УДК 517.9 DOI: 10.14529/mmp190308

АНАЛИЗ СТОЙКОСТИ НЕКОТОРЫХ КОДОВЫХ КРИПТОСИСТЕМ, ОСНОВАННЫЙ НА РАЗЛОЖЕНИИ КОДОВ В ПРЯМУЮ СУММУ

В.М. Деундяк[1,2]***, Ю.В. Косолапов***[1]
[1]Южный федеральный университет, г. Ростов-на-Дону, Российская Федерация
[2]Научно-исследовательский институт «Специализированные вычислительные устройства защиты и автоматика», г. Ростов-на-Дону, Российская Федерация

Строится полиномиальный алгоритм разложения произвольного линейного кода C в прямую сумму неразложимых подкодов с попарно непересекающимися носителями. В основе построенного алгоритма лежит нахождение базиса линейного кода, состоящего из минимальных кодовых векторов, то есть таких векторов, носители которых не содержатся в носителях других кодовых векторов этого линейного кода. Такой базис находится за полиномиальное от длины кода число операций. По найденному базису, используя сцепленность носителей минимальных кодовых векторов, за полиномиальное от длины кода число операций далее находятся базисные векторы неразложимых подкодов, в прямую сумму которых раскладывается исходный линейный код. На базе построенного алгоритма строится алгоритм структурной атаки на кодовую асимметричную криптосистему типа Мак-Элиса, основанную на коде C, который полиномиально зависит от сложности структурных атак на криптосистемы типа Мак-Элиса, основанные на подкодах, в прямую сумму которых раскладывается код C. Таким образом, показано, что использование прямой суммы кодов не позволяет существенно усилить стойкость криптосистемы типа Мак-Элиса к атакам на ключ.

Ключевые слова: прямая сумма кодов; криптосистема типа Мак-Элиса; атака на ключ.

Введение

В постквантовую эпоху одной из альтернатив современным криптосистемам рассматриваются кодовые криптосистемы типа Мак-Элиса [1]. Для практического применения используемые в таких криптосистемах коды должны быть трудно отличимыми от случайных кодов, но при этом эти коды должны иметь быстрый декодер. Первое свойство, как правило, необходимо для обеспечения высокой стойкости криптосистем к атакам на ключ, а второе – для обеспечения высокой скорости расшифрования данных легальными получателями. С точки зрения стойкости, наилучшими для использования являются случайные коды, однако сложность легального расшифрования в таких криптосистемах будет сравнима со сложностью взлома этой криптосистемы. С другой стороны, многие коды с быстрыми декодерами обладают алгебраической структурой, позволяющей провести эффективную атаку на ключ. Например, в настоящее время известны эффективные атаки на ключ для криптосистем типа Мак-Элиса на кодах Рида – Соломона и двоичных кода Рида – Маллера (см. [2–6]).

Одним из возможных подходов в построении новых кодов является использование конструкций на основе известных кодов. В [7] предложена криптосистема на основе индуцированного кода C, который в категории линейных пространств изоморфен l-кратной прямой сумме одного базового кода с быстрым алгоритмом декодирования. В [7] предположена высокая стойкость такой криптосистемы к структурным атакам, так как найденный авторами способ криптоанализа неполиномиально зависит от длины

базового кода. В [8] подтверждена высокая стойкость этой криптосистемы к атаке, основанной на применении алгоритма расщепления носителя индуцированного кода.

В настоящей статье рассматривается кодовая криптосистема типа Мак-Элиса на коде C, представляющем собой прямую сумму неразложимых кодов $\tilde{C}_1$, ..., $\tilde{C}_v$. Такая криптосистема является обобщением криптосистемы, предложенной в [7]. Для рассматриваемой криптосистемы строится алгоритм структурной атаки, отличный от алгоритмов, построенных в [7, 8]. В работе показано, что стойкость системы типа Мак-Элиса на коде C сравнима со стойкостью криптосистемы типа Мак-Элиса на коде $\tilde{C}_i$, где $\tilde{C}_i$ – такой код, что криптосистема на этом коде обладает наибольшей стойкостью среди всех криптосистем типа Мак-Элиса на кодах $\tilde{C}_1$, ..., $\tilde{C}_v$.

Статья имеет следующую структуру. В первом разделе рассматриваются необходимые свойства прямых сумм кодов. Алгоритмы структурных атак для кодовых криптосистем, основанных на прямой сумме неразложимых кодов, строятся в третьем разделе, а второй раздел посвящен построению вспомогательного эффективного алгоритма разложения произвольного кода в прямую сумму неразложимых кодов.

1. Прямая сумма кодов

Сначала приведем необходимые предварительные сведения. Пусть $\mathbb{F}_q$ – поле Галуа мощности q, $[n] = \{1, ..., n\}$, $\mathbb{F}_q^n$ – n-мерное линейное пространство над полем $\mathbb{F}_q$. Под тензорным произведением $(k \times n)$-матрицы $A = (a_{i,j})$ и произвольной матрицы B над полем $\mathbb{F}_q$ будем понимать, как обычно, матрицу вида:

$$A \otimes B = \begin{pmatrix} a_{1,1}B & ... & a_{1,n}B \\ a_{2,1}B & ... & a_{2,n}B \\ ... & ... & ... \\ a_{k,1}B & ... & a_{k,n}B \end{pmatrix}. \tag{1}$$

В пространстве $\mathbb{F}_q^n$ рассмотрим линейный $[n, k, d]_q$-код C размерности k, длины n, имеющий кодовое расстояние d [9]. Пусть G_C и H_C – порождающая и проверочная матрицы этого кода. Группу перестановочных матриц размера $(n \times n)$ обозначим MP_n, а симметрическую группу перестановок множества $[n]$ обозначим $\mathcal{S}_n$. Отметим, что произвольной перестановке $\sigma(\in \mathcal{S}_n)$ можно поставить в соответствие перестановочную $(n \times n)$-матрицу, которую будем обозначать P_σ. Код D длины n называется перестановочно–эквивалентным коду C, если существует такая перестановка $\sigma(\in \mathcal{S}_n)$, что $G_D = G_C P_\sigma$; при этом будем писать $D = \sigma(C)$. Пусть $\mathrm{PAut}(C)(\subseteq \mathrm{MP}_n)$ – группа перестановочных автоморфизмов $[n, k, d]_q$-кода C, то есть группа таких матриц, что для любой порождающей матрицы G_C и любой матрицы $P \in \mathrm{PAut}(C)$ матрица $G_C P$ также является порождающей для C.

Носителем вектора $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{F}_q^n$ назовем множество $\mathrm{supp}(\mathbf{x}) = \{i \in [n] : x_i \neq 0\}$, а носителем множества $A \subseteq \mathbb{F}_q^n$ будем называть множество номеров

$$\mathrm{SUPP}(A) = \cup_{\mathbf{a} \in A} \mathrm{supp}(\mathbf{a}).$$

Для множества $\tau \subseteq [n]$ рассмотрим проектор $\pi_\tau : \mathbb{F}_q^n \to \mathbb{F}_q^n$, который вектору $\mathbf{x} = (x_1, ..., x_n)(\in \mathbb{F}_q^n)$ ставит в соответствие вектор $\pi_\tau(\mathbf{x})$, i-ая координата которого имеет вид:

$$(\pi_\tau(\mathbf{x}))_i = \begin{cases} x_i, & \text{если } i \in \tau, \\ 0, & \text{иначе.} \end{cases}$$

Отметим, что $\mathrm{supp}(\pi_\tau(\mathbf{x})) \subseteq \tau$. Напомним, что $(k \times n)$-матрица G ранга k имеет систематический вид, если существует такое упорядоченное множество τ, $|\tau| = k$, что $\hat{\pi}_\tau(G) = I_k$, где $\hat{\pi}_\tau(G)$ – матрица, составленная из столбцов матрицы G с номерами, принадлежащими множеству τ.

Рассмотрим конструкцию прямой суммы кодов. Пусть $\tilde{C}_i$ – $[\tilde{n}_i, \tilde{k}_i, \tilde{d}_i]_q$-код с порождающей матрицей $G_{\tilde{C}_i}$, $|\mathrm{SUPP}(\tilde{C}_i)| = \tilde{n}_i > 0$, $i = 1, ..., v$. Рассмотрим код:

$$C = \tilde{C}_1 \oplus ... \oplus \tilde{C}_v = \{\mathbf{c} = (\mathbf{c}_1 \parallel ... \parallel \mathbf{c}_v) : \mathbf{c}_i \in \tilde{C}_i, i = 1, ..., v\}, \tag{2}$$

где $\mathbf{a} \parallel \mathbf{b}$ – конкатенация векторов $\mathbf{a}$ и $\mathbf{b}$. Код C будем называть внешней прямой суммой кодов $\tilde{C}_1$, ..., $\tilde{C}_v$. Очевидно, что C является $[n, k, d]_q$-кодом, причем $d = \min\{\tilde{d}_1, ..., \tilde{d}_v\}$, $n = \sum_{i=1}^{v} \tilde{n}_i$, $k = \sum_{i=1}^{v} \tilde{k}_i$, а порождающая матрица G_C кода C может быть представлена в виде:

$$G_C = \mathrm{diag}(G_{\tilde{C}_1}, ..., G_{\tilde{C}_v}) := \begin{pmatrix} G_{\tilde{C}_1} & & \\ & \ddots & \\ & & G_{\tilde{C}_v} \end{pmatrix}. \tag{3}$$

Пусть $\tau_1 = \{1, ..., \tilde{n}_1\}$, $\tau_2 = \{\tilde{n}_1 + 1, ..., \tilde{n}_1 + \tilde{n}_2\}$, ..., $\tau_v = \{\sum_{i=1}^{v-1} \tilde{n}_i + 1, ..., n\}$. Коду $\tilde{C}_i$ сопоставим подкод $C_i = \pi_{\tau_i}(C)$ кода C. Тогда

$$C = C_1 + ... + C_v, \;\; \mathrm{SUPP}(C_l) \cap \mathrm{SUPP}(C_j), \tag{4}$$

где $l \neq j$. В этом случае говорят, что C – прямая сумма подкодов C_i.

Рассмотрим простые свойства суммы кодов. Следующая лемма легко вытекает из определений.

Лемма 1. *Пусть $\tilde{C}_i$ – $[\tilde{n}_i, \tilde{k}_i, \tilde{d}_i]_q$-код, $|\mathrm{SUPP}(\tilde{C}_i)| = \tilde{n}_i$, $i = 1, ..., v$, C – $[n, k, d]_q$-код вида* (2) *представлен в виде* (4). *Тогда*

1) если $\sigma \in \mathcal{S}_n$ – перестановка, действующая на $[n]$, то

$$\sigma(C) = \sigma(C_1) + ... + \sigma(C_v); \tag{5}$$

2) код $C^\perp$, дуальный коду C, представим в виде: $C^\perp = C_1^\perp + ... + C_v^\perp$;

3) если

$$\Theta_1 = \{\mathrm{diag}(D_1, ..., D_v) : D_i \in \mathrm{PAut}(\tilde{C}_i)\},$$

то $\Theta_1 \subseteq \mathrm{PAut}(C)$.

Для $j = 1, 2$ рассмотрим $[n_j, k_j, d_j]_q$-код K_j с порождающей матрицей G_{K_j}. Код с порождающей матрицей $G_{K_1} \otimes G_{K_2}$ является тензорным произведением кодов K_1 и K_2, т.е. $[n_1 n_2, k_1 k_2, d_1 d_2]_q$-кодом $K_1 \otimes K_2$ [10]. Код C вида (2), где коды $\tilde{C}_j$ для всех j совпадают с $[\tilde{n}, \tilde{k}, \tilde{d}]_q$-кодом $\tilde{C}$, равен $[v\tilde{n}, v\tilde{k}, \tilde{d}]_q$-коду $\mathbb{F}_q^v \otimes \tilde{C}$. Несложно видеть, что имеет место представление кода $\mathbb{F}_q^v \otimes \tilde{C}$ в виде суммы изоморфных кодов (см. (4)):

$$\mathbb{F}_q^v \otimes \tilde{C} = C_1 + ... + C_v, \;\; \mathrm{SUPP}(C_i) = \tau_i = \{(i-1)\tilde{n} + 1, ..., i\tilde{n}\}. \tag{6}$$

Лемма 2. *Пусть $C = \mathbb{F}_q^v \otimes \tilde{C}$, где $\tilde{C}$ – $[\tilde{n}, \tilde{k}, \tilde{d}]_q$-код,*

$$\Theta_2 = \{(V \otimes I_{\tilde{n}})\mathrm{diag}(D_1, ..., D_v) : V \in \mathrm{MP}_v, D_i \in \mathrm{PAut}(\tilde{C})\}.$$

Тогда $\Theta_1 \subset \Theta_2 \subseteq \mathrm{PAut}(C)$.

Доказательство. Для доказательства достаточно показать, что матрицы вида $V \otimes I_{\tilde{n}}$ и $\mathrm{diag}(D_1, ..., D_v)$ по отдельности принадлежат $\mathrm{PAut}(\mathbb{F}_q^v \otimes \tilde{C})$. Отметим, что, по определению, $\Theta_1 \subset \Theta_2$, а принадлежность матрицы $\mathrm{diag}(D_1, ..., D_v)$ группе $\mathrm{PAut}(\mathbb{F}_q^v \otimes \tilde{C})$ следует из утверждения 3) леммы 1. Покажем, что $V \otimes I_{\tilde{n}} \in \mathrm{PAut}(\mathbb{F}_q^v \otimes \tilde{C})$. Так как порождающая матрица G_C может быть представлена в виде $I_v \otimes G_{\tilde{C}}$, то, используя свойства тензорного произведения, получим:

$$G_C(V \otimes I_{\tilde{n}}) = (I_v \otimes G_{\tilde{C}})(V \otimes I_{\tilde{n}}) = V \otimes G_{\tilde{C}} = (V \otimes I_{\tilde{k}})(I_v \otimes G_{\tilde{C}}) = (V \otimes I_{\tilde{k}})G_C.$$

Равенство $G_C(V \otimes I_{\tilde{n}}) = (V \otimes I_{\tilde{k}})G_C$ означает, что матрица $G_C(V \otimes I_{\tilde{n}})$ является порождающей матрицей кода C, следовательно, $V \otimes I_{\tilde{n}} \in \mathrm{PAut}(C)$.

□

2. Разложение кода в прямую сумму подкодов

$[n, k, d]_q$-код C будем называть разложимым, если он может быть представлен в виде (4), где $v \geq 2$. Будем говорить, что код C является разложимым длины разложения v, если он может быть представлен в виде суммы (4), где каждый из подкодов C_i не является разложимым. Заметим, что в этом случае представление (4) по существу единственно с точностью до перестановки подкодов C_i в сумме. Неразложимый код C для удобства можно называть разложимым кодом длины разложения один.

В работе [12] используется введенное в [11] понятие минимальных кодовых векторов для изучения группы автоморфизмов линейных кодов над простым полем. Напомним, что кодовый вектор $\mathbf{c}(\in C)$ называется *минимальным* вектором, если в C не существует вектора $\mathbf{c}'$, линейно независимого с вектором $\mathbf{c}$, такого, что $\mathrm{supp}(\mathbf{c}') \subset \mathrm{supp}(\mathbf{c})$ [11]. В [12, с. 215], на основе использования свойства носителей базисных минимальных кодовых векторов показана возможность представления кодов в виде прямой суммы кодов. Ниже в этом разделе решается задача построения эффективного алгоритма разложения произвольного линейного $[n, k, d]_q$-кода C в прямую сумму вида (4), в которой все слагаемые C_i являются неразложимыми подкодами кода C.

Два вектора будем называть сцепленными, если их носители пересекаются по непустому множеству. Рассмотрим множество $M(C)$, где C – произвольный линейный $[n, k, d]_q$-код, состоящее из всех минимальных векторов этого кода. Множество минимальных векторов $\{\mathbf{c}_1, ..., \mathbf{c}_t\}(\subseteq M(C))$, назовем *связным*, если для любой пары векторов найдется такая последовательность векторов, что она начинается с одного вектора, заканчивается другим вектором пары, и при этом подряд идущие векторы последовательности сцеплены. Отметим, что два связных множества пересекаются, то их объединение связно. Максимальное связное множество назовем компонентой связности. Множество всех компонент связности кода C обозначим $Z(C)$. Отметим, что аналогичные понятия содержатся в [12].

Известно, что строки произвольной порождающей матрицы кода C в систематическом виде являются минимальными кодовыми векторами, образующими базис [13]. Такой базис будем обозначать $B_M(C)$. Так как любая порождающая матрица кода может быть приведена к систематическому виду с помощью алгоритма Гаусса, то сложность нахождения базиса $B_M(C)$ – $\mathcal{O}(n^3)$. Алгоритм нахождения базиса $B_M(C)$ по произвольной порождающей матрице кода C обозначим FindMinBasis.

Лемма 3. *Пусть C – разложимый код вида* (4)*, где C_j – неразложимые подкоды. Тогда*

1) $M(C) = \cup_{i=1}^{v} M(C_i)$*;*
2) $Z(C) = \{M(C_1), ..., M(C_v)\}$*;*
3) $B_M(C) = \cup_{i=1}^{v} B_M(C_i)$*.*

Доказательство. Первые два утверждения непосредственно вытекают из условий леммы и определений. Третье утверждение вытекает из первых двух.

□

Построим алгоритм Decomposition (см. алгоритм 1), который для произвольного линейного кода C строит такие наборы векторов B_1, ..., B_v из $M(C)$, что для кода C имеет место разложение (4), где коды C_i неразложимы и $B_i = B_M(C_i)$.

Исходные параметры: G_C – порождающая матрица $[n, k, d]_q$-кода C
Результат: $B_1, ..., B_v$– базисы кодов C_i, составленные из минимальных кодовых векторов
$B_M(C) = \{\mathbf{g}'_1, ..., \mathbf{g}'_k\} = \text{FindMinBasis}(G_C)$
$V = [k]$, $i = 1$
до тех пор, пока $V \neq \varnothing$ **выполнять**
  Для произвольного $j \in V$: $V_i = \{j\}$, $W_i = \text{supp}(\mathbf{g}'_j)$,
  $changed = true$
  до тех пор, пока $changed = true$ **выполнять**
    $changed = false$
    для каждого $l \in V \setminus \{j\}$ **выполнять**
      если $\text{supp}(\mathbf{g}'_l) \cap W_i \neq \varnothing$ **тогда**
        $changed = true$
        $V_i = V_i \cup \{l\}$
        $W_i = W_i \cup \text{supp}(\mathbf{g}'_l)$
      конец условия
    конец цикла
  конец цикла
  $B_i = \{\mathbf{g}'_j : j \in V_i\}$, $V = V \setminus V_i$, $i = i + 1$,
конец цикла
возвратить $B_1, ..., B_v$

Алгоритм 1. Decomposition

Теорема 1. *Пусть C – разложимый код длины разложения v. Тогда по произвольной порождающей матрице G_C этого кода алгоритм* Decomposition *находит v базисов неразложимых подкодов C_1,..., C_v, носители которых попарно не пересекаются; причем найденные базисы состоят из минимальных кодовых векторов, а сложность алгоритма – $\mathcal{O}(n^3 + k^2 n)$.*

Доказательство. На первом шаге алгоритма Decomposition строится базис $B_M(C)$ из минимальных кодовых векторов. Сложность этого шага – $O(n^3)$. В оставшейся части алгоритма из найденных минимальных базисных кодовых векторов строятся связные множества B_i, $i = 1, ..., v$. Так как носители множеств B_i не пересекаются и построенный на первом шаге базис $B_M(C)$ состоит из минимальных кодовых векторов, то

из п.3 леммы 3 следует, что B_i – базисы $B_M(C_i)$ кодов C_i, состоящие из минимальных кодовых векторов. Сложность построения множеств B_i – $O(k^2n)$. Таким образом, $\mathcal{O}(n^3 + k^2n)$ – сложность алгоритма Decomposition.

□

Рассмотрим примеры неразложимых кодов.

Пример 1. $[n, k, d]_q$–код C с максимальным достижимым расстоянием (МДР-код) является неразложимым кодом. Сначала рассмотрим случай, когда $k \leq \lfloor n/2 \rfloor$. Так как C – МДР-код, то $d = n - k + 1 \geq \lceil n/2 \rceil + 1$. Отсюда получаем, что любые два кодовых вектора кода C сцеплены, поэтому C неразложим. Рассмотрим случай $k > \lfloor n/2 \rfloor$. Так как $C^\perp$ – также МДР-код размерности $n - k$ и для него выполняется условие $n - k \leq \lfloor n/2 \rfloor$, то $C^\perp$ – неразложимый код. Из второго утверждения леммы 1 следует, что код C – неразложимый. К классу МДР-кодов относятся такие коды, как коды Рида – Соломона [9], некоторые коды в ранговой метрике [14].

Пример 2. Пусть $\mathrm{RM}(r, m)$ – двоичный код Рида – Маллера порядка r и длины 2^m [9]. Коды $\mathrm{RM}(1, m)$ и $\mathrm{RM}(m-r-1, m)$ являются неразложимыми. Рассмотрим сначала код $\mathrm{RM}(1, m)$. Это $[2^m, m+1, 2^{m-1}]_q$-код. Отсюда следует, что этот код не может быть разложимым, в противном случаем имелись бы подкоды, с минимальным кодовым расстоянием менее 2^{m-1}. Так как для $\mathrm{RM}(1, m)$ дуальным кодом является код порядка $m - r - 1$, то из второго утверждения леммы 1 вытекает, что код $\mathrm{RM}(m - r - 1, m)$ также является неразложимым кодом.

На основе известных неразложимых кодов могут быть построены некоторые другие неразложимые коды. Как следует из [15], если C – неразложимый $[n, k, d]_q$-код с порождающей $(k \times n)$-матрицей G_C, G_0 –произвольная $(k \times n_0)$-матрица, то $[n + n_0, k, \hat{d}]_q$-код $\mathcal{K}$ с порождающей матрицей $G_\mathcal{K} = (G_C \parallel G_0)$ является неразложимым кодом, причем $\hat{d} \geq d$. Отметим, что задача подсчета числа неразложимых $[n, k]_q$-кодов для заданных n, k и q решена в [16].

3. Структурные атаки на кодовые криптосистемы

3.1. Кодовые криптосистемы

В [1] Р. Мак-Элисом впервые была предложена асимметричная кодовая криптосистема на линейном коде Гоппы. Стойкость таких криптосистем основана на том, что матрица публичного ключа неотличима за полиномиальное время от порождающей матрицы случайного кода, задача декодирования которого, как известно из теории кодирования, относится к NP-полным задачам [9]. В этом разделе приводится описание криптосистемы типа Мак-Элиса $\mathrm{McE}(C)$ на произвольном коде C.

Рассмотрим криптосистему $\mathrm{McE}(C)$ на $[N, K, D]_q$-коде C: секретным ключом является пара (S, P), где S – невырожденная $(K \times K)$-матрица, P – перестановочная $(N \times N)$-матрица из MP_N. Публичным ключом является пара $(\widetilde{G}, t = \lfloor (D-1)/2 \rfloor)$, где матрица $\widetilde{G}$ имеет вид:

$$B = SG_CP. \tag{7}$$

Шифрование вектора $\mathbf{m}(\in \mathbb{F}_q^K)$ выполняется по правилу: $\mathbf{m}B + \mathbf{e} = \mathbf{c}$, где $\mathrm{wt}(\mathbf{e}) \leq t$. Для расшифрования $\mathbf{c}$ достаточно декодировать вектор $\mathbf{c}P^{-1}$ в вектор $\mathbf{m}S$, из которого с помощью умножения на матрицу S^{-1} найти $\mathbf{m}$.

Среди атак на кодовые криптосистемы выделяются атаки на шифрограмму и структурные атаки – атаки на открытый ключ. Целью первых может являться, например, нахождение зашифрованного сообщения по известной шифрограмме или набору шифрограмм, или модификация шифрограммы без обнаружения приемной стороной факта модификации. Атаки на открытый ключ, также называемые структурными атаками, направлены на получение информации о секретном ключе по известному открытому ключу. В этой работе нас интересуют структурные атаки. Для криптосистем типа Мак-Элиса целью структурных атак является нахождение по матрице B *подходящего секретного ключа* (S', P') такого, что

$$S'G_CP' = B.$$

Отметим, что в общем случае $S \neq S'$ и/или $P \neq P'$, однако известно (см., например, [9]), что $PP'^{-1} \in \mathrm{PAut}(C)$, и этот ключ может быть использован при расшифровании по приведенному выше правилу.

3.2. Алгоритм атаки на систему $\mathrm{McE}(\mathbb{F}_q^v \otimes \tilde{C})$

Пусть $\tilde{C}$ – неразложимый $[\tilde{n}, \tilde{k}, \tilde{d}]_q$-код, v – натуральное число. Рассмотрим представление кода $\mathbb{F}_q^v \otimes \tilde{C}$ в виде суммы изоморфных кодов C_i (см. (6)).

Теорема 2. *Пусть* $B = S(I_v \otimes G_{\tilde{C}})P$ *– матрица публичного ключа криптосистемы* $\mathrm{McE}(\mathbb{F}_q^l \otimes \tilde{C})$*, где* S *– невырожденная* $(v\tilde{k} \times v\tilde{k})$*-матрица,* $P \in \mathrm{MP}_{v\tilde{n}}$*,* Attack *– алгоритм нахождения подходящего секретного ключа для системы* $\mathrm{McE}(\tilde{C})$*,* $Q(\tilde{n})$ *– сложность этого алгоритма. Тогда существует алгоритм нахождения подходящего секретного ключа для системы* $\mathrm{McE}(\mathbb{F}_q^v \otimes \tilde{C})$ *со сложностью* $\mathcal{O}(2v^3\tilde{n}^3 + v^3\tilde{k}^2\tilde{n} + v\tilde{n} + vQ(\tilde{n}))$.

Доказательство. Доказательство основано на построении алгоритма нахождения подходящего секретного ключа.

Из теоремы 1 вытекает, что с помощью алгоритма Decomposition можно найти такие непересекающиеся подмножества $\psi_i (\subseteq [v\tilde{n}])$, $|\psi_i| = \tilde{n}$, что для каждого $i = 1, ..., v$ линейная оболочка строк матрицы $\hat{\pi}_{\psi_i}(B)$ изоморфна коду $\tilde{C}$. Без нарушения общности будем полагать, что элементы множеств $\psi_i = \{p_1^i, ..., p_{\tilde{n}}^i\}$ упорядочены: $p_m^i < p_j^i$ для любых $m < j$. Найдем такую перестановку $\sigma \in \mathcal{S}_{v\tilde{n}}$, что $\sigma(i) = p_{i-(s-1)\tilde{n}}^s$ для $i = (s-1)\tilde{n} + 1, ..., s\tilde{n}$, $s = 1, ..., v$. Пусть P_σ – перестановочная $(v\tilde{n} \times v\tilde{n})$-матрица, соответствующая перестановке σ. Тогда матрица PP_σ^{-1} имеет вид:

$$PP_\sigma^{-1} = (V \otimes I_{\tilde{n}})\mathrm{diag}(W_1, ..., W_v),$$

где $V \in \mathrm{MP}_v$, $W_i \in \mathrm{MP}_{\tilde{n}}$. Из леммы 2 следует, что матрица $V \otimes I_{\tilde{n}}$ принадлежит группе автоморфизмов кода $\mathbb{F}_q^v \otimes \tilde{C}$. Поэтому матрица BP_σ^{-1} может быть представлена в виде:

$$BP_\sigma^{-1} = \hat{S}(I_v \otimes G_{\tilde{C}})\mathrm{diag}(W_1, ..., W_v).$$

Пусть $\tau_i = \{(i-1)\tilde{n} + 1, ..., i\tilde{n}\}$, $i = 1, ..., v$. Заметим, что для всех $i \in [v]$:

$$\hat{\pi}_{\tau_i}(BP_\sigma^{-1}) = \hat{\pi}_{\tau_i}(\hat{S}(I_v \otimes G_{\tilde{C}}))W_i = \hat{\pi}_{\omega_i}(\hat{S})G_CW_i,$$

где $\omega_i = \{(i-1)k+1, ..., ik\}$, $i = 1, ..., v$. Так как матрица $\hat{S}$ квадратная и полного ранга kv, то $\mathrm{rank}(\hat{\pi}_{\omega_i}(\hat{S})) = k$. Поэтому по матрице $\hat{\pi}_{\tau_i}(BP_\sigma^{-1})$ за полиномиальное время может быть построена $(k \times \tilde{n})$-матрица β_i ранга k, которая имеет представление: $\beta_i = \hat{S}_i G_{\tilde{C}} W_i$, где $\hat{S}_i$ – $(k \times k)$-матрица ранга k. Таким образом, по матрице B с полиномиальной по $\tilde{n}$ сложностью могут быть найдены v матриц, каждая из которых представляет матрицу публичного ключа криптосистемы $\mathrm{McE}(\tilde{C})$.

Применяя алгоритм Attack к матрицам β_i, найдем соответствующие подходящие ключи $(\hat{S}'_i, W'_i)$. При этом $W_i W_i'^{-1} \in \mathrm{PAut}(\tilde{C})$. Из леммы 2 получаем, что матрица

$$\mathrm{diag}(W_1 W_1'^{-1}, ..., W_l W_v'^{-1}) = P P_\sigma^{-1} \mathrm{diag}(W_1'^{-1}, ..., W_v'^{-1})$$

принадлежит группе автоморфизмов кода $\mathbb{F}_q^v \otimes \tilde{C}$, поэтому из уравнения

$$S' G_C = B P_\sigma^{-1} \mathrm{diag}(W_1'^{-1}, ..., W_v'^{-1}), \tag{8}$$

где $G_C = I_v \otimes G_{\tilde{C}}$, с полиномиальной по n сложностью может быть найдена матрица S'. Отсюда получаем, что $(S', \mathrm{diag}(W'_1, ..., W'_v)P_\sigma)$ – подходящий секретный ключ для системы $\mathrm{McE}(\mathbb{F}_q^v \otimes \tilde{C})$ с матрицей публичного ключа B.

В алгоритме Crack1 (см. алгоритм 2) приведены шаги нахождения подходящего секретного ключа. Из теоремы 1 вытекает, что сложность первого шага этого алгоритма – $\mathcal{O}(v^3\tilde{n}^3 + v^3\tilde{k}^2\tilde{n})$. Сложность второго шага – $\mathcal{O}(v\tilde{n})$. Третий шаг имеет сложность $\mathcal{O}(vQ(\tilde{n}))$, а сложность четвертого и пятого шагов – $\mathcal{O}(v^3\tilde{n}^3)$. Отсюда получаем сложность алгоритма Crack1.

□

Исходные параметры: B, Attack
Результат: (S', P') – подходящий секретный ключ
1. $(B_1, ..., B_v) = \mathrm{Decomposition}(B)$
2. $(\mathrm{SUPP}(B_1), ..., \mathrm{SUPP}(B_v)) \to P_\sigma$
3. $W'_i = \mathrm{Attack}(\hat{\pi}_{\tau_i}(BP_\sigma^{-1}))$, $\tau_i = \{(i-1)\tilde{n}+1, ..., i\tilde{n}\}$, $i = 1, ..., v$
4. Из уравнения (8) найти S'
5. $P' = \mathrm{diag}(W'_1, ..., W'_v)P_\sigma$
возвратить (S', P')

Алгоритм 2. Crack1

3.3. Алгоритм атаки на систему $\mathrm{McE}(\tilde{C}_1 \oplus ... \oplus \tilde{C}_v)$

Пусть $\tilde{C}_i$ – неразложимый $[n_i, k_i, d_i]_q$-код над полем $\mathbb{F}_q$, $i = 1, ..., v$, $\tilde{C}_1 \oplus ... \oplus \tilde{C}_v$ – код с порождающей матрицей вида (3), $\mathrm{McE}(\tilde{C}_1 \oplus ... \oplus \tilde{C}_v)$ – криптосистема типа Мак-Элиса на основе этого кода, Attack_i – алгоритм нахождения подходящего секретного ключа для криптосистемы $\mathrm{McE}(\tilde{C}_i)$, $Q(n_i)$ – сложность этого алгоритма, $i = 1, ..., v$,

$$\mathcal{A} = \{\mathrm{Attack}_i\}_{i=1}^v. \tag{9}$$

Пусть $\mathcal{K}(\tilde{C}_i)$ – множество всех матриц публичных ключей криптосистемы $\mathrm{McE}(\tilde{C}_i)$. Если коды C_i и C_j имеют одинаковую размерность и длину, но не являются комбинаторно-эквивалентными кодами, то $\mathcal{K}(\tilde{C}_i) \cap \mathcal{K}(\tilde{C}_j) = \varnothing$. Будем предполагать, что если на вход алгоритма Attack_i подается $(k_i \times n_i)$-матрица $A(\notin \mathcal{K}(\tilde{C}_i))$, то этот алгоритм завершает свою работу с сообщением об ошибке $\perp$ за полиномиальное время.

Теорема 3. *Пусть* $B = S \cdot \mathrm{diag}(G_{\tilde{C}_1}, ..., G_{\tilde{C}_v}) \cdot P$ *– матрица публичного ключа криптосистемы* $\mathrm{McE}(\tilde{C}_1 \oplus ... \oplus \tilde{C}_v)$*, где* $\tilde{C}_i$ *– неразложимый* $[n_i, k_i, d_i]_q$*-код,* $i = 1, ..., v$*,* $k = \sum_{i=1}^{v} \tilde{k}_i$*,* $n = \sum_{i=1}^{v} \tilde{n}_i$*,* S *– невырожденная* $(k \times k)$*-матрица,* $P \in \mathrm{MP}_n$*,* $\mathcal{A}$ *– набор вида* (9)*,* $Q = \max_{i \in [v]}\{Q(n_i)\}$*. Тогда существует алгоритм нахождения подходящего секретного ключа для системы* $\mathrm{McE}(\tilde{C}_1 \oplus ... \oplus \tilde{C}_v)$ *со сложностью* $\mathcal{O}(2n^3 + k^2 n + n + (v+1)vQ/2)$*.*

Доказательство. Для удобства код с порождающей матрицей B обозначим $\mathcal{B}$. Сначала рассмотрим случай, когда $(n_i, k_i) \neq (n_j, k_j)$ для всех $i \neq j$. В этом случае для нахождения подходящего секретного ключа можно воспользоваться модификацией алгоритма Crack1. Модификация заключается в изменении шагов 2 и 3. В частности, так как по предположению, коды $\tilde{C}_i$ попарно отличаются параметрами, то по набору базисов, полученных на первом шаге, несложно построить такую перестановочную матрицу P_σ, что

$$\sigma^{-1}(\mathcal{B}) = \tilde{\mathcal{B}}_1 \oplus ... \oplus \tilde{\mathcal{B}}_v, \tilde{\mathcal{B}}_i \cong \tilde{C}_i.$$

Модификация шага 3 заключается, с одной стороны, в том, $\tau_i = \mathrm{SUPP}(C_i)$, а с другой стороны, в том, что к матрице $\hat{\pi}_{\tau_i}(BP_\sigma^{-1})$ применяется алгоритм Attack_i.

Теперь рассмотрим другой частный случай, когда параметры всех кодов одинаковые: $(n_i, k_i) = (\tilde{n}, \tilde{k})$ для всех $i = 1, ..., v$. После применения первых трех шагов алгоритма Crack1, будет найдена такая перестановка σ, что $\sigma^{-1}(\mathcal{B}) = \tilde{\mathcal{B}}_1 \oplus ... \oplus \tilde{\mathcal{B}}_v$. Так как параметры кодов одинаковые, то для определения, какому коду из набора $\tilde{C}_1, ..., \tilde{C}_v$ изоморфен каждый код $\tilde{\mathcal{B}}_i$, необходимо выполнить перебор по алгоритмам из набора (9). Шаги нахождения подходящего секретного ключа в этом случае приведены в алгоритме Crack2 (см. алгоритм 3).

Исходные параметры: $B, (\mathrm{Attack}_1, ..., \mathrm{Attack}_v)$
Результат: (S', P') – подходящий секретный ключ
1. $(B_1, ..., B_v) = \mathrm{Decomposition}(B)$
2. $(\mathrm{SUPP}(B_1), ..., \mathrm{SUPP}(B_v)) \to P_\sigma$
3. $A = [v]$, $\mathbf{g} = (g_1, ..., g_v) \in [v]^v$
4. **для каждого** $i \in [v]$ **выполнять**
   для каждого $a \in A$ **выполнять**
   если $\mathrm{Attack}_a(\hat{\pi}_{\tau_i}(BP_\sigma^{-1})) = W_i' \neq \perp$ **тогда**
   $g_i = a$
   $A = A \setminus \{a\}$
   выйти из внутреннего цикла
   конец условия
   конец цикла
конец цикла
5. По вектору $\mathbf{g}$ найти перестановку γ такую, что $\gamma(i) = g_i$
6. Из уравнения $S'G_C = BP_\sigma^{-1}(P_\gamma^{-1} \otimes I_{\tilde{n}})\mathrm{diag}({W_{\gamma^{-1}(1)}^{-1}}', ..., {W_{\gamma^{-1}(v)}^{-1}}')$ найти S'
7. $P' = \mathrm{diag}(W'_{\gamma^{-1}(1)}, ..., W'_{\gamma^{-1}(v)})(P_\gamma \otimes I_{\tilde{n}})P_\sigma$
возвратить (S', P')

Алгоритм 3. Crack2

Особенность алгоритма Crack2 в отличие от алгоритма Crack1 состоит в том, что необходимо выполнять перебор по алгоритмам взлома из набора (9). В худшем случае

на шаге 4 алгоритма Crack2 выполняется обращение $(v+1)v/2$ раз к алгоритмам из этого набора. Поэтому, в силу того, что $\mathcal{O}(2v^3\tilde{n}^3 + v^3\tilde{k}^2\tilde{n} + v\tilde{n} + vQ(\tilde{n}))$ – сложность алгоритма Crack1, отсюда легко вытекает, что алгоритма Crack2 имеет сложность $\mathcal{O}(2n^3 + k^2n + n + (v+1)vQ/2)$.

□

Отметим, что алгоритм Crack2 является обобщением алгоритма Crack1 и может быть применен для нахождения подходящего секретного ключа для $\mathrm{McE}(\mathbb{F}_q^v \otimes \tilde{C})$, если положить $\mathrm{Attack}_i = \mathrm{Attack}$ для всех $i = 1, ..., v$.

Заключение

Попытки усилить стойкость криптосистемы типа Мак-Элиса предпринимаются, например, за счет использования новых кодов в классическом протоколе криптосистемы и/или путем модификации самого протокола криптосистемы (см., например, работы [7, 13–20]). В связи с этим актуальна задача анализа стойкости полученных модификаций.

С одной стороны, результаты настоящей работы показывают, что структурный криптоанализ криптосистемы типа Мак-Элиса $\mathrm{McE}(C)$, построенной на основе $[n, k, d]$-кода $C = \tilde{C}_1 \oplus ... \oplus \tilde{C}_v$, сводится к структурному анализу стойкости криптосистем $\mathrm{McE}(\tilde{C}_1)$, ..., $\mathrm{McE}(\tilde{C}_v)$. С другой стороны, $d = \min\{\tilde{d}_1, ..., \tilde{d}_v\}$, где $\tilde{d}_i$ – минимальное кодовое расстояние кода $\tilde{C}_i$, и $k = \sum_{i=1}^{v} \tilde{k}_i$. Поэтому стойкость системы $\mathrm{McE}(C)$ к атакам *на шифрограмму* методом декодирования по информационным совокупностям, как следует, например, из результатов работы [21], не превышает стойкости к соответствующим атакам для криптосистемы $\mathrm{McE}(\tilde{C}_{i'})$, где $\tilde{d}_{i'} = d$. Более того, используя алгоритм Decomposition (см. алгоритм 1), имеется возможность усилить атаку на шифрограмму, так как этот алгоритм позволяет определить носители подкодов. В этом случае алгоритм декодирования по информационным совокупностям может применяться не к коду с порождающей матрицей B, а к v подкодам с базисами B_1, ..., B_v. Таким образом, использование прямой суммы кодов не усиливает криптосистему типа Мак-Элиса ни к атакам на ключ, ни к атакам на шифрограмму. Отметим, что аналогичный вывод получен в [13] для модификации протокола Мак-Элиса, в которой используется кодовая конструкция типа конкатенации кодов.

Литература

1. McEliece, R.J. A Public-Key Cryptosystem Based on Algebraic Coding Theory / R.J. McEliece // DSN Progress Report. – 1978. – P. 42–44.

2. Sidel'nikov, V.M. On an Encoding System Constructed on the Basis of Generalized Reed – Solomon Codes / V.M. Sidel'nikov, S.O. Shestakov // Discrete Mathematics and Applications. – 1992. – V. 2, № 4. – P. 439–444.

3. Деундяк, В.М. Модификация криптоаналитического алгоритма Сидельникова – Шестакова для обобщенных кодов Рида – Соломона и ее программная реализация / В.М. Деундяк, М.А. Дружинина, Ю.В. Косолапов // Известия высших учебных заведений. Северо-Кавказский регион. Технические науки. – 2006. – № 4. – С. 15–19.

4. Wieschebrink, C. Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes / C. Wieschebrink // Proceedings of Third International Workshop. – Berlin, 2010. – P. 61–72.

5. Minder, L. Cryptanalysis of the Sidelnikov cryptosystem / L. Minder, A. Shokrollahi // Advances in Cryptology – EUROCRYPT 2007, Lecture Notes Computer Science. – 2007. – № 4515. – P. 347–360.
6. Бородин, М.А. Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида – Маллера / М.А. Бородин, И.В. Чижов // Дискретная математика. – 2014. – Т. 26, № 1. – С. 10–20.
7. Деундяк, В.М. Криптосистема на индуцированных групповых кодах / В.М. Деундяк, Ю.В. Косолапов // Моделирование и анализ информационных систем. – 2016. – Т. 23, № 2. – P. 137–152.
8. Косолапов, Ю.В. Об алгоритме расщепления носителя для индуцированных кодов / Ю.В. Косолапов, А.Н. Шигаев // Моделирование и анализ информационных систем. – 2018. – Т. 25, № 3. – P. 276–290.
9. Сидельников, В.М. Теория кодирования / В.М. Сидельников. – М.: Физматлит, 2008.
10. Morelos-Zaragoza, R.H. The Art of Error Correcting Coding / R.H. Morelos-Zaragoza. – Chichester, West Sussex: John Wiley & Sons, 2006.
11. Massey, J.L. Minimal Codewords and Secret Sharing / J.L. Massey // Proceeding of 6th Joint Swedish-Russian Workshop on Information Theory. – 1993. – P. 276–279.
12. Августинович, С.В. Об автоморфизмах линейных кодов над простым полем / С.В. Августинович, Е.В. Горкунов // Сибирские электронные математические известия. – 2017. – № 14. – С. 210–217.
13. Sendrier, N. On the Concatenated Structure of a Linear Code / N. Sendrier // Applicable Algebra in Engineering, Communication and Computing. – 1998. – V. 9, № 3. – P. 221–242.
14. Berger, T.P. Construction of New MDS Codes from Gabidulin Codes / T.P. Berger, A.V. Ourivski // Proceeding of ACCT'9. – 2004. – С. 40–47.
15. Assmus, E.F. The Category of Linear Codes / E.F. Assmus // IEEE Transaction on Information Theory. – 1998. – V. 44, № 2. – P. 612–629.
16. Fripertinger, H. Isometry Classes of Indecomposable Linear Codess / H. Fripertinger, A. Kerber // Lecture Notes in Computer Science. – 1995. – V. 948. – P. 194–204.
17. Сидельников, В.М. Открытое шифрование на основе двоичных кодов Рида – Маллера / В.М. Сидельников // Дискретная математика. – 1994. – Т. 6, № 2. – С. 3–20.
18. Deundyak, V.M. On the Berger – Loidreau Cryptosystem on the Tensor Product of Codes / V.M. Deundyak, Yu.V. Kosolapov // Journal of Computational and Engineering Mathematics. – 2018. – V. 5, № 2. – P. 16–33.
19. Красавин, А.А. Использование модифицированной $(u|u+v)$-конструкции в криптосистеме McEliece / А.А. Красавин // Труды МФТИ. – 2018. – Т. 10, № 2. – С. 189–191.
20. Kabatiansky, G. A New Code-Based Cryptosystem via Pseudorepetition of Codes / G. Kabatiansky, C. Tavernier // Proceedings of ACCT XVI. – 2018. – P. 189–191.
21. Деундяк, В.М. Использование тензорного произведения кодов Рида – Маллера в асимметричной криптосистеме типа Мак-Элиса и анализ ее стойкости к атакам на шифрограмму / В.М. Деундяк, Ю.В. Косолапов // Вычислительные технологии. – 2017. – Т. 22, № 4. – С. 43–60.

Владимир Михайлович Деундяк, кандидат физико-математических наук, доцент, кафедра «Алгебра и дискретная математика», Южный федеральный университет (г. Ростов-на-Дону, Российская Федерация); старший научный сотрудник, ФГАНУ НИИ «Спецвузавтоматика» (г. Ростов-на-Дону, Российская Федерация), vl.deundyak@gmail.com.

Юрий Владимирович Косолапов, кандидат технических наук, кафедра «Алгебра и дискретная математика», Южный федеральный университет (г. Ростов-на-Дону, Российская Федерация), itaim@mail.ru.

Поступила в редакцию 17 января 2019 г.

MSC 68P30, 94A60 **DOI: 10.14529/mmp190308**

THE USE OF THE DIRECT SUM DECOMPOSITION ALGORITHM FOR ANALYZING THE STRENGTH OF SOME McELIECE TYPE CRYPTOSYSTEMS

***V.M. Deundyak*[1,2], *Yu.V. Kosolapov*[1]**
[1]Southern Federal University, Rostov-on-Don, Russian Federation
[2]Research Institute "Specialized Computing Protection Devices and Automation", Rostov-on-Don, Russian Federation
E-mails: vl.deundyak@gmail.com, vl.deundyak@gmail.com

We construct a polynomial algorithm for decomposing an arbitrary linear code C into a direct sum of indecomposable subcodes with pairwise disjoint supports. The main idea of the constructed algorithm is to find the basis of a linear code consisting of minimal code vectors, that is, such vectors whose supports are not contained in the supports of other code vectors of this linear code. Such a basis is found in the polynomial number of operations, which depends on the code length. We use the obtained basis and the cohesion of supports of minimal code vectors in order to find the basic vectors of indecomposable subcodes such that the original linear code is the direct sum of these subcodes. Based on the obtained algorithm, we construct an algorithm of structural attack for asymmetric McEliece type cryptosystem based on code C, which polynomially depends on the complexity of structural attacks for McEliece type cryptosystems based on subcodes. Therefore, we show that the use of a direct sum of codes does not significantly enhance the strength of a McEliece-type cryptosystem against structural attacks.

Keywords: direct sum of codes; McEliece type cryptosystem; attack on the key.

References

1. McEliece R.J. A Public-Key Cryptosystem Based on Algebraic Coding Theory. *DSN Progress Report*, 1978, pp. 42–44.
2. Sidel'nikov V.M., Shestakov S.O. On an Encoding System Constructed on the Basis of Generalized Reed–Solomon Codes. *Discrete Mathematics and Applications*, 1992, vol. 2, no. 4, pp. 439–444.
3. Deundyak V.M., Druzhinina M.A., Kosolapov Yu.V. [Modification of the Sidelnikov–Shestakov Cryptanalytic Algorithm for Generalized Reed–Solomon Codes and its Software Implementation]. *Izvestiya vysshih uchebnyh zavedenij. Severo-Kavkazskij region. Tekhnicheskie nauki*, 2006, no. 4, pp. 15–19. (in Russian)
4. Wieschebrink C. Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes. *Third International Workshop*, Berlin, 2010, pp. 61–72.
5. Minder L., Shokrollahi A. Cryptanalysis of the Sidelnikov Cryptosystem. *Advances in Cryptology – EUROCRYPT 2007, Lecture Notes Computer Science*, 2007, no. 4515, pp. 347–360.

6. Borodin M.A., Chizhov I.V. Effective Attack on the McEliece Cryptosystem Based on Reed–Muller Codes. *Discrete Mathematics and Applications*, 2014, vol. 26, no. 1, pp. 273–280.

7. Deundyak V.M., Kosolapov Yu.V. Cryptosystem on Induced Group Codes. *Modelling and Analysis of Information Systems*, 2016, vol. 23, no. 2, pp. 137–152.

8. Kosolapov Yu.V., Shigaev A.N. [On the Support Splitting Algorithm for Induced Codes] *Modelling and Analysis of Information Systems*, 2018, vol. 25, no. 3, pp. 276–290. (in Russian)

9. Sidel'nikov V.M. *Teoriya kodirovaniya* [Coding Theory]. Moscow, Fizmatlit, 2008.

10. Morelos-Zaragoza R.H. *The Art of Error Correcting Coding*. Chichester, West Sussex, John Wiley & Sons, 2006.

11. Massey J.L. Minimal Codewords and Secret Sharing. *Proceeding of 6th Joint Swedish-Russian Workshop on Information Theory*, 1993, pp. 276–279.

12. Avgustinovich S.V., Gorkunov E.V. [On Automorphisms of Linear Codes over a Simple Field] *Siberian Electronic Mathematical Reports*, 2017, vol. 14, pp. 210–217. (in Russian)

13. Sendrier N. On the Concatenated Structure of a Linear Code. *Applicable Algebra in Engineering, Communication and Computing*, 1998, vol. 9, no. 3, pp. 221–242.

14. Berger T.P., Ourivski A.V. Construction of New MDS Codes from Gabidulin Codes. *Proceedings of ACCT'9*, 2004, pp. 40–47.

15. Assmus E.F. The Category of Linear Codes. *IEEE Transaction on Information Theory*, 1998, vol. 44, no. 2, pp. 612–629.

16. Fripertinger H., Kerber A. Isometry Classes of Indecomposable Linear Codess. *Lecture Notes in Computer Science*, 1995, vol. 948, pp. 194–204.

17. Sidel'nikov V.M. A Public-Key Cryptosystem Based on Binary Reed–Muller Codes. *Discrete Mathematics and Applications*, 1994, vol. 4, no. 3, pp. 191–208.

18. Deundyak V.M., Kosolapov Yu.V. On the Berger–Loidreau Cryptosystem on the Tensor Product of Codes. *Journal of Computational and Engineering Mathematics*, 2018, vol. 5, no. 2, pp. 16–33.

19. Krasavin A.A. Using the Modified $(u|u+v)$-Construction in the McEliece Cryptosystem. *Trudy MFTI*, 2018, vol. 10, no. 2, pp. 189–191. (in Russian)

20. Kabatiansky G., Tavernier C. A New Code-Based Cryptosystem via Pseudorepetition of Codes. *Proceedings of ACCT XVI*, 2018, pp. 189–191.

21. Deundyak V.M., Kosolapov Yu.V. [Using the Tensor Product of Reed–Muller Codes in an Asymmetric McEliece Type Cryptosystem and Analyzing its Resistance to Attacks on a Cipher]. *Computational Technologies*, 2017, vol. 22, no. 4, pp. 43–60. (in Russian)

Received January 17, 2019