Использование тензорного произведения кодов Рида — Маллера в асимметричной криптосистеме типа Мак-Элиса и анализ ее стойкости к атакам на шифрограмму

В. М. Деундяк[1,2], Ю. В. Косолапов[2,*]
[1]НИИ "Специализированные устройства защиты и автоматика", Ростов-на-Дону, Россия
[2]Южный федеральный университет, Ростов-на-Дону, Россия
[*]Контактный e-mail: itaim@mail.ru

Одной из наиболее известных реализаций асимметричной кодовой криптосистемы типа Мак-Элиса является криптосистема на основе двоичных кодов Рида — Маллера. Однако недавно для этой реализации найден эффективный алгоритм структурной атаки (атаки на ключ), поэтому криптосистема на кодах Рида — Маллера на настоящий момент не является стойкой. С другой стороны, если C_1 и C_2 — двоичные коды Рида — Маллера, то их тензорное произведение $C_1 \otimes C_2$ не является кодом Рида — Маллера, при этом известно, что для $C_1 \otimes C_2$ имеется алгоритм эффективного (непереборного) декодирования.

С целью усиления стойкости асимметричной кодовой криптосистемы предлагается использовать тензорное произведение кодов Рида — Маллера. Исследуется стойкость такой криптосистемы к атакам на шифрограмму, характерным для кодовых криптосистем типа Мак-Элиса независимо от используемого кода.

Ключевые слова: тензорное произведение кодов, коды Рида — Маллера, криптосистема Мак-Элиса, атаки на шифрограмму, криптостойкость.

Введение и постановка задачи

Однонаправленная функция с секретом является основой таких асимметричных криптосистем, как система RSA [1], система Рабина [2] и система Эль-Гамаля [3]. С одной стороны, для обеспечения стойкости криптосистемы требуется, чтобы без знания секрета по значению функции было вычислительно сложно найти значение аргумента, а с другой стороны, чтобы при известном секрете эта задача решалась быстро. В 1978 г. Робертом Мак-Элисом предложена и обоснована идея использования помехоустойчивых кодов для построения однонаправленной функции с секретом [4]. Сложность обращения такой функции связана с задачей декодирования случайного кода, которая является NP-полной, а простота вычисления функции следует из простоты умножения вектора на матрицу. В [4] однонаправленная функция с секретом была реализована на основе двоичных кодов Гоппы. В сравнении с криптосистемами из [1 – 3] система Мак-Элиса обладает более быстрыми операциями шифрования и расшифровывания [5], поэтому может найти применение во встроенных устройствах [6]. Также согласно [7] криптографические системы, в основе которых лежит применение помехоустойчивых кодов,

в постквантовую эпоху рассматриваются как одна из альтернатив используемым асимметричным криптографическим системам, таким как RSA, Рабина, Эль-Гамаля. Это обусловлено тем, что с развитием квантовых вычислений задачи обращения односторонних функций с секретом, на которых основаны системы RSA, Рабина и Эль-Гамаля, могут быть решены с помощью эффективных алгоритмов [8]. Широкое применение системы Мак-Элиса сдерживается, с одной стороны, тем, что квантовые вычисления пока недостаточно развиты, а с другой — тем, что используемые на практике криптосистемы, такие как RSA, обладают размером ключа, на два порядка меньшим, чем криптосистема Мак-Элиса [9] (при обеспечении одинаковой стойкости). В частности, как показано в [9], стойкость, обеспечиваемая с помощью криптосистемы RSA с длиной ключа 1717 битов, достигается для криптосистемы Мак-Элиса при размере ключа порядка 81 кбайт.

Построено множество реализаций идеи Мак-Элиса, некоторые из них можно найти в работах [10 – 14]. Отмеченные реализации основаны на применении кодов, отличных от кодов Гоппы, использованных изначально Р. Мак-Элисом [4]. Кроме новых кодов в некоторых из указанных реализаций предложены новые способы вложения информации в шифрограмму [10], новые метрики [11], а также новые конструкции кодов [13, 14].

Далее в общем случае асимметричные кодовые криптосистемы будем называть криптосистемами типа Мак-Элиса и обозначать McE(C), где C — линейный код, лежащий в основе криптосистемы. Широкий спектр криптосистем типа Мак-Элиса связан с попытками построить криптосистему, с одной стороны, имеющую размеры ключей, близкие к размерам ключей используемых в настоящее время криптосистем, а с другой — обладающую высокой стойкостью к структурным атакам (атакам на ключ) и атакам на шифрограмму.

Отметим, что сегодня эффективные атаки на ключ классической криптосистемы Мак-Элиса неизвестны. В то же время для других перечисленных выше криптосистем такие атаки имеются. В частности, для криптосистемы из [10], основанной на расширенных кодах Рида — Соломона, В.М. Сидельниковым и С.О. Шестаковым построен полиномиальный по времени алгоритм нахождения подходящего секретного ключа [15]; построены редукции криптоаналитического алгоритма Сидельникова — Шестакова для классических кодов Рида — Соломона [16, 17], а также найден универсальный способ взлома многих асимметричных криптосистем, в которых используются коды Рида — Соломона [18]. В [19] показано, что криптосистема из работы [11] на ранговых кодах небольших параметров не является стойкой к атакам на ключ; построены атаки на ключ для некоторых модификаций системы на ранговых кодах [20]. Для криптосистемы из [12] построен алгоритм успешной атаки на ключ [21], а затем он существенно ускорен [22, 23].

Для криптосистем типа Мак-Элиса реализации атак на ключ не являются универсальными, так как во многом определяются кодом, который лежит в основе криптосистемы. В то же время большинство криптосистем типа Мак-Элиса подвержены атакам на шифрограмму, которые могут быть описаны для произвольного линейного C. Это атаки на основе декодирования по информационным совокупностям [24, 25] и двух шифрограмм, соответствующих одному информационному сообщению (далее — атака повторного перехвата) [26]. Они зависят по существу только от размерности кода, его длины и кодового расстояния.

Под стойкостью криптосистемы к атаке на шифрограмму будем понимать вероятность успеха атаки — нахождения зашифрованного информационного сообщения. Если p — вероятность успеха атаки, то для нахождения зашифрованного сообщения потре-

буется произвести в среднем $1/p$ дешифрований, а вычислительная сложность такой атаки будет $\mathcal{O}((1/p)\alpha)$, где α — вычислительная сложность одного дешифрования.

В настоящей работе для усиления стойкости к атакам на ключ строится криптосистема типа Мак-Элиса на основе тензорного произведения $C_1 \otimes C_2$ двух кодов Рида — Маллера C_1 и C_2. Так как код $C_1 \otimes C_2$ не является кодом Рида — Маллера, то представляется, что известные структурные атаки для криптосистем $\mathrm{McE}(C_1)$ и $\mathrm{McE}(C_2)$ [21 – 23], успех реализации которых существенно зависит от строения кодов Рида — Маллера, могут без существенной модификации не пройти для криптосистемы $\mathrm{McE}(C_1 \otimes C_2)$. Причем код $C_1 \otimes C_2$ может успешно применяться в криптосистеме Мак-Элиса, так как для него существует быстрый алгоритм декодирования [27, 28]. С другой стороны, отмеченные выше атаки на шифрограмму для криптосистем типа Мак-Элиса слабо зависят от кода, при этом одна из наиболее сильных атак — это атака повторного перехвата. Поэтому в работе ставятся задачи, во-первых, модификации криптосистемы Мак-Элиса таким образом, чтобы затруднить атаку повторного перехвата, а во-вторых — нахождения параметров криптосистемы $\mathrm{McE}(C_1 \otimes C_2)$, при которых обеспечивается приемлемая стойкость к отмеченным атакам на шифрограмму.

Работа имеет следующую структуру. В первом разделе приводится определение криптосистемы типа Мак-Элиса и описываются атаки на основе декодирования по информационным совокупностям и атака повторного перехвата. В частности, атака повторного перехвата, впервые описанная в [26] для двоичного поля, обобщена на случай поля $\mathbb{F}_q$, $q \geq 2$. Во втором разделе предложен способ усиления стойкости криптосистемы типа Мак-Элиса к атаке повторного перехвата путем применения техники случайного шифрования; там же проводится анализ этого способа. В третьем разделе рассмотрена конструкция тензорного произведения двух двоичных кодов Рида — Маллера C_1 и C_2 и приведены результаты оценки стойкости криптосистемы $\mathrm{McE}(C_1 \otimes C_2)$ к атакам на шифрограмму. В приложение для облегчения понимания существа статьи вынесены доказательства лемм.

1. Криптосистема типа Мак-Элиса и атаки на шифрограмму

Пусть $\mathbb{F} = \mathbb{F}_q$ — поле Галуа мощности q, q — степень простого числа; $C(\subseteq \mathbb{F}^n)$ — линейный $[n, k, d]$-код длины n, размерности k, с кодовым расстоянием d. Порождающую матрицу кода C будем обозначать $G(C)$. Под криптосистемой типа Мак-Элиса на основе $[n, k, d]$-кода C здесь понимаем асимметричную криптосистему, в которой открытый ключ $\mathbf{k}_{\mathrm{pub}}$ — это пара $(\widetilde{G}, t = \lfloor (d-1)/2 \rfloor)$, а секретный ключ $\mathbf{k}_{\mathrm{sec}}$ — пара матриц (S, P), где S — случайная невырожденная $(k \times k)$-матрица, P — случайная перестановочная $(n \times n)$-матрица, причем $\widetilde{G} = S \cdot G(C) \cdot P$. Правило шифрования произвольного информационного сообщения $\mathbf{s}(\in \mathbb{F}^k)$ имеет вид

$$\mathbf{z} = \mathbf{s}\widetilde{G} + \mathbf{e}, \tag{1}$$

где вес Хэмминга добавляемой ошибки $\mathbf{e} = (e_1, ..., e_n)$ удовлетворяет неравенству $w(\mathbf{e}) \leq t$. Для расшифровывания шифрограммы $\mathbf{c}$ секретный ключ $\mathbf{k}_{\mathrm{sec}}$ используется по правилу $\mathbf{s} = \mathrm{Dec}_C(\mathbf{z}P^{-1})S^{-1}$, где $\mathrm{Dec}_C : \mathbb{F}^n \to \mathbb{F}^k$ — декодер кода C, гарантированно исправляющий t и менее ошибок и восстанавливающий вектор $\mathbf{s}$. Предполагается, что вектор ошибок $\mathbf{e}$ выбирается случайно и равновероятно из множества $\mathbb{F}^{n,t} = \mathbb{F}_q^{n,t}(\subseteq \mathbb{F}_q^n)$, состоящего из векторов веса t, $|\mathbb{F}^{n,t}| = C_n^t(q-1)^t$.

Ниже приводится описание атаки на основе декодирования по информационным совокупностям, а также описание атаки повторного перехвата для поля $\mathbb{F}_q$ и дается ее анализ.

1.1. Атака на основе декодирования по информационным совокупностям

Пусть $\underline{n} = \{1; ...; n\}$. Для множества $D \subseteq \mathbb{F}^n$ символом $\mathrm{supp}(D)$ обозначим носитель этого множества:

$$\mathrm{supp}(D) = \{i \in \underline{n} | \exists \mathbf{x} = (x_1, ..., x_n) \in D, \;\; x_i \neq 0\}.$$

Для $(k \times n)$-матрицы $M = (\mathbf{g}_i)_{i=1}^k$, где $\mathbf{g}_i$ — строка матрицы, носителем будем называть множество номеров ненулевых столбцов: $\mathrm{supp}(M) = \cup_{i=1}^k \mathrm{supp}(\mathbf{g}_i)$. Рассмотрим криптосистему $\mathrm{McE}(C)$ на основе $[n, k, d]$-кода C. Одним из способов проведения атаки на шифрограмму для криптосистемы $\mathrm{McE}(C)$ является способ декодирования по информационным совокупностям [29].

Суть этого способа заключается в следующем. Пусть $\tau (\subseteq \underline{n})$ — множество номеров мощности k, $\pi_\tau : \mathbb{F}^n \to \mathbb{F}^\tau = \{\mathbf{x} \in \mathbb{F}^n : \mathrm{supp}(\mathbf{x}) \subseteq \tau\}$ — линейный оператор проекции пространства $\mathbb{F}^n$ на координатное пространство $\mathbb{F}^\tau$ параллельно координатному подпространству $\mathbb{F}^{\overline{\tau}}$, $\overline{\tau} = \underline{n} \backslash \tau$. Этот оператор естественным образом можно определить для $(k \times n)$-матрицы $M = (\mathbf{g}_i)_{i=1}^k$, представленной как набор k строк: $\widehat{\pi}_\tau(M) = (\pi_\tau(\mathbf{g}_i))_{i=1}^k$. Множество τ называется *информационной совокупностью*, если $\mathrm{rank}(\widehat{\pi}_\tau(G(C))) = k$. Если P — перестановочная матрица, а Π — перестановка множества чисел $\{1; ....; n\}$, которой соответствует матрица P, то очевидно, что если $\tau = \{t_1; ...; t_k\}$ — информационная совокупность для кода с порождающей матрицей $G(C)$, то $\Pi(\tau) = \{\Pi(t_1); ...; \Pi(t_k)\}$ — информационная совокупность для кода с порождающей матрицей $G(C) \cdot P$.

Атака на шифрограмму $\mathbf{z}$ криптосистемы $\mathrm{McE}(C)$ путем декодирования по информационным совокупностям сводится к нахождению такой информационной совокупности τ для кода с порождающей матрицей $\widetilde{G}$, у которой в шифрограмме $\mathbf{z}$ координаты с номерами из τ не были испорчены помехой $\mathbf{e}$ (см. правило шифрования (1)). Если $\tau = \{i_1; ...; i_k\}$ — информационная совокупность и координаты из множества τ не испорчены помехой, то

$$\mathbf{s} = \pi_\tau(\mathbf{z}) \left(\widehat{\pi}_\tau(\widetilde{G})\right)^{-1}. \tag{2}$$

Рассмотрим событие $\mathcal{E}_{n,k}^t$, где $t \leq n$ и $k \leq n - t$, состоящее в том, что в некотором неизвестном векторе из $\mathbb{F}^{n,t}$ после случайного выбора k номеров координат значения этих координат оказались равными нулю. Пусть $p(\mathcal{E}_{n,k}^t)$ — вероятность этого события. Если векторы множества $\mathbb{F}^{n,t}$ распределены равновероятно, то

$$p(\mathcal{E}_{n,k}^t) = C_{n-t}^k (C_n^k)^{-1}. \tag{3}$$

Замечание 1. При наступлении события $\mathcal{E}_{n,k}^t$ может возникнуть ситуация, когда выбранное множество координат $\tau (\subseteq \underline{n})$ таково, что $\mathrm{rank}(\widehat{\pi}_\tau(\widetilde{G})) < k$. В этом случае выбранное множество τ не является информационной совокупностью в выше определенном смысле. Поэтому вероятность правильного декодирования вектора $\mathbf{z}$ вида (1) методом декодирования по информационным совокупностям не превышает $p(\mathcal{E}_{n,k}^t)$.

Отсюда получаем, что для выбора информационной совокупности, не содержащей испорченных координат, потребуется сделать в среднем не менее $\left\lceil 1/p(\mathcal{E}_{n,k}^t) \right\rceil$ попыток.

1.2. Атака повторного перехвата

В работе [26] предложена атака на шифрограмму в случае, если криптоаналитик (наблюдатель) располагает двумя шифрограммами, полученными путем шифрования одного сообщения, но с использованием разных векторов ошибок в (1). Наличие двух шифрограмм, соответствующих одному открытому тексту, дает криптоаналитику дополнительную информацию о координатах, которые были испорчены искусственно добавленными помехами при шифровании. Отметим, что для случая, когда мощность поля Галуа q — простое число, некоторый способ проверки факта повторного шифрования одного и того же сообщения предложен в [30].

Рассмотрим два равномерно распределенных на $\mathbb{F}^{n,t}$ случайных вектора $\mathbf{E}_1$, $\mathbf{E}_2$. Тогда

$$\forall \mathbf{e} \in \mathbb{F}^{n,t}, \quad \forall i \in \{1;2\}: \;\; p_{\mathbf{E}_i}(\mathbf{e}) = (C_n^t (q-1)^t)^{-1}, \tag{4}$$

где $p_{\mathbf{E}_i}(\mathbf{e})$ — это вероятность события $\mathbf{E}_i = \mathbf{e}$. Пусть

$$\mathbf{Z}_i = \mathbf{s}\widetilde{G} + \mathbf{E}_i, \quad i = 1, 2, \tag{5}$$

— случайные векторы, соответствующие одному сообщению $\mathbf{s}$; $\mathbf{Y} = \mathbf{Z}_1 - \mathbf{Z}_2 = \mathbf{E}_1 - \mathbf{E}_2$. Так как векторы ошибок при шифровании выбираются случайно, равновероятно и взаимно независимо, то с большой вероятностью значение случайного вектора $\mathbf{Y}$ отлично от нуля. Поэтому криптоаналитик по двум шифрограммам $\mathbf{z}_1$ и $\mathbf{z}_2$, являющимся реализациями соответствующих случайных векторов $\mathbf{Z}_1$ и $\mathbf{Z}_2$, может определить, что, по крайней мере, координаты с номерами из множества $\tau = \operatorname{supp}(\mathbf{z}_1 - \mathbf{z}_2)$ испорчены помехами. Следовательно, он может воспользоваться методом декодирования по информационным совокупностям, учитывая имеющуюся у него информацию о подмножестве номеров испорченных координат. Проведем анализ вероятности успеха применения этого метода для поля $\mathbb{F}_q$, где q — степень простого числа. Отметим, что более простой случай $q = 2$ описан в [26].

Лемма 1. *Пусть* $\mathbf{E}_1$, $\mathbf{E}_2$ *— случайные векторы с распределением* (4), *а* $\mathbf{e}_1$, $\mathbf{e}_2$ *— значения соответствующих случайных векторов. Пусть* H_j *— гипотеза о том, что* $|\operatorname{supp}(\mathbf{e}_1) \cap \operatorname{supp}(\mathbf{e}_2)| = j$, $j = 0, ..., t$, $p(H_j)$ *— вероятность гипотезы* H_j. *Рассмотрим событие* A_i, *состоящее в том, что векторы* $\mathbf{e}_1$ *и* $\mathbf{e}_2$ *совпадают в* i*-х ненулевых координатах, где* $i \le j$. *Тогда*

$$p(H_j) = C_t^j C_{n-t}^{t-j} (C_n^t)^{-1}, \tag{6}$$

$$p(A_i|H_j) = C_j^i (q-2)^{j-i} (q-1)^{-t}, \tag{7}$$

$$p(A_i H_j) = C_j^i (q-2)^{j-i} C_t^j C_{n-t}^{t-j} ((q-1)^t C_n^t)^{-1}. \tag{8}$$

В табл. 1 приведены результаты вычисления $p(H_j)$ в случае бинарного кода Рида — Маллера $\mathcal{RM}(1,5)$, необходимые сведения о которых имеются в разд. 3.

Рассмотрим случайные векторы (5), соответствующие одному сообщению $\mathbf{s}$. Пусть $\mathbf{z}_1 = \mathbf{s}\widetilde{G} + \mathbf{e}_1$ и $\mathbf{z}_2 = \mathbf{s}\widetilde{G} + \mathbf{e}_2$ — значения соответствующих случайных векторов $\mathbf{Z}_1$ и $\mathbf{Z}_2$,

Т а б л и ц а 1. Значения $P(H_j)$ для McE(C), $C = \mathcal{RM}(1,5)$, $t = 7$, $k = 6$, $n = 32$

j	0	1	2	3	4	5	6	7
$P(H_j)$	0.142	0.368	0.331	0.131	0.023	0.001	5.2E − 5	2.9E − 7

i — число ненулевых координат, в которых векторы $\mathbf{e}_1$ и $\mathbf{e}_2$ совпадают, $j = |\mathrm{supp}(\mathbf{e}_1) \cap \mathrm{supp}(\mathbf{e}_2)|$. Так как $\mathbf{y} := \mathbf{z}_1 - \mathbf{z}_2 = \mathbf{e}_1 - \mathbf{e}_2$, то по двум шифрограммам можно определить подмножество $\mathrm{supp}(\mathbf{e}_1 - \mathbf{e}_2)$ номеров координат, которые наверняка испорчены ошибками. Отметим, что при этом неизвестно, какие именно из этих координат испорчены в первой и второй шифрограммах. Для векторов $\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{F}^{n,t}$ обозначим $\Delta(\mathbf{e}_1, \mathbf{e}_2) = |\mathrm{supp}(\mathbf{e}_1) \cap \mathrm{supp}(\mathbf{e}_2)|$. Пусть $\nabla(\mathbf{e}_1, \mathbf{e}_2)$ — число координат, в которых ненулевые значения векторов $\mathbf{e}_1$ и $\mathbf{e}_2$ совпадают. Заметим, что $0 \le \nabla(\mathbf{e}_1, \mathbf{e}_2) \le \Delta(\mathbf{e}_1, \mathbf{e}_2) \le t$.

Лемма 2. *Для любых $\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{F}^{n,t}$ вес разности $\mathbf{e}_1$ и $\mathbf{e}_2$ вычисляется по формуле*

$$w(\mathbf{e}_1 - \mathbf{e}_2) = 2t - \Delta(\mathbf{e}_1, \mathbf{e}_2) - \nabla(\mathbf{e}_1, \mathbf{e}_2). \tag{9}$$

Заметим, что по известному вектору $\mathbf{e}_1 - \mathbf{e}_2$ и одной из двух величин $\Delta(\mathbf{e}_1, \mathbf{e}_2)$, $\nabla(\mathbf{e}_1, \mathbf{e}_2)$ можно по лемме 2 найти другую величину.

Рассмотрим событие $\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})$, заключающееся в том, что случайно и равновероятно выбраны из $\mathbb{F}^{n,t}$ два вектора $\mathbf{e}_1$, $\mathbf{e}_2$, которые полагаются неизвестными, однако известны $\boldsymbol{\epsilon} = \mathbf{e}_1 - \mathbf{e}_2$ и число $\delta = \nabla(\mathbf{e}_1, \mathbf{e}_2)$. Отметим, что вектор $\boldsymbol{\epsilon}$ из $\mathbb{F}^n$ принадлежит множеству векторов веса не более $2t$, которое далее будем обозначать $\mathbb{F}^{n,\le 2t}$. Если для заданных $(\delta, \boldsymbol{\epsilon}) \in \{0; ...; t\} \times \mathbb{F}^{n,\le 2t}$ не существует такого $j \in \{0; ...; t\}$, для которого бы выполнялось равенство $w(\boldsymbol{\epsilon}) = 2t - j - \delta$ (см. соотношение (9)), то $p(\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})) = 0$.

Лемма 3. *Если пара чисел $(\delta, l) \in \{0; ...; t\} \times \{0; ...; 2t\}$ такая, что $l = 2t - j - \delta$ для некоторого $j \in \{0; ...; t\}$, то $p(\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})) \ne 0$ для любого вектора $\boldsymbol{\epsilon}$ ($\in \mathbb{F}^{n,\le 2t}$) веса l.*

В случае $p(\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})) \ne 0$ пару $(\delta, \boldsymbol{\epsilon})$ будем называть допустимой парой из $\{0; ...; t\} \times \mathbb{F}^{n,\le 2t}$. Все пары $(\delta, l) \in \{0; ...; t\} \times \{0; ...; 2t\}$, для которых выполняется условие леммы 3, также будем называть допустимыми парами из $\{0; ...; t\} \times \{0; ...; 2t\}$.

Рассмотрим событие $\mathcal{D}_{n,k}^t$, состоящее в том, что для двух случайно и равновероятно выбранных из $\mathbb{F}^{n,t}$ векторов $\mathbf{e}_1$ и $\mathbf{e}_2$, для которых известно множество $\mathrm{supp}(\mathbf{e}_1 - \mathbf{e}_2)$, во множестве $\underline{n} \setminus \mathrm{supp}(\mathbf{e}_1 - \mathbf{e}_2)$ случайно выбрано множество τ мощности k так, что

$$\tau \cap \mathrm{supp}(\mathbf{e}_1) = \emptyset, \quad \tau \cap \mathrm{supp}(\mathbf{e}_2) = \emptyset. \tag{10}$$

Тогда вероятность этого события вычисляется по формуле полной вероятности

$$p(\mathcal{D}_{n,k}^t) = \sum_{\boldsymbol{\epsilon} \in \mathbb{F}^{n,\le 2t}} \sum_{\delta=0}^{t} p(\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})) p(\mathcal{D}_{n,k}^t | \mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})), \tag{11}$$

так как набор $\{\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})\}_{(\delta,\boldsymbol{\epsilon}) \in \{0;...;t\} \times \mathbb{F}^{n,\le 2t}}$ является полной группой событий. Для вычисления $p(\mathcal{D}_{n,k}^t | \mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon}))$ понадобится введенное в подразд. 1.1 событие $\mathcal{E}_{n-w(\boldsymbol{\epsilon}),k}^t$, состоящее в том, что в зафиксированном, но неизвестном векторе, принадлежащем $\mathbb{F}^{n-w(\boldsymbol{\epsilon}),t}$, после случайного выбора k номеров координат значения этих координат оказались равными нулю.

Лемма 4. *Для любой допустимой пары $(\delta, \boldsymbol{\epsilon})$ из $\{0; ...; t\} \times \mathbb{F}^{n,\le 2t}$*

$$p(\mathcal{D}_{n,k}^t | \mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})) = p(\mathcal{E}_{n-w(\boldsymbol{\epsilon}),k}^{\delta}). \tag{12}$$

Теорема 1. *Имеет место равенство*

$$p(\mathcal{D}_{n,k}^t) = \sum_{j=0}^{t} \sum_{\delta=0}^{j} \frac{C_t^j C_{n-t}^{t-j} C_{n-[2t-j]}^k C_j^{\delta} (q-2)^{j-\delta}}{C_n^t C_{n-[2t-j-\delta]}^k (q-1)^t}. \tag{13}$$

Доказательство. Как следует из леммы 4, вероятность $p(\mathcal{D}_{n,k}^t|\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon}))$ не зависит от значения вектора $\boldsymbol{\epsilon}$, а зависит от его веса. Поэтому, используя (11) и (12), получаем

$$p(\mathcal{D}_{n,k}^t) = \sum_{l=0}^{2t} \sum_{\substack{\boldsymbol{\epsilon}\in\mathbb{F}^{n,\leq 2t}: \\ w(\boldsymbol{\epsilon})=l}} \sum_{\delta=0}^{t} p(\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon}))p(\mathcal{D}_{n,k}^t|\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})) = \sum_{l=0}^{2t}\sum_{\delta=0}^{t} p(\mathcal{E}_{n-l,k}^{\delta}) \sum_{\substack{\boldsymbol{\epsilon}\in\mathbb{F}^{n,\leq 2t}: \\ w(\boldsymbol{\epsilon})=l}} p(\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})).$$

Заметим, что для фиксированных δ и l внутренняя сумма в последнем равенстве — это вероятность того, что разность двух случайно выбранных из $\mathbb{F}^{n,t}$ векторов имеет вес l и эти векторы совпадают в δ координатах. С учетом леммы 1 получаем

$$\sum_{\substack{\boldsymbol{\epsilon}\in\mathbb{F}^{n,\leq 2t}: \\ w(\boldsymbol{\epsilon})=l}} p(\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})) = p(A_\delta H_{2t-\delta-l}). \tag{14}$$

Так как $2t-\delta-l \geq 0$, то

$$p(\mathcal{D}_{n,k}^t) = \sum_{l=0}^{2t} \sum_{\substack{(\delta,j): \\ \delta+j=2t-l}} p(\mathcal{E}_{n-l,k}^{\delta})p(A_\delta H_j) = \sum_{j=0}^{t}\sum_{\delta=0}^{j} p(\mathcal{E}_{n-(2t-j-\delta),k}^{\delta})p(A_\delta H_j). \tag{15}$$

Отсюда в силу (3) и (8) получаем (13). ■

Таким образом, имея две шифрограммы $\mathbf{z}_1 = \mathbf{s}\widetilde{G}+\mathbf{e}_1$ и $\mathbf{z}_2 = \mathbf{s}\widetilde{G}+\mathbf{e}_2$, криптоаналитик сможет найти разность ошибок $\mathbf{e}_1-\mathbf{e}_2$ и попробовать применить метод декодирования по информационным совокупностям (либо для шифрограммы $\mathbf{z}_1$, либо для $\mathbf{z}_2$), выбирая k координат из множества $\underline{n}\setminus \mathrm{supp}(\mathbf{e}_1-\mathbf{e}_2)$. В среднем вероятность $p(\mathcal{D}_{n,k}^t)$ успешного выбора k координат, не испорченных помехами $\mathbf{e}_1$ и $\mathbf{e}_2$, согласно теореме 1 вычисляется по формуле (13). Отметим, что вероятность успешного декодирования (вероятность успеха атаки) в среднем будет *не более* $p(\mathcal{D}_{n,k}^t)$, так как для случайно выбранного множества τ, $|\tau| = k$, возможен случай, когда $\mathrm{rank}(\widehat{\pi}_\tau(\widetilde{G})) < k$ (см. замечание 1).

2. Усиление стойкости криптосистемы типа Мак-Элиса к атакам на шифрограмму при повторном перехвате

Рассмотрим криптосистему McE(C), где C — линейный $[n,k,d]$-код, $k>1$. Для защиты от атаки повторного перехвата предлагается следующий способ формирования шифрограмм. К каждому информационному блоку $\mathbf{s}$ длины $k'(1\leq k'<k)$ дописывается слева случайно выбранный зашумляющий вектор $\boldsymbol{\omega}$ длины $k-k'$. Полученный вектор длины k шифруется по правилу (1). Такая техника *случайного шифрования* предложена в [31] для усиления стойкости симметричных кодовых криптосистем, а для усиления стойкости асимметричных кодовых криптосистем типа Мак-Элиса этот прием также использован в [32], где эффект от случайной добавки при шифровании исследуется в рамках теоретико-информационного подхода: исследуется количество информации, которое получает перехватчик в рамках различных атак на шифрограмму. Идея этой модификации для асимметричных криптосистем сформулирована также в [14]. Ниже анализируется эффект от применения техники случайного шифрования для защиты от атаки повторного перехвата, чего ранее сделано не было.

При использовании дополнительного зашумляющего вектора $\boldsymbol{\omega}(\in \mathbb{F}^{k-k'})$ правило шифрования (1) примет вид

$$(\boldsymbol{\omega}, \mathbf{s})\widetilde{G} + \mathbf{e} = \mathbf{z}, \tag{16}$$

где $\mathbf{s}(\in \mathbb{F}^{k'})$ — информационный блок, а запись $(\boldsymbol{\omega}, \mathbf{s})$ означает приписывание вектора $\boldsymbol{\omega}$ слева к вектору $\mathbf{s}$. Для расшифровывания $\mathbf{z}$ достаточно применить правило расшифровывания из разд. 1, а затем отбросить случайный вектор $\boldsymbol{\omega}$. Криптосистему типа Мак-Элиса с правилом шифрования (16) будем обозначать McE(C, k').

Замечание 2. Криптосистемы McE(C) и McE(C, k') различаются только правилами шифрования/расшифровывания, при этом структуры секретных и открытых ключей совпадают. Поэтому эти системы эквивалентны по стойкости к атакам на ключ. Они также совпадают по стойкости к атаке на основе декодирования по информационным совокупностям при атаке на одну шифрограмму, так как по одной шифрограмме нет возможности получить какую-либо дополнительную информацию о векторе ошибок, кроме его веса.

Покажем, насколько использование зашумляющих векторов затрудняет проведение атаки декодирования по информационным совокупностям при повторном перехвате. Рассмотрим случайные, равномерно распределенные векторы $\boldsymbol{\Omega}_1$, $\boldsymbol{\Omega}_2$, принимающие значения в $\mathbb{F}_q^{k-k'}$, а также случайные, равномерно распределенные векторы $\mathbf{E}_1$, $\mathbf{E}_2$, принимающие значения в $\mathbb{F}^{n,t}$ (см. (4)). Пусть

$$\mathbf{Z}_i = (\boldsymbol{\Omega}_i, \mathbf{s})\widetilde{G} + \mathbf{E}_i, \quad i \in \{1; 2\}, \tag{17}$$

$$\mathbf{Y} = \mathbf{Z}_1 - \mathbf{Z}_2 = \boldsymbol{\Omega}\widehat{G} + \mathbf{X}, \tag{18}$$

где $\boldsymbol{\Omega} = \boldsymbol{\Omega}_1 - \boldsymbol{\Omega}_2$, $\mathbf{X} = \mathbf{E}_1 - \mathbf{E}_2$; $\widehat{G}$ — матрица, состоящая из верхних $k - k'$ строк матрицы $\widetilde{G}$. Отметим, что

$$p_{\boldsymbol{\Omega}}(\boldsymbol{\omega}) = p_{\boldsymbol{\Omega}_i}(\boldsymbol{\omega}) = 1/q^{k-k'}$$

для всех $\boldsymbol{\omega} \in \mathbb{F}_q^{k-k'}$. Пусть $\mathbf{z}_i$ — реализация случайного вектора $\mathbf{Z}_i$ вида (17), $i = 1, 2$, и

$$\mathbf{y} = \mathbf{z}_1 - \mathbf{z}_2 = \boldsymbol{\omega}\widehat{G} + \mathbf{x}, \quad \boldsymbol{\omega} = \boldsymbol{\omega}_1 - \boldsymbol{\omega}_2, \quad \mathbf{x} = \mathbf{e}_1 - \mathbf{e}_2. \tag{19}$$

Как видим, в этом случае разность $\mathbf{e}_1 - \mathbf{e}_2$ “замаскирована” вектором $\boldsymbol{\omega}\widehat{G}$, значение которого для криптоаналитика неизвестно. Чтобы найти $\mathbf{x}$, криптоаналитику необходимо декодировать вектор $\mathbf{y}$, рассматривая его как зашумленный кодовый вектор линейного кода с порождающей матрицей $\widehat{G}$. (Под декодированием здесь без нарушения общности понимается восстановление вектора $\boldsymbol{\omega}$ по вектору $\mathbf{y}$.) Если криптоаналитику удастся декодировать вектор $\mathbf{y}$ в вектор $\boldsymbol{\omega}$, то вектор $\mathbf{x}$ очевидным образом находится из выражения $\mathbf{x} = \mathbf{y} - \boldsymbol{\omega}\widehat{G}$. Далее к какой-либо из шифрограмм ($\mathbf{z}_1$ или $\mathbf{z}_2$) можно применить метод декодирования по информационным совокупностям, учитывая, что ему известен вектор $\mathbf{x} = \mathbf{e}_1 - \mathbf{e}_2$ (вычислению вероятности успеха применения этого метода посвящен предыдущий раздел). Например, он может применить этот метод для шифрограммы $\mathbf{z}_1$. В случае успеха, т. е. когда удалось выбрать такое множество τ, $|\tau| = k$, что выполняется условие (10), он сможет восстановить значение вектора $(\mathbf{s}, \boldsymbol{\omega}_1)$, применив правило (2) для значения $\pi_\tau(\mathbf{z}_1)$ при условии $\operatorname{rank}(\widehat{\pi}_\tau(\widetilde{G})) = k$. Сообщение $\mathbf{s}$ далее находится отбрасыванием крайних справа $k - k'$ координат результата декодирования.

Оценим вероятность успешного декодирования вектора $\mathbf{y}$. Так как матрица $\widehat{G}$, с точки зрения криптоаналитика, является порождающей матрицей линейного кода общего положения, будем полагать, что для восстановления значения вектора $\boldsymbol{\omega}$ криптоаналитик использует метод декодирования по информационным совокупностям.

Замечание 3. Если $|\mathrm{supp}(\widehat{G})| < n$ и $\mathrm{supp}(\mathbf{x}) \not\subseteq \mathrm{supp}(\widehat{G})$, то наблюдатель по вектору $\mathbf{y}$ может найти $\partial(\mathbf{x})$ координат вектора ошибок $\mathbf{x}$ путем простого сравнения носителя значения вектора $\mathbf{y}$ с носителем матрицы $\widehat{G}$, где

$$\partial(\mathbf{x}) = |\mathrm{supp}(\mathbf{x}) \setminus \mathrm{supp}(\widehat{G})| = w(\mathbf{x}) - |\mathrm{supp}(\mathbf{x}) \cap \mathrm{supp}(\widehat{G})|.$$

Поэтому k' надо выбирать так, чтобы $|\mathrm{supp}(\widehat{G})| = n$, что далее и предполагается.

Лемма 5. *Пусть вектор* $\mathbf{y}$ *имеет вид* (19), $\boldsymbol{\omega}$ *и* $\mathbf{x}$ *— неизвестны,* $\mathrm{supp}(\widehat{G})$ *— множество номеров ненулевых столбцов матрицы* $\widehat{G}$, $|\mathrm{supp}(\widehat{G})| = n$. *Тогда в случае, когда вес* $w(\mathbf{x})$ *вектора* $\mathbf{x}$ *известен, методом декодирования по информационным совокупностям вектор* $\boldsymbol{\omega}$ *может быть восстановлен с вероятностью, не превышающей* $p(\mathcal{E}^{w(\mathbf{x})}_{n,k-k'})$.

Из леммы 5 получаем, что вектор $\mathbf{x}$ по вектору $\mathbf{y}$ вида (19) может быть восстановлен методом декодирования по информационным совокупностям с вероятностью, не превышающей $p(\mathcal{E}^{w(\mathbf{x})}_{n,k-k'})$, когда $w(\mathbf{x})$ известно. При этом вероятность $p(\mathcal{E}^{w(\mathbf{x})}_{n,k-k'})$ не зависит от вектора $\boldsymbol{\omega}$, а зависит только от вектора $\mathbf{x} = \mathbf{e}_1 - \mathbf{e}_2$.

Рассмотрим случайный вектор $\mathbf{Y}$ вида (18). Пусть $\mathcal{U}^{t,\delta,l}_n$ — событие, заключающееся в том, что выбрано значение $\mathbf{y} = \boldsymbol{\omega}\widehat{G} + \mathbf{x}$ случайного вектора $\mathbf{Y}$, причем вес вектора $\mathbf{x} = \mathbf{e}_1 - \mathbf{e}_2$ равен l и $\nabla(\mathbf{e}_1, \mathbf{e}_2) = \delta$. Таким образом, событие $\mathcal{U}^{t,\delta,l}_n$ состоит из элементарных событий $(\boldsymbol{\omega}, \mathbf{e}_1, \mathbf{e}_2)$ случайного вектора $\boldsymbol{\Psi} = (\boldsymbol{\Omega}, \mathbf{E}_1, \mathbf{E}_2)$, для которых $\boldsymbol{\omega} \in \mathbb{F}^{k-k'}$, $\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{F}^{n,t}$ и $w(\mathbf{e}_1 - \mathbf{e}_2) = l$, $\nabla(\mathbf{e}_1, \mathbf{e}_2) = \delta$. Отметим, что случайные векторы $\boldsymbol{\Omega}$, $\mathbf{E}_1$ и $\mathbf{E}_2$ независимые, поэтому вероятность $p_{\boldsymbol{\Psi}}(\boldsymbol{\omega}, \mathbf{e}_1, \mathbf{e}_2)$ вычисляется по формуле

$$p_{\boldsymbol{\Psi}}(\boldsymbol{\omega}, \mathbf{e}_1, \mathbf{e}_2) = p_{\boldsymbol{\Omega}}(\boldsymbol{\omega}) p_{\mathbf{E}_1}(\mathbf{e}_1) p_{\mathbf{E}_1}(\mathbf{e}_1). \tag{20}$$

Лемма 6. *Имеет место равенство* $p(\mathcal{U}^{t,\delta,l}_n) = p(A_\delta H_{2t-l-\delta})$.

Рассмотрим событие $\mathcal{S}^t_{n,k,k'}$, заключающееся в том, что для случайно выбранных векторов $\mathbf{e}_1$ и $\mathbf{e}_2$ (в соответствии с распределением (4)) и случайно выбранного вектора $\boldsymbol{\omega}$ (реализация случайного вектора Ω) по известному вектору $\mathbf{y}$ вида (19) методом декодирования по информационным совокупностям найдено значение вектора $\mathbf{e}_1 - \mathbf{e}_2$ и на основе этого вектора выбрано множество $\tau(\subseteq \underline{n})$ мощности k, удовлетворяющее условию (10). Пусть $p(\mathcal{S}^t_{n,k,k'})$ — априорная вероятность события $\mathcal{S}^t_{n,k,k'}$. Так как набор $\{\mathcal{U}^{t,\delta,l}_n\}_{(\delta,l)\in\{0;\ldots;t\}\times\{0;\ldots;2t\}}$ — это полная группа событий, то

$$p(\mathcal{S}^t_{n,k,k'}) = \sum_{l=0}^{2t} \sum_{\delta=0}^{t} p(\mathcal{U}^{t,\delta,l}_n) p(\mathcal{S}^t_{n,k,k'} | \mathcal{U}^{t,\delta,l}_n). \tag{21}$$

Лемма 7. *Для любой допустимой пары* $(\delta, l) \in \{0; \ldots; t\} \times \{0; \ldots; 2t\}$

$$p(\mathcal{S}^t_{n,k,k'} | \mathcal{U}^{t,\delta,l}_n) \le p(\mathcal{E}^l_{n,k-k'}) p(\mathcal{E}^\delta_{n-l,k}).$$

Теорема 2. *Имеет место равенство*

$$p(\mathcal{S}^t_{n,k,k'}) \le \sum_{j=0}^{t}\sum_{\delta=0}^{j} \frac{C^{k-k'}_{n-[2t-j-\delta]} C^j_t C^{t-j}_{n-t} C^k_{n-[2t-j]} C^\delta_j (q-2)^{j-\delta}}{C^{k-k'}_n C^t_n C^k_{n-[2t-j-\delta]} (q-1)^t}. \tag{22}$$

Доказательство. Применив в (21) оценку для $p(\mathcal{S}^t_{n,k,k'}|\mathcal{U}^{t,\delta,l}_n)$ из леммы 7 и заменив $p(\mathcal{U}^{t,\delta,l}_n)$ в соответствии с леммой 6, получим

$$\begin{aligned} p(\mathcal{S}^t_{n,k,k'}) &\le \sum_{l=0}^{2t}\sum_{\delta=0}^{t} p(\mathcal{E}^l_{n,k-k'}) p(\mathcal{E}^\delta_{n-l,k}) p(A_\delta H_{2t-l-\delta}) = \\ &= \sum_{j=0}^{t}\sum_{\delta=0}^{j} p(\mathcal{E}^{2t-j-\delta}_{n,k-k'}) p(\mathcal{E}^\delta_{n-(2t-j-\delta),k}) p(A_\delta H_j). \end{aligned} \tag{23}$$

С учетом равенств (3) и (8) получаем (22). ■

Таким образом, как следует из сравнения формул (15) и (23), криптосистемы McE(C) и McE(C,k') различаются по стойкости к атаке повторного перехвата: в формуле (23) каждое слагаемое из (15) умножено на число $p(\mathcal{E}^{2t-j-\delta}_{n,k-k'})$, меньшее единицы (за исключением случая $\delta = j = t$, когда одно слагаемое умножается на единицу). Это позволяет сделать вывод, что использование техники случайного шифрования усиливает стойкость криптосистемы к атаке повторного перехвата.

3. Криптосистема типа Мак-Элиса на основе тензорного произведения кодов Рида — Маллера и оценка ее стойкости к атакам на шифрограмму

Для построения криптосистемы Мак-Элиса необходимо, чтобы лежащий в основе криптосистемы код имел быстрый алгоритм декодирования, а также для достижения высокой стойкости этот код не должен обладать "простой" алгебраической структурой. В настоящей работе предлагается в качестве помехоустойчивого кода использовать тензорное произведение $C_1 \otimes C_2$ мажоритарно декодируемых кодов C_1 и C_2. Код $C_1 \otimes C_2$ является мажоритарно декодируемым кодом, для которого имеется быстрый алгоритм декодирования [27, 28]. При этом представляется, что алгебраическая структура кода $C_1 \otimes C_2$ не является более простой, чем структура кода C_1 или кода C_2. В частности, если C_1 и C_2 — коды Рида — Маллера, то $C_1 \otimes C_2$ не является кодом Рида — Маллера. В этом случае имеющиеся структурные атаки для криптосистемы на основе кодов Рида — Маллера неприменимы для криптосистемы на основе тензорного произведения кодов Рида — Маллера. В настоящем разделе оценивается стойкость криптосистемы типа Мак-Элиса на основе тензорного произведения кодов Рида — Маллера к атакам на шифрограмму, рассмотренным в первом разделе.

Замечание 4. Для оригинальной криптосистемы Мак-Элиса на $[1024, 524, 50]$-коде Гоппы вероятность успеха атаки на основе декодирования по информационным совокупностям в соответствии с (3) не превышает числа $q_G := 7.2\text{E}-17 (= 7.2\cdot 10^{-17})$. В настоящем разделе вероятности успеха атак на шифрограмму будем сравнивать с q_G, считая криптосистему практически стойкой, если вероятность успеха атаки меньше q_G, и нестойкой

в противном случае. Такой подход выбран с целью сравнения стойкости криптосистемы в случае использования тензорного произведения кодов со стойкостью криптосистемы без применения тензорного произведения кодов.

Под тензорным произведением $A \otimes B$ матрицы $A = (a_{i,j})$ размера $(r \times s)$ и матрицы B будем понимать, как обычно, матрицу вида

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

Если C_1 — $[n_1, k_1, d_1]$-код с порождающей матрицей $G(C_1)$, а C_2 — $[n_2, k_2, d_2]$-код с порождающей матрицей $G(C_2)$, то под тензорным произведением кодов $C_1 \otimes C_2$ будем понимать код с порождающей матрицей $G(C_1 \otimes C_2) = G(C_1) \otimes G(C_2)$. Известно, что код $C_1 \otimes C_2$ является $[n_1 n_2, k_1 k_2, d_1 d_2]$-кодом [33].

Ниже будем использовать $[n, k, d]$-коды Рида — Маллера $\mathcal{RM}(r, m)$, где $n = 2^m$, $k = \sum_{i=0}^{r} C_m^i$, $d = 2^{m-r}$ [33]. Для кода $C' = \mathcal{RM}(r, m)$ при $m \le 16$, $r \le \min\{m; 7\}$ в настоящей работе вычислена вероятность события $\mathcal{E}_{n,k}^t$ в соответствии с (3), где $n = 2^m$, $k = \sum_{i=0}^{r} C_m^i$, $t = 2^{m-r-1} - 1$. В первом столбце табл. 2 приведены параметры (n, k, t), для которых $p(\mathcal{E}_{n,k}^t)$ меньше q_G (см. замечание 4). В соответствии с замечанием 2 криптосистемы McE(C') и McE(C', k') эквивалентны в рамках атаки декодирования по информационным совокупностям для одной шифрограммы. Поэтому значения из второго столбца табл. 2 характеризуют соответствующую стойкость как криптосистемы McE(C'), так и McE(C', k') $(k' \le k)$. В третьем столбце приведена скорость передачи информации при использовании криптосистемы McE(C'), а в четвертом — McE(C', k'), когда $k' = \lfloor k/2 \rfloor$. Заметим, что в [22] показано, что криптосистема McE(C'), где $C' = \mathcal{RM}(r, m)$ при $m \le 16$, $r \le \min\{m; 7\}$, не является стойкой к атаке на ключ: при $r \le 7$ и $m = 16$ на поиск секретного ключа тратится не более семи часов на ноутбуке с процессором 2.1 ГГц. В силу замечания 2 система McE(C', k') также не является стойкой к атаке на ключ. Поэтому системы McE(C') и McE(C', k') в целом не являются стойкими из-за наличия успешной атаки на ключ.

Для усиления стойкости криптосистемы заменим код Рида — Маллера тензорным произведением кодов Рида — Маллера, а именно рассмотрим криптосистему McE$(C_1 \otimes C_2)$, где C_i — $[n_i, k_i, d_i]$-код Рида — Маллера $\mathcal{RM}(r_i, m_i)$, $n_i = 2^{m_i}$, $r_i \le m_i$, $k_i = \sum_{j=0}^{r_i} C_{r_i}^j$,

Т а б л и ц а 2. Характеристики криптосистем McE(C') и McE(C', k'), обеспечивающих высокую стойкость к атакам на одну шифрограмму, где C' — код $\mathcal{RM}(r, 16)$, $k' = k/2$

$(\mathbf{n}, \mathbf{k}, \mathbf{t})$	$p(\mathcal{E}_{n,k}^t)$	$\mathbf{k/n}$	$(\mathbf{k} - \mathbf{k}')/\mathbf{n}$
(65 536,697,4095)	2.296E-20	0.010	0.005
(65 536,2517,2047)	4.144E-36	0.038	0.019
(65 536,6885,1023)	1.886E-50	0.105	0.052
(65 536,14 893,511)	3.409E-58	0.227	0.113
(65 536,26 333,255)	*8.899E-58*	*0.401*	*0.200*
(65 536,39 203,127)	4.280E-51	0.598	0.299
(65 536,50 643,63)	2.603E-41	0.772	0.386
(65 536,58 651,31)	4.343E-31	0.894	0.447
(65 536,63 019,15)	5.605E-22	0.961	0.480

$d_i = 2^{m_i - r_i}$, $i \in \{1;2\}$. Для криптосистем McE$(C_1 \otimes C_2)$ и McE$(C_1 \otimes C_2, k')$ (см. замечание 2) на настоящий момент атак на ключ не наблюдалось: как отмечалось выше, код $C_1 \otimes C_2$ не является кодом Рида — Маллера, поэтому весьма вероятно, что имеющиеся атаки на ключ в неадаптированном виде не могут быть к ним применимы.

Проведенные в настоящей работе вычисления в соответствии с (3) и (13) показали, что криптосистема McE$(C_1 \otimes C_2)$ обладает высокой стойкостью только к атаке на основе декодирования по информационным совокупностям, но к атаке повторного перехвата при всех возможных сочетаниях параметров $r_i = 1, ..., 8$ и $m_i = 3, ..., 8$, $i \in \{1;2\}$, не может рассматриваться стойкой, так как вероятность успеха такой атаки существенно больше q_G ($p(\mathcal{D}^t_{n,k}) \geq 0.2$ для $n = 2^{m_1+m_2}$, $k = \dim(C_1) \cdot \dim(C_2)$, $t = 2^{m_1-r_1+m_2-r_2-1}$). С другой стороны, для криптосистемы McE$(C_1 \otimes C_2, k')$ имеются параметры (n, k, t, k'), при которых обеспечивается высокая стойкость (т. е. вероятность атак меньше q_G) к атаке как на основе декодирования по информационным совокупностям, так и повторного перехвата.

Для $k' = \lfloor k/2 \rfloor$ в табл. 3 представлена сводка параметров кодов-произведений, обеспечивающих высокую стойкость криптосистемы McE$(C_1 \otimes C_2, k')$, C_i — код Рида — Маллера $\mathcal{RM}(r_i, m_i)$, $r_i = 1, ..., 8$, $m_i = 3, ..., 8$, $i \in \{1;2\}$. При вычислении $p(\mathcal{S}^t_{n,k,k'})$ использован тот факт, что в блочном виде порождающей матрицы кода Рида — Маллера первая строка состоит из всех единиц, а следовательно, в порождающей матрице кода $C_1 \otimes C_2$ первая строка также состоит из всех единиц. Поэтому с высокой вероятностью носитель верхних $\dim(C_1) \cdot \dim(C_2)/2 - k'$ строк матрицы $\widetilde{G}$ (открытый ключ криптосистемы McE$(C_1 \otimes C_2)$) будет равен носителю $\widetilde{G}$ (см. замечание 3).

Отметим, что $C_1 \otimes C_2$ — это $[n_1 n_2, k_1 k_2, d_1 d_2]$-код. Поэтому для определения эффекта от использования тензорного произведения стойкость криптосистемы McE$(C_1 \otimes C_2, k')$ следует сравнивать со стойкостью криптосистемы McE$(\widehat{C}, k'')$, построенной на основе $[\widehat{n}, \widehat{k}, \widehat{d}]$-кода Рида — Маллера $\widehat{C}$, для которого $\widehat{k} - k'' \approx k_1 k_2 - k'$ и $\widehat{n} \approx n_1 n_2$. Для примера рассмотрим криптосистему McE$(\widehat{C}, k'')$ на $[65\,536, 26\,333, 512]$-коде Рида — Маллера $\widehat{C}$ при $k'' = \lfloor 26\,333/2 \rfloor = 13166$ (см. табл. 2, пятая строка снизу, $t = \lfloor (512-1)/2 \rfloor = 255$) и криптосистему McE$(C_1 \otimes C_2, k')$ для $[65\,636, 26\,569, 256]$-кода $C_1 \otimes C_2$, соответствующего последней строке табл. 3, $k' = \lfloor 26\,569/2 \rfloor = 13\,284$. Эти строки в таблицах выделены курсивом. Заметим, что длины кода $\widehat{C}$ и кода $C_1 \otimes C_2$ совпадают и скорости передачи информации также близки: в первом случае 0.2, а во втором — 0.202. Однако крипто-

Т а б л и ц а 3. Характеристики криптосистемы McE$(C_1 \otimes C_2, k')$, обеспечивающей высокую стойкость к атакам на шифрограмму, где C_i — код Рида — Маллера $\mathcal{RM}(r_i, m_i)$, $n_i = 2^{m_i}$, $r_i \leq m_i$, $k_i = \sum_{j=0}^{r_i} C^j_{r_i}$, $m_i = 1, ..., 8$, $i \in \{1;2\}$, $k = k_1 k_2$, $n = n_1 n_2$ $k' = k/2$

$\mathbf{n}$	$(\mathbf{m}_1, \mathbf{m}_2, \mathbf{r}_1, \mathbf{r}_2)$	$\mathbf{k}_{\text{pub}}$, Мб	$\mathbf{k}_{\text{sec}}$, Мб	$(\mathbf{k} - \mathbf{k}')/\mathbf{n}$	$p(\mathcal{E}^t_{n,k})$	$p(\mathcal{S}^t_{n,k,k'})$
32 768	(7,8,2,3)	10.54	0.93	0.041	9.056E-19	1.704E-18
32 768	(7,8,3,3)	23.25	4.28	0.090	5.293E-21	4.579E-20
32 768	(7,8,3,4)	40.75	13.03	0.159	2.087E-19	1.400E-17
65 636	(8,8,2,2)	10.70	0.35	0.010	3.360E-19	2.225E-19
65 636	(8,8,2,3)	26.88	1.54	0.026	9.169E-24	1.263E-23
65 636	(8,8,2,4)	47.12	4.46	0.046	1.366E-20	3.675E-20
65 636	(8,8,3,3)	67.57	9.04	0.065	2.395E-30	2.068E-29
65 636	(8,8,3,4)	118.43	27.52	0.115	2.760E-27	1.359E-25
65 536	(8,8,4,4)	207.57	84.28	0.202	4.832E-26	1.047E-22

система $\mathrm{McE}(\widehat{C}, k'')$ не может применяется на практике, так как для нее имеется эффективная атака на ключ [22, 23]). Не исключается, что криптосистема $\mathrm{McE}(C_1 \otimes C_2, k')$ может быть применима на практике, так как на настоящий момент неизвестны структурные атаки и при этом обеспечивается высокая стойкость к рассмотренным атакам на шифрограмму: $p(\mathcal{E}^t_{n,k,})$ и $p(\mathcal{S}^t_{n,k,k'})$ меньше q_G.

Отметим, что при использовании тензорного произведения кодов стойкость к атаке на основе декодирования по информационным совокупностям снижается по сравнению со стойкостью криптосистемы на коде Рида — Маллера с сопоставимыми параметрами. Например, для криптосистемы $\mathrm{McE}(\widehat{C}, k'')$ вероятность успеха этой атаки намного меньше, чем для $\mathrm{McE}(C_1 \otimes C_2, k')$ (см. табл. 2 и 3: $8.899\mathrm{E}-58 \ll 4.832\mathrm{E}-26$). Это связано с тем, что код $C_1 \otimes C_2$ позволяет исправлять существенно меньше ошибок, чем код $\widehat{C}$. Добиться подходящей стойкости можно путем увеличения параметров кода и использования техники случайного шифрования.

Заключение

Предложен способ построения асимметричной кодовой криптосистемы типа Мак-Элиса на основе тензорного произведения двоичных кодов Рида — Маллера. С одной стороны, такая криптосистема представляется стойкой к атакам на ключ, так как получаемые в результате произведения коды являются новыми и для них известные атаки могут быть неприменимы. С другой стороны, как показали вычисления для тензорного произведения двоичных кодов Рида — Маллера, стойкость криптосистем, основанных на таких кодах, к атакам на шифрограмму ниже, чем на основе кодов Рида — Маллера при сопоставимых параметрах кодов (длине и размерности).

Повышения стойкости до приемлемого уровня (который определяется контекстом прикладной задачи) можно добиться увеличением параметров кодов, используемых в тензорном произведении, и путем применения техники случайного шифрования. Однако это приводит к увеличению размеров ключей криптосистемы (см. третий слева столбец в табл. 3). Но несмотря на это, использование тензорного произведения кодов представляется одним из способов повышения стойкости криптосистем типа Мак-Элиса. В пользу этого утверждения говорит, например, то, что найдены параметры кодов Рида — Маллера для тензорного произведения кодов, при которых соответствующая криптосистема обладает высокой стойкостью к атакам на шифрограмму и одновременно представляется стойкой к структурным атакам, в то время как криптосистема на коде Рида — Маллера при сопоставимых параметрах не является одновременно стойкой к атакам на шифрограмму и структурным атакам. Уменьшения размера ключа представляется возможным добиться путем использования кодов над недвоичными полями, а также путем использования случайного шифрования с заранее неизвестным перехватчику местом размещения шифруемого информационного сообщения.

Приложение. Доказательства лемм

Доказательство леммы 1. Равенство (6) доказывается фактически по схеме из [26]. Действительно, зафиксируем значение $\mathbf{e}_1 (\in \mathbb{F}^{n,t})$ для случайного вектора $\mathbf{E}_1$. Всего имеется $C^t_n (q-1)^t$ возможных выборов такого вектора. Найдем количество векторов во множестве $\mathbb{F}^{n,t}$, носители которых пересекаются с носителем вектора $\mathbf{e}_1$ по $j (\in \{0; ...; t\})$ координатам. Таких векторов $C^j_t C^{t-j}_{n-t} (q-1)^t$, так как для t ненулевых координат вектора $\mathbf{e}_1$

имеется C_t^j вариантов выбора j координат, по которым носители будут пересекаться, и для каждого из этих вариантов имеется C_{n-t}^{t-j} вариантов выбора номеров координат так, чтобы соответствующие координаты в векторе $\mathbf{e}_1$ были нулевыми. Множитель $(q-1)^t$ учитывает количество возможных ненулевых значений зафиксированных t координат значений случайного вектора $\mathbf{E}_2$. Отсюда получаем (6).

Теперь докажем (7). Вектор $\mathbf{e}_1$ может иметь $(q-1)^t$ различных значений. Пусть известно множество $T = \mathrm{supp}(\mathbf{e}_1) \cap \mathrm{supp}(\mathbf{e}_2)$ и $|T| = j$. Тогда вектор $\mathbf{e}_2$ должен совпадать с вектором $\mathbf{e}_1$ по любым i координатам из множества T, а по остальным координатам из этого множества он должен отличаться от значений вектора $\mathbf{e}_1$. Имеется C_j^i позиций, по которым значения вектора $\mathbf{e}_2$ могут совпадать с вектором $\mathbf{e}_1$, а на остальных $j-i$ координатах вектор $\mathbf{e}_2$ может принимать $(q-2)^{j-i}$ значений, отличающихся от значений вектора $\mathbf{e}_1$ на этих же координатах. Отсюда следует (7).

Равенство (8) следует из (6), (7) и равенства $p(A_i H_j) = p(A_i|H_j)p(H_j)$.

Доказательство леммы 2. Для доказательства достаточно заметить, что

$$w(\mathbf{e}_1 - \mathbf{e}_2) = |\mathrm{supp}(\mathbf{e}_1) \cup \mathrm{supp}(\mathbf{e}_2)| - \nabla(\mathbf{e}_1, \mathbf{e}_2) = \\ = w(\mathbf{e}_1) + w(\mathbf{e}_2) - |\mathrm{supp}(\mathbf{e}_1) \cap \mathrm{supp}(\mathbf{e}_2)| - \nabla(\mathbf{e}_1, \mathbf{e}_2).$$

С учетом равенств $w(\mathbf{e}_1) = w(\mathbf{e}_2) = t$ и $|\mathrm{supp}(\mathbf{e}_1) \cap \mathrm{supp}(\mathbf{e}_2)| = \Delta(\mathbf{e}_1, \mathbf{e}_2)$ получаем (9).

Доказательство леммы 3. Пусть выполняется условие леммы $\boldsymbol{\epsilon} = (\epsilon_1, \epsilon_2, ..., \epsilon_n) (\in \mathbb{F}^{n,\leq 2t})$, $w(\boldsymbol{\epsilon}) = l$. Для доказательства леммы достаточно показать, что найдется хотя бы одна пара $(\mathbf{e}_1, \mathbf{e}_2) \in \mathbb{F}^{n,t} \times \mathbb{F}^{n,t}$, такая, что $\Delta(\mathbf{e}_1, \mathbf{e}_2) = j$, $\nabla(\mathbf{e}_1, \mathbf{e}_2) = \delta$ и $\boldsymbol{\epsilon} = \mathbf{e}_1 - \mathbf{e}_2$. Пусть, без потери общности, вектор $\boldsymbol{\epsilon}$ такой, что $\epsilon_1 = ... = \epsilon_\delta = 0$, $\epsilon_f \neq 0$ для $f = \delta + 1, ..., \delta + l$. Выберем вектор $\mathbf{e}_1 = (e_{1,1}, e_{1,2}, ..., e_{1,n})$ из $\mathbb{F}^{n,t}$ так, чтобы $\mathrm{supp}(\mathbf{e}_1) = \{1; ...; t\}$ и $e_{1,s} \neq \epsilon_s$ для $s = \delta + 1, ..., j$. Вектор $\mathbf{e}_2 = (e_{2,1}, e_{2,2}, ..., e_{2,n})$ выберем так, чтобы $e_{2,i} = e_{1,i}$ для $i = 1, ..., \delta$, $e_{2,g} = e_{1,g} - \epsilon_g$ для $g = \delta + 1, ..., j$, $e_{2,h} = -\epsilon_h$ для $h = t + 1, ..., 2t - j$. Получим, что $\mathbf{e}_1 - \mathbf{e}_2 = \boldsymbol{\epsilon}$ и $\Delta(\mathbf{e}_1, \mathbf{e}_2) = j$ и $\nabla(\mathbf{e}_1, \mathbf{e}_2) = \delta$. Следовательно, $p(\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})) \neq 0$.

Доказательство леммы 4. По условию леммы наступило событие $\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})$, т. е. выбранные векторы $\mathbf{e}_1$ и $\mathbf{e}_2$ неизвестны, но вектор $\boldsymbol{\epsilon} = \mathbf{e}_1 - \mathbf{e}_2$ и число $\delta = \nabla(\mathbf{e}_1, \mathbf{e}_2)$ известны. Поэтому согласно определению события $\mathcal{D}_{n,k}^t$ в этом случае его вероятность — это вероятность случайно выбрать множество τ мощности k во множестве $\underline{n} \setminus \mathrm{supp}(\boldsymbol{\epsilon})$ так, чтобы выполнялось условие (10). Этот выбор должен осуществляться среди $n - w(\boldsymbol{\epsilon})$ нулевых координат вектора $\boldsymbol{\epsilon}$ с учетом того, что $\nabla(\mathbf{e}_1, \mathbf{e}_2) = \delta$. В итоге, ввиду определения события $\mathcal{E}_{n-w(\boldsymbol{\epsilon}),k}^{\delta}$, получаем искомое равенство.

Доказательство леммы 5. Вектор $\mathbf{y}$ будет декодирован правильно в вектор $\boldsymbol{\omega}$, если в векторе $\mathbf{y}$ удастся выбрать $k - k'$ координат из множества $\underline{n}$ так, что выбранные координаты не будут испорчены помехой $\mathbf{x}$, учитывая при этом, что среди n номеров испорчено $w(\mathbf{x})$ штук. Вероятность этого события равна вероятности события $\mathcal{E}_{n,k-k'}^{w(\mathbf{x})}$. Учитывая замечание 1, получаем доказываемое утверждение.

Доказательство леммы 6. Ввиду (20) по определению $\mathcal{U}_n^{t,\delta,l}$ получаем

$$p(\mathcal{U}_n^{t,\delta,l}) = \sum_{\substack{(\boldsymbol{\omega},\mathbf{e}_1,\mathbf{e}_2) \in \mathbb{F}^{k-k'} \times \mathbb{F}^{n,t} \times \mathbb{F}^{n,t}: \\ w(\mathbf{e}_1-\mathbf{e}_2)=l, \nabla(\mathbf{e}_1,\mathbf{e}_2)=\delta}} p_{\boldsymbol{\Psi}}(\boldsymbol{\omega}, \mathbf{e}_1, \mathbf{e}_2) = \\ = \sum_{\boldsymbol{\omega} \in \mathbb{F}^{k-k'}} p_{\boldsymbol{\Omega}}(\boldsymbol{\omega}) \sum_{\substack{(\mathbf{e}_1,\mathbf{e}_2) \in \mathbb{F}^{n,t} \times \mathbb{F}^{n,t}: \\ w(\mathbf{e}_1-\mathbf{e}_2)=l, \nabla(\mathbf{e}_1,\mathbf{e}_2)=\delta}} p_{\mathbf{E}_1}(\mathbf{e}_1) p_{\mathbf{E}_2}(\mathbf{e}_2) = \sum_{\substack{(\mathbf{e}_1,\mathbf{e}_2) \in \mathbb{F}^{n,t} \times \mathbb{F}^{n,t}: \\ w(\mathbf{e}_1-\mathbf{e}_2)=l, \nabla(\mathbf{e}_1,\mathbf{e}_2)=\delta}} p_{\mathbf{E}_1}(\mathbf{e}_1) p_{\mathbf{E}_2}(\mathbf{e}_2).$$

Несложно видеть, что из определения $\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})$, введенного в подразд. 1.2, следует

$$\sum_{\substack{(\mathbf{e}_1,\mathbf{e}_2)\in\mathbb{F}^{n,t}\times\mathbb{F}^{n,t}:\\ w(\mathbf{e}_1-\mathbf{e}_2)=l,\nabla(\mathbf{e}_1,\mathbf{e}_2)=\delta}} p_{\mathbf{E}_1}(\mathbf{e}_1)p_{\mathbf{E}_2}(\mathbf{e}_2) = \sum_{\substack{\boldsymbol{\epsilon}\in\mathbb{F}^{n,\leq 2t}:\\ w(\boldsymbol{\epsilon})=l}} p(\mathcal{H}_n^{t,\delta}(\boldsymbol{\epsilon})).$$

Тогда с учетом (14) получаем доказываемое равенство.

Доказательство леммы 7. Так как по условию леммы событие $\mathcal{U}_n^{t,\delta,l}$ наступило, то известен вектор $\mathbf{y}$ вида (19), для которого также известно, что $w(\mathbf{x}) = l$ и $\nabla(\mathbf{e}_1, \mathbf{e}_2) = \delta$. Тогда наступление события $\mathcal{S}_{n,k}^t$ — это произведение двух событий, где первое событие — нахождение методом декодирования по информационным совокупностям вектора $\mathbf{x}$ при известном $w(\mathbf{x}) = l$ и второе событие — это выбор множества τ, удовлетворяющего условию (10), когда известен вектор $\mathbf{x} = \mathbf{e}_1 - \mathbf{e}_2$ и известно число $\nabla(\mathbf{e}_1, \mathbf{e}_2) = \delta$. Из леммы 5 получаем, что вероятность первого события не превышает $p(\mathcal{E}_{n,k-k'}^l)$, а вероятность второго события равна $p(\mathcal{D}_{n,k}^t|\mathcal{H}_n^{t,\delta}(\mathbf{x})) = p(\mathcal{E}_{n-l,k}^\delta)$ (см. лемму 4).

Список литературы / References

[1] **Rivest, R., Shamir, A., Adleman, L.** A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. 1978. Vol. 21, No. 2. P. 120–126.

[2] **Rabin, M.** Digitalized signatures and public-key functions as intractable as factorization. Cambridge: MIT Lab. for Computer Sci., 1979. 20 p. Available at: http://publications.csail.mit.edu/lcs/pubs/pdf/MIT-LCS-TR-212.pdf (accessed 28.03.2017).

[3] **ElGamal, T.** A public-key cryptosystem and a signature scheme based on discrete logarithms // IEEE Trans. on Inform. Theory. 1985. Vol. 31, No. 4. P. 469–472.

[4] **McEliece, R.J.** A public-key cryptosystem based on algebraic coding theory // JPL Deep Space Network Progress Report. 1978. No. 42. P. 114–116.

[5] eBACS: ECRYPT benchmarking of cryptographic systems. Available at: http://bench.cr.yp.to (accessed 28.03.2017).

[6] **Eisenbarth, T., Guneysu, T., Heyse, S., Paar, Ch.** MicroEliece: McEliece for embedded devices // Lecture Notes in Comput. Sci. 2009. Vol. 5747. P. 49–64.

[7] **Sendrier, N., Tillich, J.-P.** Code-based cryptography: new security solutions against a quantum adversary. 2016. 3 p. Available at: https://hal.archives-ouvertes.fr/hal-01410068/document (accessed 28.03.2017).

[8] **Shor, P.W.** Algorithms for quantum computation: Discrete logarithms and factoring // Proc. 35th Annual Symp. on Foundations of Comput. Sci. IEEE Comput. Soc. Press, 1994. P. 124–134.

[9] **Niebuhr, R., Meziani, M., Bulygin, S., Buchmann, J.** Selecting parameters for secure McEliece-based cryptosystems // Intern. J. of Inform. Security. 2012. Vol. 11, No. 3. P. 137–147.

[10] **Niederreiter, H.** Knapsack-type cryptosystem and algebraic coding theory // Probl. Control and Inform. Theory. 1986. Vol. 15. P. 159–166.

[11] **Gabidulin, E.M., Paramonov A.V., Tretjakov O.V.** Ideals over a non-commutative ring and their application in cryptology // Advances in Cryptology–EUROCRYPT'91 / D.W. Davies (Ed.). Lecture Notes in Comput. Sci. 1991. Vol. 547. P. 482–489.

[12] **Сидельников В.М.** Открытое шифрование на основе двоичных кодов Рида—Маллера // Дискретная математика. 1994. Т. 6, № 2. С. 3–20.
Sidel'nikov, V.M. Open coding based on Reed–Muller binary codes // Discrete Math. and Applications. 1994. Vol. 4, No. 3. P. 191–207.

[13] **Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P.S.L.** MDPC-McEliece: New McEliece variants from moderate density parity-check codes // IEEE Intern. Symp. on Inform. Theory-ISIT '13, Istanbul, Turkey, 2013. IEEE, 2013. P. 2069–2073.

[14] **Деундяк В.М., Косолапов Ю.В.** Криптосистема на индуцированных групповых кодах // Моделирование и анализ информ. систем. 2016. Т. 23, №. 2. С. 137–152.
Deundyak, V.M., Kosolapov, Yu.V. Cryptosystem based on induced group codes // Modeling and Anal. of Inform. Systems. 2016. Vol. 23, No. 2. P. 137–152. (In Russ.)

[15] **Сидельников В.М., Шестаков С.О.** О системе шифрования, основанной на обобщенных кодах Рида — Соломона // Дискретная математика. 1992. Т. 4, №. 3. С. 57–63.
Sidel'nikov, V.M., Shestakov, S.O. On an encoding system constructed on the basis of generalized Reed — Solomon codes // Discrete Math. and Applications. 1992. Vol. 2, No. 4. P. 439–444.

[16] **Wieschebrink, C.** Cryptanalysis of the niederreiter public key scheme based on GRS subcodes // Third Intern. Workshop, PQCrypto. Darmstadt, Germany, May 25–28, 2010. P. 61–72.

[17] **Деундяк В.М., Дружинина М.А., Косолапов Ю.В.** Модификация криптоаналитического алгоритма Сидельникова — Шестакова для обобщенных кодов Рида — Соломона и ее программная реализация // Изв. высших учеб. заведений. Северо-Кавказский регион. Техн. науки. 2006. № 4. С. 15–20.
Deundyak, V.M., Drouzhinina, M.A., Kosolapov, Yu.V. Sidelnikov — Shestakov kriptoanalytical algorithm modification for generalized Reed — Solomon codes and its softwear implementation // Univ. News. North-Caucasian Region. Technical Sci. 2006. No. 4. P. 15–20. (In Russ.)

[18] **Couvreur, A., Gaborit, Ph., Gauthier-Umana, V., Otmani, A., Tillich, J.-P.** Distinguisher-based attacks on public-key cryptosystems using Reed — Solomon codes // Des. Codes Cryptography. 2014. Vol. 73, No. 2. P. 641–666.

[19] **Gibson, J.K.** The security of the gabidulin public key cryptosystem // Advances in Cryptology EUROCRYPT. 1996. Vol. 1070. P. 212–223.

[20] **Overbeck, R.** Structural attacks for public key cryptosystems based on gabidulin codes // J. of Cryptology. 2008. Vol. 21, No. 2. P. 280–301.

[21] **Minder, L., Shokrollahi, A.** Cryptanalysis of the Sidelnikov cryptosystem // Lecture Notes in Comput. Sci. 2007. Vol. 4515. P. 347–360.

[22] **Чижов И.В., Бородин М.А.** Уязвимость криптосистемы Мак-Элиса, построенной на основе двоичных кодов Рида — Маллера // Прикл. дискрет. математика. Приложение. 2013. № 6. С. 48–49.
Chizhov, I.V., Borodin, M.A. Vulnerability of McEliece cryptosystem based on binary Reed — Muller codes // Appl. Discrete Math. 2013. No. 6. P. 48–49. (In Russ.)

[23] **Бородин М.А., Чижов И.В.** Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида — Маллера // Дискрет. матем. 2014. Т. 26, №. 1. С. 10–20.
Chizhov, I.V., Borodin, M.A. Effective attack on the McEliece cryptosystem based on Reed — Muller codes // Discrete Math. and Applications. 2014. Vol. 24, No. 5. P. 273–280.

[24] **Hamdaoui, Y., Sendrier, N.** A non asymptotic analysis of information set decoding. IACR Cryptology ePrint Archive. 2013. P. 162.

[25] **Torres, R.C., Sendrier, N.** Analysis of information set decoding for a sub-linear error weight // Proc. 7th Intern. Workshop, PQCrypto 2016, Fukuoka, Japan, Feb. 24–26, 2016. Springer Intern. Publ., 2016. P. 144–161.

[26] **Berson, T.** Failure of the McEliece public-key cryptosystem under message-resend and related-message attack // Proc. 17th Annual Intern. Cryptology Conf., Santa Barbara, California, USA. Aug. 17–21, 1997. CRYPTO '97, 1997. Vol. 1294. P. 213–220.

[27] **Gore, W.C.** Futher results on product codes // IEEE Trans. on Inform. Theory. 1970. Vol. IT-16, No. 4. P. 446–451.

[28] **Kasami, T., Lin, S.** On majority-logic decoding for duals of primitive polynomial codes // IEEE Trans. on Inform. Theory. 1971. Vol. IT-17, No. 3. P. 322–331.

[29] **Федоренко С.В.** Методы быстрого декодирования линейных кодов. СПб.: ГУАП, 2008. 199 с.
Fedorenko, S.V. Methods of fast decoding for linear codes. SPb.: GUAP, 2008. 199 p. (In Russ.)

[30] **Зубков А.М., Круглов В.И.** Статистические характеристики весовых спектров случайных линейных кодов на GF(p) // Матем. вопр. криптографии. 2014. Т. 5, № 1. С. 27–38.
Zubkov, A.M., Kruglov, V.I. Statistical characteristics of weight spectra of random linear codes over GF(p) // Math. Aspects of Cryptography. 2014. Vol. 5, No. 1. P. 27–38. (In Russ.)

[31] **Косолапов Ю.В., Чекунов Е.С.** Симметричные кодовые криптосистемы на основе кодов в $\mathcal{F}$-метриках // Изв. ЮФУ. Техн. науки. 2010. Т. 112, № 11. С. 106–116.
Kosolapov, Yu.V., Chekunov, E.S. Symmetric cryptosystems based on error correction codes in $\mathcal{F}$-metric // Izvestiya SFedU. Engineering Sci. 2010. Vol. 112, No. 11. P. 106–116. (In Russ.)

[32] **Zhang, K., Tomlinson, M., Ahmed, M.Z.** A modified McEliece public key encryption system with a higher security level // Proc. of IEEE Third Intern. Conf. on Inform. Sci. and Techn. (ICIST). 2013. Vol. 1. P. 1–5.

[33] **Morelos-Zaragoza, R.H.** The art of error correcting coding, 2nd Edition. Chichester, West Sussex, England: John Wiley & Sons, 2006. 572 p.

Поступила в редакцию 31 января 2017 г.,
с доработки — 26 апреля 2017 г.

The use of the tensor product of Reed — Muller codes in asymmetric McEliece type cryptosystem and analysis of its resistance to attacks on the cryptogram

Deundyak, Vladimir M.[1,2], Kosolapov, Yury V.[2,*]

[1]NII "Spetsializirovannye Vychislitel'nye Ustroystva Zashchity i Avtomatika", Rostov-on-Don, 344002, Russia
[2]South Federal University, Rostov-on-Don, 344006, Russia

*Corresponding author: Kosolapov, Yury V., e-mail: itaim@mail.ru

Purpose. Increasing resistance of McEliece cryptosystem against structural attacks (attacks on the key).

Methodology. To solve this problem it is encouraged to apply tensor product codes for which there are majority decoders. In this case, for the tensor product code there is a fast decoder, but there are no effective structural attacks for the McEliece cryptosystem based on the tensor product codes currently.

Findings. The study has revealed that the tensor product codes on the one hand, increases the resistance of cryptographic code to the known attacks on key, but on the other hand reduces the cryptosystem to the attacks on the cryptogram. In this regard, the paper proposes a method for enhancing the stability of cryptosystems such as McEliece to the attacks on the cryptogram by the use of a randomized encryption.

Originality/value. We have studied a method for constructing asymmetric cryptosystems code based on the tensor product codes. As shown by the calculations for tensor product of binary Reed — Muller codes, their resistance to attacks on cryptosystems is lower compared to the resistance of cryptosystems based on the ordinary Reed — Muller codes with comparable lengths. Despite this, cryptosystems based on the tensor product are presently more robust overall because they do not yet experience effective key attacks, while such attacks for cryptosystems based on Reed — Muller codes are already known. The disadvantages of cryptosystems based on tensor product codes include a large key size.

Keywords: tensor product codes, Reed — Muller codes, the McEliece cryptosystem, ciphertext attacks.

Received 31 January 2017
Received in revised form 26 April 2017