

Invariant Subspace Attack on the GOST 28147-89 Block Cipher

June 4, 2026

Stepan Davydov, Ph. D.,
JSRPC Kryptonite

1. Introduction

2. Invariant subspace method

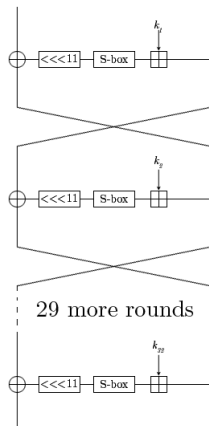
3. Attack on the GOST 28147-89

[1/3] Introduction

GOST 28147-89

GOST 28147-89:

1. 32-round Feistel network
2. 64-bit block, 256-bit key
3. Key addition $\boxplus$ modulo 2^{32}
4. 8 4-bit S-boxes ($S_1, \dots, S_8$)
5. Cyclic rotation on 11



Round keys are $K_1, K_2, \dots, K_8, K_1, K_2, \dots, K_8, K_1, K_2, \dots, K_8, K_8, K_7, \dots, K_2, K_1$

S-boxes are not defined by the
standard!¹

¹GOST 28147-89. Information processing systems. Cryptographic protection. Cryptographic transformation algorithm. 1989 (canceled in 2019)

1. 8 different S-boxes:²
 - ▶ id-Gost28147-89-CryptoPro-A-ParamSet
 - ▶ ...
2. id-Gost28147-89-CryptoPro-Z-ParamSet (MAGMA block cipher)³
3. Using one PRESENT S-box Axel Poschman 2010⁴
4. Using two different S-boxes 2-GOST ⁵

²RFC 4357

³GOST 34.12-2018, RFC 7836

⁴A. Poschmann, S. Ling, H. Wang. 256 Bit Standardized Crypto for 650 GE — GOST Revisited. Cryptographic Hardware and Embedded Systems, CHES 2010.

⁵A. A. Dmukh, D. M. Dygin, G. B. Marshalko, "A lightweight-friendly modification of GOST block cipher Math. vops. cryptogr., 5:2 (2014), 47–55

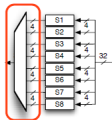
One S-box for lightweight implementation

Implementation Results I



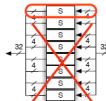
UMCL18G212T3 library

GOST-FB

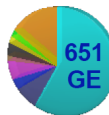
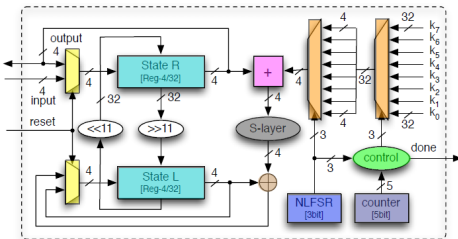


serial 264 CLK

GOST-PS



serial 264 CLK



[2/3] Invariant subspace method

Invariant subspace method

If for some $u \in V_n$
 $F(W) = W$ and $k \in W \Rightarrow$

$$F(W + k) = F(W) = W$$

If every round key $k_i \in W$

$$E_K(W) = W$$

Leander, G., Abdelraheem, M.A., AlKhzaimi, H., Zenner, E. (2011). A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. In: Rogaway, P. (eds) Advances in Cryptology – CRYPTO 2011. Lecture Notes in Computer Science, vol 6841. Springer, Berlin, Heidelberg.

Invariant subspace method

$$\mathbf{S} = (S_1, \dots, S_m)$$

$$\mathbf{F} = \mathbf{S} \cdot \mathbf{L}$$

How can we find invariant subspace of $\mathbf{F}$?

- ▶ Invariant subspaces of $\mathbf{S}$
- ▶ Invariant subspaces of $\mathbf{L}$

Let $\mathbb{F}_{2^s}$ be a symmetric group on $\mathbb{F}_{2^s}$

Definition

If $W < \mathbb{F}_{2^s}^m$ is invariant subspace of any $S = (S, S, \dots, S)$, $S \in \text{Sym}(\mathbb{F}_{2^s})$ then W is *type 1* invariant subspace.

GOST LT is defined by circulant matrix

$$M_{32 \times 32} = \begin{pmatrix} 0 & \dots & 0 & 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 1 & 0 & \dots & 0 \end{pmatrix} \in (\mathbb{F}_2)_{32,32},$$

$$M_{32 \times 32} = \text{Circ}_2(c_1, \dots, c_{32}), \quad c_{22} = 1, \quad c_i = 0, i \in \overline{1, 32} \setminus \{22\}$$

Matrix B

Let

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\otimes k} \in \mathbb{P}_{2^k, 2^k},$$

where $\otimes k$ means Kronecker exponentiation.

Example

matrix B , $k = 2$

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

Theorem (VolKru17⁶)

The next subspaces are invariant for any circulant $2^k \times 2^k$ matrix over field $\mathbb{P}$

$$\langle \vec{B}_{2^k} \rangle, \langle \vec{B}_{2^k}, \vec{B}_{2^{k-1}} \rangle, \langle \vec{B}_{2^k}, \vec{B}_{2^{k-1}}, \vec{B}_{2^{k-2}} \rangle, \dots, \langle \vec{B}_{2^k}, \vec{B}_{2^{k-1}}, \vec{B}_{2^{k-2}}, \dots, \vec{B}_1 \rangle. \quad (1)$$

Every subspace in chain

$$\langle \vec{B}_{2^k} \rangle, \langle \vec{B}_{2^k}, \vec{B}_{2^{k-1}} \rangle, \langle \vec{B}_{2^k}, \vec{B}_{2^{k-1}}, \vec{B}_{2^{k-2}} \rangle, \dots, \langle \vec{B}_{2^k}, \vec{B}_{2^{k-1}}, \vec{B}_{2^{k-2}}, \dots, \vec{B}_{2^{k-1}} \rangle \quad (2)$$

is **type 1 invariant subspace**.

⁶A. Volgin, G. Kryuchkov, "Characterization of linear transformations defined by Finite Field Hadamard Matrices and circulant matrices", Prikl. Diskr. Mat. Suppl., 2017, no. 10, 10–11. In Russian.

Theorem (SD24⁷)

- ▶ Let $\mathbb{P} = \mathbb{F}_{2^s}$, $r \in \mathbb{N}$, $C = \text{Circ}_{2^s}(c_{2^k-1}, \dots, c_0) \in \mathbb{P}_{2^k, 2^k}$ and $c_2 + c_4 + c_6 + \dots + c_{2^k} \neq 0$.
- ▶ Then only (1) are invariant subspaces of matrix C .

Corollary

- ▶ If $C = \text{Circ}(c_1, \dots, c_{2^k}) \in \mathbb{P}_{2^k, 2^k}$ is **MDS** matrix,
- ▶ then only (1) are invariant subspaces of C .

⁷S. Davydov, “Invariant subspaces of circulant and recursive matrices”, Diskr. Mat., 36:4 (2024), 44–63. In Russian.

Invariant subspaces of GOST 28147-89

We consider field $\mathbb{F}_2$

Example

- ▶ In GOST 28147-89 block cipher $c_{22} = 1$, $c_i = 0$ $i \neq 22$.
- ▶ Only (1) are invariant subspaces of GOST matrix.
- ▶ Only (2) are *type 1* invariant subspaces of GOST matrix.

We consider field $\mathbb{F}_{2^4}$

Example

- ▶ Only subspaces whose dimension is a multiple of 4 from (2) are *type 1* invariant subspaces of GOST matrix.
- ▶ $W^{(16)} = \langle \vec{B}_{32}, \vec{B}_{31}, \dots, \vec{B}_{17} \rangle$ is a maximal subspace having the given property.
- ▶ $W^{(16)} = \{(a, b, c, d, a, b, c, d) | a, b, c, d \in \mathbb{F}_{2^4}\}.$

Corollary

- ▶ $W^{(16)}$ is invariant under cyclic rotation on 11 and nonlinear transformation $\mathbf{S} = (S, S, \dots, S)$, $S \in \text{Sym}(\mathbb{F}_{2^4})$.
- ▶ In general, $W^{(16)}$ is invariant under $\mathbf{S} = (S_1, S_2, \dots, S_8)$ with $S_1 = S_5, S_2 = S_6, S_3 = S_7, S_4 = S_8$.

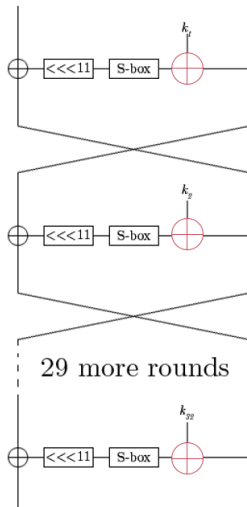
[3/3] Attack on the GOST 28147-89

GOST 28147-89 with XOR keys and one S-box

$A^{\times k}$ — Cartesian power of A

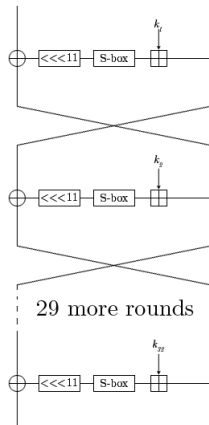
- ▶ We replace keys addition modulo 2^{32} on XOR keys addition
- ▶ Let input block be (L_1, R_1) , $L_1, R_1 \in W^{(16)}$ and all the round keys $K_i \in W^{(16)}$.
- ▶ After the first round holds $(L_2, R_2) \in W^{(16) \times 2}$.
- ▶ ...
- ▶ After the last round holds $(L_{33}, R_{33}) \in W^{(16) \times 2}$.

The attack is straightforward!



GOST 28147-89 with one S-box

- ▶ Let $(L_j, R_j) \in W^{(16) \times 2}$ and $K_i \in W^{(16)}$,
is $R_j \boxplus K_i \in W^{(16)}$?
- ▶ $K_i = (a_i, b_i, c_i, d_i, a_i, b_i, c_i, d_i)$,
 $R_j = (a_j, b_j, c_j, d_j, a_j, b_j, c_j, d_j)$.
- ▶ **We need** $k_i + r_j < 2^{16}$, where
 $k_i = 2^{12}a_i + 2^8b_i + 2^4c_i + d_i$ and
 $r_j = 2^{12}a_j + 2^8b_j + 2^4c_j + d_j$,
 k_i, r_j are integer, "+" is an integer addition.



GOST 28147-89 with one S-box

$$\Pr\{k_i + r_j < 2^{16}\} = \Pr\{r_j < 2^{16} - k_i\} = \frac{2^{16} - k_i}{2^{16}}.$$

Let A be an event $\{(L_{33}, R_{33}) \in W^{(16) \times 2} | (L_1, R_1) \in W^{(16) \times 2}\}$.

For fixed $(K_1, \dots, K_8) \in W^{(16) \times 8}$:

$$\Pr\{A | (K_1, \dots, K_8)\} = \prod_{i=1}^8 \left(\frac{2^{16} - k_i}{2^{16}} \right)^4.$$

An **average** probability for $(K_1, \dots, K_8) \in W^{(16) \times 8}$:

$$\begin{aligned} \Pr\{A|K_i \in W^{(16)}, i \in \overline{1,8}\} &= \frac{1}{2^{128}} \sum_{k_1=0}^{2^{16}-1} \dots \sum_{k_8=0}^{2^{16}-1} \prod_{i=1}^8 \left(\frac{2^{16} - k_i}{2^{16}} \right)^4 = \\ &= \frac{1}{2^{128+512}} \sum_{k_1=1}^{2^{16}} \dots \sum_{k_8=1}^{2^{16}} \prod_{i=1}^8 k_i^4 = \frac{1}{2^{640}} \prod_{i=1}^8 \sum_{k_i=1}^{2^{16}} k_i^4 = \frac{1}{2^{640}} \left(\sum_{k=1}^{2^{16}} k^4 \right)^8 \approx 1,34 \cdot 2^{-19} \end{aligned} \quad (3)$$

GOST 28147-89 with one S-box

Another classes of **weak keys**:

$$W_j^{(16)} = \{(a, b, c, d, a, b, c, d) \mid a, b, c, d \in \mathbb{F}_{2^4}, a = \underbrace{(0, \dots, 0)}_j, *) \in V_4\}.$$

The «**worst**» key in $W_j^{(16)}$: $k_i = 2^{16-j} - 1, i \in \overline{1, 8}$.

For worst key:

$$\Pr\{A \mid k_i = 2^{16-j} - 1, i \in \overline{1, 8}\} = \left(\frac{2^{16} - 2^{16-j} + 1}{2^{16}} \right)^{32} \approx (1 - 2^{-j})^{32}$$

GOST 28147-89 with one S-box

- ▶ We need $P = (L_1, R_1) \in W^{(16) \times 2}$ and ciphertext $(L_{33}, R_{33}) = E_K(L_1, R_1)$.
- ▶ If $K \in W^{(16) \times 8}$ then $(L_{33}, R_{33}) \in W^{(16) \times 2}$ with prob. $p_1 = 1,34 \cdot 2^{-19}$.
- ▶ If $K \notin W^{(16) \times 8}$ then $(L_{33}, R_{33}) \in W^{(16) \times 2}$ with prob. $\frac{|W^{(16) \times 2}|}{2^{64}} = p_2 = 2^{-32}$.
- ▶ Let us consider $\text{Bin}(n, p_1), \text{Bin}(n, p_2)$
- ▶ Let us choose type I error $\alpha = 0.05$ type II error $\beta = 0.05$ and estimate n – the number of chosen PT/CT
- ▶ If we have at least 1 event A we decide $K \in W^{(16) \times 8}$
- ▶ We don't need additional computation or memory

GOST 28147-89 with one S-box

Condit. for $K_i, i \in \overline{1,8}$	Weak keys	$\Pr(A)$ (aver. case)	$\Pr(A)$ (worst case)	Number of chosen PT/CT ($\alpha = \beta = 0.05$)	Number of success exp./ all exp.
$K_i \in W^{(16)}$	2^{128}	$1,34 \cdot 2^{-19}$	impossible	$1,12 \cdot 2^{20}$	10/10
$K_i \in W_1^{(16)}$	2^{120}	$1,04 \cdot 2^{-11}$	2^{-32}	$1,44 \cdot 2^{12}$	10/10
$K_i \in W_2^{(16)}$	2^{112}	$1,08 \cdot 2^{-4}$	$1,64 \cdot 2^{-14}$	43	8/10
$K_i \in W_3^{(16)}$	2^{104}	$1,09 \cdot 2^{-3}$	$1,78 \cdot 2^{-7}$	21	9/10
$K_i \in W_8^{(16)}$	2^{64}	—	0,88	2	10/10

1. **Trivial** key schedule provides conditions for **invariant subspace attack**.
2. Modular **key addition** « $\boxplus$ » makes the **attack** more **hard**, but **possible**.
3. Attack is possible only if $S_1 = S_5, S_2 = S_6, S_3 = S_7, S_4 = S_8$.
4. Attack is **impossible** in cases of:
 - ▶ S-boxes from **RFC 4357**,
 - ▶ **Magma** block cipher (**all subspaces** $W : F(W) = W$ are checked),
 - ▶ **2-GOST** block cipher (**all subspaces** $W : F(W) = W$ are checked).

Another subspaces

What can we obtain in case of another subspaces?

$$W^{(28)} = \langle \vec{B}_{32}, \vec{B}_{31}, \vec{B}_{30}, \dots, \vec{B}_5 \rangle,$$

$$W^{(31)} = \langle \vec{B}_{32}, \vec{B}_{31}, \vec{B}_{30}, \dots, \vec{B}_2 \rangle.$$

It is easy to check

$$W^{(28)} = \{(a_1, a_2, a_3, \dots, a_8) | a_i \in \mathbb{F}_{2^4}, i \in \overline{1, 8}, \sum_{j=1}^8 a_j = 0\},$$

$$W^{(31)} = \{(a_1, a_2, a_3, \dots, a_{32}) | a_i \in \mathbb{F}_2, i \in \overline{1, 32}, \sum_{j=1}^{32} a_j = 0\}.$$

Differential uniformity

In case of $W^{(28)}$:

$$\sum_{j=1}^8 a_j = a \Rightarrow \sum_{j=1}^8 S_j(a_j) = b.$$

For any **fixed** $(a_3, a_4, \dots, a_8)$ we obtain

$$a_1 + a_2 = a' \Rightarrow S_1(a_1) + S_2(a_2) = b'$$

or

$$S_1(a_1) + S_2(a_1 + a') = b'$$

for some a', b' and any a_1 .

In case of $W^{(31)}$:

$$\sum_{j=1}^{32} a_j = a \Rightarrow \sum_{j=1}^{32} b_j = b, \mathbf{S}(a_1, \dots, a_{32}) = (b_1, \dots, b_{32}),$$

$$a_i, b_j \in \mathbb{F}_2, i, j \in \overline{1, 32}.$$

We **obtain** $\langle \alpha, x \rangle = \langle \beta, \overline{S}(x) \rangle$ for $\alpha = \beta = (1, 1, \dots, 1)$,

$\langle \alpha, x \rangle$ — scalar product.

Abdelraheem, M.A., Ågren, M., Beelen, P., Leander, G. (2012). On the Distribution of Linear Biases: Three Instructive Examples. In: Safavi-Naini, R., Canetti, R. (eds) Advances in Cryptology – CRYPTO 2012. CRYPTO 2012. Lecture Notes in Computer Science, vol 7417. Springer, Berlin, Heidelberg.

Thanks for your attention! Questions?

Stepan Davydov, Ph. D.,

JSRPC Kryptonite

s.davydov@kryptonite.ru

