sciendo

TATRA MOUNTAINS
Mathematical Publications
DOI: 10.2478/tmmp-2024-0022
Tatra Mt. Math. Publ. **87** (2024), 43–54

# ONE FORMALIZED APPROACH TO TRUNCATED DIFFERENTIAL CRYPTANALYSIS OF BLOCK CIPHERS

Oleksii Yakymchuk — Serhii Yakovliev

Institute of Physics and Technology, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, UKRAINE

ABSTRACT. We propose a formalized approach to truncated differential cryptanalysis based on ternary masks that separately account for unchanged, obligatorily changed, and unknown bits in differences. We introduce a security parameter for S-boxes and encryption mappings, which bounds the probability of truncated differentials from below, and examine its basic algebraic properties. Our approach enables the adaptation of existing techniques used in classical differential attacks to truncated differential cryptanalysis, allowing us to extract more information from the encryption process and evaluate the complexity of truncated differential attacks.

## Introduction

Differential cryptanalysis, first proposed by Biham and Shamir in 1991 [3], is a powerful tool for block cipher attacks. It focuses on analyzing differences between plaintexts as they propagate during encryption. Security against differential cryptanalysis is a necessary condition for any modern cipher. Over the years, several attempts have been made to ease the requirements of this cryptanalytical method and enhance its applicability. One such attempt is truncated differential cryptanalysis, first proposed by Knudsen [8] in 1994. Truncated differential cryptanalysis examines differences that are only partially determined or combine multiple possible ordinary differences simultaneously. In [8], Knudsen described a successful attack on 6 rounds of the DES cipher using truncated differential cryptanalysis. Other successful applications of this method include

© 2024 Mathematical Institute, Slovak Academy of Sciences.
2020 Mathematics Subject Classification: 94A60.
Keywords: symmetric cryptography, differential cryptanalysis, truncated differentials, block ciphers.
Licensed under the Creative Commons BY-NC-ND 4.0 International Public License.

attacks on 5 rounds of the Salsa20 [5], KLEIN cipher [12], RoadRunneR cipher [16], and others. The theory of truncated differential cryptanalysis has since been further refined in various works (e.g. [1,6]) and combined with other attack methods (e.g. [2]), leading to the broader concept of multiple differential cryptanalysis [4]. This approach has proven effective against word-oriented ciphers, such as bytewise SP-networks and generalized Feistel networks.

In this work we propose a new formalized approach to truncated differential analysis, specifying truncated differentials with ternary masks which consider unchanged, obligatory changed and unknown bits. This method allows us to describe sets of differences more effectively. While particularly efficient when the linear layer of an encryption round is a form of bit permutation, this approach is potentially applicable to ciphers with arbitrary structures. We also propose a new security parameter for S-boxes and encryption mappings which limits the probability of truncated differential from below, and study its properties. This parameter potentially opens up the possibility of adapting existing techniques of searching for ordinary high-probability differentials to truncated differential cryptanalysis.

The rest of the paper is organized as follows. Section 1 provides a standard notation and a brief description of truncated differential cryptanalysis. In Section 2.1, we introduce our approach to truncated differential cryptanalysis, a notion of mask-based differentials and a new parameter — a transition differential probability with its basic algebraic properties. Section 2.2 contains the results of experimental application of proposed approach to some S-boxes and a model cipher.

## 1. Truncated differential cryptanalysis

Let $V_n = \{0,1\}^n$ be the linear space of all $n$-length binary vectors. A *differential* of a Boolean function $f\colon V_n \to V_n$ is an arbitrary pair of vectors $(\alpha, \beta)$, $\alpha, \beta \in V_n$, which are interpreted as the difference (with respect to bit-wise addition $\oplus$) between inputs and as the difference between outputs of the function $f$.

The *probability of a differential* $(\alpha, \beta)$ (with respect to $\oplus$) for a function $f$ is defined as

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

where $[\dots]$ represents Iverson's brackets: $[P] = 1$, if $P$ is true, and 0, if false. If $f$ is parameterized with a key, then the probability of the differential is averaged over all possible keys. For a detailed explanation of differential attacks, we refer to [7].

A *truncated differential* is defined as a pair of sets $(A, B)$, $A, B \subseteq V_n$, where for any $\alpha \in A$ and $\beta \in B$, the pair $(\alpha, \beta)$ is treated as an ordinary differential [8].

The probability of the truncated differential $(A, B)$ for a function $f$ is defined as

$$\Pr\{A \to B\} = \Pr_{x,y}\{f(x) \oplus f(y) \in B \,|\, x \oplus y \in A\},$$

where $x, y \in V_n$ are independent and uniformly random vectors (see, e.g. [1]). This formula is equivalent to

$$\Pr\{A \to B\} = \frac{1}{|A|} \sum_{\substack{\alpha \in A, \\ \beta \in B}} \mathrm{DP}^F(\alpha \to \beta),$$

which can also be used as the definition [6].

The truncated differential $(A, B)$ enables the construction of distinguishing attacks and is generally useful for cryptanalysis if its probability is greater than $|B| \cdot 2^{-n}$ — the probability expected from a random permutation.

The effectiveness of the analysis using this method is directly related to the ability to effectively describe the sets $A$ and $B$ for a given cipher or its components (S-boxes, encryption rounds etc.). One of the most successful approaches is the template approach, where differential sets are described with a template of unchanged (zero) and unknown bits. For word-oriented ciphers, it is common practice to use templates of "zero" (unchanged) and "active" (somehow changed) words [1, 10]. However, no effective techniques currently exist for finding truncated differentials for ciphers of arbitrary structures, such as bit-oriented ciphers.

In summary, truncated differential cryptanalysis is a powerful ad hoc tool for analyzing certain classes of block ciphers. However, the lack of formalization in some aspects prevents this method from being used to its full potential.

## 2. New formalized approach to truncated differential cryptanalysis of block ciphers

### 2.1. Proposed approach

In this section, we propose a new template-based approach for truncated differential cryptanalysis, which can be applied primarily to bit-oriented block ciphers. The main idea is to consider masks at the bit level that distinguish between unchanged and obligatorily changed bits in differences. This approach allows us to extract more information during the encryption process. We also propose a new cryptographic parameter for S-boxes and encryption functions that provides a lower bound for the probability of truncated differentials.

Let $T_n$ represent the space of all possible ternary vectors of length $n$, with elements from the set $\{0, 1, ?\}$. We interpret vectors $\alpha, \beta \in T_n$ (masks for input and output differences, respectively) as follows:

- If the mask contains 0 at a specific position, the actual difference at that position is 0.
- If the mask contains 1 at a specific position, the actual difference at that position is 1.
- If the mask contains "?" at a specific position, the difference at that position could be either 0 or 1 (this position is excluded from analysis).

With every mask $\alpha \in T_n$ we can associate a set $\Delta(\alpha)$ of all non-trivial differences $\alpha' \in V_n \setminus \{0\}$ which correspond to the mask $\alpha$; for example,

$$\Delta(1?0) = \{100, 110\}, \qquad \Delta(0??) = \{001, 010, 011\}.$$

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

We denote an arbitrary pair of vectors $(\alpha, \beta)$, $\alpha, \beta \in T_n$ as the *ternary pattern-based truncated differential* of a Boolean function $f\colon V_n \to V_n$. For simplicity, throughout this paper, we refer to these as "truncated differentials."

By definition, to analyze the introduced truncated differentials, we need to consider the following event: a pair of inputs which have a difference from $\Delta(\alpha)$ maps into a pair of outputs which have a difference that corresponds to the mask $\beta$. Also, we need to guarantee that for any input difference we get corresponding value of the output difference. Define the *transition differential probability* of the mask $\alpha$ into the mask $\beta$ as

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

This definition expresses the minimal probability that any input difference of $f$ fitting the input mask $(\forall \alpha' \in \Delta(\alpha))$ for any input $x$ produces an output difference that fits the output mask (from $\Delta(\beta)$).

Like the classical differential probability, transition differential probability can be represented by the following set of binary vectors that correspond to non-zero indicators in the numerator:

$$\mathrm{TD}^f(\alpha, \beta) = \{x \in V_n \mid \forall \alpha' \in \Delta(\alpha)\colon f(x \oplus \alpha') \oplus f(x) \in \Delta(\beta)\}.$$

It should be noted that the TDP (unlike DP) is only a lower bound on the true values of the truncated differentials probabilities, because a certain differential can have the probability greater than the value of TDP (see below for an example). In particular, a zero TDP value does not imply that the corresponding differentials are impossible, because TDP considers all the differentials that correspond to the specified masks simultaneously. However, the TDP value shows the *guaranteed* probability of difference transition; hence, if the TDP is

larger than $|\Delta(\beta)| \cdot 2^{-n}$ (probability of truncated differential for random permutation), the encryption mapping should be considered insecure against the truncated differentials analysis. Note that $|\Delta(\beta)| = 2^q$, where $q$ is the number of "?" in $\beta$. Therefore, the more "?" characters in the output difference, the less useful the truncated differential will be for cryptanalysis (e.g., the trivial pattern $\beta = ?? \ldots ?$ has TDP $= 1$ and is of no use).

This probability bound allows us to extend existing differential cryptanalysis techniques to analyze truncated differentials. In particular, it enables restating all available methods for searching for high-probability differentials to build an attack on iterative block ciphers. The complexity of a truncated differential attack will be inversely proportional to the maximum value of TDP (or, more accurately, bounded from above with this value). Also note that the definition of TDP does not depend on introduced ternary pattern-based truncated differential: one can replace $\Delta(\alpha)$ and $\Delta(\beta)$ with arbitrary sets of differences $A, B \subseteq V_n$.

We should mention that another possible way of TDP definition, namely,

$$\overline{\mathrm{TDP}}^f(\alpha, \beta) = \frac{1}{2^n} \sum_{x \in V_n} [\exists \alpha' \in \Delta(\alpha) : f(x \oplus \alpha') \oplus f(x) \in \Delta(\beta)]$$

may initially seem more intuitively correct, but it introduces significant inconsistencies. Indeed, consider two suitable differentials

$$(\alpha', \beta') \quad \text{and} \quad (\alpha'', \beta'').$$

If there exists an $x$ such that

$$f(x \oplus \alpha') = f(x) \oplus \beta', \qquad f(x \oplus \alpha'') \neq f(x) \oplus \beta'',$$

then $x$ does not transit $\alpha''$ to $\beta''$ as actual differences. Yet, the $\overline{\mathrm{TDP}}$ value would still count this situation as possible because $x$ transits $\alpha'$ to $\beta'$. This leads to a situation where the $\overline{\mathrm{TDP}}$ value can be significantly larger than the actual probability and does not reflect the real situation.

This discrepancy between intuition and facts is, in our opinion, largely due to the wide application of truncated differential cryptanalysis to word-oriented ciphers. Due to strict limits of non-zero word-spreading patterns in these ciphers, there is no such counter-example $x$ value in most attack scenarios. With further clarification, $\overline{\mathrm{TDP}}$ can possibly become a meaningful parameter for such ciphers. However, for bit-oriented ciphers, this alternative $\overline{\mathrm{TDP}}$ definition is not applicable at all.

Below, we provide some basic algebraic properties of the TDP.

**Lemma 2.1.** *If the mask of the input difference is* 0*, then*

$$\mathrm{TDP}^f(0, \beta) = \begin{cases} 1, & \textit{if } \beta \textit{ is } 0; \\ 0, & \textit{otherwise.} \end{cases}$$

P r o o f. The only differential with an input difference of 0 that has a non-zero probability is the trivial differential $(0,0)$. Therefore, for a non-zero probability with an input difference of 0, $\Delta(\beta)$ must contain 0, which is only possible if $\beta$ is 0 by definition. For any output difference mask $\beta$ that contains at least one obligatorily changed bit 1 or an unpredictable bit ?, $\Delta(\beta)$ does not contain 0. □

**Lemma 2.2.** *For all $\alpha \in T_n \setminus \{0\}$:*

$$\mathrm{TDP}^f(\alpha, ??\ldots?) = 1.$$

P r o o f. It is evident that the mask "??...?" covers all possible non-zero differentials: $\Delta(?\ldots?) = V_n \setminus \{0\}$. So, for any non-zero input difference and any input $x$, the output difference will be in the $\Delta(??\ldots?)$ set. □

**Lemma 2.3.** *If both $\alpha, \beta \in \{0,1\}^n$, then*

$$\mathrm{TDP}^f(\alpha, \beta) = \mathrm{DP}^f(\alpha, \beta).$$

P r o o f. If a mask does not include any "?" symbols, it corresponds to exactly one difference, which is identical to this mask. Therefore, for any $\alpha, \beta \in \{0,1\}^n$ we have $\Delta(\alpha) = \{\alpha\}$ and $\Delta(\beta) = \{\beta\}$. The rest follows from the definition of TDP. □

**Lemma 2.4.** *For any $\alpha \in \{0,1\}^n$, $\beta \in T_n$:*

$$\mathrm{TDP}^f(\alpha, \beta) = \sum_{\beta' \in \Delta(\beta)} \mathrm{DP}^f(\alpha, \beta').$$

P r o o f. From the previous lemma, we have $\Delta(\alpha) = \{\alpha\}$ for $\alpha \in \{0,1\}^n$. Consider the sets $\mathrm{D}^f(\alpha, \beta') = \{x \colon f(x \oplus \alpha) \oplus f(x) = \beta'\}$ for $\beta' \in \Delta(\beta)$. These sets are disjoint when $\alpha$ is fixed, so

$$\mathrm{TDP}^f(\alpha, \beta) = \frac{1}{2^n} \sum_{\beta' \in \Delta(\beta)} \left|\mathrm{D}^f(\alpha, \beta')\right| = \sum_{\beta' \in \Delta(\beta)} \mathrm{DP}^f(\alpha, \beta'),$$

which concludes the proof. □

As a corollary, if $\alpha \in \{0,1\}^n$, then the set $\Delta(\alpha)$ consists of only one element $\alpha$ and

$$\mathrm{TDP}^f(\alpha, \beta) \geq \max_{\beta' \in \Delta(\beta)} \mathrm{DP}^f(\alpha, \beta').$$

Note that this inequality may not hold for $\alpha \notin \{0,1\}^n$, because in that case

$$\mathrm{TDP}^f(\alpha, \beta) = \frac{1}{2^n} \left|\mathrm{TD}^f(\alpha, \beta)\right| = \frac{1}{2^n} \left| \bigcap_{\alpha' \in \Delta(\alpha)} \bigcup_{\beta' \in \Delta(\beta)} \mathrm{D}^f(\alpha', \beta') \right|,$$

and the cardinality of the described $\mathrm{TD}^f$ set may not be connected to any particular $\mathrm{D}^f(\alpha', \beta')$ cardinality.

We say that mask $\alpha$ *dominates* mask $\tilde{\alpha}$, if for all $i$ either $\alpha_i = \tilde{\alpha}_i$, or $\alpha_i = ?$ and $\tilde{\alpha}_i \in \{0, 1\}$. In this case $\Delta(\alpha)$ includes all the elements from $\Delta(\tilde{\alpha})$. We denote this domination as $\alpha \succcurlyeq \tilde{\alpha}$.

**Lemma 2.5.** *For all $\beta_1, \beta_2 \in T_n$, if $\beta_1 \succcurlyeq \beta_2$, then $\forall \alpha \in T_n$:*

$$\mathrm{TDP}^f(\alpha, \beta_1) \geq \mathrm{TDP}^f(\alpha, \beta_2).$$

Proof. For any $\beta_1, \beta_2 \in T_n$, if $\beta_1$ dominates $\beta_2$, then $\beta_1$ covers at least all the differences of $\beta_2$. Hence, $\Delta(\beta_1) \supseteq \Delta(\beta_2)$ and the lemma's statement follows from the definition of TDP. □

Domination helps us to filter the masks, leaving the most useful ones for attacks.

Now, consider the keyed mapping $F_k(x) = f(x \oplus k)$. For keyed mappings, probabilities of differentials are introduced as the average over the keys, so we can introduce the *expected transition differential probability* for $F_k$ as

$$\mathrm{ETDP}^{F_k}(\alpha, \beta) = \frac{1}{2^n} \sum_{k \in V_n} \mathrm{TDP}^{F_k}(\alpha, \beta).$$

However, since $F_k$ is a Markov cipher [9], it follows from definition of TDP that $\mathrm{ETDP}^{F_k}(\alpha, \beta) = \mathrm{TDP}^f(\alpha, \beta)$.

Next, consider the iterative $r$-round block cipher $E$ with round functions of form $F_k$ (the so-called *key alternating cipher*). Recall that a *differential characteristic* of $E$ is a sequence $(\omega_0, \omega_1, \ldots, \omega_r)$, where every $\omega_i \in V_n \setminus \{0\}$, $i = \overline{0, r}$, is treated as a difference between intermediate ciphertexts after the $i$-th round. The cipher $E$ is also a Markov cipher and, under the assumption of round key independence, round differentials $(\omega_{i-1}, \omega_i)$ are also pairwise independent. Therefore, the probability of the differential characteristic is equal to [13]

$$\prod_{i=1}^{r} \mathrm{DP}^f(\omega_{i-1}, \omega_i).$$

It is natural to introduce a *truncated (ternary pattern-based) differential characteristic* $(\alpha_0, \alpha_1, \ldots, \alpha_r)$, $\alpha_i \in T_n$, $i = \overline{0, r}$, where $(\alpha_{i-1}, \alpha_i)$ is considered a truncated differential of $i$-th round. Since $\mathrm{TDP}^f(\alpha_{i-1}, \alpha_i)$ represents the lower bound of the round's truncated differential probability, and the round differentials are independent, we can say that the formal product

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

is the lower bound for the truncated differential characteristic. This allows us to construct multi-round truncated differentials for a key-alternating cipher by combining round truncated differentials.

### 2.2. Experimental results

We illustrate the behavior of the proposed TDP parameter using a four-bit S-box $\sigma$ (denoted as $K1$ in [14]), which is defined as follows:

$$\sigma = (7, 9, 4, D, 0, 2, C, B, A, 8, 1, 6, E, 5, F, 3)$$

(all numbers are four-bit hexadecimals). Part of the calculations is presented in Table 1.

TABLE 1. Values of max DP, TDP and TD for selected truncated differentials of the S-box $\sigma$.

| $(\alpha, \beta)$ | $\max\limits_{\substack{\alpha' \in \Delta(\alpha),\\ \beta' \in \Delta(\beta)}} \mathrm{DP}^{\sigma}(\alpha', \beta')$ | $\mathrm{TDP}^{\sigma}(\alpha, \beta)$ | $\mathrm{TD}^{\sigma}(\alpha, \beta)$ |
|---|---|---|---|
| $(001?, 10?1)$ | 0.125 | 0.125 | $\{0111, 1010\}$ |
| $(001?, 11??)$ | 0.25 | 0.125 | $\{0110, 1011\}$ |
| $(001?, 1???)$ | 0.25 | 0.5 | $\{0100, 0101, 0110, 0111,$ $1000, 1001, 1010, 1011\}$ |
| $(001?, ?101)$ | 0.25 | 0 | $\varnothing$ |
| $(001?, ?10?)$ | 0.25 | 0.0625 | $\{0001\}$ |

In cases where $|\Delta(\alpha)| > 3$, for all $\beta$ except for the pattern "????", the values of $\mathrm{TDP}^{\sigma}(\alpha, \beta)$ are equal to 0. For small-size S-boxes, this can be explained by the strong conditions for events in TDP. When the cardinality of $\Delta(\alpha)$ is 2 or 3, the truncated differential probability lies in the interval $[0, 0.5]$; in most cases TDP $= 0$, but there are sufficient truncated differentials with non-zero probability.

As we can see from Table 1, it is difficult to describe a direct relationship between the value of TDP and the probabilities of ordinary differentials corresponding to the given truncated differentials. TDP can be either greater or smaller than the value of the associated ordinary differential probability and, in some cases, can even be equal. As a result, ciphers that are secure against classical differential cryptanalysis may still be insecure against truncated differential cryptanalysis in terms of the proposed formal method.

For illustrative purposes we applied our method to a model cipher. We considered the Heys cipher [7] with block size of 64 bits as the model cipher. One encryption round of this cipher consists of the following steps (Fig. 1):

(1) Bitwise addition with a round key;
(2) Eight 8-to-8-bit S-boxes (we used the S-box $\pi_0$ from the Kalyna cipher [11]);
(3) A specific bit permutation: the $i$-th bit of the $j$-th block is swapped with the $j$-th bit of the $i$-th block.

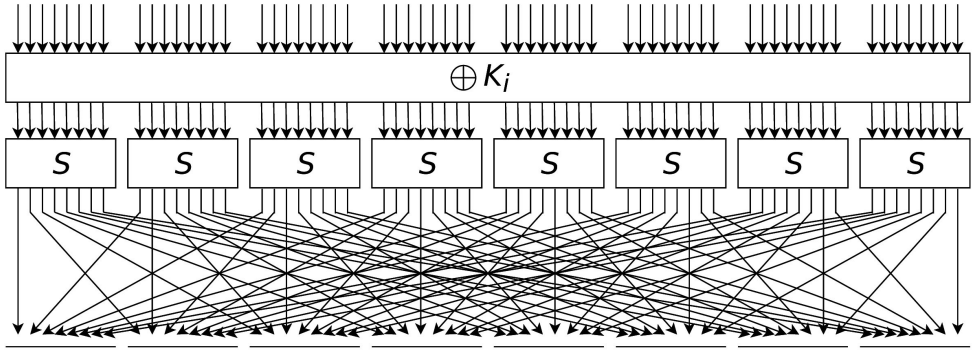


FIGURE 1. One round of considered Heys cipher.

Introduce 8-bits vectors:
$\overrightarrow{0} = 00000000$; $\overrightarrow{1} = 00000001$; $\overrightarrow{a} = 0000000?$; $\overrightarrow{b} = ?0000000$; $\overrightarrow{c} = ?0?00000$.

To construct a truncated differential characteristic we considered:

a mask of input difference
$$\alpha = [\overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{1}],$$
two intermediate masks
$$\gamma_1 = [\overrightarrow{a}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}],$$
$$\gamma_2 = [\overrightarrow{b}, \overrightarrow{0}, \overrightarrow{b}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}, \overrightarrow{0}],$$
as well as the output difference mask
$$\beta = [\overrightarrow{b}, \overrightarrow{b}, \overrightarrow{c}, \overrightarrow{c}, \overrightarrow{b}, \overrightarrow{c}, \overrightarrow{b}, \overrightarrow{c}].$$

Table 2 presents the truncated differential characteristic of the 3-round model Heys cipher. The characteristic is presented with the calculated values of TDP for each consecutive truncated differential of this characteristic and calculated values of TDCP after each round.

TABLE 2. Values of TDP of round truncated differentials and TDCP of truncated differential characteristic for 3-round model Heys cipher.

| Round number | Mask | TDP | | TDCP | |
|---|---|---|---|---|---|
| 0 | $\alpha$ | 1 | 1 | 1 | 1 |
| 1 | $\gamma_1$ | $1.56 \cdot 10^{-2}$ | $2^{-6}$ | $1.56 \cdot 10^{-2}$ | $2^{-6}$ |
| 2 | $\gamma_2$ | $3.9 \cdot 10^{-2}$ | $2^{-4.68}$ | $6.1 \cdot 10^{-4}$ | $2^{-10.68}$ |
| 3 | $\beta$ | $8.59 \cdot 10^{-2}$ | $2^{-3.54}$ | $5.25 \cdot 10^{-5}$ | $2^{-14.22}$ |

The TDCP of the presented truncated differential characteristic $(\alpha, \gamma_1, \gamma_2, \beta)$ is equal to $2^{-14.22}$ after the 3 rounds of the model Heys cipher. That means, that if the input text has only the last bit changed, then with a probability of *at least* $2^{-14.22}$, the output text will have unchanged bits except for the "?" bits: the first bit of the first, second, fifth, and seventh blocks, and the first and third bits of third, fourth, sixth, and eighth blocks. In general, the TDCP values of all the found truncated differentials are significantly greater than the expected probability of $2^{12}/2^{64} = 2^{-52}$, which would be the case for a random 64-bit permutation. This enables the possibility of setting up, for example, a distinguishing attack.

## Conclusions

In this paper, we propose a formal approach to constructing and analyzing truncated differentials based on ternary masks. This approach considers both unchanged and obligatorily changed bits in the input and output differences of S-boxes and encryption mappings, allowing us to effectively describe truncated differentials for further usage in cryptanalytic attacks. We also introduce a new security parameter, the transition differential probability (TDP), which shows the guaranteed probability of truncated differentials and thus provides a lower bound on the actual probabilities. Consequently, the complexity of a truncated differential attack is inversely proportional to the maximum value of TDP. We have proven several algebraic properties of TDP. Notably, the values of the proposed parameter did not show a clear correlation with the probabilities of ordinary differentials.

The formal approach we present is efficient for analyzing ciphers that combine S-boxes and bit permutations in their encryption rounds. We believe that it could also be applicable to other classes of ciphers, which is a subject for future research. However, it should be noted that the formal approach introduced in this paper does not prove the security of block ciphers against truncated differential cryptanalysis; rather, it helps to find suitable truncated differentials to mount an attack. Proving security against this cryptanalytic method would require other theoretical approaches.

**Acknowledgement.** Most of the results of this work were presented at the Central European Conference on Cryptography (CECC'22, Slovakia) [15]. We are thankful to anonymous reviewers for valuable comments. We are very grateful to the anonymous reviewer of the journal Tatra Mt. Math. Publ. whose insightful and critical comments allow us to significantly improve this text. We also thank Anastasiia Rusova for her estimable notes and remarks.

## REFERENCES


[1] AHMADIAN, Z.—KHALESI, A.—M'FOUKH, D.—MOGHIMI, H.—NAYA-PLASENCIA, M.: *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.

[2] BARIANT, A.—LEURENT, G.: *Truncated Boomerang Attacks and Application to AES-based Ciphers*. Cryptology ePrint Archive, Report 2022/701, 2022. http://eprint.iacr.org/2022/701.

[3] BIHAM, E.—SHAMIR, A.: *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptology **4** (1991), 3–72.

[4] BLONDEAU, C.—GÉRARD, B.: *Multiple differential cryptanalysis: theory and practice*. In: *Fast Software Encryption* (A. Joux, ed.), Springer-Verlag, Berlin, Heidelberg 2011, pp. 35–54. https://www.iacr.org/archive/fse2011/67330035/67330035.pdf.

[5] CROWLEY, P.: *Truncated Differential Cryptanalysis of Five Rounds of Salsa20*. Cryptology ePrint Archive, Report 2005/375, 2005. http://eprint.iacr.org/2005/375.

[6] EICHLSEDER, M.—LEANDER, G.—RASOOLZADEH, S.: *Computing expected differential probability of (truncated) differentials and expected linear potential of (multidimensional) linear hulls in SPN block ciphers*. Cryptology ePrint Archive, Paper 2020/1356, 2020. https://eprint.iacr.org/2020/1356.

[7] HEYS, H. M.: *A Tutorial on Linear and Differential Cryptanalysis*, Cryptologia 26 (2001), no. 3, 189–221. http://dx.doi.org/10.1080/0161-110291890885.

[8] KNUDSEN, L. R.: *Truncated and Higher Order Differentials*. In: *Fast Software Encryption* (B. Preneel, ed.), Springer-Verlag, Berlin, Heidelberg, 1995, pp. 196–211.

[9] LAI, X.—MASSEY, J. L.—MURPHY, S.: *Markov Ciphers and Differential Cryptanalysis*. In: *Advances in Cryptology — EUROCRYPT '91* (D. W. Davies, ed.), Springer--Verlag, Berlin Heidelberg, 1991, pp. 17–38.

[10] LI, L.—JIA, K.—WANG, X.—DONG, X.: *Meet-in-the-Middle Technique for Truncated Differential and Its Applications to CLEFIA and Camellia*. In: *Fast Software Encryption* (G. Leander, ed.), Springer-Verlag, Berlin Heidelberg, 2015, pp. 48–70. https://doi.org/10.1007/978-3-662-48116-5_3.

[11] OLIYNYKOV, R.—GORBENKO, I.—KAZYMYROV, O.— RUZHENTSEV, V.— KUZNETSOV, O.—GORBENKO, Y.— DYRDA, O.—DOLGOV, V.—PUSHKARYOV, A.— MORDVINOV, R.—KAIDALOV, D.: *A New Encryption Standard of Ukraine: The Kalyna Block Cipher*. Cryptology ePrint Archive, Report 2015/650, 2015. http://eprint.iacr.org/2015/650.

[12] RASOOLZADEH, S.—AHMADIAN, Z.—SALMASIZADEH, M.—AREF, M. R.: *An Improved Truncated Differential Cryptanalysis of Klein*, Tatra Mt. Math. Publ. **67** (2017), 135–147.

[13] VAUDENAY, S.: *On the security of CS-cipher*. In: *Fast Software Encryption* (L. Knudsen, ed.), Springer-Verlag, Berlin, Heidelberg, 1999, pp. 260–274.

[14] YAKOVLIEV, S.: *Balanced Quality Criteria of Long-term Key Elements of the Encryption Algorithm GOST 28147–89*, Information Technology and Computer Engineering **14** (2009), 48–55. (In Ukrainian)

[15] YAKYMCHUK, O.—YAKOVLIEV, S.: *On a Formalized Approach to Truncated Differential Cryptanalysis of Block Ciphers*. In: *Proceedings of Central European Conference on Cryptology CECC '22* (K. Nemoga, R. Ploszek, P. Zajac, eds.), Mathematical Institute of Slovak Academy of Sciences, Bratislava, Slovakia, June 2022, pp. 104–106.

[16] YANG, Q.—HU, L.—SUN, S.—SONG, L.: *Truncated Differential Analysis of Round-Reduced RoadRunneR Block Cipher*. Cryptology ePrint Archive, Report 2016/084, 2016. `http://eprint.iacr.org/2016/084`.

Received September 29, 2022
Revised July 29, 2024
Accepted August 19, 2024
Publ. online November 20, 2024

*Oleksii Yakymchuk*
*Serhii Yakovliev*
*Department of Mathematical Methods of Information Security*
*Institute of Physics and Technology,*
*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"*
*37, Prospect Beresteiskyi,*
*03056, Kyiv*
*UKRAINE*

*E-mail*, 1: oleksii.yakymchuk@gmail.com
*E-mail*, 2: yasv@rl.kiev.ua