Cryptology*, vol. 2022, no. 2, pp. 92–112, 2022.

[15] L. Sun, W. Wang, and M. Wang, *Key-Recovery Attacks on CRAFT and WARP (full version)*, IACR Cryptology ePrint Archive, 2022.

[16] Z. Xiang, W. Zhang, Z. Bao, and D. Lin, "Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers," in *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, J. H. Cheon and T. Takagi, Eds., pp. 648–678, vol. 10031 of *Lecture Notes in Computer Science*, 2016.

[17] S. Delaune, P. Derbez, and M. Vavrille, "Catching the fastest boomerangs application to SKINNY," *IACR Transactions on Symmetric Cryptology*, vol. 2020, no. 4, pp. 104–129, 2020.

[18] J. S. Teh and A. Biryukov, "Differential cryptanalysis of WARP," *Journal of Information Security and Applications*, vol. 70, Article ID 103316, 2022.

[19] M. Kumar and T. Yadav, "MILP based differential attack on round reduced WARP," in *Security, Privacy, and Applied Cryptography Engineering - 11th International Conference, SPACE 2021, Kolkata, India, December 10-13, 2021, Proceedings*, L. Batina, S. Picek, and M. Mondal, Eds., vol. 13162 of *Lecture Notes in Computer Science*, pp. 42–59, Springer, Kolkata, India, 2021.

[20] J. Shi, G. Liu, and C. Li, "Improved the automated evaluation algorithm against differential attacks and its application to warp," EasyChair Preprint no. 8736, EasyChair, 2022.

[21] J. Shi, G. Liu, and C. Li, "Constructing the impossible differential of type-ii gfn with boolean function and its application to WARP," *Chinese Journal of Electronics*, vol. 32, Article ID 1, 2022.

[22] H. Hadipour, M. Nageler, and M. Eichlseder, "Throwing boomerangs into feistel structures application to clefia, warp, lblock, lblock-s and TWINE," *IACR Transactions on Symmetric Cryptology*, vol. 2022, no. 3, pp. 271–302, 2022.

[23] J. Daemen, R. Govaerts, and J. Vandewalle, "Correlation matrices," in *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, B. Preneel, Ed., vol. 1008 of *Lecture Notes in Computer Science*, pp. 275–285, Springer, Leuven, Belgium, 1994.

[24] K. Nyberg, "Linear approximation of block ciphers," in *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, A. De Santis, Ed., vol. 950 of *Lecture Notes in Computer Science*, pp. 439–444, Springer, Perugia, Italy, 1994.

[25] Y. Zheng, T. Matsumoto, and H. Imai, "On the construction of block ciphers provably secure and not relying on any unproved hypotheses," in *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, G. Brassard, Ed., vol. 435 of *Lecture Notes in Computer Science*, pp. 461–480, Springer, Santa Barbara, California, USA, 1989.

[26] S. Banik, A. Bogdanov, T. Isobe et al., "Midori: A block cipher for low energy," in *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, T. Iwata and J. Cheon, Eds., vol. 9453 of *Lecture Notes in Computer Science*, pp. 411–436, Springer, Auckland, New Zealand, 2015.

[27] S. J. Russell and P. Norvig, *Artificial Intelligence - A Modern Approach, Third International Edition*, Pearson Education, 2010.

[28] S. A. Cook, "The complexity of theorem-proving procedures," in *Proceedings of the 3rd Annual ACM Symposium on Theory of Computing, May 3-5, 1971, Shaker Heights, Ohio, USA*, M. A. Harrison, R. B. Banerji, and J. D. Ullman, Eds., pp. 151–158, Association for Computing Machinery, Ohio, USA, 1971.

[29] M. Soos, K. Nohl, and C. Castelluccia, "Extending SAT solvers to cryptographic problems," in *Theory and Applications of Satisfiability Testing - SAT 2009, 12th International Conference, SAT 2009, Swansea, UK, June 30 - July 3, 2009. Proceedings*, O. Kullmann, Ed., vol. 5584 of *Lecture Notes in Computer Science*, pp. 244–257, Springer, Swansea, UK, 2009.

[30] S. Wang, D. Feng, B. Hu, J. Guan, T. Shi, and K. Zhang, "The simplest sat model of combining matsui's bounding conditions with sequential encoding method," Cryptology ePrint Archive, Paper 2022/626, 2022.

[31] C. Sinz, "Towards an optimal CNF encoding of boolean cardinality constraints," in *Principles and Practice of Constraint Programming - CP 2005, 11th International Conference, CP 2005, Sitges, Spain, October 1-5, 2005, Proceedings*, P. van Beek, Ed., vol. 3709 of *Lecture Notes in Computer Science*, pp. 827–831, Springer, Sitges, Spain, 2005.

[32] L. Sun, W. Wang, and M. Wang, "More accurate differential properties of LED64 and midori64," *IACR Transactions on Symmetric Cryptology*, vol. 2018, no. 3, pp. 93–123, 2018.

[33] M. Matsui, "On correlation between the order of s-boxes and the strength of DES," in *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, A. De Santis, Ed., vol. 950 of *Lecture Notes in Computer Science*, pp. 366–375, Springer, Perugia, Italy, 1994.