UDC 003.26.09

Application of Ternary Pattern-based Truncated Differential Cryptanalysis to Specific Block Ciphers

Oleksii Yakymchuk, Kostiantyn Medvedtskyi[1]

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

Abstract

In the previous work [1], we proposed a formalized approach to truncated differential cryptanalysis based on ternary masks which separately consider unchanged, obligatory changed and unknown bits in differences. A security parameter for S-boxes and encryption mappings that bounds the probability of truncated differentials from below was also proposed in the previous paper. The subsequent step involves applying the proposed method to existing real-world ciphers, calculating the defined security parameter, and assessing the method's effectiveness and potential applications. Additionally, this paper extends the applicability of the proposed approach by formalizing the XOR operation rules for ternary masks. This allows us to apply the proposed method to ciphers with a structure of Feistel network.

Keywords: differential cryptanalysis, truncated differentials, truncated differential characteristic

Introduction

Truncated differential cryptanalysis, first proposed by Knudsen [2] in 1994, is a generalization of differential cryptanalysis. Truncated differential cryptanalysis considers differences between texts which are only partially determined. The successful attack on 6 rounds of DES cipher using truncated differential cryptanalysis was described in [2] by Knudsen. There exists a variety of works that describe application of truncated differential cryptanalysis to existing ciphers, such as SAFER [3], KATAN-32 [4], PRINCE [5], Skinny-64 [6] and others. In general, to date, this metodology has proved its efficiency against word-oriented ciphers, like byte-wise SP-networks or generalized Feistel networks. For word-oriented ciphers, it is common practice to use templates of two types of words: unchanged and somehow changed [7, 8]. A formal approach to truncated differential cryptanalysis was proposed in [9] and then expanded in [10] and [1]. It is a template-based approach for truncated differential cryptanalysis that can be applied to bit-oriented block ciphers in the first place. This approach is applicable on bit level and specifies truncated differentials with ternary masks which consider unchanged, obligatory changed, and unknown bits. There was proposed the security parameter that shows lower bound of the probability of truncated differentials.

In this work, we explore the applicability of the previously proposed approach to existing lightweight ciphers. We examine the applicability of known methods of differential search to proposed approach of truncated differential construction. We define the rules of XOR operation for ternary masks which expand the applicability of the approach to a wider set of ciphers, for example, Feistel networks. As practical examples, we construct high-probability truncated differential characteristics for ciphers PRESENT [11] and LBlock [12].

The paper is organized as follows. Section 1 provides a standard notation and a brief description of proposed approach to truncated differential cryptanalysis. In section 2.1, we examine the applicability of branch-and-bound method to constructing truncated differentials according to considered approach. In sections 2.2, 2.3, and 2.4 we construct truncated differential characteristics for PRESENT cipher. Section 3.1 provides the rules of operation XOR for ternary masks. Finally, in section 3.2 we construct truncated differential characteristics for LBlock cipher.

1. Main terms and notations

1.1. Basics

An *encryption function* f is a function

$$f : \mathcal{M} \times \mathcal{K} \to \mathcal{C},$$

where $\mathcal{M}$ — set of plain texts, $\mathcal{K}$ — set of keys, $\mathcal{C}$ — set of cipher texts, and for all $k \in \mathcal{K}$ function f_k is bijective. The index k means specific value $k \in \mathcal{K}$.

Consider a composition of r encryption transformation functions f one by one using different keys as a new function $\mathcal{M} \times \mathcal{K}^r \to \mathcal{C}$. This transformation could be presented as sequence of encryption functions $f_{k_r}(\dots f_{k_2}(f_{k_1}(x)))$, $x \in \mathcal{M}$ and we will call it *multi-round encryption transformation.*

Let $V_n = \{0,1\}^n$ be a linear space of all n-length binary vectors. We consider sets $\mathcal{M}$ and $\mathcal{C}$ as linear space of n-length binary vectors, so $\mathcal{M} = \mathcal{C} = V_n$, and set $\mathcal{K}$ as linear space of m-length binary vectors, $\mathcal{K} = V_m$. And we consider encryption functions f as Boolean functions.

To abbreviate the notation of an n-bit vector with a large number of identical bits, we use the notation 0^r to denote a sequence of r zeros, and 1^r — sequence of r ones, for arbitrary $r \geq 1$. For example, $0^3 1^2 0 1^2$ denotes the vector 00011011.

1.2. Differentials

A *differential* of Boolean function f_k is an arbitrary pair of vectors (α, β), $\alpha, \beta \in B_n$, which are interpreted as difference between inputs and as difference between outputs of function f_k with respect to bitwise addition $\oplus$. The equation associated with differential (α, β) for a function f_k is $f_k(z \oplus \alpha) = f_k(z) \oplus \beta$.

Differential characteristic of multi-round transformation is sequence of n-length binary vectors $(\alpha_0, \alpha_1, \dots, \alpha_r)$, $\alpha_i \in V_n$, $i = 0, \dots, r$. This sequence we consider as sequence of differences between intermediate cipher texts of multi-round transformation after each round. So, every intermediate difference α_i, $i = 1, \dots, r-1$, is a difference of outputs after i round of multi-round transformation. And α_r is a final difference after the last round of multi-round transformation.

In this paper, we consider only Boolean functions which use bitwise addition $\oplus$ as operation with key. In such case, considered Boolean functions are examples of Markov ciphers [13]. So, in these cases $\forall x \in M$, $\forall k \in K$, $f_k(x) = f(x \oplus k)$, then an equation associated with differential (α, β) we can present as

$$f(x \oplus k \oplus \alpha) = f(x \oplus k) \oplus \beta.$$

Let denote $y = x \oplus k$, $y \in M$, then

$$f(y \oplus \alpha) = f(y) \oplus \beta.$$

So, we have made sure that value of key in such Boolean functions has no influence on differential probabilities distribution. That is why we will use notation $f(x), x \in M$ for Boolean functions further, assuming all used keys to be random, uniform and pairwise independent.

A *probability of differential* (α, β) for a function f is defined as

$$DP^f(\alpha, \beta) = \frac{1}{2^n} \sum_{x \in B_n} [f(x \oplus \alpha) = f(x) \oplus \beta],$$

where $[\dots]$ is an Iverson's brackets (indicator function): $[P] = 1$, if P is true, and $[P] = 0$, if P is false.

Probability of differential characteristic $(\alpha_0, \alpha_1, \dots, \alpha_r)$ of r-round Markov transformation as a composition of functions f is defined as the product of probabilities of consecutive round differentials [14]:

$$DCP^f(\alpha_0, \alpha_1, \dots, \alpha_r) = \prod_{i=1}^{r} DP^f(\alpha_{i-1}, \alpha_i).$$

1.3. Truncated Differentials

In 1994 Lars Knudsen [2] proposed a method that allows to ease requirements of regular differential cryptanalysis and enhance its applicability — *truncated differential cryptanalysis.* Using this method, Knudsen has achieved successful attack on 6 rounds of DES cipher. In general, truncated differential cryptanalysis considers sets of differences which combine several possible ordinary differences at the same time.

Truncated differential by Knudsen [2] is pair of bit vectors (α_1, β_1), where α_1 is subsequence of α and β_1 is subsequence of β, and (α, β) — is ordinary differential. So, for every truncated differential (α_1, β_1), α_1 and β_1 can be considered as masks of the input and output differences of a function. More general, a differential that predicts only parts of an n-bit value is called a *truncated differential.*

For now, there exists other approaches in theory of truncated differentials (see, e.g., [15]). In the modern sense, truncated differentials are considered as pairs (A, B), where A and B are a sets of differences. These sets can be described in different ways, depending on the approach. For instance, approaches based on masks or templates have been demonstrated to be effective.

Each mask α is associated with a set of possible differences $\Delta(\alpha)$. The set of possible differences $\Delta(\alpha)$ is the set of all possible differences that are subsequences of α:

$$\Delta(\alpha) = \{\alpha' \in V_n \setminus \{0\} : \alpha' \vee \alpha = \alpha\}.$$

In work [1], it was proposed an alternative form of the truncated differential as *ternary pattern-based truncated differential* (α, β) of a Boolean function $f\colon V_n \to V_n$ (we will address it *truncated differential* further in this paper), in which the both masks of input and output differences are defined as ternary vectors:

$$\alpha, \beta \in T_n = \{0, 1, ?\}^n.$$

In this case, $\Delta(\alpha)$ will contain the ordinary differences α' constructed by following rules:

1) if 0 is in mask α at a certain position, then 0 is in difference α' at the same position;
2) if α has 1 at a certain position, then α' has 1 at the same position;
3) if $?$ is in α at a certain position, then α' can have both 0 and 1 at the same position.

For each mask $\alpha \in T_n$, we define the set $\Delta(\alpha)$ as the set of differences $\alpha' \in V_n \setminus \{0\}$ that correspond to the mask α. For example,

$$\Delta(10?) = \{100, 101\},$$
$$\Delta(??0) = \{010, 100, 110\}.$$

In addition, by definition $\Delta(0) = \{0\}$ for a zero mask.

With every introduced truncated differential an event is associated: each input difference from $\Delta(\alpha)$ maps into an output difference from $\Delta(\beta)$. A *transition differential probability* of the truncated differential for a Boolean function f is defined as follows:

$$TDP^f(\alpha, \beta) = \frac{1}{2^n} \sum_{x \in V_n} \left[\substack{\forall \alpha' \in \Delta(\alpha): \\ f(x \oplus \alpha') \oplus f(x) \in \Delta(\beta)} \right].$$

This parameter provides the lower bound for the probability of truncated differential, but not the exact value.

Parameter TDP have any sense only if its value is higher than $\frac{|\Delta(\beta)|}{2^n}$, as symbol ? in output difference mask brings some level of uncertainty in possible real output differences.

Ternary pattern-based truncated differential characteristic (we will address it *truncated differential characteristic* further in this article) of r-round function F is the sequence of masks $(\alpha_0, \alpha_1, \ldots, \alpha_r), \alpha_i \in T_n, i = \overline{0, r}$. In r-round function F, each round is a Boolean function f independent of other rounds. In truncated differential characteristic, each consecutive pair of masks (α_{i-1}, α_i) is considered as truncated differential of corresponding round i, $i = \overline{1, r}$.

Similar to ordinary differential characteristics, for the truncated differential characteristic $(\alpha_0, \alpha_1, \ldots, \alpha_r)$ of r-round function F, where one round is a Boolean function f, we can introduce the *transition differential characteristic probability* as

$$TDCP^F(\alpha_0, \alpha_1, \ldots, \alpha_r) = \\ = \prod_{i=1}^{r} TDP^f(\alpha_{i-1}, \alpha_i).$$

Since $TDP^f(\alpha_{i-1}, \alpha_i)$ is the lower bound of the probability of the round truncated differential, and all round differentials are independent, we can say that $TDCP$ is the lower bound for the truncated differential characteristic.

Furthermore, we illustrate the potential and limitations of utilizing the approach outlined in [1] and [9] to search for truncated differentials and truncated differential characteristics with high transition probability.

2. Approaches to Construct High-probability Truncated Differentials and Differential Characteristics

In this section, we examine the potential of using the branch-and-bound method to construct high-probability truncated differentials similarly to ordinary differentials. We will also provide the advantages and disadvantages of constructing truncated differential characteristics in comparison with ordinary ones.

2.1. Branch-and-bound Method

The branch-and-bound method is usually used to find differentials or differential characteristics with high probability. In general, its goal is to optimize the solution search on a decision tree, considering only branches that meet certain criteria. When branch-and-bound method is utilized it differential cryptanalysis, the decision tree is built as follows:

- a root is the input difference,
- edges are rounds of encryption,
- selection criteria is the probability of the differential or differential characteristics.

The differential probability for a single round of encryption is usually easy to calculate. The differential probability after several rounds of encryption for one branch of the tree is the product of the probabilities of all one-round differentials for that branch. In the case, where different branches are mapped to one output difference, the differential probability from the root to this output difference will be the sum of probabilities across all possible branches.

Let's consider f — a 8-bit Boolean function with two S-boxes of the PRESENT cipher [11] and the bit permutation layer described in Table 1.

Table 1
8-bit permutation layer of model Boolean function f

i	0	1	2	3	4	5	6	7
$P(i)$	0	4	1	5	2	6	3	7

Let's try to find high-probability masks of truncated differentials for as many rounds as possible of such encryption round.

Consider as the input of the first round $0^4 0001$. Here are TDP values for three truncated differentials:

- $TDP^f(0^4 0001, 0^4 0100) = 0.25$;
- $TDP^f(0^4 0001, 0^4 0101) = 0.125$;
- $TDP^f(0^4 0001, 0^4 010?) = 0.375$.

The next step is to provide each of the mentioned output masks as input to the second round and compute TDP with one output mask $???1?^4$:

- $TDP^f(0^4 0100, ???1?^4) = 0.75$ — by definition of TDP, this means that $\frac{3}{4}$ of all plaintexts $x \in V_8$ transition input mask $0^4 0100$ into output mask $???1?^4$ for function f;
- $TDP^f(0^4 0101, ???1?^4) = 0.75$ — this also means that $\frac{3}{4}$ of all plaintexts $x \in V_n$ transition input mask $0^4 0101$ into output mask $???1?^4$;
- $TDP^f(0^4 010*, ???1?^4) = 0.5$ — and this means that $\frac{1}{2}$ of all plaintexts $x \in V_n$ transition both input mask $0^4 0100$ and input mask $0^4 0101$ in the same time into output mask $???1?^4$, because by definition of the masks, the set $\Delta(0^4 010?)$ consists of two differences $0^4 0100$ and $0^4 0101$.

Let denote differences we use:

- $\alpha = 0^4 0001$
- $\beta_1 = 0^4 0100$
- $\beta_2 = 0^4 0101$
- $\beta_3 = 0^4 010?$
- $\gamma = ???1?^4$

According to branch-and-bound method, to calculate $TDP^{\{f,f\}}(\alpha, \gamma)$ (the probability of the mask α transitions to the mask γ after two encryption rounds f), we have to add all the probabilities of the truncated differential characteristics below (using different branches):

- $TDCP(\alpha, \beta_1, \gamma) = 0.25 \cdot 0.75 = 0.1875$;
- $TDCP(\alpha, \beta_2, \gamma) = 0.125 \cdot 0.75 = 0.09375$;
- $TDCP(\alpha, \beta_3, \gamma) = 0.375 \cdot 0.5 = 0.1875$.

However, this is not possible with our definition of TDP, because a half of all plaintexts $x \in V_n$ in the second encryption round will be taken into account three times in each of the transitions. This situation can result to a value of $TDP > 1$ with an essential number of branches for a given output mask, which leads to the inconsistency of the parameter TDP as probability bound.

Therefore, we demonstrated that the branch-and-bound method in unsuitable for the search of high-probability ternary pattern-based truncated differentials.

2.2. Truncated Differential Characteristics of PRESENT

PRESENT [11] cipher was selected to examine the feasibility of the proposed approach of constructing truncated differentials and to evaluate the security of encryption transformations against cryptanalysis based on truncated differentials.

PRESENT cipher is a 31-round 64-bit SP-network, one round of which consists of key addition, 16 4-bit S-boxes and a linear transformation. Further, we denote one round of PRESENT cipher as f.

Since the branch-and-bound method cannot be applied to truncated differentials, we will consider differential characteristics based on truncated differentials in the same way as ordinary differentials.

Consider one round of encryption, $\alpha = 0^{63}1$ as the input mask, and both $\beta_1 = 0^{15}10^{15}?0^{31}1$ and $\beta_2 = 0^{15}10^{15}00^{31}1$ as output masks. The output masks are distinguished by a difference in a single bit in the 32^{nd} position. Calculated TDP values for considered input and output masks for one encryption round of PRESENT cipher f are:

- $TDP^f(\alpha, \beta_1) = 0.5$,
- $TDP^f(\alpha, \beta_2) = 0.25$.

As one can see, the value of TDP is larger for a truncated differential that has an output mask containing the character "?". If the mask does not contain the "?" character, then it plays the role of an ordinary difference between two texts.

At the same time, according to our calculations the most probable (in terms of TDP) output mask for input mask β_1 is mask $\gamma_1 = 0^3 10^{11} 10^3 10^{11} 10^7 ?0^{11} 10^3 ?0^7 1$:

$$TDP^f(\beta_1, \gamma_1) = 0.015625,$$

and the most probable output mask for input mask β_2 is mask $\gamma_2 = 0^3 10^{11} 10^3 10^{11} ?0^{19} 10^{11} 1$:

$$TDP^f(\beta_2, \gamma_2) = 0.125.$$

Then, if we calculate $TDCP$ values for considered truncated differential characteristics, we will get the next result:

- $TDCP^{\{f,f\}}(\alpha, \beta_1, \gamma_1) = 0.0078125$,
- $TDCP^{\{f,f\}}(\alpha, \beta_2, \gamma_2) = 0.03125$.

Therefore, the $TDCP$ value for the most probable characteristic where the mask in the middle of the characteristic contains the ? symbol is much smaller than the other. So, we can observe that the usage of a truncated differential in a differential characteristic gives an advantage over ordinary differential characteristic if the mask has the symbol "?" in the last round only.

2.3. Comparison of Truncated and Ordinary Differential Characteristics for PRESENT Cipher

The paper [16] gives us the differential characteristic for 4 rounds of the cipher PRESENT with the probability 2^{-18}. The differential characteristic have differences:

- $\omega_0 = 0^{49} 10^{11} 10^2$,
- $\omega_1 = 0^{28} 10^2 10^{28} 10^2 1$,
- $\omega_2 = 0^{23} 10^7 10^{32}$,
- $\omega_3 = 0^5 1010^{45} 1010^8$,
- $\omega_4 = 0^{49} 10^{11} 10^2$;

In this characteristic, the probability of the last round differential is equal to 2^{-6}. We substitute the last round differential with a truncated differential with output difference $\omega_4' = 010^{11} 10^3 10^{11} 10^{31} ?0^2$. New the last round truncated differential have high value of TDP:

$$TDP^f(\omega_3, \omega_4') = 0.09375 = 3 \times 2^{-3}.$$

We did not change the differentials of the previous rounds. So, we can achieve a higher value of $TDCP$ for the truncated differential characteristic:

$$TDCP^{f^{(4)}}(\omega_0, \omega_1, \omega_2, \omega_3, \omega_4') = 3 \times 2^{-15}.$$

In this case, the value of $TDCP = 3 \cdot 2^{-15}$ is much larger than the value 2^{-18} of differential characteristic achieved by ordinary differentials. Note that only one symbol "?" is used in the last template. So, the effective probability is

$$\frac{TDP}{|\Delta(\omega_4')|} = \frac{3 \cdot 2^{-15}}{2} = 3 \cdot 2^{-16},$$

which is still more than 2^{-18}.

Table 2 shows examples of two truncated differential characteristics C_2 and C_3 and compares the value of TDP with the differential characteristic given in [16] — C_1.

In the table 2 the following notations are used:

- $\alpha_0 = 0^{49} 10^{11} 10^2$
- $\alpha_1 = 0^{28} 10^2 10^{28} 10^2 1$
- $\alpha_2 = 0^{23} 10^7 10^{32}$
- $\alpha_3 = 0^5 1010^{45} 1010^8$
- $\alpha_4 = 0^{49} 10^{11} 10^2$
- $\beta_4 = 010^{11} 10^3 10^{11} 10^{31} ?0^2$
- $\gamma_1 = 0^{28} 10^2 10^{15} ?0^{12} 10^2 1$
- $\gamma_2 = 0^7 10^7 10^7 10^7 10^7 10^3 ?0^3 10^{11} ?0^4$
- $\gamma_3 = (01)^6 0^5 (10)^6 0^{13} ?0^3 ?0^2 (10)^4 1?10^2 ?0$

Table 2
Comparison of 4 round differential characteristics of the cipher PRESENT. $TDP(\omega_{i-1}, \omega_i)$ is a one round transition probability.

Round difference	C_1	$TDP(\omega_{i-1}, \omega_i)$	C_2	$TDP(\omega_{i-1}, \omega_i)$	C_3	$TDP(\omega_{i-1}, \omega_i)$
ω_0	α_0	—	α_0	—	α_0	—
ω_1	α_1	2^{-4}	α_1	2^{-4}	γ_1	3×2^{-3}
ω_2	α_2	2^{-4}	α_2	2^{-4}	γ_2	2^{-6}
ω_3	α_3	2^{-4}	α_3	2^{-4}	γ_3	2^{-16}
ω_4	α_4	2^{-6}	β_4	3×2^{-3}	—	—

The differential characteristic C_2 is constructed in such a way that the differential of only the last round is changed compared to the given characteristic C_1. This allows C_2 to obtain a higher probability than C_1.

The differential characteristic C_3 is constructed using a different method: at each round, the truncated differential with the highest TDP value is selected. This leads to a better transition probability only for the first round (when a truncated differential with output mask contains ”?” appears). But then the transition probabilities become lower than in the ordinary differential characteristic proposed in [16].

2.4. Improved Differential Characteristic for PRESENT Cipher

In the paper [16], it was presented differential characteristic of 14 rounds PRESENT cipher with probability 2^{-62}. Truncated differentials helps us to at least improve probability for 14 rounds differential characteristics.

We can construct truncated differential characteristic as ordinary differential characteristic provided in [16], but instead of the last (14) round ordinary differential we use truncated differential

$$(0^{49}10^{11}10^2, 0^{28}10^210^{12}?0^2?0^{12}10^21).$$

This truncated differential has TDP value for one round of PRESENT cipher encryption equal to $2^{-2.83}$. Full constructed truncated differential could be obtained as combination of presented in the Table 3 and presented in [16].

In the Table 3 we denote $\alpha_{14} = 0^{28}10^210^{12}?0^2?0^{12}10^21$.

The $TDCP$ of the 14 round truncated differential characteristic of PRESENT is equal to $2^{-60.83}$. This value is greater then the probability of ordinary differential characteristic provided in [16] — 2^{-62}. At the same time, truncated differential characteristic we constructed allows to estimate change of the same amount of bits as ordinary. In our case, we have 2 unpredicted bits (”?”) in the final mask. This means that probability of guessing the rest of the bits is equal to $2^{-(64-2)} = 2^{-62}$. So, since the calculated value of $TDCP$ is less then 2^{-62}, it also show us that such truncated differential characteristic can be useful for cryptanalysis.

Table 3
The 14 round truncated differential characteristic of PRESENT

Round diff.	Mask	$TDP(\omega_{i-1}, \omega_i)$
ω_0	$0^51^30^{45}1^30^8$	—
$\vdots$	$\vdots$	$\vdots$
ω_{13}	$0^{49}10^{11}10^2$	2^{-6}
ω_{14}	α_{14}	$2^{-2.83}$

3. Truncated Differentials for Functions with More Complex Structure

The approach described above is not applicable to ciphers whose structure uses more complex linear transformations than bit permutations. For example, Feistel-like ciphers. In this section, we provide rules for applying the bitwise addition (XOR, $\oplus$) operation to ternary masks we consider, which allows to adopt proposed approach to Feistel-like ciphers and SP-networks with relatively simple linear layers. As example, we construct truncated differential characteristic for 7 rounds of LBlock cipher.

3.1. Definition of Bitwise Addition Operation (XOR) for Ternary Masks

Since we use ternary masks (that contain element ”?”) instead of bit vectors, it is impossible to apply the usual bitwise modulo two addition operation to them. Therefore, we have to extend bitwise addition to our ternary masks.

By definition of ternary mask, the element ”?” means that both 0 and 1 could be at this position in actual difference (actual bit vector). Sine XOR operation is commutative, it is enough to determine the interaction of each element with each element of $\{0, 1, ?\}$ without taking into account the order of elements. Let us consider further examples:

$$1)\quad 0 \oplus ? = \begin{cases} 0 \oplus 0 = 0 \\ 0 \oplus 1 = 1 \end{cases} \Rightarrow ?;$$

$$2)\quad 1 \oplus ? = \begin{cases} 1 \oplus 0 = 1 \\ 1 \oplus 1 = 0 \end{cases} \Rightarrow ?;$$

$$3)\quad ? \oplus ? = \begin{cases} 0 \oplus ? = ? \\ 1 \oplus ? = ? \end{cases} \Rightarrow ?.$$

We can see that addition with the element ”?” results in the element ”?”. So, it is possible to define the bitwise addition operation for ternary masks as it given in the Table 4.

Table 4
XOR operation for ternary masks

x \ y	0	1	?
0	0	1	?
1	1	0	?
?	?	?	?

3.2. Truncated Differential Characteristics of LBlock Cipher

LBlock [12] is a 32 rounds lightweight block cipher with the 64-bit block size and the structure of Feistel-like network. The i-th round of LBlock is a transformation

$$(X_i, X_{i-1}) \to (L(X_{i-1}) \oplus F(X_i, K_i), X_i),$$

where F is the round function described in Fig. 1, L is the cyclic shift of 32-bit vectors by 8 bits to the left, K_i is a round subkey.

Internal function F consists of confusion and diffusion layers. Confusion layer consists of eight 4-bit S-boxes (defined in [12]) in parallel. Diffusion layer is defined as a permutation of eight 4-bit words, described in Fig. 1.

Thus far, no comprehensive search for differential characteristics has been conducted for LBlock. The existing researches only provide upper bounds on the probabilities of differential characteristics, which were obtained with relatively coarse methods, primarily based on estimating the number of active S-boxes [12].

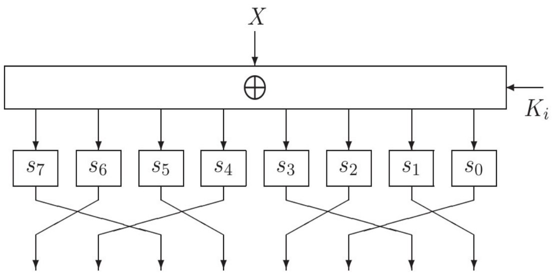

Figure 1: Internal function F of LBlock cipher

Further we describe a truncated differential characteristic for LBlock. Input difference is $0^{63}1$. For each encryption round we select an output mask with maximum value of TDP. At the same time, the output mask should have at most one more ”?” element than the input mask. If no output mask with at most one more ”?” element was found, we select the output mask with minimum number of ”?” elements. As a result, we construct truncated differential characteristic for 7 rounds of LBlock cipher with $TDCP$ value 2^{-44} and 19 unpredicted bits (19 elements ”?” in the final output mask). Used difference masks are:

- $\alpha_0 = 0^{63}1$,
- $\alpha_1 = 0^{23}10^{40}$,
- $\alpha_2 = 0^{17}?10^{36}10^{8}$,
- $\alpha_3 = 0^{15}10^{8}?0010^{21}?10^{13}$,
- $\alpha_4 = 0^{5}(10)^{2}?10^{16}(01)^{2}?0^{15}10^{8}?0010^{4}$,
- $\alpha_5 = (100)^{2}010^{4}1??1?001^{3}0?0^{13}(10)^{2}?10^{8}0^{8}(01)^{2}?$,
- $\alpha_6 = 1?00?1??110^{7}1?(01)^{2}?0?1(10)^{2}11001 0^{3}10^{4}1??1?001^{3}0?0^{8}$,
- $\alpha_7 = ?^{4}(1??)^{2}001^{3}?01?1(10)^{2}0^{3}?1?001?00? 1??10^{7}1?(01)^{2}?0?1(10)^{2}1$.

Transition probabilities of truncated differential characteristic is presented in the Table 5.

Constructed truncated differential characteristic allow us to predict the values of 45 bits after 7 rounds of encryption. Also, our characteristic is better than random guessing of 45 bits, because 2^{-45} is less than calculated $TDCP$ value.

This demonstrates that proposed ternary pattern-based approach can be used for cryptanalysis of Feistel-like ciphers.

Table 5
7 round LBlock truncated differential characteristic. $TDP(\alpha_{i-1}, \alpha_i)$ is a (α_{i-1}, α_i) differential transition probability. $TDCP$ is a (α_0, α_i) characteristic transition probability.

Mask	$TDP(\alpha_{i-1}, \alpha_i)$	$TDCP$
α_0	—	—
α_1	1	1
α_2	2^{-1}	2^{-1}
α_3	2^{-4}	2^{-5}
α_4	2^{-6}	2^{-11}
α_5	2^{-6}	2^{-17}
α_6	2^{-12}	2^{-29}
α_7	2^{-15}	2^{-44}

Conclusions

In this paper, we examine the applicability of the branch-and-bound method to the construction of truncated differentials and characteristics, based on the previously proposed ternary pattern-based approach and proposed earlier parameter TDP which limits the probabilities of truncated differentials from below. We demonstrated that the branch-and-bound method is unsuitable for constructing high-probability multi-round truncated differentials in terms of usage TDP parameter for evaluation the probabilities. In general, the branch-and-bound method could be used for constructing multi-round truncated differentials, but it should be considered different methods or parameters for evaluation of truncated differentials probability. Despite this, the branch-and-bound method remains viable for the construction of truncated differential characteristics in terms of parameter TDP.

Furthermore, we extended the XOR operation to ternary masks, enabling the application of the proposed differential cryptanalysis approach to a broader class of block ciphers, including Feistel-like structures. This enhancement expands the practical utility of the method, making it applicable to both simple and moderately complex cipher structures. By providing specific examples, such as the construction of truncated differential characteristics for a 14-round PRESENT cipher and a 7-round LBlock, we illustrated the practicality of our approach. These examples achieved a lower bound of probability better than random guessing, showcasing the method's potential for real-world cryptanalysis.

The presented results demonstrate that the proposed ternary pattern-based approach is not only theoretically robust but also practically applicable to real bit-oriented ciphers. However, the method's full potential can only be realized through further research. Future work should focus on developing advanced algorithms for construction of high-probability truncated differential characteristics and exploring their applications to a wider range of cryptographic primitives.

Acknowledgments

We gratefully acknowledge Serhii Yakovliev for his invaluable feedback and guidance throughout the development of this work. His support played a crucial role in shaping the direction and overall quality of this work.

The results of the Section 2 were presented at the XXII Ukrainian scientific and practical conference of students, Ph. D. students and young scientists *Theoretical and Applied Problems of Physics, Mathematics and Computer Science* (2024, Kyiv, Ukraine) [17]. The results of the Section 3 were presented at the II Ukrainian scientific and practical conference *Theoretical and Applied Cibersecurity* (2024, Kyiv, Ukraine) [18]. We thank the reviewers for their valuable comments and suggestions, which helped to improve the clarity and quality of this work.

References

[1] O. Yakymchuk and S. Yakovliev, "One formalized approach to truncated differential cryptanalysis of block ciphers," Tatra Mountains Mathematical Publications, 2024. https://doi.org/10.2478/tmmp-2024-0022.

[2] L. R. Knudsen, "Truncated and higher order differentials," in Fast Software Encryption (B. Preneel, ed.), pp. 196–211, Springer Berlin Heidelberg, 1995.

[3] L. R. Knudsen and T. A. Berson, "Truncated Differentials of SAFER," in Fast Software Encryption (D. Gollmann, ed.), pp. 15–26, Springer Berlin Heidelberg, 1996.

[4] M. Albrecht and G. Leander, "An All-In-One Approach to Differential Cryptanalysis for Small Block Ciphers." Cryptol-

ogy ePrint Archive, Paper 2012/401, 2012. https://eprint.iacr.org/2012/401.

[5] A. Canteaut, T. Fuhr, H. Gilbert, M. Naya-Plasencia, and J.-R. Reinhard, "Multiple Differential Cryptanalysis of Round-Reduced PRINCE (Full version)." Cryptology ePrint Archive, Paper 2014/089, 2014. https://eprint.iacr.org/2014/089.

[6] R. Ankele and S. Kölbl, "Mind the Gap — A Closer Look at the Security of Block Ciphers against Differential Cryptanalysis." Cryptology ePrint Archive, Paper 2018/689, 2018. https://eprint.iacr.org/2018/689.

[7] L. Li, K. Jia, X. Wang, and X. Dong, "Meet-in-the-middle technique for truncated differential and its applications to clefia and camellia," in Fast Software Encryption (G. Leander, ed.), (Berlin, Heidelberg), pp. 48–70, 2015. https://doi.org/10.1007/978-3-662-48116-5_3.

[8] Z. Ahmadian, A. Khalesi, D. M'foukh, H. Moghimi, and M. Naya-Plasencia, "Truncated differential cryptanalysis: New insights and application to QARMAv1-n and QARMAv2-64." Cryptology ePrint Archive, Paper 2023/1449, 2023. https://eprint.iacr.org/2023/1449.

[9] O. Yakymchuk, "A method for block ciphers security estimation against truncated differential cryptanalysis." master's thesis (in Ukrainian), Kyiv, 2020. https://ela.kpi.ua/handle/123456789/34327.

[10] O. Yakymchuk and S. Yakovliev, "On a Formalized Approach to Truncated Differential Cryptanalysis of Block Ciphers," in Central European Conference on Cryptology, (Smolenice, Slovakia), pp. 104–106, Slovak University Of Technology In Brtislava, 2022.

[11] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "Resent: An ultra-lightweight block cipher," in Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings, vol. 4727 of Lecture Notes in Computer Science, pp. 450–466, Springer, 2007.

[12] W. Wu and L. Zhang, "LBlock: A Lightweight Block Cipher." Cryptology ePrint Archive, Paper 2011/345, 2011. https://eprint.iacr.org/2011/345.

[13] X. Lai, J. L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," in Advances in Cryptology — EUROCRYPT '91 (D. W. Davies, ed.), pp. 17–38, Springer Berlin Heidelberg, 1991.

[14] S. Vaudenay, "On the security of cs-cipher," in Fast Software Encryption (L. Knudsen, ed.), (Berlin, Heidelberg), pp. 260–274, 1999.

[15] Z. Ahmadian, A. Khalesi, D. M'foukh, H. Moghimi, and M. Naya-Plasencia, "Truncated Differential Cryptanalysis: New Insights and Application to QARMAv1-n and QARMAv2-64." Cryptology ePrint Archive, Paper 2023/1449, 2023. https://eprint.iacr.org/2023/1449.

[16] M. Wang, "Differential Cryptanalysis of PRESENT." Cryptology ePrint Archive, Paper 2007/408, 2007. https://eprint.iacr.org/2007/408.

[17] K. Medvedtskyi and O. Yakymchuk, "Analysis of Approaches to the Search for High Probability Truncated Differentials," in Theoretical and Applied Problems of Physics, Mathematics and Computer Science, (Kyiv, Ukraine), pp. 224–227, Igor Sikorsky Kyiv Polytechnic Institute, 2024.

[18] O. Yakymchuk and K. Medvedtskyi, "Search for truncated differential characteristics of LBlock cipher," in Theoretical and Applied Cybersecurity, no. 2, (Kyiv, Ukraine), pp. 98–101, Igor Sikorsky Kyiv Polytechnic Institute, 2024.