# Differential Cryptanalysis of a Lightweight Block Cipher LELBC 

Manjeet Kaur, Tarun Yadav, Manoj Kumar<br>Dhananjoy Dey


#### Abstract

In this study, we investigate the newly developed low energy lightweight block cipher (LELBC), specifically designed for resource-constrained Internet of Things (IoT) devices in smart agriculture. The designers conducted a preliminary differential cryptanalysis of LELBC through mixed-integer linear programming (MILP). This paper further delves into LELBC's differential characteristics in both single and related-key frameworks using MILP, identifying a nine-round differential characteristic with a probability of $2^{-60}$ in a single-key framework and a 12round differential characteristic with a probability of $2^{-60}$ in a related-key framework.


Index Terms-Differential Cryptanalysis, LELBC, Lightweight Block Cipher, MILP.

## I. Introduction

Nowadays, the Internet of Things (IoT) plays a crucial role in various sectors, including agriculture, healthcare, industry, and transportation. However, IoT devices face limitations in resources, such as computing power and energy, making traditional cryptographic techniques inadequate for ensuring data security. To address this problem, lightweight cryptography has emerged, leading to the development of numerous lightweight block ciphers like PRESENT [1], SKINNY [2], GIFT [3], WARP [4], IVLBC [5], and HDLBC [6] etc. Recently, a low energy lightweight block cipher (LELBC) has been proposed by Song et al. [7] for IoT devices with limited resources, particularly for smart agriculture. This cipher is based on a novel structure called the 'permutation substitution permutation', incorporating two symmetric diffusion layers and a sublayer. The diffusion process involves left circular shifts and XOR operations, while the Sublayer is made up of 16 involutory 4-bit S-boxes. To ensure encryption and decryption are consistent, a permutation is applied after executing all 16 rounds. The designers conducted the security evaluation of LELBC, measuring its resilience against a range of attacks including dependency and avalanche effect, differential and linear attacks [8], algebraic attack, as well as meet-in-themiddle and slide attacks. In their differential cryptanalysis, the designers determined the minimal number of active S boxes through a bit-oriented mixed integer linear programming

[^0](MILP) program for up to 12 rounds, asserting that the fullround LELBC is resistant to differential attack. However, their evaluation did not take into account the probabilities associated with the S-box difference distribution table (DDT), an essential factor in determining the cipher's strength more accurately. Additionally, they did not analyze the cipher's resistance to related-key differential attack, in which attackers exploit differences in keys to slightly propagate state differences. These gaps highlight the basis of our investigation, which aims to conduct an in-depth security analysis of the cipher, specifically focusing on its resilience to differential attack in both single and related-key frameworks. Currently, differential cryptanalysis is studied through methods such as Boolean Satisfiability and Satisfiability Modulo Theory (SAT/SMT), MILP, and Constraint Programming (CP) [9]. In this study, we apply the MILP method to assess the security of LELBC against differential attack. This involves transforming the problem of finding the minimum number of active S-boxes and optimal differential characteristics into a MILP problem, which is then addressed through the Gurobi ${ }^{1}$ solver.

## Contribution

In this paper, we study the LELBC against differential cryptanalysis in single and related-key frameworks through the MILP method including the probabilities of DDT of LELBC's S-box. We determine the exact lower bounds on the number of active $S$-boxes and probabilities up to 13 rounds, providing a nine-round differential characteristic in a single-key framework. Further, we identify valid differential characteristics up to 12 rounds and present a 12-round differential characteristic in a related-key framework.

## Organization

The rest of the paper is organized as follows: Section II describes the related work to our study. The comprehensive details of the LELBC lightweight block cipher are elaborated in Section III. Section IV discusses the MILP modeling of LELBC for identifying differential characteristics of LELBC in both single and related-key frameworks. Subsequent findings and analyses of these characteristics are presented in Section V. Finally, the paper is concluded in Section VI.

[^1]
## II. Related Work

This section reviews existing studies related to the cryptanalysis of lightweight block ciphers.
Cao and Zhang [10] introduced related-key differential characteristics for the two reduced versions of block cipher GIFT (GIFT-64 and GIFT-128) through MILP model, utilizing these characteristics to execute key recovery attacks on a reduced version of GIFT-64. Weng et al. [11] analyzed LBlock's resistance to related-key differential attack, providing tighter security bounds. Their SMT-based analysis determined the minimum number of active $S$-boxes and the upper bounds of probabilities for up to 19 rounds of LBlock. Additionally, they demonstrated key-recovery attacks on both 22- and 23round of LBlock. Chan et al. [12] assessed the differential attack resilience of SLIM and LCB, two lightweight block ciphers. For SLIM, they provided differential characteristics for all rounds and demonstrated a key recovery attack on 14 rounds. Moreover, they identified LCB's linearity due to its S-box design, subsequently improving LCB by substituting its S-box with PRESENT. Teh et al. [13] presented new differential cryptanalysis results for the lightweight block cipher BORON, including high-probability differentials and key recovery attacks against BORON-80/128. For WARP, Teh and Biryukov [14] presented differential distinguishers and mounted key-recovery differential attacks in single and related-key frameworks. Further, they identified a boomerang distinguisher for rectangle attack on WARP. Mahzoun et al. [15] presented differential attack on a variant of K-Cipher with a complexity of $2^{29.7}$ for specific parameters. Zhang et al. [16] discussed an impossible differential attack on FBC128 , a block cipher. The authors constructed 9 -round truncated impossible differentials, leading to a 13 -round key recovery attack. Cui et al. [17] identified differential characteristics in MANTIS, Midori-128, and QARMA-64 using the SAT method, incorporating Matsui's bounding conditions and the technique of dichotomy. Furthermore, they provided a keyrecovery differential attack for Midori-128 and QARMA64. Nobuyuki et al. [18] assessed RBFK's vulnerability to differential, linear, and meet-in-the-middle attacks, concluding it lacks security against such attacks. They demonstrated keyrecovery attacks on full-round RBFK, highlighting weaknesses in key scheduling and round functions, and suggested improvements to withstand such attacks. Li et al. [19] constructed fullround differential characteristics with MILP for both Shadow32 and Shadow-64, versions of the lightweight block cipher Shadow. Additionally, they demonstrated a full-round keyrecovery attack on both versions. İLTER and SELÇUK [20] proposed two alternative MILP models for multiple XOR operations. They found differential and linear characteristics for Klein and Prince in single-key frameworks.

## III. LELBC

The key generation and encryption algorithms of LELBC are discussed in this section.

## A. Key Generation

Initially, the key generation process is employed on the key $(K)$ to derive the first round subkey $\left(S K_{1}\right)$. Subsequently,

```
Algorithm 1 Key Generation
Require: \(K=k_{0}| | k_{1}| | k_{3}\|\ldots\| k_{126} \| k_{127}\)
Ensure: \(S K_{i}, \forall i \in\{1,2, \ldots, 16\}\)
    for \(i \leftarrow 1\) to 16 do
        \(K_{0}\left\|K_{1}\right\| K_{2} \| K_{3} \leftarrow K\)
        \(k_{124}| | k_{125}| | k_{126}| | k_{127} \leftarrow S\left(k_{124}| | k_{125}| | k_{126}| | k_{127}\right)\)
        \(k_{121}| | k_{122}| | k_{123}| | k_{124} \leftarrow\left(k_{121}| | k_{122}| | k_{123}| | k_{124}\right) \oplus(i-1)\)
        \(k_{0}\left\|k_{1}\right\| k_{3}\|\ldots\| k_{126}\left\|k_{127} \leftarrow k_{64}\right\| k_{65}\left\|k_{66}\right\| \ldots\left\|k_{62}\right\| k_{63}\)
        \(k_{0}\left\|\left|k_{1}\left\|k_{3}\right\| \ldots\right|\left|k_{62}\right|\left|k_{63} \leftarrow k_{9}\right| \mid k_{10}\right\| k_{11}\|\ldots\| k_{7} \| k_{8}\)
        \(k_{64}\left\|k_{65}\right\| k_{66}\|\ldots\| k_{126}\left\|k_{127} \leftarrow k_{79}\right\| k_{80}\left\|k_{81}\right\| \ldots\left\|k_{77}\right\| k_{78}\)
        \(S K_{i} \leftarrow K\)
    end for
```

| TABLE I |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| S-BOX |  |  |  |  |  |  |  |
| $\mathbf{x}$ |  |  |  |  |  |  |  |
| $\mathbf{x}$ |  |  |  |  |  |  |  |
| $\mathbf{S}(\mathbf{x})$ |  |  |  |  |  |  |  |
| C |  |  |  |  |  |  |  |

for each round, the key generation process utilizes the subkey from the preceding round to obtain the subsequent round's subkey. This process comprises three operations: an S-box for substitution, an addition of a round constant, and left circular shift, as elaborated in Algorithm 1. In $i^{\text {th }}$ round, the high 64bit ( $K_{0} \| K_{1}$ ) of the subkey $\left(S K_{i}\right)$ is used, where $K_{0}$ and $K_{1}$ undergo XOR operations with the left and right 32-bit of $X$, respectively.

## B. Encryption

LELBC, a block cipher, operates on a 128-bit key and a 64-bit plaintext to produce a 64-bit ciphertext over 16 rounds. Each round consists of XOR, add round key, sublayer (see Table I), and left circular shift operations. The process starts by splitting the plaintext into two branches: left $\left(X_{0}\right)$ and right $\left(X_{1}\right)$. Initially, the left branch, $X_{0}$, is combined with the key $K_{0}$ using an XOR operation. Subsequently, the right branch, $X_{1}$, is XORed with the result of applying a 5-bit left circular shift to the updated $X_{0}$. Following the application of the sublayer to both branches, then $X_{0}$ is XORed with the result of a 5-bit left circular shift applied to $X_{1}$, and $X_{1}$ is XORed with $K_{1}$. After the final round, $X_{0}$ and $X_{1}$ are swapped to generate the ciphertext. The encryption process is illustrated in Figure 1 and Algorithm 2.

## IV. MILP Model of LELBC

The differential attack in block ciphers is currently addressed using the mixed-integer linear programming (MILP) method. This method converts the cipher's operations, including XOR, S-boxes, and left circular shift operation, into linear inequalities, as follows:

## A. XOR Operation in Terms of Linear Inequalities

For the XOR operation with input bit differences $(x, y)$ and output difference $z$, this operation is described by the

```
Algorithm 2 Encryption of LELBC
Require: \(X, S K_{i} ; \forall i \in\{1,2, \ldots, 16\}\)
Ensure: \(Y\)
    for \(i \leftarrow 1\) to 16 do
        \(K_{0}\left\|K_{1}\right\| K_{2} \| K_{3} \leftarrow S K_{i}\)
        \(X_{0} \leftarrow K_{0} \oplus X_{0}\)
        \(X_{1} \leftarrow X_{1} \oplus\left(X_{0} \lll 5\right)\)
        \(X_{0}\left\|X_{1} \leftarrow S\left(X_{0}\right)\right\| S\left(X_{1}\right)\)
        \(X_{0} \leftarrow X_{0} \oplus\left(X_{1} \lll 5\right)\)
        \(X_{1} \leftarrow K_{1} \oplus X_{1}\)
    end for
    \(Y \leftarrow X_{1} \| X_{0}\)
    return \(Y\)
```



Fig. 1. Encryption Process
following linear inequalities:

$$
\begin{align*}
-x+y+z & \geq 0 \\
x-y+z & \geq 0  \tag{1}\\
x+y-z & \geq 0 \\
x+y+z & \leq 2
\end{align*}
$$

## B. S-box in Terms of Linear Inequalities

Given $\left(u_{0}, u_{1}, u_{2}, u_{3}\right)$ and $\left(y_{0}, y_{1}, y_{2}, y_{3}\right)$ as input and output differences for a 4-bit S-box, we consider the input-output differential as a point $\left(u_{0}, u_{1}, u_{2}, u_{3}, y_{0}, y_{1}, y_{2}, y_{3}\right) \in \mathbb{F}_{2}^{8}$. Then compute the H-representation of the convex hull of all possible input-output differentials of the S-box using the double description method. This process yields numerous linear inequalities, some of which may be redundant and hinder model efficiency. To minimize these inequalities, we employ a reduction algorithm leveraging the MILP technique, as suggested by Sasaki and Todo [21]. There are 21 linear
inequalities to represent the S-box of LELBC as follows:

$$
\left.\begin{array}{rl}
1 u_{0}+1 u_{1}+0 u_{2}+1 u_{3}+1 y_{0}-2 y_{1}-1 y_{2}-2 y_{3} \geq & -3 \\
1 u_{0}-1 u_{1}-2 u_{2}-1 u_{3}+3 y_{0}+2 y_{1}+3 y_{2}+2 y_{3} \geq & 0 \\
-2 u_{0}+2 u_{1}-3 u_{2}-1 u_{3}+2 y_{0}-1 y_{1}+1 y_{2}+2 y_{3} \geq & -4 \\
1 u_{0}-1 u_{1}-1 u_{2}+2 u_{3}-1 y_{0}-2 y_{1}+2 y_{2}+2 y_{3} \geq & -3 \\
2 u_{0}+2 u_{1}+1 u_{2}-1 u_{3}-2 y_{0}-1 y_{1}-3 y_{2}+2 y_{3} \geq & -4 \\
1 u_{0}+1 u_{1}+0 u_{2}+1 u_{3}+1 y_{0}+1 y_{1}-1 y_{2}+1 y_{3} \geq & 0 \\
3 u_{0}+2 u_{1}+3 u_{2}+2 u_{3}+1 y_{0}-1 y_{1}-2 y_{2}-1 y_{3} \geq & 0 \\
1 u_{0}+3 u_{1}+0 u_{2}+2 u_{3}-3 y_{0}+1 y_{1}+1 y_{2}-3 y_{3} \geq & -3 \\
-1 u_{0}+1 u_{1}+3 u_{2}+2 u_{3}-3 y_{0}+2 y_{1}-1 y_{2}+0 y_{3} \geq & -2 \\
-1 u_{0}+2 u_{1}+2 u_{2}+1 u_{3}-3 y_{0}-1 y_{1}-1 y_{2}+2 y_{3} \geq & -3 \\
-1 u_{0}+2 u_{1}-1 u_{2}+1 u_{3}-1 y_{0}+2 y_{1}+0 y_{2}-2 y_{3} \geq & -3  \tag{2}\\
-2 u_{0}-1 u_{1}-3 u_{2}+2 u_{3}+2 y_{0}+2 y_{1}+1 y_{2}-1 y_{3} \geq & -4 \\
-3 u_{0}+1 u_{1}+1 u_{2}-3 u_{3}+1 y_{0}+3 y_{1}+0 y_{2}+2 y_{3} \geq & -3 \\
-3 u_{0}-3 u_{1}+1 u_{2}+1 u_{3}+1 y_{0}+2 y_{1}+0 y_{2}+3 y_{3} \geq & -3 \\
1 u_{0}-2 u_{1}-1 u_{2}+1 u_{3}-2 y_{0}+2 y_{1}-2 y_{2}+1 y_{3} \geq & -5 \\
-1 u_{0}-1 u_{1}+0 u_{2}-1 u_{3}+2 y_{0}+3 y_{1}+1 y_{2}+3 y_{3} \geq & 0 \\
-1 u_{0}+1 u_{1}-2 u_{2}+2 u_{3}-2 y_{0}-2 y_{1}+1 y_{2}+2 y_{3} \geq & -4 \\
1 u_{0}+0 u_{1}+0 u_{2}+0 u_{3}+0 y_{0}-1 y_{1}-1 y_{2}-1 y_{3} \geq & -2 \\
1 u_{0}-2 u_{1}+1 u_{2}-2 u_{3}-1 y_{0}-1 y_{1}+0 y_{2}-1 y_{3} \geq & -5 \\
-1 u_{0}-1 u_{1}+0 u_{2}-1 u_{3}+1 y_{0}-2 y_{1}+1 y_{2}-2 y_{3} \geq & -5 \\
0 u_{0}-1 u_{1}-1 u_{2}-1 u_{3}+1 y_{0}+0 y_{1}+0 y_{2}+0 y_{3} \geq & -2
\end{array}\right\}
$$

To find the exact probabilities of the differential characteristics of a cipher, we consider the differential behavior of the S-box with probabilities. There are three entries 2, 4, and 16 in the DDT of the S-box. Therefore, we need to take two more variables $\left(p_{0}, p_{1}\right)$ (see Equation 3) such that the inputoutput differential $\left(u_{0}, u_{1}, u_{2}, u_{3}, y_{0}, y_{1}, y_{2}, y_{3}, p_{0}, p_{1}\right) \in \mathbb{F}_{2}^{10}$. Similarly, there are 21 linear inequalities through the MILPbased reduction algorithm as shown in Equation 4.

$$
\left(p_{0}, p_{1}\right)=\left\{\begin{array}{l}
(0,0) \text { if } \operatorname{Pr}=1  \tag{3}\\
(0,1) \text { if } \operatorname{Pr}=2^{-3} \\
(1,0) \text { if } \operatorname{Pr}=2^{-2}
\end{array}\right.
$$

$$
\begin{array}{r}
1 u_{0}-1 u_{1}+0 u_{2}-1 u_{3}-1 y_{0}+0 y_{1}+0 y_{2}+0 y_{3}+3 p_{0}+2 p_{1} \geq \\
1 u_{0}-1 u_{1}+0 u_{2}-1 u_{3}-1 y_{0}+1 y_{1}-1 y_{2}+1 y_{3}+4 p_{0}+2 p_{1} \geq \\
1 u_{0}+1 u_{1}+0 u_{2}+2 u_{3}+1 y_{0}-3 y_{1}-1 y_{2}+2 y_{3}+0 p_{0}+4 p_{1} \geq \\
1 u_{0}-1 u_{1}-2 u_{2}-1 u_{3}+5 y_{0}+2 y_{1}+4 y_{2}+2 y_{3}-3 p_{0}+0 p_{1} \geq 0 \\
6 u_{0}+1 u_{1}+2 u_{2}+1 u_{3}+1 y_{0}-2 y_{1}-3 y_{2}-2 y_{3}+0 p_{0}+3 p_{1} \geq \\
3 u_{0}+3 u_{1}+0 u_{2}-1 u_{3}-1 y_{0}-2 y_{1}-2 y_{2}-1 y_{3}+3 p_{0}+5 p_{1} \geq \\
2 u_{0}+5 u_{1}+2 u_{2}+5 u_{3}-2 y_{0}-1 y_{1}+0 y_{2}-1 y_{3}+0 p_{0}-1 p_{1} \geq \\
-1 u_{0}+3 u_{1}+0 u_{2}+2 u_{3}-4 y_{0}+2 y_{1}+1 y_{2}-1 y_{3}+4 p_{0}+2 p_{1} \geq \\
3 u_{0}+1 u_{1}+4 u_{2}+3 u_{3}-1 y_{0}+3 y_{1}-2 y_{2}-4 y_{3}-1 p_{0}+4 p_{1} \geq \\
3 u_{0}-1 u_{1}+0 u_{2}+3 u_{3}-1 y_{0}-1 y_{1}-2 y_{2}-2 y_{3}+3 p_{0}+5 p_{1} \geq 0 \\
-2 u_{0}+2 u_{1}-2 u_{2}+2 u_{3}-1 y_{0}+1 y_{1}+0 y_{2}+1 y_{3}+5 p_{0}+1 p_{1} \geq \\
-5 u_{0}+2 u_{1}+1 u_{2}-2 u_{3}-1 y_{0}+4 y_{1}+0 y_{2}+3 y_{3}+5 p_{0}+3 p_{1} \geq \\
-1 u_{0}-1 u_{1}-2 u_{2}-2 u_{3}+3 y_{0}-1 y_{1}+0 y_{2}+3 y_{3}+3 p_{1} \geq 0 \\
-5 u_{0}-2 u_{1}+1 u_{2}+2 u_{3}-1 y_{0}+3 y_{1}+0 y_{2}+4 y_{3}+5 p_{0}+3 p_{1} \geq \\
-1 u_{0}-2 u_{1}-2 u_{2}-1 u_{3}+3 y_{0}+3 y_{1}+0 y_{2}-1 y_{3}+3 p_{0}+5 p_{1} \geq \\
1 u_{0}+2 u_{1}-1 u_{2}-3 u_{3}+1 y_{0}+2 y_{1}+0 y_{2}+1 y_{3}+0 p_{0}+4 p_{1} \geq \\
1 u_{0}-1 u_{1}-1 u_{2}+2 u_{3}-2 y_{0}-3 y_{1}+3 y_{2}+3 y_{3}+5 p_{0}+4 p_{1} \geq
\end{array} 00
$$

## C. Left Circular Shift in Terms of Linear Inequalities

Consider the sequences $\left(x_{0}, x_{1}, \ldots, x_{31}\right)$ and $\left(y_{0}, y_{1}, \ldots, y_{31}\right)$ represents the input and output bit differences of a 5-bit left circular shift, respectively. The relationship
$y_{i}=x_{(i+5) \% 32}$ for $0 \leq i \leq 31$ provides a set of linear equations characterizing this operation.

## D. Add Round Key in Terms of Linear Inequalities

In a related-key differential attack, adversaries exploit plaintext differences along with key differences. Therefore, we include the linear constraints for the add round key in MILP models to search related-key differential characteristics. For this operation, consider an input bit $x$, a key bit $k$, and the output bit $z$ such that $z=k \oplus x$. The following are the linear inequalities corresponding to this operation:

$$
\begin{align*}
-k+x+z & \geq 0 \\
k-x+z & \geq 0 \\
k+x-z & \geq 0  \tag{5}\\
k+x+z & \leq 2
\end{align*}
$$

## E. Objective Functions

To determine the minimum number of active S-boxes and the maximum probability for differential characteristics, objective functions are formulated as

$$
\min \sum_{i} A_{i} \text { and } \min \sum_{i}\left(2 p_{i, 0}+3 p_{i, 1}\right)
$$

## V. Result

Utilizing the Gurobi solver for MILP models, this study determines precise lower bounds on active $S$-boxes and probabilities of differential characteristics for up to 13 rounds in a single-key framework, as detailed in Table II. We determine valid single-key differential characteristics of LELBC up to nine rounds, including a nine-round differential characteristic with a probability of $2^{-60}$ shown in Table III. Additionally, our analysis identifies valid related-key differential characteristics up to 12 rounds, with a 12 -round differential characteristic of probability $2^{-60}$ as depicted in Table IV.

TABLE II
COMPARISON BETWEEN NUMBER OF ACTIVE S-BOXES (\#AS) AND PROBABILITIES OF DIFFERENTIAL CHARACTERISTICS UP TO 13 ROUNDS

| Round | This Paper (Single-key) |  | Designers' Claim <br> \#AS |
| :---: | :---: | :---: | :---: |
|  | \#AS | Probability | (1) |
| 1 | 1 | $2^{-2}$ | 1 |
| 2 | 3 | $2^{-6}$ | 3 |
| 3 | 6 | $2^{-15}$ | 6 |
| 4 | 9 | $2^{-23}$ | 9 |
| 5 | 12 | $2^{-34}$ | 13 |
| 6 | 14 | $2^{-38}$ | 14 |
| 7 | 16 | $2^{-43}$ | 17 |
| 8 | 19 | $2^{-51}$ | 20 |
| 9 | 22 | $2^{-60}$ | 26 |
| 10 | 25 | $2^{-69}$ | 27 |
| 11 | 27 | $2^{-73}$ | 30 |
| 12 | 30 | $2^{-85}$ | 34 |
| 13 | 33 | $2^{-93}$ | - |

## VI. Conclusion

This study conducted a thorough analysis of the LELBC lightweight block cipher's resilience to differential attacks under both single and related-key frameworks, utilizing MILP to

TABLE III
9-ROUND DIFFERENTIAL CHARACTERISTIC

| Round | Input Difference | Probability |
| :---: | :---: | :---: |
| 1 | $400000000020 a 008$ | $2^{-0}$ |
| 2 | 0004000000802000 | $2^{-7}$ |
| 3 | 0000000000004000 | $2^{-6}$ |
| 4 | 0002000000001000 | $2^{-3}$ |
| 5 | 1004000000801000 | $2^{-9}$ |
| 6 | 5000010000002008 | $2^{-11}$ |
| 7 | 4000000000000008 | $2^{-8}$ |
| 8 | 4000000000000000 | $2^{-3}$ |
| 9 | 1000004000000002 | $2^{-5}$ |
| 10 | 4000401000000200 | $2^{-8}$ |

TABLE IV
12-ROUND DIFFERENTIAL CHARACTERISTIC

| Round | Input Difference | Key Difference | Probability |
| :---: | :---: | :---: | :---: |
| 1 | 0004000000800000 | 0000000001000000 0000000000000000 | $2^{-0}$ |
| 2 | 0001000000000000 | 0000000000000000 0000008000000000 | $2^{-3}$ |
| 3 | 0000000000000000 | 0001000000000000 0000000000000000 | $2^{-0}$ |
| 4 | 0000000000000000 | 0000000000000000 8000000000000000 | $2^{-0}$ |
| 5 | 0000000000000100 | 0000000000000100 0000000000000000 | $2^{-0}$ |
| 6 | 0000400000000200 | 0000000000000000 0000000000800000 | $2^{-3}$ |
| 7 | 0020 200d 00010180 | 0000000100000000 0000000000000000 | $2^{-14}$ |
| 8 | 0140000008080080 | 0000000000000000 0000800000000000 | $2^{-16}$ |
| 9 | 0000080000010040 | 0100000000000000 0000000000000000 | $2^{-9}$ |
| 10 | 0000000000000010 | $\begin{aligned} & 0000000000000000 \\ & 0000000000000080 \end{aligned}$ | $2^{-5}$ |
| 11 | 0000080000010040 | 0000000000010000 0000000000000000 | $2^{-3}$ |
| 12 | 0000010000000020 | 0000000000000000 0000000080000000 | $2^{-5}$ |
| 13 | 000014000000 00a0 | $\begin{aligned} & 0000010000000000 \\ & 0000000000000000 \end{aligned}$ | $2^{-2}$ |

discover differential characteristics. Our MILP models incorporated DDT probabilities to find out characteristics for up to nine and 12 rounds in single-key and related-key frameworks, respectively. This investigation presented nine-round (singlekey) and 12 -round (related-key) differential characteristics, each with a probability of $2^{-60}$.

## REFERENCES

[1] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher," in Cryptographic Hardware and Embedded SystemsCHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9. Springer, 2007, pp. 450-466.
[2] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim, "The skinny family of block ciphers and its low-latency variant mantis," in Advances in Cryptology-CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II 36. Springer, 2016, pp. 123-153.
[3] S. Banik, S. K. Pandey, T. Peyrin, Y. Sasaki, S. M. Sim, and Y. Todo, "Gift: A small present: Towards reaching the limit of lightweight encryption," in Cryptographic Hardware and Embedded Systems-CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings. Springer, 2017, pp. 321-345.
[4] S. Banik, Z. Bao, T. Isobe, H. Kubo, F. Liu, K. Minematsu, K. Sakamoto, N. Shibata, and M. Shigeri, "Warp: Revisiting gfn for lightweight 128bit block cipher," in Selected Areas in Cryptography: 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers 27. Springer, 2021, pp. 535-564.
[5] X. Huang, L. Li, and J. Yang, "Ivlbc: An involutive lightweight block cipher for internet of things," IEEE Systems Journal, 2022.
[6] Y. Li, J. Feng, Q. Zhao, and Y. Wei, "Hdlbc: A lightweight block cipher with high diffusion," Integration, vol. 94, p. 102090, 2024.
[7] Q. Song, L. Li, and X. Huang, "Lelbc: A low energy lightweight block cipher for smart agriculture," Internet of Things, vol. 25, p. 101022, 2024.
[8] H. M. Heys, "A tutorial on linear and differential cryptanalysis," Cryptologia, vol. 26, no. 3, pp. 189-221, 2002.
[9] E. Bellini, A. De Piccoli, M. Formenti, D. Gerault, P. Huynh, S. Pelizzola, S. Polese, and A. Visconti, "Differential cryptanalysis with sat, smt, milp, and cp: a detailed comparison for bit-oriented primitives," in International Conference on Cryptology and Network Security. Springer, 2023, pp. 268-292.
[10] M. Cao and W. Zhang, "Related-key differential cryptanalysis of the reduced-round block cipher gift," IEEE Access, vol. 7, pp. 175769 175778, 2019.
[11] T. Weng, T. Cui, T. Yang, and Y. Guo, "Related-key differential attacks on reduced-round lblock." Security \& Communication Networks, 2022.
[12] Y. Y. Chan, C.-Y. Khor, J. S. Teh, W. J. Teng, and N. Jamil, "Differential cryptanalysis of lightweight block ciphers slim and lcb," in International Symposium on Emerging Information Security and Applications. Springer, 2022, pp. 55-67.
[13] J. S. Teh, L. J. Tham, N. Jamil, and W.-S. Yap, "New differential cryptanalysis results for the lightweight block cipher boron," Journal of Information Security and Applications, vol. 66, p. 103129, 2022.
[14] J. S. Teh and A. Biryukov, "Differential cryptanalysis of warp," Journal of Information Security and Applications, vol. 70, p. 103316, 2022.
[15] M. Mahzoun, L. Kraleva, R. Posteuca, and T. Ashur, "Differential cryptanalysis of k-cipher," in 2022 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2022, pp. 1-7.
[16] Y. Zhang, G. Liu, C. Li, and X. Shen, "Impossible differential cryptanalysis of fbc-128," Journal of Information Security and Applications, vol. 69, p. 103279, 2022.
[17] Y. Cui, H. Xu, L. Tan, and W. Qi, "Sat-aided differential cryptanalysis of lightweight block ciphers midori, mantis and qarma," in International Conference on Information and Communications Security. Springer, 2023, pp. 3-18.
[18] S. Nobuyuki et al., "Differential, linear, and meet-in-the-middle attacks on the lightweight block cipher rbfk," IET Information Security, vol. 2023, 2023.
[19] Y. Li, H. Lin, X. Bi, S. Huo, and Y. Han, "Milp-based differential cryptanalysis on full-round shadow," Journal of Information Security and Applications, vol. 81, p. 103696, 2024.
[20] M. B. ILTER and A. A. SELÇUK, "Milp modeling of matrix multiplication: cryptanalysis of klein and prince," Turkish Journal of Electrical Engineering and Computer Sciences, vol. 32, no. 1, pp. 183-197, 2024.
[21] Y. Sasaki and Y. Todo, "New algorithm for modeling s-box in milp based differential and division trail search," in Innovative Security Solutions for Information Technology and Communications: 10th International Conference, SecITC 2017, Bucharest, Romania, June 8-9, 2017, Revised Selected Papers 10. Springer, 2017, pp. 150-165.


[^0]:    Manjeet Kaur is a Research Scholar in the Department of Mathematics, Indian Institute of Information Technology, Lucknow, India-226 002. Email: rmm21101@iiitl.ac.in

    Tarun Yadav is working in Scientific Analysis Group, Defence R \& D Organisation, Delhi, India-110 054. Email: tarunyadav.sag @ gov.in

    Manoj Kumar is working in Scientific Analysis Group, Defence R \& D Organisation, Delhi, India-110 054. Email: manojkumar.sag@gov.in

    Dhananjoy Dey is an Associate Professor in the Department of Mathematics, Indian Institute of Information Technology, Lucknow, India-226 002. Email: ddey@iiitl.ac.in

[^1]:    ${ }^{1}$ https://www.gurobi.com

