Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44)** : 1–11.
ISSN-0037-8712
doi:10.5269/bspm.79201

Security Analysis of Lightweight Block Ciphers ANU-II and LiCi

Dheeraj Singh*, Manoj Kumar, Tarun Yadav and Shivam Kumar

ABSTRACT: ANU-II is a lightweight encryption design with 64-bit block and 80/128 bits key size which is proposed as smallest lightweight design. LiCi is a low-power lightweight block cipher with a 64-bit block and 128-bit key size. Designers have provided a proof of security for differential attack on these ciphers. In this paper, we analyse the security of ANU-II and LiCi to provide the accurate bounds for differential attack. We apply branch-and-bound-based algorithm to search the differential trail. We construct the optimal differential trails for 12 rounds that require 2^{62} chosen plaintext pairs. We also search for the differential trail of LiCi to give accurate security bounds for this attack. Our results are better than the security bounds claimed by the designers. Our analysis provides the best results available so far for a differential attack on ANU-II and differential cryptanalysis of LiCi.

Key Words: Block Cipher, Lightweight Cryptography, Differential Cryptanalysis, R-K Cryptanalys, Branch-and-bound Algorithm, Feistel Structure, IoT.

Contents

* Corresponding author.

2020 *Mathematics Subject Classification:* 94A60, 68P25.
Submitted September 27, 2025. Published December 29, 2025

1. Introduction

There was tremendous progress in the field of block cipher design and analysis during the AES competition (1997-2001). This was due to the rigorous analysis carried out by the cryptographic community for each of the submitted ciphers. However, there was little progress in the field of block cipher design after the adoption of Rijndael as AES. There was a block-cipher design, namely AES with adequate security margins, which was suitable for various types of applications. However, new and emerging technologies created new demands that led to lightweight cryptography. In the first decade of this century, a lightweight block cipher PRESENT was proposed, which became a benchmark for the new lightweight designs. The popularity of PRESENT inspired researchers from the cryptographic community to design more lightweight block ciphers [9] [10] for resource-constrained environments such as RFID tags, sensor networks, etc. Designers are continuously and dedicatedly working to reduce resource consumption without compromising security standards [17] in new lightweight designs.

There is a wide variety of cryptanalysis methods that are used to analyse the security of a block cipher. Differential and linear attacks are one of the basic cryptanalysis techniques, and new designs must provide the security assurance against this attack. However, designers usually attain the bounds for smaller number of rounds and claim the security for full round cipher by generalizing this bound. Due to the larger block sizes, it is difficult to estimate the accurate security bounds of new designs without using computer aids. There are several techniques which can be used in an automated way for finding the accurate security bounds using all possible input values of block ciphers. Branch-and-bound and MILP based methods are examples of such techniques which are widely used by designers and cryptanalysts to find accurate bounds. We can apply these methods to achieve the tight bounds for lightweight block cipher proposals against differential attack.

Differential cryptanalysis was introduced by Biham and Shamir in 1990 which exploits the non-random relationship between the input and output differences to the cipher. This is the first cryptanalytic attack which reduced the complexity of a real world cipher viz. DES. Differential attack has become the first source for evaluating the security of new block cipher designs [6] [7] [8]. A new Design is not accepted without providing the security bounds for differential attack. We can start with the lower bound on the number of active S-boxes in one round trail and join several one round trails to get a differential trail for greater number of rounds. Success of a differential attack depends on the high probability differential trails which can also serve as a distinguisher for the scheme.

Related Key Differential Attack, is an extension of the Differential Attack, was proposed by Biham in 1993 [22]. This attack utilizes related key attack and differential key attack. Since differential attack only input differences of selected plaintexts, but in edition related key differential attack also uses an extra information mainly key differences of chosen keys. Due to this reason this attack proves more powerful then the standard attack in application point of view. As this attack exploits the key schedule algorithm of a cipher after introducing the key differences. So it can be impractical if the key schedule algorithm strongly designed. Related key differential attack applied on AES [19], LOKI91 [20] ,LBOCK [21] and ANU-II [2].

We organise the remaining paper in the following way. We describe a short description of block ciphers ANU-II and LiCi in section 2. Differential and Related cryptanalysis in brief and talk about branch-and-bound based algorithm to search the differential trail in section 3. We compare the bounds on number of active S-boxes and present the optimal differential trails for ANU-II in section 4. In section 5, we present differential trial for lightweight block cipher LiCi.

2. Lightweight Block Ciphers: ANU-II and LiCi

Lightweight block cipher generally works with 64-bit message block and 80 or 128 bit key size whereas block and key size in a regular block cipher is 128-bit for optimal security [13] [9] [17]. We provide a brief description of lightweight block ciphers ANU-II and LiCi in this section. Interested readers may find the detailed description and key expansion part for these ciphers in [2] and [3] respectively.

2.1. Description of ANU-II

ANU-II was proposed by Dahiphale et. al. at IEEE conference (BID) 2017. ANU-II is the successor of lightweight block cipher ANU and it is a Feistel structure based block cipher [1]. It takes 64-bit message block and 80/128 bits key which is processed in 25 rounds. Each message block is divided into two equal halves P_1^L and P_1^R of size 32-bit each. In each round, there is an application of one 4-bit S-box 8 times in parallel. Then, right and left circular shift operations are applied on each part with key mixing operation to get the round output.

2.1.1. Encryption Algorithm. We describe the encryption algorithm using substitution operation S_B with left and right circular shift operations (Algorithm 1). Round function applies the substitution operation S_B on P_i^L. First, S_B divides 32-bit word P_i^L into 4-bit nibbles, then apply S-box (Table 1) 8 times in parallel on each nibble. After that, right circular shift by 3 bits is applied on P_i^R which is XORed with the output from S_B and round subkey RK_{i_1} to generate P_{i+1}^R. Finally, left circular shift by 10 bits is applied on P_{i+1}^R and the result is XORed with $P_i^R$and Round Subkey RK_{i_2} to obtain P_{i+1}^L. We get 32-bit round keys (RK_i) from 80/128 bits key (K) using a key expansion algorithm [2].

Algorithm 1: Encryption Algorithm of ANU-II

```
Input: $P = (P_1^L || P_1^R)$ and $K$
Output: $C = (P_{26}^L || P_{26}^R)$
for $i$=1 to 25 do
    $P_{i+1}^R = S_B(P_i^L) \oplus (P_i^R \ggg 3) \oplus RK_{i_1}$
    $P_{i+1}^L = (P_{i+1}^R \lll 10) \oplus (P_i^R) \oplus RK_{i_2}$
end
```

Table 1: S-Box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
ANU-II: S(x)	E	4	B	1	7	9	C	A	D	2	0	F	8	5	3	6

2.2. Description of LiCi

LiCi was proposed by Patil et. al. in IEEE conference ICT (ICEI) 2017. This is also a Feistel structure based design [3]. Its block size is 64-bit and key size is 128-bit. There are total 31 round. Round function applies S-box on first half 32-bit word thereafter right and left circular shifts are applied with add round key operation in each round.

2.2.1. Encryption Algorithm. First of all, 64-bit input message block is divided into two 32-bit words namely left P_i^L and right P_i^R word (Algorithm 1). Substitution operation S_B (Table 2) is applied on left half P_i^L and 32-bit output from S_B is stored in a temporary variable named $Temp$. The current values in the variables $Temp$, P_i^R and round subkeyRK_{i_1} are XORed and left circular shift by 3 bits is applied on the result to obtain P_{i+1}^L. While, current values in the variables $Temp$, P_{i+1}^L and round subkeyRK_{i_2} are XORed and right circular shift by 7 bits is applied on the result to obtain P_{i+1}^R [3].

Table 2: S-Box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
LiCi: S(x)	3	F	E	1	0	A	5	8	C	4	B	2	9	7	6	D

2.3. Comparison between ANU-II and LiCi

We compare ANU-II and LiCi on the basis of similarity and differences in the design constructions. Both ciphers are based on Feistel structure which encrypts a 64-bit message block by dividing it into two

Algorithm 2: Encryption Algorithm of LiCi

```
Input: $P = (P_1^L||P_1^R)$ and $K$
Output: $C = (P_{26}^L||P_{26}^R)$
for $i$=1 to 31 do
    $Temp = S_B(P_i^L)$
    $P_{i+1}^L = (Temp \oplus P_i^R \oplus RK_{i_1}) \lll 3$
    $P_{i+1}^R = (Temp \oplus P_{i+1}^L \oplus RK_{i_2}) \ggg 7$
end
```

32-bit words viz. left and right half. There is an application of 4-bit S-box eight times in parallel on the left 32-bit word in each cipher. Whereas, output from the substitution operation is used to modify the left and right 32-bit words. The main difference lies in the values of left and right circular shift operations. ANU-II uses the right and left circular shift by 3 and 10 bit respectively while LiCi uses the left and right circular shift by 3 and 7 bit respectively. However, values of the circular shift in each design are relatively prime and there is an application of different 4-bit S-box in each design. We will analyse both ciphers and provide the comparison of our results with the designers bounds for differential cryptanalysis.

3. Cryptanalysis Approaches

There is a long list of cryptanalysis methods which can be applied on block ciphers. Security assessment to provide the accurate bounds from the basic attacks like differential, linear and related key cryptanalysis etc. are essential for new proposals. We discuss differential, related key cryptanalytic attacks and branch-and-bound based algorithm to get the differential trail in this section.

3.1. Differential Cryptanalysis

Block ciphers are designed in such a way that its output is indistinguishable from a random permutation. This means that there should not exist any exploitable relationship between the input and output to the system. However, we can get the non-random relation by observing the input and output in pairs. For this, take a plaintext pair (P_1, P_2) and find input difference $(\triangle P = P_1 \oplus P_2)$, study the propagation of output difference $(\triangle C = C_1 \oplus C_2)$ through the encryption process [?]. For a block cipher with n-bit block size, probability of random distribution is 2^{-n} for all input and output pairs. But in real practice, we observe the input difference $(\triangle P = P_1 \oplus P_2)$ which results in the output difference $(\triangle Q = Q_1 \oplus Q_2)$ with high probability p. If probability of the trail is significantly greater than the probability in random case $(i.e.\ p \gg 2^{-n})$ then differential trail can be used to distinguish the block cipher from random permutation. An adversary will need to choose $1/p$ plaintext pairs approximately and get their corresponding encrypted text through an oracle that will be used to distinguish or to recover the secret key. The main desideratum to mount the attack is the existence of high probability differential trail in a block cipher. Branch-and-bound based algorithm can be used to construct the high probability differential trails.

3.2. Related Key Cryptanalysis

In practice, related key differential cryptanalysis utilizes the relations between two keys in addition to the relation among the plaintext pairs as used in a differential attack. Here, we choose plaintexts (P_1, P_2) and keys (K_1, K_2) then find input differences $(\triangle P = P_1 \oplus P_2)$, $(\triangle K = K_1 \oplus K_2)$, and observe propagation of $\triangle P$ and $\triangle K$ through several rounds of a cipher to the output difference, with a purpose to know whether the output of the cipher behaves randomly or not in the related key settings. We find the probability of a related key differential trail, $(\triangle P_i, \triangle K_i, \triangle C_i)$, using the branch-and-bound based technique and use it as a related key differential distinguisher which can also be used to recover the round subkeys of a cipher.

3.3. Branch-and-bound based Algorithm

The first and foremost requirement of the differential cryptanalysis is a high probability differential trail. In 1994, Matsui proposed branch-and-bound based algorithm to find the best differential trails in DES [15]. This was the first approach to search the optimal differential trail of DES in automated way. Thereafter, various other methods like MILP based, STP based etc. are proposed to search the differential trail in automated way.

Branch-and-bound based algorithm applies induction on the number of rounds. It derives the best r-round trail with probability B_r from the knowledge of best i-round trail with probability B_i $(1 \leq i \leq r-1)$. In general, it selects a 3-round trail with high probability and use it as initial value to find the best r-round trail with optimal probability B_r. This algorithm have provided the best results for block ciphers with S-boxes in round function, therefore we can use it to obtain the best results for lightweight block ciphers ANU-II and LiCi. We apply this algorithm to get differential trails with least number of active S-boxes and calculate the probability of each trail to filter out the trails with maximum probability. For 64-bit block size, it is feasible to start with $r = 1$ and apply this algorithm iteratively to find the optimal differential trails for greater rounds by adding one round at a time.

We improve the branch-and-bound based algorithm presented by Kumar el al. in [13] to analyse the security of lightweight block ciphers ANU and PICO [1] [4]. We describe the generalized algorithm that takes n-bit block X as input and nibble (S-box) size is m-bit for differential trail search (Algorithm 3). The input block X is divided in $t(= n/m)$ nibbles, then DDT is applied on each nibble in left half 32-bit word. Any non-zero input to DDT contributes towards the probability of trail. We start with one non-zero nibble in the input X and track the propagation of this difference. We can also start with two non-zero nibbles in the input X and track the difference in same way. After trying the all possible values for each nibble, we filter out the trails with least number of active S-boxes and best probability.

4. Analysis of ANU-II

We analyse the lightweight block cipher ANU-II for differential attack only. We apply our approach based on branch-and-bound technique (Algorithm 3) to search the optimal differential trails in ANU-II that provide the best result as compared to the designers bound.

4.1. Differential Trails Search

ANU-II uses round key addition, left and right rotation, bitwise XOR and substitute nibble operations [2] in each round. Circular shift and bitwise XOR are linear operations which provide the fixed difference before and after the application of each operation. While, state variables U_1, U_2 provides the same difference value $\triangle U = U_1 \oplus U_2$ before and after the add round key operation. Substitute nibble is a non-linear operation which does not output the fix difference value. Therefore, we generate a distribution table for each possible input and output difference that is known as difference distribution table (DDT) [12]. Dimension of DDT for m-bit S-box is $2^m \times 2^m$. For any non-zero input $(\triangle_i \neq 0)$, we get more than one non-zero outcomes $(\triangle_o \neq 0)$. For 4-bit S-box of ANU-II, there are 256 possible input and output difference pairs $(\triangle_i, \triangle_o)$ (Table 3).

In table 3, (0,0) is the trivial pair that occurs 16 times. The maximum and minimum value of occurrence for non-trivial pairs $(\triangle_i, \triangle_o)$ are 4 and 2 that occurs 24 and 72 times respectively. We apply algorithm 3 to search the differential trails and filter the highest probability trails that covers the maximum number of rounds. We start with all possible non-zero values for each 4-bit nibble position and use bounds on two factors in the search algorithm. First bound is used to select the trails with least number of active S-boxes and then second bound is applied to filter the highest probability differential trails out of the remaining trails after first bound. These trails are used to mount the key recovery attack and distinguish the block cipher from random permutations.

In table 4, we provide a comparison of our results with bounds estimated by Dahiphale *et.al*. We get seven as a lower bound on the number of active S-boxes in any 4-round trail as compared with the 13 active S-boxes. Our analysis reduces the lower bound value by 50% approximately. We use search algorithm 3 to find the maximum number of rounds that can be distinguished using a differential attack. We get the optimal trails for 12 rounds that requires 2^{62} chosen plaintext pairs to distinguish 12 rounds of ANU from a random permutations (Table 5). We need to add more rounds at the top and bottom of this trail to recover the key used while encrypting.

Algorithm 3: Branch-and-bound based algorithm for differential trail

```
Input: $X$, S-box size (bits) = $m$, $least = A$, $optimal = B$ and $N_{SB} = 0$
Output: Optimal Differential Trails with best probability $P_T$
for $i$=1 to $t$ do
    for $j$=1 to $2^m - 1$ do
        $Nibble_i = j; Nibble_{(\neq i)} = 0;$
        $X = (Nibble_1, Nibble_2, \dots, Nibble_t);$
        for Round=1 to r do
            Count($\neq$ Non-zero nibbles in $X$);
            $N_{SB} = N_{SB} + Count;$
            for $k_1 = 1$ to 15 do
                for $k_2 = 1$ to 15 do
                    ....................
                    for $k_t = 1$ to 15 do
                        $p_1 = DDT[Nibble_1][k_1];$
                        If($p_1 = 0$) continue;
                        $p_2 = DDT[Nibble_2][k_2];$
                        If($p_2 = 0$) continue;
                        ..........................
                        $p_t = DDT[Nibble_t][k_t];$
                        If($p_t = 0$) continue;
                        $Y = (k_1, k_2, \dots, k_t);$
                        $X = P_{Layer}(Y);$
                        $P_r = p_1 * p_2 * ... * p_t$
                    end
                end
            end
        end
        $P_T = P_1 * P_2 * ... * P_r$
        if $N_{SB} \leq least$ and $P_T \leq optimal$ then
            Return: Optimal differential trail with probability $P_T$
        end
    end
end
```

4.2. Related Key Differential Trails Search

The propagation of input differences across successive rounds of the Related Key Differential is shown in Table 6. Each row corresponds to a single round and tells the round input differences, the number of active S-boxes, and the corresponding differential probabilities.

The Input Difference ($\triangle P_i^L \mid\mid \triangle P_i^R$) column shows the left and right half input differences expressed in hexadecimal notation. The Related Key Difference column shows the key difference in the respective rounds of the trail. The Active S-box column indicates the number of S-boxes that process a non-zero difference in each round. This metric is critical, as a higher number of active S-boxes generally results in a faster decrease of the overall differential probability, therefore gives better results against RK differential cryptanalysis. The Probability column provides the base-2 negative logarithm of the transition probability for each round. Lower values denote transitions with higher likelihood, whereas larger values correspond to less probable transitions. The Cumulative Probability column aggregates these values across rounds, giving the total cost of the differential trail up to that point.

Thus it is observed that the first five rounds exhibit no active differences, meaning that no S-boxes are involved and the differential probability remains unchanged. Starting from round six, non-zero differences

Table 3: Difference Distribution Table of ANU-II

$\triangle_o \rightarrow$ $\triangle_i \downarrow$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	2	2	0	0	0	4	0	0	2	2	4
2	0	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0
3	0	0	4	0	0	2	2	0	0	0	0	0	0	2	2	4
4	0	0	0	2	0	2	0	4	0	4	0	2	0	2	0	0
5	0	2	0	2	0	0	2	2	2	0	2	0	2	2	0	0
6	0	0	2	0	2	0	0	0	4	0	2	0	2	0	4	0
7	0	2	2	0	2	2	2	2	2	0	0	2	0	0	0	0
8	0	0	0	2	0	0	2	0	0	0	0	2	4	0	2	4
9	0	4	2	0	2	0	0	0	0	4	2	0	2	0	0	0
A	0	0	0	2	4	0	2	0	0	0	0	2	0	0	2	4
B	0	4	2	0	2	0	0	0	0	4	2	0	2	0	0	0
C	0	2	0	0	0	2	2	2	2	0	2	2	2	0	0	0
D	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0
E	0	2	2	2	2	0	2	2	2	0	0	0	0	2	0	0
F	0	0	0	0	0	0	0	4	4	4	0	0	0	0	4	0

Table 4: Lower Bound on active S-boxes in ANU-II

Round Index	#Active S-boxes (Lower Bound)	# Active S-boxes (Lower Bound)
1	0	0
2	2	2
3	6	5
4	13	7
Ref.	[2]	This Paper

appear, leading to the activation of one or more S-boxes. As the rounds progress, the number of active S-boxes increases, and the cumulative probability decreases sharply. In the last round, five S-boxes are active and the cumulative probability reaches 2^{-63}, shows that the cipher achieves strong diffusion and significant resistance to Related Key differential attack over multiple rounds.

5. Analysis of LiCi

LiCi is also a Feistel structure based lightweight block cipher which uses round key addition, nibble substitution and bit permutation operations in each round [3]. We analyse LiCi for differential and linear attacks.

5.1. Differential Trails Search

S-box is the only non-linear operation in LiCi while other operations are linear in nature. Therefore, we need to find the occurrence of all possible input and output difference combinations for S-box. We construct a distribution table for all possible difference combinations $(\triangle_i, \triangle_o)$ (Table 7). The maximum and minimum value for difference pairs $(\triangle_i, \triangle_o)$ is 4 and 2 that appears 24 and 72 times respectively. We will use the high probability difference occurrences to construct the optimal differential trails.

We use algorithm 3 to find the differential trails with minimum number of active S-boxes. As per designers estimates [3], there are at least 12 active S-boxes in any 4-round differential trail of LiCi. However, we constructed the differential trails with four active S-boxes in four rounds of LiCi (Table 8). This improves the bound on the number of active S-boxes from 12 to 3 that is approximately 70% reduction. We apply algorithm 3 and get the optimal differential trails for 11 rounds with probability 2^{-67} (Table 9). We can use 10-round trails with probability 2^{-56} to distinguish the ten rounds of LiCi

Table 5: Differential Trail of ANU-II

Round	Input Difference	#Active	Prob.	Prob.
Index	($\triangle P_i^L \| \triangle P_i^R$)	S-box	($-log_2 p_i$)	($-\Sigma_i log_2 p_i$)
1	00000000 00000006	0	0	0
2	00000306 c0000000	2	6	6
3	c0100b00 c0000402	3	8	14
4	00300500 40b00c00	2	5	19
5	009c0f00 c0100b00	3	7	26
6	30000800 c03c0400	2	5	31
7	c0300500 40000300	3	6	37
8	00100300 00100400	2	6	43
9	c0000703 c0f00400	3	7	50
10	c0c00000 00000c01	2	4	54
11	00000c03 00800000	2	4	58
12	00b00700 c0000c01	2	4	62
13	80040f01 c0100100	–	–	–

Table 6: Related Key Differential Trail of ANU-II

Round	Input Difference	Related Key	#Active	Prob.	Prob.
Index	($\triangle P_i^L \| \triangle P_i^R$)	Difference	S-box	($-log_2 p_i$)	($-\Sigma_i log_2 p_i$)
1	00000000 00000000	00000000 00008000 00000000 00000000	0	0	0
2	00000000 00000000	00000000 10000000 00000000 00000000	0	0	0
3	00000000 00000000	00000200 00000000 00000000 00000000	0	0	0
4	00000000 00000000	00400000 00000000 00000000 00000000	0	0	0
5	00000000 00000000	00000000 00000000 00000000 00000006	0	0	0
6	00001800 00000006	00000000 00000000 00000000 0000c000	1	3	3
7	00700306 c0001c00	00000000 00000000 00000000 18000000	2	5	8
8	80060c00 00100184	00000000 00000000 00000300 00000000	3	8	16
9	0030c104 e0000830	00000000 00000000 00600000 00000000	3	9	25
10	600c0c40 1c201b01	00000000 0000000c 00000000 00000000	4	9	34
11	0800580f c3850810	00000000 00018000 00000000 00000000	4	10	44
12	00b12041 1470cd0a	00000000 30000000 00000000 00000000	4	9	53
13	44d7a000 429429db	00000600 00000000 00000000 00000000	5	10	63

from a random permutation. This trail can be used to recover the secret key by adding some rounds at the bottom/top of the trail.

Table 8: Lower Bound for Differential Trails in LiCi

Round	#Active S-boxes	# Active S-boxes
Index	(Lower Bound)	(Lower Bound)
1	1	1
2	2	1
3	6	2
4	12	4
Ref.	[3]	This Paper

Table 7: Difference Distribution Table of LiCi

$\triangle_o \rightarrow$																
$\triangle_i \downarrow$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2
2	0	0	2	0	0	2	2	2	0	0	2	0	0	2	2	2
3	0	4	2	0	2	0	0	0	2	0	0	0	0	0	2	4
4	0	0	0	4	0	4	0	0	0	2	0	2	0	2	0	2
5	0	0	0	0	4	0	4	0	0	2	0	2	0	2	0	2
6	0	0	2	0	0	2	2	2	0	2	2	2	0	0	2	0
7	0	4	2	0	2	0	0	0	0	0	2	4	2	0	0	0
8	0	0	0	4	0	4	0	0	0	2	0	2	0	2	0	2
9	0	0	0	4	0	0	0	4	2	0	2	0	2	0	2	0
A	0	0	2	0	0	2	2	2	2	0	0	0	2	2	0	2
B	0	4	2	0	2	0	0	0	0	0	2	0	2	4	0	0
C	0	0	0	0	0	0	0	0	4	0	4	0	4	0	4	0
D	0	0	0	4	4	0	4	4	0	0	0	0	0	0	0	0
E	0	0	2	0	0	2	2	2	2	2	0	2	2	0	0	0
F	0	4	2	0	2	0	0	0	2	4	0	0	0	0	2	0

Table 9: Differential Trail of LiCi

Round	Input Difference	#Active	Prob.	Prob.
index	$\triangle P_i$	S-box	$(-log_2 p_i)$	$(-\Sigma_i log_2 p_i)$
1	00000002 00000002	1	3	3
2	00000000 04000000	0	0	3
3	20000000 00400000	1	3	6
4	02000003 06c40000	2	6	12
5	06200020 48004000	3	9	21
6	0b020502 4404c40b	4	11	32
7	000e000a 00081608	2	6	38
8	0000b000 10001160	1	2	40
9	80000b00 01000036	2	5	45
10	880009b7 6ef00011	5	11	56
11	df804002 27d50090	5	11	67
12	b7298490 250c3369	–	–	–

6. Conclusion

We presented the optimal differential trails in lightweight block ciphers ANU-II and the differential trail in LiCi. We obtained accurate bounds for the number of active S-boxes in the differential trail of these ciphers. Optimal differential trails for ANU-II are presented up to 12 rounds with probability 2^{-62} and optimal RK differential trails for ANU-II are presented up to 13 rounds with probability 2^{-63}. We presented the 11-round differential trails of LiCi with probability 2^{-67}. Our results provide tighter/more accurate bounds for differential attacks on ANU-II and LiCi published in the open literature so far.

Acknowledgments

I would like to thank my supervisor Dr Manoj Kumar, Scientist 'E' in DRDO, Delhi, for his support and guidance in this paper. Also, I would like to thank all the authors for assisting in completing this paper.

References

1. Bansod, G., Patil, A., Sutar, S., & Pisharoty, N. (2016). *ANU: An Ultra Lightweight Block Cipher for Security in IoT*, Security and Communication Networks, 9(18), 5238–5251. https://doi.org/10.1002/sec.1692

2. Dahiphale, V., Bansod, G., & Patil, J. (2017).*ANU-II: a fast and efficient lightweight encryption design for security in IoT*. In Proceedings of the International Conference on Big Data, IoT and Data Science (BID) (pp. 130–137). Pune, India.

3. Patil, J., Bansod, G., & Shashikant, K. (2017).*LiCi: A New Ultra Lightweight Block Cipher*, In International Conference on Emerging Trends and Innovation in ICT (ICEI) (pp. 40–45). IEEE.

4. Bansod, G., Pisharoty, N., & Patil, A. (2016).*PICO: An Ultra Lightweight and Low Power Encryption Design for Ubiquitous Computing*, Defence Science Journal, 66(3), 259–265. https://doi.org/10.14429/dsj.66.9276

5. Bauer, C. P. (2013).*Secret History: The Story of Cryptology*, Chapman & Hall/CRC Press, Taylor & Francis Group.

6. Biham, E., & Shamir, A. (1991).*Differential Cryptanalysis of FEAL and N-hash*,In D. W. Davies (Ed.), Advances in Cryptology — EUROCRYPT '91 (pp. 1–16). Springer. https://doi.org/10.1007/3-540-46416-6 1

7. Biham, E., & Shamir, A. (1991).*Differential Cryptanalysis of DES-like Cryptosystems*, Journal of Cryptology, 4(1), 3–72. https://doi.org/10.1007/BF00192340

8. Biham, E., & Shamir, A. (1992).*Differential Cryptanalysis of the full 16-round DES*, In Advances in Cryptology — CRYPTO '92 (pp. 487–496). Springer. https://doi.org/10.1007/3-540-48000-5 44 (LNCS vol. 740)

9. Bogdanov, A. (2009).*Analysis and Design of Block Cipher Constructions*, [Doctoral dissertation, Ruhr-University Bochum].

10. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., & Vikkelsoe, C. (2007).*PRESENT: An Ultra-Lightweight Block Cipher*, In Cryptographic Hardware and Embedded Systems — CHES 2007 (pp. 450–466). Springer. https://doi.org/10.1007/978-3-540

11. Daemen, J., & Rijmen, V. (2002).*The Design of Rijndael*, AES — The Advanced Encryption Standard. Springer-Verlag. https://doi.org/10.1007/978-3-662-60770-1

12. Hays, H. M. (2002).*A Tutorial on Linear and Differential Cryptanalysis*, Cryptologia, 26(3), 188–221. https://doi.org/10.1080/0161-110291890878 (journal DOI)

13. Knudsen, L., Robshaw, M.J.B.(2011). *Block Cipher Companion*, Book Springer, ISBN 978-3-642-17341-7, 2011.

14. Kumar, M., Pal, S. K., & Panigrahi, A. (2014).*FeW : A Lightweight Block Cipher*, Cryptology ePrint Archive, Report 2014/326. https://eprint.iacr.org/2014/326

15. Matsui, M. (1994).*On Correlation between the Order of S-boxes and the Strength of DES*, In Advances in Cryptology — EUROCRYPT '94 (pp. 366–375). Springer. https://doi.org/10.1007/3-540-49264-X 30

16. National Bureau of Standards. (1977). *Data Encryption Standard*, (Federal Information Processing Standards Publication 46). U.S. Department of Commerce.

17. Poschmann, A. Y. (2009).*Lightweight Cryptography: Cryptographic Engineering for a Pervasive World*, [Doctoral dissertation, Ruhr-University Bochum].

18. Sorkin, A. (1984).*Lucifer: A Cryptographic Algorithm*, Cryptologia, 8(1), 22–41. https://doi.org/10.1080/0161-118491858800

19. Bertoni, G., Breveglieri, L., & Pelosi, G. (2008). *Related-key Differential Cryptanalysis of AES-256*, Journal of Cryptology, 21(1), 19–42. https://doi.org/10.1007/s00145-007-9006-6

20. Knudsen, L. R. (1993).*Differential Cryptanalysis of LOKI and LOKI91*, In Advances in Cryptology — AUSCRYPT '92 (pp. 344–351). Springer. https://doi.org/10.1007/3-540-57220-1 70 (LNCS vol. 718)

21. Long, W., Mei-Qin, W., & Jing-Yuan, Z. (2022). *Related Key Differential Attacks on Reduced-Round LBlock*, Security and Communication Networks. https://doi.org/10.1155/2022/1-11

22. Biham, E. (1994).*New Types of Cryptanalytic Attacks Using Related Keys*, In Advances in Cryptology — EUROCRYPT '93 (pp. 398–409). Springer. https://doi.org/10.1007/3-540-48285-7 35

Table 10: Differential Trails in ANU-II

S.	Input Difference	7_R	Output Difference	Prob.
No	$\triangle_{in}$	$\longrightarrow$	$\triangle_{out}$	$-log_2p$
1	0000 0000 0840 0000	$\longrightarrow$	a989 0500 2200 8088	62
2	0000 0000 0840 0000	$\longrightarrow$	a989 1410 2200 8088	62
3	0000 0000 0840 0000	$\longrightarrow$	a989 1411 2200 8088	62
4	0000 0000 0840 0000	$\longrightarrow$	a989 1511 2200 8088	62
5	0000 0000 0840 0000	$\longrightarrow$	a989 4544 2200 8088	62
6	0000 0000 0840 0000	$\longrightarrow$	a989 5454 2200 8088	62
7	0000 0000 0840 0000	$\longrightarrow$	a989 5455 2200 8088	62
8	0000 0000 0840 0000	$\longrightarrow$	a989 5555 2200 8088	62

Table 11: Differential Trails in LiCi

S.	Input Difference	21_R	Output Difference	Prob.
No	$\triangle_{in}$	$\longrightarrow$	$\triangle_{out}$	$-log_2p$
1	0002 0000 0000 0000	$\longrightarrow$	0000 0040 8000 0000	64
2	0002 0000 0000 0000	$\longrightarrow$	0000 0040 0008 0000	64
3	0000 0000 0002 0000	$\longrightarrow$	0000 0040 8000 0000	64
4	0000 0000 0002 0000	$\longrightarrow$	0000 0040 8000 0000	64

7. Appendix: Optimal Trails in ANU-II and LiCi

8. CONTRIBUTORS

Mr Dheeraj Singh completed his M.Phil. from the University of Delhi and pursuing Ph.D. from the University of Delhi. He is currently working as an Assistant Professor at Aryabhatta College, University of Delhi. His research area includes: Design and analysis of block ciphers. In the current study, his contributions are in the design and analysis of the lightweight block ciphers and the implementation of various security analysis.

Dr Manoj Kumar obtained his Ph.D. from the Department of Mathematics, University of Delhi. He is currently working as a Scientist in the DRDO-SAG. His research area includes: Design and analysis of symmetric cryptographic primitives. In the current study, his contributions are in the overall design sketch and implementation of various attacks on the lightweight block ciphers.

Mr Tarun Yadav completed his B.Tech. in Computer Science and Engineering from IIT Ropar. He is currently working as a Scientist at DRDO-SAG. His research area includes: Protocol analysis and cryptanalysis of block ciphers. In the current study, his contributions are in implementation of S-box and analysis of the lightweight block ciphers.

Mr Shivam Kumar completed his M.Sc. in Mathematics from Department of Mathematics SDC, University of Delhi. He is seeking to pursue his research in the field of mathematics (Cryptology, Coding Theory & Number Theory etc.). In the current study, his contributions are in the design and analysis of the lightweight block ciphers and the implementation of method.

Dheeraj Singh,
Department of Mathematics,
University of Delhi, Delhi-110 007
India.
E-mail address: panipatdheeraj@gmail.com

and

Manoj Kumar,
Scientific Analysis Group, DRDO,
Metcalfe House Complex, Delhi-110 054
India.
E-mail address: manojkumar.sag@gov.in

and

Tarun Yadav,
Scientific Analysis Group, DRDO,
Metcalfe House Complex, Delhi-110 054
India.
E-mail address: tarunyadav.sag@gov.in

and

Shivam Kumar,
Deparment of Mathematics SDC,
University of Delhi, Delhi-110 021
India.
E-mail address: sksishodiya13@gmail.com