The permutation group insight on diffusion property of linear mappings

Burov D.A., Pogorelov B.A.

SPN block ciphers

Substitution-permutation network (SPN) is an important type of iterated block ciphers. Round function $f_k : V_n \to V_n$, $k \in V_n$ is represented by a composition of 3 layers:

X – key addition layer $(\alpha \mapsto \alpha \oplus k)$

S – confusion s-box layer $(s : (\alpha_1, \ldots, \alpha_m) \mapsto (\alpha_1^{s_1}, \ldots, \alpha_m^{s_m})$, $\alpha \in V_n$, $\alpha_i \in V_d$, $s_i \in S(V_d), i = 1, \ldots, m$, $n = md$);

L – diffusion linear layer $(\alpha \mapsto \alpha h$, $h \in GL_n(2)$ – an invertible $(n \times n)$-matrix over the field $GF(2))$.

An approach to study properties of block ciphers

Let G_{XS} be the permutation group generated by key addition layer and s-box layer, i.e. $G_{XS} = \langle V_n^+, s \rangle$, where V_n^+ is the translation group of the vector space V_n.

Let G_{XL} be the group generated by key addition layer and linear layer, i.e. $G_{XL} = \langle V_n^+, h \rangle$.

B.A. Pogorelov suggested the following approach to study properties of block ciphers:

1. study G_{XL}-invariant ($G_{XS}-$invariant) structures;
2. study how s-box layer (linear layer) breaks these structures.

Examples of G_{XS}- and G_{XL}-invariant structures

1. If linear mapping h is reducible, then G_{XL} is an imprimitive group, i.e. there is G_{XL}-invariant system of blocks. The attack on Khazad block cipher was caused by reducibility of linear mapping (Burov D.A., Pogorelov B.A.). Implicitly reducibility of linear mapping is used for attacks on PRINT, Robbin, iSCREAM, Zorro (Leander G. et al), Midori (Guo J. et al).
2. If h is not a primitive linear mapping, then G_{XL} is an uniprimitive group, i.e. there are G_{XL}-invariant metrics. G_{XL}-invariant metrics are described by Pogorelov B.A. and Pudovkina M.A.
3. If $m \geq 2$, then G_{XS} is an imprimitive group. Block systems of G_{XS} is implicitly are used in truncated differential method.

Branch number of linear mapping

The main cryptographic characteristics of linear mapping are differential and linear branch numbers. These characteristics have influence on resistance of block ciphers to differential and linear methods.

For $\alpha = (\alpha_1, \ldots, \alpha_m) \in V_n$, $\alpha_i \in V_d$, $i = 1, \ldots, m$, suppose $\mathrm{wt}(\alpha) = |\{i \in \{1, \ldots, m\} \,|\alpha_i \neq 0_d\}|$.

$$\mathrm{bn}_d(h) = \min\left\{\mathrm{wt}(\alpha) + \mathrm{wt}\left(\alpha^h\right) |\alpha \in V_n \setminus \{0\}\right\},$$

$$\mathrm{bn}_l(h) = \min\left\{\mathrm{wt}(\alpha) + \mathrm{wt}\left(\alpha^{\,{}^t h}\right) |\alpha \in V_n \setminus \{0\}\right\}.$$

Here ${}^t h$ is a transpose matrix. It is easily to show that $\mathrm{bn}_d(h) \leq m + 1$. If $\mathrm{bn}_d(h) = m + 1$, then h is called MDS linear mapping.

$G_{XS}-$invariant system of blocks

Suppose

$$V(i_1,\dots,i_t) = \\ = \left\{ (\overbrace{0_d,\dots,0_d}^{i_1-1},\alpha_1,\overbrace{0_d,\dots,0_d}^{i_t-1},\alpha_t,0_d,\dots,0_d) | \alpha_1,\dots,\alpha_t \in V_d \right\}.$$

Let $\mathbf{V}(i_1,\dots,i_t)$ be a partition of cosets of $V(i_1,\dots,i_t)$ in the vector space V_n.

Proposition

For all $m \geq 2$, $d \geq 2$, $1 \leq i_1 < \dots < i_t \leq m$, $t = \{1,\dots,m-1\}$ the group G_{XS} is imprimitive and $\mathbf{V}(i_1,\dots,i_t)$ is a system of blocks for the group G_{XS}.

Suppose $\mathbf{W}=\mathbf{V}(i_1,\ldots,i_t)$, $\mathbf{W}'=\mathbf{V}(j_1,\ldots,j_r)$.
Diffusion property of linear mapping h with respect to the pair of partitions $(\mathbf{W},\mathbf{W}')$ is characterized by $\left(2^{(m-t)d}\times 2^{(m-r)d}\right)$-matrix $\mathbf{c}_{\mathbf{W},\mathbf{W}'}(h)=\|c_{i,j}(h)\|$, where

$$c_{i,j}(h)=\left|W_i^h\cap W_j'\right|.$$

We study the Euclidean distance

$$\rho\left(\mathbf{c}_{\mathbf{W},\mathbf{W}'}(h),\mathbf{u}_{t,r}\right)$$

between matrix $\mathbf{c}_{\mathbf{W},\mathbf{W}'}(h)$ and the uniform $\left(2^{(m-t)d}\times 2^{(m-r)d}\right)$-matrix $\mathbf{u}_{t,r}=\left\|2^{(t+r-m)d}\right\|$.
The less the Euclidean distance is the better linear property of mapping h is.

Lower bound for the Euclidean distance

Proposition

Let $h \in GL_n(2)$, $\mathbf{W}=\mathbf{V}(i_1,\ldots,i_t)$, $\mathbf{W}'=\mathbf{V}(j_1,\ldots,j_r)$, $1 \le i_1 < \cdots < i_t \le m$, $1 \le j_1 < \cdots < j_r \le m$, $n = md$, $m, d \ge 2$.

Then we have

$$\rho\left(\mathbf{c}_{\mathbf{W},\mathbf{W}'}(h), \mathbf{u}_{t,r}\right) \ge \varphi_m(t,r),$$

$$\varphi_m(t,r) = \begin{cases} 0, & if\ t+r \ge m, \\ \sqrt{2^{md} - 2^{(t+r)d}}, & if\ t+r < m. \end{cases}$$

Characterization of MDS linear mappings

Proposition

The equalities

$$\rho\left(\mathbf{c}_{\mathbf{W},\mathbf{W}'}(h), \mathbf{u}_{t,r}\right) = \varphi_m(t,r)$$

hold for all $t, r \in \{1, \ldots, m\}$, $1 \leq i_1 < \cdots < i_t \leq m$, $1 \leq j_1 < \cdots < j_r \leq m$, *if and only if* h *is MDS linear mapping.*

Remark

MDS linear mappings diffuse G_{XS}*-invariant structures. But there exist reducible MDS linear mappings. In particularly attack on Khazad block cipher was caused by reducibility of MDS linear mapping.*

Expression of branch number via the Euclidean distance

For any linear mapping $h \in GL_n(2)$ suppose

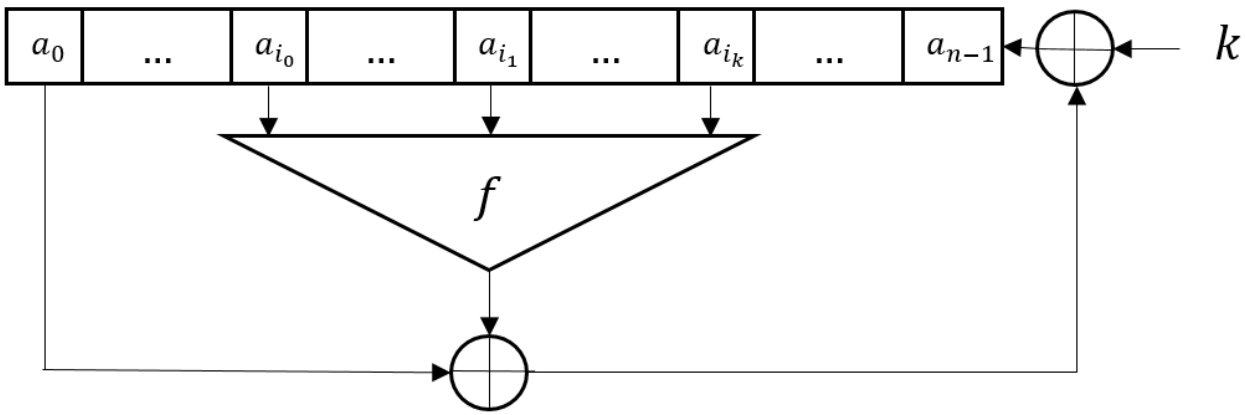
$$B_h = \left\{ (t,r) \left| \begin{array}{l} t+r \le m, \exists\ 1 \le i_1 < \cdots < i_t \le m,\ 1 \le j_1 < \cdots < j_r \le m, \\ \rho\left(\mathbf{c}_{\mathbf{V}(i_1,\ldots,i_t),\mathbf{V}(j_1,\ldots,j_r)}(h), \mathbf{u}_{t,r}\right) > \varphi_m(t,r) \end{array} \right. \right\}$$

Proposition

For any $h \in GL_n(2)$ we have

$$\mathrm{bn}_d(h) = \begin{cases} \min\{t+r \,|\, (t,r) \in B_h\}, & if\ B_h \neq \emptyset, \\ m+1, & if\ B_h = \emptyset. \end{cases}$$

Metrics



Let G be the group of the shift register. If

$$\mathrm{GCD}\{i_1, i_2 - i_1, \ldots, i_k - i_{k-1}, n\} = d > 1,$$

then there are G-invariant metrics (*Pogorelov B.A.* Permutation group, 1986).

$G_{XS}-$invariant metrics

Let $\mathbf{A} = \{A_1, \ldots, A_u\}$ be a partition of the set $\{1, \ldots, m\}$, $|A_i| = \frac{m}{u},\ i = 1, \ldots, u$. Define a weight of the vector $\alpha = (\alpha_1, \ldots, \alpha_m) \in V_n,\ \alpha_i \in V_d,\ i = 1, \ldots, m$, with respect to partition $\mathbf{A}$ by

$$\mathrm{wt}_{\mathbf{A}}(\alpha) = \left|\{i \in \{1, \ldots, u\} \,|\exists j \in A_i,\ \alpha_j \neq 0\}\right|.$$

The isometric group $G_{\mathbf{A}} < S(V_n)$ of metric $\chi_{\mathbf{A}}$ is permutation isomorphic to the exponentiation $S_{2^{\frac{n}{u}}} \uparrow S_u$.

Proposition

For all partitions $\mathbf{A} = \{A_1, \ldots, A_u\}$ of the set $\{1, \ldots, m\}$, $|A_i| = \frac{m}{u},\ i = 1, \ldots, u$, the metric $\chi_{\mathbf{A}}$ is G_{XS}-invariant.

Hamming distance between MDS linear mappings and isometric groups

Proposition

Let $h \in GL_n(2)$, $n = md$, be a MDS linear mapping,
$\mathbf{A} = \{A_1, \ldots, A_u\}$ be a partition of the set $\{1, \ldots, m\}$, $|A_i| = \frac{n}{u}$.
Then we have

$$\chi\left(h, G_{\mathbf{A}}\right) \geq 2^n - 2^{n-\frac{n}{u}}.$$