On the Impossibility of an Invariant Attack on Kuznyechik

Denis Fomin

HSE University
E-mail: dfomin@hse.ru

Abstract Currently numerous cryptographic systems are based on SP-networks. These primitives are supposed to be secure but recent investigations show that some attacks are possible. The aim of this work is to study how secure the Russian standardized block cipher Kuznyechik over invariant attacks. We study the already known decompositions of its permutation and show the ways of constructing invariant subsets. A new approach to invariant attacks is presented and it proves that there are no subsets based on S-Box properties that are invariant under round functions of Kuznyechik.

Keywords Kuznyechik · block cipher · invariant attack · nonlinear invariant · decomposition · S-Box, permutation

1 Introduction

Invariant attacks are some of the best known approaches to studing cryptographic algorithm security based on its structural properties. Modern cryptographic primitives have a round based structure, and several algorithms have been broken using this type of attack [1–3].

A lot of researches focus on the cryptographic properties of the Russian standardized block cipher Kuznyechik, [4–6]. At the same there is no proof of any practical attacks on it. The authors [4] have suggested that recently founded decompositions of the permutation of Kuznyechik may lead to some attacks on it. In this work we propose a new approach to generalizing invariant attacks based on S-Box properties of the algorithm and analyse the resistance of the Kuznyechik block cipher on it. In particular, the algebraic properties of the permutation structure was analyzed using computer evaluations. It is shown that the structure of the permutation cannot be used for proprosed variant of invariant attacks.

2 Preliminaries

Let $\mathbb{F}_q$ be a finite field of characteristic 2 with $q = 2^p$ elements, $\mathbb{F}_q^n$ — an n-dimensional vector space over $\mathbb{F}_q$. The additive group $(\mathbb{F}_q, \oplus)$ is homomorphic to the group $(\mathbb{F}_2^p, \oplus)$ with exclusive-or operator $\oplus$. By $\mathrm{GL}_m(q)$ we denote a group of $n \times n$ invertible matrices over $\mathbb{F}_q$.

Block cipher design is based on Shannon's principles of confusion and diffusion [7]. Function $F\colon \mathbb{F}_q^m \to \mathbb{F}_q^m$ of key-alternating substitution-permutation networks (SP-networks or SPN) is composed of a layer of substitution boxes (S-boxes), and a layer of bit permutations. Let

$$F_K(x) = F(x) \oplus K = \mathrm{X}[K]\left(F\left(x\right)\right)$$

be a round function (incuding the key addition), $F(x) = \mathrm{L} \circ \mathrm{S}(x)$, $x \in \mathbb{F}_q^m$, where

- $\mathrm{S}\colon \mathbb{F}_q^m \to \mathbb{F}_q^m$, $\mathrm{S}(x) = \mathrm{S}(x_1, \ldots, x_m) = (\pi(x_1), \ldots, \pi(x_m))$;
- $\mathrm{L}\colon \mathbb{F}_q^m \to \mathbb{F}_q^m$, $\mathrm{L}(x) = x \cdot L$, $L \in \mathrm{GL}_m(q)$, $L = (l_{i,j})_{m \times m}$, $l_{i,j} \in \mathbb{F}_q^*$.

Such an SP-network will be denoted as SPN*.

According to [3] the core idea of a nonlinear invariant attack is to find a function $g\colon \mathbb{F}_q^m \to \mathbb{F}_2$ so that there are many keys K:

$$g\left(F_K(x)\right) = g(x \oplus k) \oplus c = g(x) \oplus g(k) \oplus c \;\forall x \in \mathbb{F}_q^m.$$

In particular, if there is a subset $\mathcal{G}$ of $\mathbb{F}_q^m$ so that

$$\{F_K(x + a),\ x \in \mathcal{G}\} = \mathcal{G},\ \text{where } a, b \in \mathbb{F}_q^m \tag{1}$$

for a lot of keys K, the function g is an indicator function of the subset $\mathcal{G}$. This idea can be generalized as follows. Let $\mathcal{G} \subset \mathbb{F}_q^m$, $r \in \mathbb{N}$ and

$$F_{K_{i+r}} \circ \ldots \circ F_{K_i}(\mathcal{G}) = \mathcal{G}$$

for a set of vectors of keys $\{(K_i, \ldots, K_{i+r})\}$. The set $\mathcal{G}$ can be used to apply an invariant attack. The problem is how to find a way to construct such a subset. The easiest way to do it is to use the invariants of functions S and L. This paper proposes a different approach, which involves in constructing an invariant for a round transformation, which, in general, is not an invariant of S or L.

Let $\mathcal{A}$ and $\mathcal{B}$ be a pair of families of sets

$$\mathcal{A} = \{A_1, A_2, \ldots, A_{e_a}\},\ A_i \subseteq \mathbb{F}_q,$$

$$\mathcal{B} = \{B_1, B_2, \ldots, B_{e_b}\},\ B_i \subseteq \mathbb{F}_q$$

and for any $i \in \{1, \ldots, e_a\}$ there is $j \in \{1, \ldots, e_b\}$ so that $\pi\left(A_i\right) \subseteq B_j$.

If families $\mathcal{A}^m$ and $\mathcal{B}^m$ are the Cartesian product of families $\mathcal{A}$ and $\mathcal{B}$ correspondingly, then for any element $A_{i_1} \times \ldots \times A_{i_m} \in \mathcal{A}^m$, there is an element $B_{j_1} \times \ldots \times B_{j_m} \in \mathcal{B}^m$ so that

$$\mathrm{S}\left(A_{i_1} \times \ldots \times A_{i_m}\right) = (\pi(A_{i_1}) \times \ldots \times \pi(A_{i_m})) \subseteq B_{j_1} \times \ldots \times B_{j_m}.$$

Suppose that set $\mathcal{G}$ is a subset of family $\mathcal{A}^m$ and $r = 0$. That means that there is a key K so that the following diagram is true:

$$A_{i_1} \times \ldots \times A_{i_m} \xrightarrow{\mathrm{S}} \underbrace{B_{j_1} \times \ldots \times B_{j_m}}_{\in \mathcal{B}^m} \xrightarrow{\mathrm{L}} \underbrace{C}_{\in \mathcal{C}} \xrightarrow{\mathrm{X}[K]} \underbrace{A_{i_1} \times \ldots \times A_{i_m}}_{\in \mathcal{A}^m}. \tag{2}$$

An obvious consequence of this diagram is the following

Proposition 1 *Let $F\colon \mathbb{F}_q^m \to \mathbb{F}_q^m$ be a round function of a key-alternating SPN*. If there is a key K so that the diagram* (2) *is true, then the family*

$$C = \mathrm{LS}\left(A_{i_1} \times \ldots \times A_{i_m}\right)$$

has a form $C_{l_1} \times \ldots \times C_{l_m}$, where C_{l_j}, $j \in \{1, \ldots, m\}$ is a subset of a $\mathbb{F}_q$.

Using the same idea we can generalise this approach for $r \geq 0$. Let $\mathfrak{G} = (V, E)$ be an oriented graph, with vertices

$$V = \left\{ A_{i_1} \times \ldots \times A_{i_m} \,\middle|\, A_{i_j} \subseteq \mathbb{F}_q, j \in \{1, \ldots, m\} \right\}.$$

An edge $\left(A_{i'_1} \times \ldots \times A_{i'_m}, A_{i''_1} \times \ldots \times A_{i''_m}\right)$ is in E if and only if there is a key K so that

$$F_K\left(A_{i'_1} \times \ldots \times A_{i'_m}\right) = A_{i''_1} \times \ldots \times A_{i''_m}.$$

The generalization of an invariant attack is possible if there is a cycle in $\mathfrak{G}$. If diagram (2) is true then there is a loop in $\mathfrak{G}$, if $|E| = 0$ then the attack is impossible. If there is a cycle of length $r + 1$ in $\mathfrak{G}$ then the following diagram is true:

$$\begin{aligned} A_{i_1} \times \ldots \times A_{i_m} \xrightarrow{\mathrm{S}} B_{j_1} \times \ldots \times B_{j_m} \xrightarrow{\mathrm{L}} C_{l_1} \times \ldots \times C_{l_m} \xrightarrow{\mathrm{X}[K_i]} \\ \xrightarrow{\mathrm{X}[K_i]} A_{o_1} \times \ldots \times A_{o_m} \xrightarrow{\mathrm{S}} \ldots \xrightarrow{\mathrm{X}[K_{i+r}]} A_{i_1} \times \ldots \times A_{i_m}. \end{aligned} \tag{3}$$

Then $A_{i_1} \times \ldots \times A_{i_m} \in \mathcal{G}$ and

$$F_{K_{i+r}} \circ \ldots \circ F_{K_i}\left(A_{i_1} \times \ldots \times A_{i_m}\right) = A_{i_1} \times \ldots \times A_{i_m}.$$

Using the graph representation and the fact that $L \in \mathrm{GL}_m(q)$ the following proposition can be easily proved.

Proposition 2 *Let $F\colon \mathbb{F}_q^m \to \mathbb{F}_q^m$ be a round function of a key-alternating SPN*, $A' = A_{i'_1} \times \ldots \times A_{i'_m}$ and $A'' = A_{i''_1} \times \ldots \times A_{i''_m}$ be two vertices of the same cycle of graph $\mathfrak{G}$,*

$$B' = \mathrm{S}\left(A'\right),\ C' = \mathrm{LS}\left(A'\right),\ B'' = \mathrm{S}\left(A''\right),\ C'' = \mathrm{LS}\left(A''\right).$$

Then

- $B' = B_{j'_1} \times \ldots \times B_{j'_m}$, $B'' = B_{j''_1} \times \ldots \times B_{j''_m} \in \mathcal{B}^m$,
- $C' = C_{l'_1} \times \ldots \times C_{l'_m}$, $C'' = C_{l''_1} \times \ldots \times C_{l''_m} \in \mathbb{F}_q^m$,
- $\left|A_{i'_1}\right| = \ldots = \left|A_{i'_m}\right| = \left|B_{j'_1}\right| = \ldots = \left|B_{j'_m}\right| = \left|C_{l'_1}\right| = \ldots = \left|C_{l'_m}\right|$,

- $|A_{i'_1}| = |A_{i''_1}|$.

Proof Let's cosiser the cycle (3) of graph $\mathcal{G}$. Obviously $|C_{c_v}| = |A_{o_v}|$ for any $v = 1, \ldots, m$. Moreover:

$$|B_{j_v}| \geq |A_{j_v}|, \;\; v = 1, \ldots, m,$$

and because of the form of L:

$$|C_{l_v}| \geq |B_{j_w}|, \;\; v, w = 1, \ldots, m.$$

Then for any $A_{i_1} \times \ldots \times A_{i_m}$ in the cycle (3) and for any $v = 1, \ldots, m$

$$|A_{i_v}| \leq |B_{j_v}| \leq |C_{l_v}| = |A_{o_v}| \leq \ldots \leq |A_{i_v}|.$$

Let's prove that $|C_{l_1}| = |C_{l_2}|$. The remaining equalities can be proved similarly:

$$|C_{l_1}| = |A_{o_1}| \leq \ldots \leq |A_{i_1}| \leq |B_{j_1}| \leq |C_{l_2}|,$$
$$|C_{l_2}| = |A_{o_2}| \leq \ldots \leq |A_{i_2}| \leq |B_{j_2}| \leq |C_{l_1}|.$$

Using these cardinality relations it is possible to show on algebraic structure of vertices in cycles of $\mathfrak{G}$.

Theorem 1 *Let $F\colon \mathbb{F}_q^m \to \mathbb{F}_q^m$ be a round function of a key-alternating SPN*, $A_{i_1} \times \ldots \times A_{i_m}$ is a vertex of a cycle of graph $\mathfrak{G}$,*

- $\mathrm{S}\,(A_{i_1} \times \ldots \times A_{i_m}) = B_{j_1} \times \ldots \times B_{j_m}$,
- $\mathrm{L}(B_{j_1} \times \ldots \times B_{j_m}) = C_{l_1} \times \ldots \times C_{l_m}$.

Then

1. *$A_{i_z} = a_{i_z} + \mathsf{A}_{i_z}$, $B_{j_z} = b_{j_z} + \mathsf{B}_{j_z}$, $C_{l_z} = c_{l_z} + \mathsf{C}_{i_z}$ are some cosets in $(\mathbb{F}_q, \oplus)$, $z = \{1, \ldots, m\}$, where $a_{i_z}, b_{j_z}, c_{l_z} \in \mathbb{F}_1$, A_{i_z}, B_{j_z}, C_{l_z} are some subgroups of $(\mathbb{F}_q, \oplus)$;*
2. *for any $z \in \{1, \ldots, m\}$ there is $c \in \mathbb{F}_q$ where $\pi(c \oplus C_{l_z})$ is a coset of a subgroup of $(\mathbb{F}_q, \oplus)$.*

Proof To prove this theorem we show that for every j_z, $z \in \{1, \ldots, m\}$ set B_{j_z} is a coset $b_{j_z} + \mathsf{B}_{j_z}$ in $(\mathbb{F}_q, \oplus)$ of the subspace B_{j_z}. For the sets C_{l_z} the proof can be done in the same way. Then A_{i_z} is also a coset in $(\mathbb{F}_q, \oplus)$ of some subspace of the second part of the theorem is obvious.

Without losing generality, let us consider $z = 1$.

$$C_{l_1} = \left\{ \sum_{v=1}^{m} b_v \cdot l_{v,l_1} \,\middle|\, b_v \in B_{i_v}, \;\; v \in \{1, \ldots, m\} \right\}.$$

Let v', v'' be arbitrary numbers in set $\in \{1, \ldots, m\}$ and $x_v \in B_{i_v}$, $v \in \{1, \ldots, m\}$. Using the fact that $|C_{l_1}| = |B_{i_v}|$ for any $v \in \{1, \ldots, m\}$ the following equations are true:

$$C_{l_1} = \left\{ \sum_{v \in \{1, \ldots, m\} \setminus \{v'\}} x_v \cdot l_{v,l_1} \oplus y_{v'} \cdot l_{v',l_1} \,\middle|\, y_{v'} \in B_{i_{v'}} \right\},$$

$$C_{l_1} = \left\{ \sum_{v \in \{1,\ldots,m\} \setminus \{v''\}} x_v \cdot l_{v,l_1} \oplus y_{v''} \cdot l_{v'',l_1} \middle| y_{v''} \in B_{i_{v''}} \right\}.$$

Then the set

$$C'(x_{v''}) = \left\{ x_{v''} \cdot l_{v'',w} \oplus y_{v'} \cdot l_{v',w} \middle| y_{v'} \in B_{i_{v'}} \right\}$$

is equal to the set

$$C''(x_{v'}) = \left\{ x_{v'} \cdot l_{v',w} \oplus y_{v''} \cdot l_{v'',w} \middle| y_{v''} \in B_{i_{v''}} \right\}.$$

To facilitate further prove, let us write these sets in the following form:

$$C'(x_{v''}) = B_{i_{v'}} \cdot l_{v',w} \oplus x_{v''} \cdot l_{v'',w},$$

$$C''(x_{v'}) = B_{i_{v''}} \cdot l_{v'',w} \oplus x_{v'} \cdot l_{v',w}.$$

Then

$$C'(x_{v''}) = C''(x_{v'}) \ \forall \ x_{v'} \in B_{i_{v'}}, \ x_{v''} \in B_{i_{v''}}. \tag{4}$$

Using (4) we have that

$$\left(B_{i'_v} + x_{v'}\right) \cdot l_{v',w} = \left(B_{i''_v} + x_{v''}\right) \cdot l_{v'',w}.$$

Then

$$B_{i_{v'}} \oplus x_1 = B_{i_{v'}} \oplus x_2 \ \forall x_1, x_2 \in B_{i_{v'}}. \tag{5}$$

because $l_{v',w} \in \mathbb{F}_q^*$.

If $0 \in B_{i_{v'}}$then using equation (5) we have:

$$B_{i_{v'}} = B_{i_{v'}} \oplus x_1 \ \forall x_1 \in B_{i_{v'}}.$$

That means that $B_{i_{v'}}$ is closed under the operation "$\oplus$".

If $0 \notin B_{i_{v'}}$ then consider $H = x_1 \oplus B_{i_{v'}}$ for any $x_1 \in B_{i_{v'}}$. The obvious consequence is that 0 is in H. Let's show that H is closed under the operation "$\oplus$". If we fix any $x_1, x_2 \in B_{i_{v'}}$ their sum is in the set $B_{i_{v'}}$ according to the equation (5):

$$B_{i_{v'}} = B_{i_{v'}} \oplus (x_1 \oplus x_2).$$

This completes the proof.

This theorem sets up a way of finding the invariant subset $\mathcal{A}^m$. First of all we need to enumerate pairs (A_i, B_i) of coset of $(\mathbb{F}_q, \oplus)$ so that $\pi(A_i) = B_i$.

In this work we analyze the Kuznyechik block cipher that is known to be an SPN* and prove that $|E| = 0$. To prove this fact, let us first prove the following theorem.

Theorem 2 *Let $F\colon \mathbb{F}_q^m \to \mathbb{F}_q^m$ be a round function of a key-alternating SPN*, $A_{i_1}\times\ldots\times A_{i_m}$ is a vertex of a cycle of graph $\mathfrak{G}$, $B_{j_1}\times\ldots\times B_{j_m} = \mathrm{S}\left(A_{i_1}\times\ldots\times A_{i_m}\right)$. For any $z\in\{1,\ldots,m\}$ A_{i_z}, $B_{j_z} = \mathsf{B}_{j_z}\oplus b_{j_z}$ is a coset in $(\mathbb{F}_q,\oplus)$, where B_{j_z} is a subgroup, and*

$$U_z = \underbrace{\{0\}\times\ldots\times\{0\}\times\mathsf{B}_{j_z}}_{z}\times\{0\}\times\ldots\times\{0\}.$$

Then the set $W_z = \mathrm{L}\left(U_z\right)$ takes the form of:

$$W_z = W_{z_1}\times\ldots\times W_{z_m},$$

where W_{z_h} is a coset of some subgroup of $(\mathbb{F}_q,\oplus)$ so that there is a constant c_h where $\pi\left(W_{z_h}\oplus c_h\right)$ is also coset of a subgroup of $(\mathbb{F}_q,\oplus)$, $h=\{1,\ldots,m\}$.

Proof Let's consider the following set

$$B_{j_1}\times\ldots\times B_{j_m} = \mathsf{B}_{j_1}\times\ldots\times\mathsf{B}_{j_m}\oplus\left(b_{j_1},\ldots,b_{j_m}\right).$$

Without a loss of generality let's consider $h=1$.

$$\begin{aligned}\mathrm{L}(B_{j_1}\times\ldots\times B_{j_m}) &= \mathrm{L}(\mathsf{B}_{j_1}\times\ldots\times\mathsf{B}_{j_m})\oplus\mathrm{L}\left(b_{j_1},\ldots,b_{j_m}\right) = \\ &= \mathrm{L}(\{0\}\times\mathsf{B}_{j_2}\times\ldots\times\mathsf{B}_{j_m})\oplus\mathrm{L}\left(b_{j_1},\ldots,b_{j_m}\right)\oplus\mathrm{L}(U_1) = \\ &= \mathrm{L}(\{0\}\times\mathsf{B}_{j_2}\times\ldots\times\mathsf{B}_{j_m})\oplus\mathrm{L}\left(b_{j_1},\ldots,b_{j_m}\right)\oplus W_1. \quad (6)\end{aligned}$$

U_1 is a subgroup in $\mathbb{F}_q^m$ then $\mathrm{L}(U_1) = W_1$ is a subgroup in $\mathbb{F}_q^m$ too. Moreover, let

$$W_1 = \left\{\left(w_{1,1}^{(j)},\ldots,w_{1,m}^{(j)}\right)\middle| j\in\{1,\ldots,|U_1|\}\right\}.$$

Then for any $z=\{1,\ldots,m\}$ $W_{1,z} = \left\{w_{1,z}^{(j)}\middle| j\in\{1,\ldots,|U_1|\}\right\}$ is a subgroup in $\mathbb{F}_q$ because $L=(l_{i,j})_{m\times m}$, $l_{i,j}\in\mathbb{F}_q^*$.

According to theorem 1

$$\mathrm{L}(B_{j_1}\times\ldots\times B_{j_m}) = C_{l_1}\times\ldots\times C_{l_m} = \mathsf{C}_{l_1}\times\ldots\times\mathsf{C}_{l_m}\oplus(c_{l_1},\ldots,c_{l_m}), \quad (7)$$

where C_{l_z} is a subgroup in $(\mathbb{F}_q,\oplus)$, $c_{l_z}\in\mathbb{F}_q$, $z\in\{1,\ldots,m\}$. From equations (6) and (7) it follows that set W_1 is a subset in

$$\mathsf{C}_{l_1}\times\ldots\times\mathsf{C}_{l_m}\oplus(c_{l_1},\ldots,c_{l_m})\oplus\mathrm{L}\left(b_{j_1},\ldots,b_{j_m}\right)$$

because

$$(0,\ldots,0)\in\mathrm{L}(\{0\}\times\mathsf{B}_{j_2}\times\ldots\times\mathsf{B}_{j_m}).$$

At the same time $|W_{1,z}| = |\mathsf{C}_{l_1}|$ from which it follows that $\mathsf{C}_{l_1} = W_{1,z}$. Using theorem 1 this theorem is proven.

3 Kuznyechik permutation properties

Increased attention has been paid to the permutation of the Russian startedized algorithm Kuznyechik [8] in recent years. Its first decomposition was found by Alex Biryukov, Leo Perrin, and Aleksei Udovenko [9]. In this work we call it a BPU-decomposition. Some other curious properties were found in [10,4]. The BPU-decomposition has a rather simple design (see fig. 1) which can be used for an efficient implementation on various platforms [11].

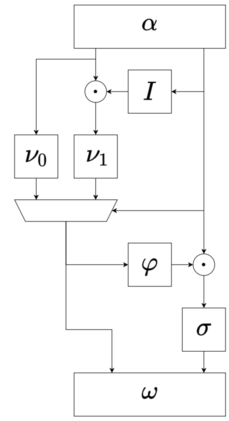

Fig. 1 BPU-decomposition, [9]

The following algorithm was found by [9] to implement the S-Box of Kuznyechik. Let $\mathbb{F}_{2^4} = GF(2^4, \cdot, \oplus) = GF(2)[y]/(f(y))$ be a finite field with 2^4 elements and an irreducible polynomial $f(y) = y^4 \oplus y^3 \oplus 1$. Every element $x \in \mathbb{F}_{2^8}$ can be considered as a concatenation of $l, r \in \mathbb{F}_{2^4}$ using a bit representation of x:

$$x = (x_1, \dots, x_8) = (l \| r), \ l = (x_1, \dots, x_4), \ r = (x_5, \dots, x_8).$$

Using this bijection, the algorithm from [9] can be presented as follows:

```
1. $(l \parallel r) := \alpha(l \parallel r)$,
2. if $r = 0$, then $l := \nu_0(l)$, else $l := \nu_1(l \cdot I(r))$;
3. $r := \sigma(r \cdot \varphi(l))$,
4. return $(l \parallel r) := \omega(l \parallel r)$,
```

where nonlinear transformations ν_0, ν_1, I, σ, φ are given in the following table (we consider that elements of $\mathbb{F}_{2^4}$ can be shown in the hexadecimal representation):

I	0,	1,	c,	8,	6,	f,	4,	e,	3,	d,	b,	a,	2,	9,	7,	5
ν_0	2,	5,	3,	b,	6,	9,	e,	a,	0,	4,	f,	1,	8,	d,	c,	7
ν_1	7,	6,	c,	9,	0,	f,	8,	1,	4,	5,	b,	e,	d,	2,	3,	a
φ	b,	2,	b,	8,	c,	4,	1,	c,	6,	3,	5,	8,	e,	3,	6,	b
σ	c,	d,	0,	4,	8,	b,	a,	e,	3,	9,	5,	2,	f,	1,	6,	7

and linear transformations α and ω are the following:

$$\alpha = \begin{pmatrix} 0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0\,1 \\ 0\,1\,0\,0\,0\,0\,1\,1 \\ 1\,1\,1\,0\,1\,1\,1\,1 \\ 1\,0\,0\,0\,1\,0\,1\,0 \\ 0\,1\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,1\,1\,0\,1\,0 \\ 0\,0\,1\,0\,0\,0\,0\,0 \end{pmatrix}, \quad \omega = \begin{pmatrix} 0\,0\,0\,0\,1\,0\,1\,0 \\ 0\,0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0\,0 \\ 1\,0\,0\,1\,1\,0\,1\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,1\,0\,0\,0\,1\,0\,0 \\ 1\,0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,1 \end{pmatrix}.$$

According to Theorem 1, we must look for a coset A_i of some subgroup of $(\mathbb{F}_q, \oplus)$, which is mapped by the S-Box to some coset B_i of a subgroup of $(\mathbb{F}_q, \oplus)$. Let us show that the BPU-decomposition allows us to extract such cosets.

Proposition 3 *For S-Box π of Kuznyechik there are two pairs of subgroups* $(\mathsf{A}_i, \mathsf{B}_i)$

- $\mathsf{A}_1 = \left\{ \alpha^{-1} \left(0\text{xd} \cdot x \| x \right) \middle| \, x \in \mathbb{F}_{2^4} \right\}$, $\mathsf{B}_1 = \left\{ \beta \left(0 \| y \right) \middle| \, y \in \mathbb{F}_{2^4} \right\}$,
- $\mathsf{A}_2 = \left\{ \alpha^{-1} \left(x \| 0 \right) \middle| \, x \in \mathbb{F}_{2^4} \right\}$, $\mathsf{B}_2 = \left\{ \beta \left(y \| 0 \right) \middle| \, y \in \mathbb{F}_{2^4} \right\}$,

so that there is $a, b \in \mathbb{F}_2^8$: $\pi(\mathsf{A}_i \oplus a) = \mathsf{B}_i \oplus b$.

Proof Let $\widehat{\pi}$ be an affine-equivalent permutation of π (see fig. 2):

$$\widehat{\pi}(x) = \omega^{-1} \left(\pi \left(\alpha^{-1}(x) \right) \oplus (0\text{x}2 \| 0\text{xc}) \right).$$

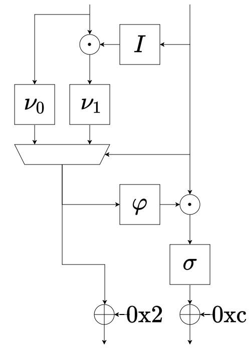

Fig. 2 Decomposition of $\widehat{\pi}$

If we show that for

- $\mathsf{A}'_1 = \left\{ \left(0\text{xd} \cdot x \| x \right) \middle| \, x \in \mathbb{F}_{2^4} \right\}$, $\mathsf{B}'_1 = \left\{ \left(0 \| y \right) \middle| \, y \in \mathbb{F}_{2^4} \right\}$,
- $\mathsf{A}'_2 = \left\{ \left(x \| 0 \right) \middle| \, x \in \mathbb{F}_{2^4} \right\}$, $\mathsf{B}'_2 = \left\{ \left(y \| 0 \right) \middle| \, y \in \mathbb{F}_{2^4} \right\}$,

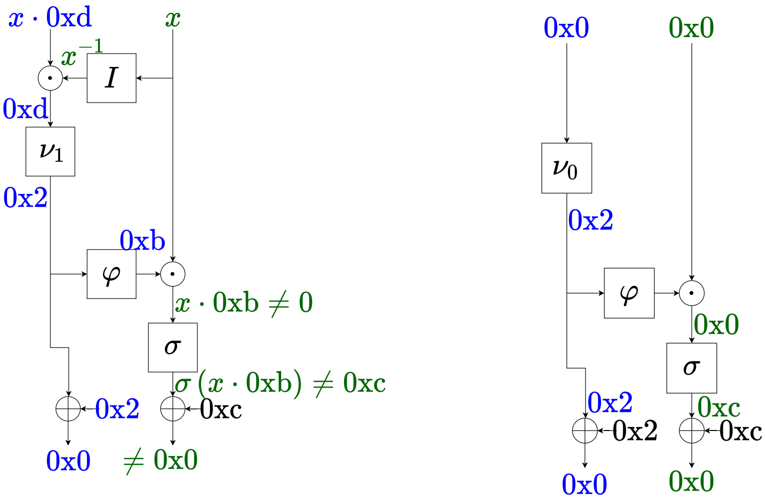

Fig. 3 $\widehat{\pi}$ maps A'_1 to B'_1

equation $\widehat{\pi}(\mathsf{A}'_i) = \mathsf{B}'_i$ is true for every $i \in \{1, 2\}$, we'll be able to prove the proposition.

Without a loss of generality, let's consider case $i = 1$ (fig. 3) case $i = 2$ can be considered similarly (fig. 4).

If x is not equal to 0, then $x{\cdot}0\mathrm{xd}{\cdot}x^{-1} = 0\mathrm{xd}$ is a constant and $\nu_1(0\mathrm{xd}) \oplus 0\mathrm{x2} = 0\mathrm{x0}$.

It's obvious that $\widehat{\pi}$ maps the set $\{(x \cdot 0\mathrm{xd} \| x),\ x \in \mathbb{F}^*_{2^4}\}$ to $\{(0 \| y),\ y \in \mathbb{F}^*_{2^4}\}$ because of the facts: $\varphi(0\mathrm{x2}) \neq 0$, $x_1 \cdot 0\mathrm{x2} = x_2 \cdot 0\mathrm{x2} \Leftrightarrow x_1 = x_2$, σ is a bijection and $\sigma(0) = 0\mathrm{xc}$.

If x is equal to 0 then $\widehat{\pi}(0 \| 0) = (0 \| 0)$.

The proved proposition only indicates that such cosets exist, but does not prove that others do not exist. To enumerate them all, let's consider an algorithm that works for any permutation. Let span(S) be a linear span of set S. Using the ideas from [12] the following algorithm can be proposed:

Algorithm 1.

```
1. $i := 0$
2. **for every** $a, b \in \mathbb{F}_q$:
   (a) $\mathsf{A}_i \leftarrow \{0\}$;
   (b) $\mathsf{B}_i \leftarrow \mathrm{span}(\pi(\mathsf{A}_i \oplus a) \oplus b)$;
   (c) $\mathsf{A}_i \leftarrow \mathrm{span}\left(\pi^{-1}(\mathsf{A}_i \oplus b) \oplus a\right)$;
   (d) **if** $\mathsf{A}_i = \mathrm{span}(\mathsf{A}_i)$ **then:**
       – **if** $|\mathsf{A}_i| \neq 2^8$, **print**$(A_i = \mathsf{A}_i \oplus a, B_i = \mathsf{B}_i \oplus b)$, $i \leftarrow i + 1$;
       – **for every** $x \in \mathbb{F}_2^8 \backslash \mathsf{A}_i$: $\mathsf{A}_i \leftarrow \mathrm{span}(\mathsf{A}_i \cup x)$, **go to step** (2.b);
```

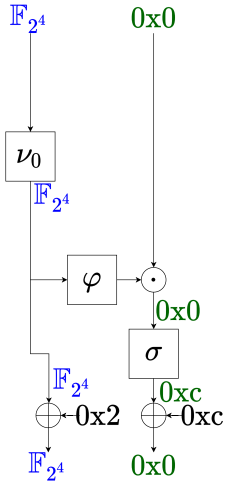

Fig. 4 Invariant subspace of $\widehat{\pi}$

Proposition 4 *Algorithm 1 is correct.*

Proof It's obvious that if there is coset $A_i \subset \mathbb{F}_2^8$ so that a permutation π maps it into coset $B_i \subset \mathbb{F}_2^8$ then algorithm 1 will print it.

Definition 1 A pair of sets $(\mathsf{A}_i, \mathsf{B}_i)$ is an I pair of sets for permutation $\pi\colon \mathbb{F}_q \to \mathbb{F}_q$ if there is $a, b \in \mathbb{F}_q$ so that

$$\pi(\mathsf{A}_i \oplus a) = \mathsf{B}_i \oplus b.$$

Subspaces A_i and B_i are called LI and RI sets for π correspondingly.

In proprosition 3 we found two I pairs of sets $(\mathsf{A}_i, \mathsf{B}_i)$ for permutation π; every set consists of 16 elements. Using algorithm 1 one can find such pairs of sets of any size. We implemented it and founded:

- 2 I pairs $(\mathsf{A}_i, \mathsf{B}_i)$, $|\mathsf{A}_i| = |\mathsf{B}_i| = 16$;
- 1 943 I pairs $(\mathsf{A}_i, \mathsf{B}_i)$, $|\mathsf{A}_i| = |\mathsf{B}_i| = 4$;
- 2 730 I pairs $(\mathsf{A}_i, \mathsf{B}_i)$, $|\mathsf{A}_i| = |\mathsf{B}_i| = 2$.

4 Impossibility attack details

Using theorem 2 we can propose the following approach to prove the impossibility of an invariant attack. Let $(\mathsf{A}_i, \mathsf{B}_i)$ be an I pair for permutation π. Consider

$$B_i^{(j)} = \underbrace{\{0\} \times \ldots \times \{0\}}_{j-1} \times \mathsf{B}_i \times \{0\} \times \ldots \times \{0\},$$

$$\mathrm{L}\left(B_i^{(j)}\right) = C_i^{(j)} = \left\{\left(c_{i,k}^{(j,1)}, \ldots, c_{i,k}^{(j,m)}\right),\ k = 1, \ldots, |\mathsf{B}_i|\right\}.$$

It follows from theorem 2 that every set

$$C_i^{(j,l)} = \left\{c_{i,k}^{(j,l)},\ k = 1, \ldots, |\mathsf{B}_i|\right\}$$

must be A_d — a subset of an LI set for π. Then

$$\exists\ c_1, c_2 \in \mathbb{F}_{2^4} : \pi\left(\mathsf{A}_d \oplus c_1\right) \oplus c_2$$

is a subgroup of $(\mathbb{F}_q, \oplus)$. Using a computer calculation and the ideas presented above we proved the following

Proposition 5 *Let π be a permutation,* L *be a linear and* S *be a nonlinear transformation of the Kuznyechik algorithm. Then for every I pair $(\mathsf{A}_i, \mathsf{B}_i)$, $|\mathsf{B}_i| > 1$, for permutation π and for every $j = \{1, \ldots, m\}$, there is $l = \{1, \ldots, m\}$ so that $C_i^{(j,l)}$ is not a subset of any subgroup A_d so that*

$$\exists\ c_1, c_2 \in \mathbb{F}_{2^4} : \pi\left(\mathsf{A}_d \oplus c_1\right) \oplus c_2$$

is a subgroup of $(\mathbb{F}_q, \oplus)$.

Let's consider the most interesting example and take into account an I pair of sets $(\mathsf{A}_i, \mathsf{B}_i)$ proposition 3:

- $\mathsf{A}_1 = \{$0x00, 0x05, 0x22, 0x27, 0x49, 0x4c, 0x6b, 0x6e, 0x8b, 0x8e, 0xa9, 0xac, 0xc2, 0xc7, 0xe0, 0xe5$\}$, $\mathsf{B}_1 = \{$0x00, 0x01, 0x0a, 0x0b, 0x44, 0x45, 0x4e, 0x4f, 0x92, 0x93, 0x98, 0x99, 0xd6, 0xd7, 0xdc, 0xdd$\}$;
- $\mathsf{A}_2 = \{$0x00, 0x01, 0x0a, 0x0b, 0x44, 0x45, 0x4e, 0x4f, 0x92, 0x93, 0x98, 0x99, 0xd6, 0xd7, 0xdc, 0xdd$\}$, $\mathsf{B}_2 = \{$0x00, 0x02, 0x04, 0x06, 0x10, 0x12, 0x14, 0x16, 0x20, 0x22, 0x24, 0x26, 0x30, 0x32, 0x34, 0x36$\}$;

There are the largest LI and RI sets for π. We also can mention that $\mathsf{B}_1 = \mathsf{A}_2$. If we consider

$$B_1^1 = \mathsf{B}_1 \times \{0\} \times \ldots \times \{0\}$$

then $C_1^{1,1} = \mathsf{B}_1 = \mathsf{A}_2$ because according to [8] the linear transformation of Kuznyechik is based on LFSR with the least feedback coefficient equal to $e \in \mathbb{F}_2^8$. At the same time neither $C_1^{1,2} \neq \mathsf{A}_1 \oplus a$ nor $C_1^{1,2} \neq \mathsf{A}_2 \oplus a$ for any $a \in \mathbb{F}_{2^8}$ which means that A_{i_1} in $\mathcal{G}$ is not $\mathsf{A}_1 \oplus c$ for any $c \in \mathbb{F}_{2^8}$. Much simpler:

$$B_2^1 = \mathsf{B}_2 \times \{0\} \times \ldots \times \{0\}.$$

In this case $C_2^{1,1} = \mathsf{B}_2 \neq \mathsf{A}_1$ and $C_2^{1,1} = \mathsf{B}_2 \neq \mathsf{A}_1$.

5 Conclusion

We presented a new approach to invariant attacks based on S-box properties of an SPN*. Kuznyechik is an SPN* since it has a linear layer based on an MDS-matrix. Using a computer calculation we enumerated all I pairs for permutation π of the Kuznyechik algorithm and proved the impossibility of a generalised invariant attack.

References

1. Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. In Phillip Rogaway, editor, *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 206–221. Springer, 2011.
2. Gregor Leander, Brice Minaud, and Sondre Rønjom. A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro. *IACR Cryptology ePrint Archive*, 2015:68, 2015.
3. Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear Invariant Attack – Practical Attack on Full SCREAM, iSCREAM, and Midori64. Cryptology ePrint Archive, Report 2016/732, 2016. `https://eprint.iacr.org/2016/732`.
4. Léo Perrin. Partitions in the S-Box of Streebog and Kuznyechik. *IACR Cryptology ePrint Archive*, 2019:92, 2019.
5. Vitaly Kiryukhin. An algorithm for bounding non-minimum weight differentials in 2-round LSX-ciphers. Cryptology ePrint Archive, Report 2020/1208, 2020. `https://eprint.iacr.org/2020/1208`.
6. Riham AlTawy and Amr M. Youssef. A Meet in the Middle Attack on Reduced Round Kuznyechik. Cryptology ePrint Archive, Report 2015/096, 2015. `https://eprint.iacr.org/2015/096`.
7. Henk C. A. van Tilborg, editor. *Encyclopedia of Cryptography and Security*. Springer, 2005.
8. GOST R 34.12-2015 Information technology. Cryptographic data security. Block ciphers., 2015.
9. Alex Biryukov, Léo Perrin, and Aleksei Udovenko. Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT (1)*, volume 9665 of *Lecture Notes in Computer Science*, pages 372–402. Springer, 2016.
10. Léo Perrin and Aleksei Udovenko. Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog. *IACR Trans. Symmetric Cryptol.*, 2016(2):99–124, 2016.
11. Alexander Smirnov Denis Fomin Olga Avraamova, Vladimir Serov and Vasily Shokhov. A Compact Bit-sliced Representation of Kuznechik S-box. In *CTCrypt'20*, 2020.
12. Gregor Leander. On Invariant Attacks. 2019. Invited talk.