*Моделирование и анализ информационных систем*. Т. 23, № 2 (2016), с. 137–152
*Modeling and Analysis of Information Systems*. Vol. 23, No 2 (2016), pp. 137–152


**DOI:** 10.18255/1818-1015-2016-2-137-152
УДК 517.9

# Криптосистема на индуцированных групповых кодах

**Деундяк В. М., Косолапов Ю. В.**

*получена 15 марта 2016*

**Аннотация.** Код $C$ на группе $\mathcal{G}$, индуцированный кодом $N$ на подгруппе $\mathcal{H}$, обладает тем свойством, что для декодирования кода $C$ может применяться декодер кода $N$. Поэтому, если для $N$ имеется эффективный алгоритм декодирования, то по $N$ с помощью конструкции индуцирования можно построить класс кодов с известными алгоритмами декодирования. Эта особенность используется в настоящей работе для построения кодовой криптосистемы с открытым ключом типа Мак-Элиса на индуцированных групповых кодах. Для этой криптосистемы описаны операции шифрования и расшифрования, приводится анализ стойкости к атаке на ключ, а также выделены слабые ключи, в случае использования которых взлом криптосистемы типа Мак-Элиса на индуцированном коде $C$ сводится к взлому этой криптосистемы на коде $N$. Показано, что практически стойкая криптосистема на индуцированном коде $C$ может быть построена на коде $N$ малой длины. На основе предложенной криптосистемы разработан протокол выработки общего ключа по открытому каналу.

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

**Для цитирования:** Деундяк В. М., Косолапов Ю. В., "Криптосистема на индуцированных групповых кодах", *Моделирование и анализ информационных систем*, **23**:2 (2016), 137–152.

**Об авторах:**
Деундяк Владимир Михайлович, orcid.org/0000-0001-8258-2419, канд. физ.-мат. наук, доцент,
ФГНУ НИИ "Спецвузавтоматика", пер. Газетный, 51, г. Ростов-на-Дону, 344002, Россия,
Южный Федеральный Университет, ул. Большая Садовая, 105/42, г. Ростов-на-Дону, 344006, Россия,
e-mail: vl.deundyak@gmail.com,
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

## Введение

В [1] Р. Мак-Элисом была предложена криптосистема с открытым ключом, основанная на применении помехоустойчивых кодов Гоппы. В дальнейшем идея применения помехоустойчивых кодов в асимметричных криптосистемах получила развитие. Именно, были построены такие наиболее известные в настоящее время кодовые криптосистемы, как система Нидеррайтера на основе кодов Рида–Соломона [2], система Габидулина–Парамонова–Третьякова (ГПТ) на основе ранговых кодов [3], система Сидельникова на основе кодов Рида–Маллера [4]. Ниже такие криптосистемы

будем называть криптосистемами *типа* Мак-Элиса, так как правила построения открытого и секретного ключа в таких системах во многом схожи с соответствующими правилами из работы [1].

Отметим, что к настоящему моменту эффективные атаки на ключ классической криптосистемы Мак-Элиса не известны. В то же время для других перечисленных выше криптосистем такие атаки имеются. В частности, для криптосистемы Нидеррайтера, основанной на расширенных кодах Рида–Соломона, в [5] Сидельниковым В.М. и Шестаковым С.О. построен полиномиальный по времени алгоритм нахождения подходящего секретного ключа; в [6] и [7] построены редукции криптоаналитического алгоритма Сидельникова–Шестакова для классических кодов Рида–Соломона. В [8] показано, что классическая криптосистема ГПТ на ранговых кодах небольших параметров также не является стойкой к атакам на ключ; в [9] построены атаки на ключ для некоторых модификаций системы ГПТ. Для криптосистемы Сидельникова алгоритм успешной атаки на ключ построен в [10], а в [12] этот алгоритм существенно ускорен.

В настоящей работе с целью усиления стойкости криптосистемы к атакам на ключ строится новая кодовая асимметричная криптосистема на основе индуцированных групповыми кодами. Индуцированные групповые коды представляют интерес по той причине, что их декодирование может быть выполнено с помощью декодера для кода, на основе которого строятся индуцированные коды. В работе рассматривается задача усиления стойкости криптосистемы за счет использования индуцированных кодов.

Статья имеет следующую структуру. В первом разделе приводится определение групповых кодов и рассматривается конструкция индуцированных кодов; для последующих криптографических приложений уточняются операции кодирования и декодирования групповых и индуцированных кодов; формулируется ряд утверждений, необходимых при анализе стойкости криптосистемы типа Мак-Элиса на индуцированных кодах. В разделе 2 на индуцированных кодах конструируется криптосистема типа Мак-Элиса и проводится анализ ее криптостойкости. В третьем разделе на основе построенной криптосистемы строится протокол выработки общего секретного ключа.

# 1. Индуцированные групповые коды

## 1.1. Групповые коды

Пусть $\mathbb{F}$ — поле Галуа, $V = \mathbb{F}^m$ и $(V, \rho)$ — метрическое пространство с метрикой Хэмминга $\rho$ и стандартным базисом $B$. Для вектора $\mathbf{x}(\in V)$ множество базисных векторов, коэффициенты при которых в разложении $\mathbf{x} = \sum_{\mathbf{b}\in B} x_{\mathbf{b}}\mathbf{b}$ ненулевые, называется носителем вектора $x$ относительно базиса $B$ и обозначается $\mathrm{supp}_B(\mathbf{x})$. Тогда $w(\mathbf{x}) = |\mathrm{supp}_B(\mathbf{x})|$ – вес вектора $\mathbf{x}$. Носителем множества $D$ ($D \subseteq V$) называется множество $\mathrm{supp}_B(D) := \cup_{\mathbf{x}\in D}\mathrm{supp}_B(\mathbf{x})$.

Всякое линейное подпространство $C$ метрического пространства $(V, \rho)$ называется линейным кодом. Размерность, длину (мощность множества $\mathrm{supp}(C)$) и минимальное расстояние (относительно метрики $\rho$) кода $C$ будем обозначать соответственно $k(C)$, $n(C)$ и $d(C)$, а код $C$ с такими параметрами будем называть

$[n(C), k(C), d(C)]$-кодом [13]. Двойственный код к коду $C$ обозначим $C^{\perp}$. Если $G(C)$ – порождающая матрица кода $C$, то кодирование удобно представить в виде отображения: $\mathrm{Enc}_C : \mathbb{F}^{k(C)} \to \mathbb{F}^{n(C)}$, причем $\mathrm{Enc}_C(\mathbf{s}) = \mathbf{s}G(C)$ для любого информационного вектора $\mathbf{s} \in \mathbb{F}^k(C)$. Будем полагать, что для $C$ имеется эффективный алгоритм декодирования $\mathrm{Dec}_C$ который позволяет исправить до $t := \lfloor (d(C) - 1)/2 \rfloor$ ошибок и реализует отображение $\mathrm{Dec}_C : \mathbb{F}^{n(C)} \to \mathbb{F}^{k(C)}$.

Пусть $\mathcal{G}$ — конечная группа, $\hat{1}(\in \mathcal{G})$ – нейтральный элемент. Рассмотрим групповую алгебру $\mathbb{F}\mathcal{G}$, элементами которой являются формальные суммы (функции)

$$\sum_{g \in \mathcal{G}} a_g g, a_g \in \mathbb{F}. \tag{1}$$

Группа $\mathcal{G}$ действует слева на $\mathbb{F}\mathcal{G}$ по правилу:

$$\mathcal{G} \times \mathbb{F}\mathcal{G} \ni (g, \phi = \sum_{h \in \mathcal{G}} \phi_h h) \mapsto \phi g^{-1} := \sum_{h \in \mathcal{G}} \phi_{hg^{-1}} h \in \mathbb{F}\mathcal{G}. \tag{2}$$

В $\mathbb{F}\mathcal{G}(\cong \mathbb{F}^{|\mathcal{G}|})$ зафиксируем базис $B = B^{\mathcal{G}} := \{\delta_g = 1g\}_{g \in \mathcal{G}}$, что позволяет рассматривать в этой алгебре метрику Хэмминга $d_B$. Групповым $\mathbb{F}\mathcal{G}$–кодом, следуя [14], будем называть левый идеал алгебры $\mathbb{F}\mathcal{G}$. Отметим, что длина группового кода равна $|\mathcal{G}|$.

Пусть $C$ — групповой $[n(C), k(C), d(C)]$-код, $C \subseteq \mathbb{F}\mathcal{G}$, $n(C) = |\mathcal{G}|$, $B(C) := \{\epsilon_1; ...; \epsilon_{k(C)}\}$ – базис кода $C$, где для $i = 1, ..., k(C)$ имеет место представление:

$$\epsilon_i = \sum_{g \in \mathcal{G}} \alpha_{i,g} \delta_g, \quad \alpha_{i,g} \in \mathbb{F}.$$

Тогда при кодировании произвольному информационному вектору $\mathbf{s} = (s_1, ..., s_{k(C)})$ ставится в соответствие кодовый вектор $\mathbf{c} = \mathrm{Enc}_C(\mathbf{s})$ вида:

$$\mathbf{c} = \sum_{i=1}^{k(C)} s_i \epsilon_i = \sum_{i=1}^{k(C)} s_i \sum_{g \in \mathcal{G}} \alpha_{i,g} \delta_g = \sum_{g \in \mathcal{G}} (\sum_{i=1}^{k(C)} s_i \alpha_{i,g}) \delta_g.$$

Для определения порождающей матрицы $G(C)$ группового $\mathbb{F}\mathcal{G}$–кода $C$ зададим линейный порядок $\{g_1 = \hat{1}; ...; g_{|\mathcal{G}|}\}$ на группе $\mathcal{G}$, который естественным образом однозначно определяет линейный порядок на базисе $B$. Зафиксированный на группе порядок будем обозначать $\mathrm{ord}(\mathcal{G})$. Порядок $\mathrm{ord}(\mathcal{G})$ определяет отображение $\nu_{\mathcal{G}} : \mathbb{F}\mathcal{G} \to \mathbb{F}^{|\mathcal{G}|}$, поэтому матрица $G(C)$ имеет вид:

$$G(C) = \begin{pmatrix} \nu_{\mathcal{G}}(\epsilon_1) \\ ... \\ \nu_{\mathcal{G}}(\epsilon_{k(C)}) \end{pmatrix}.$$

Другими словами, порождающая матрица $G(C)$ – это матричное представление базиса $B(C)$ через стандартный базис $B$ алгебры $\mathbb{F}\mathcal{G}$.

В работе [15] разработаны алгоритмы для мажоритарного декодирования групповых кодов. В основе разработанных алгоритмов лежит мажоритарный декодер Дж. Мэсси [16], использующий декодирующие деревья [14], а представление кодов

в виде идеалов групповых алгебр позволяет эффективно строить декодирующие деревья. Для кода $C$ декодирующим деревом $\mathrm{WB}_{\mathbf{b},r,L_{\mathbf{b}}} = \mathrm{WB}_{\mathbf{b},r,L_{\mathbf{b}}}[C]$ будем называть помеченное дерево с корнем $\mathbf{b}$, обладающее следующими свойствами:

• множество вершин этого дерева состоит из $L_{\mathbf{b}}+1$ уровня; корень $\mathbf{b}(\in B)$ находится на уровне 0, а листья – на уровне $L_{\mathbf{b}}$;

• каждая вершина, не являющаяся листом, имеет не менее $r(\in \mathbb{N})$ непосредственно следующих за ней вершин;

• листья дерева помечены элементами из $C^{\perp}$;

• метки $\mathbf{v}^{(1)},...,\mathbf{v}^{(r)}$ вершин, непосредственно следующих из произвольной вершины $\mathbf{v}$, находящейся на уровне $i(0 \le i < L_{\mathbf{b}})$, образуют в совокупности множество, $M$-ортогональное $\mathbf{v}$: $\mathrm{supp}_B(\mathbf{v}^{(i)}) \cap \mathrm{supp}_B(\mathbf{v}^{(j)}) = \mathrm{supp}_B(\mathbf{v})$ для всех $i \ne j$.

Далее полагается, что

$$r_{\mathbf{b}} := \max\{r \in \mathbb{N} : \exists \ \ \mathrm{WB}_{\mathbf{b},r,L_{\mathbf{b}}}[C] \text{ для некоторого натурального } L_{\mathbf{b}}\}. \tag{3}$$

Пусть $\mathcal{W}[C] = \{\mathrm{WB}_{\mathbf{b},r_{\mathbf{b}},L_{\mathbf{b}}}[C]\}_{\mathbf{b}\in B}$ — набор декодирующих деревьев кода $C$. Величина

$$\mathrm{dmaj}_B(C) := \min_{\mathbf{b}\in B}\{r_{\mathbf{b}}\} \tag{4}$$

называется MLD-расстоянием кода $C$ [14], с. 53. Отметим, что если для $[n(C), k(C), d(C)]$-кода $C$ выполняется равенство $d(C) = \mathrm{dmaj}_B(C)+1$, то он называется MLD-кодом [14]. Обозначим символом $\mathrm{MajDecoder}_C$ декодер, описанный в алгоритме Decoder3 работы [15], который по принятому из канала слову $\mathbf{v} = \mathbf{c}+\mathbf{e}$, соответствующему информационному вектору $\mathbf{s}(\in \mathbb{F}^{k(C)})$, и набору декодирующих деревьев $\mathcal{W}[C]$ возвращает вектор $\mathbf{s}'(\in \mathbb{F}^{k(C)})$, при этом $\mathbf{s}' = \mathbf{s}$, если $w(\mathbf{e}) \le \lfloor \mathrm{dmaj}_B(C)/2 \rfloor$.

## 1.2. Конструкция индуцированных групповых кодов

Пусть $\mathcal{H}$ — подгруппа группы $\mathcal{G}$, $|\mathcal{H}| = u$. Определенный выше порядок $\mathrm{ord}(\mathcal{G})$ на группе $\mathcal{G}$ индуцирует естественным образом линейный порядок $\mathrm{ord}(\mathcal{H}) = \{h_1 = \hat{1}; ....; h_u\}$ на подгруппе $\mathcal{H}$ и отображение $\nu_{\mathcal{H}} : \mathbb{F}\mathcal{H} \to \mathbb{F}^{|\mathcal{H}|}$. Группа $\mathcal{G}$ разбивается на множество непересекающихся правых классов смежности $\{\mathcal{H}y\}_{y\in Y}$ по $\mathcal{H}$, где $Y(\subset \mathcal{G})$ — правая трансверсаль $\mathcal{G}$ по $\mathcal{H}$. Отметим, что порядок $\mathrm{ord}(\mathcal{G})$ естественным образом индуцирует порядок $\mathrm{ord}(Y) = \{y_1; y_2; ...; y_\lambda\}$ на выбранной трансверсали $Y$, где $\lambda = [\mathcal{G} : \mathcal{H}]$. Так как $\mathbb{F}\mathcal{G}$ является свободным левым $\mathbb{F}\mathcal{H}$-модулем с базисом $Y$, т.е.

$$\mathbb{F}\mathcal{G} = \bigoplus_{i=1}^{\lambda} (\mathbb{F}\mathcal{H})\delta_{y_i}, \tag{5}$$

то базис $B^{\mathcal{G}}$ представим в виде: $B^{\mathcal{G}} = \cup_{i=1}^{\lambda} B^{\mathcal{H}}\delta_{y_i}$, где $B^{\mathcal{H}} = \{\delta_h\}_{h\in\mathcal{H}}$ — базис в линейном векторном пространстве $\mathbb{F}\mathcal{H}$. Индуцированный порядок на подгруппе $\mathcal{H}$ однозначно определяет линейный порядок на базисе $B^{\mathcal{H}}$.

Рассмотрим $\mathbb{F}\mathcal{H}$–код $N$ размерности $k(N) = |B(N)|$ и длины $n(N) = |\mathcal{H}| = u$ с $\mathbb{F}$-базисом $B(N) = \{\eta_1; ...; \eta_{k(N)}\}$, $\eta_i = \sum_{h\in\mathcal{H}} \beta_{i,h}\delta_h$, $i = 1, ..., k(N)$. Порождающая

матрица $G(N)$ имеет вид:

$$G(N)=\begin{pmatrix}\nu_{\mathcal{H}}(\eta_1)\\ \dots\\ \nu_{\mathcal{H}}(\eta_{k(N)})\end{pmatrix}=\begin{pmatrix}\beta_{1,h_1} & \beta_{1,h_2} & \dots & \beta_{1,h_{n(N)}}\\ \beta_{2,h_1} & \beta_{2,h_2} & \dots & \beta_{2,h_{n(N)}}\\ \dots & \dots & \dots & \dots\\ \beta_{k(N),h_1} & \beta_{k(N),h_2} & \dots & \beta_{k(N),h_{n(N)}}\end{pmatrix}=\left(B_1|...|B_{n(N)}\right), \tag{6}$$

где $B_j=(\beta_{1,h_j},...,\beta_{k(N),h_j})^{\top}$ – вектор-столбец.

Тензорное произведение $\mathbb{F}\mathcal{G}\otimes_{\mathbb{F}\mathcal{H}}N(\subseteq\mathbb{F}\mathcal{G})$ является $\mathbb{F}\mathcal{G}$-кодом и называется кодом, индуцированным $\mathbb{F}\mathcal{H}$-кодом $N$ [14], с. 41. (Теория тензорных произведений модулей, в рамках которой изучаются тензорные произведения групповых кодов, изложена, например, в [17].) Базис индуцированного кода может быть выражен через базис кода $N$ и трансверсаль $Y$:

$$B(\mathbb{F}\mathcal{G}\otimes_{\mathbb{F}\mathcal{H}}N)=\cup_{i=1}^{\lambda}B(N)\delta_{y_i}. \tag{7}$$

Таким образом, размерность $k(\mathbb{F}\mathcal{G}\otimes_{\mathbb{F}\mathcal{H}}N)$ индуцированного кода $\mathbb{F}\mathcal{G}\otimes_{\mathbb{F}\mathcal{H}}N$ равна $|Y|k(N)$, а длина $n(\mathbb{F}\mathcal{G}\otimes_{\mathbb{F}\mathcal{H}}N)$ этого кода равна $|\mathcal{G}|=|Y|n(N)$. Отметим, что если $\mathrm{supp}_B(B(N))=B^{\mathcal{H}}$, то

$$\mathrm{supp}_B(B(N)\delta_x)\cap\mathrm{supp}_B(B(N)\delta_z)=\begin{cases}\mathrm{supp}_B(B(N)\delta_x), & \text{если } x-z\in\mathcal{H},\\ \emptyset, & \text{если } x-z\notin\mathcal{H}.\end{cases}$$

Опишем правило кодирования для индуцированного кода. Из (7) следует, что базис индуцированного кода состоит из векторов (функций) вида:

$$\kappa_{i,j}=\eta_i\delta_{y_j},\quad i=1,...,k(N),\quad j=1,...,\lambda.$$

Введем одинарную нумерацию на базисных векторах $\kappa_{i,j}$, полагая, что $\kappa_l:=\kappa_{i,j}$, если $l=i+(j-1)k(N)$. Рассмотрим две такие вспомогательные функции

$$\widehat{i}:\{1;...;k(N)\lambda\}\to\{1;...;k(N)\},\quad \widehat{j}:\{1;...;k(N)\lambda\}\to\{1;...;\lambda\},$$

что $\widehat{i}(l)+(\widehat{j}(l)-1)k(N)=l$. Эти две функции связывают одинарную нумерацию базисных векторов с двойной. Тогда кодирование произвольного вектора $\mathbf{s}=(s_1,...,s_{k(N)\lambda})(\in\mathbb{F}^{k(N)\lambda})$ можно представить в виде:

$$\begin{aligned}\mathbf{s}\to\mathbf{c}&=\sum_{l=1}^{k(N)\lambda}s_l\kappa_l=\sum_{l=1}^{k(N)\lambda}s_l\kappa_{\widehat{i}(l),\widehat{j}(l)}=\sum_{l=1}^{k(N)\lambda}s_l\eta_{\widehat{i}(l)}\delta_{y_{\widehat{j}(l)}}\\ &=\sum_{l=1}^{k(N)\lambda}s_l\sum_{h\in\mathcal{H}}\beta_{\widehat{i}(l),h}\delta_h\delta_{y_{\widehat{j}(l)}}=\sum_{h\in\mathcal{H}}\sum_{l=1}^{k(N)\lambda}s_l\beta_{\widehat{i}(l),h}\delta_{hy_{\widehat{j}(l)}}\\ &=\sum_{p=1}^{n(N)}\sum_{v=1}^{\lambda}\left(\sum_{i=1}^{k(N)}s_{i+(v-1)k(N)}\beta_{i,h_p}\right)\delta_{h_py_v}.\end{aligned}$$

Если $\mathbf{s} = (\mathbf{s}_1, ..., \mathbf{s}_\lambda)$ — представление информационного вектора $\mathbf{s}$ в виде конкатенации $\lambda$ подвекторов длины $k(N)$ каждый, то получаем, что в ходе кодирования для фиксированного $h_j(\in \mathcal{H})$ вычисляются $\lambda$ коэффициентов кодового вектора $\mathbf{c}$ при базисных элементах $\delta_{h_j y_1}, ..., \delta_{h_j y_\lambda}$:

$$c_{\delta_{h_j y_v}} = \left\langle \mathbf{s}_v, B_j^\top \right\rangle \quad v = 1, ..., \lambda, \tag{8}$$

где $\langle \mathbf{a}, \mathbf{b} \rangle$ — скалярное произведение векторов $\mathbf{a}$ и $\mathbf{b}$, $B_j$ — $j$-ый столбец матрицы (6). Для выбранной трансверсали $Y$ и подгруппы $\mathcal{H}$ определим на элементах группы $\mathcal{G}$ новый линейный порядок с помощью индуцированных на $Y$ и $\mathcal{H}$ соответствующих порядков $\mathrm{ord}(Y)$ и $\mathrm{ord}(\mathcal{H})$:

$$\mathrm{ord}(\mathcal{H}, Y) = \{\underbrace{h_1 y_1; h_2 y_1; ...; h_{n(N)} y_1}_{\mathcal{H} y_1}; \underbrace{h_1 y_2; h_2 y_2; ...; h_{n(N)} y_2}_{\mathcal{H} y_2}; ...; \underbrace{h_1 y_\lambda; h_2 y_\lambda; ...; h_{n(N)} y_\lambda}_{\mathcal{H} y_\lambda}\}. \tag{9}$$

Порядок $\mathrm{ord}(\mathcal{H}, Y)$, вообще говоря, отличается от исходного порядка $\mathrm{ord}(\mathcal{G})$ и задает отображение $\nu_{\mathcal{H},Y} : \mathbb{F}\mathcal{G} \to \mathbb{F}^{|\mathcal{G}|}$. Отметим, что порядок выбранной трансверсали $Y$ индуцирует порядок $\mathrm{ord}(Y, \mathcal{G}/\mathcal{H})$ на смежных классах фактор-группы $\mathcal{G}/\mathcal{H}$, из которых выбраны соответствующие элементы трансверсали.

Пусть $\omega_{(\mathcal{H},Y);\mathcal{G}} : \mathbb{F}^{|\mathcal{G}|} \to \mathbb{F}^{|\mathcal{G}|}$ — такое линейное отображение, что

$$\nu_{\mathcal{G}} = \nu_{\mathcal{H},Y} \circ \omega_{(\mathcal{H},Y);\mathcal{G}}, \tag{10}$$

где в композиции отображений $\nu_{\mathcal{H},Y} \circ \omega_{(\mathcal{H},Y);\mathcal{G}}$ сначала применяется отображение $\nu_{\mathcal{H},Y}$, а затем $\omega_{(\mathcal{H},Y);\mathcal{G}}$. Отметим, что отображению $\omega_{(\mathcal{H},Y);\mathcal{G}}$ соответствует перестановочная $(|\mathcal{G}| \times |\mathcal{G}|)$-матрица $W_{(\mathcal{H},Y);\mathcal{G}}$, которую назовем матрицей перехода от порядка $\mathrm{ord}(\mathcal{H}, Y)$ к порядку $\mathrm{ord}(\mathcal{G})$. В дальнейшем для $a(\in \mathbb{N})$ множество перестановочных $(a \times a)$-матриц будем обозначать $\mathrm{MP}(a)$.

**Лемма 1.** *Пусть $G(C)$ — порождающая матрица кода $C = \mathbb{F}\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N$ в зафиксированном порядке $\mathrm{ord}(\mathcal{G})$; $\mathrm{ord}(\mathcal{H})$ и $\mathrm{ord}(Y)$ — индуцированные порядки соответственно на подгруппе $\mathcal{H}$ и выбранной трансверсали $Y$, тогда*

$$G(C) = G_0(C) W_{(\mathcal{H},Y);\mathcal{G}}, \tag{11}$$

*где*

$$G_0(C) = \left(\begin{array}{c|c|c|c} G(N) & O & ... & O \\ \hline O & G(N) & ... & O \\ \hline ... & ... & ... & ... \\ \hline O & ... & ... & G(N) \end{array}\right). \tag{12}$$

*Доказательство.* Учитывая вид (6) матрицы $G(N)$, правило вычисления коэффициентов кодового слова (8) и порядок $\mathrm{ord}(\mathcal{H}, Y)$ (см. (9)), получим, что порождающая матрица кода $C = \mathbb{F}\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N$ имеет вид (12) (ср. [15], формула (16)). Для перехода к зафиксированному на $\mathcal{G}$ порядку необходимо, как следует из (10), матрицу $G_0(C)$ умножить на матрицу перехода $W_{(\mathcal{H},Y);\mathcal{G}}$. □

Очевидно, что если $Y'$ — трансверсаль, отличная от $Y$, с индуцированным на ней порядком $\mathrm{ord}(Y)'$, то существуют такие линейные отображения $\omega_{(\mathcal{H},Y);(\mathcal{H},Y')} : \mathbb{F}^{|\mathcal{G}|} \to \mathbb{F}^{|\mathcal{G}|}$ и $\omega_{(\mathcal{H},Y');\mathcal{G}} : \mathbb{F}^{|\mathcal{G}|} \to \mathbb{F}^{|\mathcal{G}|}$, что

$$\omega_{(\mathcal{H},Y);\mathcal{G}} = \omega_{(\mathcal{H},Y);(\mathcal{H},Y')} \circ \omega_{(\mathcal{H},Y');\mathcal{G}}. \tag{13}$$

Перестановочные матрицы, соответствующие отображениям $\omega_{(\mathcal{H},Y);(\mathcal{H},Y')}$ и $\omega_{(\mathcal{H},Y');\mathcal{G}}$ в (13), обозначим $W_{(\mathcal{H},Y);(\mathcal{H},Y')}$ и $W_{(\mathcal{H},Y');\mathcal{G}}$ . Далее для сокращения записи понадобится тензорное произведение $A \otimes B$ матрицы $A = (a_{i,j})$ размера $(r \times s)$ и матрицы $B$ , под которым понимается матрица вида:

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \dots & a_{1,s}B \\ a_{2,1}B & \dots & a_{2,s}B \\ \dots & \dots & \dots \\ a_{r,1}B & \dots & a_{r,s}B \end{pmatrix}.$$

**Лемма 2.** *Пусть $G(C)$ — порождающая матрица кода $C = \mathbb{F}\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N$ в зафиксированном порядке $\mathrm{ord}(\mathcal{G})$; $\mathrm{ord}(\mathcal{H})$, $\mathrm{ord}(Y)$, $\mathrm{ord}(Y')$ — индуцированные порядки соответственно на подгруппе $\mathcal{H}$ и выбранных разных трансверсалях $Y$ и $Y'$. Тогда*

$$W_{(\mathcal{H},Y);(\mathcal{H},Y')} = (M \otimes I_{n(N)})\mathrm{diag}(D_1, ..., D_\lambda), \tag{14}$$

*где $I_p$ — единичная матрица порядка $p$, $M \in \mathrm{MP}(\lambda)$, $D_i \in \mathrm{MP}(n(N))$, $i = 1, ..., \lambda$, $\mathrm{diag}(D_1, ..., D_\lambda)$ — блочно-диагональная $(n(N)\lambda \times n(N)\lambda)$-матрица.*

*Доказательство.* Непосредственно из определения порядка (9) следует, что если трансверсаль $Y'$ отличается от $Y$ только представителями смежных классов, из которых выбраны соответствующие представители (то есть если $y'_i y^{-}1_i \in \mathcal{H}$ для всех $i = 1, ..., \lambda$), то найдутся такие перестановочные $(n(N) \times n(N))$–матрицы $D_1, ..., D_\lambda$, что $W_{(\mathcal{H},Y),\mathcal{G}} = \mathrm{diag}(D_1, ..., D_\lambda)W_{(\mathcal{H},Y'),\mathcal{G}}$. В этом случае порядки на смежных классах $\mathrm{ord}(Y, \mathcal{G}/\mathcal{H})$ и $\mathrm{ord}(Y', \mathcal{G}/\mathcal{H})$, индуцированные соответствующими порядками $\mathrm{ord}(Y, \mathcal{H})$ и $\mathrm{ord}(Y', \mathcal{H})$, не отличаются. Если же трансверсаль $Y'$ выбирается произвольно, то порядки $\mathrm{ord}(Y, \mathcal{G}/\mathcal{H})$ и $\mathrm{ord}(Y', \mathcal{G}/\mathcal{H})$ совпадают с точностью до некоторой перестановки. Отсюда для произвольных $Y$ и $Y'$ следует (14). □

Из леммы 1 непосредственно следует, что $d(\mathbb{F}\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N) = d(N)$. В [14] показано также, что $\mathrm{dmaj}_{B^{\mathcal{G}}}(\mathbb{F}\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N) = \mathrm{dmaj}_{B^{\mathcal{H}}}(N)$, где $B^{\mathcal{G}}$ и $B^{\mathcal{H}}$ — канонические базисы групповых алгебр $\mathbb{F}\mathcal{G}$ и $\mathbb{F}\mathcal{H}$ соответственно. Декодирование индуцированного группового кода $\mathbb{F}\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N$ выполняется с помощью декодирующих деревьев группового кода $N$. В [14] показано, что для построения всех декодирующих деревьев индуцированного кода достаточно иметь одно дерево для кода $N$, например, $\mathrm{WB}_{\mathbf{1},r_1,L_1}[N]$, где $\mathbf{1} = 1\delta_{\hat{1}}$, $\hat{1}$ – нейтральный элемент группы $\mathcal{H}$; в [15] построен соответствующий алгоритм MakeGWBTree, который по дереву $\mathrm{WB}_{\mathbf{1},r_1,L_1}[N]$ для любого $g \in \mathcal{G}$ строит дерево $\mathrm{WB}_{1g,r_{1g},L_{1g}}[C]$, используя действие (2). Таким образом, по дереву $\mathrm{WB}_{\mathbf{1},r_1,L_1}[N]$ набор декодирующих деревьев для индуцированного кода определяется однозначно. Заметим, что правило декодирования индуцированного кода зависит от выбора трансверсали $Y$ и зафиксированного линейного порядка на группе $\mathcal{G}$. Эта зависимость раскрывается в следующем разделе, где рассматривается стойкость криптосистемы типа Мак-Элиса на индуцированных групповых кодах.

Очевидно, что если на группе $\mathcal{G}$ зафиксирован порядок $\mathrm{ord}(\mathcal{H}, Y)$, то любое кодовое слово индуцированного кода $\mathbb{F}\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N$ представляет собой конкатенацию $\lambda$ кодовых слов кода $N$. Поэтому если на группе $\mathcal{G}$ зафиксирован порядок (9), то из представления (12) порождающей матрицы кода $C = \mathbb{F}\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N$ следует, что исправление ошибок в принятом векторе $\mathbf{z}(\in \mathbb{F}^{n(N)\lambda})$ можно выполнить путем применения $\lambda$ раз декодера $\mathrm{Dec}_N(= \mathrm{MajDecoder}_N)$ для кода $N$ к подвекторам $\mathbf{z}_i(\in \mathbb{F}^{n(N)})$ вектора $\mathbf{z} = (\mathbf{z}_1, ..., \mathbf{z}_{n(N)})$ и последующей конкатенации результатов декодирования. Обозначим такой декодер кода $C = \mathbb{F}\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N$ символом $\mathrm{Dec}_C^0$.

Таким образом, для зафиксированного порядка $\mathrm{ord}(\mathcal{G})$, если $\mathbf{z} = \mathbf{c} + \mathbf{e}(\in \mathbb{F}^{n(N)\lambda})$ – принятый вектор, соответствующий информационному вектору $\mathbf{s} \in \mathbb{F}^{k(N)\lambda}$, и $w(\mathbf{e}) \leq \mathrm{dmaj}(N)/2$, то правило декодирования вектора $\mathbf{z}(\in \mathbb{F}^{n(N)\lambda})$ имеет вид:

$$\mathrm{Dec}_{\mathbb{F}\mathcal{G}\otimes_{\mathbb{F}\mathcal{H}}N}(\mathbf{z}) = \mathrm{Dec}_C^0(\mathbf{z}W^{-1}_{(\mathcal{H},Y);\mathcal{G}}). \tag{15}$$

# 2. Криптосистемы типа Мак-Элиса на индуцированных групповых кодах

## 2.1. Криптосистема типа Мак-Элиса

Опишем криптосистему типа Мак-Элиса в случае произвольного $[n(C), k(C), d(C)]$-кода $C$; для такой криптосистемы будем использовать обозначение $\mathrm{McE}(C)$. Пусть $G(C)$ — порождающая матрица кода $C$. Для шифрования сообщений из пространства $\mathbb{F}^{k(C)}$ используется открытый ключ $\mathbf{k}_{\mathrm{pub}} = (\widetilde{G}, t = \lfloor (d(C)-1)/2 \rfloor)$, где $\widetilde{G} = SG(C)P$, $S$ – случайная невырожденная $(k(C) \times k(C))$-матрица, случайная $P$ – перестановочная $(n(C) \times n(C))$-матрица, а для расшифрования применяется секретный ключ $\mathbf{k}_{\mathrm{sec}} = (S, P)$. Правило шифрования произвольного сообщения $\mathbf{s}(\in \mathbb{F}^{k(C)})$ имеет вид: $\mathbf{z} = \mathbf{s}\widetilde{G} + \mathbf{e}$, где вес искусственно добавляемой ошибки $\mathbf{e}$ удовлетворяет неравенству $w(\mathbf{e}) \leq t$. Для расшифрования $\mathbf{c}$ секретный ключ $\mathbf{k}_{\mathrm{sec}}$ используется по правилу: $\mathbf{s} = \mathrm{Dec}_C(\mathbf{z}P^{-1})S^{-1}$.

Пусть теперь $N$ – групповой $[n(N), k(N), d(N) = \mathrm{dmaj}(N)+1]$-код, $N \subseteq \mathbb{F}\mathcal{H}$, $\mathcal{H}$ — подгруппа группы $\mathcal{G}$, $C := \mathbb{F}\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N$ —индуцированный $[\lambda n(N), \lambda k(N), d(N)]$-код, где $\lambda = (\mathcal{G} : \mathcal{H})$ – индекс подгруппы $\mathcal{H}$ в группе $\mathcal{G}$, $\mathrm{ord}(\mathcal{G})$ — зафиксированный на $\mathcal{G}$ порядок, не являющийся секретом. Рассмотрим два варианта криптосистемы типа Мак-Элиса: криптосистему $\mathrm{WeakMcE}(C)$, в которой трансверсаль является частью секретного ключа и $P = W_{(\mathcal{H},Y);\mathcal{G}}$, и криптосистему $\mathrm{InducedMcE}(C)$, в которой трансверсаль не является секретной, а $P$ случайно и равновероятно выбирается из множества перестановочных матриц размера $(n(N)\lambda \times n(N)\lambda)$. Полное описание этих криптосистем приведено в Таблице 1.

Отметим, что длины открытых и секретных ключей криптосистем $\mathrm{WeakMcE}(C)$ и $\mathrm{InducedMcE}(C)$ возрастают не более чем в $\lambda^2$ раз по сравнению с размерами соответствующих ключей криптосистемы $\mathrm{McE}(N)$.

Таблица 1. Описание криптосистем WeakMcE($C$) и InducedMcE($C$)
Table 1. Description of WeakMcE($C$) and InducedMcE($C$) cryptosystems

| | WeakMcE($C$) | InducedMcE($C$) |
|---|---|---|
| $\mathrm{ord}(\mathcal{G})$ и $\mathrm{ord}(\mathcal{H})$ | не секретные | |
| трансверсаль $Y$ | секретная | не секретная |
| матрица $S$ | случайная и равновероятная | |
| матрица $P$ | $W_{(\mathcal{H},Y);\mathcal{G}}$ | случайная и равновероятная |
| матрица $\widetilde{G}$ | $SG_0(C)P = SG_0(C)W_{(\mathcal{H},Y);\mathcal{G}}$ | $SG(C)P = SG_0(C)W_{(\mathcal{H},Y);\mathcal{G}}P$ |
| $t$ | $\lfloor \mathrm{dmaj}(N)/2 \rfloor$ | |
| шифрование $\mathbf{s}$ | $\mathbf{z} = \mathbf{s}\widetilde{G} + \mathbf{e}, w(\mathbf{e}) \le t$ | |
| расшифрование $\mathbf{z}$ | $\mathrm{Dec}_C^0\left(\mathbf{z}W^{-1}_{(\mathcal{H},Y);\mathcal{G}}\right)S^{-1}$ | $\mathrm{Dec}_C^0\left(\mathbf{z}P^{-1}W^{-1}_{(\mathcal{H},Y);\mathcal{G}}\right)S^{-1}$ |
| длина $\mathbf{k}_{\mathrm{pub}}$, битов | $\lceil (k(N)n(N)\lambda^2)\log_2\lvert\mathbb{F}\rvert\rceil$ | |
| длина $\mathbf{k}_{\mathrm{sec}}$, битов | $\left\lceil \log_2\left(\lvert\mathbb{F}\rvert^{(k(N)\lambda)^2} n(N)^\lambda \lambda!\right)\right\rceil$ | $\left\lceil \log_2\left(\lvert\mathbb{F}\rvert^{(k(N)\lambda)^2} (n(N)\lambda)!\right)\right\rceil$ |

## 2.2. Анализ стойкости криптосистем типа Мак-Элиса на индуцированных групповых кодах к атакам на ключ

В качестве модели нарушителя рассмотрим наблюдателя, целью которого является нахождение подходящего секретного ключа для правильного расшифрования криптограмм. Предполагается, что наблюдатель имеет алгоритм Attack, с помощью которого может быть эффективно найден подходящий секретный ключ для криптосистемы McE($N$).

### 2.2.1. Анализ криптосистемы WeakMcE($C$)

Так как наблюдателю неизвестна трансверсаль $Y$, то он может зафиксировать произвольную трансверсаль $Y'$, на которой зафиксированный порядок $\mathrm{ord}(\mathcal{G})$ индуцирует порядок $\mathrm{ord}(Y)$. В соответствии с леммой 2, существуют такие перестановочные матрицы $M(\in \mathrm{MP}(\lambda))$ и $D_1, ..., D_\lambda(\in \mathrm{MP}(n(N)))$, что

$$W_{(\mathcal{H},Y);\mathcal{G}} = (M \otimes I_{n(N)})\mathrm{diag}(D_1, ..., D_\lambda)W_{(\mathcal{H},Y');\mathcal{G}}. \tag{16}$$

Тогда

$$\widetilde{G} = SG_0(C)(M \otimes I_{n(N)})\mathrm{diag}(D_1, ..., D_\lambda)W_{(\mathcal{H},Y');\mathcal{G}}.$$

Так как матрицу $W_{(\mathcal{H},Y');\mathcal{G}}$ наблюдатель может построить по общеизвестному порядку $\mathrm{ord}(\mathcal{G})$ и порядку $\mathrm{ord}(\mathcal{H}, Y)$, то несложно видеть, что матрица $\widetilde{G}W^{-1}_{(\mathcal{H},Y');\mathcal{G}}$ может

быть представлена в виде:

$$\begin{aligned}\widetilde{G}W^{-1}_{(\mathcal{H},Y');\mathcal{G}} &= SG_0(C)(M \otimes I_{n(N)})\mathrm{diag}(D_1, ..., D_\lambda) \\ &= (M \otimes I_{k(N)})SG_0(C)\mathrm{diag}(D_1, ..., D_\lambda).\end{aligned} \tag{17}$$

Представим матрицу $S' = M \otimes I_{k(N)}S (\in \mathrm{GL}(k(N)\lambda, \mathbb{F}))$ в блочном виде:

$$S' = \left(\begin{array}{c|c|c|c} S'_{11} & S'_{12} & ... & S'_{1\lambda} \\ \hline S'_{21} & S'_{22} & ... & S'_{2\lambda} \\ \hline ... & ... & ... & ... \\ \hline S'_{\lambda 1} & S'_{\lambda 2} & ... & S'_{\lambda\lambda} \end{array}\right), \tag{18}$$

где $S'_{ij}$ – $(k(N) \times k(N))$-матрица. Тогда

$$\widetilde{G}W^{-1}_{(\mathcal{H},Y');\mathcal{G}} = \left(\begin{array}{c|c|c|c} S'_{11}G(N)D_1 & S'_{12}G(N)D_2 & ... & S'_{1\lambda}G(N)D_\lambda \\ \hline S'_{21}G(N)D_1 & S'_{22}G(N)D_2 & ... & S'_{2\lambda}G(N)D_\lambda \\ \hline ... & ... & ... & ... \\ \hline S'_{\lambda 1}G(N)D_1 & S'_{\lambda 2}G(N)D_2 & ... & S'_{\lambda\lambda}G(N)D_\lambda \end{array}\right). \tag{19}$$

Заметим, что, несмотря на то, что матрица $S'$ имеет полный ранг, каждая из подматриц $S'_{ij}$ может быть неполного ранга, поэтому применение алгоритма Attack непосредственно к блокам матрицы (19) не представляется корректным. С другой стороны, каждый блочный столбец в матрице (18) имеет ранг $k(N)$, следовательно, для каждого $j = 1, ..., \lambda$ в матрице

$$\left(\begin{array}{c} S'_{j1}G(N)D_j \\ \hline S'_{j2}G(N)D_j \\ \hline ... \\ \hline S'_{j\lambda}G(N)D_j \end{array}\right) = \left(\begin{array}{c} S'_{j1} \\ \hline S'_{j2} \\ \hline ... \\ \hline S'_{j\lambda} \end{array}\right) G(N)D_j \tag{20}$$

найдутся $k(N)$ линейно независимых строк, которые образуют матрицу вида $G_j = \widehat{S}_j G(N)D_j$, $\mathrm{rank}(\widehat{S}_j) = k(N)$. Тогда к матрице $G_j$ может быть применен алгоритм атаки Attack для нахождения подходящих матриц $(\widehat{S}'_j, D'_j)$ таких, что $G_j = \widehat{S}'_j G(N)D'_j$:

$$(\widehat{S}'_j, D'_j) = \mathrm{Attack}(G_j). \tag{21}$$

Таким образом, подходящий секретный ключ криптосистемы $\mathrm{WeakMcE}(C)$ может быть найден по алгоритму AttackWeakInduced.

**Теорема 1.** *Пусть $Q$ — вычислительная сложность алгоритма* Attack*, применяемого для нахождения подходящего секретного ключа для криптосистемы* $\mathrm{McE}(N)$*, тогда $\mathcal{O}(\lambda Q + (k(N)\lambda)^3)$ – вычислительная сложность* AttackWeakInduced *нахождения подходящего секретного ключа криптосистемы* $\mathrm{WeakMcE}(C)$.

*Доказательство.* В алгоритме AttackWeakInduced алгоритм Attack применяется $\lambda$ раз для нахождения перестановочной матрицы $P'$, а для нахождения матрицы $S'$ необходимо решить матричное уравнение. □

Таким образом, сложность взлома криптосистемы $\mathrm{WeakMcE}(C)$ линейно зависит от сложности взлома системы $\mathrm{McE}(N)$. Отметим также, что для каждого $i = 1, ..., \lambda$ матрица $D_i$ выбирается не из множества мощности $|\mathcal{H}|!$ всех возможных перестановочных матриц, а из множества матриц, которое имеет мощность $|\mathcal{H}|$. Поэтому алгоритм Attack, возможно, может быть существенно упрощен.

**Алгоритм 1** AttackWeakInduced

**Вход:** Матрицы $\widetilde{G}$ и $W_{(\mathcal{H},Y');\mathcal{G}}$
**Выход:** Подходящий секретный ключ $(S', P')$
**Для** $j \in \{1; ...; \lambda\}$ **выполнять**
  выбрать из матрицы $\widetilde{G}W^{-1}_{(\mathcal{H},Y');\mathcal{G}}$ столбцы с номерами $(j-1)n(N)+1, ..., jn(N)$;
  из выбранных столбцов составить матрицу $\widetilde{G}_j$;
  в $\widetilde{G}_j$ выбрать $k(N)$ линейно независимых строк;
  из выбранных строк составить матрицу $G_j$;
  $(\widehat{S}'_j, D'_j) = \mathrm{Attack}(G_j)$;// найти секретный ключ для McE$(N)$, см. (21)
**конец Для**
$P' := \mathrm{diag}(D'_1, ..., D'_\lambda)W_{(\mathcal{H},Y');\mathcal{G}}$;
решить матричное уравнение $\widetilde{G}P'^{-1} = S'G_0(C)$ относительно $S'$;
**Вернуть** $(S', P')$

### 2.2.2. Анализ криптосистемы InducedMcE$(C)$

Рассмотрим криптосистему InducedMcE$(C)$, в которой перестановочная матрица $P$ выбирается случайно и равновероятно из MP$(n(N)\lambda)$. Из (11) следует, что открытый ключ этой криптосистемы имеет вид: $\widetilde{G} = SG_0(C)W_{(\mathcal{H},Y);\mathcal{G}}P$. Отметим, что найдется такая матрица $P' \in \mathrm{MP}(n(N)\lambda)$, что $PW^{-1}_{(\mathcal{H},Y);\mathcal{G}} = W^{-1}_{(\mathcal{H},Y);\mathcal{G}}P'$, то имеет место представление

$$\widetilde{G}W^{-1}_{(\mathcal{H},Y);\mathcal{G}} = SG_0(C)P', \tag{22}$$

где $P'$ – неизвестная (секретная) матрица. Следующая лемма очевидна.

**Лемма 3.** *Множество перестановочных* $(n(N)\lambda \times n(N)\lambda)$*-матриц*

$$\Theta = \{(M \otimes I_\lambda)\mathrm{diag}(D_1, ..., D_\lambda) | M \in \mathrm{MP}(\lambda), D_i \in \mathrm{MP}(n(N)), i = 1, ..., \lambda\}. \tag{23}$$

*является подгруппой группы* MP$(n(N)\lambda)$, $|\Theta| = (n(N)!)^\lambda \lambda!$.

Таким образом, секретная матрица $P'$ (см. (22)) принадлежит одному из фактор-классов фактор-множества $\mathrm{MP}(n(N)\lambda)/\Theta = \{\Gamma_j\}_{j=1}^g$, где $g = \frac{|\mathrm{MP(n(N)\lambda)}|}{|\Theta|} = \frac{(n(N)\lambda)!}{(n(N)!)^\lambda \lambda!}$. Пусть $\Gamma \in \mathrm{MP}(n(N)\lambda)/\Theta$ — фактор-класс, которому принадлежит матрица $P'$. Тогда имеет место представление: $\Gamma = \{TP' | T \in \Theta\}$. Рассмотрим произвольную матрицу $\Pi = TP'$ из фактор-класса $\Gamma$. Из (22) следует, что

$$\begin{aligned} \widetilde{G}W^{-1}_{(\mathcal{H},Y);\mathcal{G}}\Pi^{-1} &= SG_0(C)P'\Pi^{-1} \\ &= SG_0(C)T^{-1}. \end{aligned} \tag{24}$$

В силу леммы 3, матрица $T^{-1}$ принадлежит $\Theta$. Следовательно, матрица (24) имеет вид (17), и поэтому к ней может быть применен алгоритм AttackWeakInduced. Алгоритм AttackInduced для нахождения подходящего ключа системы InducedMcE$(C)$ основан на переборе представителей смежных классов из $\mathrm{MP}(n(N)\lambda)/\Theta$.

**Алгоритм 2** AttackInduced

**Вход:** Матрицы $\widetilde{G}$ и $W_{(\mathcal{H},Y);\mathcal{G}}$
**Выход:** $(S', P')$
1: **Для** $\Gamma \in \mathrm{MP}(n(N)\lambda)/\Theta$ **выполнять**
2: выбрать любую матрицу $\Pi$ из $\Gamma$;
3: $(S', P') = \mathrm{AttackWeakInduced}(\widetilde{G}\Pi^{-1}, W_{(\mathcal{H},Y);\mathcal{G}})$;
4: **Если** $\mathrm{rank}(S') = k(N)\lambda$ **и** $P' \in \mathrm{MP}(n(N)\lambda)$ **и** $S'G_0(C)P' = \widetilde{G}\Pi^{-1}$ **тогда**
5: выйти из цикла;// подходящий ключ найден
6: **конец Если**
7: **конец Для**
8: **Вернуть** $(S', P')$;

**Теорема 2.** *Пусть $Q$ — вычислительная сложность алгоритма* Attack, *применяемого для нахождения подходящего ключа для криптосистемы* $\mathrm{McE}(N)$, *тогда*

$$\mathcal{O}\left(\left(\frac{\lambda^{n(N)-1}}{e}\right)^{\lambda}(\lambda Q + (k(N)\lambda)^3)\right)$$

*– вычислительная сложность алгоритма* AttackInduced *нахождения подходящего секретного ключа криптосистемы* $\mathrm{InducedMcE}(C)$.

*Доказательство.* Утверждение вытекает из того, что для нахождения ключа методом перебора достаточно перебрать множество представителей фактор-классов множества $\mathrm{MP}(n(N)\lambda)/\Theta$. Сложность проверки одного представителя, в соответствии с теоремой 1, составляет $\mathcal{O}(\lambda Q + (k(N)\lambda)^3)$, а всего $\frac{(n(N)\lambda)!}{(n(N)!)^{\lambda}\lambda!}$ смежных классов. Используя формулу Стирлинга ($t! \approx \sqrt{2\pi t}\left(\frac{t}{e}\right)^t$), получим искомую оценку. □

Проиллюстрируем эффект от использования индуцированных кодов на примере. Пусть $\mathbb{F} = \mathbb{F}_2$, $\mathcal{G} = \mathbb{Z}_\lambda \oplus \mathbb{Z}_2^p$, $\mathcal{H} \cong \mathbb{Z}_2^p$, $N$ — двоичный код Бермана, изоморфный двоичному коду Рида-Маллера $\mathcal{RM}(r, p)$ длины $n(N) = 2^p$ и размерности $k(N) = \sum_{i=0}^{r} C_r^i$. Согласно [11], криптосистема $\mathrm{McE}(N)$ при $p \leq 16$ может быть взломана за приемлемое время на ноутбуке с процессором 2.1 ГГц. В частности, при $p \leq 8$ ($n(N) \leq 256$) взлом длится менее одной секунды. Пусть $C = \mathbb{F}_2\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N$. Для взлома криптосистемы $\mathrm{InducedMcE}(C)$, согласно теореме 2, необходимо перебрать порядка $K(\lambda, n(N)) = \left(\frac{\lambda^{n(N)-1}}{e}\right)^{\lambda}$ ключей. В Таблице 2 приведены значения $\log_2(K(\lambda, n(N)))$ для $\lambda = 2, ..., 9$ и $n(N) = 2, 4, 8, 16, 32, 64, 128, 256$.

В настоящее время, согласно [18], считается вычислительно неосуществимым перебор по ключевому множеству мощности $2^{128}$ и более. В таблице 2 жирным шрифтом выделены те соотношения $(n(N), \lambda)$, для которых криптосистема $\mathrm{InducedMcE}(C)$ представляется стойкой. Как видно из таблицы, конструкция индуцированных кодов позволяет строить стойкие криптосистемы даже на кодах малой длины.

Таблица 2. Значения величины $\log_2(K(\lambda, n(N)))$
Table 2. Values of $\log_2(K(\lambda, n(N)))$

| | $n(N)$ | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $\lambda$ | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 |
| 2 | 0,13 | 4,13 | 12,13 | 28,13 | 60,13 | 124,13 | **252,13** | **508,13** |
| 3 | 2,04 | 11,55 | 30,57 | 68,61 | **144,69** | **296,84** | **601,16** | **>1024** |
| 4 | 4,27 | 20,27 | 52,27 | 116,27 | **244,27** | **500,27** | **1012,27** | **>1024** |
| 5 | 6,77 | 29,99 | 76,42 | **169,30** | **355,06** | **726,56** | **>1024** | **>1024** |
| 6 | 9,50 | 40,52 | 102,56 | **226,63** | **474,79** | **971,10** | **>1024** | **>1024** |
| 7 | 12,43 | 51,73 | **130,34** | **287,55** | **601,97** | **>1024** | **>1024** | **>1024** |
| 8 | 15,54 | 63,54 | **159,54** | **351,54** | **735,54** | **>1024** | **>1024** | **>1024** |
| 9 | 18,80 | 75,86 | **189,98** | **418,21** | **874,68** | **>1024** | **>1024** | **>1024** |

Примечание: $K(\lambda, n(N))$ — количество перебираемых ключей в атаке AttackInduced на криптосистему InducedMcE($\mathbb{F}_2\mathcal{G} \otimes_{\mathbb{F}\mathcal{H}} N$), $\mathcal{G} = \mathbb{Z}_\lambda \oplus \mathbb{Z}_2^p$, $\mathcal{H} \cong \mathbb{Z}_2^p$, $N \cong \mathcal{RM}(r, p)$, $n(N) = 2^p$, $\lambda = 2, ..., 9$, $p \in \{1; ...; 8\}$.

Заметим, что сохранение в секрете трансверсали $Y$ в системе InducedMcE($C$) не усиливает стойкость. Действительно, наблюдатель может выбрать любую трансверсаль $Y'$ и, как следует из (16) и (22), матрица открытого ключа тогда может быть приведена к виду:

$$\widetilde{G}W^{-1}_{(\mathcal{H},Y');\mathcal{G}} = SG_0(C)(M \otimes I_{n(N)})\mathrm{diag}(D_1, ..., D_\lambda)P'. \tag{25}$$

Если $\Pi = TP'$ — произвольная матрица из смежного класса, которому принадлежит неизвестная матрица $P'$, то

$$\widetilde{G}W^{-1}_{(\mathcal{H},Y');\mathcal{G}}\Pi^{-1} = SG_0(C)T',$$

где $T' = (M \otimes I_{n(N)})\mathrm{diag}(D_1, ..., D_\lambda)T^{-1}$ принадлежит $\Theta$ в силу леммы 3. В этом случае для нахождения подходящего секретного ключа может быть применен алгоритм AttackInduced.

## 3. Протокол генерации общего ключа

Пусть $N$ – групповой $[n(N), k(N), d(N)]$-код, $C$ – соответствующий индуцированный $[n(N)\lambda, k(N)\lambda, d(N)]$-код. Как следует из предыдущего раздела, криптосистема InducedMcE($C$) на индуцированных групповых кодах обладает высокой стойкостью к атаке на ключ. В то же время представляется, что стойкость этой криптосистемы к атакам на шифрограмму снижается по сравнению со стойкостью криптосистемы McE($N$) к аналогичным атакам. Это связано с тем, что длина кодового слова увеличивается в $\lambda$ раз, а количество ошибок, добавляемых в кодовый вектор при шифровании, остается прежним. В этом случае, во-первых, повышается вероятность успеха атаки путем декодирования по обобщенным информационным совокупностям [19],

а во-вторых, повышается вероятность успеха атаки, в ходе которой анализируется разность двух шифрограмм, соответствующих одному информационному сообщению [20]. Отметим, что одним из способов противодействия последней атаке может быть следующий. Вместо одного из $\lambda$ информационных подблоков длины $k(N)$ использовать случайный вектор длины $k(N)$, выбираемый равновероятно каждый раз заново при шифровании сообщения. Номер случайного подблока может быть общеизвестен. В этом случае разность двух шифрограмм, соответствующих одному информационному сообщению, уже не будет равна разности векторов ошибок, добавленных при шифровании.

Снижения вероятностей успеха отмеченных атак на шифрограмму $\mathbf{z} = \mathbf{c} + \mathbf{e}$ (см. правило шифрования в Таблице 1) можно добиться, например, путем увеличения веса добавляемой ошибки $\mathbf{e}$ при шифровании. Однако превышение веса $w(\mathbf{e})$ величины $t = \lfloor (d(N) - 1)/2 \rfloor$ может привести к тому, что при расшифровании на стороне получателя не все подблоки длины $n(N)$ вектора $\mathbf{z}P^{-1}W^{-1}_{(\mathcal{H},Y);\mathcal{G}}$ могут быть декодированы корректно с помощью алгоритма декодирования $\mathrm{Dec}_N$. Это связано с тем, что при умножении вектора $\mathbf{z}$ на матрицу $P^{-1}W^{-1}_{(\mathcal{H},Y);\mathcal{G}}$ в одном из таких подблоков может быть сгурппировано более $t$ ошибочных координат. С другой стороны, если в правиле шифрования криптосистемы InducedMcE($C$) выполняется неравенство $w(\mathbf{e}) \leq \lambda t$, то, как минимум, один из $\lambda$ подблоков длины $n(N)$ будет расшифрован корректно. Эта особенность позволяет построить на основе системы InducedMcE($C$) следующий протокол выработки общего секретного ключа.

Пусть $A$ и $B$ — пользователи, намеревающиеся выработать общий секретный ключ; $\mathbf{k}^A_{\mathrm{pub}} = (\widetilde{G}^A, \lambda t)$, $\mathbf{k}^A_{\mathrm{sec}} = (S^A, P^A)$, $\mathbf{k}^B_{\mathrm{pub}} = (\widetilde{G}^B, \lambda t)$, $\mathbf{k}^B_{\mathrm{sec}} = (S^B, P^B)$ — соответствующие открытые и секретные ключи пользователей $A$ и $B$. Пользователи независимо друг от друга генерируют случайные последовательности $\mathbf{s}^A (\in \mathbb{F}^{k(N)\lambda})$ и $\mathbf{s}^B (\in \mathbb{F}^{k(N)\lambda})$, шифруют их на ключах друг друга и обмениваются соответствующими шифрограммами. Каждый из пользователей расшифровывает соответствующий принятый вектор и сообщает другому участнику по открытому каналу номер кодового подблока, декодированного корректно. Даже если декодировано корректно более одного подблока, представляется целесообразным отправлять только номер одного подблока, чтобы защититься от нечестного участника, генерирующего вектора ошибок специального вида с целью получения информации о перестановочной матрице второго легитимного участника. Таким образом, пользователь $A$ отправляет пользователю $B$ номер $a$, а пользователь $B$ отправляет пользователю $A$ номер $b$, после чего строится общий ключ. Ниже приведен протокол выработки общего ключа.

**Протокол** Выработки общего секретного ключа $\mathbf{k}$

1: $A$, $B$ : Генерируют соответствующие пары ключей $(\mathbf{k}^A_{\text{pub}}, \mathbf{k}^A_{\text{sec}})$ и $(\mathbf{k}^B_{\text{pub}}, \mathbf{k}^B_{\text{sec}})$: $\mathbf{k}^A_{\text{pub}} = (\widetilde{G}^A, \lambda t)$, $\mathbf{k}^A_{\text{sec}} = (S^A, P^A)$, $\mathbf{k}^B_{\text{pub}} = (\widetilde{G}^B, \lambda t)$, $\mathbf{k}^B_{\text{sec}} = (S^B, P^B)$. Публикуют открытые ключи $\mathbf{k}^A_{\text{pub}}$ и $\mathbf{k}^B_{\text{pub}}$;
2: $A$, $B$ : Случайно и равновероятно генерируют последовательности $\mathbf{s}^A (\in \mathbb{F}^{k(N)\lambda})$ и $\mathbf{s}^B (\in \mathbb{F}^{k(N)\lambda})$;
3: $A \to B : \mathbf{z}^A = (\mathbf{z}^A_1, ..., \mathbf{z}^A_\lambda) = \mathbf{s}^A \widetilde{G}^B + \mathbf{e}^A = \mathbf{c}^A + \mathbf{e}^A$, $w(\mathbf{e}^A) \le \lambda t$;
4: $B \to A : \mathbf{z}^B = (\mathbf{z}^B_1, ..., \mathbf{z}^B_\lambda) = \mathbf{s}^B \widetilde{G}^A + \mathbf{e}^B = \mathbf{c}^B + \mathbf{e}^B$, $w(\mathbf{e}^B) \le \lambda t$;
5: $A : \hat{\mathbf{c}}^B := \text{Dec}_C(\mathbf{z}^B (P^A)^{-1}) \widetilde{G}^A = (\widehat{\mathbf{c}}^B_1, ..., \widehat{\mathbf{c}}^B_\lambda)$;
6: $A \to B : a (\in \{1; ...; \lambda\})$, где $\rho(\widehat{\mathbf{c}}^B_a, \mathbf{z}^B_a) \le t$;
7: $B : \hat{\mathbf{c}}^A := \text{Dec}_C(\mathbf{z}^A (P^B)^{-1}) \widetilde{G}^B = (\widehat{\mathbf{c}}^A_1, ..., \widehat{\mathbf{c}}^A_\lambda)$;
8: $B \to A : b (\in \{1; ...; \lambda\})$, где $\rho(\widehat{\mathbf{c}}^A_b, \mathbf{z}^A_b) \le t$;
9: $A$, $B$: $\mathbf{k} := \text{Dec}_N(\hat{\mathbf{c}}^A_b + \hat{\mathbf{c}}^B_a)$.

# Список литературы / References

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

[2] Niederreiter H., “Knapsack-Type Cryptosystem and Algebraic Coding Theory”, *Probl. Control and Inform. Theory*, **15** (1986), 94–34.

[3] Gabidulin E.M. et al., “Ideals Over a Non-Commutative Ring and Their Application in Cryptology.”, *Advances in Cryptology–EUROCRYPT’91 / Ed. by D.W. Davies. Lect. Notes in Comp. Sci. Springer-Verlag*, **547** (1991), 482–489.

[4] Сидельников В.М., “Открытое шифрование на основе двоичных кодов Рида–Маллера”, *Дискретная математика*, **6**:2 (1994), 3–20; [Sidel’nikov V.M., “Open coding based on Reed–Muller binary codes”, *Diskr. Mat.*, **6**:2 (1994), 3–20, (in Russian)].

[5] Сидельников В.М., Шестаков С.О., “О системе шифрования, основанной на обобщенных кодах Рида–Соломона”, *Дискретная математика*, **3**:3 (1992), 57–63; [Sidel’nikov V.M., Shestakov S.O., “O sisteme shifrovanija, osnovannoj na obobshhennyh kodah Rida–Solomona”, *Diskr. Mat.*, **3**:3 (1992), 57–63, (in Russian).]

[6] Деундяк В.М. и др., “Модификация криптоаналитического алгоритма Сидельникова–Шестакова для обобщенных кодов Рида–Соломона и ее программная реализация”, *Известия высших учебных заведений. Северо-Кавказский регион. Технические науки*, 2006, № 4, 15–20; [Deundyak V.M. et al., “Modifikatsiya kriptoanaliticheskogo algoritma Sidel’nikova–Shestakova dlya obobshchennykh kodov Rida–Solomona i ee programmnaya realizatsiya”, *Izvestiya vysshikh uchebnykh zavedeniy. Severo-Kavkazskiy region. Tekhnicheskie nauki*, 2006, № 4, 15–20, (in Russian).]

[7] Wieschebrin C., “Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes”, *Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25–28*, 2010, 61–72.

[8] Gibson J.K., “The Security of the Gabidulin Public Key Cryptosystem”, *Advances in Cryptology EUROCRYPT’ 96. Ed. By U.M. Maurer, LNCS 1070*, **1070** (1996), 212–223.

[9] Overbeck R., “Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes”, *Journal of Cryptology*, **21**:2 (2008), 280–301.

[10] Minder L., Shokrollahi A., “Cryptanalysis of the Sidelnikov cryptosystem”, *Lecture Notes in Computer Science*, **4515** (2007), 347–360.

[11] Чижов И.И., Бородин М.А., "Уязвимость криптосистемы Мак-Элиса, построенной на основе двоичных кодов Рида–Маллера", *Прикладаная дискрет. матем. Приложение*, 2013, № 6, 48–49; [Chizhov I.I., Borodin M.A., "Ujazvimost kriptosistemy Mak-Jelisa, postroennoj na osnove dvoichnyh kodov Rida–Mallera", *Prikladnaya diskr. mat. Prilozhenie*, 2013, № 6, 48–49, (in Russian).]

[12] Чижов И.И., Бородин М.А., "Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера", *Дискрет. матем.*, **26**:1 (2014), 10–20. [Chizhov I.I., Borodin M.A., "Jeffektivnaja ataka na kriptosistemu Mak-Jelisa, postroennuju na osnove kodov Rida–Mallera", *Diskr. Mat.*, **26**:1 (2014), 10–20, (in Russian).]

[13] Сидельников В.М., *Теория кодирования*, ФИЗМАТЛИТ, М., 2011; [Sidel'nikov V.M., *Teoriya kodirovaniya*, FIZMATLIT, M., 2011, (in Russian).]

[14] Циммерман К.-Х., *Методы теории модулярных представлений в алгебраической теории кодирования*, МЦНМО, М., 2011; [Tsimmerman K.-Kh., *Metody teorii modulyarnykh predstavleniy v algebraicheskoy teorii kodirovaniya*, MTsNMO, M., 2011, (in Russian).]

[15] Деундяк В.М., Косолапов Ю.В., "Алгоритмы для мажоритарного декодирования групповых кодов", *Моделирование и анализ информационных систем*, **22**:4 (2015), 464–482; [Deundyak V.M., Kosolapov Yu.V., "Algorithms for Majority Decoding of Group Codes", *Modeling and Analysis of Information Systems*, **22**:4 (2015), 464–482, (in Russian).]

[16] Massey J.L., *Threshold Decoding*, MIT Press, Cambridge, 1963.

[17] Curtis C.W., Reiner I., *Representation Theory of Finite Groups and Associative Algebras*, Intersclence Publishers, New York, 1962.

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

[19] Федоренко С.В., *Методы быстрого декодирования линейных кодов*, ГУАП, СПб, 2008; [Fedorenko S.V., *Metody bystrogo dekodirovaniya lineynykh kodov*, GUAP, SPb, 2008, (in Russian).]

[20] Berson T., "Failure of the McEliece public-key cryptosystem under message resend and related-message attack", *Proceedings of CRYPTO*, **1294** (1997), 213–220.

---

**Deundyak V. M., Kosolapov Y. V.**, "Cryptosystem Based on Induced Group Codes", *Modeling and Analysis of Information Systems*, **23**:2 (2016), 137–152.

**DOI:** 10.18255/1818-1015-2016-2-137-152

**Abstract.** The code $C$ on a group $\mathcal{G}$, induced by the code $N$ on a subgroup $\mathcal{H}$, has the property that for decoding the code $C$ one can use the decoder for the code $N$. Therefore, if $N$ has an efficient algorithm for decoding, we can build a class of induced codes with known decoding algorithms. This feature is used in this paper to build the code McEliece-type public key cryptosystems on induced group codes. For this cryptosystem we described operations of encryption and decryption, an analysis of the resistance to the attack on the private key is proposed, and also weak keys are highlighted, which is used while breaking McEliece-type cryptosystem on the induced code $C$ is reduced to breaking this cryptosystem on the code $N$. It is shown that a practically resistant cryptosystem on the induced code $C$ can be built on the code $N$ with small length. Based on the proposed cryptosystem a common protocol for open channel key generation is developed.

**Keywords:** group codes, induced group codes, the McEliece cryptosystem

**On the authors:** Deundyak Vladimir Mikhailovich, orcid.org/0000-0001-8258-2419, PhD,
FGNU NII "Specvuzavtomatika", 51 Gazetniy lane, Rostov-on-Don, 344002, Russia
South Federal University, 105/42 Bolshaya Sadovaya Str., Rostov-on-Don, 344006, Russia, e-mail: vl.deundyak@gmail.com,
Kosolapov Yury Vladimirovich, 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