On the Impossibility of an Invariant Attack on Kuznyechik

Denis Fomin

dfomin@hse.ru

HSE University

June 3, 2021

Preliminaries

Let function $F\colon \mathbb{F}_q^m \to \mathbb{F}_q^m$ be a key-alternating substitution-permutation networks (SP-networks or SPN). We suppose that F 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), $F(x) = \mathrm{L} \circ \mathrm{S}(x)$, 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*.

Invariant attacks

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

$$\{F_K(x),\ x \in \mathcal{G}\} = \mathcal{G} \text{ (or for the simplicity } F_K(\mathcal{G}) = \mathcal{G}). \tag{1}$$

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.

Set $\mathcal{G}$ construction I

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 $\pi(A_i) \subseteq B_j$.
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

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

Set $\mathcal{G}$ construction II

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

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*

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

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 $\mathbb{F}_q$.

Set $\mathcal{G}$ construction III

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.

Set $\mathcal{G}$ construction IV

If there is a cycle of length $r+1$ in $\mathfrak{G}$ then the following diagram is true:

$$A_{i_1} \times \ldots \times A_{i_m} \xrightarrow{\mathrm{S}} B_{j_1} \times \ldots \times B_{j_m} \xrightarrow{\mathrm{L}} C_{l_1} \times \ldots \times C_{l_k} \xrightarrow{\mathrm{X}[K_i]}$$

$$\xrightarrow{\mathrm{X}[K_i]} A_{o_1} \times \ldots \times A_{o_k} \xrightarrow{\mathrm{X}[K_{i+r}]} \ldots \xrightarrow{\mathrm{X}[K_{i+r}]} A_{i_1} \times \ldots \times A_{i_m}.$$

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

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

Set $\mathcal{G}$ construction V

Proposition

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* $\mathfrak{G}$*,*

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

Then

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

Set $\mathcal{G}$ construction VI

Theorem

Let $F : \mathbb{F}_q^m \to \mathbb{F}_q^m$ 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 $\mathfrak{G}$,*

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

Then

1. A_{i_z}, B_{j_z}, C_{l_z} *are some cosets of* $(\mathbb{F}_q, \oplus)$, $z = \{1, \ldots, m\}$;
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* $(\mathbb{F}_q, \oplus)$.

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

Set $\mathcal{G}$ construction VII

Theorem

Let $F : \mathbb{F}_q^m \to \mathbb{F}_q^m$ *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 of* $(\mathbb{F}_q, \oplus)$, B_{j_z} *is a subgroup, and*

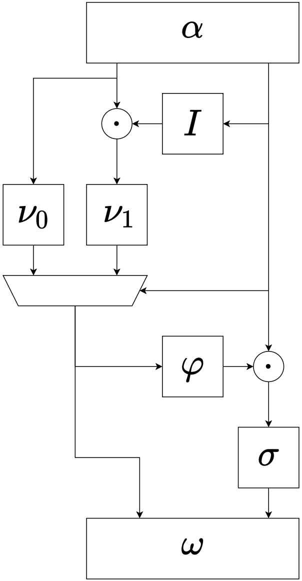
$$U_z = \underbrace{\{0\} \times \ldots \times \{0\} \times \mathsf{B}_{j_z}}_{z} \times \{0\} \times \ldots \times \{0\}.$$

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

Kuznyechik permutation properties I



The TU-decomposition was first presented in “Reverse-engineering the SBox of Streebog, Kuznyechik and STRIBOBr1” by Alex Biryukov, Leo Perrin, and Aleksei Udovenko., 2016

It consists of:

- linear transformations $V_8 \to V_8$: α and ω
- non-linear transformations $V_4 \to V_4$: ν_0, ν_1, I, σ, φ
- multiplication in Galois field $GF\left(2^4, \odot, \oplus\right) = GF(2)[x]/(f(x))$ with irreducible polynomial $f(x) = x^4 \oplus x^3 \oplus 1$
- multiplexer (if-else construction)

Kuznyechik permutation properties II

According to Theorem 1, we must look for coset A_i, which is mapped by the S-Box to some coset B_i. Let us show that the BPU-decomposition allows us to extract such cosets.

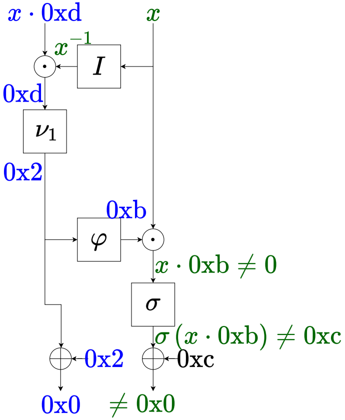
Proposition

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

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

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

Kuznyechik permutation properties III



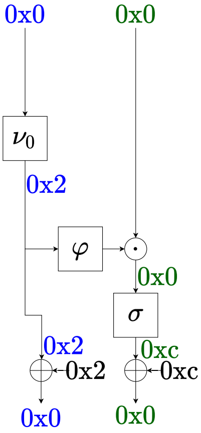


Figure: $\widehat{\pi}$ maps A'_1 to B'_1

Kuznyechik permutation properties IV

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 [**?**] the following algorithm can be proposed:

Algorithm 1. (Naive)

```
1 $i := 0$
2 **for every** $a, b \in \mathbb{F}_q$:
    1 $\mathsf{A}_i \leftarrow \{0\}$;
    2 $\mathsf{B}_i \leftarrow \text{span}\left(\pi\left(\mathsf{A}_i \oplus a\right) \oplus b\right)$;
    3 $\mathsf{A}_i \leftarrow \text{span}\left(\pi^{-1}\left(\mathsf{A}_i \oplus b\right) \oplus a\right)$;
    4 **if** $\mathsf{A}_i = \text{span}(\mathsf{A}_i)$ **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** $x \in \mathbb{F}_2^8 \backslash \mathsf{A}_i$: $\mathsf{A}_i \leftarrow \text{span}\left(\mathsf{A}_i \cup x\right)$, **go to step** (2.b);
```

Kuznyechik permutation properties V

Definition

A pair of sets $(\mathsf{A}_i, \mathsf{B}_i)$ is an I pair of sets for permutation $\pi : \mathbb{F}_q \to \mathbb{F}_q$ 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 $(\mathsf{A}_i, \mathsf{B}_i)$, $|\mathsf{A}_i| = |\mathsf{B}_i| = 2$.

Impossibility attack details I

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 $(\mathbb{F}_q, \oplus)$.

Impossibility attack details II

Using a computer calculation and the ideas presented above we proved the following

Proposition

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 $(\mathbb{F}_q, \oplus)$.

Impossibility attack details III

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 $\mathsf{B}_1 = \mathsf{A}_2$.

Impossibility attack details IV

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

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.