Full-Round Differential Attack on ULC and LICID Block Ciphers Designed for IoT

Manjeet Kaur[*1], Tarun Yadav[†2], Manoj Kumar[‡3], and Dhananjoy Dey[§4]

[1,4]Indian Institute of Information Technology, Lucknow, U.P., INDIA-226 002
[2,3]Scientific Analysis Group, DRDO, Delhi, INDIA-110 054

Abstract

The lightweight block ciphers ULC and LICID are introduced by Sliman et al. (2021) and Omrani et al. (2019) respectively. These ciphers are based on substitution permutation network structure. ULC is designed using the ULM method to increase efficiency, memory usage, and security. On the other hand, LICID is specifically designed for image data. In the ULC paper, the authors have given a full-round differential characteristic with a probability of 2^{-80}. In the LICID paper, the authors have presented an 8-round differential characteristic with a probability of $2^{-112.66}$. In this paper, we present the 15-round ULC and the 14-round LICID differential characteristics of probabilities 2^{-45} and 2^{-40} respectively using the MILP model.

Keywords: Differential Cryptanalysis, Lightweight Block Ciphers, MILP, S-box

1 Introduction

Lightweight cryptography is used on resource-constrained devices. Many lightweight block ciphers like PRINCE [1], PRESENT [2], GIFT [3], and WARP [4] are designed in past two decades. The security analysis of lightweight block ciphers is necessary to measure the strength against differential attack. In this attack [5–7], we exploit the non-uniform behavior of the input-output differential of the ciphers. For a successful key recovery attack against a differential attack, high-probability differential characteristics are needed. Nowadays, the problem of differential cryptanalysis is solved using the mixed-integer linear programming (MILP) model. An MILP problem is defined as follows: finding $x = (x_1, x_2, \ldots, x_m) \in \mathbb{R}^m$ (some of x_i are integers) with linear constraints $Ax^T \leq b$ to optimize the linear objective function $f(x) = \sum_{i=1}^{m} c_i x_i$, where $A \in \mathbf{M}_{n\times m}(\mathbb{R})$, $b \in \mathbb{R}^n$, and $c \in \mathbb{R}^m$. Gurobi and CPLEX are well-known solvers that are used to solve optimization problems. The problem of finding

*Email: rmm21101@iiitl.ac.in
†Email: tarunyadav.sag@gov.in
‡Email: manojkumar.sag@gov.in
§Email: ddey@iiitl.ac.in

the differential characteristics is divided into two parts: (i) to calculate the minimum number of active S-boxes, and (ii) to find the high-probability differential characteristics. Mouha et al. [8] proposed a technique based on MILP to count the minimum number of active S-boxes of word-oriented block ciphers (SPN structures). This method is not applicable to bit-oriented block ciphers. Then, Sun et al. [9] extended this method to S-bP structures. After that, Sun et al. [10] proposed a method to generate the linear inequalities from the H-representation of the convex hull of all possible differential patterns of an S-box. Sasaki and Todo [11] introduced the reduction algorithm based on MILP to minimize the linear inequalities. Based on this MILP technique, Zhu et al. [12] presented a differential attack on the lightweight block cipher GIFT. Kumar and Yadav [13] also provided a differential attack on lightweight block cipher WARP using the MILP technique.

Motivation The designers of the ULC cipher have given a full-round differential characteristic with a probability of 2^{-80}. They have not provided any lower bound on active S-boxes for full-round differential characteristics. On the other hand, the designers of the LICID cipher have provided an 8-round differential characteristic with a probability of $2^{-112.66}$. They have not given full-round differential characteristics with a lower bound on active S-boxes. However, there is no third-party differential cryptanalysis on these two ciphers.

Contribution In this paper, we provide the differential characteristics for full-round ULC and LICID ciphers using the MILP technique. Our contributions are as follows:

i. Compute a 15-round differential characteristic with a probability of 2^{-45} (minimum 15 active S-boxes)

ii. Construct a 14-round differential characteristic with a probability of 2^{-40} (minimum 14 active S-boxes)

In comparison to the findings presented by the authors of ULC and LICID, these two differential characteristics have less complexity.

Organization The rest of our paper is organized as follows: we present a detailed description of the ciphers in Section 2. In Section 3, we provide the linear inequalities generation and reduction methods. In Section 4, we give a MILP-based construction of differential characteristics. We calculate the lower bounds on active S-boxes and provide full-round differential characteristics of ULC and LICID in Section 5. We conclude our paper in Section 6.

2 Preliminaries

In this section, we discuss the ultra-lightweight cryptosystem (ULC) [14,15] and lightweight image cryptosystem (LICID) [16] for IoT Devices.

$\mathcal{K}$	A key of 80-bit (ULC) or 112-bit (LICID)
$\mathcal{K}^r$	The r^{th} round key
$\mathcal{X}$	An input block of 64-bit
$\mathcal{X}_{[i,j]}$	The i^{th} to j^{th} bits of $\mathcal{X}$
$\mathcal{Y}$	An output block of 64-bit
B_i	A bitstring of 8 bits
$B_i[r:t]$	The r^{th} to t^{th} bits of B_i
$\|A\|$	Cardinality of a set A

2.1 Notations

2.2 Description of ULC

ULC is designed based on the ultra-lightweight method (ULM) which is the combination of bit-slice, WTS, and involutive methods. Here, we describe its key generation and encryption algorithm.

2.2.1 Key Generation

Initially, we have an 80-bit key. Then, each 64-bit round key is generated from it as follows:

i. An S-box is applied to the last 4 bits of an 80-bit key

ii. An updated key is rotated to the left by 61 bits

iii. The last 64 bits are extracted as a round key. It is described in Algorithm 1.

Algorithm 1: Key Generation Algorithm

Input : $\mathcal{K}= k_{79}k_{78}\dots k_2k_1k_0$
Output: $\mathcal{K}^r= k^r_{63}k^r_{62}\dots k^r_2k^r_1k^r_0$, where $1 \leq r \leq 16$
for *r=1 to 16* **do**
  $(k_{79}k_{78}k_{77}k_{76}) = S(k_{79}k_{78}k_{77}k_{76})$
  $\mathcal{K} = \mathcal{K} \lll 61$
  $\mathcal{K}^r = (k_{79}k_{78}\dots k_{18}k_{17}k_{16})$
end

2.2.2 Encryption Algorithm

The round function of ULC takes two inputs: a 64-bit block and a 64-bit key. It is composed of an add round key, a bitslice S-box, and an involutory 64-bit permutation. First, a 64-bit round key (derived from the 80-bit key) is XORed with the intermediate ciphertext. Next, a 4-bit S-box is applied, as shown in Table 1. Finally, a 64-bit permutation is used, as shown in Table 2. This process is applied 15 times consecutively. In addition, the output of the last round is XORed with a 64-bit round key, as described in Algorithm 2. The encryption of ULC is shown in Figure 1 [14].

Table 1: S-box of ULC (Decimal Values)

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(x)	6	5	12	10	1	14	7	9	11	0	3	13	8	15	4	2

Table 2: P-box of ULC

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(x)	63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
P(x)	62	58	54	50	46	42	38	34	30	26	22	18	14	10	6	2
x	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
P(x)	61	57	53	49	45	41	37	33	29	25	21	17	13	9	5	1
x	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
P(x)	60	56	52	48	44	40	36	32	28	24	20	16	12	8	4	0

Algorithm 2: Encryption Algorithm

Input : $\mathcal{X}= x_{63}x_{62}\dots x_2x_1x_0$
$\mathcal{K}^r= k^r_{63}k^r_{62}\dots k^r_2k^r_1k^r_0$, where $1 \le r \le 16$
Output: $\mathcal{Y}= y_{63}y_{62}\dots y_2y_1y_0$
for *r=1 to 15* **do**
  $\mathcal{X} = \mathcal{X} \oplus \mathcal{K}^r$
  for *j=0 to 15* **do**
    $\mathcal{X}_{[4*j+3,4*j]} = S(\mathcal{X}_{[4*j+3,4*j]})$
  end
  $\mathcal{X} = P(\mathcal{X})$
end
$\mathcal{Y} = \mathcal{X} \oplus \mathcal{K}^{16}$

2.3 Description of LICID

LICID is based on the SPN structure. It is used for image encryption on IoT devices. Here, we explain its key generation and encryption algorithm.

2.3.1 Key Generation

First, we have a 112-bit key. Then, each 64-bit round key is generated from it as follows:

i. A 4×4 S-box is used on odd nibbles of a 112-bit key

ii. A modular addition ($\boxplus$) is applied to the bytes of the updated key

iii. Extract the first 64-bit to get the round key. It is shown in Algorithm 3.

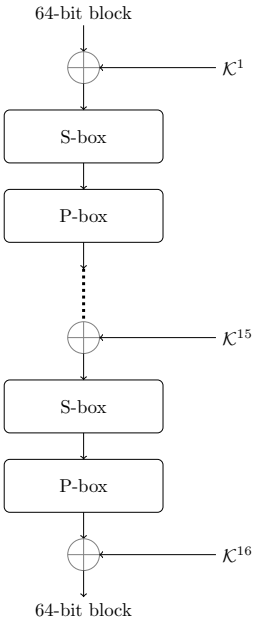

Figure 1: Encryption Diagram of ULC

Algorithm 3: Key Generation Algorithm

Input : $\mathcal{K} = B_0B_1B_2 \dots B_{12}B_{13}$
Output: $\mathcal{K}^r = k^r_{63}k^r_{62} \dots k^r_2k^r_1k^r_0$, where $1 \leq r \leq 15$
for *r=1 to 15* **do**
  for *i=0 to 13* **do**
    $B_i[7:4] = S(B_i[7:4])$
  end
  for *i=1 to 13* **do**
    $B_i = B_i \boxplus B_{i-1}$
  end
  $B_0 = B_0 \boxplus B_{13}$
  for *j=12 to 0* **do**
    $B_j = B_j \boxplus B_{j+1}$
  end
  $B_{13} = B_{13} \boxplus B_0$
  $\mathcal{K}^r$=first 64-bit of $\mathcal{K}$
end

2.3.2 Encryption Algorithm

LICID consists of two phases: (i) an outer phase, and (ii) an inner phase. The outer phase consists of two operations: horizontal ADD-Diffusion (HAD) and vertical ADD-Diffusion (VAD), as shown in Figure 2 [16]. The inner phase is an iterative function that takes two inputs: a 64-bit block and a 64-bit key. It consists of three operations: (i) an add round key, (ii) a substitution (S)-box, and (iii) a permutation (P)-box. It is applied 14 times successively, as described in Algorithm 4. Moreover, a round key is applied at the end of the

last round. The S-box and the P-box of LICID are shown in Table 3 and Table 4, respectively. The encryption of LICID is given in Figure 3 [16].

Algorithm 4: Encryption Algorithm (Inner Phase)

Input : $\mathcal{X}= x_{63}x_{62}\dots x_2x_1x_0$
$\mathcal{K}^r= k^r_{63}k^r_{62}\dots k^r_2k^r_1k^r_0$, where $1 \le r \le 15$
Output: $\mathcal{Y}= y_{63}y_{62}\dots y_2y_1y_0$
for *r=1 to 14* **do**
  for *i=0 to 63* **do**
    $x_i = x_i \oplus k^r_i$
  end
  for *j=0 to 15* **do**
    $\mathcal{X}_{[4*j+3,4*j]} = S(\mathcal{X}_{[4*j+3,4*j]})$
  end
  $\mathcal{X} = P(\mathcal{X})$
end
for *i=0 to 63* **do**
  $y_i = x_i \oplus k^{15}_i$
end

(a) HAD (b) VAD

Figure 2: Outer-phase operations

Table 3: S-box of LICID (Decimal Values)

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(x)	0	7	10	14	4	1	6	13	5	9	8	15	12	2	11	3

Table 4: P-box of LICID

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(x)	2	63	8	5	62	59	4	1	58	55	0	61	54	51	60	57
x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
P(x)	18	15	24	21	14	11	20	17	10	7	16	13	6	3	12	9
x	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
P(x)	34	31	40	37	30	27	36	33	26	23	32	29	22	19	28	25
x	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
P(x)	50	47	56	53	46	43	52	49	42	39	48	45	38	35	44	41

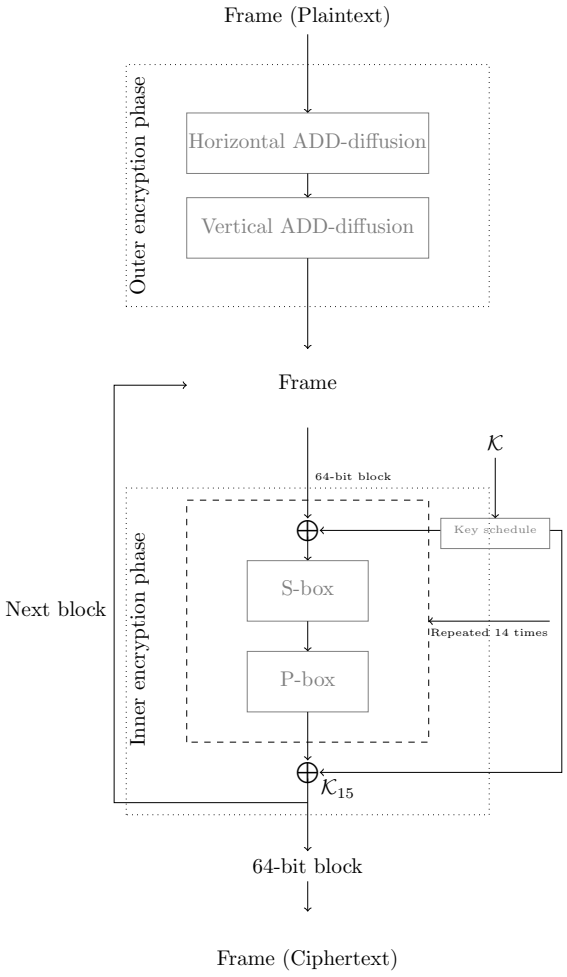

Figure 3: Encryption of LICID

3 Generation and Reduction of Linear Inequalities for S-box

In this section, we discuss the H-representation of the convex hull to generate linear inequalities and the reduction algorithm to minimize the linear inequalities.

Definition 3.1 (Convex Hull)**.** *The convex hull of a set S of finite discrete points is the smallest convex set $\mathcal{C}$ such that $S \subseteq \mathcal{C}$.*

Definition 3.2 (Difference Distribution Table)**.** *The difference distribution table (DDT) of an S-box S is a $2^n \times 2^n$ matrix with entry at row $\Delta_i \in \mathbf{F}_2^n$ and column $\Delta_o \in \mathbf{F}_2^n$ equal to*

$$|\{t \in \mathbf{F}_2^n | S(t) \oplus S(t \oplus \Delta_i) = \Delta_o\}|.$$

The non-zero and zero entries in DDT represent the possible and impossible differential propagations of an S-box respectively. The DDT of ULC and LICID are shown in Table 5 and Table 6, respectively. We use the possible differential propagations to generate the linear inequalities of an S-box. We discuss the H-representation of the convex hull to generate the linear inequalities in the next subsection.

3.1 H-representation of Convex Hull

Consider that $\Delta_i = (x_1, x_2, \ldots, x_n)$ and $\Delta_o = (y_1, y_2, \ldots, y_n)$ be the input and corresponding output difference of an n-bit S-box respectively. We can represent the possible differential propagation of an S-box as a point $(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^{2n}$. Now, consider the set of all possible differential propagations of an S-box in $\mathbb{F}_2^{2n}$.

Then, using SageMath, compute the convex hull of this set as a system of linear inequalities (the H-representation of the convex hull). SageMath provides a large set of linear inequalities, including redundant ones, with solution space $\mathbb{F}_2^{2n} - \mathcal{R}$, where $\mathcal{R}$ is the set of all impossible propagations of an S-box. MILP with these constraints cannot be solved efficiently. We can represent the differential behavior of an S-box with these inequalities. Now, we need to reduce the set of these inequalities to construct an efficient MILP model. In the next subsection, we discuss the reduction algorithm.

3.2 Reduction Algorithm

We discuss the reduction algorithm [11] to minimize the linear inequalities (say $\mathbf{N}$ inequalities) resulting from the H-representation of the convex hull. Consider $\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_{|\mathcal{R}|-1}$ are the elements of $\mathcal{R}$. We minimize the linear inequalities such that the selected inequality removes at least one $\mathcal{R}_i$, $i \in \{0, 1, \ldots, |\mathcal{R}| - 1\}$. Define $\overline{\mathcal{R}_i} = \{i_{k_1}, i_{k_2}, \ldots, i_{k_t}\}$ such that for each $i_{k_r} \in \overline{\mathcal{R}_i}$, $z_{i_{k_r}}$ removes $\mathcal{R}_i$ from $\mathbb{F}_2^{2n}$. We solve this minimization problem using MILP. For this MILP, we define binary variables $z_0, z_1, \ldots, z_{\mathbf{N}-1}$, where $z_i = 1$ or $z_i = 0$ represents that linear inequality i is included or not in the system respectively. The objective function

to minimize the linear inequalities is defined as follows:

$$\sum_{i=0}^{\mathbf{N}-1} z_i.$$

Using Gurobi, we solve this MILP to get minimized linear inequalities. The minimized linear inequalities for ULC and LICID are shown in Table 7 and Table 8, respectively.

Table 5: DDT of ULC (Decimal Values)

Δ_i \ Δ_o	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	0	4	2	0	0	0	2	0	0	4	2
2	0	0	0	0	0	0	2	2	2	0	2	0	2	4	0	2
3	0	0	0	2	0	0	2	0	2	4	2	2	2	0	0	0
4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4
5	0	2	0	0	4	2	0	0	4	2	0	0	0	2	0	0
6	0	2	4	0	2	0	0	0	0	0	0	2	2	2	0	2
7	0	0	4	0	2	2	0	0	0	2	0	2	2	0	0	2
8	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2
9	0	2	0	0	0	2	4	0	0	2	0	0	0	2	4	0
10	0	0	0	0	0	4	2	2	2	0	2	0	2	0	0	2
11	0	4	0	2	0	0	2	0	2	0	2	2	2	0	0	0
12	0	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0
13	0	2	0	0	0	2	0	0	0	2	4	0	0	2	4	0
14	0	0	4	2	2	2	0	2	0	2	0	0	2	0	0	0
15	0	2	4	2	2	0	0	2	0	0	0	0	2	2	0	0

Table 6: DDT of LICID (Decimal Values)

Δ_i \ Δ_o	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	2	2	0	4	2	0	0	2	2	0	2	0
2	0	2	2	0	0	0	2	2	0	2	2	0	2	2	0	0
3	0	2	0	0	0	0	0	2	0	4	2	0	0	2	2	2
4	0	0	0	4	2	0	2	0	0	2	0	2	4	0	0	0
5	0	2	0	2	2	2	0	4	2	0	0	2	0	0	0	0
6	0	0	0	0	2	0	2	0	0	0	4	0	0	2	4	2
7	0	2	2	2	0	0	2	0	0	0	4	2	0	2	0	0
8	0	2	2	2	0	2	0	0	2	0	0	0	0	2	4	0
9	0	0	2	0	0	4	6	0	0	2	0	0	0	2	0	0
10	0	0	2	0	0	0	0	2	4	0	2	0	0	0	0	6
11	0	2	0	2	2	0	0	2	0	0	2	2	0	0	0	4
12	0	4	2	0	0	2	0	0	2	0	0	0	2	2	2	0
13	0	0	2	0	2	4	0	0	0	4	0	2	0	2	0	0
14	0	0	0	2	4	0	2	0	0	0	0	2	4	0	2	0
15	0	0	2	2	0	0	0	0	4	2	0	2	2	0	0	2

4 MILP Modeling of Differential Characteristic Search Problem

In this section, we discuss how to find high-probability differential characteristics using a MILP model.

4.1 Active S-boxes Minimization

First, we construct the linear inequalities of the S-boxes using DDT in SageMath [17]. Then, minimize them using the MILP-based reduction algorithm as discussed in Section 3 by Gurobi optimization solver [18]. There are 267 and 360 linear inequalities for ULC and LICID using SageMath, respectively. Then, there are 21 linear inequalities from the MILP problem based on impossible differentials for both ciphers using Gurobi, as presented in Table 7 and Table 8, respectively. These sets of minimized linear inequalities are used in a MILP problem to minimize the number of active S-boxes.

Table 7: Linear inequalities for the minimizing number of active S-boxes in ULC

Sr. No.	Linear Inequalities
1	$-1x_3 - 2x_2 - 1x_1 - 1x_0 - 1y_3 + 2y_2 + 1y_1 + 1y_0 \geq -4$
2	$+0x_3 + 1x_2 - 2x_1 + 0x_0 + 2y_3 + 1y_2 + 1y_1 + 2y_0 \geq -0$
3	$+0x_3 + 1x_2 + 1x_1 - 2x_0 + 1y_3 + 2y_2 + 0y_1 + 2y_0 \geq -0$
4	$-1x_3 - 2x_2 + 1x_1 + 2x_0 - 1y_3 - 1y_2 + 1y_1 - 1y_0 \geq -4$
5	$-1x_3 - 3x_2 + 2x_1 + 3x_0 + 4y_3 + 4y_2 + 2y_1 + 1y_0 \geq -0$
6	$+2x_3 + 1x_2 + 2x_1 + 1x_0 + 0y_3 + 0y_2 + 1y_1 - 2y_0 \geq -0$
7	$+2x_3 + 0x_2 + 1x_1 + 2x_0 + 1y_3 - 1y_2 + 2y_1 - 1y_0 \geq -0$
8	$+3x_3 + 4x_2 - 1x_1 - 1x_0 + 3y_3 - 1y_2 + 3y_1 - 1y_0 \geq -0$
9	$+0x_3 + 1x_2 - 1x_1 - 1x_0 - 1y_3 - 1y_2 - 1y_1 + 0y_0 \geq -4$
10	$+3x_3 - 1x_2 + 2x_1 + 4x_0 - 2y_3 + 2y_2 + 4y_1 - 1y_0 \geq -0$
11	$-1x_3 + 1x_2 + 2x_1 - 1x_0 + 0y_3 + 0y_2 + 2y_1 + 2y_0 \geq -0$
12	$+0x_3 + 3x_2 + 2x_1 + 3x_0 - 1y_3 - 1y_2 - 1y_1 + 3y_0 \geq -0$
13	$+3x_3 - 3x_2 + 1x_1 + 0x_0 - 1y_3 - 1y_2 - 2y_1 + 3y_0 \geq -4$
14	$+0x_3 + 1x_2 - 1x_1 + 1x_0 + 0y_3 + 1y_2 + 0y_1 - 1y_0 \geq -1$
15	$+2x_3 - 2x_2 - 1x_1 - 1x_0 + 2y_3 + 1y_2 - 1y_1 - 2y_0 \geq -5$
16	$-1x_3 - 1x_2 + 2x_1 - 1x_0 + 0y_3 + 0y_2 - 2y_1 - 2y_0 \geq -5$
17	$+1x_3 - 3x_2 - 1x_1 + 0x_0 + 1y_3 - 3y_2 - 3y_1 + 2y_0 \geq -7$
18	$-1x_3 + 1x_2 - 2x_1 - 2x_0 + 1y_3 - 2y_2 + 1y_1 - 1y_0 \geq -6$
19	$-1x_3 + 1x_2 - 1x_1 + 0x_0 - 1y_3 + 0y_2 + 1y_1 - 1y_0 \geq -3$
20	$+1x_3 + 1x_2 - 1x_1 - 2x_0 - 1y_3 - 2y_2 + 1y_1 - 2y_0 \geq -6$
21	$-1x_3 - 1x_2 - 1x_1 + 0x_0 - 1y_3 + 0y_2 - 1y_1 + 0y_0 \geq -4$

4.2 Optimize the Probability of Differential Characteristic

First, we consider the differential probabilities of the S-boxes to find the high-probability differential characteristics. There are three possible differential probabilities: 1, 2^{-2}, and 2^{-3} for ULC's S-box. We need two binary variables (p_0, p_1) to represent these probabilities. The differential patterns, including these two extra variables, satisfy Equation 1. Then, compute 543 linear inequalities for ULC using SageMath. Similarly, for LICID's S-box, there are four possible probabilities: 1, $2^{-1.415}$, 2^{-2}, and 2^{-3}; and three binary variables (p_0, p_1, p_2) to represent these probabilities, satisfying Equation 2. Then, compute 3606 linear inequalities for LICID using SageMath. We use the reduction algorithm to get a

Table 8: Linear inequalities for the minimizing number of active S-boxes in LICID

Sr. No.	Linear Inequalities
1	$-1x_3 + 2x_2 - 1x_1 - 2x_0 - 2y_3 + 0y_2 + 2y_1 + 1y_0 \geq -4$
2	$-1x_3 + 0x_2 + 0x_1 + 1x_0 - 1y_3 + 1y_2 + 1y_1 - 1y_0 \geq -2$
3	$-2x_3 + 3x_2 - 3x_1 + 1x_0 - 1y_3 - 3y_2 - 1y_1 + 3y_0 \geq -7$
4	$+1x_3 + 2x_2 - 1x_1 + 2x_0 - 1y_3 + 2y_2 - 3y_1 - 3y_0 \geq -5$
5	$-1x_3 - 1x_2 + 1x_1 + 1x_0 - 2y_3 + 2y_2 - 2y_1 + 1y_0 \geq -4$
6	$+0x_3 - 1x_2 - 2x_1 - 1x_0 + 2y_3 - 2y_2 + 1y_1 - 1y_0 \geq -5$
7	$-1x_3 + 3x_2 + 1x_1 + 3x_0 + 2y_3 - 3y_2 + 2y_1 + 4y_0 \geq -0$
8	$+1x_3 + 0x_2 + 1x_1 - 1x_0 - 1y_3 + 0y_2 + 1y_1 - 1y_0 \geq -2$
9	$+3x_3 + 2x_2 + 3x_1 + 2x_0 - 1y_3 - 1y_2 + 0y_1 - 1y_0 \geq -0$
10	$+3x_3 + 2x_2 + 1x_1 - 2x_0 + 2y_3 + 2y_2 - 1y_1 + 1y_0 \geq -0$
11	$+2x_3 + 4x_2 - 2x_1 - 4x_0 + 4y_3 + 1y_2 - 1y_1 + 3y_0 \geq -3$
12	$+2x_3 - 2x_2 + 1x_1 + 1x_0 + 1y_3 + 2y_2 + 0y_1 + 2y_0 \geq -0$
13	$-2x_3 + 2x_2 + 2x_1 - 1x_0 - 1y_3 + 0y_2 - 2y_1 - 1y_0 \geq -5$
14	$+2x_3 - 3x_2 - 2x_1 + 3x_0 + 4y_3 - 1y_2 + 1y_1 - 4y_0 \geq -6$
15	$+2x_3 - 2x_2 - 2x_1 + 1x_0 - 1y_3 + 2y_2 + 3y_1 + 1y_0 \geq -2$
16	$-1x_3 - 1x_2 - 2x_1 + 1x_0 + 3y_3 + 4y_2 + 3y_1 + 2y_0 \geq -0$
17	$-1x_3 + 0x_2 + 1x_1 - 1x_0 + 1y_3 + 2y_2 + 2y_1 + 1y_0 \geq -0$
18	$-2x_3 - 1x_2 - 2x_1 + 1x_0 + 0y_3 - 1y_2 + 1y_1 - 2y_0 \geq -6$
19	$-1x_3 - 1x_2 + 0x_1 - 2x_0 - 1y_3 - 1y_2 - 2y_1 + 2y_0 \geq -6$
20	$-2x_3 - 1x_2 + 1x_1 + 0x_0 + 1y_3 - 1y_2 - 2y_1 - 1y_0 \geq -5$
21	$+1x_3 - 3x_2 + 1x_1 - 2x_0 - 2y_3 - 2y_2 - 1y_1 + 1y_0 \geq -7$

minimized set of 19 and 20 linear inequalities for ULC and LICID, respectively. The minimized linear inequalities for optimizing the probability of ULC and LICID are shown in Table 9 and Table 10, respectively.

$$\left.\begin{aligned} (p_0, p_1) = (0,0), \quad & if\ Pr[\Delta_i \to \Delta_o] = 1 = 2^{-0} \\ (p_0, p_1) = (0,1), \quad & if\ Pr[\Delta_i \to \Delta_o] = 4/16 = 2^{-2} \\ (p_0, p_1) = (1,0), \quad & if\ Pr[\Delta_i \to \Delta_o] = 2/16 = 2^{-3} \end{aligned}\right\} \tag{1}$$

$$\left.\begin{aligned} (p_0, p_1, p_2) = (0,0,0), \quad & if\ Pr[\Delta_i \to \Delta_o] = 1 = 2^{-0} \\ (p_0, p_1, p_2) = (0,0,1), \quad & if\ Pr[\Delta_i \to \Delta_o] = 6/16 = 2^{-1.415} \\ (p_0, p_1, p_2) = (0,1,0), \quad & if\ Pr[\Delta_i \to \Delta_o] = 4/16 = 2^{-2} \\ (p_0, p_1, p_2) = (1,0,0), \quad & if\ Pr[\Delta_i \to \Delta_o] = 2/16 = 2^{-3} \end{aligned}\right\} \tag{2}$$

5 Experiments

We construct the high probability full-round differential characteristics with the minimum number of active S-boxes for both ciphers in this section. We have given the lower bound on the number of active S-boxes from 1 to 15 (1 to 14) of ULC (LICID) to get these full-round differential characteristics respectively. The lower bounds and time taken by the MILP models to generate them are mentioned in Table 13.

5.1 Differential Characteristics of 15-round ULC

In this subsection, a 15-round differential characteristic has been generated with probability 2^{-45} based on the MILP method. It is presented in Table 11. There are 15 active S-boxes in this differential characteristic.

Table 9: Linear inequalities for optimizing the probability (ULC)

Sr. No.	Linear Inequalities
1	$+0x_3 + 0x_2 - 2x_1 + 0x_0 - 1y_3 - 1y_2 - 1y_1 + 1y_0 + 3p_1 + 4p_0 \geq -0$
2	$+0x_3 - 1x_2 - 2x_1 + 0x_0 + 0y_3 + 1y_2 + 2y_1 + 1y_0 + 1p_1 + 2p_0 \geq -0$
3	$+0x_3 + 0x_2 + 1x_1 + 0x_0 + 0y_3 + 0y_2 + 0y_1 + 1y_0 + 0p_1 - 1p_0 \geq -0$
4	$-2x_3 + 2x_2 - 4x_1 + 3x_0 + 5y_3 + 3y_2 + 2y_1 + 1y_0 + 2p_1 + 1p_0 \geq -0$
5	$+5x_3 + 2x_2 + 1x_1 + 3x_0 - 2y_3 + 3y_2 + 2y_1 - 4y_0 + 2p_1 + 1p_0 \geq -0$
6	$+4x_3 + 1x_2 + 2x_1 + 3x_0 + 1y_3 - 1y_2 + 2y_1 - 1y_0 - 1p_1 - 2p_0 \geq -0$
7	$+1x_3 + 2x_2 + 1x_1 + 1x_0 + 1y_3 + 1y_2 + 2y_1 + 1y_0 - 5p_1 - 2p_0 \geq -0$
8	$+1x_3 + 3x_2 - 3x_1 + 4x_0 + 1y_3 + 4y_2 - 1y_1 - 3y_0 + 1p_1 + 3p_0 \geq -0$
9	$+0x_3 - 1x_2 + 1x_1 + 1x_0 + 0y_3 + 0y_2 + 2y_1 - 2y_0 + 1p_1 + 2p_0 \geq -0$
10	$+1x_3 + 1x_2 - 1x_1 - 1x_0 + 4y_3 + 3y_2 + 2y_1 + 2y_0 - 1p_1 - 2p_0 \geq -0$
11	$+1x_3 - 3x_2 + 2x_1 + 0x_0 + 1y_3 + 0y_2 - 3y_1 + 2y_0 + 4p_1 + 1p_0 \geq -0$
12	$-1x_3 + 0x_2 + 1x_1 - 1x_0 + 0y_3 + 0y_2 - 1y_1 - 2y_0 + 3p_1 + 4p_0 \geq -0$
13	$+0x_3 + 1x_2 - 2x_1 - 1x_0 + 0y_3 - 1y_2 - 3y_1 - 2y_0 + 5p_1 + 8p_0 \geq -0$
14	$+1x_3 + 1x_2 - 1x_1 - 5x_0 - 1y_3 - 5y_2 + 2y_1 - 2y_0 + 9p_1 + 12p_0 \geq -0$
15	$-7x_3 + 1x_2 - 2x_1 + 1x_0 - 7y_3 - 2y_2 + 2y_1 - 2y_0 + 13p_1 + 18p_0 \geq -0$
16	$-7x_3 + 1x_2 - 2x_1 - 2x_0 - 7y_3 + 1y_2 + 2y_1 - 2y_0 + 13p_1 + 18p_0 \geq -0$
17	$-1x_3 + 1x_2 - 2x_1 - 5x_0 + 1y_3 - 5y_2 + 2y_1 - 1y_0 + 9p_1 + 12p_0 \geq -0$
18	$-1x_3 - 1x_2 - 2x_1 + 0x_0 - 2y_3 + 0y_2 - 1y_1 - 1y_0 + 5p_1 + 7p_0 \geq -0$
19	$+0x_3 + 0x_2 + 0x_1 + 0x_0 + 0y_3 + 0y_2 + 0y_1 + 0y_0 - 1p_1 - 1p_0 \geq -1$

Table 10: Linear inequalities for optimizing the probability (LICID)

Sr. No.	Linear Inequalities
1	$-3x_3 + 0x_2 + 2x_1 - 4x_0 - 2y_3 - 1y_2 - 1y_1 + 2y_0 + 9p_2 + 7p_1 + 8p_0 \geq -0$
2	$-6x_3 + 3x_2 - 6x_1 + 1x_0 - 3y_3 - 2y_2 + 3y_1 - 2y_0 + 16p_2 + 15p_1 + 13p_0 \geq -0$
3	$+1x_3 - 3x_2 - 4x_1 + 1x_0 - 2y_3 + 3y_2 + 2y_1 + 3y_0 - 3p_2 + 7p_1 + 4p_0 \geq -0$
4	$+2x_3 - 1x_2 + 1x_1 - 5x_0 - 3y_3 + 2y_2 + 3y_1 - 3y_0 - 2p_2 + 10p_1 + 9p_0 \geq -0$
5	$-4x_3 - 4x_2 - 3x_1 + 3x_0 + 5y_3 + 4y_2 + 7y_1 + 1y_0 - 10p_2 + 7p_1 + 3p_0 \geq -0$
6	$+1x_3 - 3x_2 - 8x_1 + 2x_0 + 4y_3 - 2y_2 + 1y_1 - 10y_0 + 14p_2 + 12p_1 + 19p_0 \geq -0$
7	$+4x_3 + 2x_2 - 4x_1 - 1x_0 + 2y_3 - 4y_2 + 2y_1 + 1y_0 - 1p_2 + 2p_1 + 6p_0 \geq -0$
8	$-1x_3 + 0x_2 + 2x_1 + 3x_0 - 3y_3 + 1y_2 + 1y_1 - 1y_0 + 1p_2 + 2p_1 + 4p_0 \geq -0$
9	$-3x_3 + 2x_2 + 2x_1 - 3x_0 + 3y_3 - 1y_2 + 1y_1 - 1y_0 + 6p_2 + 8p_1 + 5p_0 \geq -0$
10	$-4x_3 + 6x_2 + 1x_1 + 2x_0 - 1y_3 - 5y_2 - 2y_1 + 4y_0 + 9p_2 + 12p_1 + 6p_0 \geq -0$
11	$+2x_3 + 2x_2 - 2x_1 + 1x_0 + 0y_3 + 3y_2 - 3y_1 - 3y_0 + 3p_2 + 4p_1 + 5p_0 \geq -0$
12	$+5x_3 + 1x_2 + 5x_1 + 3x_0 - 2y_3 - 5y_2 - 1y_1 - 3y_0 + 1p_2 + 6p_1 + 5p_0 \geq -0$
13	$+2x_3 + 1x_2 + 2x_1 + 1x_0 + 1y_3 + 1y_2 + 0y_1 + 0y_0 - 4p_2 - 1p_1 - 2p_0 \geq -0$
14	$-1x_3 + 4x_2 - 3x_1 - 4x_0 + 4y_3 - 2y_2 - 5y_1 + 7y_0 + 12p_2 + 4p_1 + 10p_0 \geq -0$
15	$-2x_3 + 2x_2 + 6x_1 + 2x_0 - 5y_3 + 10y_2 - 5y_1 + 1y_0 - 5p_2 + 2p_1 + 7p_0 \geq -0$
16	$-2x_3 + 0x_2 + 2x_1 + 1x_0 + 3y_3 - 2y_2 - 1y_1 + 1y_0 + 4p_2 + 2p_1 + 3p_0 \geq -0$
17	$+2x_3 + 1x_2 + 1x_1 - 2x_0 + 4y_3 + 4y_2 + 2y_1 + 3y_0 - 6p_2 - 6p_1 - 2p_0 \geq -0$
18	$+3x_3 - 6x_2 + 2x_1 - 3x_0 - 4y_3 - 5y_2 - 3y_1 + 1y_0 + 8p_2 + 16p_1 + 15p_0 \geq -0$
19	$-7x_3 - 3x_2 + 2x_1 + 1x_0 + 2y_3 - 3y_2 - 7y_1 - 3y_0 + 16p_2 + 15p_1 + 18p_0 \geq -0$
20	$+0x_3 + 0x_2 + 0x_1 + 0x_0 + 0y_3 + 0y_2 + 0y_1 + 0y_0 - 1p_2 - 1p_1 - 1p_0 \geq -1$

5.2 Differential Characteristics of 14-round LICID

In this subsection, a 14-round differential characteristic has been constructed with probability 2^{-40} using the MILP method. It is given in Table 12. There are 14 active S-boxes in this differential characteristic.

6 Conclusion

In this paper, we have presented full-round differential characteristics for lightweight block ciphers ULC and LICID. We have introduced a 15-round ULC

Table 11: Differential Characteristic (15-rounds) of ULC with Probability $2^{-45.0}$

Round	Input difference	Probability
1	0x0000000000005000	2^{-0}
2	0x0000000000008000	2^{-3}
3	0x0000000000008000	2^{-3}
4	0x0000000000008000	2^{-3}
5	0x0000000000008000	2^{-3}
6	0x0000000000008000	2^{-3}
7	0x0000000000008000	2^{-3}
8	0x0000000000008000	2^{-3}
9	0x0000000000008000	2^{-3}
10	0x0000000000008000	2^{-3}
11	0x0000000000008000	2^{-3}
12	0x0000000000008000	2^{-3}
13	0x0000000000008000	2^{-3}
14	0x0000000000008000	2^{-3}
15	0x0000000000008000	2^{-3}
16	0x0000000000008880	2^{-3}

Table 12: Differential Characteristic (14-rounds) of LICID with Probability $2^{-40.0}$

Round	Input difference	Probability
1	0x000000000000000e	2^{-0}
2	0x0000000010000000	2^{-2}
3	0x0000000100000000	2^{-3}
4	0x1000000000000000	2^{-3}
5	0x0000000000000001	2^{-3}
6	0x0000000002000000	2^{-3}
7	0x0000000008000000	2^{-3}
8	0x0000000008000000	2^{-3}
9	0x0000000008000000	2^{-3}
10	0x0000000008000000	2^{-3}
11	0x0000000008000000	2^{-3}
12	0x0000000008000000	2^{-3}
13	0x0000000008000000	2^{-3}
14	0x0000000040000000	2^{-3}
15	0x0000000120000000	2^{-2}

Table 13: Lower Bounds on # Active S-boxes and Time

Cipher	**Lower Bounds on # Active S-boxes**	**Time**
ULC	15	29s
LICID	14	1s

differential characteristic with a minimum of 15 active S-boxes and a probability of 2^{-45}. We have also introduced a 14-round LICID differential characteristic with a minimum of 14 active S-boxes and a probability of 2^{-40}. Furthermore,

a full-round key recovery attack can be mounted on ULC and LICID using the high probability differential characteristics provided in this paper.

References

[1] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, *et al.*, "Prince–a low-latency block cipher for pervasive computing applications," in *International conference on the theory and application of cryptology and information security*, pp. 208–225, Springer, 2012.

[2] 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 *International workshop on cryptographic hardware and embedded systems*, pp. 450–466, Springer, 2007.

[3] S. Banik, S. K. Pandey, T. Peyrin, Y. Sasaki, S. M. Sim, and Y. Todo, "Gift: a small present," in *International conference on cryptographic hardware and embedded systems*, pp. 321–345, Springer, 2017.

[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 128-bit block cipher," in *Selected Areas in Cryptography: 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers 27*, pp. 535–564, Springer, 2021.

[5] H. M. Heys, "A tutorial on linear and differential cryptanalysis," *Cryptologia*, vol. 26, no. 3, pp. 189–221, 2002.

[6] D. R. Stinson and M. B. Paterson, *Cryptography: theory and practice*. CRC Press, 2019.

[7] L. R. Knudsen and M. Robshaw, *The block cipher companion*. Springer Science & Business Media, 2011.

[8] N. Mouha, Q. Wang, D. Gu, and B. Preneel, "Differential and linear cryptanalysis using mixed-integer linear programming," in *Information Security and Cryptology: 7th International Conference, Inscrypt 2011, Beijing, China, November 30–December 3, 2011. Revised Selected Papers 7*, pp. 57–76, Springer, 2012.

[9] S. Sun, L. Hu, L. Song, Y. Xie, and P. Wang, "Automatic security evaluation of block ciphers with s-bp structures against related-key differential attacks," in *Information Security and Cryptology: 9th International Conference, Inscrypt 2013, Guangzhou, China, November 27-30, 2013, Revised Selected Papers 9*, pp. 39–51, Springer, 2014.

[10] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song, "Automatic security evaluation and (related-key) differential characteristic search: application to simon, present, lblock, des (l) and other bit-oriented block ciphers," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 158–178, Springer, 2014.

[11] Y. Sasaki and Y. Todo, "New algorithm for modeling s-box in milp based differential and division trail search," in *International Conference for Information Technology and Communications*, pp. 150–165, Springer, 2017.

[12] B. Zhu, X. Dong, and H. Yu, "Milp-based differential attack on round-reduced gift," in *Cryptographers' Track at the RSA Conference*, pp. 372–390, Springer, 2019.

[13] M. Kumar and T. Yadav, "Milp based differential attack on round reduced warp," in *Security, Privacy, and Applied Cryptography Engineering: 11th International Conference, SPACE 2021, Kolkata, India, December 10–13, 2021, Proceedings*, pp. 42–59, Springer, 2022.

[14] L. Sliman, T. Omrani, Z. Tari, A. E. Samhat, and R. Rhouma, "Towards an ultra lightweight block ciphers for internet of things," *Journal of information security and applications*, vol. 61, p. 102897, 2021.

[15] K. Zhang, X. Lai, L. Wang, J. Guan, and B. Hu, "Slide attack on full-round ulc lightweight block cipher designed for iot," *Security and Communication Networks*, vol. 2022, 2022.

[16] T. Omrani, R. Rhouma, and R. Becheikh, "Licid: a lightweight image cryptosystem for iot devices," *Cryptologia*, vol. 43, no. 4, pp. 313–343, 2019.

[17] "https://www.sagemath.org."

[18] "https://www.gurobi.com."