КРИПТОНИТ

Invariant subspaces of the circulant matrices

Stepan Davydov

JSRPC «Kryptonite»
Lomonosov MSU

CTCrypt 2024

Table of contents

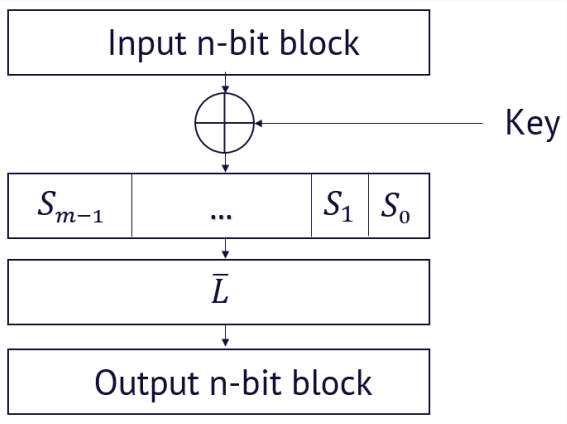
Introduction

XSL-schemes

$\mathbb{F}_{q^s}$ — finite field of q^s elements, $V_n = \{0,1\}^n$,

$Q_{n,n}$ is ring of square $n \times n$ matrices over field Q

n-bit block, s-bit S-boxes, $n = ms$

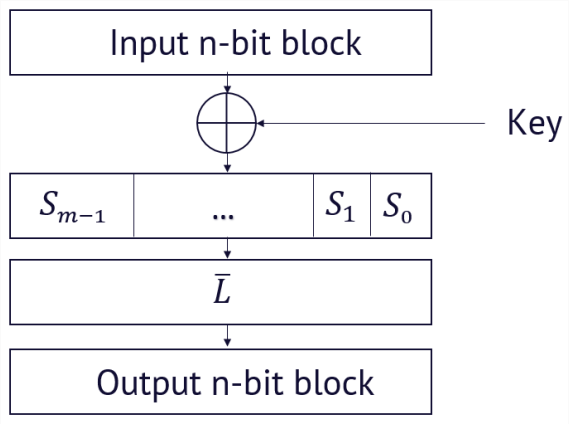


Round of the XSL-scheme:

- Key addition XOR
- Nonlinear transformation $\overline{S} = (S_{m-1}, ..., S_0)$
- Linear transformation $\overline{L}$

Synonyms of the XSL-schemes: SP-network, XSPL, LSX

XSL-schemes



XSL-schemes in block ciphers and hash functions:

- Kuznyechik (XSL)
- AES (XSPL, P – ShiftRows, L – MixColumns)
- SM4 (Feistel network with four 32-bit blocks)
- DES (Feistel network with SP)
- Streebog (XSPL)
- Whirlpool (XSPL)

The Invariant Subspace Attack

The Invariant Subspace Attack

The next approach was proposed at Advances in Cryptology - CRYPTO 2011[1].

Let $F_k(u) = F(u + k)$ be a round function of the XSL-scheme

$$F = \overline{S}\,\overline{L} : V_n \to V_n$$

If there exist subspace $W < V_n$ and constants $c, d \in V_n$ such that

$$F(W + c) = W + d$$

then any round key $k \in W + c + d$ is «weak», since
$F_k(W + d) = F(W + c) = W + d$.

[1] 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.

The Invariant Subspace Attack

Definition

Let $F : V_n \to V_n$. We say subspace $W < V_n$ is invariant subspace of the bijective transformation F, if there exist constants $c, d \in V_n$ such that $F(W + c) = W + d$.

Remark

In case of the linear bijective transformation L proposed definition is equivalent to classic invariant subspace definition ($L(W) = W$).

The Invariant Subspace Attack

Remark

It is important that every round key should be weak ($k \in W + c + d$) in the invariant subspace attack.

$$F_k(W + d) = F(W + c) = W + d \Rightarrow$$

$$Enc_K(W + d) = W + d$$

Some attacks were proposed on the following block ciphers: PRINT, Robin, CAESAR, ZORRO, Midori64, Khazad.

The Invariant Subspace Attack

Easy way to construct invariant subspace is to find among both $\overline{S}$ and $\overline{L}$ invariants (we denote $\overline{S} \bigcap \overline{L}$).

Let $\overline{S} = (S, ..., S)$.

The next subspaces (examples) from $\overline{S} \bigcap \overline{L}$ were found for Khazad block cipher (Hadamard matrix used), which provides attack on 6 of 8 rounds of the Khazad block cipher[2].

$$W^{(1)} = \{(a, a, b, b, e, e, d, d) \mid a, b, e, d \in \mathbb{F}_{2^8}\}$$

$$W^{(2)} = \{(a, b, a, b, e, d, e, d) \mid a, b, e, d \in \mathbb{F}_{2^8}\}$$

$$U^{(1)} = \{(a, a, a, a, b, b, b, b) \mid a, b \in \mathbb{F}_{2^8}\}$$

[2] D. A. Burov, B. A. Pogorelov, “An attack on 6 rounds of Khazad”, Матем. вопр. криптогр., 7:2 (2016), 35–46

The Invariant Subspaces

We denote the next subspaces of V_{2s}: $W_{(\alpha,\alpha)} = \{(\alpha,\alpha), \alpha \in V_s\}$, $W_{(0,\alpha)} = \{(0,\alpha), \alpha \in V_s\}$, $W_{(\alpha,0)} = \{(\alpha,0), \alpha \in V_s\}$.

Proposition

Let $W < V_{ms}$ be subspace of dimension d, W_{jk} is projection W on j,k coordinates.

Subspace W is invariant under any transformation $\overline{S} = (S,S,...,S)$, $S : V_s \to V_s$ if and only if

for any j,k the W_{jk} subspace is one of the next subspaces: $\{(0,0)\}, W_{(\alpha,0)}, W_{(0,\alpha)}, W_{(\alpha,\alpha)}, V_{2s}$.

Definition

In case of proposition we say W is subspace of *type 1*.

Nonlinear invariants

At ASIACRYPT 2016 conference using nonlinear invariants was proposed [3].

Authors proposed to find the next $F = \overline{SL}$ function invariants:

$$g : V_n \to V_1,\ g(F(x)) + g(x) \equiv c$$

Namely, the next invariants were used for constructing attack on the SCREAM, iSCREAM and Midori64 block ciphers:

$$g(x_{ms-1}, ..., x_{(m-1)s}) + ... + g(x_{2s-1}, ..., x_s) + g(x_{s-1}, ..., x_0) \qquad (1)$$

[3] Todo, Yosuke, Gregor Leander and Yu Sasaki. "Nonlinear Invariant Attack: Practical Attack on Full SCREAM, iSCREAM, and Midori64." Journal of Cryptology 32 (2016): 1383 - 1422.

Nonlinear invariants

D. Burov [4] considered the next nonlinear invariants

$$\varphi(g(x_{ms-1}, ..., x_{(m-1)s}), ..., g(x_{2s-1}, ..., x_s), g(x_{s-1}, ..., x_0)) \qquad (2)$$

and proved that such invariants do not exist for

- Kuznyechik block cipher,
- Present, GIFT block ciphers,
- AES, LED, Anubis block ciphers,

round functions.

[4] Д. А. Буров, “О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов”, Дискрет. матем., 33:2 (2021), 31–45; Discrete Math. Appl., 33:2 (2023), 65–75.

Nonlinear invariants

D. Fomin[5] proposed to consider $U < V_n : F_{k_t} \circ ... \circ F_{k_0}(U) = U$.

It was shown that for Kuznyechik block cipher and $U = A_1 \times ... \times A_{16}$, $A_i \subset V_8$ such an invariants do not exist.

[5] Denis Fomin. "On the Impossibility of an Invariant Attack on Kuznyechik" 10-th Workshop on Current Trends in Cryptology (CTCrypt 2021). Pre-proceedings. June 1-4, 2021, Dorokhovo, Ruza District, Moscow Region, Russia.

Invariant subspaces of the circulant matrices

Circulant matrix

Definition

$n \times n$ circulant matrix over $\mathbb{F}_{q^s}$ is

$$C_{n\times n} = Circ_{q^s}(c_{n-1}, ..., c_0) = \begin{pmatrix} c_0 & c_{n-1} & ... & c_2 & c_1 \\ c_1 & c_0 & ... & c_3 & c_2 \\ ... & & & & \\ c_{n-2} & c_{n-3} & ... & c_0 & c_{n-1} \\ c_{n-1} & c_{n-2} & ... & c_1 & c_0 \end{pmatrix}$$

Upper-triangular matrix

The next proposition was claimed by A. Volgin and G. Kryuchkov in[6].

Proposition

Let $Q = \mathbb{F}_{2^s}$, $r \in \mathbb{N}$, $C = Circ_{q^s}(c_{2^r-1}, ..., c_0)$, then the characteristic polynomial of the matrix C is equal to $\chi_C(x) = (x + t)^{2^r}$, where $t = \sum_{i=0}^{2^r-1} c_i$. Matrix C is similar to upper-triangular matrix via similarity matrix B:

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\otimes r} \in Q_{2^r,2^r} \tag{3}$$

[6] А. В. Волгин, Г. В. Крючков, “Характеризация линейных преобразований, задающихся матрицами Адамара над конечным полем и циркулянтными матрицами”, ПДМ. Приложение, 2017, № 10, 10–11.

Upper-triangular matrix

Matrix B provides the chain of the invariant subspaces of the linear transformation defined by circulant matrix C:
$\langle \vec{B}_0 \rangle, \langle \vec{B}_0, \vec{B}_1 \rangle, ..., \langle \vec{B}_0, \vec{B}_1, ..., \vec{B}_{2^r-1} \rangle$.

Example of the matrix B.

$$B_{8\times 8} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}_{8\times 8}$$

Upper-triangular matrix

Theorem

Let $Q = \mathbb{F}_{2^s}$, $r \in \mathbb{N}$, $C = Circ(c_{2^r-1}, ..., c_0) \in Q_{2^r,2^r}$ *and matrix* B *is equal*

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\otimes r} \in Q_{2^r,2^r}, \tag{4}$$

then the next equality holds $B^{-1}CB = T$, *where* $T \in Q_{2^r,2^r}$ *is upper-triangular Toeplitz matrix*

$$T = \begin{pmatrix} t_0 & t_1 & t_2 & ... & t_{2^r-1} \\ 0 & t_0 & t_1 & ... & t_{2^r-2} \\ ... & & & & \\ 0 & 0 & ... & t_0 & t_1 \\ 0 & 0 & 0 & ... & t_0 \end{pmatrix}$$

Upper-triangular matrix

Theorem

$$T = \begin{pmatrix} t_0 & t_1 & t_2 & \dots & t_{2^r-1} \\ 0 & t_0 & t_1 & \dots & t_{2^r-2} \\ \dots & & & & \\ 0 & 0 & \dots & t_0 & t_1 \\ 0 & 0 & 0 & \dots & t_0 \end{pmatrix}, \qquad t_i = \sum_{j \le (2^r-1-i)} c_{(j+1 \bmod 2^r)}. \tag{5}$$

"$j \le j'$" means for every $i \in \overline{0, r-1}$ $j_i \le j'_i$, where

$j = j_{r-1}2^{r-1} + \dots + j_1 2 + j_0$ — bit representation of the number j

Invariant subspaces description

Proven theorem provides description of all invariant subspaces of the circulant matrix under some condition.

Theorem

Let $Q = \mathbb{F}_{2^s}$, $r \in \mathbb{N}$, $C = Circ(c_{2^r-1}, ..., c_0) \in Q_{2^r,2^r}$ *and* $t_1 = c_1 + c_3 + ... + c_{2^r-1} \neq 0$ *holds. Then there are no invariant subspaces of the circulant* C *matrix except subspaces from Proposition p. 13-14.*

$$T = \begin{pmatrix} t_0 & t_1 & t_2 & ... & t_{2^r-1} \\ 0 & t_0 & t_1 & ... & t_{2^r-2} \\ ... & & & & \\ 0 & 0 & ... & t_0 & t_1 \\ 0 & 0 & 0 & ... & t_0 \end{pmatrix}, \qquad t_i = \sum_{j \leq (2^r-1-i)} c_{(j+1 \ mod \ 2^r)}.$$

AES and Whirlpool matrices

Example

Invariant subspaces of the AES and Whirlpool matrices are only subspaces from Proposition p. 13-14.

We remind these matrices.

- AES: $Circ_{2^8}(0x03, 0x01, 0x01, 0x02)$;
- Whirlpool: $Circ_{2^8}(0x01, 0x04, 0x01, 0x08, 0x05, 0x02, 0x09, 0x01)$.

According to the Theorem p. 17 it is enough to check the sum $c_1 + c_3 + ... + c_{2r-1} \neq 0$ in every matrix.

The Second Normal Form of the circulant matrix

Corollary

Under Theorem p. 17 conditions the Second Normal Form of the circulant matrix is

$$N_2(C) = S((x+t)^{2^r}) = \begin{pmatrix} 0 & 0 & \dots & 0 & t^{2^r} \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}_{2^r \times 2^r}, \qquad t = \sum_{j=0}^{2^r-1} c_j.$$

Binary circulant matrices

Remark

In case $Q = \mathbb{F}_2$, $C = Circ_2(c_{2^r-1}, ..., c_0) \in Q_{n,n}$, $n = 2^r = ms$ and XSL-scheme with equal S-boxes $\overline{S} = (S, ..., S)$, $S : V_s \to V_s$ subspaces of *type 1* from Proposition p. 13-14 are only subspaces of $ks, k \in \mathbb{N}$ dimension.

Binary circulant matrices

Theorem

Let $Q = \mathbb{F}_2$, $C = Circ_2(c_{n-1}, ..., c_0) \in Q_{n,n}$, $n = 2^r = ms$, $S : V_s \to V_s$ and there exist $i \in \overline{1,s} : t_i = 1$ then there are no invariant subspaces of type 1 of the circulant matrix C except subspaces of type 1 from Proposition p. 13-14.

$$T = \begin{pmatrix} t_0 & t_1 & t_2 & ... & t_{2^r-1} \\ 0 & t_0 & t_1 & ... & t_{2^r-2} \\ ... & & & & \\ 0 & 0 & ... & t_0 & t_1 \\ 0 & 0 & 0 & ... & t_0 \end{pmatrix}, \qquad t_i = \sum_{j \le (2^r-1-i)} c_{(j+1 \ mod \ 2^r)}.$$

SM4 matrix

Example

Invariant subspaces of of *type 1* ($s = 8$) of the SM4 matrix are subspaces of *type 1* from Proposition p. 13-14 and only they.

We remind SM4 matrix.

$Circ_2(0x01, 0x04, 0x04, 0x05)$.

It is enough to calculate $t_1 = 0, t_2 = 1$ and use Theorem p.21.

Invariant subspaces of the recursive matrices

Generalized Reed-Solomon Codes

Definition

Let $Q = \mathbb{F}_q, m \leq q-1, w_1, ..., w_m$ are distinct elements of Q and $u_1, ..., u_m$ are nonzero elements of Q.

Generalized Reed-Solomon Code is

$GRS_Q(m,k)_{w_1,...,w_m}^{u_1,...,u_m} = \{(u_1 f(w_1), ..., u_m f(w_m)) \in Q^m | f \in Q[x], deg\ f < k\}$.

$GRS_Q(m,k)$ is $[m, k, m-k+1]$ MDS code.

Definition

Let $k \leq m, f(x) \in Q[x]$ is polynomial of degree k, $L_Q(f)$ are set of the linear recurrence sequences with charasteristic polynomial $f(x)$.

Linear recursive code is $L_Q^{\overline{0,m-1}}(f) = \{(v(0), ..., v(m-1)) \mid v \in L_Q(f)\}$.

Recursive matrices on GRS codes

Let $m = 2k$ then generation matrix of $L_Q^{\overline{0,m-1}}(f)$ in standard form is equal to

$$(E_{k\times k}, S(f)^k)_{k\times 2k} \tag{6}$$

and branch number of $S(f)^k$ is equal to code distance of the $L_Q^{\overline{0,m-1}}(f)$ code.

Let $w_i = \alpha^{i-1}, u_i = \theta^i, i \in \overline{1,m}; ord\ \alpha \geq m$. Then $GRS_Q(2m,m)_{1,\alpha,\ldots,\alpha^{m-1}}^{\theta,\theta^2,\ldots,\theta^m}$ is recursive $[2m, m, m+1]$ MDS code with polynomial $f(x) = (x-\theta)(x-\theta\alpha)\ldots(x-\theta\alpha^{m-1})$ then recursive matrix $S(f(x))^m$ is MDS matrix.

Definition

In such a case we say $S(f(x))^m$ is constructed on the Generalized Reed-Solomon Code.

Recursive matrices on GRS codes

Proposition

If recursive matrix $S(f(x))^m = S^m$, *is constructed on the Generalized Reed-Solomon Code* $GRS_Q(2m, m)^{\theta,\theta^2,...,\theta^m}_{e,\alpha,...,\alpha^{m-1}}$ *then the next equations holds*

$$S^m = V_1^{-1} D^m V_1 = \theta^m (V_1^{-1} V_2),$$

where $D = diag(\theta, \theta\alpha, ..., \theta\alpha^{m-1})$,

$V_1 = Vand(\theta, \theta\alpha, ..., \theta\alpha^{m-1})$, $V_2 = Vand(\theta\alpha^m, \theta\alpha^{m+1}, ..., \theta\alpha^{2m-1})$.

$$Vand(u_1, ..., u_m) = \begin{pmatrix} 1 & 1 & ... & 1 \\ u_1 & u_2 & ... & u_m \\ u_1^2 & u_2^2 & ... & u_m^2 \\ ... & ... & ... & ... \\ u_1^{m-1} & u_2^{m-1} & ... & u_m^{m-1} \end{pmatrix}_{m \times m}$$

Recursive matrices on GRS codes

Corollary

In case of Proposition p. 25 if for any root of $f(x)$ $i \in \overline{0, m-1}$ $ord(\theta\alpha^i) > m-1$ *then there are no invariant subspaces of type 1 for the recursive matrix* $S(f(x))^m$.

Example

There are no invariant subspaces of *type 1* for Kuznyechik block cipher matrix.

$Q = \mathbb{F}_{2^8}$, $m = 16$, α is a primitive element of Q and $\theta = \alpha^{120}$.

For every $i \in \overline{120, 135}$: $\dfrac{255}{gcd(i, 255)} > 15$.

Thanks for your attention

Stepan Davydov, s.davydov@kryptonite.ru