Group Properties of Block Ciphers of the Russian Standards GOST R 34.11-2012 and GOST R 34.12-2015

V. Vlasova, M. Pudovkina

CTCrypt2017, June 5, 2017

XSL-cipher

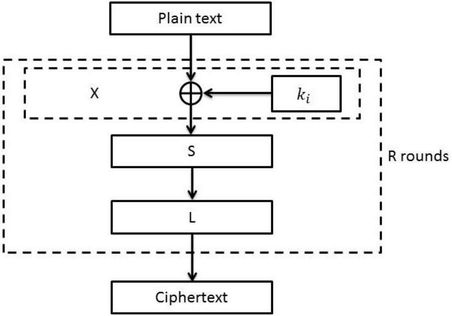

Figure 1: XSL-cipher general scheme

Examples

AES, Kuznyechik, Stribog, Kalyna, Whirlpool, ...

Group generated by the set of all round functions

Consider an XSL-cipher.
Let $a, s, x[k]\colon V_{mn} \to V_{mn}$:

- a is an invertible linear transformation
- s is an S-box mapping, $s = (s_1, ..., s_n) \in S(V_m)^n$

$$s\colon (\alpha_1, ..., \alpha_n) \mapsto (s(\alpha_1), ..., s(\alpha_n)), (\alpha_1, ..., \alpha_n) \in {V_m}^n$$

- $x[k]\colon \alpha \mapsto \alpha \oplus k,\ k \in V_{mn}$.

Let $g_k\colon V_{mn} \to V_{mn}$ be a round function:

$$g_k\colon \alpha \mapsto a \circ s \circ x[k](\alpha)$$

Consider a group $G = \langle g_k \mid k \in V_{mn} \rangle$

Some known results

The property $G = A_d$ was proved for the following block ciphers.

Cipher	Type	Proof provided by
DES	Feistel	R. Wernsdorf, EUROCRYPT'92
IDEA(32)	Feistel	G. Hornauer, W. Stephan, R. Wernsdorf, EUROCRYPT'93
SAFER	XSL	R. Dittmar, G. Hornauer, R. Wernsdorf, PRAGOCRYPT'96
SERPENT	XSL	R. Wernsdorf, 2000
AES	XSL	R. Wernsdorf, 2002
AES, WHIRLPOOL	XSL	R. Sparr, R. Wernsdorf, 2008
AES	XSL	A. Caranti, F. Dalla Volta, M. Sala, 2009
KASUMI	Feistel	R. Sparr, R. Wernsdorf, 2014
GOST 28147-89	Feistel	R. Aragona, A. Caranti, M. Sala, 2015

Definitions and Notations

$M_{p,q}(u)$	the set of all $p \times q$ matrices over $GF(u)$
$M_p(u)$	the set of all $p \times p$ matrices over $GF(u)$

Elements of $GF(u)^{pq}$ are identified with matrices from $M_{p,q}(u)$.

Definition

Let a be a linear transformation.
We say that digraph $\Gamma(a)$ is a *graph of essential dependence* of a, if

$$\Gamma(a) = (\{1, ..., n\}, X),$$

$(i, j) \in X \Leftrightarrow j^{th}$ coordinate function of a essentially depends on i^{th} coordinate.

Properties of Generated Group

For a vector $\alpha = (\alpha_1, ...\alpha_n) \in V_m^n$, we will assign a set

$$I(\alpha) = \{i \in \{1, \ldots, n\} \mid \alpha_i \neq 0_m\}.$$

Let $L \subseteq \{1, ..., n\}$ be a subset of vertices of the digraph $\Gamma(a)$.
Let $J(L)$ be the set of ends of edges which starts at the set L.
For the permutations s_i, we will assign the permutations

$$s_{i,k,k'} \colon \alpha \mapsto s_i^{-1}(k' \oplus s_i(\alpha \oplus k)),$$

where $k, k' \in V_m$ for all $i \in \{1, \ldots, n\}$.

$$H(s_i) = \langle s_{i,k,k'} \mid k, k' \in V_m^2 \rangle.$$

Properties of Generated Group

Theorem 1 [Maslov, 2007]

Suppose that the following conditions hold:

1) digraph $\Gamma(a)$ is primitive;
2) for any set $L \subseteq \{1, \ldots, n\}$

$$\max_{\{\alpha \in V_{mn} | I(\alpha) = L\}} |I(a(\alpha))| \geq |L|,$$

   with inequality strict if $|J(I)| > |I|$;
3) groups $H(s_1), \ldots, H(s_n)$ are 2-transitive, and there is a permutation $s \in H(s_j)$ such that

$$|\{\alpha \in V_m \mid s(\alpha) = \alpha\}| \notin \{0, 2^0, 2^1, 2^2, \ldots, 2^m\}.$$

Then $G = \langle g_k \mid k \in V_{mn} \rangle = A(V_{mn})$.

Properties of the Linear Transformations

Linear transformation $a\colon M_p(u) \to M_p(u) : a = l \circ t$

$\widetilde{T}$-transformation Transpose+MixRows	$\widetilde{R}$-transformation ShiftRows+MixColumns	$\widetilde{R}'$-transformation ShiftColumns+MixRows
$t(\boldsymbol{\alpha}) = \boldsymbol{\beta}$: $\beta_{i,j} = \alpha_{j,i}$	$t(\boldsymbol{\alpha}) = \boldsymbol{\beta}$: $\beta_{ij} = \alpha_{i,(j-c(i)) \bmod p}$	$t(\boldsymbol{\alpha}) = \boldsymbol{\beta}$: $\beta_{ij} = \alpha_{(i-c(j)) \bmod p,j}$
$l(\boldsymbol{\alpha}) = \boldsymbol{\alpha} \cdot \mathbf{d}$	$l(\boldsymbol{\alpha}) = \mathbf{d} \cdot \boldsymbol{\alpha}$	$l(\boldsymbol{\alpha}) = \boldsymbol{\alpha} \cdot \mathbf{d}$

$\boldsymbol{\alpha}, \boldsymbol{\beta} \in M_p(u)$, $\mathbf{d} \in M_p(u)$, $c \in S(\{0, \ldots, p-1\})$

Theorem 2.

Let $a = l \circ t$ be a $\widetilde{T}$-, $\widetilde{R}$- or $\widetilde{R}'$-transformation and the matrix $\mathbf{d}$ corresponding the transformation l does not contain zero elements. Then the digraph $\Gamma(a)$ of essential dependence of the transformation a is primitive.

The main idea

For $\widetilde{T}$-, $\widetilde{R}$- or $\widetilde{R}'$-transformation $a\colon M_p(u) \to M_p(u)$, the matrix $\mathbf{m} \in M_{p^2}(u)$ has been found such that

$$a(\alpha) = \alpha \cdot \mathbf{m}.$$

The adjacency matrix $\mathbf{a} = (a_{ij})$ has been found using the matrix $\mathbf{m} = (m_{ij})$ by rule

$$a_{ij} = \begin{cases} 0, & \text{if } m_{ij} = 0, \\ 1, & \text{if } m_{ij} \neq 0 \end{cases}$$

for all $i, j \in \{0, \ldots, n-1\}$.
It has been shown that $\mathbf{a^2}$ doesn't contain zero elements if the matrix $\mathbf{d}$ doesn't contain zero elements.

Group properties of the Kuznyechik block cipher and the Stribog block cipher

Theorem 3.

Let G be the group generated by the set of round functions of a block cipher. Than G is equal to

- $A(V_{128})$ for Kuznyechik,
- $A(V_{512})$ for Stribog.

Proof of Theorem 3 (condition 1)

Linear transformations can be represented as:

Kuznyechik	**Stribog**
$a_k\colon GF(2^8)^{16} \to GF(2^8)^{16}$	$a_s\colon GF(2^8)^{64} \to GF(2^8)^{64}$
$a_k\colon \alpha \mapsto \alpha \cdot \mathbf{m_k}$,	$a_s = l \circ t$,
	$t\colon \boldsymbol{\alpha} \mapsto \boldsymbol{\alpha}^T$
	$l\colon \boldsymbol{\alpha} \mapsto \boldsymbol{\alpha} \cdot \mathbf{d_s}$
$\mathbf{m_k} \in M_{16}(2^8)$, $\alpha \in GF(2^8)^{16}$	$\mathbf{d_s} \in M_8(2^8)$, $\boldsymbol{\alpha} \in M_8(2^8)$

- The digraph $\Gamma(a_k)$ is primitive because the matrix $\mathbf{m_k}$ does not contain any zero elements.
- The digraph $\Gamma(a_s)$ is primitive according to Theorem 2 (a_s is a $\widetilde{T}$-transformation).

For Kuznyechik the multiplication is performed in $GF(2^8)$ with irreducible polynomial $p_k(x) = x^8 + x^7 + x^6 + x + 1$.
The matrix $\mathbf{m_k}$ is

$$
\begin{pmatrix}
CF & 6E & A2 & 76 & 72 & 6C & 48 & 7A & B8 & 5D & 27 & BD & 10 & DD & 84 & 94 \\
98 & 20 & C8 & 33 & F2 & 76 & D5 & E6 & 49 & D4 & 9F & 95 & E9 & 99 & 2D & 20 \\
74 & C6 & 87 & 10 & 6B & EC & 62 & 4E & 87 & B8 & BE & 5E & D0 & 75 & 74 & 85 \\
BF & DA & 70 & 0C & CA & 0C & 17 & 1A & 14 & 2F & 68 & 30 & D9 & CA & 96 & 10 \\
93 & 90 & 68 & 1C & 20 & C5 & 06 & BB & CB & 8D & 1A & E9 & F3 & 97 & 5D & C2 \\
8E & 48 & 43 & 11 & EB & BC & 2D & 2E & 8D & 12 & 7C & 60 & 94 & 44 & 77 & C0 \\
F2 & 89 & 1C & D6 & 02 & AF & C4 & F1 & AB & EE & AD & BF & 3D & 5A & 6F & 01 \\
F3 & 9C & 2B & 6A & A4 & 6E & E7 & BE & 49 & F6 & C9 & 10 & AF & E0 & DE & FB \\
0A & C1 & A1 & A6 & 8D & A3 & D5 & D4 & 09 & 08 & 84 & EF & 7B & 30 & 54 & 01 \\
BF & 64 & 63 & D7 & D4 & E1 & EB & AF & 6C & 54 & 2F & 39 & FF & A6 & B4 & C0 \\
F6 & B8 & 30 & F6 & C4 & 90 & 99 & 37 & 2A & 0F & EB & EC & 64 & 31 & 8D & C2 \\
A9 & 2D & 6B & 49 & 01 & 58 & 78 & B1 & 01 & F3 & FE & 91 & 91 & D3 & D1 & 10 \\
EA & 86 & 9F & 07 & 65 & 0E & 52 & D4 & 60 & 98 & C6 & 7F & 52 & DF & 44 & 85 \\
8E & 44 & 30 & 14 & DD & 02 & F5 & 2A & 8E & C8 & 48 & 48 & F8 & 48 & 3C & 20 \\
4D & D0 & E3 & E8 & 4C & C3 & 16 & 6E & 4B & 7F & A2 & 89 & 0D & 64 & A5 & 94 \\
6E & A2 & 76 & 72 & 6C & 48 & 7A & B8 & 5D & 27 & BD & 10 & DD & 84 & 94 & 01
\end{pmatrix}.
$$

For Stribog the multiplication is performed in $GF(2^8)$ with irreducible polynomial $p_s(x) = x^8 + x^4 + x^3 + x^2 + 1$.
The matrix $\mathbf{d_s}$ is

$$
\begin{pmatrix}
83 & 47 & 8B & 07 & B2 & 46 & 87 & 64 \\
46 & B6 & 0F & 01 & 1A & 83 & 98 & 8E \\
AC & CC & 9C & A9 & 32 & 8A & 89 & 50 \\
03 & 21 & 65 & 8C & BA & 93 & C1 & 38 \\
5B & 06 & 8C & 65 & 18 & 10 & A8 & 9E \\
F9 & 7D & 86 & D9 & 8A & 32 & 77 & 28 \\
A4 & 8B & 47 & 4F & 9E & F5 & DC & 18 \\
64 & 1C & 31 & 4B & 2B & 8E & E0 & 83
\end{pmatrix}.
$$

Proof of Theorem 3 (condition 2)

We have used Theorem 2 proved in [Maslov, 2007].
According to this theorem, condition 2 is correct if

$$2^{mn} < (2^{m-1})^{n-1}(2^m + 2^{m-1} - 2) \tag{1}$$

Kuznyechik	**Stribog**
$3{,}4028 \times 10^{38} < 4{,}7881 \times 10^{38}$	$1{,}3408 \times 10^{154} < 1{,}5635 \times 10^{154}$

Proof of Theorem 3 (condition 3)

Groups $H(s_1), \ldots, H(s_n)$ are 2-transitive

S-boxes permutations are the same for Kuznyechik and Stribog.

- $\boldsymbol{\lambda}$ is the difference distribution matrix
- the matrix $\boldsymbol{\mu}$ has been calculated by rule $\boldsymbol{\mu} = \boldsymbol{\lambda} \cdot \boldsymbol{\lambda}^T$
- graph $\Lambda(s)$ which vertices α and β from V_m are connected by an edge if and only if $\mu_{\alpha\beta} > 0$.

According to Theorem 3 proved in [Maslov, 2007], the group $H(s)$ is 2-transitive $\Leftrightarrow$ the graph $\Lambda(s)$ is connected.

Connectivity of the graph Λ for Kuznyechik and Stribog has been verified by direct calculations.

Proof of Theorem 3 (condition 3)

There is $s \in H(s_j)$ such that

$$|\{\alpha \in V_m \mid s(\alpha) = \alpha\}| \notin \{0, 2^0, 2^1, 2^2, \ldots, 2^m\}.$$

Proving it is equal to existence of elements υ of the difference distribution matrix $\boldsymbol{\lambda}$ such that $\upsilon \notin \{0, 2^0, 2^1, 2^2, \ldots, 2^m\}$.

Such elements which are equal to 6, have been found in the calculated matrix $\boldsymbol{\lambda}$.

$\square$

Thank you for your attention!