*Моделирование и анализ информационных систем*. Т. 25, №3 (2018), с. 276–290
*Modeling and Analysis of Information Systems*. Vol. 25, No 3 (2018), pp. 276–290

Криптосистемы


**DOI:** 10.18255/1818-1015-2018-3-276-290
УДК 517.9

# Об алгоритме расщепления носителя для индуцированных кодов

**Косолапов Ю. В., Шигаев А. Н.**

*получена 12 февраля 2018*

**Аннотация.** В 2000 г. Н. Сендриер показал, что если для линейного $[n, k, d]$-кода $C(\subseteq \mathbb{F}_q^n)$ длины $n$ и размерности $k$ с кодовым расстоянием $d$ группа автоморфизмов $\mathrm{PAut}(C)$ этого кода тривиальна, то может быть построен детерминированный алгоритм расщепления носителя, позволяющий для кода $D$, перестановочно-эквивалентного коду $C$, найти такую перестановку $\sigma$, что $\sigma(C) = D$. Этот алгоритм, в частности, может быть применен для осуществления атаки на ключ кодовой криптосистемы типа Мак-Элиса на коде $C$. Целью настоящей работы является построение и анализ алгоритма расщепления носителя для кода $\mathbb{F}_q^l \otimes C$, индуцированного кодом $C$, $l \in \mathbb{N}$. Так как группа автоморфизмов $\mathrm{PAut}(\mathbb{F}_q^l \otimes C)$ нетривиальна даже в случае, когда группа автоморфизмов базового кода $C$ тривиальна, то это позволяет предположить потенциально высокую стойкость криптосистемы типа Мак-Элиса на коде $\mathbb{F}_q^l \otimes C$ к атаке на основе расщепления носителя. В работе строится алгоритм расщепления носителя для кода $\mathbb{F}_q^l \otimes C$ и сравнивается эффективность этого алгоритма с имеющейся атакой на ключ криптосистемы типа Мак-Элиса на основе кода $\mathbb{F}_q^l \otimes C$.

**Ключевые слова:** групповые коды, индуцированные групповые коды, алгоритм расщепления носителя, криптосистема Мак-Элиса

**Для цитирования:** Косолапов Ю. В., Шигаев А. Н., "Об алгоритме расщепления носителя для индуцированных кодов", *Моделирование и анализ информационных систем*, **25**:3 (2018), 276–290.

**Об авторах:**
Косолапов Юрий Владимирович, orcid.org/0000-0002-1491-524X, канд. техн. наук,
Южный Федеральный Университет,
ул. Большая Садовая, 105/42, г. Ростов-на-Дону, 344006, Россия, e-mail: itaim@mail.ru,

Шигаев Алексей Николаевич, orcid.org/0000-0001-6363-4332, магистр,
Южный Федеральный Университет,
ул. Большая Садовая, 105/42, г. Ростов-на-Дону, 344006, Россия, e-mail: aleksejshig@gmail.com

## 1. Введение

В постквантовую эпоху кодовые криптосистемы типа Мак-Элиса [1] рассматриваются как возможные альтернативы тем асимметричным криптосистемам, стойкость которых в настоящее время основана на сложности факторизации больших целых чисел или на сложности дискретного логарифмирования в конечной группе [2]. Необходимым условием построения криптосистем типа Мак-Элиса на основе

линейных кодов является существование для этих кодов эффективных (полиномиальных) алгоритмов декодирования. Однако это условие не является достаточным. В частности, например, для кодов Рида–Соломона и кодов Рида–Маллера имеются быстрые алгоритмы декодирования [3], однако, как показано в [4] и [5], соответствующие криптосистемы типа Мак-Элиса на этих кодах не являются стойкими к атакам на ключ (к структурным атакам). Результаты исследования стойкости криптосистем типа Мак-Элиса показывают, что чем более код похож по структуре на случайный код, тем сложнее анализ соответствующей криптосистемы типа Мак-Элиса. Одним из возможных способов построения стойкой криптосистемы типа Мак-Элиса является поиск или построение кода, для которого, с одной стороны, имеется эффективный декодер, а с другой стороны, который похож на случайный.

В [6] показано, что если для базового кода $C$ существует эффективный мажоритарный декодер, то для индуцированного кода $\mathbb{F}_q^l \otimes C$, $l \in \mathbb{N}$, также может быть построен эффективный мажоритарный декодер. В связи с этим в [7] предложена криптосистема типа Мак-Элиса на основе индуцированного кода $\mathbb{F}_q^l \otimes C$. При этом установлено, что если криптосистема типа Мак-Элиса на основе базового кода $C$ является нестойкой к атакам на ключ, то атакующий хотя и может построить атаку на ключ для соответствующей криптосистемы на основе индуцированного кода $\mathbb{F}_q^l \otimes C$, однако эта атака не будет эффективной при тщательном подборе параметров индуцированного кода.

Целью настоящей работы является построение алгоритма расщепления носителя для индуцированных кодов и оценка эффективности его применения при нахождении секретного ключа кодовой криптосистемы типа Мак-Элиса на основе индуцированного кода $\mathbb{F}_q^l \otimes C$. Работа имеет следующую структуру. Второй раздел содержит необходимые сведения о кодах, об алгоритме расщепления носителя и предварительные результаты об индуцированных кодах. Также здесь строится алгоритм расщепления носителя для индуцированных кодов. В третьем разделе рассматривается применение этого алгоритма для нахождения секретной перестановки криптосистемы типа Мак-Элиса на индуцированном коде, сравнивается эффективность построенного алгоритма с эффективностью алгоритма из работы [7]. Дополнительно рассматривается возможное применение индуцированных кодов в алгоритме идентификации.

# 2. Алгоритм расщепления носителя для индуцированных кодов

## 2.1. Предварительные сведения

Пусть $\mathbb{F}_q$ — поле Галуа мощности $q$, где $q$ — степень простого числа. Для вектора $\mathbf{x}$ из пространства $\mathbb{F}_q^n$ размерности $n$ определим вес $\mathrm{wt}(\mathbf{x})$ как мощность множества ненулевых координат вектора $\mathbf{x}$. В пространстве $\mathbb{F}_q^n$ рассмотрим $[n, k, d]$-код $C$ размерности $k$, длины $n$ с кодовым расстоянием $d$. Пусть $G(C)$ – порождающая матрица кода, $C \subseteq \mathbb{F}_q^n$. Коды $C$ и $D$ размерности $k$ и длины $n$ называются перестановочно-эквивалентными, если существует такая перестановка $\sigma$ из группы симметрической

группы $S_n$, действующей на элементах множества $I_n = \{1, ..., n\}$, что

$$D = \{(c_1, ..., c_n) | (c_{\sigma^{-1}(1)}, ..., c_{\sigma^{-1}(n)}) \in C\}.$$

В этом случае будет использоваться принятое обозначение $D = \sigma(C)$. Далее нам понадобятся определения инварианта и сигнатуры из [8]. Для некоторого подмножества $J(\subseteq I_n)$ символом $C_J$ обозначим множество векторов, полученных из векторов кода $C$ путем зануления координат с номерами из $J$. Пусть $\mathcal{L}_n$ – множество всех кодов длины $n$, $\mathcal{L} = \bigcup_{n>0} \mathcal{L}_n$. Отображение $\mathcal{V} : \mathcal{L} \to E$ называется *инвариантом* над множеством $E$, если для любых двух перестановочно-эквивалентных кодов $C$ и $D$ выполняется равенство: $\mathcal{V}(C) = \mathcal{V}(D)$. *Сигнатурой* над множеством $F$ называется отображение $\mathcal{S} : \mathcal{L}_n \times I_n \to F$, такое, что для любой перестановки $\sigma(\in S_n)$ и любого кода $C \in \mathcal{L}_n$ выполняется равенство: $\mathcal{S}(C, i) = \mathcal{S}(\sigma(C), \sigma(i))$. Далее мы будем рассматривать только сигнатуры, которые построены на основе инварианта по следующему правилу:

$$\mathcal{S}(C, i) = \mathcal{V}(C_i), \tag{1}$$

где $C_i = C_{\{i\}}$. Дискриминантом кода $C$ называется такая сигнатура $S$, для которой существуют такие $i$ и $j$ из $I_n$, что $\mathcal{S}(C, i) \neq \mathcal{S}(C, j)$. Тогда *полным дискриминантом* для кода $C$ называется такая сигнатура $\mathcal{S}$, что $\mathcal{S}(C, i) \neq \mathcal{S}(C, j)$ для всех разных $i$ и $j$ из $I_n$. Приведем в виде леммы известный факт.

**Лемма 1.** *Пусть $C$ — $[n, k, d]$-код, $\sigma \in S_n$, $D = \sigma(C)$. Равенство $D = \gamma(C)$ выполняется тогда и только тогда, когда $\gamma \in \sigma\mathrm{PAut}(C)$, где $\sigma\mathrm{PAut}(C)$ — фактор-класс из фактор-множества $S_n/\mathrm{PAut}(C)$.*

*Доказательство.* Очевидно, что если $\gamma \in \sigma\mathrm{PAut}(C)$, то $D = \gamma(C)$. Докажем в обратную сторону. Предположим, что выполняется равенство $D = \gamma(C)$, но $\gamma \notin \sigma\mathrm{PAut}(C)$. Так как $\gamma(C) = \sigma(C)$, то $\gamma^{-1}\sigma \in \mathrm{PAut}(C)$. Отсюда получаем, что имеет место представление $\gamma^{-1} = \phi\sigma^{-1}$, $\phi \in \mathrm{PAut}(C)$. Следовательно, $\gamma \in \sigma\mathrm{PAut}(C)$. □

Рассмотрим алгоритм SSA, который с помощью дискриминанта $\mathcal{S}$ находит такую перестановку $\sigma'$ для двух перестановочно-эквивалентных кодов $C$ и $D = \sigma(C)$, что $D = \sigma'(C)$. Заметим, что в общем случае $\sigma \neq \sigma'$, однако, в силу леммы 1, ${\sigma'}^{-1}\sigma \in \mathrm{PAut}(C)$. Перестановку $\sigma'$, возвращаемую алгоритмом SSA, будем называть подходящей. Если $\mathcal{S}$ — полный дискриминант, то $\sigma = \sigma'$, при этом перестановка $\sigma$ будет найдена на первой итерации цикла этого алгоритма. Как следует из утверждения 8 работы [8], для кода $C$ полный дискриминант существует тогда и только тогда, когда группа автоморфизмов $\mathrm{PAut}(C)$ кода $C$ тривиальна. Отметим, что коды с тривиальной группой автоморфизмов существуют (см., например, [9]).

В [8] отмечено, что даже если существует полный дискриминант кода $C$, его вычисление может оказаться вычислительно сложным, поэтому в [8] предложена техника, которая может позволить построить вычислительно простые полные дискриминанты на основе неполных дискриминантов. Так как, в соответствии с (1), рассматриваются только сигнатуры, основанные на инвариантах, то необходимо, чтобы инварианты были также вычислительно простыми.

**Исходные параметры**: $C \in \mathcal{L}_n$ , $D = \sigma(C)$, $\mathcal{S}$
**Результат**: $\sigma' : D = \sigma'(C)$
1. Вычислить $\mathcal{D} = (\mathcal{S}(D, i))_{i=1}^n$
2. Вычислить $\mathcal{C} = (\mathcal{S}(, i))_{i=1}^n$
3. $\Sigma = \varnothing$, exit $= false$;
**до тех пор, пока** exit! $= true$ **выполнять**
  Выбрать $\sigma'$ из $S_n \setminus \Sigma$
  **если** $\sigma'(C) \neq D$ **тогда**
    $\Sigma = \Sigma \cup \{\sigma'\}$
  **конец условия**
  **иначе**
    exit $= true$
  **конец условия**
**конец цикла**
**возвратить** $\Omega$

**Алгоритм 1:** SSA

Примером просто вычислимого инварианта для кодов малой размерности является отображение $\mathcal{V}^W : \mathcal{L} \to \mathbb{Z}[X]$, ставящее в соответствие коду $C$ его нумератор весов $\mathcal{W}(C) = \sum_{i=0}^n W_i X^i$, где $W_i$ — число векторов веса $i$ в коде $C$, $\mathbb{Z}[X]$ — множество полиномов от одной переменной с коэффициентами из $\mathbb{Z}$. На основе этого инварианта может быть построена сигнатура $\mathcal{S}^W : \mathcal{L}_n \times I_n \to \mathbb{Z}[X]$, определенная по правилу: $\mathcal{S}^W(C, i) = \mathcal{V}^W(C_i) = \mathcal{W}(C_i)$. Заметим, что сложность вычисления инварианта $\mathcal{V}^W(C_i)$ растет неполиномиально с ростом размерности кода $C_i$. Поэтому в [8] дискриминант строится на основе вычисления нумератора весов остова кода. Под остовом (hull) кода $C$ в [8] понимается пересечение кода $C$ с его дуальным кодом $C^\perp$:

$$\mathcal{H}(C) = C \cap C^\perp. \tag{2}$$

Выбор этой характеристики кода обоснован тем, что размерность остова в среднем существенно меньше размерности кода $C$, что позволяет эффективно вычислять нумераторы и строить простые для вычисления дискриминанты даже в случае большой размерности кода $C$.

## 2.2. Индуцированные коды и их свойства

Пусть $C^i$ — $[n_i, k_i, d_i]$-код с порождающей матрицей $G(C^i)$ и проверочной матрицей $H(C^i)$, $i = 1, 2$. Под декартовым произведением $C^1 \times C^2$ кодов $C^1$ и $C^2$ будем понимать множество вида

$$C^1 \times C^2 = \{(\mathbf{a} \parallel \mathbf{b}) : \mathbf{a} \in C^1, \mathbf{b} \in C^2\},$$

где $\mathbf{a} \parallel \mathbf{b}$ – конкатенация векторов $\mathbf{a}$ и $\mathbf{b}$. Легко проверить, что порождающая и проверочная матрицы кода $C^1 \times C^2$ могут быть представлены в виде

$$G(C^1 \times C^2) = \begin{pmatrix} G(C^1) & O_{k_1 \times n_2} \\ O_{k_2 \times n_1} & G(C^2) \end{pmatrix}, \quad H(C^1 \times C^2) = \begin{pmatrix} H(C^1) & O_{n_1 - k_1 \times n_2} \\ O_{n_2 - k_2 \times n_1} & H(C^2) \end{pmatrix},$$

где $O_{a\times b}$ — нулевая $(a \times b)$-матрица. Из определения (2) следует, что

$$\mathcal{H}(C^1 \times C^2) = \mathcal{H}(C^1) \times \mathcal{H}(C^2). \tag{3}$$

**Лемма 2.** *Пусть* $C^i$ – $[n_i, k_i]$*-код,* $\mathcal{W}(C^i) = \sum_{j=0}^{n_i} W_j^{(i)} X^{(i)}$ – *нумератор кода* $C^i$, $i = 1, 2$. *Тогда нумератор кода* $C^1 \times C^2$ *имеет вид*

$$\mathcal{W}(C^1 \times C^2) = \mathcal{W}(C^1) \cdot \mathcal{W}(C^2).$$

*Доказательство.* Каждый кодовый вектор $\mathbf{c}$ из $C^1 \times C^2$ представим в виде конкатенации $(\mathbf{a} \parallel \mathbf{b})$ двух векторов $\mathbf{a}$ и $\mathbf{b}$ из $C^1$ и $C^2$ соответственно. Найдем количество векторов веса $j$ $(0 \le j \le n_1+n_2)$ в коде $C^1 \times C^2$. Для этого рассмотрим всевозможные упорядоченные пары $(j_1, j_2)$ неотрицательных целых чисел таких, что $j_1 + j_2 = j$. Для каждой такой пары $(j_1, j_2)$ в коде $C^1 \times C^2$ имеется множество из $W_{j_1}^{(1)} \cdot W_{j_2}^{(2)}$ векторов веса $j$. Для различных пар эти множества не пересекаются. Поэтому в коде $C^1 \times C^2$ будет всего

$$\sum_{(j_1,j_2):j_1+j_2=j} W_{j_1}^{(1)} \cdot W_{j_2}^{(2)}$$

векторов веса $j$. Отсюда следует

$$\mathcal{W}(C^1 \times C^2) = \sum_{j=0}^{n_1+n_2} \left( \sum_{(j_1,j_2):j_1+j_2=j} W_{j_1}^{(1)} \cdot W_{j_2}^{(2)} \right) X^j = \mathcal{W}(C^1) \cdot \mathcal{W}(C^2).$$

□

Под тензорным произведением $A \otimes B$ матриц $A = (a_{i,j})_{i=1,m;j=1,l}$ и $B$ будем понимать матрицу вида

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \dots & a_{1,l}B \\ \dots & \dots & \dots \\ a_{m,1}B & \dots & a_{m,l}B \end{pmatrix}.$$

Пусть $C$ – $[n, k, d]$-код с порождающей матрицей $G(C)$, $E_l$ – единичная матрица порядка $l$. Подпространство, порожденное строками матрицы $E_l \otimes G(C)$, обозначим $\mathbb{F}_q^l \otimes C$ и, в соответствии с [7], будем называть индуцированным кодом (кодом, который индуцирован кодом $C$). Порождающая матрица этого кода $G(\mathbb{F}_q^l \otimes C) = E_l \otimes G(C)$ имеет блочный вид

$$G(\mathbb{F}_q^l \otimes C) = \underbrace{\begin{pmatrix} G(C) & O_{k\times n} & \dots & O_{k\times n} \\ O_{k\times n} & G(C) & \dots & O_{k\times n} \\ \dots & \dots & \dots & \dots \\ O_{k\times n} & O_{k\times n} & \dots & G(C) \end{pmatrix}}_{l \text{ блоков}}, \tag{4}$$

где в каждой блочной строке $l-1$ нулевых матриц $O_{k\times n}$ и одна матрица $G(C)$. Так как

$$\mathbb{F}_q^l \otimes C = \underbrace{C \times \ldots \times C}_{l \text{ раз}},$$

то из леммы 2 вытекает

**Следствие 1.** *Пусть $C$ – $[n,k]$-код с порождающей матрицей $G(C)$ и $\mathcal{W}(C)$ – нумератор кода $C$. Тогда*

*1)* $\mathcal{W}(\mathbb{F}_q^l \otimes C) = \underbrace{\mathcal{W}(C) \cdot \ldots \cdot \mathcal{W}(C)}_{l \text{ раз}}$;

*2)* $\forall i \in \{1,\ldots,ln\} \exists j \in \{1,\ldots,n\}$: $\mathcal{W}((\mathbb{F}_q^l \otimes C)_i) = \mathcal{W}(C_j) \cdot \underbrace{\mathcal{W}(C) \cdot \ldots \cdot \mathcal{W}(C)}_{l-1 \text{ раз}}$.

Также получаем, что проверочная матрица кода $\mathbb{F}_q^l \otimes C$ имеет вид $H(\mathbb{F}_q^l \otimes C) = E_l \otimes H(C)$, где $H(C)$ – проверочная матрица кода $C$, а из (3) следует, что остов кода $\mathbb{F}_q^l \otimes C$ имеет вид

$$\mathcal{H}(\mathbb{F}_q^l \otimes C) = \mathbb{F}_q^l \otimes \mathcal{H}(C). \tag{5}$$

Рассмотрим индуцированный код $\mathbb{F}_q^l \otimes C$, $l \in \mathbb{N}$. Группа автоморфизмов $\mathrm{PAut}(\mathbb{F}_q^l \otimes C)$ этого кода нетривиальна. Действительно, порождающая матрица кода $\mathbb{F}_q^l \otimes C$ имеет блочно-диагональный вид (4) и при любой перестановке блоков этой матрицы получается порождающая матрица того же кода. Перестановка блочных столбцов этой матрицы эквивалентна перестановке блочных строк. Всего имеется $l!$ таких перестановок блочных столбцов. Поэтому мощность группы автоморфизмов кода $\mathbb{F}_q^l \otimes C$ не менее $l!$. Отсюда справедлива следующая

**Лемма 3.** *Группа автоморфизмов* $\mathrm{PAut}(\mathbb{F}_q^l \otimes C)$ *кода* $\mathbb{F}_q^l \otimes C$ *содержит подгруппу* $\mathcal{G}(\mathbb{F}_q^l \otimes C)$, *изоморфную группе* $S_l$.

Отметим, что каждый элемент группы $\mathcal{G}(\mathbb{F}_q^l \otimes C)$ имеет вид

$$\begin{pmatrix} 1 & \ldots & n & \ldots & (l-1)n+1 & \ldots & ln \\ (\sigma(1)-1)n+1 & \ldots & \sigma(1)n & \ldots & (\sigma(l)-1)n+1 & \ldots & \sigma(l)n \end{pmatrix}, \quad \sigma \in S_l. \tag{6}$$

Пусть $I_{i,n} = \{i, i+n, \ldots, i+(l-1)\cdot n\}$, где $i \in \{1,\ldots,n\}$, $S(I_{i,n})$ — подгруппа группы $S_{ln}$, перестановки из которой переставляют только элементы множества $I_{i,n}$, а элементы из множества $\{1,\ldots,ln\} \setminus I_{i,n}$ оставляют на месте. Рассмотрим группу $Q = S(I_{1,n}) \times S(I_{2,n}) \times \cdots \times S(I_{n,n}) \subset S_{ln}$, $|Q| = (l!)^n$. Несложно проверить, что

$$\mathcal{G}(\mathbb{F}_q^l \otimes C) \subseteq \mathrm{PAut}(\mathbb{F}_q^l \otimes C) \cap Q. \tag{7}$$

Напомним, что орбитой элемента $i \in \{1,\ldots,ln\}$ под действием подгруппы $\mathcal{G} \subseteq S_{ln}$ называется множество $\{g(i) : g \in \mathcal{G}\}$. Тогда $I_{i,n}$, $i = 1,\ldots,n$, — это орбиты, образующиеся под действием подгруппы $\mathcal{G}(\mathbb{F}_q^l \otimes C)$ на элементах множества $\{1,\ldots,ln\}$. Из (7) вытекает следующая вспомогательная

**Лемма 4.** *Длина каждой орбиты, образующейся под действием группы* $\mathrm{PAut}(\mathbb{F}_q^l \otimes C)$ *на элементы множества* $\{1,\ldots,ln\}$, *кратна* $l$.

## 2.3. Алгоритм расщепления носителя

Выше было отмечено, что для двух перестановочно-эквивалентных кодов с полным дискриминантом $\mathcal{S}$ для нахождения подходящей перестановки потребуется не более одной итерации внутреннего цикла алгоритма SSA. Из леммы 3 следует, что для кода $\mathbb{F}_q^l \otimes C$ не существует полного дискриминанта, так как группа автоморфизмов этого кода нетривиальна. Рассмотрим задачу построения для кодов $\mathbb{F}_q^l \otimes C$ и $D = \sigma(\mathbb{F}_q^l \otimes C)$ алгоритма нахождения такой подходящей перестановки $\sigma'$, что $\sigma'(\mathbb{F}_q^l \otimes C) = D$.

**Лемма 5.** *Пусть $C$ – $[n,k,d]$-код. Тогда для $i = 1,...,n$ и любой сигнатуры $\mathcal{S}$, определенной по правилу (1), имеет место равенство*

$$\mathcal{S}(\mathbb{F}_q^2 \otimes C, i) = \mathcal{S}(\mathbb{F}_q^2 \otimes C, i+n). \tag{8}$$

*Доказательство.* По определению (1), $\mathcal{S}(\mathbb{F}_q^2 \otimes C, i) = \mathcal{V}((\mathbb{F}_q^2 \otimes C)_i)$. Пусть $\mathcal{V}((\mathbb{F}_q^2 \otimes C)_i) \neq \mathcal{V}((\mathbb{F}_q^2 \otimes C)_{i+n})$ Для любой перестановки $\pi$ из определения инварианта получаем: $\mathcal{V}((\mathbb{F}_q^2 \otimes C)_i) = \mathcal{V}(\pi((\mathbb{F}_q^2 \otimes C)_i))$. Рассмотрим произвольную нетривиальную перестановку $\pi \in \mathcal{G}(\mathbb{F}_q^2 \otimes C)$. Получаем

$$\mathcal{V}((\mathbb{F}_q^2 \otimes C)_i) = \mathcal{V}(\pi(\,(\mathbb{F}_q^2 \otimes C)_i\,)\,) = \mathcal{V}(\pi(\mathbb{F}_q^2 \otimes C)_{\pi(i)}) = \mathcal{V}((\mathbb{F}_q^2 \otimes C)_{\pi(i)}).$$

Так как $\pi$ — нетривиальная перестановка, то из вида (6) элементов группы $\mathcal{G}(\mathbb{F}_q^2 \otimes C)$ для $l = 2$ получим: $\pi(i) = i + n$. Пришли к противоречию. □

Учитывая представление (6), из леммы 5 вытекает

**Следствие 2.** *Для кода $\mathbb{F}_q^l \otimes C$ и $i \in \{1,...,n\}$ имеем: $\mathcal{S}(\mathbb{F}_q^l \otimes C, i) = \mathcal{S}(\mathbb{F}_q^l \otimes C, i + n \cdot k)$, для всех $k = \{0,\ldots,l-1\}$.*

Таким образом, любая сигнатура для кода $\mathbb{F}_q^l \otimes C$, определенная по правилу (1), имеет не более $n$ различных значений. Заметим, что чем больше значений имеет сигнатура для кода, тем меньше в среднем потребуется циклов алгоритма SSA для нахождения подходящей перестановки.

**Лемма 6.** *Если $\mathcal{G}(\mathbb{F}_q^l \otimes C) \subset \mathrm{PAut}(\mathbb{F}_q^l \otimes C)$, то любая сигнатура для кода $C$, определенная по правилу (1), имеет менее $n$ значений.*

*Доказательство.* Из следствия 2 получаем, что любая сигнатура для кода $\mathbb{F}_q^l \otimes C$, определенная по правилу (1), имеет не более $n$ различных значений. Отсюда и из утверждения 8 работы [8] следует, что под действием группы $\mathrm{PAut}(\mathbb{F}_q^l \otimes C)$ на множестве $\{1,...,ln\}$ образуется не более $n$ различных орбит. Пусть $\sigma \in \mathrm{PAut}(\mathbb{F}_q^l \otimes C) \setminus \mathcal{G}(\mathbb{F}_q^2 \otimes C)$, тогда существует такой элемент $i \in \{1,...,n\}$, что $\sigma(i) \neq i + n \cdot k$ для некоторого $k \in \{0,\ldots,l-1\}$. Поэтому из леммы 4 получаем, что, как минимум, одна из орбит имеет длину не мнее $2l$. Следовательно, под действием группы $\mathrm{PAut}(\mathbb{F}_q^l \otimes C)$ образуется не более $n-1$ орбит. Из утверждения 8 работы [8] получаем, что сигнатура имеет не более $n-1$ различных значений. □

**Следствие 3.** *Пусть сигнатура $\mathcal{S}$ определена в соответствии с правилом (1). Если $\mathcal{S}$ для кода $\mathbb{F}_q^l \otimes C$ имеет $n$ различных значений, то $\mathrm{PAut}(\mathbb{F}_q^l \otimes C) = \mathcal{G}(\mathbb{F}_q^l \otimes C)$.*

**Пример 1.** *Рассмотрим код $C^1 \times C^2$ и найдем нумератор весов кода $(C^1 \times C^2)_i$, когда $i \in \{1,...,n_1+n_2\}$. Если $i \leq n_1$, то $\mathcal{W}((C^1 \times C^2)_i) = \mathcal{W}(C_i^1) \cdot \mathcal{W}(C^2)$; если $n_1 < i \leq n_1 + n_2$, то $\mathcal{W}((C^1 \times C^2)_i) = \mathcal{W}(C^1) \cdot \mathcal{W}(C^2_{i-n_1})$. Тогда*

$$\mathcal{S}^W(C^1 \times C^2, i) = \mathcal{W}((C^1 \times C^2)_i) = \mathcal{W}(C^a_{i-(a-1)\cdot n_1}) \cdot \mathcal{W}(C^b), \tag{9}$$

*где*

$$a = \begin{cases} 1, & \text{при } 1 \leq i \leq n_1 \\ 2, & \text{при } n_1 + 1 \leq i \leq n_1 + n_2 \end{cases},$$

$b = \{1,2\} \setminus \{a\}$. *В случае* $C^1 = C^2 = C$ *получаем:* $C^1 \times C^2 = \mathbb{F}_q^2 \otimes C$, *поэтому*

$$\mathcal{S}^W(\mathbb{F}_q^2 \otimes C, i) = \mathcal{W}(C) \cdot \mathcal{W}(C_j), \tag{10}$$

*где*

$$j = \begin{cases} i, & \text{при } 1 \le i \le n \\ i-n, & \text{при } n < i \le 2n. \end{cases}$$

*Если* $C$ — *такой* $[n,k]$*-код, что* $\mathcal{S}^W$ — *его полный дискриминант, то, как непосредственно вытекает из следствия 1 и из обобщения формулы* (10) *на случай* $l \ge 2$, *сигнатура* $\mathcal{S}^W$ *для кода* $\mathbb{F}_q^l \otimes C$ *имеет* $n$ *различных значений. Из следствия 3 тогда вытекает, что в этом случае группа автоморфизмов кода* $\mathbb{F}_q^l \otimes C$ *имеет простое описание.*

**Лемма 7.** *Пусть* $\mathcal{S}$ — *сигнатура, определенная по правилу* (1). *Тогда для любого* $\pi \in Q$ *выполняются равенства:*
*1)* $\mathcal{S}(\mathbb{F}_q^l \otimes C, i) = \mathcal{S}(\mathbb{F}_q^l \otimes C, \pi(i))$, $i = 1, ..., ln$;
*2)* $(\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln} = (\mathcal{S}(\mathbb{F}_q^l \otimes C, \pi(i)))_{i=1}^{ln}$;
*3)* $(\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln} = \pi((\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln})$.

*Доказательство.* Доказательство равенства 1) вытекает из следствия 2; равенство 2) следует из 1). Докажем утверждение 3). Из 2) следует

$$\begin{aligned}(\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln} &= (\mathcal{S}(\mathbb{F}_q^l \otimes C, \pi(i)))_{i=1}^{ln} \\ &= (\mathcal{S}(\mathbb{F}_q^l \otimes C, j))_{\pi^{-1}(j)=1}^{ln} = \pi((\mathcal{S}(\mathbb{F}_q^l \otimes C, j))_{j=1}^{ln}).\end{aligned}$$

Так как $\pi$ — произвольная перестановка из группы $Q$, то утверждение доказано. □

Символом $\sigma Q$ обозначим фактор-класс $\{\sigma\pi : \pi \in Q\}$ фактор-множества $S_{nl}/Q$.

**Лемма 8.** *Если сигнатура* $\mathcal{S}$ *для кода* $\mathbb{F}_q^l \otimes C$ *определена по правилу* (1) *и имеет* $n$ *различных значений,* $D = \sigma(\mathbb{F}_q^l \otimes C)$ *и*

$$(\mathcal{S}(D, i))_{i=1}^{ln} = \gamma((\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln}), \tag{11}$$

*то* $\sigma \in \gamma Q$.

*Доказательство.* Из утверждения 3) леммы 7 и условия (11) получаем, что для любого $\pi \in Q$ выполняются равенства

$$(\mathcal{S}(D, i))_{i=1}^{ln} = \gamma((\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln}) = \gamma\pi((\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln}).$$

Так как, по условию, сигнатура имеет максимальное количество различных значений – $n$, то $\sigma \in \gamma Q$ по построению группы $Q$ ($Q$ — максимальная в этом случае подгруппа, не меняющая порядка элементов в наборе $(\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln}$). □

Пусть $Q/\mathcal{G}(\mathbb{F}_q^l \otimes C) = \{G_i\}_{i=0}^{x}$ — фактор-множество группы $Q$ по подгруппе $\mathcal{G}(\mathbb{F}_q^l \otimes C)$, $x+1 = |Q|/|\mathcal{G}(\mathbb{F}_q^l \otimes C)| = (l!)^n/l! = (l!)^{n-1}$. Пусть также $\Omega = \{\omega_0, \ldots, \omega_x\}$ — трансверсаль фактор-множества $Q/\mathcal{G}(\mathbb{F}_q^l \otimes C)$, или множество представителей классов смежности, $G_i = \omega_i \mathcal{G}(\mathbb{F}_q^l \otimes C)$, $i = 0, ..., x$. Одним из возможных алгоритмов построения множества $Q$ является алгоритм MakeRepresentatives.

**Исходные параметры**: $Q$, $\mathcal{G}(\mathbb{F}_q^l \otimes C)$
**Результат**: $\Omega$ — множество представителей классов фактор-множества $Q/\mathcal{G}(\mathbb{F}_q^l \otimes C)$
1. $\Omega = \varnothing$
2. **до тех пор, пока** $|\Omega| < (l!)^{n-1}$ **выполнять**
   Случайно сгенерировать перестановку $\pi' \in Q$
   **если** $\pi' \notin \mathcal{G}(\mathbb{F}_q^l \otimes C)$ *и* $\pi'^{-1}\sigma \notin \mathcal{G}(\mathbb{F}_q^l \otimes C)$ $\forall \sigma \in \Omega$ **тогда**
      $\Omega = \Omega \cup \{\pi'\}$
   **конец условия**
**конец цикла**
**возвратить** $\Omega$

**Алгоритм 2:** MakeRepresentatives

**Теорема 1.** *Пусть $C$ — $[n,k]$-код, $D = \sigma(\mathbb{F}_q^l \otimes C)$, $\mathcal{S}$ — сигнатура, определенная по правилу (1) и имеющая $n$ различных значений для кода $\mathbb{F}_q^l \otimes C$, $\Omega$ — трансверсаль фактор-множества $Q/\mathcal{G}(\mathbb{F}_q^l \otimes C)$. Тогда существует алгоритм с вычислительной сложностью $\mathcal{O}(|\Omega|)$, который находит подходящую перестановку $\sigma'$ такую, что $D = \sigma'(\mathbb{F}_q^l \otimes C)$.*

*Доказательство.* Пусть $(\mathcal{S}(D,i))_{i=1}^{ln} = \gamma((\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln})$. Такая перестановка $\gamma$ может быть найдена простым вычислением сигнатур кодов $D$ и $C$. Тогда из леммы 8 получаем, что $\sigma \in \gamma Q$. Из леммы 1 видим, что подходящей перестановкой, переводящей код $\mathbb{F}_q^l \otimes C$ в код $D$, является перестановка вида $\sigma\pi$, где $\pi \in \mathrm{PAut}(\mathbb{F}_q^l \otimes C)$. Так как сигнатура имеет $n$ различных значений, то из следствия 3 получаем, что $\mathrm{PAut}(\mathbb{F}_q^l \otimes C) = \mathcal{G}(\mathbb{F}_q^l \otimes C)$. Отсюда получаем, что подходящая перестановка может быть найдена путем перебора элементов трансверсали $\Omega$. Таким образом, для нахождения подходящей перестановки достаточно выполнить алгоритм SSAForTensor, сложность которого $\mathcal{O}(|\Omega|)$, так как в этом алгоритме осуществляется перебор по трансверсали $\Omega$. □

**Исходные параметры**: $\mathbb{F}_q^l \otimes C \in \mathcal{L}_{ln}$, $D = \sigma(\mathbb{F}_q^l \otimes C)$, $\mathcal{S}$, $\Omega$
**Результат**: $\sigma' : \sigma'(\mathbb{F}_q^l \otimes C) = D$
1. Вычислить $\mathcal{D} = (\mathcal{S}(D,i))_{i=1}^{ln}$.
2. Вычислить $\mathcal{C} = (\mathcal{S}(\mathbb{F}_q^l \otimes C, i))_{i=1}^{ln}$.
3. Найти подходящую перестановку $\gamma$ такую, что $\gamma(\mathcal{C}) = \mathcal{D}$.
4. **для каждого** $\omega \in \Omega$ **выполнять**
   **если** $(\gamma\omega)^{-1}(D) = \mathbb{F}_q^l \otimes C$ **тогда**
      $\sigma' = \gamma\omega$
      выход
   **конец условия**
**конец цикла**
**возвратить** $\sigma'$

**Алгоритм 3:** SSAForTensor

Отметим, что в теореме 1 при оценке сложности алгоритма SSAForTensor учитывается только мощность трансверсали, но не учитывается сложность вычисления

сигнатур (шаги 1 и 2), сложность проверки совпадения двух кодов (шаг 4), а также сложность построения трансверсали $\Omega$, используемой в качестве входного параметра. Совпадение двух кодов можно проверить, умножив порождающую матрицу кода $(\gamma\omega)^{-1}(D)$ на проверочную матрицу $H(\mathbb{F}_q^l \otimes C)$ кода $\mathbb{F}_q^l \otimes C$. Таким образом, сложность этой проверки полиномиально зависит от $ln$, т.е. эта проверка может быть выполнена эффективным способом. В то же время построение эффективно вычислимых сигнатур является отдельной задачей [8]. В частности, в [8] для построения эффективных сигнатур применяется нумератор остова кода, который с большой вероятностью имеет малую размерность. Из (5) следует, что размерность остова для индуцированного кода увеличивается в $l$ раз по сравнению с остовом базового кода. Это в свою очередь может существенно замедлить подсчет нумераторов его проекций в общем случае и усложнит вычисление сигнатур, так как для вычисления нужно перебрать все векторы проекции остова для всех координат. Построение трансверсали $\Omega$ также представляется сложной задачей при достаточно больших значениях $ln$. Например, предложенный алгоритм MakeRepresentatives имеет неполиномиальную от $ln$ сложность, хотя и может выполняться заранее.

Тем не менее, если для кода $\mathbb{F}_q^l \otimes C$ имеется эффективно вычисляемая сигнатура, определенная по правилу (1) и имеющая $n$ различных значений, а также имеется трансверсаль $\Omega$, то при нахождении подходящей перестановки алгоритм SSAForTensor будет эффективнее алгоритма SSA. Это обусловлено тем, что алгоритм SSA выполняет поиск подходящей перестановки по всему классу смежности $\sigma Q$, а алгоритм SSAForTensor выполняет поиск только по множеству $\sigma\Omega$, мощность которого в $l!$ меньше $|\sigma Q|$, так как $|Q|/|\Omega| = |\mathcal{G}(\mathbb{F}_q^l \otimes C)| = l!$.

# 3. Применение индуцированных кодов в криптографии

## 3.1. Криптосистема типа Мак-Элиса на основе индуцированных кодов

Рассмотрим криптосистему типа Мак-Элиса на основе $[ln, lk, d]$-кода $\mathbb{F}_q^l \otimes C$, где $C$ — $[n, k, d]$-код с порождающей матрицей $G(C)$. В этой криптосистеме открытый ключ $\mathbf{k}_{\text{pub}}$ — это пара $(\widetilde{G}, t = \lfloor (d-1)/2 \rfloor)$, а секретный ключ $\mathbf{k}_{\text{sec}}$ — пара матриц $(S, P)$, где $S$ – случайная невырожденная $(lk \times lk)$-матрица, $P$ – случайная перестановочная $(ln \times ln)$-матрица, причем $\widetilde{G} = S \cdot (E_l \otimes G(C)) \cdot P$, где $E_l$ — единичная матрица размера $l \times l$. Правило шифрования произвольного сообщения $\mathbf{s}(\in \mathbb{F}_q^{lk})$ имеет вид

$$\mathbf{z} = \mathbf{s}\widetilde{G} + \mathbf{e}, \tag{12}$$

где $\mathbf{e} \in \mathbb{F}_q^{ln}$ и $\text{wt}(\mathbf{e}) \leq t$.

При расшифровании используется правило $\mathbf{s} = \text{Dec}_C(\mathbf{z}P^{-1})S^{-1}$, где $\text{Dec}_{\mathbb{F}_q^l \otimes C} : \mathbb{F}_q^{ln} \to \mathbb{F}_q^{lk}$ — декодер кода $\mathbb{F}_q^l \otimes C$, гарантированно исправляющий $t$ и менее ошибок и восстанавливающий вектор $\mathbf{s}$. Криптосистему Мак-Элиса на коде $\mathbb{F}_q^l \otimes C$ обозначим $\text{McE}(\mathbb{F}_q^l \otimes C)$.

Так как код с порождающей матрицей $\widetilde{G}$ и код $\mathbb{F}_q^l \otimes C$ являются перестановочно-эквивалентными, то, как следует, например, из [4], для взлома $\mathrm{McE}(\mathbb{F}_q^l \otimes C)$, достаточно найти такую пару матриц $(S', P')$, что $S'(E_l \otimes G(C))P' = \widetilde{G}$ и перестановка, соответствующая перестановочной матрице $P'^{-1}P$, принадлежит $\mathrm{PAut}(\mathbb{F}_q^l \otimes C)$.

В [7] показано, что если криптосистема Мак-Элиса $\mathrm{McE}(C)$ на основе базового кода $C$ является нестойкой к атакам на ключ, то существует алгоритм нахождения подходящей перестановочной матрицы (подходящей перестановки) для криптосистемы $\mathrm{McE}(\mathbb{F}_q^l \otimes C)$, сложность выполнения которого оценивается величиной $\mathcal{O}(\frac{(nl)!}{(n!)^l l!})$. По формуле Стирлинга получаем, что

$$\frac{(nl)!}{(n!)^l l!} \approx \frac{\sqrt{2\pi nl}(\frac{nl}{e})^{nl}}{(\sqrt{2\pi n}(\frac{n}{e})^n)^l \sqrt{2\pi l}(\frac{l}{e})^l} = \sqrt{\frac{n}{(2\pi n)^l}} \cdot e^l \cdot l^{l\cdot(n-1)}. \tag{13}$$

Кроме того, для нахождения подходящей перестановки, в случае существования дискриминанта для кода $\mathbb{F}_q^l \otimes C$, может быть применен алгоритм SSA. Рассмотрим наиболее выгодные, с точки зрения атакующего, условия, когда для кода $\mathbb{F}_q^l \otimes C$ известна эффективно вычисляемая сигнатура $\mathcal{S}$, имеющая $n$ различных значений для кода $\mathbb{F}_q^l \otimes C$, а также построена трансверсаль $\Omega$ фактор-множества $Q/\mathcal{G}(\mathbb{F}_q^l \otimes C)$. Таким образом, выполняются условия теоремы 1, и поэтому вместо алгоритма SSA атакующим может быть применен алгоритм SSAForTensor. Из теоремы 1 получаем, что стойкость криптосистемы $\mathrm{McE}(\mathbb{F}_q^l \otimes C)$ оценивается величиной $\mathcal{O}(|\Omega|) = \mathcal{O}((l!)^{n-1})$. Используя формулу Стирлинга, получаем

$$(l)!^{n-1} \approx \left(\sqrt{2\pi l}\left(\frac{l}{e}\right)^l\right)^{n-1} = \left(\frac{\sqrt{2\pi l}}{e^l}\right)^{n-1} \cdot l^{l\cdot(n-1)}. \tag{14}$$

Заметим, что (13) и(14) — это оценки на мощности множеств ключей, по которым перебором осуществялется поиск подходящих перестановок соответственно алгоритмом из [7] и алгоритмом SSAForTensor. В настоящее время, согласно [10], считается вычислительно не осуществимым перебор по ключевому множеству мощности $2^{128}$ и более. Для наглядного сравнения оценок (13) и (14) рассмотрим пример, когда для построения индуцированного кода $\mathbb{F}_q^l \otimes C$ используется двоичный $[n, k, d]$-код $C$ Рида–Маллера, $n \in \{8, 16, 32, 64, 128, 256\}$, $q = 2$.

В таблицах 2 и 1 приведены результаты вычисления величины $\log_2 K$ для атаки на криптосистему $\mathrm{McE}(\mathbb{F}_2^l \otimes C)$, $l \in \{2, 3, 4, 5, 6, 7, 8, 9\}$, где для таблицы 1 значение $K$ вычисляется в соответствии с (13), а для таблицы 2 – в соответствии с (14). В таблицах 1 и 2 выделены ячейки, соответствующие тем параметрам индуцированного кода $\mathbb{F}_2^l \otimes C$, для которых сложность перебора не менее $2^{128}$. Сравнение соответствующих значений из таблиц показывает, что атака на основе алгоритма расщепления носителя SSAForTensor существенно эффективнее атаки, описанной в [7], однако при подборе параметров $n$ и $l$ эта атака может быть также неосуществимой.

В [11] показано, что применение индуцированных кодов в криптосистемах типа Мак-Элиса приводит к ослаблению стойкости этой системы к атакам на шифрограмму на основе метода декодирования по информационным совокупностям. Приемлемая стойкость к таким атакам достигается при больших длинах кода. Это связано с тем, что размерность и длина индуцированных кодов увеличиваются в $l$ раз,

Таблица 1. Значения величины $\log_2(\frac{(nl)!}{(n!)^l l!})$.

Table 1. Values of $\log_2(\frac{(nl)!}{(n!)^l l!})$.

| $l$ / n | 8 | 16 | 32 | 64 | 128 | 256 |
|---|---|---|---|---|---|---|
| 2 | 12.73 | 28.23 | 59.73 | 123.23 | **250.73** | **506.23** |
| 3 | 30.63 | 67.67 | **142.75** | **293.90** | **597.22** | **>1024** |
| 4 | 51.96 | 114.46 | **240.96** | **495.46** | **1006** | **>1024** |
| 5 | 75.85 | **166.72** | **350.48** | **719.99** | **>1024** | **>1024** |
| 6 | 101.77 | **223.34** | **469** | **962.81** | **>1024** | **>1024** |
| 7 | **129.37** | **283.59** | **595.01** | **>1024** | **>1024** | **>1024** |
| 8 | **158.43** | **346.93** | **727.43** | **>1024** | **>1024** | **>1024** |
| 9 | **188.75** | **412.99** | **865.46** | **>1024** | **>1024** | **>1024** |

Таблица 2. Значения величины $\log_2(((l)!)^{n-1})$.

Table 2. Values of $\log_2(((l)!)^{n-1})$.

| $l$ / n | 8 | 16 | 32 | 64 | 128 | 256 |
|---|---|---|---|---|---|---|
| 2 | 7 | 15 | 31 | 63 | 127 | **255** |
| 3 | 18.09 | 38.77 | 80.13 | **162.85** | **328.29** | **659.16** |
| 4 | 32.09 | 68.77 | **142.13** | **288.85** | **582.29** | **>1024** |
| 5 | 48.34 | 103.60 | **214.11** | **435.13** | **877.17** | **>1024** |
| 6 | 66.44 | **142.37** | **294.24** | **597.98** | **>1024** | **>1024** |
| 7 | 86.09 | **184.48** | **381.27** | **774.85** | **>1024** | **>1024** |
| 8 | 107.09 | **229.48** | **474.27** | **963.84** | **>1024** | **>1024** |
| 9 | **129.28** | **277.03** | **572.54** | **>1024** | **>1024** | **>1024** |

однако кодовое расстояние не меняется. Тем не менее, применение криптосистемы $\mathrm{McE}(\mathbb{F}_2^l \otimes C)$ возможно в тех случаях, когда при шифровании добавляются векторы ошибок веса, большего, чем может исправить декодер $\mathrm{Dec}_{\mathbb{F}_2^l \otimes C}$. Например, в [7] предложен протокол выработки общего секретного ключа на основе построенной криптосистемы. В следующем подразделе предлагается еще одно применение индуцированных кодов: применение в криптографических протоколах идентификации.

## 3.2. Протокол идентификации на основе индуцированных кодов

В [12] М. Жиро построил протокол идентификации на основе сложности нахождения перестановки для двух перестановочно-эквивалентных кодов над бинарным полем. Приведем этот протокол для случая $\mathbb{F}_q$. Пусть $H$ — это $(N-K \times N)$-матрица над полем $\mathbb{F}_q$, общая для всех пользователей протокола. Каждый пользователь $\mathcal{P}$

выбирает случайно вектор $\mathbf{e}$ небольшого веса $w$ и вычисляет $H\mathbf{e}^\top = \mathbf{s}^\top$. Вектор $\mathbf{s}$ является публичным идентификатором пользователя $\mathcal{P}$. В случае, когда проверяющая сторона $\mathcal{V}$ намерена провести аутентификацию пользователя $\mathcal{P}$, то есть проверить, что аутентифицируемый пользователь знает вектор $\mathbf{e}$, выполняется 3-шаговый протокол.

**Шаг 1:** $\mathcal{P}$ случайно и равновероятно выбирает перестановочную $(N \times N)$-матрицу $P$ и невырожденную $(N-K \times N-K)$-матрицу $S$, вычисляет $\widetilde{H} = SHP$, $\mathbf{s}' = S\mathbf{s}$ и отправляет $\mathcal{V}$ матрицу $\widetilde{H}$ и вектор $\mathbf{s}'$.
**Шаг 2:** $\mathcal{V}$ случайно и равновероятно выбирает бит $c \in \{0, 1\}$ и посылает его $\mathcal{P}$.
**Шаг 3а:** Если $c = 0$, то $\mathcal{P}$ передает матрицы $S$ и $P$ стороне $\mathcal{V}$, которая проверяет, что $SHP = \widetilde{H}$ и $\mathbf{s}' = S\mathbf{s}$.
**Шаг 3б:** Если $c = 1$, то $\mathcal{P}$ передает $\mathbf{e}' = P^{-1}\mathbf{e}$ стороне $\mathcal{V}$, которая проверяет, что $\mathrm{wt}(\mathbf{e}') = w$ и $\widetilde{H}\mathbf{e}' = \mathbf{s}$.

Этот протокол выполняется $m$ раз, где параметр безопасности $m$ выбирается так, чтобы вероятность $1/2^m$ мошенничества доказывающей стороны была менее наперед заданного порога. Оценим коммуникационную сложность этого протокола. На Шаге 1 доказывающая сторона передает $(N-K)(N+1)\log_2 q$ бит данных. На втором шаге проверящая сторона передает один бит. Количество передаваемых данных на Шаге 3 зависит от значения бита $c$: при $c = 0$ передается $(N-K)^2 \log_2 q + N \log_2 N$ бит, а при $c = 1$ передается $N \log_2 q$ бит. Учитывая, что значение бита $c$ выбирается случайно и равновероятно, то в среднем за $m$ итераций коммуникационная сложность протокола составит

$$\left(1 + \frac{3N-K}{2}\right) m(N-K)\log_2 q + N(\log_2 N + m/2 \log_2 q) + m \text{ бит}. \qquad (15)$$

В [13] отмечено, что если матрица $H$ выбирается случайно, то протокол Жиро не является стойким. В то же время отмечено, что возможно применение кодов, для которых остов имеет большую размерность, так как сложность вычисления сигнатуры $\mathcal{S}^W$, предложенной в [8], зависит нелинейно от размерности остова. К таким кодам, например, относятся индуцированные коды вида $\mathbb{F}_q^l \otimes C$, так как размерность остова таких кодов, как следует из (5), в $l$ раз больше размерности остова базового кода $C$. Если не учитывать сложность вычисления сигнатуры (т.е. полагать, что сигнатура вычисляется эффективно), то, как следует из таблицы 2, для реализации протокола Жиро может быть использован такой код $\mathbb{F}_q^l \otimes C$ на основе кода Рида–Маллера, для которого значение ячейки в таблице 2 больше 128. Учитывая, что коммуникационная сложность (15) растет с ростом $N = ln$, следует выбирать те параметры индуцированного кода, для которого $ln$ принимает наименьшее из допустимых значений. В рассмотренном в предыдущем подразделе примере минимально допустимое значение $ln$ равно $72 = 9 \cdot 8$.

# Список литературы / References

[1] McEliece R. J., "A Public-Key Cryptosystem Based on Algebraic Coding Theory", *JPL Deep Space Network Progress Report*, 1978, № 42–44, 114–116.

[2] Sendrier N., Tillich J. P., *Code-Based Cryptography: New Security Solutions Against a Quantum Adversary*, ERCIM News, ERCIM, 2016 https://hal.archives-ouvertes.fr/hal-01410068/document.

[3] Morelos-Zaragoza R. H., *The Art of Error Correcting Coding*, 2nd Edition, John Wiley & Sons, Inc., 2006.

[4] Sidel'nikov V. M., Shestakov S. O, "On an encoding system constructed on the basis of generalized Reed-Solomon codes", *Discrete Mathematics and Applications*, **2**:4 (1992), 439–444.

[5] Бородин М. А., Чижов И. В., "Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера", *Дискрет. матем.*, **26**:1 (2014), 10–20; English transl.: Borodin M. A., Chizhov I. V., "Effective attack on the McEliece cryptosystem based on Reed-Muller codes", *Discrete Mathematics and Applications*, **24**:5 (2014), 273–280.

[6] Деундяк В. М., Косолапов Ю. В., "Алгоритмы для мажоритарного декодирования групповых кодов", *Модел. и анализ информ. систем*, **22**:4 (2015), 464–482; [Deundyak V. M., Kosolapov Yu. V., "Algorithms for majority decoding of group codes", *Model. Anal. Inform. Sist.*, **22**:4 (2015), 464–482, (in Russian).]

[7] Деундяк В. М., Косолапов Ю. В., "Криптосистема на индуцированных групповых кодах", *Модел. и анализ информ. систем*, **23**:2 (2016), 137–152; [Deundyak V. M., Kosolapov Yu. V., "Cryptosystem based on induced group codes", *Model. Anal. Inform. Sist.*, **23**:2 (2016), 137–152, (in Russian).]

[8] Sendrier N., "Finding the Permutation Between Equivalent Linear Codes: The Support Splitting Algorithm", *IEEE Trans. on IT*, **46**:4 (2000), 1193–1203.

[9] Haily A., Harzalla D., "On Binary Linear Codes Whose Automorphism Group is Trivial", *Journal of Discrete Mathematical Sciences and Cryptography*, **18**:5 (2015), 495–512.

[10] Lenstra A. K., Verheul E. R., "Selecting Cryptographic Key Sizes", *Journal of Cryptology*, **14**:4 (2001), 255–293.

[11] Деундяк В. М., Косолапов Ю. В., "Использование тензорного произведения кодов Рида–Маллера в асимметричной криптосистеме типа Мак-Элиса и анализ ее стойкости к атакам на шифрограмму", *Вычислительные технологии*, **22**:4 (2017), 43–60; [Deundyak V. M., Kosolapov Yu. V., "The use of the tensor product of Reed-Muller codes in asymmetric McEliece type cryptosystem and analysis of its resistance to attacks on the cryptogram", *Computational Technologies*, **22**:4 (2017), 43–60, (in Russian).]

[12] Girault M., "A (non-practical) three-pass identification protocol using coding theory", *Advances in Cryptology AUSCRYPT '90*, Lecture Notes in Computer Science, **453**, 1990, 265–272.

[13] Sendrier N., Simos D. E., "The Hardness of Code Equivalence over $\mathbb{F}_q$ and its Application to Code-based Cryptography", *Post-Quantum Cryptography. PQCrypto 2013*, Lecture Notes in Computer Science, **7932**, 2013, 203–216.

**Kosolapov Yu. V., Shigaev A. N.**, "The Support Splitting Algorithm for Induced Codes", *Modeling and Analysis of Information Systems*, **25**:3 (2018), 276–290.

**DOI:** 10.18255/1818-1015-2018-3-276-290

**Abstract.** In the paper, the analysis of the stability of the McEliece-type cryptosystem on induced codes for key attacks is examined. In particular, a model is considered when the automorphism group is trivial for the base code $C$, on the basis of which the induced code $\mathbb{F}_q^l \otimes C$ is constructed. In this case, as shown by N. Sendrier in 2000, there exists such a mapping, called a complete discriminant, by means of which a secret permutation that is part of the secret key of a McEliece-type cryptosystem can be effectively found. The automorphism group of the code $\mathbb{F}_q^l \otimes C$ is nontrivial, therefore there is no complete discriminant for this code. This suggests a potentially high resistance of the McEliece-type cryptosystem on the code $\mathbb{F}_q^l \otimes C$. The algorithm for splitting the support for the code $\mathbb{F}_q^l \otimes C$ is constructed and the efficiency of this algorithm is compared with the existing attack on the key of the McElice type cryptosystem based on the code $\mathbb{F}_q^l \otimes C$.

**Keywords:** group codes, induced group codes, support splitting algorithm, the McEliece cryptosystem

**On the authors:**
Yury V. Kosolapov , orcid.org/0000-0002-1491-524X, PhD,
South Federal University,105/42 Bolshaya Sadovaya Str., Rostov-on-Don, 344006, Russia, e-mail: itaim@mail.ru

Aleksey N. Shigaev, orcid.org/0000-0001-6363-4332, graduate student,
South Federal University, 105/42 Bolshaya Sadovaya Str., Rostov-on-Don, 344006, Russia, e-mail: aleksejshig@gmail.com