Math-Net.Ru

Общероссийский математический портал

D. A. Burov, V. A. Pogorelov, Рассеивающие свойства линейных преобразований с точки зрения теории групп подстановок, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 2, 47–58

DOI: <https://doi.org/10.4213/mvk252>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.205.19.152

26 апреля 2023 г., 17:57:13

The permutation group insight on the diffusion property of linear mappings

D. A. Burov¹, B. A. Pogorelov²,

¹ TVP Laboratories, Moscow

² Academy of Cryptography of the Russian Federation, Moscow

Получено 05.II.2017

Abstract. We investigate the properties of linear mappings related to the structures of the group generated by S-box layer and the group of key addition layer, i. e. the translation group of a vector space. We propose new parameters characterizing the diffusion properties of linear mapping. A new characterization of MDS linear mappings is given. MDS linear mappings that have arisen to provide the security with respect to the differential and linear methods, as well as other components of the round transformation, may be synthesized on the base of the permutation groups theory.

Key words: block cipher, linear mapping, wreath product, exponentiation, structures of permutation groups, metrics

Рассеивающие свойства линейных преобразований с точки зрения теории групп подстановок

Д. А. Буров¹, Б. А. Погорелов²

¹ Лаборатории ТВП, Москва

² Академия криптографии Российской Федерации, Москва

Аннотация. Исследуются свойства линейных преобразований, связанные со структурами группы, порожденной нелинейным слоем блочного алгоритма шифрования, и группы, порожденной слоем наложения ключа, т. е. группы трансляций векторного пространства. Вводятся новые параметры, которые характеризуют рассеивающие свойства линейного отображения. Приводится новая характеристика MDS-матриц. Показано, что максимально рассеивающие преобразования, которые возникли в связи с обеспечением стойкости относительно разностного и линейного методов, а также другие составляющие раундового преобразования могут быть синтезированы с точки зрения теории групп подстановок.

Ключевые слова: блочный шифр, линейное отображение, сплетение, экспоненцирование, структуры групп подстановок, метрики

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 2, pp. 47–58 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

1. Introduction

Linear and differential methods are the most well known methods of block cipher cryptanalysis. These methods had an influence on principles of block ciphers construction. In particular, differential characteristic and linear characteristic are one of the main properties of S-boxes. Linear and differential branch numbers are the main characteristics of a linear mapping. Linear and differential branch numbers are associated with linear and differential methods of cryptanalysis.

In this paper we consider XSL block ciphers. The round function of XSL block ciphers consists of three layers: key addition layer, nonlinear S-box layer, linear layer.

Let G_{XS} be the group generated by S-box layer and the group of key addition layer, i.e. the translation group of a vector space, G_{XL} be the group generated by linear mapping and the group of key addition layer. We show that the group G_{XS} is a subgroup of the wreath product of symmetric permutation group and a subgroup of exponentiation of the symmetric permutation group [11, 6]. Moreover there exist G_{XS} -invariant partitions and G_{XS} -invariant metrics. Linear mapping is intended to diffuse these structures in order to avoid some attacks. G_{XL} -invariant metrics were studied by B. A. Pogorelov and M. A. Pudovkina [13]. Here we study the properties of a linear mapping from the viewpoint of diffusion of structures of the group G_{XS} . In particular we show that a linear mapping optimally diffuses the partitions if and only if it is a MDS mapping. Nevertheless even MDS mappings may be reducible. This property leads to an imprimitivity of the group G_{XL} . The reducibility of a linear mapping was used in attacks on Khazad block cipher [2, 3]. Implicitly the reducibility of a linear mapping was used in attacks on Print [9], Zorro, Robin, iSCREAM [10], Midori [7].

2. Preliminaries

Recall some definitions. Let K and H be groups and suppose H acts on the nonempty set Ω . Denote by $\text{Fun}(\Omega, K)$ the set of all functions from Ω into K . The set $\text{Fun}(\Omega, K)$ with respect to a product

$$(fg)(\gamma) = f(\gamma)g(\gamma) \quad \forall f, g \in \text{Fun}(\Omega, K), \gamma \in \Omega,$$

is a group. The wreath product of K by H with respect to this action is defined to be the semidirect product $\text{Fun}(\Omega, K) \rtimes H$, where the action of H on the group $\text{Fun}(\Omega, K)$ is defined by the formula

$$f^g(\gamma) = f(\gamma^{g^{-1}}), \quad \forall f \in \text{Fun}(\Omega, K), \gamma \in \Omega, g \in H.$$

Denote this group by $K \wr H$.

The wreath product $K \wr H$ has two actions. Namely, if K acts on a set Δ , then we can define an action of $K \wr H$ on $\Delta \times \Omega$ by

$$(\delta, \gamma)^{(f, u)} = (\delta^{f(\gamma)}, \gamma^u) \quad \forall (\delta, \gamma) \in \Delta \times \Omega,$$

where $(f, u) \in K \wr H$. Denote the group $(K \wr H, \Delta \times \Omega)$ by $K \wr H$.

Suppose that K acts on a set Δ . Define the action of the group $K \wr H$ on the set $\text{Fun}(\Omega, \Delta)$ as follows:

$$\varphi(\gamma)^{(f, x)} = \varphi(\gamma^{x^{-1}})^{f(\gamma^{x^{-1}})} \quad \forall \gamma \in \Omega.$$

Denote the group $(K \wr H, \text{Fun}(\Omega, \Delta))$ by $K \wr H$.

Denote the symmetric permutation group on a finite set Ω of n elements by $S_n = S(\Omega)$.

Let us do some remarks on the properties of these actions. Suppose that

$$\mathbf{W} = \{W_1, \dots, W_r\}$$

is a partition of the set Ω and $|W_i| = w$, $i = 1, \dots, r$. Then the group $G = \{g \in S(\Omega) \mid \mathbf{W}^g = \mathbf{W}\}$ is equal to the group $S(W) \wr S_r$ (strictly speaking, G is a permutation isomorphic to $S(W) \wr S_r$).

Suppose Ω is equal to A^n for some set A and $n \in \mathbb{N}$. Then the isometry group of Hamming metric on the set A^n is equal to the group $S_{|A|} \wr S_n$ (strictly speaking, the isometry group is permutation isomorphic to $S_{|A|} \wr S_n$). For other properties of the wreath product actions we refer to [11, 6].

Denote by V_n the vector space of dimension n over the field $GF(2)$. Suppose $v_\alpha: x \mapsto x \oplus \alpha$ for all $x \in V_n$, where binary operation $\oplus$ is the operation of vector addition. Denote by V_n^+ the translation group of the vector space V_n , i. e.

$$V_n^+ = \{v_\alpha \mid \alpha \in V_n\}.$$

Let $s \in S(V_n)$ be a parallel action of substitutions $s_1, \dots, s_m \in S(V_d)$, $n = md$, i. e.

$$s: (\alpha_1, \dots, \alpha_m) \mapsto (\alpha_1^{s_1}, \dots, \alpha_m^{s_m}), \quad \alpha_i \in V_d, \quad i = 1, \dots, m.$$

Mapping s is used in XSL ciphers as an S-box layer.

Let $GL_n(2)$ be the group of invertible $(n \times n)$ -matrices. Each matrix $h \in GL_n(2)$ induces the bijective linear mapping of the vector space V_n by multiplying vector-rows by h . Denote this linear mapping also by h . Further we use special submatrices of matrix h . Namely, suppose $n = md$, $t, r \in \{1, \dots, m\}$, $1 \leq i_1 < \dots < i_t \leq m$, $1 \leq j_1 < \dots < j_r \leq m$. Let $h \begin{pmatrix} i_1, \dots, i_t \\ j_1, \dots, j_r \end{pmatrix}$ be a $(td \times rd)$ -submatrix of the matrix h which is obtained by deleting rows with numbers

$$\{1, \dots, n\} \setminus \{(i_1 - 1)d + 1, \dots, (i_1 - 1)d + d, \dots, (i_t - 1)d + d\}$$

and columns with numbers

$$\{1, \dots, n\} \setminus \{(j_1 - 1)d + 1, \dots, (j_1 - 1)d + d, \dots, (j_r - 1)d + d\}.$$

Denote the vector $(0, \dots, 0) \in V_d$ by 0_d . For $\alpha = (\alpha_1, \dots, \alpha_m) \in V_n$, $\alpha_i \in V_d$, $i = 1, \dots, m$, put $\text{wt}(\alpha) = |\{i \in \{1, \dots, m\} \mid \alpha_i \neq 0_d\}|$. Usually diffusion property of linear mappings is characterized by the differential branch number $\text{bn}_d(h)$ and linear branch number $\text{bn}_l(h)$ [5] defined as

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

$$\text{bn}_l(h) = \min \left\{ \text{wt}(\alpha) + \text{wt}(\alpha^{th}) \mid \alpha \in V_n \setminus \{0\} \right\}.$$

Here th is a transpose matrix. It is easy to show that $\text{bn}(h) \leq m + 1$. If $\text{bn}_d(h) = m + 1$, then h is called MDS linear mapping. Besides if $\text{bn}_d(h) = m + 1$, then $\text{bn}_l(h) = m + 1$ [4]. The differential and linear branch numbers have influence on resistance of block ciphers against differential and linear cryptanalysis, respectively.

3. Structures of the group G_{XS}

Recall that G_{XS} is equal to $\langle V_n^+, s \rangle$. Let

$$V(i_1, \dots, i_t) = \left\{ \underbrace{(0_d, \dots, 0_d)}_{i_1-1}, \underbrace{\alpha_1, 0_d, \dots, 0_d}_{i_t-1}, \alpha_t, 0_d, \dots, 0_d \mid \alpha_1, \dots, \alpha_t \in V_d \right\}$$

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

Since V_n^+ is a regular group and $V(i_1, \dots, i_t) < V_n$, the partition $\mathbf{V}(i_1, \dots, i_t)$ is a system of blocks for the group V_n^+ . It is easy to show that the partition $\mathbf{V}(i_1, \dots, i_t)$ is s -invariant. Therefore $\mathbf{V}(i_1, \dots, i_t)$ is a system of blocks for the group G_{XS} . Maximal subgroup of symmetric group $S(V_n)$ preserving partition $\mathbf{V}(i_1, \dots, i_t)$ is the wreath product $S(V(i_1, \dots, i_t)) \wr S_{2^{n-dt}}$. Hence, G_{XS} is a subgroup of the wreath product $S(V(i_1, \dots, i_t)) \wr S_{2^{n-dt}}$ for all $t = 1, \dots, m-1$, $1 \leq i_1 < \dots < i_t \leq m$. Therefore, we have the following proposition.

Proposition 1. *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} .*

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

$$\text{wt}_{\mathbf{A}}(\alpha) = |\{i \in \{1, \dots, u\} \mid \exists j \in A_i, \alpha_j \neq 0\}|.$$

Note that if $A_i = \{i\}$, $i = 1, \dots, m$, then $\text{wt}_{\mathbf{A}}(\alpha)$ is equal to $\text{wt}(\alpha)$ for all $\alpha \in V_n$. Let $\chi_{\mathbf{A}}: V_n \times V_n \rightarrow \{0, \dots, u+1\}$ be a metric defined by $\chi_{\mathbf{A}}(\alpha, \beta) = \text{wt}_{\mathbf{A}}(\alpha \oplus \beta)$. The isometric group $G_{\mathbf{A}} < S(V_n)$ of metric $\chi_{\mathbf{A}}$ is the permutation one isomorphic to the exponentiation (product action) $S_{2^{n/u}} \uparrow S_u$. It is clear that $\chi_{\mathbf{A}}(\alpha, \beta) = \chi(\alpha^s, \beta^s)$ and $\chi_{\mathbf{A}}(\alpha, \beta) = \chi_{\mathbf{A}}(\alpha \oplus \gamma, \beta \oplus \gamma)$ for all $\alpha, \beta, \gamma \in V_n$. Hence, we have the following proposition.

Proposition 2. *For all partitions $\mathbf{A} = \{A_1, \dots, A_u\}$ of the set $\{1, \dots, m\}$, $|A_i| = m/u$, $i = 1, \dots, u$, the metric $\chi_{\mathbf{A}}$ is G_{XS} -invariant.*

For any $p \in S_m$ denote by $\hat{p} \in S(V_n)$ the action of permutation p on V_n , i. e. for all $\alpha = (\alpha_1, \dots, \alpha_m) \in V_n$, $\alpha_i \in V_d$, $i = 1, \dots, m$,

$$\hat{p}: (\alpha_1, \dots, \alpha_m) \mapsto (\alpha_{1^{p^{-1}}}, \dots, \alpha_{m^{p^{-1}}}).$$

Proposition 3. *Let $\mathbf{A} = \{A_1, \dots, A_u\}$ be a partition of the set $\{1, \dots, m\}$, $A_i = \{i_1, \dots, i_{m/u}\} \subset \{1, \dots, m\}$, $i = 1, \dots, u$. Suppose g belongs to $G_{\mathbf{A}}$, $G_{\mathbf{A}} < S(V_n)$, $n = md$. Then there exists a permutation $p_g \in S_m$ such that*

$$g\hat{p}_g \in S(V(i_1, \dots, i_{m/u})) \wr S_{2^{n-n/u}}.$$

Proof. There exists $p \in S_m$ such that

$$A_i^p = \left\{ (i-1) \frac{m}{u} + 1, \dots, (i-1) \frac{m}{u} + \frac{m}{u} \right\}.$$

Let $\mathbf{A}' = \{A'_1, \dots, A'_u\}$ be a partition of the set $\{1, \dots, m\}$ and $A'_i = A_i^p$. Hence, $\chi_{\mathbf{A}'}$ is the Hamming metric, $\chi_{\mathbf{A}}(\alpha, \beta) = \chi_{\mathbf{A}'}(\alpha^{\widehat{p}}, \beta^{\widehat{p}})$, $G_{\mathbf{A}} = \widehat{p} G_{\mathbf{A}'} \widehat{p}^{-1}$. Suppose that $g \in G_{\mathbf{A}}$, $g = \widehat{p} f \widehat{p}^{-1}$, $f \in G_{\mathbf{A}'}$. Since $G_{\mathbf{A}'}$ is the group of isometry of the Hamming metric, for any $f \in G_{\mathbf{A}'}$ there exist $f_1, \dots, f_u \in S(V_{dm/u})$, $r \in S_u$ such that

$$f : (\beta_1, \dots, \beta_u) \rightarrow \left(\beta_{1^{r-1}}^{f_{1^{r-1}}}, \dots, \beta_{u^{r-1}}^{f_{u^{r-1}}} \right), \quad \beta_i \in V_{dm/u}, \quad i = 1, \dots, u.$$

Hence, for any $f \in G_{\mathbf{A}'}$ there exist $f_1, \dots, f_u \in S(V_{dm/u})$, $q \in S_m$ such that

$$f : (\beta_1, \dots, \beta_u) \rightarrow \left(\beta_1^{f_1}, \dots, \beta_u^{f_u} \right)^{\widehat{q}}$$

and

$$f \widehat{q}^{-1} \in \underbrace{S(V_{dm/u}) \times \dots \times S(V_{dm/u})}_u < S\left(V\left(1, \dots, \frac{m}{u}\right)\right) \wr S_{2^{n-n/u}}.$$

Suppose that $q' \in S_m$ is such that $p^{-1}q' = qp^{-1}$.

Thus, for $g \in G_{\mathbf{A}}$

$$\begin{aligned} g \widehat{q}' &= \widehat{p} f \widehat{p}^{-1} \widehat{q}' = \widehat{p} f \widehat{q} \widehat{p}^{-1} \in \widehat{p} S\left(V\left(1, \dots, \frac{m}{u}\right)\right) \wr S_{2^{n-n/u}} \widehat{p}^{-1} = \\ &= S\left(V\left(i_1, \dots, i_{\frac{m}{u}}\right)\right) \wr S_{2^{n-n/u}}. \end{aligned} \quad \square$$

4. Diffusion properties of linear mapping

Since partitions $\mathbf{V}(i_1, \dots, i_t)$ are G_{XS} -invariant, diffusion properties of linear mapping h are important. Let $\mathbf{W} = \mathbf{V}(i_1, \dots, i_t)$, $\mathbf{W}' = \mathbf{V}(j_1, \dots, j_r)$. Denote by $\rho(\mathbf{a}, \mathbf{b})$ the Euclid distance between real matrices $\mathbf{a}, \mathbf{b} \in \mathbb{R}_{n \times m}$, i. e.

$$\rho(\mathbf{a}, \mathbf{b}) = \sqrt{\sum_{i,j} (a_{i,j} - b_{i,j})^2}.$$

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

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

More precisely, we study the Euclid distance between matrix $\mathbf{c}_{\mathbf{W}, \mathbf{W}'}(h)$ and the uniform $(2^{(m-t)d} \times 2^{(m-r)d})$ -matrix $\|2^{(t+r-m)d}\|$. The smaller Euclid distance the better is diffusion property of a linear mapping h . For example,

$$\rho(\mathbf{c}_{\mathbf{W}, \mathbf{W}'}(h), \|2^{(t+r-m)d}\|)$$

takes maximal value, i. e. $2^{-td} \mathbf{c}_{\mathbf{W}, \mathbf{W}'}(h)$ is a substitution matrix, if and only if $h \in S(V(i_1, \dots, i_t)) \wr S_{2^{(m-t)d}}$, i. e. partition $\mathbf{W}$ is h -invariant. On the other hand, h has optimal diffusion property under pair of partitions $(\mathbf{W}, \mathbf{W}')$ if

$$\rho(\mathbf{c}_{\mathbf{W}, \mathbf{W}'}(h), \|2^{(t+r-m)d}\|)$$

takes minimal possible value. In the next proposition the lower bound for $\rho(\mathbf{c}_{\mathbf{W}, \mathbf{W}'}(h), \|2^{(t+r-m)d}\|)$ is derived.

Proposition 4. Let $h \in GL_n(2)$, $\mathbf{W} = \mathbf{V}(i_1, \dots, i_t)$, $\mathbf{W}' = \mathbf{V}(j_1, \dots, j_r)$, $1 \leq i_1 < \dots < i_t \leq m$, $1 \leq j_1 < \dots < j_r \leq m$, $n = md$, $m, d \geq 2$. Then

$$\rho(\mathbf{c}_{\mathbf{W}, \mathbf{W}'}(h), \|2^{(t+r-m)d}\|_{2^{(m-t)d}, 2^{(m-r)d}}) \geq \begin{cases} 0, & \text{if } t+r \geq m, \\ \sqrt{2^{md} - 2^{(t+r)d}}, & \text{if } t+r < m, \end{cases}$$

$$\mathbf{c}_{i,j}(h) \in \left\{ 0, 2^{td - \text{rank } h \left(\begin{smallmatrix} i_1, \dots, i_t \\ j'_1, \dots, j'_{m-r} \end{smallmatrix} \right)} \right\}, \quad (1)$$

where $\{j'_1, \dots, j'_{m-r}\} = \{1, \dots, m\} \setminus \{j_1, \dots, j_r\}$, $1 \leq j'_1 < \dots < j'_{m-r} \leq m$.

Proof. By definition we have

$$c_{i,j}(h) = |W_i^h \cap W_j'| = |(V(i_1, \dots, i_t) \oplus \delta)^h \cap (V(j_1, \dots, j_r) \oplus \gamma)|$$

for appropriate $\delta = (\delta_1, \dots, \delta_m)$, $\gamma = (\gamma_1, \dots, \gamma_m) \in V_n$, $\delta_l, \gamma_l \in V_d$, $l = 1, \dots, m$. Therefore $c_{i,j}(h)$ is equal to the number of solutions of the linear system

$$\alpha h \left(\begin{smallmatrix} i_1, \dots, i_t \\ j'_1, \dots, j'_{m-r} \end{smallmatrix} \right) = \left(\gamma_{j'_1}, \dots, \gamma_{j'_{m-r}} \right).$$

Hence, (1) holds true.

It is easy to show that $\rho(\mathbf{c}_{\mathbf{W}, \mathbf{W}'}(h), \|2^{(t+r-m)d}\|)$ takes its minimal value if and only if

$$\text{rank } h \left(\begin{smallmatrix} i_1, \dots, i_t \\ j'_1, \dots, j'_{m-r} \end{smallmatrix} \right) = \min \{td, (m-r)d\}.$$

Suppose that $t + r \geq m$. If

$$\text{rank } h \begin{pmatrix} i_1, \dots, i_t \\ j'_1, \dots, j'_{m-r} \end{pmatrix} = (m-r)d,$$

then $c_{i,j}(h) = 2^{(t+r-m)d}$ for all i, j . Hence

$$\mathbf{c}_{\mathbf{W}, \mathbf{W}'}(h) = \|2^{(t+r-m)d}\| \quad \text{and} \quad \rho(\mathbf{c}_{\mathbf{W}, \mathbf{W}'}(h), \|2^{(t+r-m)d}\|) = 0.$$

Suppose that $t + r < m$. Then we have

$$\begin{aligned} |\{(i, j) \in \{1, \dots, 2^{(m-t)d}\} \times \{1, \dots, 2^{(m-r)d}\} \mid c_{i,j}(h) = 1\}| &= 2^{md}, \\ |\{(i, j) \in \{1, \dots, 2^{(m-t)d}\} \times \{1, \dots, 2^{(m-r)d}\} \mid c_{i,j}(h) = 0\}| &= 2^{(2m-(t+r))d} - 2^{md}. \end{aligned}$$

Hence,

$$\begin{aligned} \rho(\mathbf{c}_{\mathbf{W}, \mathbf{W}'}(h), \|2^{(t+r-m)d}\|) &= \\ &= \sqrt{2^{dt} (1 - 2^{(t+r-m)d})^2 + (2^{d(m-r)} - 2^{dt}) (2^{(t+r-m)d})^2} = \\ &= \sqrt{2^{md} - 2^{(t+r)d}}. \end{aligned} \quad \square$$

Therefore $\rho(\mathbf{c}_{\mathbf{W}, \mathbf{W}'}(h), \|2^{(t+r-m)d}\|_{2^{n-t}d, 2^{n-tr}})$ depends on a rank of an appropriate submatrix only.

Let

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

Corollary 5. *The equalities*

$$\rho(\mathbf{c}_{\mathbf{R}, \mathbf{R}'}(h), \|2^{(t+r-m)d}\|_{2^{(m-t)d}, 2^{(m-r)d}}) = \varphi_m(t, r)$$

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

Proof. It is known [1] that $h \in GL_n(2)$ is an MDS linear mapping if and only if for all $t \in \{1, \dots, m\}$, $1 \leq i_1 < \dots < i_t \leq m$, $1 \leq j_1 < \dots < j_t \leq m$

$$\text{rank } h \begin{pmatrix} i_1, \dots, i_t \\ j_1, \dots, j_t \end{pmatrix} = t.$$

Therefore h is MDS linear mapping if and only if for all $t, r \in \{1, \dots, m\}$, $1 \leq i_1 < \dots < i_t \leq m$, $1 \leq j_1 < \dots < j_r \leq m$

$$\text{rank } h \left(\begin{smallmatrix} i_1, \dots, i_t \\ j_1, \dots, j_{m-r} \end{smallmatrix} \right) = \min \{td, (m-r)d\}.$$

Hence, h is an MDS linear mapping if and only if the equalities

$$\rho \left(\mathbf{c}_{\mathbf{R}, \mathbf{R}'}(h), \|2^{(t+r-m)d}\|_{2^{(m-t)d}, 2^{(m-r)d}} \right) = \varphi_m(t, r)$$

hold for all $t, r \in \{1, \dots, m\}$, $1 \leq i_1 < \dots < i_t \leq m$, $1 \leq j_1 < \dots < j_r \leq m$. $\square$

Corollary 5 gives a new characterization of MDS linear mappings. Moreover, MDS linear mappings which are used to increase the resistance to linear and differential methods may be derived from permutation group viewpoint. Taking into account this fact and papers [2, 3, 9, 12–14] we see that permutation group strategy may be a general approach for the design of block cipher primitives.

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

$$B_h = \left\{ (t, r) \left| \begin{array}{l} t+r \leq m, \exists 1 \leq i_1 < \dots < i_t \leq m, 1 \leq j_1 < \dots < j_r \leq m, \\ \rho(\mathbf{c}_{\mathbf{V}(i_1, \dots, i_t), \mathbf{V}(j_1, \dots, j_r)}(h), \|2^{(t+r-m)d}\|_{2^{(m-t)d}, 2^{(m-r)d}}) > \varphi_m(t, r) \end{array} \right. \right\}.$$

In the following proposition the differential branch number of a linear mapping h is expressed using the set B_h .

Proposition 6. For any $h \in GL_n(2)$

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

Proof. Let $\text{bn}_d(h) = b$ and $b < m+1$. Then there exist $t, r \in \mathbb{N}$, $\alpha \in V_n$ such that $t+r = b$, $\text{wt}(\alpha) = t$, $\text{wt}(\alpha^h) = r$. Therefore, there exist $1 \leq i_1 < \dots < i_t \leq m$, $1 \leq j_1 < \dots < j_r \leq m$ such that $|V(i_1, \dots, i_t)^h \cap V(j_1, \dots, j_r)| > 1$ and

$$\rho \left(\mathbf{c}_{\mathbf{V}(i_1, \dots, i_t), \mathbf{V}(j_1, \dots, j_r)}(h), \|2^{(t+r-m)d}\|_{2^{(m-t)d}, 2^{(m-r)d}} \right) > \varphi_m(t, r).$$

Hence, $(t, r) \in B_h$ and $\text{bn}_d(h) \geq \min \{t+r \mid (t, r) \in B_h\}$. On the other hand, if $(t_0, r_0) \in B_h$, then there exists $\alpha \in V_n$ such that $\text{wt}(\alpha) = t_0$, $\text{wt}(\alpha^h) = r_0$. Hence, $\text{bn}_d(h) \geq t_0 + r_0 \geq \min \{t+r \mid (t, r) \in B_h\}$. $\square$

Note that the linear branch number may be expressed similarly to the differential branch number using matrix ${}^t h$.

5. The distances from the linear mappings to the groups

$S(V(i_1, \dots, i_t)) \wr S_{2^{n-dt}}$ and $S_{2^{n/u}} \uparrow S_u$

Since G_{XS} is a subgroup of the wreath product $S(V(i_1, \dots, i_t)) \wr S_{2^{n-dt}}$ and $S_{2^{n/u}} \uparrow S_u$ it is important to study the Hamming distances from h to the groups $S(V(i_1, \dots, i_t)) \wr S_{2^{n-dt}}$ and $S_{2^{n/u}} \uparrow S_u$. If the Hamming distance is small, then there exist good approximations for h in the group $S_{2^{n/u}} \uparrow S_u$. Such approximations may be used for construction of a distinguisher of a cipher function.

Put $\chi_{\mathbf{W}}(h) = \min\{\chi(h, g) \mid g \in S(W) \wr S_{2^{n-dt}}\}$, where $\chi(h, g)$ is the Hamming distance between g and h , i.e. $\chi(g, h) = 2^n - \sum_{\alpha \in V_n} \text{Ind}\{\alpha^g = \alpha^h\}$.

Let $\mathbf{c}_{\mathbf{W}}(h) = c_{\mathbf{W}, \mathbf{W}}(h)$, $\mathbf{W} = \{W_i \mid i = 1, \dots, 2^{n-dt}\}$ be a partition of the vector space V_n and $|W_i| = 2^{dt}$, $i = 1, \dots, 2^{n-dt}$. It is known [14] that for all substitution $h \in S(V_n)$

$$\chi_{\mathbf{W}}(h) = 2^n - \max \left\{ \sum_{i=1}^{2^{n-dt}} c_{i,if}(h) \mid f \in S_{2^{dt}} \right\},$$

$$\chi_{\mathbf{W}}(h) \leq 2^n - 2^{n-dt} \lceil 2^{2dt-n} \rceil.$$

In the following proposition we obtain $\chi_{\mathbf{W}}(h)$ for linear mapping $h \in GL_n$ using the rank of its submatrix.

Proposition 7. Let $h \in GL_n(2)$, $t \in \{1, \dots, m-1\}$, $1 \leq i_1 < \dots < i_t \leq m$, $\mathbf{W} = \mathbf{V}(i_1, \dots, i_t)$, $n = md$. Then

$$\chi_{\mathbf{W}}(h) = 2^n - 2^{n - \text{rank } h \begin{pmatrix} i_1, \dots, i_t \\ i'_1, \dots, i'_{m-t} \end{pmatrix}},$$

where $\{i'_1, \dots, i'_{m-t}\} = \{1, \dots, m\} \setminus \{i_1, \dots, i_t\}$, $1 \leq i'_1 < \dots < i'_{m-t} \leq m$.

Proof. Using proposition 4, we get

$$c_{i,j}(h) \in \left\{ 0, 2^{td - \text{rank } h \begin{pmatrix} i_1, \dots, i_t \\ i'_1, \dots, i'_{m-t} \end{pmatrix}} \right\}, \quad i, j = 1, \dots, 2^{n-dt}.$$

It is easy to show that the matrix

$$2^{\text{rank } h \begin{pmatrix} i_1, \dots, i_t \\ i'_1, \dots, i'_{m-t} \end{pmatrix} - td} \mathbf{c}_{\mathbf{W}}(h)$$

is a doubly stochastic matrix. Therefore, there exists $g \in S_{2^{dt}}$ such that

$$c_{i,ig}(h) = 2^{td - \text{rank } h \begin{pmatrix} i_1, \dots, i_t \\ i'_1, \dots, i'_{m-t} \end{pmatrix}}, \quad i = 1, \dots, 2^{dt}.$$

Hence, we have

$$\begin{aligned}\chi_{\mathbf{W}}(h) &= 2^n - \max \left\{ \sum_{i=1}^{2^{n-dt}} c_{i,if}(h) \mid f \in S_{2^{dt}} \right\} = \\ &= 2^n - \sum_{i=1}^{2^{n-dt}} c_{i,ig}(h) = 2^n - 2^{n-\text{rank } h \left(\begin{smallmatrix} i_1, \dots, i_t \\ i'_1, \dots, i'_{m-t} \end{smallmatrix} \right)}.\end{aligned}\quad \square$$

Since

$$\text{rank } h \left(\begin{smallmatrix} i_1, \dots, i_t \\ i'_1, \dots, i'_{m-t} \end{smallmatrix} \right) = \min \{td, (m-t)d\},$$

we obtain the following corollary.

Corollary 8. *Let $h \in GL_n(2)$ be an MDS linear mapping. Then for all $t \in \{1, \dots, m-1\}$, $1 \leq i_1 < \dots < i_t \leq m$ the function $\chi_{\mathbf{W}}(h)$ achieves the maximum possible value, i. e.*

$$\chi_{\mathbf{W}}(h) = 2^n - 2^{n-dt} \lceil 2^{2dt-n} \rceil.$$

In the following proposition we obtain lower bounds for distances from MDS linear mappings to the groups $G_{\mathbf{A}}$.

Proposition 9. *Let $h \in GL_{md}$ be a MDS linear mapping, $\mathbf{A} = \{A_1, \dots, A_u\}$ be a partition of the set $\{1, \dots, m\}$, $|A_i| = n/u$. Then*

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

Proof. Suppose $\chi(h, G_{\mathbf{A}})$ is equal to r , $g \in G_{\mathbf{A}}$ and $\chi(h, g) = r$. Taking into account proposition 3, we obtain that there exists permutation $p \in S_m$ such that

$$g\hat{p} \in S(V(i_1, \dots, i_{n/u})) \wr S_{2^{n-n/u}}.$$

Notice that $h\hat{p}$ is MDS linear mapping. Using corollary 8, we get

$$\chi(h, g) = \chi(h\hat{p}, g\hat{p}) \geq \chi_{\mathbf{W}}(h\hat{p}) = 2^n - 2^{n-n/u}.\quad \square$$

From proposition 9 it follows that there are no good approximations for MDS linear mapping in the group $G_{\mathbf{A}}$.

References

- [1] Blaum M., Roth R.M., “On the lowest density MDS codes”, *IEEE Trans. Inf. Theory*, **45** (1999), 46–59.
- [2] Burov D. A., Pogorelov B. A., “An attack on 6 rounds of Khazad”, *Mathematical Aspects of Cryptography*, **7:2** (2016), 35–46.
- [3] Burov D. A., Pogorelov B. A., “The influence of linear mapping reducibility on choice of round constants”, *Mathematical Aspects of Cryptography*, **8:2** (2017), 51–64.
- [4] Daemen J., *Cipher and hash function design strategies based on linear and differential cryptanalysis. PhD thesis*, K. U. Leuven, 1995.
- [5] Daemen J., Rijmen V., *The design of Rijndael: AES — The Advanced Encryption Standard*, Heidelberg etc.: Springer, 2002.
- [6] Dixon J. D., Mortimer B., *Permutation groups*, Heidelberg etc.: Springer, 1996.
- [7] Guo J., Jean J., Nicolic I., Qiao K., Sasaki Y., Meng Sim S., *Invariant subspace attack against full Midori64*, Cryptology ePrint Archive. Report 2015/1189, <http://eprint.iacr.org/2015/1189>.
- [8] Kaluznin L. A., Klin M. Kh., Sushchanskii V. I., “The operation of exponentiation of permutation groups. I”, *Izvesiya VUZov. Ser. Matem.*, **8** (1979), 26–33 (in Russian).
- [9] Leander G., Abdelraheem M., Alkhzaimi H., Zenner E., “A cryptanalysis of PRINT cipher: The invariant subspace attack”. In: “CRYPTO’11”, Lect. Notes Comput. Sci., **6841**, 2011, 206–221.
- [10] Leander G., Minaud B., Sonjom S., “A generic approach to invariant subspace attacks: cryptanalysis of Robin, iSCREAM and Zorro”. In: “EUROCRYPT’15”, Lect. Notes Comput. Sci., **9056**, 2015, 254–283.
- [11] Pogorelov B. A., *Permutation groups. Part I, general questions*, Moscow, 1986 (in Russian).
- [12] Pogorelov B. A., Pudovkina M. A., “On the distance from permutations to imprimitive groups for a fixed system of imprimitivity”, *Discretnaya Matematika*, **25:3** (2013), 78–95 (In Russian); *Discrete Mathematics and Applications*, **24:2** (2014), 95–108.
- [13] Pogorelov B. A., Pudovkina M. A., “Combinatorial characterization of XL-layers”, *Mathematical Aspects of Cryptography*, **4:3** (2013), 99–129 (In Russian).
- [14] Pudovkina M. A., “Properties of X, S-layers”, *Prikl. Diskr. Mat. Suppl.*, № 5 (2012), 26–28 (In Russian).