

# Ключевое пространство криптосистемы Мак-Элиса–Сидельникова

Дипломная работа

Чижов Иван Владимирович

*Научный руководитель:*

*к.ф.-м.н. доцент Карпунин Григорий Анатольевич*

Московский государственный университет имени М. В. Ломоносова

Факультет вычислительной математики и кибернетики

Кафедра информационной безопасности

27 апреля 2021 г.



# Содержание

Криптосистема Мак-Элиса

Криптосистема Мак-Элиса–Сидельникова

Устройство криптосистемы Мак-Элиса–Сидельникова

Пространство ключей

Описание множества открытых ключей

Случай произвольного числа блоков

Случай двух блоков

О полиномиальной эквивалентности криптосистем Мак-Элиса и  
Мак-Элиса–Сидельникова с ограничениями на ключевое пространство.

Восстановление части ключа

Заключение

Список публикаций



# Криптосистемы Мак-Элиса

- ▶ Криптосистема с открытым ключом. Предложена в 1978 году Р.Дж. Мак-Элисом.



# Криптосистемы Мак-Элиса

- ▶ Криптосистема с открытым ключом. Предложена в 1978 году Р.Дж. Мак-Элисом.
- ▶ Стойкость основана на трудности некоторых задачах теории кодов, исправляющих ошибки.



# Криптосистемы Мак-Элиса

- ▶ Криптосистема с открытым ключом. Предложена в 1978 году Р.Дж. Мак-Элисом.
- ▶ Стойкость основана на трудности некоторых задачах теории кодов, исправляющих ошибки.
- ▶ Р.Дж. Мак-Элис предложил использовать семейство кодов Гоппы с параметрами  $[1024, 524, 101]$ ;



# Криптосистемы Мак-Элиса

- ▶ Криптосистема с открытым ключом. Предложена в 1978 году Р.Дж. Мак-Элисом.
- ▶ Стойкость основана на трудности некоторых задачах теории кодов, исправляющих ошибки.
- ▶ Р.Дж. Мак-Элис предложил использовать семейство кодов Гоппы с параметрами  $[1024, 524, 101]$ ;
- ▶ Г. Нидеррайтер в 1986 году предложил использовать обобщённые коды Рида–Соломона. В 1992 году В.М. Сидельников и С.О. Шестаков взломали криптосистему Мак-Элиса на основе этих кодов.



# Криптосистемы Мак-Элиса

- ▶ Криптосистема с открытым ключом. Предложена в 1978 году Р.Дж. Мак-Элисом.
- ▶ Стойкость основана на трудности некоторых задачах теории кодов, исправляющих ошибки.
- ▶ Р.Дж. Мак-Элис предложил использовать семейство кодов Гоппы с параметрами  $[1024, 524, 101]$ ;
- ▶ Г. Нидеррайтер в 1986 году предложил использовать обобщённые коды Рида–Соломона. В 1992 году В.М. Сидельников и С.О. Шестаков взломали криптосистему Мак-Элиса на основе этих кодов.
- ▶ В.М. Сидельников в 1994 году предложил использовать двоичные коды Рида–Маллера  $RM(r, m)$ .



# Содержание

Криптосистема Мак-Элиса

Криптосистема Мак-Элиса–Сидельникова

Устройство криптосистемы Мак-Элиса–Сидельникова

Пространство ключей

Описание множества открытых ключей

Случай произвольного числа блоков

Случай двух блоков

О полиномиальной эквивалентности криптосистем Мак-Элиса и  
Мак-Элиса–Сидельникова с ограничениями на ключевое пространство.

Восстановление части ключа

Заключение

Список публикаций





## Общие сведения

- ▶ Предложена В.М. Сидельниковым в 1994 году как альтернатива криптосистеме Мак-Элиса.



## Общие сведения

- ▶ Предложена В.М. Сидельниковым в 1994 году как альтернатива криптосистеме Мак-Элиса.
- ▶ Оригинальная криптосистема строится на основе двоичных кодов Рида–Маллера  $RM(r, m)$ .



# Секретный и открытый ключ.

- ▶ Параметры:
  - ▶  $r$  — натуральное число;
  - ▶  $m$  — натуральное число,  $m \geq r$ ;
  - ▶  $R$  — порождающая матрица кода Рида–Маллера  $RM(r, m)$ ;
  - ▶  $u$  — натуральное число.



# Секретный и открытый ключ.

- ▶ Параметры:
  - ▶  $r$  — натуральное число;
  - ▶  $m$  — натуральное число,  $m \geq r$ ;
  - ▶  $R$  — порождающая матрица кода Рида–Маллера  $RM(r, m)$ ;
  - ▶  $u$  — натуральное число.
- ▶ Секретный ключ:
  - ▶  $H_1, \dots, H_u$  — невырожденные  $(k \times k)$ -матрицы над полем  $GF(2)$ .
  - ▶  $\Gamma$  — перестановочная  $(un \times un)$ -матрица,  $\Gamma \in S_{u \cdot n}$ .



## Секретный и открытый ключ.

- ▶ Параметры:
  - ▶  $r$  — натуральное число;
  - ▶  $m$  — натуральное число,  $m \geq r$ ;
  - ▶  $R$  — порождающая матрица кода Рида–Маллера  $RM(r, m)$ ;
  - ▶  $u$  — натуральное число.
- ▶ Секретный ключ:
  - ▶  $H_1, \dots, H_u$  — невырожденные  $(k \times k)$ -матрицы над полем  $GF(2)$ .
  - ▶  $\Gamma$  — перестановочная  $(un \times un)$ -матрица,  $\Gamma \in S_{u \cdot n}$ .
- ▶ Открытый ключ — матрица

$$G' = (H_1 R \| H_2 R \| \dots \| H_u R) \Gamma.$$



# Содержание

Криптосистема Мак-Элиса

Криптосистема Мак-Элиса–Сидельникова

Устройство криптосистемы Мак-Элиса–Сидельникова

Пространство ключей

Описание множества открытых ключей

Случай произвольного числа блоков

Случай двух блоков

О полиномиальной эквивалентности криптосистем Мак-Элиса и  
Мак-Элиса–Сидельникова с ограничениями на ключевое пространство.

Восстановление части ключа

Заключение

Список публикаций



## Основные определения.

- ▶ Секретные ключи  $(H'_1, \dots, H'_u, \Gamma')$  и  $(H''_1, \dots, H''_u, \Gamma'')$  называются **эквивалентными**, если

$$(H'_1 R \parallel \dots \parallel H'_u R) \Gamma' = (H''_1 R \parallel \dots \parallel H''_u R) \Gamma''$$

- ▶  $[(H_1, \dots, H_u, \Gamma)]$  — класс эквивалентности с представителем  $(H_1, \dots, H_u, \Gamma)$ .



## Основные определения.

- ▶ Секретные ключи  $(H'_1, \dots, H'_u, \Gamma')$  и  $(H''_1, \dots, H''_u, \Gamma'')$  называются **эквивалентными**, если

$$(H'_1 R \parallel \dots \parallel H'_u R) \Gamma' = (H''_1 R \parallel \dots \parallel H''_u R) \Gamma''$$

- ▶  $[(H_1, \dots, H_u, \Gamma)]$  — класс эквивалентности с представителем  $(H_1, \dots, H_u, \Gamma)$ .
- ▶ Введём множество  $\mathcal{G}(H_1, \dots, H_u)$ :

$$\mathcal{G}(H_1, \dots, H_u) = \{\Gamma \in S_{un} \mid \exists H'_1, \dots, H'_u \text{ такие, что} \\ (H_1 R \parallel \dots \parallel H_u R) \Gamma = (H'_1 R \parallel \dots \parallel H'_u R)\}$$





# Оценка мощности множества открытых ключей

## Теорема 1

Справедливы неравенства для числа  $|\mathcal{E}|$  открытых ключей криптосистемы Мак-Элиса–Сидельникова с  $u > 1$  блоками на основе кодов Рида–Маллера  $RM(r, m)$

$$\frac{(u \cdot n)! h_k}{(u!)^n |Aut(RM(r, m))|} \leq |\mathcal{E}| < \frac{(u \cdot n)! (h_k)^u}{u! |Aut(RM(r, m))|^u}.$$

Здесь

- ▶  $n$  — длина кода Рида–Маллера  $RM(r, m)$ ,
- ▶  $h_k$  — число обратимых  $(k \times k)$ -матриц над полем  $GF(2)$ ,
- ▶  $Aut(RM(r, m))$  — группа автоморфизмов кода  $RM(r, m)$ .

Оценка сверху принадлежит Г.А. Карпунину (2004).



# Содержание

Криптосистема Мак-Элиса

Криптосистема Мак-Элиса–Сидельникова

Устройство криптосистемы Мак-Элиса–Сидельникова

Пространство ключей

Описание множества открытых ключей

Случай произвольного числа блоков

Случай двух блоков

О полиномиальной эквивалентности криптосистем Мак-Элиса и  
Мак-Элиса–Сидельникова с ограничениями на ключевое пространство.

Восстановление части ключа

Заключение

Список публикаций



## Множество эквивалентных ключей.

### Теорема 2а

Пусть

- ▶ матрицы  $D_1, D_2, \dots, D_u$  задают автоморфизмы  $\sigma_1, \sigma_2, \dots, \sigma_u$  кода Рида–Маллера  $RM(r, m)$ ;
- ▶  $\sigma_j[i]$  — расширенный автоморфизм, соответствующий  $\sigma_j$ ,
- ▶  $H$  — любая невырожденная матрица.

Тогда класс эквивалентности  $[(HD_1, HD_2, \dots, HD_u, \Gamma)]$  состоит из кортежей вида

$$(HA_1, HA_2, \dots, HA_u, \gamma_1^{-1}[1] \cdot \gamma_2^{-1}[2] \dots \gamma_u^{-1}[u] \Gamma' \cdot \sigma_1[1] \cdot \sigma_2[2] \dots \sigma_u[u] \Gamma),$$

здесь для  $\Gamma'$  выполнено  $(R\|R\| \dots \|R)\Gamma' = (R\|R\| \dots \|R)$ .



# Содержание

Криптосистема Мак-Элиса

Криптосистема Мак-Элиса–Сидельникова

Устройство криптосистемы Мак-Элиса–Сидельникова

Пространство ключей

Описание множества открытых ключей

Случай произвольного числа блоков

Случай двух блоков

О полиномиальной эквивалентности криптосистем Мак-Элиса и  
Мак-Элиса–Сидельникова с ограничениями на ключевое пространство.

Восстановление части ключа

Заключение

Список публикаций



## Специальный тип матриц.

Рассмотрим матрицу  $T_{\tilde{A}}^I, I = \{i_1, i_2, \dots, i_p\}$  вида

$$\left( \begin{array}{cccccccccc} & & & & i_1 & & i_2 & & i_p & & \\ & & & & \downarrow & & \downarrow & & \downarrow & & \\ & 1 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ & 0 & 1 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ & \vdots & \vdots & \dots & \vdots & \dots & \vdots & \dots & \vdots & \dots & \vdots \\ i_1 \rightarrow & \alpha_1^{i_1} & \alpha_2^{i_1} & \dots & \alpha_{i_1}^{i_1} & \dots & \alpha_{i_2}^{i_1} & \dots & \alpha_{i_p}^{i_1} & \dots & \alpha_k^{i_1} \\ & \vdots & \vdots & \dots & \vdots & \dots & \vdots & \dots & \vdots & \dots & \vdots \\ i_2 \rightarrow & \alpha_1^{i_2} & \alpha_2^{i_2} & \dots & \alpha_{i_1}^{i_2} & \dots & \alpha_{i_2}^{i_2} & \dots & \alpha_{i_p}^{i_2} & \dots & \alpha_k^{i_2} \\ & \vdots & \vdots & \dots & \vdots & \dots & \vdots & \dots & \vdots & \dots & \vdots \\ i_p \rightarrow & \alpha_1^{i_p} & \alpha_2^{i_p} & \dots & \alpha_{i_1}^{i_p} & \dots & \alpha_{i_2}^{i_p} & \dots & \alpha_{i_p}^{i_p} & \dots & \alpha_k^{i_p} \\ & \vdots & \vdots & \dots & \vdots & \dots & \vdots & \dots & \vdots & \dots & \vdots \\ & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{array} \right),$$



Первый случай.  $|I| = 1$ ,  $I = \{i\}$ .

### Теорема 2b

Класс эквивалентности  $[(H, HT_{\tilde{\alpha}}^i, \Gamma)]$  состоит из кортежей вида

$$(HT_{\tilde{\beta}}^i D_1, HT_{\tilde{\gamma}}^i D_2, \sigma_L^{-1}[1]\sigma_R^{-1}[2]\Gamma'^{-1}\Gamma).$$

Здесь  $\sigma_L, \sigma_R$  — автоморфизмы кода Рида–Маллера  $RM(r, m)$ , соответствующие матрицам  $D_1$  и  $D_2$ , а для перестановки  $\Gamma'$  выполняются два условия

- 1) Если  $R'$  —  $(k-1) \times n$ -матрица, получающаяся удалением строки с номером  $i$  из матрицы  $R$ , то  $(R' \| R')\Gamma' = (R' \| R')$ ;
- 2) Если  $\vec{r}_i$  — строка матрицы  $R$  с номером  $i$ , то

$$(\vec{r}_i \| \tilde{\alpha}R)\Gamma' = (\tilde{\beta}R \| \tilde{\gamma}R) \in RM(r, m) \times RM(r, m).$$



## Третий случай. $|| > 1$

### Теорема 2с

Пусть  $\Gamma_g^{-1}$  — перестановка из  $\mathcal{G}(E, T_A^I)$ , представимая в виде  $\Gamma' \sigma_L[1] \sigma_R[2]$ , где  $\Gamma'$  такая перестановка, что  $(R' \| R') \Gamma' = (R' \| R')$ . Тогда класс эквивалентности  $[(H, HT_{\tilde{A}}^I, \Gamma)]$ , содержит кортежи вида

$$(HT_{\tilde{B}}^I D_1, HT_{\tilde{C}}^I D_2, \sigma_L^{-1}[1] \sigma_R^{-1}[2] \Gamma'^{-1} \Gamma).$$

Здесь  $\sigma_L, \sigma_R$  — автоморфизмы кода Риды–Маллера  $RM(r, m)$ , соответствующие матрицам  $D_1$  и  $D_2$ ,  $\tilde{B} = \{\tilde{\beta}^{i_1}, \tilde{\beta}^{i_2}, \dots, \tilde{\beta}^{i_p}\}$ ,  $\tilde{C} = \{\tilde{\gamma}^{i_1}, \tilde{\gamma}^{i_2}, \dots, \tilde{\gamma}^{i_p}\}$ , а для перестановки  $\Gamma'$  выполняется условие

$$(\vec{r}_i \| \vec{\alpha}^i R) \Gamma' = (\tilde{\beta}^i R \| \tilde{\gamma}^i R) \in RM(r, m) \times RM(r, m) \text{ для любого } i \in I.$$



## Задача mcRMi

### Вход

Число  $m$  большее  $2r$  и  $1 \leq i \leq k$ , матрица  $G = H' \cdot R' \cdot \gamma'$ , где  $H'$  — невырожденная двоичная  $(k-1) \times (k-1)$ -матрица,  $R'$  —  $((k-1) \times n)$ -матрица, получающаяся из порождающей матрицы  $R$  кода Рида–Маллера  $RM(r, m)$  выкидыванием строки с номером  $i$  и  $\gamma'$  — перестановочная  $(n \times n)$ -матрица.

### Найти

Невырожденную матрицу  $M'$  размера  $(k-1) \times (k-1)$  и перестановочную  $(n \times n)$ -матрицу  $\sigma'$ , для которых найдётся невырожденная  $((k-1) \times (k-1))$ -матрица  $L'$ , что

$$M' \cdot G \cdot \sigma' = L' \cdot R'.$$





# Задача mcSRM

## Вход

Матрица  $G = (H_1 \cdot R \| H_2 \cdot R) \cdot \Delta$ , где  $H_1$  и  $H_2$  — невырожденные двоичные  $(k \times k)$ -матрицы, принадлежащие классу эквивалентности  $[(H, HT_{\alpha}^i, \Gamma)]$  и  $\Delta$  — перестановочная  $(2n \times 2n)$ -матрица.

## Найти

Невырожденные матрицы  $H'_1$  и  $H'_2$  размера  $(k \times k)$  и перестановочную  $(2n \times 2n)$ -матрицу  $\Delta'$  такие, что

$$G \cdot \Delta' = (H'_1 R \| H'_2 R).$$



## Теорема 3

Пусть существует алгоритм, который решает задачу  $\text{mcRMi}$  за полиномиальное время.  
Тогда существует алгоритм, который решает задачу  $\text{mcSRM}$  за полиномиальное время.



# Восстановление части ключа

## Определение

$\widehat{\mathcal{A}}_u(RM(r, m))$  — это множество перестановок вида  $\nabla\gamma$ , где  $\gamma$  — это перестановка из группы расширенных автоморфизмов  $\mathcal{A}_u(RM(r, m))$ , а  $\nabla$  — это произвольная перестановка блоков матрицы  $(H_1 R \parallel \dots \parallel H_u R)$ .

## Утверждение

Справедливо равенство

$$\bigcap_{H_1, \dots, H_u \in GL(k, 2)} \mathcal{G}(H_1, \dots, H_u) = \widehat{\mathcal{A}}_u(RM(r, m)),$$



# Восстановление части ключа

## Теорема 4

Пусть перестановка  $\Gamma = \Gamma_{I \leftrightarrow J} \gamma[1] \sigma[2]$  принадлежит множеству  $\mathcal{G}(E, H)$ . Тогда используя эту перестановку, можно построить  $p_{\bar{I}} + p_{\bar{J}}$  линейно независимых уравнений относительно  $n$  неизвестных  $HR_1, HR_2, \dots, HR_n$ . Здесь  $R_i$  столбец с номером  $i$  порождающей матрицы кода Рида–Маллера  $RM(r, m)$ .




## Основные результаты диссертации


- 1) Получена нижняя оценка мощности множества открытых ключей криптосистемы Мак-Элиса–Сидельникова — **Теорема 1**;
- 2) Описан ряд классов эквивалентности секретных ключей криптосистемы Мак-Элиса–Сидельникова — **Теорема 2a, Теорема 2b, Теорема 2c**;
- 3) Доказана полиномиальная эквивалентность задачи восстановления секретного ключа по открытому оригинальной криптосистемы Мак-Элиса и аналогичной задачи для криптосистемы Мак-Элиса–Сидельникова с ограничениями на ключевое пространство — **Теорема 3**;
- 4) Предложен метод восстановления части секретного ключа криптосистемы Мак-Элиса–Сидельникова, использующий знание структуры класса эквивалентности, в который попадает секретный ключ — **Теорема 4**.




## Список публикаций (3 из 7), в журналах ВАК — 2.

### Из списка ВАК

 *Чижов И. В.* — Ключевое пространство криптосистемы Мак-Элиса-Сидельникова. — // Дискретная математика. — 2009. — Т. 21, № 3. — С. 132—158. — ISSN 0234-0860.

 *Чижов И. В.* — Число открытых ключей криптосистемы Мак-Элиса-Сидельникова. — // Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика. — 2009. — № 3. — С. 40—45. — ISSN 0137-0782.

### Другие

 *Чижов И. В.* — Эквивалентные подпространства кодов Риды-Маллера и множество открытых ключей криптосистемы Мак-Элиса-Сидельникова. — // Материалы VI общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2008). — 2009. — С. 28—32.

