Research Article

Marco Calderini, Roberto Civino*, and Riccardo Invernizzi

Differential experiments using parallel alternative operations

https://doi.org/10.1515/jmc-2023-0030
received September 06, 2023; accepted October 20, 2023

Abstract: The use of alternative operations in differential cryptanalysis, or alternative notions of differentials, is lately receiving increasing attention. Recently, Civino et al. managed to design a block cipher that is secure with respect to the classical differential cryptanalysis performed using XOR-differentials, but weaker with respect to the attack based on an alternative difference operation acting on the first s-box of the block. We extend this result to parallel alternative operations, i.e. acting on each s-box of the block. First, we recall the mathematical framework needed to define and use such operations. After that, we perform some differential experiments against a toy cipher and compare the effectiveness of the attack with respect to the one that uses XOR-differentials.

Keywords: differential cryptanalysis, alternative operations, distinguisher, block ciphers

MSC 2020: 20B35, 94A60, 68P25

1 Introduction

Differential cryptanalysis is a powerful tool introduced in the beginning of the 90s to attack some cryptographic symmetric primitives, namely block ciphers [1]. The attack, which has later been generalised [2–4], is typically a chosen-plaintext attack that takes advantage of nonuniform relations between input differences and corresponding output differences.

To mitigate vulnerability to these attack methods, the cryptographic transformations employed within the substitution boxes (s-boxes) of the cipher should aim for the lowest possible level of differential uniformity [5] (for a comprehensive exploration of the differential uniformity of vectorial Boolean functions, readers can refer to Mesnager et al.'s survey [6]). It is essential to emphasize that the calculation of differential uniformity is based on the XOR operation. Indeed, in a traditional scenario of cryptanalysis of block ciphers, the difference operation classically taken into consideration by both designers and cryptanalysts is the one used to mix the key during the encryption process. In many cases, this operation is the bit-wise addition modulo two, i.e. the XOR. Nevertheless, it is worth noting that alternative types of operations may also be contemplated. For example, Berson introduces the modular difference to study the MD/SHA family of hash functions [7], and a similar method has been used [8] to cryptanalyze the block cipher PRESENT [9]. Borisov et al. [10] proposed a new type of differential known as multiplicative differential to attack IDEA [11]. This inspired the definition of c-differential uniformity [12], which has been extensively studied in the last couple of years, even if the cryptographic implication of such c-differential uniformity on attacking block ciphers remains a subject of

*** Corresponding author: Roberto Civino,** Department of Information Engineering, Computer Science and Mathematics, University of l'Aquila, Via Vetoio 67100 L'Aquila, Italy, e-mail: roberto.civino@univaq.it
Marco Calderini: Department of Mathematics, University of Trento, Via Sommarive 14, 38122, Povo, Italy, e-mail: marco.calderini@unitn.it
Riccardo Invernizzi: KU Leuven, Celestijnenlaan 200a, 3001, Leuven, Belgium, e-mail: riccardo.invernizzi@kuleuven.be

ongoing debate [13]. In 2019, Civino et al. showed that a differential attack making use of alternative differences may be effective against XOR-based ciphers that are resistant to the classical differential attack [14]. More precisely, they designed a small-scale substitution-permutation network (SPN) inspired by the block cipher PRESENT, with five s-boxes of three bits each. They introduced a new sum on the whole message space that acts as the XOR on the last four s-boxes, while the first one matches with one of the alternative sums defined by Calderini et al. [15], coming from another elementary abelian regular group of translations (*translation groups* in short). Using such operation, they were able to mount a distinguishing attack on five rounds of the cipher. Moreover, they showed that this result cannot be obtained with the traditional differential approach, i.e. by looking at the distribution of classical differentials.

In this work, we show that this idea can be extended to the whole block, attacking all the s-boxes at the same time. The difference operator that we consider comes again from the family of alternative operations introduced by Calderini et al. [15]. Although it could be made more general without effort, for the ease of description, we focus here on the case of translation-based ciphers [16], which are the most common form of SPNs nowadays, where the encryption is realised by subsequent iterations of a non-linear s-box layer, a (usually) linear permutation, and an XOR-based key addition.

In order to guarantee deterministic propagation of differences through the diffusion layers of the ciphers, as happens in the classical scenario, we need to characterise the XOR-linear bijective maps that are also linear with respect to another (parallel) sum. As we will discuss later, the mentioned problem is of general interest in cryptography, and results in this direction will produce examples of XOR-based trapdoor ciphers for which a non-XOR distinguisher may exist. Unfortunately, only partial solutions to this problem are known [14,17,18]. Keeping our focus in this direction, after performing some computational experiments, we are able to design a toy cipher similar to the one suggested in the study by Civino et al. [14], with four parallel s-boxes of four bits each[1] together with an alternative parallel operation $\circ$ that can be used to attack it. A computer-aided direct check shows that the diffusion layer of the proposed cipher is a linear permutation with respect to both the operations + and $\circ$, which is the pivotal condition for the success of the attack.

We show the results of a distinguishing attack for a number of rounds up to 17, concluding that differentials based on our alternative operation have much higher probabilities. Moreover, the difference in probability between alternative differentials and classical differentials that we obtain is higher than the one obtained in the study by Civino et al. [14], showing the effectiveness of our approach.

The article is organised as follows: in Section 2, we introduce the notation and describe the general setting for our attack; in Section 2.1, a brief summary on the construction of alternative operations coming from elementary abelian regular groups is given; in Section 3, we design a 16-bit cipher and a suitable parallel alternative operation, and perform experiments to study its resistance to differential cryptanalysis. We show the consistent improvement of our approach with respect to the classical one; and in Section 4, we conclude the article with the discussion of some open problems.

2 Preliminaries

Let $V = (\mathbb{F}_2)^n$ be a binary vector space, with canonical basis $e_1, \dots, e_n$, which will represent the plaintext-ciphertext space of an n-bit block cipher. We denote by

$$T \coloneqq \{\sigma_a | a \in V, \sigma_a : x \mapsto x + a\} < \mathrm{Sym}(V)$$

the group of translations on V. We stress that the action of this translation group on the message space V represents the XOR-based key-addition layer in a block cipher. Let us also note that T as a subgroup of the symmetric group $\mathrm{Sym}(V)$ is elementary, abelian, and regular. We recall here the definition of regularity.

1 It is important to specify that the design technique is completely scalable and that we decided to perform experiments on a small-sized cipher only for a matter of efficiency.

Definition 1. A permutation group G acting transitively on a set V is said to be regular if, for all $v \in V$, the stabilizer of G at v $G_v \coloneqq \{g \in G | vg = v\}$ is trivial.

It is well known that any other elementary abelian regular subgroup of $\mathrm{Sym}(V)$ is conjugated to T.

Theorem 1. [19] *Let $\mathcal{T} < \mathrm{Sym}(V)$ be an elementary abelian regular subgroup. Then, there exists $g \in \mathrm{Sym}(V)$ such that $\mathcal{T} = \mathrm{T}^g = g^{-1}\mathrm{T}g$.*

Let us now show how to define another operation on V starting from another elementary abelian regular group of translations.

Definition 2. Let $\mathcal{T} < \mathrm{Sym}(V)$ be an elementary abelian regular group. Let us define an additive group operation $\circ$ on V by letting for each a and b in V

$$a \circ b \coloneqq a\tau_b,$$

where τ_b is the unique element of $\mathcal{T}$ sending 0 to b.

Proposition 1. *If $\circ$ is defined as above, then $(V, \circ)$ is a vector space over $\mathbb{F}_2$, with associated translation group $T_\circ = \mathcal{T}$. Moreover, $(V, \circ) \cong (V, +)$.*

The subspaces introduced below are essential to understand the structure of alternative operations coming from translation groups. We refer to Civino et al. for a more detailed discussion [14].

Definition 3. Given an operation $\circ$ as above, a vector $k \in V$ is called a *weak key* if, for each $x \in V$, it holds $x + k = x \circ k$. The set

$$W_\circ \coloneqq \{k | k \in V, k \text{ is a weak key}\}$$

is called the *weak-key space*, and is a subspace of both $(V, +)$ and $(V, \circ)$. We denote by $d \geq 1$ its dimension. Moreover, let us define a dot product on V such that for each $a, b \in V$,

$$a \cdot b \coloneqq a + b + a \circ b.$$

The set of elements that can be expressed as dot products is denoted by

$$U_\circ \coloneqq \{x \cdot y | x, y \in V\}$$

and is called the *set of errors*.

Finally, denoting by $\mathrm{GL}(V, +)$ and $\mathrm{GL}(V, \circ)$ the groups of linear permutations with respect, $+$ and $\circ$, respectively, we define

$$H_\circ \coloneqq \mathrm{GL}(V, +) \cap \mathrm{GL}(V, \circ).$$

We now briefly present the impact of an alternative sum $\circ$ on the differential cryptanalysis of SPNs. The classical differential attack relies on the property that each XOR-difference is maintained the same after the key is XOR-ed to the state. This is not the case when considering $\circ$-differences. Indeed, let us consider two inputs with difference Δ, denoted by x and $x \circ \Delta$. After the key addition, the difference becomes

$$(x + k) \circ ((x \circ \Delta) + k) \coloneqq \Delta^\circ.$$

However, it can be shown [14] that if $T < \mathrm{AGL}(V, \circ)$ and $T_\circ < \mathrm{AGL}(V, +)$, then

$$\Delta^\circ = \Delta + k \cdot \Delta, \tag{1}$$

i.e. in a particular setting, the output difference after the key-addition layer can be expressed in terms of the dot product introduced in Definition 3. By definition, $k \cdot \Delta$ belongs to $U_\circ$, and therefore, the number of possible output differences is bounded by $|U_\circ|$. The presence of the *error* in equation (1), of course, forces us to consider $\circ$-differential probabilities introduced by the key-addition layer, unlike in the classical case, yielding a disadvantage in terms of the final probability of the differential propagation.

On the other hand, the s-box is usually designed to have the lowest possible differential uniformity with respect to the XOR. This may no longer be true with respect to the operation $\circ$. A higher differential uniformity creates trails with higher probability for $\circ$ and counterbalances the effect of differential probability introduced by the key addition.

Finally, and more importantly, the diffusion layer λ of an SPN is usually an XOR-linear map. In order to mount a successful $\circ$-differential attack, we need λ to be $\circ$-linear as well, i.e. $\lambda \in H_\circ$. Otherwise, λ would be a $\circ$-non-linear map and the effect of block-sized differential probabilities introduced by the diffusion layer would make the approach completely ineffective. This represents a strong motivation to the study of $H_\circ$.

We are now ready to show explicitly how operations coming from new translation groups are constructed.

2.1 Construction of alternative operations

For the reason explained above (equation (1)), it is convenient to consider operations $\circ$ on V coming from a translation group $T < \mathrm{Sym}(V)$ such that $T < \mathrm{AGL}(V, \circ)$ and $T_\circ < \mathrm{AGL}(V, +)$, which is the setting in which we will assume to be from now on. We will make use of the construction of such operations as presented in the study by Calderini et al. [15], but we will omit here many of the details, that the interested reader can find in the cited article.

Recall that we denote $n = \dim(V)$ and that we have $1 \le d = \dim(W_\circ) \le n - 2$ [15]. We will focus on the particular case $d = n - 2$. The reason for this is that the case when the dimension of the weak-key space reaches its upper bound is one of those in which the structure of $H_\circ$ is known (Theorem 2). Thanks to Calderini et al. [15, Theorem 3.9], we may assume, up to conjugation, that $W_\circ$ is spanned by $\{e_3, \ldots, e_n\}$. In this setting, from Calderini et al. [15, Theorem 3.11] (but see also Civino et al. [14, Theorem 3.3]), we have

$$a \circ e_i = a\tau_{e_i} = aM_{e_i} + e_i,$$

where

$$M_{e_1} = \left(\begin{array}{c|c} \mathbb{1}_2 & \begin{matrix} \mathbf{0} \\ \boldsymbol{b} \end{matrix} \\ \hline \mathcal{O}_{n-2,2} & \mathbb{1}_{n-2} \end{array}\right), \quad M_{e_2} = \left(\begin{array}{c|c} \mathbb{1}_2 & \begin{matrix} \boldsymbol{b} \\ \mathbf{0} \end{matrix} \\ \hline \mathcal{O}_{n-2,2} & \mathbb{1}_{n-2} \end{array}\right),$$

and $M_{e_j} = \mathbb{1}_n$ for $j \ge 3$, where $\mathbb{1}_k$ denotes the identity matrix of size $k \times k$ and $\mathcal{O}_{k,\ell}$ is the zero matrix of size $k \times \ell$. The element $\boldsymbol{b}$ is a non-zero vector in $(\mathbb{F}_2)^{n-2}$, which completely determines $\circ$. Once the operation is defined on the basis, it is easy to compute $a \circ b$, for $a, b \in V$.

Let r and s be two positive integers, and we will denote by $(\mathbb{F}_2)^{r\times s}$ the set of matrices of dimension $r \times s$. The following result is due to Civino et al. [14, Theorem 5.3] and characterises $H_\circ$ in the case $d = n - 2$.

Theorem 2. *Let $\boldsymbol{b} \in (\mathbb{F}_2)^{n-2}$ be as above and $\lambda \in (\mathbb{F}_2)^{n\times n}$. The following are equivalent*:

- $\lambda \in H_\circ$;
- *there exist $A \in \mathrm{GL}((\mathbb{F}_2)^2, +)$, $D \in \mathrm{GL}((\mathbb{F}_2)^d, +)$, and $B \in (\mathbb{F}_2)^{2\times d}$ such that*

$$\lambda = \begin{pmatrix} A & B \\ \mathcal{O}_{d,2} & D \end{pmatrix}$$

and $\boldsymbol{b}D = \boldsymbol{b}$.

3 Experiments on a 16-bit block cipher with 4-bit s-boxes

As anticipated, the idea of this work is to design an SPN that is weak with respect to a differential attack based on an alternative parallel operation $\circ$ for which it is possible to show that the diffusion layer of the cipher belongs to $H_\circ$. We start by explaining explicitly what we mean by *parallel*: letting $V = V_1 \oplus \ldots \oplus V_m$, with

$V_i \simeq (\mathbb{F}_2)^n$ for $i = 1, \dots, m$, and $x \in V$, we can split x into m vectors $x_1, \dots, x_m$ of n components each, and we can assume that the target SPN acting on a space of $m \times n$ bits contains m s-boxes $S_1, \dots, S_m$ such that S_1 acts on x_1, S_2 on x_2, and so on. For this reason, we aim to mount an alternative differential attack using a sum $\circ$ acting as

$$\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \circ \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} x_1 \circ_1 y_1 \\ \vdots \\ x_m \circ_m y_m \end{pmatrix},$$

where the sum $\circ_i$ acts on V_i. As explained previously, the feasibility of the attack relies on an extension of Theorem 2 to parallel sums.

In the absence of a general result in this sense, we have restricted our attention to the case where $W_{\circ_i} = \{k | k \in V_i \text{ is a weak key}\}$ has dimension $n - 2$, for $i = 1, \dots, m$, and we have performed some computational experiments using Magma [20], which we describe below.

3.1 The target cipher and its trapdoor

Fixing $V = (\mathbb{F}_2)^{16}$, $n = 4$, and $m = 4$ and letting $\circ$ be the parallel sum defined by applying each 4-bit block the alternative operation $\circ_4$ defined by the vector $\boldsymbol{b} = (0, 1)$ (see Section 2.1), we could check using Magma that the diffusion layer λ defined in Figure 1 belongs to $H_\circ$, i.e. it is a permutation that is linear with respect to to both $+$ and $\circ$. Note that the mentioned matrix, which will be chosen as the diffusion layer of the target SPN, is obtained from the cyclic shift of two 4×4 binary sub-matrices. For the benefit of the reader, we display the Cayley table of the 4-bit operation $\circ_4$ induced by the vector $\boldsymbol{b} = (0, 1)$ in Figure 2. The entries in which $a \circ_4 b$ differs from $a + b$ are highlighted.

The target cipher then features the 4-bit permutation $\gamma : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ defined in Figure 3 as its s-box.

Here, each vector is interpreted as a binary number, with most significant bit first. Precisely, four copies of γ will act in a parallel way on the 16-bit block. Note that the s-box γ is *optimal* according to Leander and Poschmann [21]. By computing the difference distribution table (DDT) of γ with respect to XOR, we obtain the result displayed in Figure 4. As it is known, γ is differentially 4-uniform, which is the best result for a permutation over $(\mathbb{F}_2)^4$ (see, e.g. Leander and Poschmann [21]).

However, if we compute the DDT using our new operation $\circ_4$ as difference operator, we obtain the result displayed in Figure 5.

We can note that γ turns out to be differentially 16-uniform with respect to $\circ_4$; in particular, when the input difference is 7_x, the output difference becomes 6_x with probability 1. Beside this, it is clear from the table that the differential behaviour of the s-box is completely different when the alternative operation is considered and the map looks far away from being non-linear as necessary.

$$\lambda = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&1&1&1\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&1&1&1&0&0&1&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&1&0&0&0&1&0&0&1&1&1&0&0&1&0\\
0&0&1&0&0&0&1&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0
\end{pmatrix}$$

Figure 1: The chosen diffusion layer.

$\circ_4$	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
1_x	1_x	0_x	3_x	2_x	5_x	4_x	7_x	6_x	9_x	8_x	B_x	A_x	D_x	C_x	F_x	E_x
2_x	2_x	3_x	0_x	1_x	6_x	7_x	4_x	5_x	A_x	B_x	8_x	9_x	E_x	F_x	C_x	D_x
3_x	3_x	2_x	1_x	0_x	7_x	6_x	5_x	4_x	B_x	A_x	9_x	8_x	F_x	E_x	D_x	C_x
4_x	4_x	5_x	6_x	7_x	0_x	1_x	2_x	3_x	D_x	C_x	F_x	E_x	9_x	8_x	B_x	A_x
5_x	5_x	4_x	7_x	6_x	1_x	0_x	3_x	2_x	C_x	D_x	E_x	F_x	8_x	9_x	A_x	B_x
6_x	6_x	7_x	4_x	5_x	2_x	3_x	0_x	1_x	F_x	E_x	D_x	C_x	B_x	A_x	9_x	8_x
7_x	7_x	6_x	5_x	4_x	3_x	2_x	1_x	0_x	E_x	F_x	C_x	D_x	A_x	B_x	8_x	9_x
8_x	8_x	9_x	A_x	B_x	D_x	C_x	F_x	E_x	0_x	1_x	2_x	3_x	5_x	4_x	7_x	6_x
9_x	9_x	8_x	B_x	A_x	C_x	D_x	E_x	F_x	1_x	0_x	3_x	2_x	4_x	5_x	6_x	7_x
A_x	A_x	B_x	8_x	9_x	F_x	E_x	D_x	C_x	2_x	3_x	0_x	1_x	7_x	6_x	5_x	4_x
B_x	B_x	A_x	9_x	8_x	E_x	F_x	C_x	D_x	3_x	2_x	1_x	0_x	6_x	7_x	4_x	5_x
C_x	C_x	D_x	E_x	F_x	9_x	8_x	B_x	A_x	5_x	4_x	7_x	6_x	0_x	1_x	2_x	3_x
D_x	D_x	C_x	F_x	E_x	8_x	9_x	A_x	B_x	4_x	5_x	6_x	7_x	1_x	0_x	3_x	2_x
E_x	E_x	F_x	C_x	D_x	B_x	A_x	9_x	8_x	7_x	6_x	5_x	4_x	2_x	3_x	0_x	1_x
F_x	F_x	E_x	D_x	C_x	A_x	B_x	8_x	9_x	6_x	7_x	4_x	5_x	3_x	2_x	1_x	0_x

Figure 2: Cayley table of $\circ_4$.

x	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
$x\gamma$	0_x	E_x	B_x	1_x	7_x	C_x	9_x	6_x	D_x	3_x	4_x	F_x	2_x	8_x	A_x	5_x

Figure 3: The chosen s-box γ.

$+$	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1_x	·	·	·	·	·	·	·	·	·	·	4	4	·	·	4	4
2_x	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2
3_x	·	4	4	·	·	4	·	4	·	·	·	·	·	·	·	·
4_x	·	·	4	·	·	·	·	4	·	·	2	2	·	·	2	2
5_x	·	4	·	·	·	4	·	·	2	2	·	·	2	2	·	·
6_x	·	·	·	·	·	·	4	4	2	2	·	·	2	2	·	·
7_x	·	·	·	·	·	·	4	4	2	2	·	·	2	2	·	·
8_x	·	·	·	4	2	2	·	·	·	·	·	·	·	4	2	2
9_x	·	·	·	4	2	2	·	·	·	·	·	·	4	·	2	2
A_x	·	2	2	·	2	·	2	·	·	2	·	2	·	2	2	·
B_x	·	2	2	·	2	·	2	·	2	·	2	·	2	·	·	2
C_x	·	2	2	·	2	·	2	·	·	2	2	·	·	2	·	2
D_x	·	2	2	·	2	·	2	·	2	·	·	2	2	·	2	·
E_x	·	·	·	4	2	2	·	·	·	4	2	2	·	·	·	·
F_x	·	·	·	4	2	2	·	·	4	·	2	2	·	·	·	·

Figure 4: DDT of γ with respect to +.

In our experiments described in the following section, we consider the SPN whose ith round is obtained by the composition of the parallel application of the s-box γ on every 4-bit block, of the diffusion layer λ defined above, and of the XOR with the ith round key.

3.2 Brute-forcing differentials

We study the difference propagation in the cipher in a long-key scenario, i.e. the key-schedule selects a random long key $k \in \mathbb{F}_2^{16r}$, where r is the number of rounds. In order to mitigate the possible bias due to a particular key choice, we run our experiments by taking the average over 2^{15} random long-key generations. This approach will provide us

$\circ_4$	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1_x	·	·	·	·	·	·	·	·	·	·	8	·	·	·	8	·
2_x	·	·	·	·	·	·	·	·	4	·	·	4	4	·	·	4
3_x	·	4	4	·	4	·	·	4	·	·	·	·	·	·	·	·
4_x	·	4	4	·	4	·	·	4	·	·	·	·	·	·	·	·
5_x	·	·	·	·	·	·	·	·	4	·	·	4	4	·	·	4
6_x	·	·	·	·	·	·	·	·	·	8	·	·	·	8	·	·
7_x	·	·	·	·	·	·	16	·	·	·	·	·	·	·	·	·
8_x	·	·	·	·	·	·	·	·	·	·	·	·	·	8	8	·
9_x	·	·	·	8	·	8	·	·	·	·	·	·	·	·	·	·
A_x	·	4	4	·	4	·	·	4	·	·	·	·	·	·	·	·
B_x	·	·	·	·	·	·	·	·	4	·	·	4	4	·	·	4
C_x	·	4	4	·	4	·	·	4	·	·	·	·	·	·	·	·
D_x	·	·	·	·	·	·	·	·	4	·	·	4	4	·	·	4
E_x	·	·	·	·	·	·	·	·	·	8	8	·	·	·	·	·
F_x	·	·	·	8	·	8	·	·	·	·	·	·	·	·	·	·

Figure 5: DDT of γ with respect to $\circ$.

with a good estimate of the expected differential probability of the best differentials on this cipher. The experimental computations, carried out by *brute-forcing* all the possible differentials, show that the best i-round differential for the classical XOR difference is always less likely than the best i-round differential computed using the mentioned parallel operation, for $i = 1, \ldots, 17$. The results, round per round, are displayed in Figure 6. In particular, when $i = 17$, the best +-differential is $0060_x \to 0700_x$ with probability $2^{-14.993}$, while using the $\circ$ difference associated to $\boldsymbol{b} = (0, 1)$, the best 17-round $\circ$-differential is $0070_x \to 0600_x$ with probability $2^{-14.411}$.

Computational evidence shows that similar results, even with a faster diffusion, can be obtained by choosing the diffusion layer of the cipher as a random matrix of $H_\circ$. This suggests that, in principle, every matrix of $H_\circ$ could represent a trapdoor diffusion layer for the cipher, with respect to a differential distinguishing attack that exploits the knowledge of the operation $\circ$.

4 Open problems

In this article, we have demonstrated that when the diffusion layer of an SPN exhibits linearity not only with respect to the XOR operation, as traditionally expected, but also in relation to an alternative operation

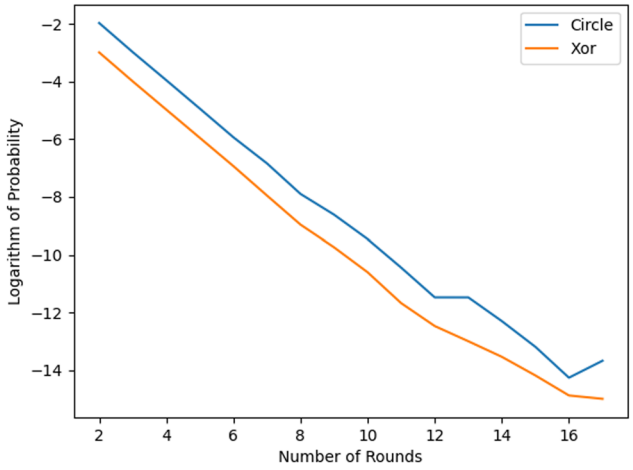

Figure 6: Best +-differential probability vs best $\circ$-differential probability.

stemming from a different translation group, this particular characteristic can be leveraged by a cryptanalyst to carry out a distinguishing attack employing alternative differentials. However, it can be quite challenging to discern which maps meet this criterion. What we require is an extension of Theorem 2 to the case of parallel operations, enabling the simultaneous targeting of all the s-boxes within the cipher and taking advantage of the lower non-linearity of the confusion layer. One potential approach to address this issue might involve attempting to represent the linear layer in a manner akin to the blocks demonstrated in Theorem 2. Based on our empirical findings, we offer the following hypothesis:

Conjecture 1. Let $V = V_1 \oplus \ldots \oplus V_m$, with $V_i \simeq (\mathbb{F}_2)^n$ for $i = 1, \ldots, m$, and let $\circ = (\circ_1, \ldots, \circ_m)$ be a parallel alternative operation as in Section 3, with $\dim(W_{\circ_i}) = n - 2$ for all i. Then, the cardinality of $H_\circ$ is at least

$$m^3 \cdot m! \cdot 3 \cdot 2^{3n-6} \prod_{h=0}^{n-4} (2^{n-3} - 2^h)[(m^2 - m)2^{n^2-5n+6} - 1].$$

This illustrates that $H_\circ$ may possess a sufficient size to contain matrices that appear to function as effective diffusion layers but, in reality, conceal trapdoor vulnerabilities.

Another crucial concern is the elimination of the assumption $d = n - 2$, as this would enable us to consider a broader range of operations. Nevertheless, as of the present writing, we are unaware of the existence of a more comprehensive version of Theorem 2 that eliminates the condition $d = n - 2$. Consequently, the prospect of an extension to the parallel case remains unknown.

In conclusion, it is evident that the influence of this approach on differential probabilities is intrinsically linked to the cipher's unique attributes. Computational evidence underscores the fact that even a minor modification in the design, such as altering the s-box or the diffusion layer, can have a profound influence on the resultant probabilities and outcomes. This heightened sensitivity to design specifics poses a challenge when attempting to establish general conjectures that can be universally applicable to different ciphers. In addition, it is important to note that these resulting probabilities are heavily contingent on the fixed alternative operations. Notably, within $\mathbb{F}_2^{16}$, a vast number of approximately 2^{27} potential parallel alternative operations can be considered, working over 4-bit blocks.

A final thought to consider is the observation that, as we have demonstrated, alternative operations have the potential to diminish the resistance of an s-box to differential cryptanalysis. This is further exemplified by the fact that a 4-bit permutation, which is considered optimal (according to the criteria in the study by Leander et al. [21]), exhibits the lowest possible differential uniformity when coupled with the operation defined in Figure 2. This raises an interesting open problem: the complete analysis of differential properties concerning alternative operations of various s-boxes, akin to what has been explored for the 4-bit permutations with respect to modular addition [22]. Even when focusing on small dimensions like 4-bit permutations, this undertaking requires some efforts. It is important to note that, in this context, there are 106 possible operations available (as detailed in the study by Calderini et al. [15, Table 1]), including the XOR. Moreover, within the same affine-equivalence class of a given s-box, different functions may exhibit varying behaviour with respect to a fixed alternative operation.

We believe that the experimental results of this article show why the mentioned problems can be of interest in this area of research in cryptanalysis.

Acknowledgements: This work has been accepted for presentation at CIFRIS23, the Congress of the Italian association of cryptography "De Componendis Cifris." M. Calderini and R. Civino are members of INdAM-GNSAGA (Italy).

Funding information: R. Civino is funded by the Centre of Excellence ExEMERGE at the University of L'Aquila.

Conflict of interest: The authors state that there is no conflict of interest.

References

[1] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. J Cryptol. 1991;4:3–72.

[2] Biham E, Biryukov A, Shamir A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. J Cryptol. 2005;18:291–311.

[3] Knudsen LR. Truncated and higher order differentials. In: Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings 2. Springer; 1995. p. 196–211.

[4] Wagner D. The boomerang attack. In: International Workshop on Fast Software Encryption. Springer; 1999. p. 156–70.

[5] Nyberg K. Differentially uniform mappings for cryptography. In: Workshop on the Theory and Application of of Cryptographic Techniques. Springer; 1993. p. 55–64.

[6] Mesnager S, Mandal B, Msahli M. Survey on recent trends towards generalized differential and boomerang uniformities. Cryptogr Commun. 2022;14:691–735.

[7] Berson TA. Differential cryptanalysis mod 2^{32} with applications to MD5. In: Advances in Cryptology–EUROCRYPT' 92. EUROCRYPT 1992. Lecture Notes in Computer Science, vol. 658. Springer, Berlin, Heidelberg; 1993.

[8] Abazari F, Sadeghian B. Cryptanalysis with ternary difference: applied to block cipher PRESENT. Cryptology ePrint Archive. 2011.

[9] Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, et al. PRESENT: an ultra-lightweight block cipher. In: Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10–13, 2007. Proceedings 9. Springer; 2007. p. 450–66.

[10] Borisov N, Chew M, Johnson R, Wagner D. Multiplicative differentials. In: Fast Software Encryption: 9th International Workshop, FSE 2002 Leuven, Belgium, February 4–6, 2002 Revised Papers 9. Springer; 2002. p. 17–33.

[11] Lai X, Massey JL. A proposal for a new block encryption standard. In: Advances in Cryptology–EUROCRYPT'90: Workshop on the Theory and Application of Cryptographic Techniques Aarhus, Denmark, May 21–24, 1990 Proceedings 9. Springer; 1991. p. 389–404.

[12] Ellingsen P, Felke P, Riera C, Stăanică P, Tkachenko A. C-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity. IEEE Trans Inform Theory. 2020;66(9):5781–9.

[13] Bartoli D, Kölsch L, Micheli G. Differential biases, c -differential uniformity, and their relation to differential attacks. 2022. arXiv: http://arXiv.org/abs/arXiv:220803884.

[14] Civino R, Blondeau C, Sala M. Differential attacks: using alternative operations. Designs Codes Cryptography. 2019;87:225–47.

[15] Calderini M, Civino R, Sala M. On properties of translation groups in the affine general linear group with applications to cryptography. J Algebra. 2021;569:658–80.

[16] Caranti A, Dalla Volta F, Sala M. On some block ciphers and imprimitive groups. Appl Algebra Eng Commun Comput. 2009;20(5-6):339–50.

[17] Brunetta C, Calderini M, Sala M. On hidden sums compatible with a given block cipher diffusion layer. Discrete Math. 2019;342(2):373–86.

[18] Aragona R, Civino R, Gavioli N, Scoppola CM. Regular subgroups with large intersection. Annali di Matematica Pura ed Applicata. 2019;198(6):2043–57.

[19] Dixon JD. Maximal abelian subgroups of the symmetric groups. Canadian J Math. 1971;23(3):426–38.

[20] Bosma W, Cannon J, Playoust C. The Magma algebra system I: the user language. J Symbolic Comput. 1997;24(3–4):235–65.

[21] Leander G, Poschmann A. On the classification of 4 bit S-boxes. In: Arithmetic of Finite Fields: First International Workshop, WAIFI 2007, Madrid, Spain, June 21–22, 2007. Proceedings 1. Springer; 2007. p. 159–76.

[22] Zajac P, Jókay M. Cryptographic properties of small bijective S-boxes with respect to modular addition. Cryptography Commun. 2020;12:947–63.