Ежегодная международная научно-практическая конференция
«РусКрипто’2023»

О свойствах MDS-матриц XSL-блочных шифрсистем

Пудовкина Марина, профессор НИЯУ МИФИ
Смирнов Антон, ассистент НИЯУ МИФИ

XSL-блочные шифрсистемы

- Пусть $n \geq 2$,
- $V_{n^2}(2^q) - n^2$-мерное подпространство над
- (Частичная) раундовой функция $g_k: V_{n^2}(2^q) \to V_{n^2}(2^q)$,

$$g_k = hsv_k,$$

$$v_k: \alpha \mapsto \alpha + k, k, \alpha \in V_{n^2}(2^q),$$

  - s – фиксированная подстановка из $S(V_{n^2}(2^q))$.
- XSL-блочные шифрсистемы – частный случай.
  - X – слой наложения ключа (v_k) (принцип усложнения К. Шеннона)
  - S – слой s-боксов, реализует принцип перемешивания
  - L – линейный слой (h), реализует принцип рассеивания

Пример. AES, Кузнечик, Liliput и т.д.

XSL-блочные шифрсистемы

- n^2 – блок текста над $\mathbb{F}_{2^q}$

$$\alpha = (\alpha_{0,0}, \dots, \alpha_{0,n-1}, \dots, \alpha_{n-1,0}, \dots, \alpha_{n-1,n-1}) \in \mathbb{F}_{2^q}^{n^2}$$

соответствует $(n \times n)$-матрица над $\mathbb{F}_{2^q}$

$$\boldsymbol{a} = \varphi(\alpha) = [\![\alpha_{i,j}]\!] = \begin{pmatrix} \alpha_{0,0} & \dots & \alpha_{0,n-1} \\ \dots & \dots & \dots \\ \alpha_{n-1,0} & \dots & \alpha_{n-1,n-1} \end{pmatrix}$$

XSL-блочные шифрсистемы

- n^2 – блок текста над $\mathbb{F}_{2^q}$

$$\alpha = (\alpha_{0,0}, \dots, \alpha_{0,n-1}, \dots, \alpha_{n-1,0}, \dots, \alpha_{n-1,n-1}) \in \mathbb{F}_{2^q}^{n^2}$$

соответствует $(n \times n)$-матрица над $\mathbb{F}_{2^q}$

$$\boldsymbol{a} = \varphi(\alpha) = [\![\alpha_{i,j}]\!] = \begin{pmatrix} \alpha_{0,0} & \dots & \alpha_{0,n-1} \\ \dots & \dots & \dots \\ \alpha_{n-1,0} & \dots & \alpha_{n-1,n-1} \end{pmatrix}$$

Раундовый ключ

$$\boldsymbol{k} = \varphi(k) = [\![k_{i,j}]\!] = \begin{pmatrix} k_{0,0} & \dots & k_{0,n-1} \\ \dots & \dots & \dots \\ k_{n-1,0} & \dots & k_{n-1,n-1} \end{pmatrix},$$

XSL-блочные шифрсистемы

S-боксу

$$s = \left(s_{0,0}, \dots, s_{0,n-1}, \dots, s_{n-1,0}, \dots, s_{n-1,n-1}\right) \in S(\mathbb{F}_{2^q})^{n^2}$$

$$\alpha^s = s(\alpha) =$$

$$= \left(\alpha_{0,0}^{s_{0,0}}, \dots, \alpha_{0,n-1}^{s_{0,n-1}}, \dots, \alpha_{n-1,0}^{s_{n-1,0}}, \dots, \alpha_{n-1,n-1}^{s_{n-1,n-1}}\right)$$

XSL-блочные шифрсистемы

S-боксу

$$s = \left(s_{0,0}, \dots, s_{0,n-1}, \dots, s_{n-1,0}, \dots, s_{n-1,n-1}\right) \in S(\mathbb{F}_{2^q})^{n^2}$$

$$\alpha^s = s(\alpha) =$$

$$= \left(\alpha_{0,0}^{s_{0,0}}, \dots, \alpha_{0,n-1}^{s_{0,n-1}}, \dots, \alpha_{n-1,0}^{s_{n-1,0}}, \dots, \alpha_{n-1,n-1}^{s_{n-1,n-1}}\right)$$

соответствует

$$\boldsymbol{s} = \begin{pmatrix} s_{0,0} & \cdots & s_{0,n-1} \\ \cdots & \cdots & \cdots \\ s_{n-1,0} & \cdots & s_{n-1,n-1} \end{pmatrix}.$$

$$\boldsymbol{\alpha^s} = \varphi(\alpha^s) = \varphi\big(s(\alpha)\big) = \begin{pmatrix} s_{0,0}(\alpha_{0,0}) & \cdots & s_{0,n-1}(\alpha_{0,n-1}) \\ \cdots & \cdots & \cdots \\ s_{n-1,0}(\alpha_{n-1,0}) & \cdots & s_{n-1,n-1}(\alpha_{n-1,n-1}) \end{pmatrix}.$$

XSL-блочные шифрсистемы

Пусть $\boldsymbol{h} - (n \times n)$-матрица линейного преобразования $h: V_{n^2}(\mathbb{F}_{2^q}) \to V_{n^2}(\mathbb{F}_{2^q})$. Рассмотрим матрицу $\boldsymbol{h}$ в блочном виде

$$\boldsymbol{h} = \begin{pmatrix} \boldsymbol{h}_{0,0} & \dots & \boldsymbol{h}_{0,n-1} \\ \dots & \dots & \dots \\ \boldsymbol{h}_{n-1,0} & \dots & \boldsymbol{h}_{n-1,n-1} \end{pmatrix},$$

- $\boldsymbol{h}_{i,j} - (n \times n)$-подматрица матрицы $\boldsymbol{h}$ над $\mathbb{F}_{2^q}$, $i, j \in \{0, \dots, n-1\}$.

XSL-блочные шифрсистемы

Пусть $\boldsymbol{h} - (n \times n)$-матрица линейного преобразования $h: V_{n^2}(\mathbb{F}_{2^q}) \to V_{n^2}(\mathbb{F}_{2^q})$. Рассмотрим матрицу $\boldsymbol{h}$ в блочном виде

$$\boldsymbol{h} = \begin{pmatrix} \boldsymbol{h}_{0,0} & \dots & \boldsymbol{h}_{0,n-1} \\ \dots & \dots & \dots \\ \boldsymbol{h}_{n-1,0} & \dots & \boldsymbol{h}_{n-1,n-1} \end{pmatrix},$$

- $\boldsymbol{h}_{i,j} - (n \times n)$-подматрица матрицы $\boldsymbol{h}$ над $\mathbb{F}_{2^q}$, $i, j \in \{0, \dots, n-1\}$.

Для каждого $\alpha \in V_{n^2}(\mathbb{F}_{2^q})$ подматрицы матрицы $\boldsymbol{h}$ и координаты $\beta_{i,j}$ вектора

$$\beta^T = \left(\beta_{0,0}, \dots, \beta_{n-1,n-1}\right)^T = \boldsymbol{h}\alpha^T, \ \beta = \alpha^h = h(\alpha)$$

удовлетворяют равенству

$$\beta_{i,j} = \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} \left(\boldsymbol{h}_{i,t_1}\right)_{j,t_2} \alpha_{t_1,t_2}, \qquad i, j \in \{0, \dots, n-1\}.$$

Соотношения для ключа (по строкам)

Теорема 1. *Пусть существуют такие* $i, j_1, j_2, r, t \in \{0, \dots, n-1\}$, $\gamma_{j_1,j_2,r} \in \mathbb{F}_{2^q}$, *что элементы подматрицы* $\boldsymbol{h}_{i,r}$ *матрицы* $\boldsymbol{h}$ *линейного преобразования* $h: V_{n^2}(\mathbb{F}_{2^q}) \to V_{n^2}(\mathbb{F}_{2^q})$ *и подстановки S-бокса удовлетворяют условиям*

$$\left(\boldsymbol{h}_{i,r}\right)_{t,j_1} = \left(\boldsymbol{h}_{i,r}\right)_{t,j_2}, \left(\boldsymbol{h}_{i,r}\right)_{t,j_1} \neq 0, \tag{1}$$

$$\beta^{s_{r,j_1}} = \beta^{s_{r,j_2}} + \gamma_{j_1,j_2,r} \text{ для каждого } \beta \in \mathbb{F}_{2^q}.$$

Тогда для каждых $\delta \in \mathbb{F}_{2^q}$, $\alpha \in V_{n^2}(\mathbb{F}_{2^q})$ *и* $k \in V_{n^2}(\mathbb{F}_{2^q})$ *существует*

$$\omega \in \langle \alpha_{r,j_1} + \alpha_{r,j_2} + k_{r,j_1} + k_{r,j_2} \rangle + \delta, \tag{2}$$

удовлетворяющее равенству

$$\left(\alpha_{r,j_1} + \omega + k_{r,j_1}\right)^{s_{r,j_1}} + \left(\alpha_{r,j_1} + \omega + \delta + k_{r,j_1}\right)^{s_{r,j_1}} + \left(\alpha_{r,j_2} + k_{r,j_2}\right)^{s_{r,j_2}} + \left(\alpha_{r,j_1} + \delta + k_{r,j_2}\right)^{s_{r,j_2}} = 0. \tag{3}$$

Соотношения для ключа (по строкам)

Для каждой пары $i, j \in \{0, \dots, n-1\}$ рассмотрим вектор $\varepsilon_{i,j} \in V_{n^2}(\mathbb{F}_{2^q})$, координаты которого заданы условием

$$\left(\varepsilon_{i,j}\right)_{t,r} = 1_{\mathbb{F}_{2^q}} \cdot \mathrm{I}\big((i,j) = (t,r)\big) \text{ при } t, r \in \{0, \dots, n-1\}.$$

- $\mathrm{I}(A)$ – индикатор выполнения условия A

Соотношения для ключа (по строкам)

Следствие 2. *Пусть существуют такие* $i, j_1, j_2, r, t \in \{0, \dots, n-1\}$, $\gamma_{j_1,j_2,r} \in \mathbb{F}_{2^q}$, *что элементы подматриц* $\boldsymbol{h}_{i,j_1}, \boldsymbol{h}_{i,j_2}$ *матрицы* $\boldsymbol{h}$ *линейного преобразования* $h: V_{n^2}(\mathbb{F}_{2^q}) \to V_{n^2}(\mathbb{F}_{2^q})$ *и подстановки S-бокса удовлетворяют условиям*

$$\left(\boldsymbol{h}_{i,r}\right)_{t,j_1} = \left(\boldsymbol{h}_{i,r}\right)_{t,j_2}, \left(\boldsymbol{h}_{i,r}\right)_{t,j_1} \neq 0,$$

$$\beta^{S_{r,j_1}} = \beta^{S_{r,j_2}} + \gamma_{j_1,j_2,r} \text{ для каждого } \beta \in \mathbb{F}_{2^q}.$$

Тогда для каждых $\delta \in \mathbb{F}_{2^q} \backslash \{0\}$, $\alpha \in V_{n^2}(\mathbb{F}_{2^q})$ *равенство*

$$\vartheta_{i,t}^{(\omega)} = 0$$

выполняется по крайней мере для двух $\omega \in \mathbb{F}_{2^q}$, *где*

$$\vartheta^{(\omega)} = \left(\alpha + \omega \cdot \varepsilon_{r,j_1} + k\right)^{sh} + \left(\alpha + \delta \cdot \varepsilon_{r,j_2} + (\omega + \delta) \cdot \varepsilon_{r,j_1} + k\right)^{sh}.$$

- $\vartheta^{(\omega)}$ – разность при зашифровании раундовой функцией пары открытых текстов

$$\alpha + \omega \cdot \varepsilon_{r,j_1}, \qquad \alpha + \delta \cdot \varepsilon_{r,j_2} + (\omega + \delta) \cdot \varepsilon_{r,j_1}.$$

В алгоритме AES

- $n = 4, q = 8,$
- $b -$ подстановка S-бокса алгоритма AES на $\mathbb{F}_{2^8}$,
- $s_{i,r} = b -$ для $i, r \in \{0, \dots, 3\}$
- Для $i, r \in \{0, \dots, 3\}$

$$u = h_{i,r} = \begin{pmatrix} \lambda & \lambda+1 & 1 & 1 \\ 1 & \lambda & \lambda+1 & 1 \\ 1 & 1 & \lambda & \lambda+1 \\ \lambda+1 & 1 & 1 & \lambda \end{pmatrix}$$

- Имеем при $t \in \{0, \dots, 3\}$:

$$(h_{i,r})_{0,2} = (h_{i,r})_{0,3},\ (h_{i,r})_{1,0} = (h_{i,r})_{1,3},$$
$$(h_{i,r})_{2,0} = (h_{i,r})_{2,1}, (h_{i,r})_{3,1} = (h_{i,r})_{3,2}.$$

Теорема 1 в атаке бумеранга на 5-раундовый AES

- *Ronjom S., Bardeh N. G., Helleseth T.*, Yoyo Tricks with AES, ASIACRYPT 2017, Part I, LNCS 10624, pp. 217–243, 2017.

Атака типа бумерангом на 5-раундовый AES основана на равенстве

$$\left(\eta_0^{(1)} + k_0\right)^{(b,b,b,b)} u + \left(\eta_0^{(2)} + k_0\right)^{(b,b,b,b)} u = (\vartheta_{0,0}, \vartheta_{0,2}, 0, \vartheta_{0,3}) \qquad (4)$$

для пары о.т.

$$\eta^{(1)} = \left(\eta_0^{(1)}, \eta_1^{(1)}, \eta_2^{(1)}, \eta_3^{(1)}\right), \eta^{(2)} = \left(\eta_0^{(2)}, \eta_1^{(2)}, \eta_2^{(2)}, \eta_3^{(2)}\right) \in V_4\left(2^8\right)^4,$$

полученных из подобранных ш.т.

- Параллельно действуем 4-мя подстановками S-бокса на 32-битные подблоки $\eta_0^{(1)}, \eta_0^{(2)}$.
- Уменьшение числа опробуемых байт подблоков раундового ключа в силу равенства (4)

Теорема 1 в атаке бумеранга на 5-раундовый AES

Каждому вектору $\theta = (\theta_0, \dots, \theta_{n-1}) \in V_n(2)$ поставим в соответствие отображение $\rho_\theta : V_n(2^q) \times V_n(2^q) \to V_n(2^q)$, заданное для всех $\alpha, \beta \in V_n(2^q)$ условием

$$\rho_\theta(\alpha, \beta)_i = \alpha_i, \text{ если } \theta_i = 1,$$

$$\rho_\theta(\alpha, \beta)_i = \beta_i, \text{ если } \theta_i = 0,$$

т.е.

$$\rho_\theta(\alpha, \beta)_i = \alpha_i\theta_i + \beta_i(\theta_i + 1).$$

Теорема 1 в атаке бумеранга на 5-раундовый AES

- Пусть $f_k^{(5)}$ – 5-раундовая функция зашифрования AES на ключе k

Общая идея:

Для каждого $\omega \in \mathbb{F}_{2^q}$:

I. Формируем пары открытых текстов

$$\alpha^{(1)}(\omega) = \omega \cdot \varepsilon_{0,1}, \qquad \alpha^{(2)}(\omega, \delta) = \delta \cdot \varepsilon_{0,0} + (\omega + \delta) \cdot \varepsilon_{0,1}$$

для всех $\delta \in \mathbb{F}_{2^q}$.

- I.1. Получаем пару ш.т.

$$\gamma^{(1)} = f_k^{(5)}\left(\alpha^{(1)}(\omega)\right), \gamma^{(2)} = f_k^{(5)}\left(\alpha^{(2)}(\omega, \delta)\right),$$

зашифровывав $\alpha^{(1)}(\omega)$, $\alpha^{(2)}(\omega, \delta)$.

Теорема 1 в атаке бумеранга на 5-раундовый AES

- I.2. Вычисляем новую пару ш.т.

$$\left(\beta^{(1)}, \beta^{(2)}\right) = (\rho_\theta(\gamma^{(1)}, \gamma^{(2)}), \rho_\theta(\gamma^{(2)}, \gamma^{(1)}))$$

и соответствующие им пары о.т.

$$(\eta^{(1)}, \eta^{(2)}) = \left(\left(f_k^{(5)}\right)^{-1}(\beta^{(1)}), \left(f_k^{(5)}\right)^{-1}(\beta^{(2)})\right).$$

Теорема 1 в атаке бумеранга на 5-раундовый AES

- I.3. Проверяем справедливость равенства

$$\left(\eta_0^{(1)} + k_0\right)^{(b,b,b,b)} u + \left(\eta_0^{(2)} + k_0\right)^{(b,b,b,b)} u = (y_0, y_1, 0, y_3) \qquad (4)$$

для пары о.т.

$$\eta^{(1)} = \left(\eta_0^{(1)}, \eta_1^{(1)}, \eta_2^{(1)}, \eta_3^{(1)}\right), \eta^{(2)} = \left(\eta_0^{(2)}, \eta_1^{(2)}, \eta_2^{(2)}, \eta_3^{(2)}\right) \in V_4\left(2^8\right)^4,$$

- Пара о.т.$\eta^{(1)}, \eta^{(2)}$ считается «правильной», справедливо равенство (4).
- Для правильно пары равенство (2)

$$\omega \in \left\{k_{0,0} + k_{0,1}, k_{0,0} + k_{0,1} + \delta\right\}. \qquad (2)$$

позволяет сократить опробование k_0 до 2^{24}.

Теорема 1 в атаке бумеранга на 5-раундовый AES

- Трудоемкость – 2^{31} (5-раундовых шифрований)
- Число адаптивно подобранных открытых и шифрованных текстов – $2^{11,32}$
  - соответствуют $2^{10,32}$ парам.

Ronjom S., Bardeh N. G., Helleseth T., Yoyo Tricks with AES, ASIACRYPT 2017, Part I, LNCS 10624, pp. 217–243, 2017.

Соотношения для ключа (по столбцам)

Теорема 2. *Пусть существуют такие* $i, j_1, j_2, r, t \in \{0, \dots, n-1\}$, $\gamma_{j_1,j_2,r} \in \mathbb{F}_{2^q}$, *что элементы подматриц* $\boldsymbol{h}_{i,j_1}, \boldsymbol{h}_{i,j_2}$ *матрицы* $\boldsymbol{h}$ *линейного преобразования* $h: V_{n^2}(\mathbb{F}_{2^q}) \to V_{n^2}(\mathbb{F}_{2^q})$ *и подстановки* S*-бокса удовлетворяют условиям*

$$\left(\boldsymbol{h}_{i,j_1}\right)_{t,r} = \left(\boldsymbol{h}_{i,j_2}\right)_{t,r}, \ \left(\boldsymbol{h}_{i,j_1}\right)_{t,r} \neq 0, \tag{5}$$

$$\beta^{s_{j_1,r}} = \beta^{s_{j_2,r}} + \gamma_{j_1,j_2,r} \text{ для каждого } \beta \in \mathbb{F}_{2^q}.$$

Тогда для каждых $\delta \in \mathbb{F}_{2^q}$, $\alpha \in V_{n^2}(\mathbb{F}_{2^q})$ *и* $k \in V_{n^2}(\mathbb{F}_{2^q})$ *существует*

$$\omega \in \langle \alpha_{j_1,r} + \alpha_{j_2,r} + k_{j_1,r} + k_{j_2,r} \rangle + \delta,$$

удовлетворяющее равенству

$$\left(\alpha_{j_1,r} + k_{j_1,r} + \delta\right)^{s_{j_1,r}} + \left(\alpha_{j_1,r} + k_{j_1,r}\right)^{s_{j_1,r}} +$$

$$+ \left(\alpha_{j_2,r} + k_{j_2,r} + \omega + \delta\right)^{s_{j_2,r}} + \left(\alpha_{j_2,r} + k_{j_2,r} + \omega\right)^{s_{j_2,r}} = 0. \tag{6}$$

В алгоритме Кузнечик

- $n = 4, q = 8,$
- $b -$ подстановка S-бокса алгоритма «Кузнечик» на $\mathbb{F}_{2^8}$,
- $s_{i,r} = b -$ для $i, r \in \{0, \dots, 3\}$

В алгоритме Кузнечик

$$L_{0,0} = \begin{pmatrix} 207 & 152 & 116 & 191 \\ 110 & 32 & 198 & 218 \\ 162 & 200 & 135 & 112 \\ 118 & 51 & 16 & 12 \end{pmatrix}, \quad L_{1,0} = \begin{pmatrix} 114 & 242 & 107 & 202 \\ 108 & 118 & 236 & 12 \\ 72 & 213 & 98 & 23 \\ 122 & 230 & 78 & 26 \end{pmatrix} \quad L_{2,0} = \begin{pmatrix} 184 & 73 & 135 & 20 \\ 93 & 212 & 184 & 47 \\ 39 & 159 & 190 & 104 \\ 189 & 149 & 94 & 48 \end{pmatrix}, \quad L_{3,0} = \begin{pmatrix} 16 & 233 & 208 & 217 \\ 221 & 153 & 117 & 202 \\ 132 & 45 & 116 & 150 \\ 148 & 32 & 133 & 16 \end{pmatrix},$$

$$L_{0,1} = \begin{pmatrix} 147 & 142 & 242 & 243 \\ 144 & 72 & 137 & 156 \\ 104 & 67 & 28 & 43 \\ 28 & 17 & 214 & 106 \end{pmatrix}, \quad L_{1,1} = \begin{pmatrix} 32 & 235 & 2 & 164 \\ 197 & 188 & 175 & 110 \\ 6 & 45 & 196 & 231 \\ 187 & 46 & 241 & 190 \end{pmatrix} \quad L_{2,1} = \begin{pmatrix} 203 & 141 & 171 & 73 \\ 141 & 18 & 238 & 246 \\ 26 & 124 & 173 & 201 \\ 233 & 96 & 191 & 16 \end{pmatrix}, \quad L_{3,1} = \begin{pmatrix} 217 & 243 & 148 & 61 \\ 151 & 68 & 90 & 224 \\ 93 & 119 & 111 & 222 \\ 194 & 192 & 1 & 251 \end{pmatrix},$$

$$L_{0,2} = \begin{pmatrix} 10 & 191 & 246 & 169 \\ 193 & 100 & 184 & 45 \\ 161 & 99 & 48 & 107 \\ 166 & 215 & 246 & 73 \end{pmatrix}, \quad L_{1,2} = \begin{pmatrix} 141 & 212 & 196 & 1 \\ 163 & 225 & 144 & 88 \\ 213 & 235 & 153 & 120 \\ 212 & 175 & 55 & 177 \end{pmatrix} \quad L_{2,2} = \begin{pmatrix} 9 & 108 & 42 & 1 \\ 8 & 84 & 15 & 243 \\ 132 & 47 & 235 & 254 \\ 239 & 57 & 236 & 145 \end{pmatrix}, \quad L_{3,2} = \begin{pmatrix} 123 & 255 & 100 & 145 \\ 148 & 166 & 49 & 211 \\ 84 & 180 & 141 & 209 \\ 1 & 192 & 194 & 16 \end{pmatrix},$$

$$L_{0,3} = \begin{pmatrix} 234 & 142 & 77 & 110 \\ 134 & 68 & 208 & 162 \\ 159 & 48 & 227 & 118 \\ 7 & 20 & 232 & 114 \end{pmatrix}, \quad L_{1,3} = \begin{pmatrix} 101 & 221 & 76 & 108 \\ 14 & 2 & 195 & 72 \\ 82 & 245 & 22 & 122 \\ 212 & 42 & 110 & 184 \end{pmatrix} \quad L_{2,3} = \begin{pmatrix} 96 & 142 & 75 & 93 \\ 152 & 200 & 127 & 39 \\ 198 & 72 & 162 & 189 \\ 127 & 72 & 137 & 16 \end{pmatrix}, \quad L_{3,3} = \begin{pmatrix} 82 & 248 & 13 & 221 \\ 223 & 72 & 100 & 132 \\ 68 & 60 & 165 & 148 \\ 133 & 32 & 148 & 1 \end{pmatrix}.$$

В алгоритме Кузнечик

- $n = 4, q = 8,$
- $b -$ подстановка S-бокса алгоритма «Кузнечик» на $\mathbb{F}_{2^8}$,
- $s_{i,r} = b -$ для $i, r \in \{0, \dots, 3\}$

- Для r-го столбца подматриц матрицы $\boldsymbol{h}$ справедливы равенства:

$$\left(\boldsymbol{h}_{i,j_1}\right)_{t,r} = \left(\boldsymbol{h}_{i,j_2}\right)_{t,r}, \left(\boldsymbol{h}_{i,j_1}\right)_{t,r} \neq 0, \quad (5)$$

- $\left(\boldsymbol{h}_{1,2}\right)_{3,0} = \left(\boldsymbol{h}_{1,3}\right)_{3,0} = 212$ при $r = 0$ $(t = 3, i = 1, j_1 = 2, j_2 = 3)$
- $\left(\boldsymbol{h}_{3,1}\right)_{3,1} = \left(\boldsymbol{h}_{3,2}\right)_{3,1} = 192$ при $r = 1$ $(t = 3, i = 3, j_1 = 1, j_2 = 2)$
- $r = 2$ не существует элементов подматриц, удовлетворяющих равенству (5)
- $\left(\boldsymbol{h}_{3,0}\right)_{3,3} = \left(\boldsymbol{h}_{3,2}\right)_{3,3} = 16$ при $r = 3$ $(t = 3, i = 3, j_1 = 0, j_2 = 2)$

В алгоритме Liliput

- $n = 4, q = 8,$
- $b -$ подстановка алгоритма Lilliput на $\mathbb{F}_{2^8}$,
- $\alpha^{s_{i,r}} = \alpha^b + \gamma_{i,r}$ для каждого $\alpha \in \mathbb{F}_{2^8}$,
  - $\gamma_{i,r}$ – фиксированные константы для $i, r \in \{0, \dots, 3\}$
  - подстановки S-бокса различны

Berger T., Francq J., Minier M., Thomas G., Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. IEEE Trans. Computers. 2015. V. 65. Iss. 7. P. 99

В алгоритме Liliput

$$P_{0,0} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, P_{1,0} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, P_{2,0} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, P_{3,0} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix},$$

$$P_{0,1} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, P_{1,1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, P_{2,1} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, P_{3,1} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix},$$

$$P_{0,2} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, P_{1,2} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, P_{2,2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, P_{3,2} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$P_{0,3} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, P_{1,3} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, P_{2,3} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, P_{3,3} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

В алгоритме Liliput

- $n = 4, q = 8,$
- $b -$ подстановка алгоритма Lilliput на $\mathbb{F}_{2^8}$,
- $\alpha^{s_{i,r}} = \alpha^b + \gamma_{i,r}$ для каждого $\alpha \in \mathbb{F}_{2^8}$,
- Для r-го столбца подматриц матрицы $\boldsymbol{h}$ справедливы равенства:

$$\left(\boldsymbol{h}_{i,j_1}\right)_{t,r} = \left(\boldsymbol{h}_{i,j_2}\right)_{t,r}, \left(\boldsymbol{h}_{i,j_1}\right)_{t,r} \neq 0, \quad (5)$$

- $r = 0$ не существует элементов подматриц, удовлетворяющих равенству (5)
- $\left(\boldsymbol{h}_{3,0}\right)_{3,1} = \left(\boldsymbol{h}_{3,1}\right)_{3,1} = 1$ при $r = 1$
- $\left(\boldsymbol{h}_{3,0}\right)_{3,2} = \left(\boldsymbol{h}_{3,1}\right)_{3,2} = 1$ при $r = 2$
- $\left(\boldsymbol{h}_{3,0}\right)_{3,3} = \left(\boldsymbol{h}_{3,3}\right)_{3,3} = 1$ при $r = 3$

Спасибо за внимание!