UDC 003.26.09

Method of Security Evaluation of the LBlock-like Ciphers against Differential Cryptanalysis

Oleksii Yakymchuk[1], Mykhailo Lopatetskyi[1]

[1]*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",*
Institute of Physics and Technology

Abstract

This paper considers the problem of estimating the security of the lightweight block cipher LBlock against differential cryptanalysis. We formalize the process and present two algorithms of computing upper bounds for differential probabilities. The baseline algorithm provides approximate estimates based on the number of active S-boxes, while the refined algorithm incorporates the full probability distributions of S-box differentials, yielding significantly better bounds.

To illustrate the efficiency of the proposed methodology, we introduce a modified version of LBlock with 8×8 S-boxes, which has lower computational complexity and allows experimental evaluation on our resources. We consider different linear permutations of encryption round, analyzing affect the estimates produced by both algorithms. The results demonstrate that the refined algorithm achieves much smaller maximum bounds (below 2^{-40} in the best cases) compared to the baseline approach and provides a more accurate characterization of security against differential cryptanalysis.

Overall, the proposed algorithms make it possible to efficiently evaluate the provable security of LBlock-like ciphers against differential cryptanalysis.

Keywords: symmetric cryptography, block cipher, differential cryptanalysis, LBlock

Introduction

Differential cryptanalysis, introduced by Biham and Shamir in the early 1990s [1], remains one of the most powerful and widely used techniques for analyzing the security of symmetric key cryptographic primitives. In a foundational contribution, Nyberg and Knudsen [2] formulated and successfully addressed the problem of provable security against differential attacks for DES-like iterated ciphers. They showed that, under the assumption of independent round keys, differential probabilities depend only on the round function of the cipher.

Keliher, Meijer, and Tavares proposed the KMT1 algorithm for efficiently computing improved upper bounds on the maximum expected differential probability (MEDP) and maximum expected linear probability (MELP) in substitution–permutation (SP) networks [3]. Later, they introduced the KMT2 algorithm, which further refines these bounds and was applied to the computation of the maximum average linear hull probability for Rijndael [4] and computation of probabilities bounds related to linear and differential cryptanalysis for the AES [5]. This line of work was subsequently adapted to Feistel structures and applied to the Camellia block cipher, yielding significantly tighter bounds than previous approaches [6]. However, the algorithms fundamentally rely on the Markov cipher assumption, which requires statistical independence of round transitions. Security estimates for non-Markov Feistel networks were previously obtained by Alexeichuk and Kovalchuk [7].

However, in many situations the analytically derived upper bounds on differential probabilities are overly conservative and do not provide a reliable basis for assessing the security of a cipher against differential cryptanalysis. For instance, applying the Nyberg–Knudsen theorem to the encryption standard DSTU GOST 28147:2009 [8] yields an upper bound of 2^{-4} for the differential probabilities, which deviates significantly from the actual values.

In our previous work [9], we introduced an algorithm for estimating the upper bounds of differential probabilities in non-Markov Feistel networks with SP-network round functions. That study focused primarily on model ciphers, highlighting the influence of S-box differential probabilities and linear transformation parameters on the security estimates.

LBlock is a lightweight block cipher proposed by Wu and Zhang [10]. Since its introduction, LBlock has attracted attention as a candidate for resource-constrained environments due to its compact structure and efficient implementation. LBlock was originally evaluated to have sufficient security against differential cryptanalysis. In particular, the designers reported that no useful differential or linear characteristic could be constructed beyond 15 rounds, and this result was obtained by the method of active S-boxes which estimates the practical security against differential cryptanalysis. Subsequent research refined this assessment, several works investigated the security against differential cryptanalysis of LBlock using more advanced techniques. For example, Minier and Naya-Plasencia demonstrated a related-key impossible differential attack covering up to 22 rounds [11], Chen and Miyaji performed a detailed analysis combining differential and boomerang techniques [12], and Shi and Liu presented improved related-key differential attacks on reduced-round variants [13]. In contrary, we do not focus on constructing explicit characteristics but instead propose a method for computing upper bounds on differential probabilities, providing a more rigorous assessment of LBlock's security against differential cryptanalysis.

In this paper, we extend those results by adapting the proposed methodology to the lightweight block cipher LBlock and its modifications. Due to its relatively simple structure, LBlock enables a more straightforward implementation of the algorithms and allows the security bounds to be computed efficiently. We analyze the role of different S-boxes and permutations, and experimentally evaluate the effectiveness of the refined estimation techniques.

The results of this paper were partially presented at the XXIII Ukrainian scientific and practical conference of students, PhD students, and young scientists *Theoretical and Applied Problems of Physics, Mathematics and Computer Science* (2025, Kyiv, Ukraine) [14].

The paper is organized as follows. Section 1 introduces the standard notation, the main terms of differential cryptanalysis, and a description of LBlock-like ciphers. Section 2.1 presents a baseline algorithm for constructing the upper-bound matrix of differential probabilities. Section 2.2 describes a refined algorithm that incorporates the probability distribution of S-boxes. Section 3 provides the description and analysis of an experiment applying the proposed algorithms to LBlock-like ciphers.

1. Main terms and notations

1.1. Basics

Block ciphers are a fundamental class of symmetric-key primitives that transform fixed-size input blocks into output blocks of the same size using a secret key, and serve as the core building blocks for many cryptographic systems.

Let $V_n = \{0,1\}^n$ be the space of n-bit vectors.

Round transformation f_k is a mapping of the form

$$f_k : V_q \times K \to V_q,$$

where V_q is the set of binary vectors of length q, K is the set of round keys (the key space), and $k \in K$. If a round transformation is a composition of a key addition, some (nonlinear) function g not parameterized by the key, and certain linear transformation, then we call such a function g a *round function*.

An *iterative r-round block cipher* E is a mapping of the form

$$E : V_q \times K^r \to V_q,$$

defined as the composition of r round transformations:

$$E_k(x) = f^{(r)}_{k_r}\big(f^{(r-1)}_{k_{r-1}}\big(\dots f^{(1)}_{k_1}(x)\dots\big)\big).$$

Note that throughout this work we assume that the round keys $k = (k_1, k_2, \dots, k_r)$ are random, independent, and uniformly distributed over the key space.

1.2. Differentials

Differential cryptanalysis, introduced by Biham and Shamir [1], is one of the most powerful and widely used techniques for analyzing the security of block ciphers, focusing on how differences in input pairs spread through the cipher to produce differences in the outputs.

Let $\circ, \bullet$ denote operations, each of which defines an abelian group structure on V_n with the neutral element being the zero vector.

The differential (ordinary) of a Boolean function f is a pair of arbitrary binary vectors (α, β). For the differential (α, β) we denote by the symbol $\alpha \xrightarrow{f} \beta$ (or simply $\alpha \to \beta$, if the function is clear from the context) the event

$$f(z \circ \alpha) = f(z) \bullet \beta,$$

which is induced by a random variable z.

The probability of the differential (α, β) of the function f is the value

$$DP^f(\alpha, \beta) = \mathrm{Pr}_z\{\alpha \xrightarrow{f} \beta\} = \\ = \frac{1}{2^q} \sum_{z \in V_q} [f(z \circ \alpha) = f(z) \bullet \beta].$$

Here, the notation [statement] denotes the *Iverson bracket*: [statement] $= 1$ if the statement is true, and [statement] $= 0$ otherwise.

We say that a differential is *impossible* if its probability equals zero. The differential $\alpha = \beta = 0$ is called *trivial*; its probability is clearly 1. All other differentials are called *nontrivial*.

For functions parameterized by a key, differentials are considered at each point separately. Accordingly, the notation $\alpha \xrightarrow{f_k, z} \beta$ denotes the event

$$f_k(z \circ \alpha) = f_k(z) \bullet \beta,$$

which is induced by a random key k and a fixed point z, or equivalently by a fixed key k and a random z.

The average over keys differential probability (α, β) of the function f_k at a point z is the value

$$DP^{f_k}(z; \alpha, \beta) = \mathrm{Pr}_{f_k, z}\{\alpha \to \beta\} = \\ = \frac{1}{|K|} \sum_{k \in K} [f_k(z \circ \alpha) = f_k(z) \bullet \beta].$$

The average differential probability (α, β) of the function f_k is the value

$$EDP^{f_k}(\alpha, \beta) = \mathrm{Pr}_{z,k}\{\alpha \xrightarrow{f_k} \beta\} \\ = \frac{1}{2^q} \sum_{z \in V_q} DP^{f_k}(z; \alpha, \beta).$$

For an iterative cipher E, we consider differentials with respect to a single operation $\oplus$; thus, the input–output differences of the transformations are computed via $\oplus$. Denote by $DP^{[r]}(z, \alpha, \beta)$ the probability of the r-round differential (α, β) at point z, where the differential function is

$$f_{k_r}^{(r)}(f_{k_{r-1}}^{(r-1)}(\ldots(f_{k_1}^{(1)}(x))\ldots)),$$

that is, the composition of the first r encryption rounds.

For a Markov cipher (with respect to $\oplus$) [15], we have $DP^{[r]}(z, \alpha, \beta) = DP^{[r]}(\alpha, \beta)$, which yields the equality [16]

$$DP^{[r]}(\alpha, \beta) = \sum_{\gamma} DP^{[r-1]}(\alpha, \gamma) \cdot DP^{[1]}(\gamma, \beta) \\ = \sum_{\gamma} DP^{[1]}(\alpha, \gamma) \cdot DP^{[r-1]}(\gamma, \beta).$$

For ciphers that are non-Markov with respect to $\oplus$, the following inequalities instead hold [7]:

$$DP^{[r]}(z; \alpha, \beta) \leq \\ \leq \sum_{\gamma} DP^{[r-1]}(z; \alpha, \gamma) \cdot \max_{y} DP^{[1]}(y; \gamma, \beta),$$

$$DP^{[r]}(z; \alpha, \beta) \leq \\ \leq \sum_{\gamma} DP^{[1]}(z; \alpha, \gamma) \cdot \max_{y} DP^{[r-1]}(y; \gamma, \beta).$$

As consequence, the security of a non-Markov cipher against differential cryptanalysis is measured by the value

$$MEDP(E) = \max_{\alpha \neq 0, \beta} EDP^{E}(\alpha, \beta).$$

However, in this section we derive security estimates defined by the value

$$MDP(E) = \max_{\alpha \neq 0, \beta, z} DP^{E}(z; \alpha, \beta).$$

Note that, due to the obvious inequality $MDP(E) \geq MEDP(E)$, these estimates are more stringent.

1.3. LBlock-like ciphers

LBlock is a lightweight block cipher introduced by Wenling Wu and Lei Zhang in 2011 [10], specifically designed for resource-constrained environments. The cipher has a Feistel structure and consists of 32 rounds. Each round applies the same operations to the block halves under a round key. The block size is 64 bits, while the key length is 80 bits.

Each round of LBlock is defined by the function f_i:

$$f_i((X_0, X_1)) = (X_1, \rho(X_0) \oplus F(X_1, K_i)),\quad i = 0, 1, \ldots, 31,$$

where i is the round number, K_i is the round key, X_0 and X_1 are the 32-bit left and right parts of the input, ρ is a cyclic left bit rotation, and F is the round function.

The round function F is defined as follows (Fig. 1):

$$F : \{0,1\}^{32} \times \{0,1\}^{32} \to \{0,1\}^{32},$$
$$F(X, K_i) = P(S(X \oplus K_i)).$$

The function S is the nonlinear layer of F and consists of eight 4×4 S-boxes. The function P is a fixed linear permutation applied to 4-bit words.

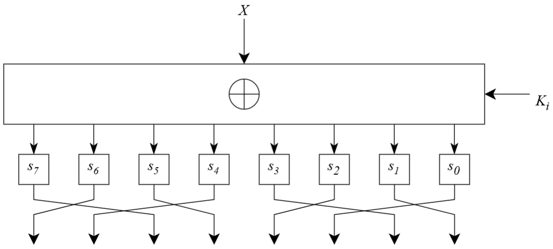

Figure 1: Internal round function F of LBlock

We define an LBlock-like cipher as a block cipher that follows the general design of the original LBlock cipher. In an LBlock-like cipher, the specific choice of S-boxes, the linear transformations (P and ρ), the number of rounds, and the block size are not fixed and may vary depending on the specific design.

2. Differential Probability Upper Bounds for LBlock

In this section, we introduce a baseline algorithm that constructs upper bounds based on approximations for active S-boxes, and then refine this approach by incorporating the actual probability distributions of differential transitions in S-boxes. The goal is to obtain more accurate and realistic estimates of the cipher's security against differential cryptanalysis.

2.1. Notation

Let $n = m \cdot u$. Then every $x \in V_n$ can be represented as

$$x = (x_1, x_2, \ldots, x_m), x_i \in V_u, i = 1, 2, \ldots, m$$

The main idea, proposed in [3], was to use so-called "templates" instead of the exact value of the difference between α and β. For any given vector $\alpha \in V_n$, we define its template $T\alpha = \hat{\alpha} \in V_m$ according to the following rule:

$$\hat{\alpha}_i = \begin{cases} 0, & \text{if } \alpha_i = 0 \\ 1, & \text{if } \alpha_i \neq 0 \end{cases} = [\alpha_i \neq 0].$$

Essentially, the template of the difference vector shows which S-blocks are active. Now we can introduce the set of all possible templates for the sum of the corresponding vectors:

$$\Phi(\hat{\alpha}, \hat{\beta}) = \{\hat{\varphi} \mid \exists \alpha, \beta \in V_n : T\alpha = \hat{\alpha},\ T\beta = \hat{\beta},\ T(\alpha \oplus \beta) = \hat{\varphi}\}.$$

Since the size of the input and output of a round transformation is $2n$ bits, it is necessary to analyze $2m$-bit templates, which are divided into two m-bit parts. Thus, a template $\hat{\alpha} = (\hat{\alpha}_x, \hat{\alpha}_y)$, where $\hat{\alpha}_x, \hat{\alpha}_y \in V_m$, corresponds to a vector $\alpha = (\alpha_x, \alpha_y)$, where $\alpha_x, \alpha_y \in V_n$.

2.2. Algorithm for Constructing Differential Probability Upper Bounds

In this subsection, we introduce a baseline algorithm for constructing security bounds for the LBlock-like cipher against differential cryptanalysis. The method is based on using an upper bound approximation of differential probabilities for active S-boxes, which provides a general estimate of cipher security. Although this approach offers a straightforward way to derive upper bounds, it does not yet account for the actual statistical distribution of differential probabilities.

Consider two rounds of the LBlock-like cipher (Fig. 2). In this case, a generalized transformation ρ was introduced, which in the original LBlock corresponds to a cyclic left shift by 8 bits ($\lll 8$).

Let us analyze the structure of a differential for two rounds of an LBlock-like cipher. Each differential (α, β) corresponds to one and only one differential characteristic $\Omega = ((\alpha_x, \alpha_y), (\alpha_y, \beta_x), (\beta_x, \beta_y))$. Therefore, the differential has a nonzero probability only if

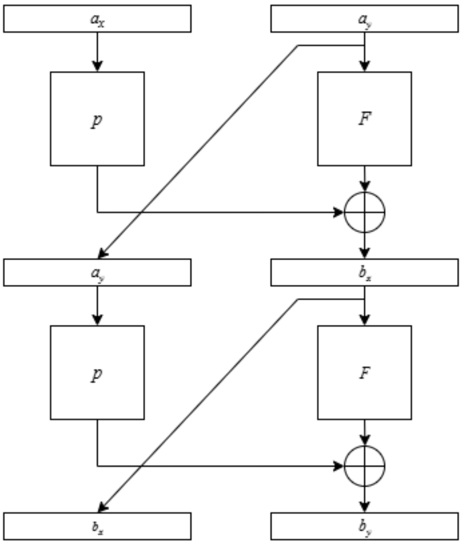

Figure 2: The structure of differentials of two rounds of the LBlock-like cipher

the corresponding round transitions occur according to the differential characteristic:

$$Pr\{\Omega\} \neq 0 \Leftrightarrow \begin{cases} \beta_x = \rho(\alpha_x) \oplus f(\alpha_y), \\ \beta_y = \rho(\alpha_y) \oplus f(\beta_x). \end{cases}$$

We can express this as a condition on the templates of the output difference of the differential:

$$\big(\hat{\beta}_x \in \Phi(\rho(\hat{\alpha}_x), P(\hat{\alpha}_y))\big) \\ \& \ \big(\hat{\beta}_y \in \Phi(\rho(\hat{\alpha}_y), P(\hat{\beta}_x))\big).$$

If this condition fails, then the probability of the characteristic is 0, and hence the probability of the differential is also 0. If the condition passes, we can estimate the probability of the differential by an inequality:

$$DP^{[2]}((x,y);\alpha,\beta) \leq DP^f\big(y;\alpha_y,\rho(\alpha_x)\oplus\beta_x\big) \\ \cdot \max_z DP^f\big(z;\beta_x,\rho(\alpha_y)\oplus\beta_y\big).$$

To lift this inequality to the level of templates, it can be reduced to estimating the number of active S-boxes in each round. Under these conditions, for the second round of the LBlock cipher, the upper-bound matrix can be constructed by formula (2).

Next, it is necessary to consider the r-round differential of LBlock (Fig. 3). For the probability of the r-round differential (α,β) at point z, the following statement holds:

$$DP^{[r]}(z;\alpha,\beta) \leq \max_{\hat{\gamma}} UB^{[r-1]}(\hat{\gamma},\hat{\beta}).$$

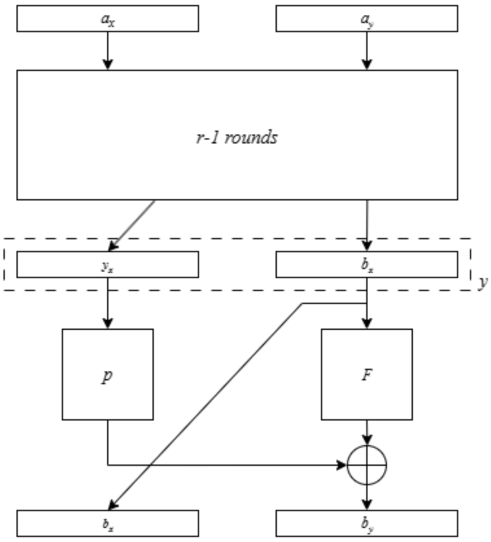

Figure 3: The structure of differentials of r-rounds of the LBlock-like cipher

Since this rule applies to any iterative block cipher, one can also use the value

$$M = \max_{\hat{\gamma}} UB^{[r-1]}(\hat{\gamma},\hat{\beta})$$

to bound $UB^{[r]}(\hat{\alpha},\hat{\beta})$ in LBlock.

Assuming that $\beta_x = 0$ in the scheme of Fig. 3, we can derive the following formula:

$$UB^{[r]}(\hat{\alpha},(0,\hat{\beta}_y)) = UB^{[r-1]}(\hat{\alpha},(\rho^{-1}(\hat{\beta}_y),0)).$$

In the case when $\beta_x \neq 0$, for the probability of the r-round differential we can derive the following inequality:

$$DP^{[r]}((x,y);\alpha,\beta) \leq \\ \leq \sum_{\gamma} DP^{[r-1]}((x,y);\alpha,(\gamma,\beta_x))\times \\ \times \max_z DP^F(z;(\gamma,\beta_x),(\beta_x,\beta_y)).$$

Express the sum over γ on the right-hand side of the inequality as a sum over templates $\hat{\gamma}$, we obtain:

$$DP^{[r]}((x,y);\alpha,\beta) \leq \\ \leq \sum_{\hat{\gamma}} \sum_{\gamma:\, T\gamma=\hat{\gamma}} DP^{[r-1]}((x,y);\alpha,(\gamma,\beta_x))\times \\ \times \max_z DP^F(z;(\gamma,\beta_x),(\beta_x,\beta_y)).$$

First, we can derive the following estimate:

$$DP^{[r-1]}((x,y);\alpha,(\gamma,\beta_x)) \leq \\ \leq UB^{[r-1]}(\hat{\alpha},(\hat{\gamma},\hat{\beta}_x)).$$

The expression on the right-hand side of the inequality does not depend on the parameter γ, so we can move it outside the first sum over $\gamma : T\gamma = \hat{\gamma}$. We obtain:

$$DP^{[r]}((x,y);\alpha,\beta) \leq$$
$$\leq \sum_{\hat{\gamma}} UB^{[r-1]}(\hat{\alpha},(\hat{\gamma},\hat{\beta}_x))\times$$
$$\times \sum_{\gamma:T\gamma=\hat{\gamma}} \max_z DP^F(z;(\gamma,\beta_x),(\beta_x,\beta_y)).$$

From the scheme in Fig. 3 we know that $\rho(\gamma) \oplus P(\beta_x)$ must map to β_y. That is, if

$$\hat{\beta}_y \notin \Phi(\rho(\hat{\gamma}), P(\hat{\beta}_x)), \qquad (1)$$

then

$$\max_z DP^F(z;(\gamma,\beta_x),(\beta_x,\beta_y)) = 0,$$

since the template $\hat{\beta}_y$ cannot transit to the required output.

From these considerations, it follows that instead of summing over all values of $\hat{\gamma}$, we only need to consider those that satisfy condition (1). Thus, the upper-bound matrix can be constructed as follows:

$$DP^{[r]}((x,y);\hat{\alpha},\hat{\beta}) =$$
$$= \sum_{\hat{\gamma}:\rho(\hat{\gamma})\in\Phi(\hat{\beta}_y,P(\hat{\beta}_x))} UB^{[r-1]}(\hat{\alpha},(\hat{\gamma},\hat{\beta}_x))\times$$
$$\times \sum_{\gamma:T\gamma=\hat{\gamma}} \max_z DP^F(z;(\gamma,\beta_x),(\beta_x,\beta_y)).$$

It is important to note that in the sum

$$\sum_{\gamma:T\gamma=\hat{\gamma}} \max_z DP^F(z;(\gamma,\beta_x),(\beta_x,\beta_y)),$$

the boundary $\gamma : T\gamma = \hat{\gamma}$ must also satisfy condition (1) within the framework of working with the template γ.

The expression

$$\max_z DP^F(z,(\gamma,\beta_x),(\beta_x,\beta_y))$$

can be bounded by the number of active S-boxes, which by construction of LBlock-like cip equals

$$p^{wt(\hat{\beta}_x)} \quad \text{(see Fig. 3).}$$

Furthermore, the sum over $\gamma : T\gamma = \hat{\gamma}$ can be removed by replacing it with $(2^u - 1)^{wt(\hat{\gamma})}$. It is the number of nonzero differences γ which corresponds to the template $\hat{\gamma}$.

Thus, we can derive the final formula for the case $\beta_x \neq 0$, which does not include the use of distribution bounds of differential probabilities of S-boxes (3).

Algorithm 1. ***Computation of upper bounds of LBlock differential probability without using distribution bounds of differential probabilities of S-boxes.***

```
Input:
  • LBlock cipher scheme,
  • number of rounds $r$.
Output: Upper-bound matrix $UB^{[r]}(*,*)$.
Precomputation:
  • system of sets $\Phi[*,*]$,
  • number $p = \max_i MDP(s_i)$.
1) For all templates $(\hat{\alpha},\hat{\beta})$, calculate $UB^{[2]}(\hat{\alpha},\hat{\beta})$ according to (2)
2) For $t = 3,4,\ldots,r$, do:
    2.1. For all templates $\hat{\beta} = (0,\hat{\beta}_y)$, set
           $UB^{[t]}(\hat{\alpha},(0,\hat{\beta}_y)) =$
               $= UB^{[t-1]}(\hat{\alpha},(\rho^{-1}(\hat{\beta}_y),0))$
    2.2. For all templates $\hat{\beta} = (\hat{\beta}_x,\hat{\beta}_y)$, where $\hat{\beta}_x \neq 0$, calculate $UB^{[t]}(\hat{\alpha},\hat{\beta})$ according to formula (3).
3) Return matrix $UB^{[r]}$.
```

It is important to note that Algorithm 1 is not the best option for deriving specific estimates. The next logical step is to formulate a similar algorithm that uses the bounds of the distributions of differential probabilities of the S-boxes.

2.3. Refined Algorithm of Constructing Differential Probabilities Upper Bounds

In this subsection, we present a refined methodology for computing probability distribution bounds of active S-boxes within differential cryptanalysis. This approach was proposed by Serhii Yakovliev and it is based on ideas of Liam Keliher [6]. Unlike the previous approach, which relied on a single upper bound approximation $p^{(\cdots)}$, the proposed method makes use of the actual statistical distribution of differential probabilities for each S-box. This allows for more accurate and realistic estimates when analyzing combinations of active S-boxes.

Let $u_i(A)$, $A = \overline{1,m}$, be the sequences of upper bounds on the nonzero differential probabilities of combinations of A active S-boxes, sorted in descending order: $u_1(A) \geq u_2(A) \geq \ldots.$

These sequences are computed as the A-fold convolution of sorted distributions of differential probabilities of active S-boxes.

The process begins with constructing the basic distribution for a single active S-box. Fix some $\alpha \in V_u$ and consider all $\beta \in V_u$. We enumerate the vectors $\beta \neq 0$ such that the sequence $DP^f_{*,i}(\alpha, \beta_i)$ is non-increasing:

$$DP^f_{*,1} \geq DP^f_{*,2} \geq \dots .$$

Then $u_1(1) = p = \max\limits_{\alpha \neq 0} DP^f_{\alpha,1}$. The sequence $u_i(1)$ is sorted in non-increasing order.

The sequences $u_i(A)$ are then computed inductively as follows:

1) Compute the convolution of sequences:
$$(v_i(A)) = (u_i(A-1)) \otimes (u_i(1)).$$
2) The sequence $(u_i(A))$ is the sorted version of $(v_i(A))$.

For convenience, the sequence $u_i(A)$ can be stored as a list of pairs

$$\{(p_j(A), N_j(A))\},$$

where $p_j(A)$ are the distinct probability values in $u_i(A)$ (assumed ordered $p_1(A) > p_2(A) > \dots$) and $N_j(A)$ are the multiplicities of $p_j(A)$ in $u_i(A)$.

Then the convolution $(u_i(A-1)) \otimes (u_i(1))$ can be computed as follows:

1) Compute all possible product values $p_l(A-1) \cdot p_t(1)$.
2) Keep only unique product values and sort them into the sequence $p_j(A)$ in descending order.
3) For each resulting value $p_j(A)$, compute its multiplicity:
$$N_j(A) = \sum_{l,t} N_l(A-1) \cdot N_t(1),$$
where the sum is taken over all pairs (l, t) such that $p_j(A) = p_l(A-1)\, p_t(1)$.

The computational complexity of constructing the sequences $u_i(A)$ is relatively low. However, even for comparatively small values of A, it is necessary to track rounding and overflow errors that may occur due to very small initial differential probability values of individual S-boxes.

Thus, we obtain an effective method for constructing the exact probability distribution for combinations of active S-boxes, which allows us to evaluate transition probabilities with high accuracy and to use these estimates in the upper-bounds differential probability calculations.

If the sequences $u_i(A)$ are known, we can formulate a more precise algorithm for computing upper bounds. Only one step of the algorithm is modified. Consider the r-round differential of LBlock (Fig. 3), specifically the case when $\beta_x \neq 0$.

Now, the term

$$\sum_{\gamma : T\gamma = \hat{\gamma}} \max_z DP^F(z; (\gamma, \beta_x), (\beta_x, \beta_y))$$

can be bounded as

$$\leq \sum_{i=0}^{(2^u-1)^{wt(\hat{\gamma})}} u_i(wt(\hat{\beta}_x)).$$

Accordingly, the final formula for the case $\beta_x \neq 0$, which incorporates the distribution bounds of differential probabilities of S-boxes, is given by formula (4).

Algorithm 2. ***Computation of upper bounds of LBlock differential probability using the probability distributions of S-boxes.***

```
Input:
  • LBlock cipher scheme,
  • number of rounds $r$.
Output: Upper-bound matrix $UB^{[r]}(*,*)$.
Precomputation:
  • System of sets $\Phi[*,*]$,
  • distributions $u_i(A)$   $(A = 1, \dots, m)$.
1) For all templates $(\hat{\alpha}, \hat{\beta})$, calculate $UB^{[2]}(\hat{\alpha}, \hat{\beta})$ according to (2).
2) For $t = 3, 4, \dots, r$, do:
    2.1. For all templates $\hat{\beta} = (0, \hat{\beta}_y)$, set
         $UB^{[t]}(\hat{\alpha},(0, \hat{\beta}_y)) = UB^{[t-1]}(\hat{\alpha}, (\rho^{-1}(\hat{\beta}_y), 0))$.
    2.2. For all templates $\hat{\beta} = (\hat{\beta}_x, \hat{\beta}_y)$, where $\hat{\beta}_x \neq 0$, set $UB^{[t]}(\hat{\alpha}, \hat{\beta})$ according to formula (4).
3) Return matrix $UB^{[r]}$.
```

3. Experimental Results

In this section, we experimentally verify the proposed method for estimating the security against differential cryptanalysis of a modified version of the LBlock cipher. The experiments focus on analyzing the influence of different permutations P and ρ on the upper bounds of dif-

$$UB^{[2]}(\hat{\alpha},\hat{\beta}) = \begin{cases} p^{wt(\hat{\alpha}_y)+wt(\hat{\beta}_x)}, & \big(\hat{\beta}_x \in \Phi(\rho(\hat{\alpha}_x), P(\hat{\alpha}_y)) \ \ \& \ \ \hat{\beta}_y \in \Phi(\rho(\hat{\alpha}_y), P(\hat{\beta}_x))\big), \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

$$UB^{[r]}(\hat{\alpha},\hat{\beta}) = \min \begin{cases} \max_{\hat{\gamma}} UB^{[r-1]}(\hat{\gamma},\hat{\beta}), \\ \sum\limits_{\hat{\gamma}:\rho(\hat{\gamma})\in\Phi(\hat{\beta}_y, P(\hat{\beta}_x))} UB^{[r-1]}(\hat{\alpha},(\hat{\gamma},\hat{\beta}_x)) \cdot p^{wt(\hat{\beta}_x)} \cdot (2^u-1)^{wt(\hat{\gamma})}. \end{cases} \tag{3}$$

$$UB^{[r]}(\hat{\alpha},\hat{\beta}) = \min \begin{cases} \max_{\hat{\gamma}} UB^{[r-1]}(\hat{\gamma},\hat{\beta}), \\ \sum\limits_{\hat{\gamma}:\rho(\hat{\gamma})\in\Phi(\hat{\beta}_y, P(\hat{\beta}_x))} UB^{[r-1]}(\hat{\alpha},(\hat{\gamma},\hat{\beta}_x)) \cdot \sum\limits_{i=0}^{(2^u-1)^{wt(\hat{\gamma})}} u_i(wt(\hat{\beta}_x)). \end{cases} \tag{4}$$

ferential probabilities, as well as on comparing the baseline algorithm with its enhanced version.

3.1. Experiment setup

Applying the algorithms to the original LBlock cipher would require constructing a matrix of size $2^{16} \times 2^{16}$ at each round, which leads to computational difficulties on our environment. Therefore, the performance of the modified algorithm is first demonstrated on a simplified version of the LBlock cipher.

Mainly, round function F was modified (Fig. 4. Instead of eight 4×4 S-boxes, only four 8×8 S-boxes are used, while still producing a 32-bit output, as in the standard LBlock cipher. Under these conditions, the value of the parameter

$$p = \max_i MDP(s_i)$$

changes slightly. Since the content of s_i is not essential for the proposed algorithm, the S-box was borrowed from AES [17]. Consequently, the parameter p is equal to $\frac{4}{256}$ (2^{-6}) instead of the usual $\frac{1}{4}$ (2^{-2}) for the original LBlock S-boxes.

The experiment is focused on evaluating different combinations of the linear permutation P and the function ρ (originally defined as a cyclic left shift by 8 bits). All 4-bit permutations were considered, and for each pair (ρ, P) the Algorithm 1 and Algorithm 2 were executed with 10 and 24 rounds of LBlock.

3.2. Analysis of Algorithm 1 Outcomes

After 10 rounds of the Algorithm 1, four distinct patterns of security estimates behavior were identified. The classification results are summarized in Table 1: the first class includes 24 permutation pairs, the second — 57, the third — 372, and the fourth — 123.

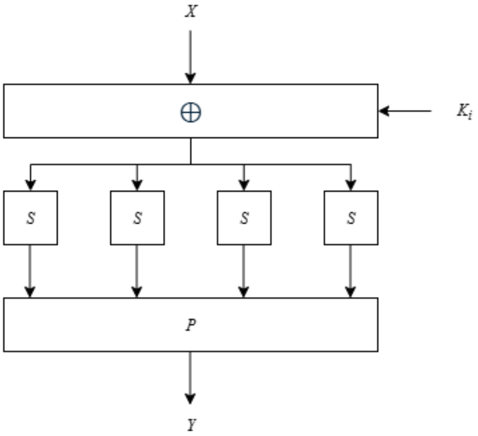

Figure 4: Round function F of the modified LBlock

Table 1
Algorithm 1 Maximum UB Estimates per Class across Rounds

Round	Class 1	Class 2	Class 3	Class 4
2	2^{-6}	2^{-6}	2^{-6}	2^{-6}
3	2^{-12}	2^{-12}	2^{-8}	2^{-6}
4	$\approx 2^{-12.02}$	2^{-12}	2^{-8}	2^{-6}
5	$\approx 2^{-12.02}$	2^{-12}	2^{-8}	2^{-6}
6	$\approx 2^{-12.02}$	2^{-12}	2^{-8}	2^{-6}
7	$\approx 2^{-12.02}$	2^{-12}	2^{-8}	2^{-6}
8	$\approx 2^{-12.02}$	2^{-12}	2^{-8}	2^{-6}
9	$\approx 2^{-12.02}$	2^{-12}	2^{-8}	2^{-6}
10	$\approx 2^{-12.02}$	2^{-12}	2^{-8}	2^{-6}

The best combinations belong to the first class, as they yield the lowest maximum estimates. In general, the results show a tendency toward a “plateau” effect (no further improvement of the estimates), which typically occurs within the first three rounds. Examples of permutations corresponding to each class are shown in Table 2.

Table 2
Class 1 Permutations found by Algorithm 1

ρ	1032	1032	1032	1032	1230	1230	1302	1302	2031	2031	2301	2301
P	2301	2310	3201	3210	2301	3012	2031	3210	1302	3210	1032	1230

ρ	2301	2301	2310	2310	3012	3012	3201	3201	3210	3210	3210	3210
P	3012	3210	1032	3201	1230	2301	1032	2310	1032	1302	2031	2301

Observations of the maximum upper bounds for first class differentials show that, starting from round three, the estimate stabilizes at approximately $2^{-12.02}$, which is the lowest among all four classes. This behavior indicates that high-probability differentials decay rapidly, i.e., the cipher exhibits effective diffusion already at early rounds. At this stage we regard permutations from this class as yielding the most secure modifications of the cipher against differential cryptanalysis. Therefore, the results for the first class can be used as guidelines when designing the experimental study for the original LBlock cipher.

3.3. Analysis of Algorithm 2 Outcomes

After 24 rounds of the Algorithm 2, 26 distinct patterns of security estimates were identified. The increased number of rounds was chosen to observe whether the estimates converge to a "plateau", as in the Algorithm 1. However, such stabilization was not observed for all classes.

Compared to the Algorithm 1, the increase in the number of patterns is expected, since the Algorithm 2 is more accurate and does not rely on rough approximations. The previously defined four classes split into smaller subclasses, while some merged into larger ones. For instance, Class 1 of the Algorithm 1 corresponds to several smaller classes (2, 3, 4, 5, 7), while Class 4 corresponds to a single new class (26). Overall, the classification became finer, reflecting a more precise differentiation of permutation pairs.

For the combinations of first class of the results of the Algorithm 1, which was further split into five subclasses by the Algorithm 2, the Algorithm 2 provided significantly more precise estimates. Instead of the previous value of about $2^{-12.02}$, the results yielded much smaller bounds, ranging between 2^{-18} and $2^{-44.74}$. Importantly, improvements such as 2^{-18} were already visible by the third round, whereas in the Algorithm 1 a plateau effect appeared at this stage.

These findings highlight a fundamental difference between the two approaches, observable even in the early rounds. While some subclasses stabilize quickly (e.g., Class 7 at 2^{-18}, Class 4 at 2^{-24}), others with lower estimates (such as Classes 2, 3, 5, 7) display a more chaotic but generally decreasing trend. In the long term, after 24 rounds, these classes continue to improve, with the best estimates reaching approximately 2^{-40}. This value can be regarded as a benchmark for assessing the eventual "success rate" of differentials under the refined analysis.

For the Algorithm 2, the most favorable permutation combinations belong to Classes 2, 3, 5, 14, 22, and 23, since they yield the lowest maximum estimates ($< 2^{-40}$). Table 3 list the permutation pairs forming these classes. Notably, in Class 14 the permutation P turned out to be fixed (identity), while in Class 22 both ρ and P were identical. A graphical comparison of the estimates for the proposed pairs is shown in Fig. 5.

Table 3
Best Classes found by Algorithm 2

Class							
2	ρ	1302	2031	3012			
	P	2031	1302	1230			
3	ρ	1230	2310	3201			
	P	3012	3201	2310			
5	ρ	1230	1302	2031	2310	3012	3201
	P	2301	3210	3210	1032	2301	1032
14	ρ	1230	1302	2031	2310	3012	3201
	P	0123	0123	0123	0123	0123	0123
22-23	ρ	1230	1302	2031	3012	3201	0123
	P	1230	1302	2031	3012	3201	1230

Conclusions

In this work we proposed and analyzed methods for upper-bounding differential probabilities in LBlock and its modifications. Two algorithms were presented. The first one provides baseline estimates based on simplified assumptions about

Table 4
Algorithm 2 Maximum UB Estimations of Best Classes across Rounds

Round	Class 2	Class 3	Class 5	Class 14	Class 22	Class 23
2	$2^{-6.00}$	$2^{-6.00}$	$2^{-6.0}$	$2^{-6.00}$	$2^{-6.00}$	$2^{-6.00}$
3	$2^{-12.00}$	$2^{-12.00}$	$2^{-12.00}$	$2^{-12.00}$	$2^{-12.00}$	$2^{-12.00}$
4	$2^{-18.00}$	$2^{-18.00}$	$2^{-18.00}$	$2^{-13.00}$	$2^{-12.00}$	$2^{-12.00}$
5	$2^{-24.00}$	$2^{-24.00}$	$2^{-23.94}$	$2^{-18.00}$	$2^{-18.00}$	$2^{-18.00}$
6	$2^{-24.00}$	$2^{-24.00}$	$2^{-24.00}$	$2^{-19.01}$	$2^{-18.00}$	$2^{-18.00}$
7	$2^{-26.0}$	$2^{-26.00}$	$2^{-24.00}$	$2^{-24.00}$	$2^{-23.98}$	$2^{-23.98}$
8	$2^{-27.40}$	$2^{-27.40}$	$2^{-24.00}$	$2^{-24.00}$	$2^{-23.98}$	$2^{-23.98}$
9	$2^{-30.00}$	$2^{-30.00}$	$2^{-26.78}$	$2^{-24.00}$	$2^{-24.00}$	$2^{-24.00}$
10	$2^{-30.00}$	$2^{-30.00}$	$2^{-27.40}$	$2^{-24.01}$	$2^{-29.98}$	$2^{-29.98}$
11	$2^{-31.00}$	$2^{-31.00}$	$2^{-30.00}$	$2^{-30.00}$	$2^{-29.98}$	$2^{-29.98}$
12	$2^{-35.51}$	$2^{-35.51}$	$2^{-30.00}$	$2^{-30.00}$	$2^{-30.00}$	$2^{-30.00}$
13	$2^{-35.69}$	$2^{-35.69}$	$2^{-31.71}$	$2^{-30.00}$	$2^{-30.00}$	$2^{-30.00}$
14	$2^{-35.91}$	$2^{-35.91}$	$2^{-33.26}$	$2^{-33.94}$	$2^{-35.01}$	$2^{-35.01}$
15	$2^{-35.92}$	$2^{-35.92}$	$2^{-35.68}$	$2^{-34.40}$	$2^{-36.41}$	$2^{-36.41}$
16	$2^{-35.97}$	$2^{-35.97}$	$2^{-35.97}$	$2^{-34.91}$	$2^{-36.80}$	$2^{-36.80}$
17	$2^{-37.83}$	$2^{-37.83}$	$2^{-36.00}$	$2^{-34.97}$	$2^{-37.98}$	$2^{-37.98}$
18	$2^{-38.87}$	$2^{-38.87}$	$2^{-37.68}$	$2^{-35.70}$	$2^{-38.20}$	$2^{-38.20}$
19	$2^{-39.25}$	$2^{-39.25}$	$2^{-39.21}$	$2^{-35.83}$	$2^{-38.29}$	$2^{-38.29}$
20	$2^{-41.61}$	$2^{-41.61}$	$2^{-41.40}$	$2^{-35.90}$	$2^{-39.08}$	$2^{-39.08}$
21	$2^{-42.53}$	$2^{-42.53}$	$2^{-42.36}$	$2^{-38.91}$	$2^{-39.17}$	$2^{-39.17}$
22	$2^{-43.83}$	$2^{-43.83}$	$2^{-43.60}$	$2^{-40.55}$	$2^{-39.24}$	$2^{-39.24}$
23	$2^{-44.54}$	$2^{-44.54}$	$2^{-43.81}$	$2^{-40.75}$	$2^{-43.01}$	$2^{-43.01}$
24	$2^{-44.74}$	$2^{-44.74}$	$2^{-44.44}$	$2^{-41.57}$	$2^{-43.44}$	$2^{-43.44}$

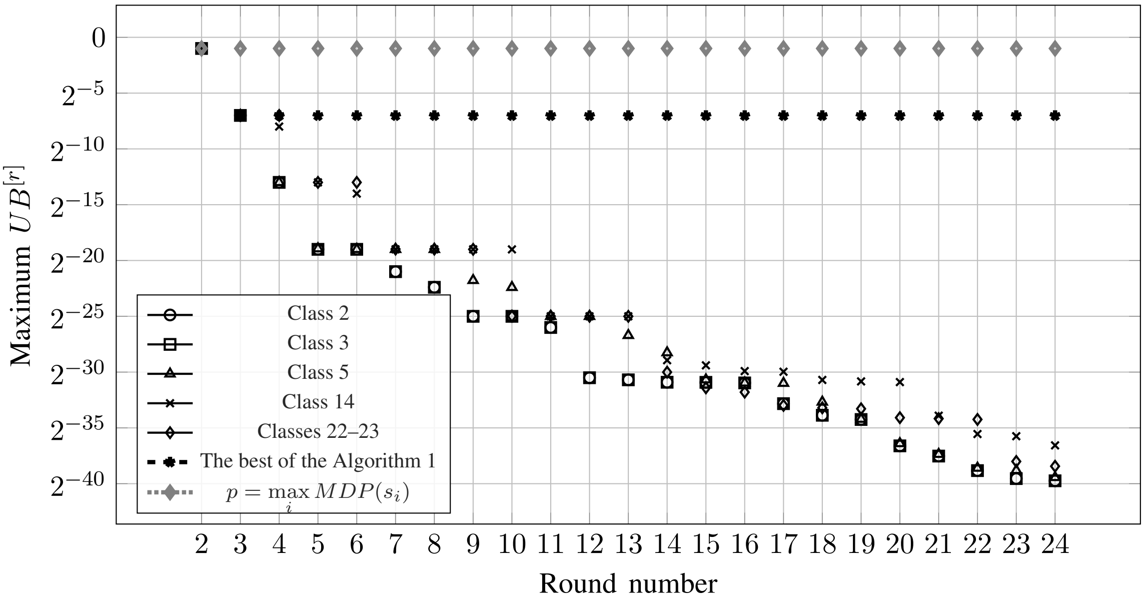

Figure 5: Algorithm 2 Maximum UB Estimates of Best-performing Classes across Rounds

active S-boxes, while the second algorithm refines the estimates by incorporating the actual probability distributions of differential transitions in the S-boxes. This refinement significantly improves the bounds and removes redundant approximations.

To illustrate the efficiency of proposed algorithms, a modified version of LBlock was introduced, where eight 4×4 S-boxes were replaced with four 8×8 S-boxes. This modification reduced computational complexity and enabled experiments with different round permutations. The results demonstrated that the refined algorithm achieves notably smaller maximum bounds (less than 2^{-40} in the best cases), clearly outperforming the baseline approach. Moreover, the experiments revealed classes of permutation pairs that provide better diffusion and stronger security against differential cryptanalysis.

Overall, the results confirm that the proposed convolution-based approach yields more accurate estimates of security against differential cryptanalysis for LBlock-like ciphers. These results can support the design of secure lightweight ciphers and further analysis of LBlock's provable security against differential cryptanalysis.

Acknowledgments

We sincerely thank Serhii Yakovliev for his invaluable feedback and guidance, which greatly influenced the direction and quality of this work.

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," Journal of Cryptology, vol. 4, pp. 3–72, 1991. https://doi.org/10.1007/BF00630563.

[2] K. Nyberg and L. R. Knudsen, "Provable Security Against Differential Cryptanalysis," in Advances in Cryptology — CRYPTO' 92, (Berlin, Heidelberg), pp. 566–574, Springer Berlin Heidelberg, 1993.

[3] L. Keliher, H. Meijer, and S. Tavares, "New Method for Upper Bounding the Maximum Average Linear Hull Probability for SPNs," in Advances in Cryptology – EUROCRYPT 2001, 06 2001.

[4] L. Keliher, H. Meijer, and S. Tavares, "Completion of Computation of Improved Upper Bound on the Maximum Average Linear Hull Probabilty for Rijndael," IACR Cryptology ePrint Archive, vol. 2004, p. 74, 04 2004.

[5] L. Keliher, "Refined Analysis of Bounds Related to Linear and Differential Cryptanalysis for the AES," in Advanced Encryption Standard – AES, (Berlin, Heidelberg), pp. 42–57, Springer Berlin Heidelberg, 2005.

[6] L. Keliher, "Toward Provable Security Against Differential and Linear Cryptanalysis for Camellia and Related Ciphers," International Journal of Network Security, vol. 5, 01 2007.

[7] L. Kovalchuk and A. Alexeychuk, "Towards a Theory of Security Evaluation for GOST-like Ciphers against Differential and Linear Cryptanalysis," in Cryptology ePrint Archive, 2011. https://eprint.iacr.org/2011/489.

[8] "Information processing systems. Cryptographic protection. Algorithm for cryptographic transformation: DSTU GOST 28147:2009." State Service of Ukraine on Food Safety and Consumer Protection, 2008. 28 p. [in Ukrainian].

[9] S. Yakovliev, Y. Dobronohov, and O. Yakymchuk, "A Method of Security Evaluation of Non-Markov Feistel Networks against Differential Cryptanalysis," in Proceedings of the 2024 IEEE 5th International Conference on Advanced Trends in Information Theory (ATIT), (Lviv, Ukraine), IEEE and IEEE Ukraine Section, 2024.

[10] W. Wu and L. Zhang, "LBlock: A lightweight block cipher *." Cryptology ePrint Archive, Paper 2011/345, 2011.

[11] M. Minier and M. Naya-Plasencia, "A related key impossible differential attack against 22 rounds of the lightweight block cipher LBlock," Information Processing Letters, vol. 112, no. 16, pp. 624–629, 2012.

[12] J. Chen and A. Miyaji, "Differential Cryptanalysis and Boomerang Cryptanalysis of LBlock," in Security Engineering and Intelligence Informatics, (Berlin, Heidelberg), pp. 1–15, Springer Berlin Heidelberg, 2013.

[13] J. Shi, G. Liu, C. Li, and T. Fan, "Improved (related-key) differential cryptanalysis on LBlock," Journal of Information Security and Applications, vol. 82, 2024.

[14] M. Lopatetskyi and O. Yakymchuk, "Security Evaluation of the LBlock Cipher Modification against Differential Cryptanalysis," in Theoretical and Applied Problems of Physics, Mathematics and Computer Science, (Kyiv, Ukraine), pp. 447–450, Igor Sikorsky Kyiv Polytechnic Institute, 2025.

[15] X. Lai, J. L. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," in Advances in Cryptology — EUROCRYPT '91, pp. 17–38, Springer Berlin Heidelberg, 1991.

[16] S. Vaudenay, "On the Security of CS-Cipher," in Fast Software Encryption, pp. 260–274, Springer Berlin Heidelberg, 1999.

[17] J. Daemen and V. Rijmen, "Advanced encryption standard," Tech. Rep. FIPS PUB 197, National Institute of Standards and Technology, 2001.