SAT-Based Differential Analysis of the Feistel Block Cipher GRANULE

Ruichen Feng[1], Yueyuan Xi[1], Hongmin Liu[2], and Laifeng Lu[1]
[1]School of Mathematics and Statistics, Shaanxi Normal University, Xi'an, 710119, China
[2]School of Innovation and Entrepreneurship, North University of China, Taiyuan, 030051, China

Given the critical role lightweight block ciphers play in resource restricted scenarios, it is essential to rigorously evaluate their security against classical cryptanalytic methods such as differential analysis. Accordingly, this paper employs automated search techniques to conduct a comprehensive investigation of the differential behavior of the lightweight Feistel-structured cipher GRANULE. In the context of differential cryptanalysis, the core of evaluating a cipher's security lies in identifying high-probability differential characteristics. We formulate the search for such characteristics as a boolean satisfiability problem (SAT), express the propagation of differences through the cipher in conjunctive normal form (CNF), invoke the SAT solver CaDiCaL to determine satisfiability, and recover the corresponding differential characteristics from the obtained solutions. Using this approach, we search for high-probability differential characteristics of GRANULE, and successfully obtain both the minimum number of active S-boxes over all rounds and a 15-round differential characteristic with probability 2^{-60}. Based on this characteristic, we further mount a 19-round key-recovery attack and provide a detailed complexity analysis. Among them, the data complexity is 2^{144}, the time complexity is 2^{144} 19-round encryptions, and the memory complexity is 2^{85}. Our results significantly improve the previously known differential cryptanalysis of GRANULE. And the proposed method is also applicable to other Feistel ciphers with similar structures.

Index Terms—**Lightweight Block Cipher, Feistel Structure, GRANULE, Differential Analysis, Automated Search, SAT.**

I. Introduction

With the widespread deployment of IoT devices [1] and satellite communication systems, block cipher applications in resource-constrained environments face significant challenges, giving rise to the development of lightweight block ciphers. Under such constraints, lightweight cipher designs must strike a balance between low power consumption and sufficient security. However, limited resources inevitably reduce structural complexity and weaken security margins, making the cryptanalysis of lightweight block ciphers increasingly crucial.

Differential cryptanalysis, first introduced by Biham and Shamir in 1990 against the DES algorithm [2], analyzes how input differences propagate through a cipher. Its core idea is to select plaintext pairs with specific input differences, observe the corresponding differences after encryption, and identify high-probability differential characteristics. Such characteristics serve as distinguishers to separate the cipher from a random permutation and can be further extended to key-recovery attacks. Over the past decades, differential cryptanalysis has evolved into multiple variants, including truncated differential attacks [3], boomerang attacks [4], and impossible differential attacks [5]. Recent studies further explore differential behavior in noisy environments, hybrid analytical techniques for grouped cipher structures, and modern developments in differential cryptanalysis [6], [7], [8].

However, as modern ciphers are designed with increasingly strong resistance to classical differential techniques, manually deriving optimal characteristics becomes infeasible due to the large search space and complex propagation rules. This motivates the use of automated approaches to systematically explore differential trails. Among them, SAT-based methods have emerged as one of the most powerful tools.

The core idea of the SAT-based automated search approach is to convert the problem into a Conjunctive normal form (CNF) and employ a SAT solver, such as CaDiCaL [9], to determine its satisfiability. If the CNF instance is satisfiable, the solver outputs the corresponding assignment of variables, which, in the context of differential analysis, directly represents the differential characteristics being searched for. This methodology was first introduced by Mouha and Preneel, who applied SAT techniques to automate the search for optimal differential characteristics of the ARX-based cipher Salsa20 [10]. Subsequently, the approach was adopted to explore differential and linear characteristics of the SIMON family of block ciphers and was later extended to more general constructions, including Feistel, SPN, and ARX designs [11]. In addition, Sun proposed in 2022 the incorporation of Matsui's bounding conditions into the SAT model, which significantly accelerates the search process [12].

The Granule cipher, proposed by Bansod in 2018, is a lightweight block cipher constructed using a Feistel network [13]. using a 64-bit block size and supporting master keys of either 80 or 128 bits. The cipher follows a 32-round Feistel structure, where each round processes data through a nonlinear S-box layer, a bit-permutation layer, and several XOR and rotation operations that ensure sufficient diffusion and confusion across rounds. In the original design, the authors evaluated the cipher against several classical cryptanalytic techniques, including differential analysis, linear analysis, and zero-correlation cryptanalysis. Their results indicated that Granule provides adequate security margins while maintaining strong resistance to these attacks.In 2019, Shi identified five-

Manuscript received July 30, 2025; revised October 17, 2025. Corresponding author: Laifeng Lu (email: lulaifeng@snnu.edu.cn).

round impossible-differential distinguishers for the GRANULE cipher and conducted an eleven-round key-recovery attack [14]. In 2020, Wu reported 144 seven-round impossible-differential distinguishers [15], and in 2024 they updated these results by extending a ten-round distinguisher to mount a sixteen-round attack [16]. Subsequently, several researchers have applied other cryptanalytic techniques to GRANULE, including meet-in-the-middle attacks [17], truncated-differential analysis [18], and linear cryptanalysis [19]. Although various cryptanalytic approaches have been evaluated against Granule, to the best of our knowledge, no systematic study has applied SAT-based automated search to its differential characteristics. Therefore, this work addresses this gap by employing automated techniques to search for the minimum number of active S-boxes and high-probability differential characteristics, thereby enabling an effective differential analysis of the cipher.

This paper investigates the resistance of the GRANULE cipher against differential cryptanalysis using SAT-based techniques. We first construct a complete SAT model that captures differential propagation through both the linear layers and the S-boxes of GRANULE. Based on this model, we systematically determine the minimum number of active S-boxes for all 32 rounds and correct inaccurate estimations reported in the original design specification. Furthermore, the SAT-based automated search enables the identification of previously unknown high-probability differential characteristics. In particular, we obtain an effective 15-round differential characteristic with probability 2^{-60} and extend it to mount a 19-round key-recovery attack, which significantly improves upon the best known differential attacks and their variants on GRANULE. Finally, we provide a detailed analysis of the data, time, and memory complexities of the proposed attack. Although the attack does not threaten the full-round security of GRANULE, it reveals structural weaknesses that reduce its differential security margin. Moreover, the proposed SAT-based framework is generic and applicable to other Feistel-based lightweight block ciphers.

The remainder of this paper is organized as follows. In Section II, we introduce the Granule cipher and the relevant principles of differential cryptanalysis. Then we outline the SAT-based automatic search method and discuss the obtained results in Section III. And in Section IV, we describe a 19-round key-recovery attack on Granule. Finally, Section V presents the conclusion of the paper.

II. Preliminaries

This section provides a brief introduction to the construction of the GRANULE algorithm and the fundamental concepts of differential cryptanalysis.

A. Notation

The main symbols and operators used in this paper are defined as follows:

- PT 64-bit input plaintext block
- CT 64-bit output ciphertext block
- K 128-bit master key
- RK_i 32-bit subkeys for round i
- F F-function
- $\oplus$ Bitwise exclusive-OR operation
- $\lll n$ Left cyclic shift by n bits
- $\ggg n$ Right cyclic shift by n bits
- $\|$ Concatenation of two strings

B. Encryption of GRANULE

The lightweight block cipher GRANULE adopts a Feistel structure. It consists of 32 encryption rounds and operates on a 64-bit block, supporting key lengths of 80 bits and 128 bits. The round key size is 32 bits. Each round function consists of a bit permutation (P-layer), an S-box layer, and a cyclic rotation operation. The overall encryption process is illustrated in Fig. 1.

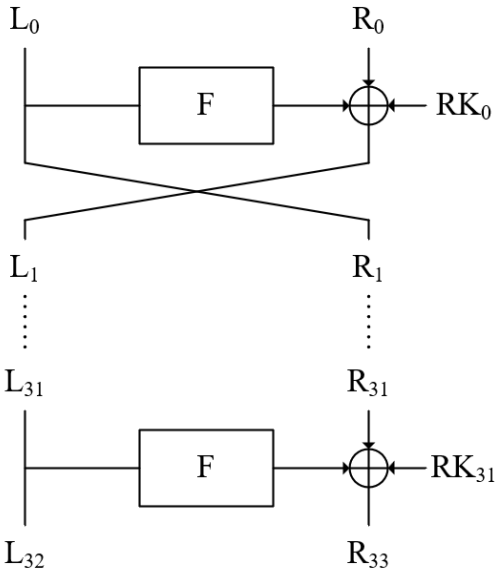

Fig. 1: Block diagram of the GRANULE

The plaintext of GRANULE is divided into two 32-bit halves, denoted by $PT = L_{32} \| R_{32}$. The encryption procedure can be described as follows:

$$\begin{cases} R_i = L_{i-1}, \\ L_i = R_{i-1} \oplus F(L_{i-1}, RK_{i-1}), \end{cases} \quad 1 \le i \le 32. \tag{1}$$

The ciphertext is given by

$$CT = L_{32} \| R_{32},$$

which denotes the concatenation of the two 32-bit halves after 32 rounds.

The round function operates as follows:

$$F(X) = ((S(P(X)) \lll 2) \oplus (S(P(X)) \ggg 7)) \tag{2}$$

P-layer: The 32 bits are divided into eight 4-bit blocks, and the specific block permutation is performed according to Table I.

TABLE I: Permutation Layer of GRANULE

x	0	1	2	3	4	5	6	7
$P[x]$	4	0	3	1	6	2	7	5

S-box: Granule employs eight identical 4×4-bit S-box. The output blocks of the P-permutation are used as the input blocks of the S-box, and the specific S-box is described in Table II.

TABLE II: S-box Layer of GRANULE

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	E	7	8	4	1	9	2	F	5	A	B	0	6	C	D	3

Rotation: The 32-bit output of the S-box layer serves as the input of the rotation layer. A left rotation by 2 bits and a right rotation by 7 bits are performed, and the XOR of the two rotation results is taken as the output of the rotation layer.

C. Differential Cryptanalysis

Differential cryptanalysis is one of the most important criteria for assessing the security of block ciphers. It was introduced by Biham and Shamir at Crypto 1990 and was successfully applied to attack DES, which rapidly established the method as a fundamental tool in the security evaluation of modern symmetric-key ciphers. Differential cryptanalysis studies how input differences of plaintext pairs propagate to output differences of ciphertext pairs during encryption, thereby revealing non-random structures within a cipher and enabling the construction of efficient key-recovery attacks. The method is particularly well suited to iterative cipher structures such as Feistel networks and SPN constructions, because the repeated application of the same round function yields accumulative and (to some extent) predictable differential propagation.

Formally, differential cryptanalysis analyzes the probability distribution of the output difference from ciphertext pair$(C, C\oplus\Delta C)$ that results from a plaintext pair $(P, P\oplus\Delta P)$ after several rounds of encryption. By selecting appropriate input differences, one may identify differential characteristics that hold with a probability significantly higher than that of a random permutation, and such deviations accumulate over multiple rounds and can ultimately be exploited to recover key material.

The propagation of differential characteristics mainly depends on the nonlinear components (notably the S-box) of the round function and on the surrounding linear layers. Since the linear layers are linear over $\mathbb{F}_2$, they do not introduce additional nonlinearity, and their primary role is to propagate and mix differences. The S-boxes, as the only nonlinear elements, are thus the principal source of differential probabilities. To describe the differential behavior of an S-box, we employ the Difference Distribution Table (DDT), which records the number of occurrences (or probabilities) of each input–output differential pair. The DDT of GRANULE is given in Table III.

Our analysis of this DDT reveals that for certain specific input differences the corresponding output differences exhibit fixed-bit patterns, with these properties summarized in Table IV.

TABLE III: Difference Distribution Table for GRANULE

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2
2	0	0	0	4	0	0	4	0	0	0	2	2	0	0	2	2
3	0	4	0	0	0	4	0	0	0	0	2	2	0	0	2	2
4	0	0	0	4	0	0	4	0	0	0	2	2	0	0	2	2
5	0	0	0	0	0	0	4	4	2	2	0	0	2	2	0	0
6	0	0	0	0	0	0	0	0	4	4	0	0	4	4	0	0
7	0	4	0	0	0	4	4	4	0	0	0	0	0	0	0	0
8	0	0	0	2	2	2	0	2	0	0	0	2	2	2	0	2
9	0	2	4	0	2	0	0	0	2	0	0	0	0	2	0	4
A	0	0	0	2	2	2	0	2	0	0	2	0	2	2	2	0
B	0	2	4	0	2	0	0	0	0	2	0	0	2	0	4	0
C	0	0	0	2	2	2	0	2	2	2	0	2	0	0	0	2
D	0	2	4	0	2	0	0	0	0	2	0	4	2	0	0	0
E	0	0	0	2	2	2	0	2	2	2	2	0	0	0	2	0
F	0	2	4	0	2	0	0	0	2	0	4	0	0	2	0	0

TABLE IV: Differential Propagation Feature of the S-box

Input Difference	Output Difference
0001	1⋆⋆⋆
0010	⋆⋆1⋆
0100	⋆⋆1⋆
0110	1⋆0⋆
0111	0⋆⋆⋆

Differential attacks generally proceed in two stages: distinguisher construction and key recovery. A differential distinguisher identifies a high-probability characteristic that distinguishes the cipher from a random permutation. The distinguisher can then be used as the basis of a key-recovery attack, which typically consists of three phases: data collection, filtering (or noise reduction), and key extraction. Using the differential properties provided by the distinguisher, the attacker can recover partial round-key bits and subsequently recover the full key by exhaustive search over the remaining bits.

When evaluating the practicality of differential attacks, three complexity measures are commonly considered: time complexity, data complexity, and memory complexity.

III. SAT-based Search for Differential Characteristics of GRANULE

This section aims to employ SAT techniques to search for the minimum number of active S-boxes and high-probability differential characteristics of the GRANULE cipher. SAT is an NP-complete decision problem that determines whether there exists an assignment of Boolean variables that satisfies a given Boolean formula. In its standard definition, the formula is expressed in Conjunctive Normal Form (CNF), where a CNF formula is a conjunction of multiple clauses, and each clause is a disjunction of literals. Solving a SAT instance is equivalent to finding whether there exists a set of assignments that satisfies all clauses simultaneously.

By modeling the problem of minimizing active S-boxes and the task of searching for high-probability differential characteristics as SAT instances in CNF, we are able to convert differential propagation into a constraint-solving problem. Specifically, we adopt the CaDiCaL solver, as its high

efficiency and good scalability make it suitable for handling large and complex SAT instances arising in cryptanalytic analysis. In the following, we introduce the SAT models for the fundamental components used in our algorithm.

A. Linear Model — 3-XOR

For an n-bit 3-XOR operation, let

$$a = (a_0, a_1, \ldots, a_{n-1}),$$
$$b = (b_0, b_1, \ldots, b_{n-1}),$$
$$c = (c_0, c_1, \ldots, c_{n-1}),$$

be the input differences, and let

$$y = (y_0, y_1, \ldots, y_{n-1})$$

be the corresponding output difference. Then the relation $a \oplus b \oplus c = y$ must satisfy the following conjunctive normal form (CNF) constraints:

$$\begin{cases} a_i \vee b_i \vee c_i \vee \overline{y_i} = 1 \\ a_i \vee b_i \vee \overline{c_i} \vee y_i = 1 \\ a_i \vee \overline{b_i} \vee c_i \vee y_i = 1 \\ \overline{a_i} \vee b_i \vee c_i \vee y_i = 1 \\ \overline{a_i} \vee \overline{b_i} \vee \overline{c_i} \vee y_i = 1 \\ \overline{a_i} \vee \overline{b_i} \vee c_i \vee \overline{y_i} = 1 \\ \overline{a_i} \vee b_i \vee \overline{c_i} \vee \overline{y_i} = 1 \\ a_i \vee \overline{b_i} \vee \overline{c_i} \vee \overline{y_i} = 1 \end{cases} \quad 0 \leqslant i \leqslant n-1.$$

B. Nonlinear Model — S-Box

To model the differential propagation through the S-box in a SAT framework, we rely on the DDT(difference distribution table) of the S-box. Let α and β denote the input and output differences of the S-box, and we introduce an auxiliary binary variable w to indicate the validity of the S-box through Boolean equations $f(\alpha \parallel \beta \parallel w)$. Specifically, the Boolean equation evaluates to 1 in the following cases: when the S-box is active and $w = 1$, or when the S-box is inactive and $w = 0$, and in all other cases, the Boolean equation evaluates to 0. The differential propagation through an active S-box is modeled by the following Boolean equations:

$$\text{If } N_S(\alpha, \beta) = 0: \quad f(\alpha \parallel \beta \parallel w) = 0,$$

$$\text{If } N_S(\alpha, \beta) = 16: \quad f(\alpha \parallel \beta \parallel w) = \begin{cases} 1, & w = 0, \\ 0, & \text{else}, \end{cases}$$

$$\text{If } N_S(\alpha, \beta) = 2 \text{ or } 4: \quad f(\alpha \parallel \beta \parallel w) = \begin{cases} 1, & w = 1, \\ 0, & \text{else}. \end{cases}$$

As an illustrative example, consider the case where the input difference in the S-box is $\alpha = 0001$. According to the difference distribution table (DDT), this input difference can lead to output differences that satisfy the pattern $1 * **$ with nonzero probability. In the SAT model, this differential behavior is captured by imposing Boolean constraints that permit any output difference β whose most significant bit equals 1, while all other output patterns are prohibited. Since the pair (α, β) corresponds to a valid differential transition of the S-box, the auxiliary variable w is constrained to take the value $w = 1$, indicating that this S-box instance is valid. In this way, the variable w correctly reflects the validity of the S-box differential transition and allows the SAT solver to count the number of valid S-boxes in a differential characteristic.

IV. Differential analysis of GRANULE

In this section, we apply the SAT-based automated search method described in Section III to determine the minimum number of active S-boxes and to identify high-probability differential characteristics of GRANULE.

All experiments were conducted on a computer running the Ubuntu operating system, equipped with an Intel(R) Core(TM) i5-8300H CPU @ 2.30 GHz and 16 GB of RAM. Regarding the software environment, all programs for differential analysis were implemented in Python 3.10, LogicFriday 1.1.4 was employed for Boolean logic simplification, and CaDiCal 2.1.3 was used as the SAT solver to perform the automated search. All experiments and evaluations were carried out under the same environment, and the entire experimental process took approximately one week.

A. Experimental Results

We search for the minimum number of active S-boxes for 1–32 rounds of the GRANULE cipher and corrected the erroneous results reported in the original design document. The complete data are summarized in Table V. We observe that the minimum number of active S-boxes increases slowly as the number of rounds grows.

TABLE V: Minimum Number of Active S-box

Round	1	2	3	4	5	6	7	8	9	10	11
S-box	0	1	2	4	5	7	8	12	13	14	16
Round	12	13	14	15	16	17	18	19	20	21	22
S-box	18	19	20	22	24	25	26	28	30	31	32
Round	23	24	25	26	27	28	29	30	31	32	
S-box	34	36	37	38	40	42	43	44	46	48	

In addition, Table VI presents the optimal differential characteristic probabilities from Round 1 to Round 32. Notably, we identified an effective 15-round differential characteristic with probability greater than or equal to 2^{-60}, outperforming all previously known differential cryptanalysis results on GRANULE. The 15-round characteristic is shown in Table VII.

TABLE VI: Optimal Differential Characteristic Probability

Round	1	2	3	4	5	6	7	8
Probability	0	2	4	8	12	18	20	28
Round	9	10	11	12	13	14	15	16
Probability	32	38	42	48	51	55	60	66
Round	17	18	19	20	21	22	23	24
Probability	68	72	76	82	85	89	94	100
Round	25	26	27	28	29	30	31	32
Probability	102	106	110	116	119	123	128	134

Note: The probability value w denotes an exponent such that the differential probability is 2^{-w}.

TABLE VII: The Optimal 15-Round Differential Characteristic

Round	ΔL	ΔR	Probability
1	0x00E00005	0x00180006	2^{-5}
2	0x00000000	0x00E00005	0
3	0x00E00005	0x00000000	2^{-6}
4	0x00200008	0x00E00005	2^{-5}
5	0x00D00009	0x00200008	2^{-6}
6	0x00000000	0x00D00009	0
7	0x00D00009	0x00000000	2^{-6}
8	0x00200008	0x00D00009	2^{-5}
9	0x00E00005	0x00200008	2^{-6}
10	0x00000000	0x00E00005	0
11	0x00E00005	0x00000000	2^{-6}
12	0x00200008	0x00E00005	2^{-5}
13	0x00D00009	0x00200008	2^{-6}
14	0x00000000	0x00D00009	0
15	0x00D00009	0x00000000	2^{-4}
xout	0x00080C04	0x00D00009	2^{-60}

B. Key Recovery Attack

We employ the distinguisher listed in Table VII and extend it by two rounds in both the forward and backward directions to launch a 19-round key-recovery attack. While analyzing the structure of GRANULE, we observe that the round keys of the first and last rounds do not participate in the round-function computation and therefore do not affect differential propagation. Consequently, we use the second-round value ΔL_1 as the plaintext difference ΔR_0, and the input difference to the last round ΔR_{18} as the ciphertext difference ΔR_{19}. The detailed attack path is illustrated in Fig. 2.

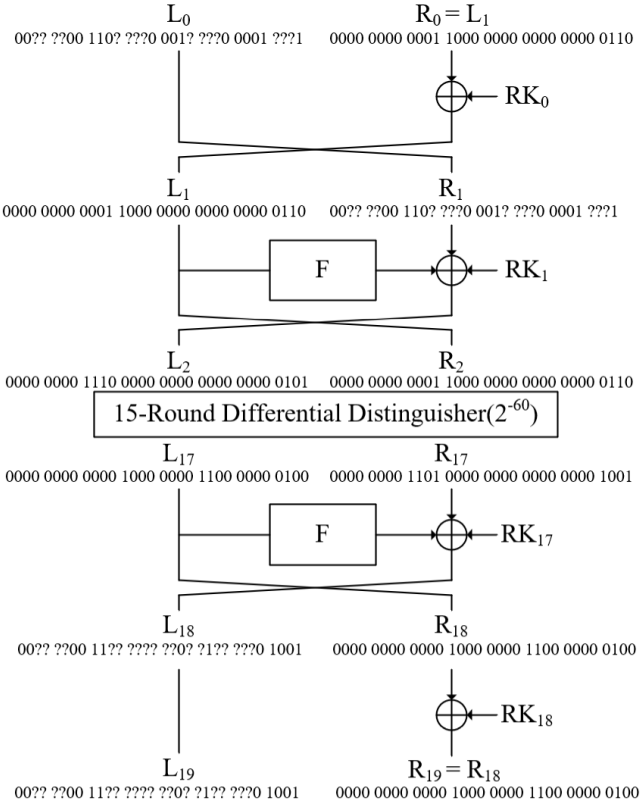

Fig. 2: 19-Round Attack Path

1) Data Collection Phase

In the data collection phase, 2^n structures are selected such that, for each structure, the plaintext pairs (P, P') satisfy the input difference $\Delta P = (\Delta L_0, \Delta R_0)$. Under this condition, there exist 15 unknown bits, and each structure can generate 2^{29} distinct plaintext pairs. These pairs are then encrypted through 19 rounds, resulting in a ciphertext difference $\Delta C = (\Delta L_{19}, \Delta R_{19})$. Given that 45 bits in the ciphertext difference are either inactive or fixed, approximately $2^{29+n-45}$ plaintext–ciphertext pairs can be preliminarily filtered for further analysis. The detailed algorithms are provided as Algorithm 1.

Algorithm 1 Data Collection

```
procedure DataCollectionPhase(n)
    structures ← 2^n
    pairs_filtered ← [ ]
    ΔP ← (ΔL_0, ΔR_0)
    for i ← 1 to structures do
        for j ← 1 to 2^29 do
            P ← random_plaintext()
            P' ← P ⊕ ΔP
            C ← encrypt_19(P)
            C' ← encrypt_19(P')
            ΔC ← C ⊕ C'
            if check_ciphertext_diff(ΔC) then
                pairs_filtered.append((P, P', C, C'))
            end if
        end for
    end for
    return pairs_filtered
end procedure
```

2) Key Recovery Phase

In the key recovery phase, the subkey bits $\mathrm{RK}_{18}[12\text{–}15, 20\text{–}23, 28\text{–}31]$ (a total of 12 bits) are first guessed. For the remaining plaintext–ciphertext pairs, one round of decryption is performed, and the pairs satisfying $\Delta R_{17} = (0000\ 0000\ 1101\ 0000\ 0000\ 0000\ 0000\ 1001)$ are selected, where $R_{17} = F(R_{18} \oplus \mathrm{RK}_{18}) \oplus \mathrm{RK}_{17}$. In the F function, the output differences of the active S-boxes are 1000, 0100, and 1100, with corresponding probabilities of 2^{-4}, 2^{-3}, and 2^{-4}, respectively. Therefore, it is expected that approximately $2^{n-16-11}$ plaintext–ciphertext pairs will remain after this filtering process.

Next, the subkey bits $\mathrm{RK}_0[8\text{–}15, 28\text{–}31]$ (a total of 12 bits) are guessed. For the filtered plaintext–ciphertext pairs, one round of encryption is performed, and the pairs satisfying $\Delta L_2 = (0000\ 0000\ 1110\ 0000\ 0000\ 0000\ 0000\ 0101)$ are selected, where $L_2 = F(R_0 \oplus \mathrm{RK}_0) \oplus \mathrm{RK}_1$. In the F function, the output differences of the active S-boxes are 1000, 0110, and 0001, with corresponding probabilities of 2^{-4}, 2^{-2}, and 2^{-4}, respectively. Consequently, it is expected that approximately $2^{n-27-10}$ plaintext–ciphertext pairs will remain after the final filtering stage.

A 24-bit counter is initialized to record the occurrence frequency of all guessed subkeys. The subkey with the highest counter value is then selected as the correct round key. The

detailed procedures of the key-recovery phase are presented as Algorithm 2.

Algorithm 2 Key Recovery

procedure KEYRECOVERYPHASE($\text{pairs}_{\text{filtered}}$)
  counter $\leftarrow$ zeros(2^{24})
  for $\text{guess}_{\text{RK}_{18}} \leftarrow 0$ to $2^{12}-1$ **do**
    $\text{pairs}_{\text{step1}} \leftarrow [\,]$
    for $(P, P', C, C') \in \text{pairs}_{\text{filtered}}$ **do**
      $R_{18} \leftarrow \text{extract\_R}(C)$
      $R'_{18} \leftarrow \text{extract\_R}(C')$
      $(R_{17}, R'_{17}) \leftarrow \text{decrypt}_1(R_{18}, R'_{18}, \text{guess}_{\text{RK}_{18}})$
      if $\Delta R_{17} = \texttt{0x000D0009}$ **then**
        $\text{pairs}_{\text{step1}}.\text{append}((P, P', C, C'))$
      end if
    end for
    for $\text{guess}_{\text{RK}_0} \leftarrow 0$ to $2^{12}-1$ **do**
      count $\leftarrow 0$
      for $(P, P', C, C') \in \text{pairs}_{\text{step1}}$ **do**
        $R_0 \leftarrow \text{extract\_R}(P)$
        $R'_0 \leftarrow \text{extract\_R}(P')$
        $(L_2, L'_2) \leftarrow \text{encrypt}_1(R_0, R'_0, \text{guess}_{\text{RK}_0})$
        if $\Delta L_2 = \texttt{0x000E0005}$ **then**
          count $\leftarrow$ count $+ 1$
        end if
      end for
      key_index $\leftarrow (\text{guess}_{\text{RK}_{18}} \ll 12) \mid \text{guess}_{\text{RK}_0}$
      counter[key_index] += count
    end for
  end for
  correct_key $\leftarrow \arg\max(\text{counter})$
  return (correct_key $\gg 12$, correct_key&0xFFF)
end procedure

3) Complexity Analysis

By setting $n = 99$, the expected counter value for the correct key is $2^{(n-37-60)} \approx 4$. Therefore, the data complexity of the 19-round differential attack on the GRANULE cipher is approximately $2^{99+15} = 2^{114}$ chosen plaintexts, and the memory complexity is about $2^{99-16} \times 4 = 2^{85}$ data blocks.

The time complexity of the proposed attack is dominated by data collection. Setting $n = 99$ yields an expected count of about 4 for the correct key, requiring roughly 2^{114} chosen plaintext pairs and thus 2^{114} evaluations of the 19-round encryption. The remaining work—key guessing, filtering, and final verification—costs about 2^{95} single-round evaluations and 2^{62} updates, which is negligible in comparison. Therefore, the overall time complexity is 2^{114} 19-round encryptions.

V. CONCLUSIONS

In this work, we conduct a differential cryptanalysis of the GRANULE block cipher to evaluate its resistance against such attacks. Based on the structural properties of the cipher, we construct a SAT-based model and employ automated search techniques to identify both the minimum number of active S-boxes over all rounds and high-probability differential characteristics. Our results successfully reveal the minimum number of active S-boxes for the full 32 rounds, as well as an effective 15-round differential characteristic, which constitutes the best differential distinguisher currently known for GRANULE. Leveraging the 15-round distinguisher, we further mount a 19-round key-recovery attack, with data, memory and time complexities of 2^{114}, $2^{85}$and 2^{114} of 19-round encryptions. Although the attack does not cover the full 32 rounds, and thus does not pose a practical threat to the overall security of GRANULE, it significantly advances the current understanding of its differential security.

Despite the effectiveness of the proposed SAT-based approach in identifying differential characteristics, several limitations should be acknowledged. In particular, the size of the SAT instance grows rapidly with the number of rounds and the level of modeling detail, which may lead to increased computational cost and limit scalability when extending the search to a larger number of rounds or more complex cipher structure.

Moreover, although the proposed 19-round key-recovery attack improves upon previously known differential attacks on GRANULE, its data complexity is extremely large and renders the attack computationally infeasible in practice. Therefore, the primary significance of this attack lies in demonstrating structural properties and reduced differential security margins of the cipher, rather than representing a practical threat to real-world deployments.

We note that reducing the data complexity of such attacks, for example through tighter bounding conditions, or hybrid automated search strategies, remains an interesting direction for future work. These potential optimizations may further enhance the practical relevance of SAT-based differential cryptanalysis.

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China (62572371, 62372076) and the Shaanxi Provincal Natural Science Foundation project (2024JC-YBMS-543).

REFERENCES

[1] G. Li, J. Xu, Q. Wang et al., *Survey of IoT Forensics*, Journal of Computer Engineering & Applications, vol. 58, no. 8, 2022.
[2] E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Journal of Cryptology, vol. 4, no. 1, pp. 3–72, 1991.
[3] L. R. Knudsen, *Truncated and higher order differentials*, in Fast Software Encryption: Second International Workshop, Springer, pp. 196–211, 1994.
[4] D. Wagner, *The Boomerang Attack*, in Fast Software Encryption: 6th International Workshop, Springer, pp. 156–170, 1999.
[5] E. Biham, A. Biryukov and A. Shamir, *Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials*, in Advances in Cryptology—EUROCRYPT'99, Springer, pp. 12–23, 1999.
[6] Y. Xi, R. Feng, Y. Zhou, H. Liu and L. Lu, *Analysis methods for block ciphers under noise interference: a case study of XOR operations*, in Proceedings of the 2025 International Conference on Satellite Internet (SAT-NET 2025), Hangzhou, China, 2025, accepted.
[7] M. Tian, J. Zhou, Z. Qin, B. Liu, L. Lu and H. Liu, *Design of a fusion scheme for linear analysis methods under differences in grouped cipher structures*, in Proceedings of the 2025 International Conference on Networking and Network Applications (NaNA 2025), Tashkent City: NaNA, 2025, doi:10.1109/NaNA66698.2025.00038.

[8] J. Zhou, M. Tian, Z. Wu, L. Lu and Y. Zhou, *Recent advances in differential cryptanalysis of block ciphers*, in Proceedings of the 2025 International Conference on Networking and Network Applications (NaNA 2025), Tashkent City: NaNA, 2025, doi:10.1109/NaNA66698.2025.00069.
[9] A. Biere, T. Faller, K. Fazekas et al., *CaDiCaL 2.0*, in International Conference on Computer Aided Verification, Springer, pp. 3–17, 2024.
[10] N. Mouha and B. Preneel, *Towards Finding Optimal Differential Characteristics for ARX: Application to Salsa20*, IACR Cryptology ePrint Archive, vol. 2013, p. 328, 2013.
[11] S. Kölbl, G. Leander and T. Tiessen, *Observations on the SIMON Block Cipher Family*, in Advances in Cryptology–CRYPTO 2015, Springer, pp. 161–185, 2015.
[12] 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.
[13] G. Bansod, A. Patil and N. Pisharoty, *GRANULE: An Ultra lightweight cipher design for embedded security*, IACR Cryptology ePrint Archive, vol. 2018, p. 600, 2018.
[14] S. Shi and J. He, *Impossible Differential Analysis of GRANULE Algorithm*, Computer Engineering, vol. 45, no. 10, p. 5, 2019.
[15] X. Wu, Y. Li, Y. Wei et al., *Impossible Differential Distinguisher Analysis of GRANULE and MANTRA Algorithms*, Journal of Communications, 2020.
[16] X. Wu, J. Kuang, R. Zhang et al., *Impossible Differential Analysis of GRANULE Algorithm Based on SAT*, Journal of Computer Applications, vol. 44, no. 3, pp. 797–804, 2024.
[17] X. Liu and Y. Zhang, *Meet-in-the-Middle Analysis of Reduced-Round GRANULE Algorithm*, Modeling and Simulation, vol. 14, 2025.
[18] X. Liu and Y. Liu, *Truncated Impossible Differential Analysis of GRANULE Algorithm*, Journal of Shanxi Normal University (Natural Science Edition), vol. 37, no. 1, pp. 41–51, 2023.
[19] Z. Yan, L. Li and Y. Wei, *Perfect Linear Approximations of Ultra-Lightweight Block Ciphers LiCi, LiCi-2 and GRANULE*, Acta Electronica Sinica, pp. 1–7, 2025.

Ruichen Feng was born in 2000. He is currently pursuing his master's degree at the School of Mathematics and Statistics, Shaanxi Normal University, specializing in cryptography. His research direction is design and security analysis of cryptographic algorithms.

Yueyuan Xi is a master's student at the School of Mathematics and Statistics, Shaanxi Normal University. Her research focuses on the analysis of cryptographic algorithms.

Hongmin Liu received the M.S. degree in computer application technology from North University of China, Taiyuan, China in 2007. Her research interests include computer application and computer network security

Laifeng Lu received the Ph.D. degree from Xidian University, Xi'an, China, in 2012. She is currently an Associate Professor of the School of Mathematics and Statistics, Shaanxi Normal University. Her research interests include cryptography and information security .