Differential Cryptanalysis of the Improved-DLBCA Lightweight Block Cipher

Yige Zhu[1], Yihui Zhou[1,2], Yanping Li[3], Zhenqiang Wu[1,2]
[1]School of Artificial Intelligence and Computer Science, Shaanxi Normal University, 710119, Xi'an, China
[2]Shaanxi Key Laboratory of Network and System Security, Xidian University, 710071, Xi'an, China
[3]School of Mathematics and Statistics, Shaanxi Normal University, 710119, Xi'an, China

As resource-constrained devices become increasingly prevalent in satellite communication systems, evaluating whether lightweight ciphers such as Improved-DLBCA can provide both efficiency and security has become an essential task. Motivated by these practical needs, this paper presents a comprehensive security assessment of Improved-DLBCA, a lightweight block cipher designed specifically for constrained environments. Through SAT-based automated search methods, we perform detailed differential cryptanalysis of the algorithm, identifying optimal 11-round differential characteristics with probability 2^{-31} and constructing a practical key-recovery attack on 14-round Improved-DLBCA with time complexity $2^{61.5}$ encryption equivalents. Our results validate the SAT methodology for lightweight cipher analysis and offer important security insights for satellite communication applications.

***Index Terms*—Block Cipher, Lightweight Cryptography, Differential Cryptanalysis, SAT, Improved-DLBCA.**

I. Introduction

In satellite communication systems, terminal devices frequently operate under stringent resource constraints, including limited computational power, memory, and energy availability [1]. Under such restricted conditions, systems must satisfy requirements related to real-time performance, reliability, and long-term autonomous operation. Traditional cryptographic algorithms, however, rely heavily on complex nonlinear components and substantial hardware resources, leading to high latency, increased power consumption, and significant implementation overhead. These limitations underscore the need for lightweight cryptographic mechanisms that can provide adequate security while remaining suitable for deployment in resource-constrained satellite environments.

Within this context, lightweight block ciphers have gained prominence in both academic research and practical applications [2], [3]. By reducing computational complexity, hardware footprint, and energy consumption while preserving essential security guarantees, such ciphers enable secure and efficient communication across satellite systems, IoT devices, and embedded platforms. Their implementation-friendly characteristics make them strong candidates for security solutions operating under strict resource limitations.

Numerous lightweight ciphers have been proposed and analyzed over the past decade, each aiming to balance security and efficiency. For instance, PRESENT and GIFT are among the most studied designs, with extensive differential analyses confirming their security margins under various attack models. Similarly, ciphers like SIMON and SPECK have undergone rigorous evaluation in both software and hardware contexts. These analyses often reveal subtle trade-offs between round count, nonlinear layer complexity, and achievable security levels. Improved-DLBCA enters this landscape as a design optimized for gate count reduction, yet its differential security—particularly in light of its reduced S-box count—remains insufficiently explored. This paper therefore contributes to the broader effort of evaluating emerging lightweight designs against established cryptanalytic benchmarks, ensuring they meet security expectations before deployment in sensitive environments such as satellite communications.

Differential cryptanalysis, introduced by Biham and Shamir in 1990 [4], remains one of the most fundamental and widely used techniques for evaluating the security of block ciphers. By analyzing how differences propagate through encryption rounds, it enables the construction of distinguishers and key-recovery attacks, making it especially relevant for lightweight designs where nonlinear resources are reduced. Advances in automated differential search, machine-learning-assisted analysis, and complex system modeling [5], [6] have further expanded the analytical capabilities available to cryptographers; these advances allow practitioners to explore large characteristic spaces efficiently and to derive more accurate estimates of a cipher's security margin in realistic operating conditions.

Improved-DLBCA is an optimized variant of the original DLBCA cipher [7], redesigned to satisfy the constraints of low-cost and low-power hardware implementations [8]. The cipher maintains the 32-bit block size, 80-bit key size, and 32-round structure but reduces the number of 4-bit S-boxes per round from eight to four, lowering the hardware cost from 1116 GE to 1028 GE. This concrete reduction in nonlinear components is attractive from an implementation perspective, since it directly translates to lower gate counts and reduced dynamic power consumption in silicon or FPGA realizations. Although the designers claimed comparable resistance to differential and boomerang attacks relative to the original design, the substantial reduction of nonlinear components raises important questions regarding its actual differential security, motivating a more thorough evaluation that examines both worst-case and typical-case differential behaviours.

This paper conducts a comprehensive differential secu-

Manuscript received September 30, 2025; revised December 9, 2025.
Corresponding author: Zhenqiang Wu (email: zqiangwu@snnu.edu.cn).

rity assessment of Improved-DLBCA based on modern SAT-solving techniques [9]. By encoding the cipher's differential propagation constraints as Boolean satisfiability problems, we systematically explore optimal differential characteristics and determine the minimum number of active S-boxes across all 32 rounds. The SAT-based approach supports exhaustive and provable searches within constrained parameter spaces, and it is particularly well suited to lightweight ciphers where combinatorial S-box interactions dominate the security analysis. In contrast to conventional manual differential search methods, which rely heavily on experience-driven reasoning and partial exploration, the proposed SAT-based framework enables the complete enumeration of all valid differential characteristics under a fixed probability bound, ensuring that no security-critical trails are overlooked even as the number of rounds increases. Using the characteristics derived from SAT solving, practical distinguishers are constructed, and feasible key-recovery attacks are demonstrated on reduced-round variants, providing both theoretical insights and empirical confirmation of the cipher's security margin. These experimental validations serve to quantify the practical impact of the S-box reduction and to identify thresholds where the trade-off between implementation efficiency and security becomes unfavorable.

The remainder of the paper proceeds as follows. In Section II, the necessary notations and the description of Improved-DLBCA are introduced. Details of the SAT-based automated methodology appear in Section III. The obtained differential characteristics and active S-box analysis are discussed in Section IV. Experimental key-recovery results are presented in Section V. Concluding remarks and future research directions are provided in Section VI.

II. Preliminaries

This section introduces the necessary preliminary knowledge. First, the notations used in this paper are presented. Then, the lightweight block cipher Improved-DLBCA is described. Finally, relevant knowledge of differential cryptanalysis is introduced.

A. Notations

The mathematical notations and terminology used in this paper are defined as follows. Let $\mathbb{F}_2$ denote the binary field, and $\mathbb{F}_2^n$ represent an n-dimensional vector space over $\mathbb{F}_2$.

TABLE I: Mathematical Notations and Terminology

Notation	Description
ΔX	XOR difference in variable X
X_L, X_R	Left and right halves of a 32-bit block X
nibble	A 4-bit unit (S-box input/output)
F	Round function of Improved-DLBCA
S	4-bit S-box used in substitution layer
P	Bit permutation layer
k_i, K_i	Round key for round i
a, b, c	Input/output differences of XOR operations
x, y	Input/output differences of S-boxes
p_0, p_1, p_2	Auxiliary probability variables
n	Bit length in operations
$\log_2 p$	Logarithmic probability of differential characteristic

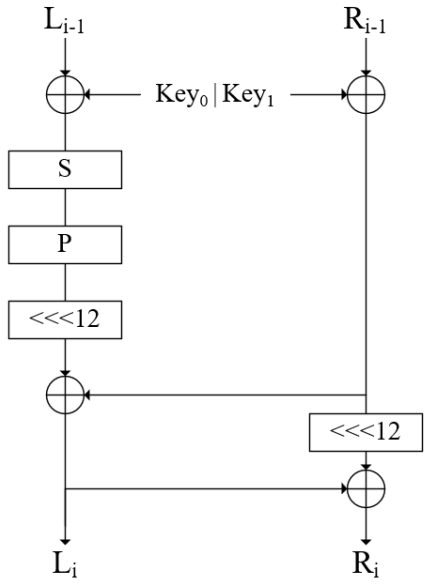

Fig. 1: Diagram of Improved-DLBCA algorithm

B. Description of the Improved-DLBCA Algorithm

The Improved-DLBCA algorithm is a lightweight block cipher improvement scheme proposed by Al-Dabbagh et al. in 2018 for the original DLBCA algorithm [8]. Its core objective is to further reduce the hardware implementation cost on resource-constrained devices while maintaining security strength. The algorithm inherits the overall framework of DLBCA, adopting a Feistel-like structure as shown in Fig. 1. It has a block length of 32 bits, a key length of 80 bits, and the encryption process iterates for 32 rounds.

The encryption process of the Improved-DLBCA algorithm is illustrated in Figure 1. In each encryption round, the 32-bit intermediate state is divided into left and right 16-bit branches. The round function F sequentially performs a series of operations on the right branch, including non-linear transformation and linear permutation. The result is then XORed with the left branch. Finally, the left and right branches are swapped to form the input for the next round. The round function primarily consists of the following four operational layers:

1) The First Layer (Key Addition)

The 32-bit round key is XORed with the 32-bit round input. The result is then split into left and right 16-bit halves, with the left half proceeding to the second layer.

2) The Second Layer (S-box Substitution)

This layer is the core for achieving the confusion property. It employs four identical 4-bit S-boxes applied in parallel to perform non-linear transformation on the 16-bit left half. The S-box used in Improved-DLBCA has good cryptographic properties. Its specific values are given in Table II.

3) The Third Layer (Permutation)

This layer provides diffusion by applying a fixed bit permutation to the 16-bit S-box output. The permutation rules are

TABLE II: 4-bit S-box Used in Improved-DLBCA

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

specified in Table III, which systematically rearranges bits to ensure effective diffusion throughout the data block.

TABLE III: 16-bit Permutation Mapping

Input	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Output	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15

4) The Fourth Layer (Branch Mixing)

This layer first cyclically left-shifts the output from the third layer (the left branch) by 12 bits. The result is then XORed with the current right branch, and this becomes the left branch for the next round. Subsequently, the original right branch is cyclically left-shifted by 12 bits and then XORed with the new left branch, with this result becoming the right branch for the next round.

The key schedule of the algorithm is used to generate the required 32-bit round keys from the 80-bit master key. Considering that in differential cryptanalysis, the XOR operation with the round key does not affect the propagation of differences, the key schedule process is not detailed in this paper. Specific details can be found in reference [8].

C. Differential Cryptanalysis

Differential cryptanalysis, a chosen-plaintext attack framework first proposed by Biham and Shamir in 1990 [4], has become one of the core analytical methods for assessing the security of block ciphers. Its fundamental principle involves analyzing the probability distribution of how a specific input difference (i.e., a fixed XOR value between a pair of plaintexts) propagates through the iterative round functions of the encryption process to form an output difference. If the probability of a particular differential path (or differential characteristic) is significantly higher than the expected probability for a random permutation, then this path constitutes a valid "distinguisher". An attacker can utilize this distinguisher by collecting a sufficient number of plaintext-ciphertext pairs, combined with partial key guessing and verification, to eventually recover the secret key.

III. SAT-Based Automated Search Method

This section establishes a differential propagation model for the Improved-DLBCA algorithm based on SAT [9]. By formally describing the algorithm's linear and nonlinear operations as a set of Boolean constraints, an SAT solver can be utilized to search for all feasible differential paths under specified input and output difference conditions. This process enables the identification of the optimal differential characteristic and the minimum number of active S-boxes [10]. This chapter details the construction methodology and the core concepts behind the model.

A. Linear Operation Model

The linear operations in the Improved-DLBCA algorithm include XOR operations, bit permutations, and cyclic shifts. Since these operations are both invertible and linear, the deterministic linear relationships between input and output differences in differential propagation analysis can be precisely characterized by a system of Boolean equations.

1) XOR Operation

For an n-bit XOR operation, let $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$ be the n-bit input differences, and $y = (y_0, y_1, \ldots, y_{n-1})$ be the n-bit output difference. Then, $(a, b) \to y$ forms a valid differential path **if and only if** the following condition holds for every bit position i where $0 \leq i \leq n-1$:

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

2) Permutation and Shift Operations

For the permutation operation, this process is a bijective mapping and does not introduce new logical variables. The cyclic shift operation can be viewed as a special form of permutation and can also be directly implemented through index mapping. Consequently, the linear layer of Improved-DLBCA can be fully embedded into the SAT model in the form of deterministic logical constraints.

B. Nonlinear Operation Model

1) S-box

For a 4-bit S-box with a differential uniformity of 4, the entries in its Differential Distribution Table (DDT) only contain the four values: 0, 2, 4, and 16, corresponding to probabilities of 0, 2^{-3}, 2^{-2}, and 1, respectively. Therefore, three auxiliary variables p_0, p_1, p_2 can be introduced, and the sum $p_0 + p_1 + p_2$ is used to represent the probability weight of the valid differential pattern.

Probability Encoding Scheme: The auxiliary variables p_0, p_1, p_2 encode the logarithmic probability weight as follows:

- $p = (1, 1, 1)$: probability 2^{-3}
- $p = (0, 1, 1)$: probability 2^{-2}
- $p = (0, 0, 0)$: probability 1

The total differential characteristic probability is computed by summing the weights of all active S-boxes along the path.

Let x and y be the 4-bit input and output differences of the S-box, respectively, and let $p = (p_0, p_1, p_2)$. The tuple $(x, y, p) \in \mathbb{F}_2^{11}$, and the differential propagation pattern of the S-box is characterized by the following Boolean function $f(x \parallel y \parallel p)$.

Based on the characterization of the S-box DDT, we first derive the corresponding truth-table representation of valid differential transitions using dedicated scripts. The resulting truth tables are then converted into conjunctive normal form (CNF) using the Logic Friday tool, which enables an efficient

TABLE IV: Minimum Active S-boxes for 1-32 Rounds

Rounds	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Active S-boxes	0	1	2	3	4	5	6	8	9	11	12	14	15	17	18	20
Rounds	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Active S-boxes	21	22	24	25	26	28	29	30	32	33	34	36	37	38	40	41

Boolean encoding of the 4-bit S-box differential probabilities for subsequent SAT solving.

$$f(x \parallel y \parallel p) = \begin{cases} 0, & \text{if } \mathrm{DP}_S(x,y) = 0 \\ 1, & \text{if } \mathrm{DP}_S(x,y) = 2^{-3} \text{ and } p = (1,1,1) \\ 1, & \text{if } \mathrm{DP}_S(x,y) = 2^{-2} \text{ and } p = (0,1,1) \\ 1, & \text{if } \mathrm{DP}_S(x,y) = 1 \text{ and } p = (0,0,0) \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

IV. Differential Distinguisher

Our SAT-based differential characteristic search was implemented using the CaDiCaL SAT solver [11] on a Kali Linux system. This section presents the experimental results of differential distinguishers constructed for the Improved-DLBCA algorithm. Using the SAT-based automated search method described in Section III, we first determined the minimum number of active S-boxes for the Improved-DLBCA algorithm from 1 to 32 rounds, correcting the erroneous values provided by the authors in the design document, as detailed in Table IV.

Furthermore, this paper presents the optimal differential characteristics for the full 32 rounds of the Improved-DLBCA algorithm. Among them, the effective differential characteristics (with probability greater than or equal to 2^{-32}) extend up to 11 rounds. Table V shows the optimal differential characteristics of Improved-DLBCA from 1 to 32 rounds, including their input differences, output differences, and probabilities in logarithmic form. In this paper, all input/output differences or values are represented in hexadecimal form, omitting the "0x" prefix.

Additionally, based on the SAT model for searching differential characteristics and by adding constraints to exclude found solutions, this paper successfully identified 12 differential characteristics for 11 rounds with probability 2^{-31}. The input and output differences of these differential characteristics are detailed in Table VI. It is worth noting that among these differential characteristics, no two share identical input and output differences.

V. Differential Attack

This section presents a systematic differential cryptanalysis of the 14-round Improved-DLBCA block cipher. The cryptanalysis is based on an 11-round differential distinguisher with probability 2^{-31}, extended by 2 rounds forward and 1 round backward to construct a key recovery attack on the full 14-round cipher.

As a hardware-optimized version of DLBCA [7], the Improved-DLBCA algorithm has significant application value in resource-constrained environments. However, the reduction in the number of S-boxes raises concerns about its differential security. This research aims to evaluate the security margin of this algorithm in practical deployment by constructing effective differential paths.

The fundamental principle of differential cryptanalysis utilizes the statistical characteristics of differential propagation in cryptographic algorithms. When the probability of a specific input difference leading to a specific output difference is significantly higher than the expected value for a random permutation, attackers can construct effective distinguishers and further obtain key information through key recovery attacks [4].

A. Differential Path Construction

Based on the SAT automated search method [10], we obtained the complete differential propagation path for 14-round Improved-DLBCA. This path is carefully optimized to ensure sufficient probability while controlling the number of active S-boxes in the extended rounds.

TABLE V: Optimal 1-32 Round Differential Characteristics

Rounds	Input Difference	Output Difference	Probability ($\log_2 p$)
1	(0000|0001)	(0001|1001)	0
2	(0000|E000)	(E600|E8E0)	-2
3	(0000|0400)	(0044|4040)	-3
4	(0C00|4000)	(0044|4040)	-4
5	(9C00|C004)	(0044|4040)	-8
6	(E000|8800)	(8008|0808)	-12
7	(0A00|8004)	(8008|0808)	-15
8	(A000|4008)	(0044|4040)	-18
9	(A000|4008)	(4073|4477)	-22
10	(3000|4480)	(9191|1111)	-26
11	(E0A0|4802)	(9191|1111)	-31
12	(3000|4480)	(3809|2389)	-35
13	(0008|1119)	(8808|0088)	-40
14	(0000|9009)	(8188|8918)	-43
15	(0000|9009)	(9090|9999)	-46
16	(0000|9009)	(9010|9910)	-50
17	(0000|9009)	(0188|0918)	-53
18	(0000|9009)	(9090|9999)	-56
19	(0000|9009)	(9009|0909)	-60
20	(0000|9009)	(0188|0918)	-63
21	(0000|9009)	(9090|9999)	-66
22	(0000|9009)	(9939|00A0)	-70
23	(0000|9009)	(0188|0918)	-73
24	(0000|9009)	(9090|9999)	-76
25	(0000|9009)	(BB19|2280)	-80
26	(0000|9009)	(8188|8918)	-83
27	(0000|9009)	(9090|9999)	-86
28	(0008|1119)	(9090|9999)	-90
29	(0000|9009)	(8188|8918)	-93
30	(0000|9009)	(9090|9999)	-96
31	(0000|9009)	(9939|00A0)	-100
32	(0000|9009)	(8188|8918)	-103

TABLE VI: All 2^{-31} Probability Differentials Characteristics

No.	Input Difference	Output Difference
1	(E00A|4801)	(9191|1111)
2	(E0A0|4802)	(1191|9111)
3	(E0A0|4802)	(9191|1111)
4	(E00A|4801)	(1191|9111)
5	(00E0|42A0)	(8191|0111)
6	(E0A0|4802)	(0191|8111)
7	(E0A0|4802)	(8191|0111)
8	(E00A|4801)	(8191|0111)
9	(00E0|42A0)	(0191|8111)
10	(E00A|4801)	(0191|8111)
11	(00E0|42A0)	(1191|9111)
12	(00E0|42A0)	(9191|1111)

TABLE VII: 14-Round Differential Propagation Path

Round		Differential State (32 bits)							
0	ΔP:	????	????	????	????	????	????	????	????
1	ΔX_1^S:	????	????	????	????	????	????	0100	????
	ΔX_1^P:	????	????	????	????	????	????	0100	????
	ΔX_1^{Sh}:	????	????	????	????	????	????	????	0100
	ΔX_1^{XOR}:	????	????	????	????	????	????	????	0100
2	ΔX_2^S:	????	????	????	0000	0010	0100	0000	0100
	ΔX_2^P:	0100	1110	0101	0000	0010	0100	0000	0100
	ΔX_2^{Sh}:	0100	1110	0100	0010	0010	0100	0000	0100
	ΔX_2^{XOR}:	0010	0100	1110	0100	0100	0010	0100	0000
3-13	Input:	0000	0000	1110	0000	0100	0010	1010	0000
	Output:	0000	0001	1001	0001	1000	0001	0001	0001
14	ΔX_{14}^S:	0000	????	????	????	1000	0001	0001	0001
	ΔX_{14}^P:	0???	0???	0???	0???	1000	0001	0001	0001
	ΔX_{14}^{Sh}:	0???	0???	0???	0???	1000	0001	0001	0001
	ΔX_{14}^{XOR}:	1???	0???	0???	0???	1???	1???	0???	0???

1) Differential Path Structure

The complete 14-round differential characteristic consists of three core components:

Forward Extension (2 rounds): 2-round extension added before the core distinguisher, ensuring smooth connection with the core distinguisher

Core Distinguisher (11 rounds): Efficient distinguisher with probability 2^{-31}

Backward Extension (1 round): 1-round extension added after the core distinguisher

2) Differential Propagation Table

Table VII shows the complete 14-round differential propagation path. Here, ΔX_i^S, ΔX_i^P, ΔX_i^{Sh}, and ΔX_i^{XOR} represent the differential states after the i-th round S-box substitution, permutation, cyclic shift, and XOR operations, respectively.

3) Active S-box Analysis

The distribution of active S-boxes in the differential path directly affects the attack complexity:

- **Round 1**: 1 active S-box (nibble 6)
- **Round 2**: 3 active S-boxes (nibbles 4, 5, 7)
- **Round 14**: 4 active S-boxes (nibbles 4, 5, 6, 7)

B. Key Recovery Attack Procedure

A systematic differential key recovery attack on 14-round Improved-DLBCA is presented in this subsection. The attack leverages an 11-round differential distinguisher with probability 2^{-31}, extended by 2 rounds forward and 1 round backward. The attack procedure is modularized into three distinct phases for recovering keys at rounds 1, 2, and 14.

1) Data Collection

We collect $N = 2^{33}$ plaintext-ciphertext pairs (P, C) satisfying the input difference condition ΔP. Given the distinguisher probability $p = 2^{-31}$, the expected number of right pairs is $N \times p = 4$, while the expected number of accidental satisfactions is approximately $N \times 2^{-32} \approx 2$. The storage requirement for these pairs is approximately 128GB. While this data complexity is feasible in academic cryptanalysis, practical deployment in resource-constrained environments like satellite communications would face challenges including time overhead, bandwidth limitations, and detectability concerns, making the attack primarily a theoretical security assessment.

2) Key Recovery Attack Procedure

The comprehensive key recovery attack integrates three sequential phases targeting rounds 1, 2, and 14, respectively. Each phase employs a dedicated algorithm to recover the corresponding round key bits, with the overall procedure processing each of the 2^{33} plaintext-ciphertext pairs through these sequential stages. The following algorithms detail the procedures for each phase.

Algorithm 1 Round 1 Key Recovery (4-bit K_1)

Input: Plaintext pair (P, P') with ΔP
Output: Candidate keys k_1 for round 1

```
candidates ← [ ]
for k1 = 0 to 2^4 − 1 do
    Compute ΔX_1^S via partial encryption with k1
    if ΔX_1^S[nibble 6] = 0100 then
        candidates.append(k1)
    end if
end for
return candidates
```

The first phase, detailed in Algorithm 1, recovers the 4-bit round key K_1 by enumerating all possible values and verifying consistency with the differential pattern at nibble 6.

Algorithm 2 Round 2 Key Recovery (12-bit K_2)

Input: (P, P'), candidate k_1 from Algorithm 1
Output: Candidate pairs (k_1, k_2)

```
candidates ← [ ]
for k2 = 0 to 2^12 − 1 do
    Compute ΔX_2^S via partial encryption with (k1, k2)
    if ΔX_2^S satisfies nibbles 4,5,7 pattern then
        candidates.append((k1, k2))
    end if
end for
return candidates
```

Building upon successful recovery of K_1, Algorithm 2 extends the attack to recover the 12-bit round key K_2 by verifying the differential patterns at nibbles 4, 5, and 7.

The final phase, implemented in Algorithm 3, recovers the 16-bit round key K_{14} through partial decryption and verification of differential patterns at nibbles 4-7. Counters are maintained for all potential 32-bit key combinations, with the most statistically prominent combination identified as correct. This enables subsequent reconstruction of the master key through reverse application of the key schedule algorithm.

3) Complexity Analysis

Detailed calculations are given below.

Time Complexity: The dominant factor in time complexity arises from the nested key guessing across three rounds. For

Algorithm 3 Round 14 Key Recovery (16-bit K_{14})

Input: (C, C'), candidate (k_1, k_2) from Algorithm 2
Output: Updated counter array

```
for k14 = 0 to 2^16 − 1 do
    Compute ΔX_14^S via partial decryption with k14
    if ΔX_14^S satisfies nibbles 4-7 pattern then
        idx ← (k1 ≪ 28) | (k2 ≪ 16) | k14
        count[idx] ← count[idx] + 1
    end if
end for
return count
```

each of the 2^{33} plaintext pairs, we test 2^4 K_1 candidates, 2^{12} K_2 candidates, and 2^{16} K_{14} candidates. The total operations are equivalent to:

$$T_{\text{total}} = 2^{33} \times (2^4 + 2^{16} + 2^{32}) \times \frac{1}{14} \approx 2^{33} \times 2^{32} \times \frac{1}{14} = 2^{61.5} \text{ encryption equivalents}$$

where the $\frac{1}{14}$ factor accounts for the reduced cost of partial encryption/decryption compared to full 14-round encryption.

Memory Complexity: The memory requirements consist of two main components:

- Plaintext-ciphertext pair storage: $2^{33} \times 16$ bytes $= 128$ GB
- Counter array for key candidates: $2^{32} \times 4$ bytes $= 16$ GB

The total memory consumption of approximately 144 GB is feasible in modern computing environments.

Success Probability: Using Selçuk's analytical model for differential cryptanalysis with parameters $N = 2^{33}$, $p = 2^{-31}$ and $a = 32$ key bits, we obtain a success probability of $P_s \approx 84\%$, indicating a high likelihood of successful key recovery.

VI. Conclusions

This paper has presented a systematic differential cryptanalysis of the Improved-DLBCA lightweight block cipher, yielding several significant contributions to the field of lightweight cryptography.

The primary contributions of this work can be summarized as follows:

- **Security Evaluation**: We have conducted the first comprehensive differential analysis of the 32-round Improved-DLBCA cipher, establishing precise security bounds for the algorithm.
- **SAT Methodology**: Our research demonstrates an efficient automated approach for differential characteristic search using the CaDiCaL solver, which successfully identified 11-round characteristics within minutes.
- **Key Findings**: Our analysis revealed several important security properties:
  - The minimum number of active S-boxes for 32 rounds is 41
  - We discovered 12 distinct 11-round differential characteristics with probability 2^{-31}
  - We constructed a 14-round key recovery attack with complexity $2^{61.5}$ encryption equivalents
- **Security Implications**: Our results indicate that Improved-DLBCA achieves a reasonable balance between hardware efficiency and security, with the 32-round version providing adequate security margins for resource-constrained applications.

This work not only validates the basic security of Improved-DLBCA but also demonstrates the effectiveness of SAT-based methods for analyzing lightweight ciphers. The methodologies developed in this study provide a foundation for future security evaluations of similar cryptographic algorithms.

Acknowledgments

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

References

[1] X. Guo and L. Ma, "Survivability Analysis of Satellite-Based Networks Under Solar Storm Hazards," *Journal of Networking and Network Applications*, vol. 4, no. 4, pp. 157–164, 2024.
[2] 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 *Proc. 2025 Int. Conf. Netw. Netw. Appl. (NaNA)*, Tashkent, Uzbekistan, 2025.
[3] P. Shao, G. Zhang, and M. Li, "Automatic Search for Differential Characteristics in ARX Ciphers," in *Proc. 2014 10th International Conference on Natural Computation (ICNC)*, pp. 1009–1013, 2014.
[4] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," in *Proc. 10th Annual International Cryptology Conference on Advances in Cryptology*, pp. 2–21, 1990.
[5] J. Zhou, M. Tian, Z. Wu, L. Lu, and Y. Zhou, "Recent Advances in Differential Cryptanalysis of Block Ciphers," in *Proc. 2025 Int. Conf. Netw. Netw. Appl. (NaNA)*, Tashkent, Uzbekistan, 2025.
[6] J. Zhou, Y. Zhu, M. Tian, L. Lu, and Y. Zhou, "Cryptanalysis of Block Ciphers with Noise: A Case Study on Permutation Operations," in *Proc. 2025 Int. Conf. Netw. Netw. Appl. (NaNA)*, Tashkent, Uzbekistan, 2025.
[7] S. Salim and M. Aldabbagh, "Design 32-bit Lightweight Block Cipher Algorithm (DLBCA)," in *Proceedings of the International Journal of Computer Applications*, vol. 166, no. 8, 2017.
[8] S. Aldabbagh, A. G. Sulaiman, I. Shaikhli, K. Al-Enezi, and A. Alenezi, "Improving the Cost Factor of DLBCA Lightweight Block Cipher Algorithm," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, no. 2, pp. 786–791, 2018.
[9] M. Soos, K. Nohl, and C. Castelluccia, "Extending SAT Solvers to Cryptographic Problems," in *Proc. SAT 2009*, LNCS, vol. 5584, pp. 244–257, 2009.
[10] L. Sun, W. Wang, and M. Wang, "Accelerating the Search of Differential and Linear Characteristics with the SAT Method," *Cryptology ePrint Archive*, Report 2021/213, 2021.
[11] A. Biere, T. Faller, K. Fazekas, M. Fleury, N. Froleyks, and F. Pollitt, "CaDiCaL 2.0," in *Proc. Computer Aided Verification - 36th International Conference, CAV 2024*, LNCS, vol. 14681, pp. 133–152, 2024.
[12] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," in *Proc. CHES 2007*, LNCS, vol. 4727, pp. 450–466, 2007.
[13] J. Zhao, S. Xu, Z. Zhang, X. Dong, and Z. Li, "Differential Cryptanalysis of the Lightweight Block Cipher GIFT," *J. Cryptologic Res.*, vol. 5, no. 4, pp. 335–343, 2018.
[14] J. Lu, G. Liu, L. Xiong, B. Sun, and C. Li, "Differential Attack on Lightweight PFP Algorithm," *J. Cryptologic Res.*, vol. 11, no. 6, pp. 1293–1307, 2024.

Yige Zhu was born in 2001. He is currently pursuing his master's degree at the School of Artificial Intelligence and Computer Science, Shaanxi Normal University. His research focuses on the design and analysis of block cipher.

Yihui Zhou received the B.S. degree in mathematics and applied mathematics, the M.S. degree in fundamental mathematics, and the Ph.D. degree in fundamental mathematics from Shaanxi Normal University, Xi'an, China, in 2003, 2006, and 2009, respectively. She is currently a Lecturer of the School of Artificial Intelligence and Computer Science, Shaanxi Normal University, Xi'an, China. Her research interests include information security and privacy preserving.

Yanping Li received the M.S. degree from Shaanxi Normal University in 2004 and the Ph.D. degree from Xidian University, Xi'an, China, in 2009. She is currently an Associate Professor of the School of Mathematics and Statistics, Shaanxi Normal University. Her research interests include public key cryptography and its applications in machine learning.

Zhenqiang Wu received the B.S. degree in 1991 from Shaanxi Normal University, China, and received the M.S. and Ph.D degrees in 2002, and 2007 respectively, all from Xidian University, China. He is currently a full professor of Shaanxi Normal University, China. Dr. Wu's research interests include computer communications networks, mainly wireless networks, network security, anonymous communication, and privacy protection etc. He is a member of ACM and senior of CCF.