© 2019 г. Х.Н. РЗАЕВ, канд.техн.наук (xazail49@mail.ru)
(Азербайджанский государственный университет нефти и промышленности, Баку)

МАТЕМАТИЧЕСКИЕ МОДЕЛИ МОДИФИЦИРОВАННЫХ КРИПТО-КОДОВЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ТКС

Разрабатываются математические модели модифицированных крипто-кодовых средств защиты информации на основе теоретико-кодовой схемы Мак-Элиса с использованием алгеброгеометрических блоковых кодов с укорочением и удлинением информационной посылки, проводится анализ стойкости и энергетических затрат на их программную реализацию.

Ключевые слова: модифицированные крипто-кодовые системы, теоретико-кодовые схемы, алгеброгеометрические коды, информационная скрытность.

DOI: 10.1134/S0005231019070080

1. Введение

Современные требования к обеспечению качества обслуживания пользователей глобальных вычислительных сетей выдвигают новые задачи по интегрированному решению основных критериев качества обслуживания – надежности и безопасности обслуживания. В эпоху высоких технологий появление квантовых компьютеров, которые "используют квантово-механические явления для решения математических задач" [1] ставит под угрозу использование современных стандартов по симметричной и несимметричной криптографии [1–5]. В отчете специалистов Национального института стандартов и технологий США (NIST) о состоянии квантовых вычислений и постквантовой криптографии излагается, что если будут построены крупномасштабные квантовые компьютеры, то они смогут сломать многие криптосистемы с открытым ключом, которые в настоящее время используются. Это серьезно подорвало бы конфиденциальность и целостность цифровых коммуникаций в Интернете и в других местах [1].

В отчете специалистами NIST в условиях постквантовой криптографии (также называемой квантово-устойчивой криптографией) отмечается, что разработка криптографических систем, защищенных как от квантовых, так и от классических компьютеров на основе крипто-кодовых систем Мак-Элиса и Нидеррайтера [1], является одним из перспективных направлений.

Упомянутые крипто-кодовые системы формируют интегрированный механизм обеспечения достоверности и гарантированной криптостойкости в условиях возросшего количества гибридных угроз на составляющие безопасности: информационную безопасность, кибербезопасность и безопасность информации [6–9].

В [5, 8] авторы используют квазициклические коды четности с низкой плотностью (QC–LDPC) [10] и коды с максимальным ранговым расстоянием [5, 8] для построения криптосистем Мак-Элиса и Нидеррайтера соответственно. В [11] рассматривается построение схем Мак-Элиса и Нидеррайтера на основе альтернантных кодов Гоппы. Однако данные коды являются двоичными, а это существенно увеличивает возможность их взлома на основе перестановочного декодера за конечное число шагов и не гарантирует защиту от атаки на основе дробно-линейных преобразований. В [4] авторы предлагают использовать коды Рида–Соломона (РС) при построении несимметричной крипто-кодовой системы (НККС) Мак-Элиса. Однако в [12, 13] показано, что группа автоморфизмов обобщенного кода РС изоморфна группе дробно-линейных преобразований. Применяя это свойство, можно эффективно снять действие используемых маскирующих матриц и восстановить быстрое правило декодирования алгебраического блокового кода [12, 13]. Этому недостатку потенциально могут быть подвержены все подкоды обобщенных кодов РС, включая перечисленные [12, 13].

Предложенные в [14, 15] несимметричные криптосистемы обеспечивают требуемые показатели оперативности, криптостойкости и достоверности передаваемых данных и использование одного программно-аппаратного (аппаратного) механизма в обеспечении требуемых показателей основных критериев качества обслуживания.

Проведенный в [15] анализ программной реализации несимметричной крипто-кодовой системы на теоретико-кодовой системы (ТКС) Нидеррайтера выявил значительные сложности реализации, что существенно затрудняет использование теоретико-кодовых схем для построения криптостойких несимметричных систем. Разработка модифицированных крипто-кодовых систем с использованием модифицированных алгеброгеометрических кодов является перспективным направлением в решении данной технической задачи.

Цель статьи – разработка формального математического описания модифицированных крипто-кодовых средств защиты информации на основе теоретико-кодовой схемы Мак-Элиса с использованием алгеброгеометрических блоковых кодов на основе укорочения/удлинения информационных символов, позволяющих обеспечить снижение объема ключевых данных при сохранении уровня криптостойкости и оценка криптостойкости и энергетических затрат на реализацию таких средств.

Известные способы модификации линейных блоковых кодов наиболее полно рассмотрены в [16–20]. На рис. 1 представлены наиболее распространенные способы модификации.

Удлинение (n, k, d) линейного блокового кода состоит в увеличении длины $n + x$ путем добавления новых информационных символов $k + x$. Расширение (n, k, d) линейного блокового кода состоит в увеличении длины $n + x$ путем добавления новых проверочных символов $r + x$. Выкалывание (n, k, d) линейного блокового кода состоит в уменьшении длины $n - x$ путем уменьшения проверочных символов $r - x$. Укорочение (n, k, d) линейного блокового кода состоит в уменьшении длины $n - x$ путем уменьшения информационных символов $k - x$. Пополнение (n, k, d) линейного блокового кода состоит в уве-

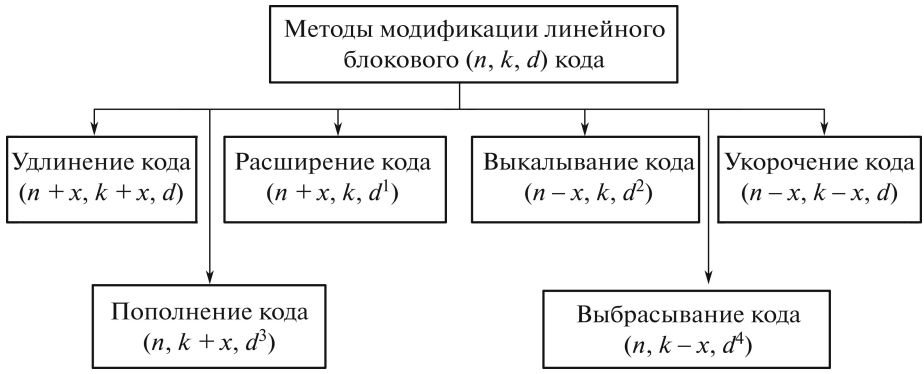

Рис. 1. Способы модификации линейных блоковых кодов.

личении длины информационных символов $k + x$ без увеличения длины кода. Выбрасывание (n, k, d) линейного блокового кода состоит в уменьшении информационных символов $k - x$ без увеличения длины кода.

Потенциальная стойкость теоретико-кодовых схем определяется сложностью декодирования случайного (n, k, d) блокового кода. Следовательно, для построения потенциально стойких теоретико-кодовых схем необходимо использовать способы модификации, не допускающие снижения минимального кодового расстояния. Маскируя код с быстрым алгоритмом декодирования (полиномиальной сложности) под произвольный (случайный) блоковый код, можно представить задачу декодирования для противника как вычислительно сложную задачу (экспоненциальной сложности). Для уполномоченного пользователя системы (имеющего секретный ключ) декодирование – полиномиально разрешимая задача. Сидельниковым в [12, 13] предложен эффективный способ взлома несимметричных схем Мак-Элиса и Нидеррайтера, построенных на обобщенных кодах Рида–Соломона. Отмечается, что одним из перспективных направлений в развитии потенциально стойких теоретико-кодовых схем являются схемы, построенные с использованием алгеброгеометрических или каскадных кодов [12]. Алгебраические блоковые коды, построенные по алгебраическим кривым (алгеброгеометрические коды), обладают хорошими асимптотическими характеристиками. Их применение в дискретных симметричных каналах позволяет получить наибольший энергетический выигрыш от кодирования (среди алгебраических блоковых кодов) и эффективно бороться с возникающими пакетами ошибок. Способы удлинения и укорочения линейных блоковых кодов, не изменяя минимального расстояния, позволяют строить стойкие к взлому несимметричные крипто-кодовые системы с меньшим объемом криптограммы и ключевых данных.

В соответствии с формальным математическим описанием несимметричных крипто-кодовых систем на основе ТКС Мак-Элиса в режиме прямого исправления ошибок и автоматического переспроса, предложенных в [14], предлагаются математические модели модифицированных несимметричных криптосистем на основе ТКС Мак-Элиса, позволяющих снизить энергетические затраты на их реализацию.

2. Математическая модель модифицированной несимметричной крипто-кодовой системы защиты информации

2.1. С использованием алгеброгеометрических блоковых кодов на основе теоретико-кодовой схемы Мак-Элиса на основе укорочения (сокращения информационных символов) эта модель формально задается совокупностью следующих элементов [14]:

— множество открытых текстов

$$M = \left\{M_1, M_2, \ldots, M_{q^k}\right\}, \quad \text{где} \quad M_i = \left\{I_0, I_{h_1}, \ldots, I_{h_j}, I_{k-1}\right\} \; \forall I_j \in GF\,(q),$$

h_j – информационные символы, равные нулю, $|h| = \frac{1}{2}k$, т.е. $I_i = 0 \; \forall I_i \in h$;

— множество закрытых текстов (кодограмм)

$$C = \left\{C_1, C_2, \ldots, C_{q^k}\right\}, \quad \text{где} \quad C_i = \left(c^*_{X_0}, c^*_{h_1}, \ldots, c^*_{h_j}, c^*_{X_{n-1}}\right) \; \forall c^*_{X_j} \in GF\,(q);$$

— множество прямых отображений (на основе использования открытого ключа – порождающей матрицы)

$$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_s\}, \quad \text{где} \quad \varphi_i : \; M \to C_{k-h_j}, \quad i = 1, 2, \ldots, s;$$

— множество обратных отображений (на основе использования закрытого (личного) ключа – матриц маскировки)

$$\varphi^{-1} = \left\{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_s^{-1}\right\}, \quad \text{где} \quad \varphi_i^{-1} : \; C_{k-h_j} \to M, \quad i = 1, 2, \ldots, s;$$

— множество ключей, параметризирующих прямые отображения (открытый ключ уполномоченного пользователя),

$$K_{a_i} = \{K_{1\,a_i}, K_{2\,a_i}, \ldots K_{s\,a_i}\} = \left\{G_X^{EC_1} a_i, G_X^{EC_2} a_i, \ldots, G_X^{EC_s} a_i\right\},$$

где $G_X^{EC_s} a_i$ – порождающая $(n \times k)$-матрица замаскированного под случайный код алгеброгеометрического блокового (n, k, d) кода с элементами из $GF\,(q)$, т.е.

$$\varphi_i : \; M \xrightarrow{K_{i_{a_i}}} C_{K-h_j}, \quad i = 1, 2, \ldots, s;$$

a_i – набор коэффициентов многочлена кривой $a_1, \ldots, a_6 \; \forall a_i \in GF(q)$, однозначно задающий конкретный набор точек кривой из пространства P^2;

— множество ключей, параметризирующих обратные отображения (личный (закрытый) ключ уполномоченного пользователя),

$$K^* = \{K_1^*, K_2^*, \ldots, K_s^*\} = \left\{\{X, P, D\}_1, \{X, P, D\}_2, \; \ldots, \{X, P, D\}_s\right\},$$
$$\{X, P, D\}_i = \{X^i, P^i, D^i\},$$

где X^i – маскирующая невырожденная случайно равновероятно сформированная источником ключей $(k \times k)$-матрица с элементами из $GF\,(q)$; P^i –

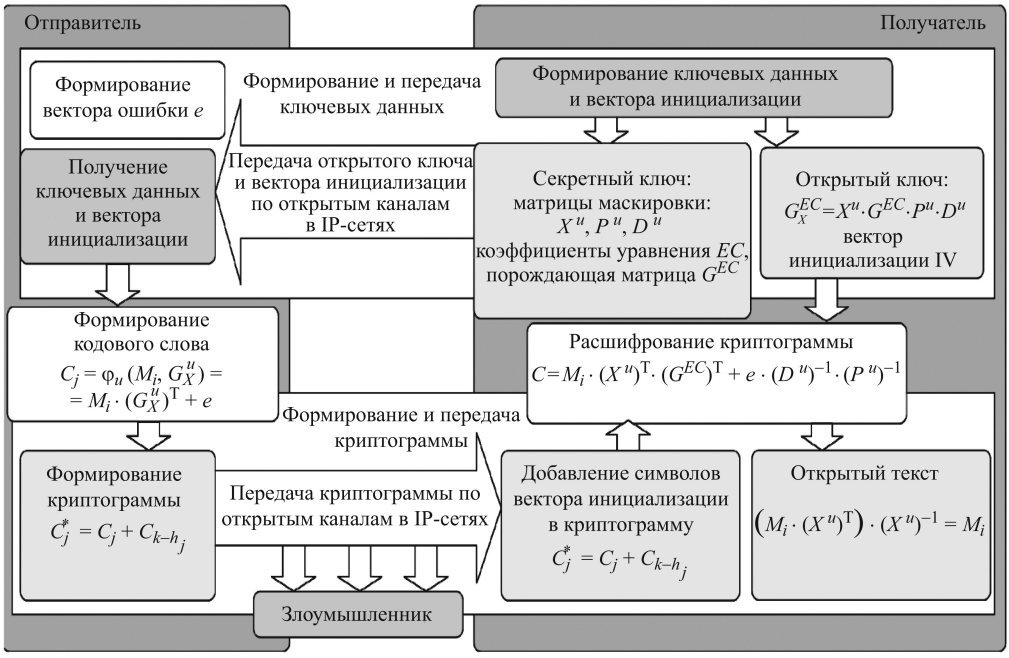

Рис. 2. Протокол обмена информацией в режиме реального времени с использованием модифицированной ТКС Мак-Элиса с укороченными ЕС.

перестановочная случайно равновероятно сформированная источником ключей $(n\times n)$-матрица с элементами из $GF(q)$; D^i – диагональная сформированная источником ключей $(n\times n)$-матрица с элементами из $GF(q)$, т.е. $\varphi_i^{-1}: C\xrightarrow{K_i^*} M$, $i=1,2,\ldots,s$, сложность выполнения обратного отображения φ_i^{-1} без знания ключа $K_i^*\in K^*$ сопряжена с решением теоретико-сложностной задачи декодирования случайного кода (кода общего положения). Таким образом, в качестве личного (закрытого) ключа (KR абонента) в модифицированной крипто-кодовой системе (МККС) Мак-Элиса выступают матрицы маскировки X, P, D и порождающая матрица G эллиптического кода, а в качестве открытого (общедоступного ключа) (KU абонента) используется сформированная путем перемножения матриц маскировки и порождающей матрицы матрица эллиптического кода $G_X^{EC_i}a_i$, вектор инициализации, определяющий места укорочения (удаления символов в кодовом слове) и вектор ошибки являются сеансовыми ключами отправителя. Структурная схема протокола обмена информацией в режиме реального времени с использованием модифицированной ТКС Мак-Элиса с укороченными эллиптическими кодами (EC) представлена на рис. 2.

Исходными данными при описании рассмотренной несимметричной крипто-кодовой системы защиты информации являются:

— алгеброгеометрический блоковый (n,k,d) код C_{k-h_j} над $GF(q)$, т.е. множество кодовых слов $C_i\in C_{k-h_j}$ таких, что выполняется равенство $C_iH^{\mathrm{T}}=0$, где H проверочная матрица алгеброгеометрического блокового кода;

— a_i — набор коэффициентов многочлена кривой $a_1, \ldots, a_6$ $\forall a_i \in GF(q)$, однозначно задающий конкретный набор точек кривой из пространства P^2, для формирования порождающей матрицы в соответствии с (14);

— h_j — информационные символы, равные нулю, $|h| = \frac{1}{2}k$, т.е. $I_i = 0$ $\forall I_i \in h$;

— маскирующие матричные отображения, заданные множеством матриц $\{X,\ P,\ D\}_i$, где X — невырожденная $(k \times k)$-матрица над $GF(q)$, P — перестановочная $(n \times n)$-матрица над $GF(q)$ с одним ненулевым элементом в каждой строке и в каждом столбце матрицы, D — диагональная $(n \times n)$-матрица над $GF(q)$ с ненулевыми элементами на главной диагонали.

В несимметричной крипто-кодовой системе на основе ТКС Мак-Элиса модифицированный (укороченный) алгеброгеометрический (n, k, d) код $C^*_{k-h_j}$ с быстрым алгоритмом раскодирования маскируется под случайный (n, k, d) код C_{k-h_j} посредством умножения порождающей матрицы G^{EC} кода C_{k-h_j} на хранящиеся в секрете маскирующие матрицы X^u, P^u и D^u [14], обеспечивающий формирование открытого ключа уполномоченного пользователя:

$$G^{ECu}_X = X^u G^{EC} P^u D^u, \quad u \in \{1, 2, \ldots, s\},$$

где G^{EC} — порождающая $(n \times k)$-матрица алгеброгеометрического блокового (n, k, d) кода с элементами из $GF(q)$, построенная на основе использования выбранных пользователем коэффициентов многочлена кривой $a_1, \ldots, a_6$ $\forall a_i$ $GF(q)$, однозначно задающих конкретный набор точек кривой из пространства P^2.

Формирование закрытого текста $C_j \in C_{k-h_j}$ по введенному открытому тексту $M_i \in M$ и заданному открытому ключу G^{ECu}_X a_i, $u \in \{1, 2, \ldots, s\}$, осуществляется путем формирования кодового слова замаскированного кода с добавлением к нему случайно сформированного вектора $e \in (e_0, e_1, \ldots, e_{n-1})$:

$$C_j = \varphi_u\left(M_i, G^u_X\right) = M_i \cdot \left(G^u_X\right)^{\mathrm{T}} + e,$$

причем вес Хемминга (число ненулевых элементов) вектора e не превышает исправляющей способности используемого алгебраического блокового кода:

$$0 \le w\left(e\right) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

$\lfloor x \rfloor$– целая часть вещественного числа x.

Для каждого формируемого закрытого текста $C_j \in C_{k-h_j}$ соответствующий вектор $e \in (e_0, e_1, \ldots, e_{n-1})$ выступает в качестве одноразового сеансового ключа, т.е. для конкретного E_j вектор e формируется случайно, равновероятно и независимо от других закрытых текстов.

В канал связи поступает $C^*_j = C_j - C_{k-h_j}$.

На приемной стороне уполномоченный пользователь, знающий правило маскировки и количество нулевых информационных символов, может воспользоваться быстрым алгоритмом раскодирования алгеброгеометрического кода (полиномиальной сложности) для восстановления открытого текста [14]:

$$M_i = \varphi^{-1}_u\left(C^*_j, \{X, P, D\}_u\right).$$

Для восстановления открытого текста уполномоченный пользователь добавляет нулевые информационные символы

$$C_j^* = C_j + C_{k-h_j},$$

с восстановленного закрытого текста C_j снимает действие секретных перестановочной и диагональной матриц P^u и D^u:

$$C = C_j^* \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \left(M_i \cdot (G_X^u)^{\mathrm{T}} + e\right) \cdot (D^u)^{-1} \cdot (P^u)^{-1} =$$
$$= \left(M_i \cdot (X^u \cdot G \cdot P^u \cdot D^u)^{\mathrm{T}} + e\right) \cdot (D^u)^{-1} \cdot (P^u)^{-1} =$$
$$= M_i \cdot (X^u)^{\mathrm{T}} \cdot (G)^{\mathrm{T}} \cdot (P^u)^{\mathrm{T}} \cdot (D^u)^{\mathrm{T}} \cdot (D^u)^{-1} \cdot (P^u)^{-1} + e \cdot (D^u)^{-1} \cdot (P^u)^{-1} =$$
$$= M_i \cdot (X^u)^{\mathrm{T}} \cdot (G)^{\mathrm{T}} + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}$$

и раскодирует полученный вектор по алгоритму Берлекэмпа–Месси [16, 17]:

$$C = M_i \cdot (X^u)^{\mathrm{T}} \cdot \left(G^{EC}\right)^{\mathrm{T}} + e \cdot \ (D^u)^{-1} \cdot (P^u)^{-1},$$

т.е. избавляется от второго слагаемого и от сомножителя $(G)^{EC^{\mathrm{T}}}$ в первом слагаемом в правой части равенства, после чего снимает действие матрицы маскирования X^u. Для этого полученный результат раскодирования $M_i \cdot (X^u)^{\mathrm{T}}$ следует умножить на $(X^u)^{-1}$:

$$\left(M_i \cdot (X^u)^{\mathrm{T}}\right) \cdot (X^u)^{-1} = M_i.$$

Полученное решение и есть открытый текст M_i.

2.2. Математическая модель модифицированной несимметричной криптокодовой системы защиты информации с использованием алгеброгеометрических блоковых кодов на основе теоретико-кодовой схемы Мак-Элиса на основе удлинения (увеличения информационных символов).

Эта модель формально задается совокупностью следующих элементов:

— множество открытых текстов

$$M = \left\{M_1, M_2, \ldots, M_{q^k}\right\}, \quad \text{где} \quad M_i = \left\{I_0, I_{h_{r_1}}, \ldots I_{h_{r_j}}, I_{k-1}\right\} \ \forall I_j \in GF\,(q)\,,$$

h_j — информационные символы, равные нулю, $|h| = \frac{1}{2}k$, т.е. $I_i = 0 \ \ \forall I_i \in h$;
h_r — информационные символы удлинения k, $|h| = \frac{1}{2}k$;

— множество закрытых текстов (кодограмм)

$$C = \{C_1, C_2, \ldots, C_{q^k}\}, \quad \text{где} \quad C_i = (c^*_{X_0}, c^*_{h_{r_1}}, \ldots, c^*_{h_{r_j}}, c^*_{X_{n-1}}) \ \forall c^*_{X_j} \in GF(q);$$

— множество прямых отображений (на основе использования открытого ключа – порождающей матрицы)

$$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_s\}, \quad \text{где} \quad \varphi_i : \ M \to C_{h_r}, \quad i = 1, 2, \ldots, s;$$

— множество обратных отображений (на основе использования закрытого (личного) ключа – матриц маскировки)

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_s^{-1}\}, \quad \varphi_i^{-1} : C_{h_r} \to M, \quad i = 1, 2, \ldots, s;$$

— множество ключей, параметризирующих прямые отображения (открытый ключ уполномоченного пользователя),

$$K_{a_i} = \{K_{1\,a_i}, K_{2\,a_i}, \ldots, K_{s\,a_i}\} = \left\{G_X^{EC_1}\ a_i, G_X^{EC_2}\ a_i, \ldots, G_X^{EC_s}\ a_i\right\},$$

где $G_X^{EC_s}\, a_i$ – порождающая $(n \times k)$-матрица замаскированного под случайный код алгеброгеометрического блокового (n, k, d) кода с элементами из $GF(q)$, т.е.

$$\varphi_i : M \xrightarrow{K_{i_{a_i}}} C_{h_r}, \quad i = 1, 2, \ldots, s;$$

a_i – набор коэффициентов многочлена кривой $a_1, \ldots, a_6\ \forall a_i \in GF(q)$, однозначно задающий конкретный набор точек кривой из пространства P^2;

— множество ключей, параметризирующих обратные отображения (личный (закрытый) ключ уполномоченного пользователя),

$$K^* = \{K_1^*, K_2^*, \ldots, K_s^*\} = \left\{\{X, P, D\}_1, \{X, P, D\}_2, \ldots, \{X, P, D\}_s\right\},$$
$$\{X, P, D\}_i = \{X^i, P^i, D^i\},$$

где X^i – маскирующая невырожденная случайно равновероятно сформированная источником ключей $(k \times k)$-матрица с элементами из $GF(q)$; P^i — перестановочная случайно равновероятно сформированная источником ключей $(n \times n)$-матрица с элементами из $GF(q)$; D^i — диагональная, сформированная источником ключей $(n \times n)$-матрица с элементами из $GF(q)$, т.е.

$$\varphi_i^{-1} : C \xrightarrow{K_i^*} M, \quad i = 1, 2, \ldots, s.$$

Сложность выполнения обратного отображения φ_i^{-1} без знания ключа $K_i^* \in K^*$ сопряжена с решением теоретико-сложностной задачи декодирования случайного кода (кода общего положения).

Исходными данными при описании рассмотренной несимметричной крипто-кодовой системы защиты информации являются параметры, описанные в модели на основе укорочения. Таким образом, отличительной особенностью МККС Мак-Элиса на модифицированных удлиненных эллиптических кодах от МККС на укороченных ЕС является использование мест укорочения для заполнения символами открытого текста. Протокол обмена с использованием данной МККС представлен на рис. 3.

В несимметричной крипто-кодовой системе на основе ТКС Мак-Элиса модифицированный (удлиненный) алгеброгеометрический (n, k, d) код C_{h_r} с быстрым алгоритмом раскодирования маскируется под случайный (n, k, d)

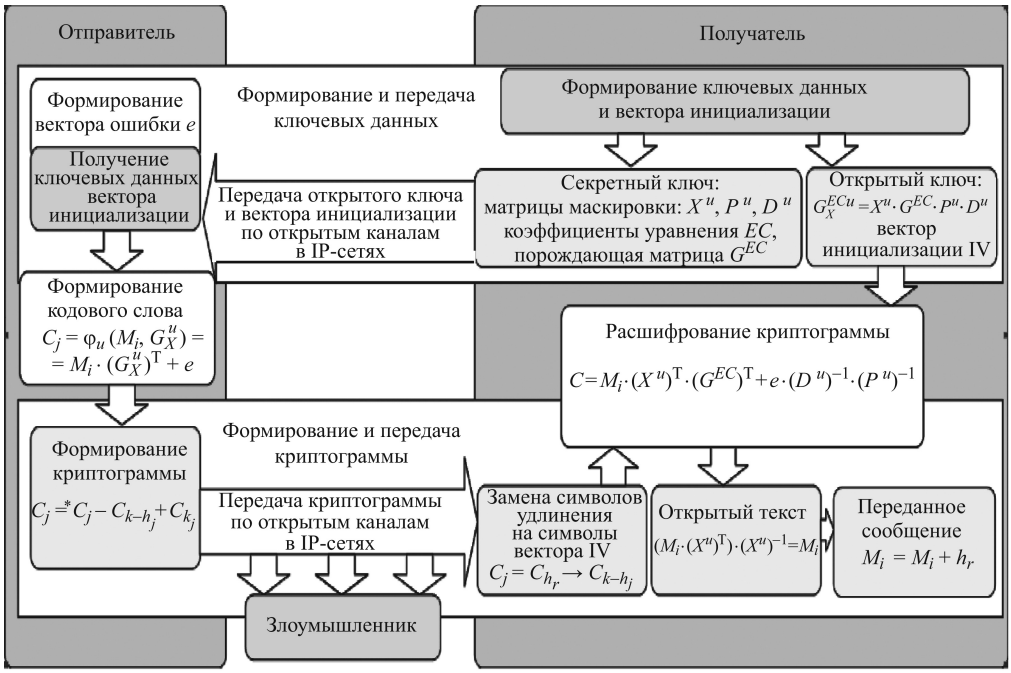

Рис. 3. Протокол обмена информацией в режиме реального времени с использованием модифицированной ТКС Мак-Элиса с удлиненными ЕС.

код $C_{h_r}^*$ посредством умножения порождающей матрицы G^{EC} кода C_{k-h_j} на хранящиеся в секрете маскирующие матрицы X^u, P^u и D^u, обеспечивающий формирование открытого ключа уполномоченного пользователя:

$$G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u, \quad u \in \{1, 2, \ldots, s\},$$

где G^{EC} – порождающая $(n \times k)$-матрица алгеброгеометрического блокового (n, k, d) кода с элементами из $GF(q)$, построенная на основе использования выбранных пользователем коэффициентов многочлена кривой $a_1, \ldots, a_6$ $\forall a_i \in GF(q)$, однозначно задающих конкретный набор точек кривой из пространства P^2.

Формирование закрытого текста $C_j \in C_{h_r}$ по введенному открытому тексту $M_i \in M$ и заданному открытому ключу $G_X^{EC_u}\, a_i$, $u \in \{1, 2, \ldots, s\}$, осуществляется путем формирования укороченного кодового слова, а затем удлинения замаскированного кода с добавлением к нему случайно сформированного вектора $e = (e_0, e_1, \ldots, e_{n-1})$:

$$C_j = \varphi_u(M_i, G_X^u) = M_i \cdot (G_X^u)^{\mathrm{T}} + e.$$

Для каждого формируемого закрытого текста $C_j \in C_{h_r}$ соответствующий вектор $e = (e_0, e_1, \ldots, e_{n-1})$ выступает в качестве одноразового сеансового ключа, т.е. для конкретного E_j вектор e формируется случайно, равновероятно и независимо от других закрытых текстов.

В канал связи поступает $C_j^* = C_j - C_{k-h_j} + C_{h_r}$.

На приемной стороне уполномоченный пользователь, знающий правило маскировки и количество и места нулевых информационных символов, может воспользоваться быстрым алгоритмом раскодирования алгеброгеометрического кода (полиномиальной сложности) для восстановления открытого текста:

$$M_i = \varphi_u^{-1}\left(C_j^*, \{X, P, D\}_u\right).$$

Для восстановления открытого текста уполномоченный пользователь заменяет символы удлинения на нулевые информационные символы

$$C_j^* = C_{h_r} \to C_{k-h_j},$$

с восстановленного закрытого текста C_j снимает действие секретных перестановочной и диагональной матриц P^u и D^u:

$$C = C_j^* \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \left(M_i \cdot (G_X^u)^{\mathrm{T}} + e\right) \cdot (D^u)^{-1} \cdot (P^u)^{-1} =$$
$$= \left(M_i \cdot (X^u \cdot G \cdot P^u \cdot D^u)^{\mathrm{T}} + e\right) \cdot (D^u)^{-1} \cdot (P^u)^{-1} =$$
$$= M_i \cdot (X^u)^{\mathrm{T}} \cdot (G)^{\mathrm{T}} \cdot (P^u)^{\mathrm{T}} \cdot (D^u)^{\mathrm{T}} \cdot (D^u)^{-1} \cdot (P^u)^{-1} + e \cdot (D^u)^{-1} \cdot (P^u)^{-1} =$$
$$= M_i \cdot (X^u)^{\mathrm{T}} \cdot (G)^{\mathrm{T}} + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}$$

и раскодирует полученный вектор по алгоритму Берлекэмпа–Месси [16; 17]:

$$C = M_i \cdot (X^u)^{\mathrm{T}} \cdot \left(G^{EC}\right)^{\mathrm{T}} + e \cdot (D^u)^{-1} \cdot (P^u)^{-1},$$

т.е. избавляется от второго слагаемого и от сомножителя $(G)^{EC^{\mathrm{T}}}$ в первом слагаемом в правой части равенства, после чего снимает действие матрицы маскирования X^u. Для этого полученный результат раскодирования M_i^* следует умножить на $(X^u)^{-1}$:

$$M_i^* \cdot (X^u)^{\mathrm{T}} \cdot (X^u)^{-1} = M_i.$$

Полученное решение – открытый текст M_i, к которому добавляются символы удлинения: $M_j = M_i + h_r$ – передаваемое сообщение.

3. Оценка энергетических затрат в предлагаемой модифицированной несимметричной крипто-кодовой системе Мак-Элиса

Для оценки временны́х и скоростных показателей принято использовать единицу измерения *cpb*, где *cpb* (*cycles per byte*) – число тактов процессора, которое необходимо потратить для обработки одного байта входящей информации.

Энергетические затраты на обработку крипто-кодовой системой одного байта входной информации вычисляем по выражению

$$Per = Utl * CPU\_clock/Rate,$$

Таблица 1. Результаты исследований зависимости длины кодовой последовательности в НККС Мак-Элиса от количества тактов процессора

Длина кодовой последовательности		Mac-Elis			Mac-Elis на укороченных кодах			Mac-Elis на удлиненных кодах		
		10	100	1000	10	100	1000	10	100	1000
Количество вызовов функций, реализующих элементарные операции	Чтение символа	11 018 042	30 800 328	80 859 933	10 294 397	28 750 457	76 759 874	1143 2131	33 460 317	82 473 442
	Сравнение строк	3 663 356	10 199 898	26 364 634	3 406 921	9 246 748	254 78 498	3 673 756	12 119 867	29 469 389
	Конкатенация строк	1 834 983	5 125 564	13 415 329	1 705 544	5 045 748	12 379 422	1 947 681	6 114 478	14 456 729
Сумма элементарных групповых операций		16 516 381	46 125 790	120 639 896	15 406 862	43 042 953	114 617 794	1705 3568	51 694 662	126 399 560
Длительность выполнения функций* в тактах процессора	Чтение символа	297 487	831 609	2 183 218	295 374	810 478	2 001 167	300 479	843 705	2 745 148
	Сравнение строк	197 821	550 794	1 423 690	178 814	531 379	1 248 684	213 478	561 754	1 739 170
	Конкатенация строк	544 990	1 522 293	3 984 353	544 990	1 328 114	3 586 486	578 174	1 647 638	4 007 883
Сумма элементарных групповых операций		1 040 298	2 904 696	7 591 261	1 006 781	2 749 548	7 247 488	1 092 131	3 053 097	8 492 201
Длительность выполнения**, мс		0,55	1,53	4	0,52	1,37	3,4	0,56	1,55	4,1

*длительность 1000 операций в тактах процессора: чтение символа – 27 тактов, сравнение строк – 54 такта, конкатенация строк – 297 тактов;

**для расчета взят процессор с тактовой частотой 2 ГГц с учетом загрузки операционной системы 5%.

где Utl – утилизация ядра процессора (%); CPU_clock – время выполнения одного такта процессора; $Rate$ – пропускная способность алгоритма (байт/с).

В табл. 1 приведены результаты исследований зависимости длины кодовой последовательности алгеброгеометрического кода в крипто-кодовой системе Мак-Элиса от количества тактов процессора на выполнение элементарных операций в программной реализации крипто-кодовых систем.

В табл. 2 приведены результаты исследований оценки временны́х и скоростных показателей процедур формирования и раскодирования информации в крипто-кодовых системах на основе НККС и МККС Мак-Элиса.

Анализ табл. 1 и 2 показывает, что использование модифицированных (укороченных/удлиненных) эллиптических кодов позволяет сохранить объе-

Таблица 2. Результаты исследований оценки временны́х и скоростных показателей процедур формирования и раскодирования информации

Крипто-кодовые системы	Длина кодовой последовательности	Пропускная способность алгоритма, Rate, (байт/с)	Утилизация ядра процессора, (%)	Сложность алгоритма, Per, с/байт
НККС Мак-Элиса	100	46 125 790	56	61,5
	1000	120 639 896	56	62,0
МККС Мак-Элиса на удлиненных эллиптических кодах	100	51 694 662	56	61,7
	1000	126 399 560	56	62,2
МККС Мак-Элиса на укороченных эллиптических кодах	100	52 721 778	56	61,5
	1000	127 389 928	56	62,1

мы передаваемых данных в несимметричной крипто-кодовой системе Мак-Элиса, но при этом обеспечить требуемый уровень криптостойкости при реализации над меньшим полем $GF\left(2^6 - 2^8\right)$ за счет использования энтропии вектора инициализации h_r.

Исследуем достоверность и информационную скрытность, обеспечиваемые модифицированными крипто-кодовыми системами на эллиптических кривых. Зафиксируем (n, k, d) эллиптический код над $GF(q)$. Зададим модифицированную крипто-кодовую схему на основе ТКС Мак-Элиса на модифицированных (удлиненных) кодах. Зададим сеансовый ключ e – вектор ошибок, который добавляется к кодовому слову при формировании кодограммы. Пусть $w(e) \le t$, $t = [(d-1)/2]$. Обозначим долю веса вектора ошибок e символом $\rho = w(e)/t$. Тогда потенциальная стойкость теоретико-кодовой схемы с эллиптическими кодами будет определяться величиной $\rho \cdot t$, а помехоустойчивость передаваемых кодограмм – величиной $(1-\rho)\cdot t$. Сложность взлома предлагаемых модифицированных систем определим выражением сложности анализа декодирования случайного кода перестановочным декодером:

$$I_{K+} = N_{\text{покрытия}} \cdot n \cdot r,$$

где

$$N_{\text{покрытия}} \ge \frac{C_n^t}{C_{n-k}^t} = \frac{n(n-1)\ldots(n-t-1)}{(n-k)(n-k-1)\ldots(n-k-t-1)}.$$

Помехоустойчивость определяется минимальным соотношением сигнал/шум, необходимым для обеспечения требуемой достоверности. Зафиксируем соотношение сигнал/шум и вид модуляции. Предположим, что передача цифровых сообщений осуществляется по дискретному каналу без памяти, т.е. ошибки в последовательно передаваемых кодовых символах происходят независимо с вероятностью $P_{\text{о}}$. Тогда вероятность ошибки кратности i на длине блока n будет равна [16–20]:

$$P_i = C_n^i P_{\text{о}}^i \left(1 - P_{\text{о}}\right)^{n-1}.$$

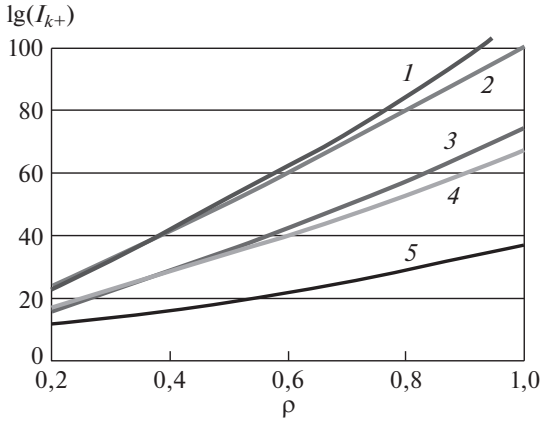

Рис. 4. Зависимость сложности взлома $I_{k+}(\rho)$ над $GF\left(2^{10}\right)$: *1* – $R = 0{,}5$; *2* – $R = 0{,}75$; *3* – $R = 0{,}9$; *4* – $R = 0{,}25$; *5* – $R = 0{,}1$.

Если процедура раскодирования позволяет исправить $t = [(d-1)/2]$ ошибок, то вероятность ошибочного раскодирования равна:

$$P_{\text{ош}} = \sum_{i=t+1}^{n} P_i = \sum_{i=t+1}^{n} C_n^i P_{\text{о}}^i \left(1 - P_{\text{о}}\right)^{n-i}.$$

При интегрированном решении задач достоверности и информационной скрытности передачи данных модифицированная крипто-кодовая система будет исправлять $(1-\rho)\cdot t$ возникших ошибок, следовательно:

$$P_{\text{ош}} = \sum_{i=(1-\rho)t+1}^{n} P_i = \sum_{i=(1-\rho)t+1}^{n} C_n^i P_{\text{о}}^i \left(1 - P_{\text{о}}\right)^{n-i}.$$

Зафиксируем $GF(2^{10})$ и $P_{\text{о}} = 10^{-3}$. На рис. 4 приведены зависимости сложности взлома теоретико-кодовой схемы перестановочным декодером $I_{k+}(\rho)$ при использовании эллиптических кодов с относительной скоростью R.

На рис. 5 приведены зависимости вероятности ошибки раскодирования $P_{\text{ош}}(\rho)$ при интегрированном решении задач достоверности и информационной скрытности.

Как видно из зависимостей, приведенных на рис. 4 и 5, модифицированные крипто-кодовые системы на основе ТКС Мак-Элиса обладают высокими показателями достоверности и информационной скрытности. Повышение показателя ρ ведет, с одной стороны, к увеличению стойкости (надежности) схемы, а с другой – к снижению ее помехоустойчивости. Исследуем интегрированное повышение достоверности и информационной скрытности передачи данных с использованием предлагаемых систем.

На рис. 6 представлены сводные зависимости вероятности ошибки раскодирования и сложности взлома теоретико-кодовой схемы с эллиптическими кодами для различных R при $\rho = 0{,}9$.

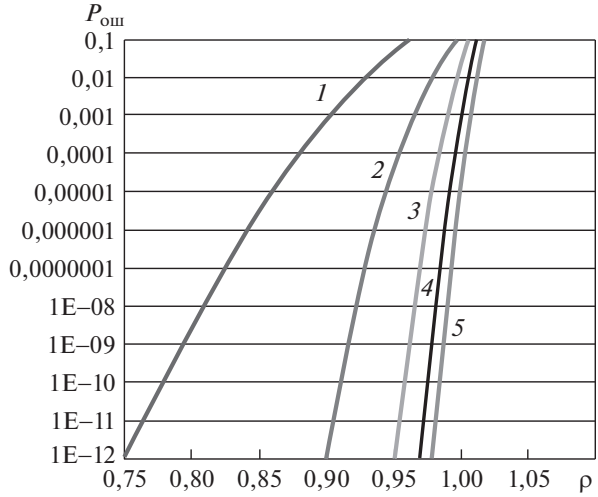

Рис. 5. Зависимость вероятности ошибки декодирования $P_{\text{ош}}(\rho)$ над $GF\left(2^{10}\right)$: *1* – $R = 0{,}1$; *2* – $R = 0{,}25$; *3* – $R = 0{,}9$; *4* – $R = 0{,}75$; *5* – $R = 0{,}5$.

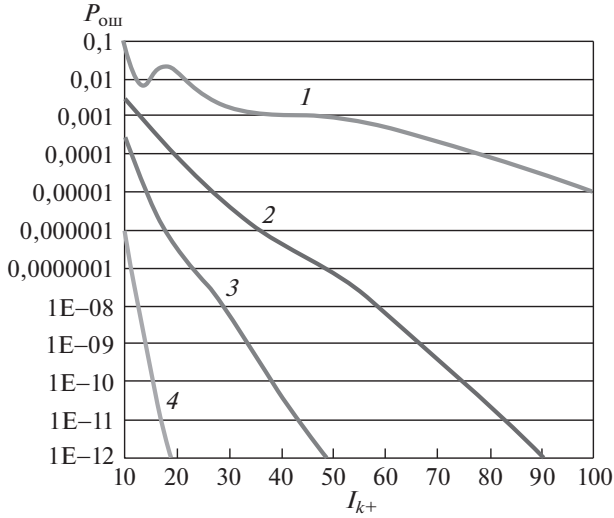

Рис. 6. Сводные зависимости вероятности ошибки раскодирования и сложности взлома $P_{\text{ош}}(I_{K+})$ для $\rho = 0{,}9$: *1* – $R = 0{,}9$; *2* – $R = 0{,}75$; *3* – $R = 0{,}5$; *4* – $R = 0{,}25$.

Как видно из зависимостей, приведенных на рис. 6, предложенные модифицированные крипто-кодовые системы на основе ТКС Мак-Элиса обеспечивают высокие показатели стойкости и достоверности обрабатываемой и передаваемой информации. Их применение позволит использовать открытые каналы IP-сетей для передачи конфиденциальной (коммерческой) информации в режиме реального времени, обеспечивая требуемые показатели безопасности и достоверности.

4. Заключение

Таким образом, предложено формальное математическое описание модифицированных крипто-кодовых средств защиты информации на основе ТКС Мак-Элиса с использованием алгеброгеометрических блоковых кодов на основе укорочения/удлинения информационных символов, позволяющее разработать практические алгоритмы и провести исследование энергетических затрат их реализации.

Передача ключевой последовательности при использовании модифицированной НККС Мак-Элиса на основе укороченных кодов позволяет использовать открытые каналы связи коммуникационных систем и существенно снизить объемы ключевых последовательностей, хранящихся у пользователей данной системы. Оценка сложности программной реализации криптокодовых средств защиты информации на основе ТКС Мак-Элиса подтверждает предположение о снижении вычислительных затрат на вычисление криптограммы/кодограммы и необходимости хранения ключевых данных (открытого ключа) уполномоченным пользователем. Использование удлиненных эллиптических кодов позволяет увеличить объем передаваемых данных на h_r символов, обеспечивая при этом стойкость криптосистемы при ее формировании в поле $GF\left(2^6 - 2^8\right)$, что существенно снижает энергетические затраты на ее реализацию и позволяет ее использование в мобильных приложениях.

Проведенные исследования применения доли веса вектора ошибок позволяют варьированием основных показателей каналов связи коммуникационной системы усиливать один из показателей интегрированного механизма – достоверность или безопасность.

СПИСОК ЛИТЕРАТУРЫ

1. NISTIR 8105. Report on Post-Quantum Cryptography. Режим доступа: http://dx.doi.org/10.6028/NIST.IR.8105
2. *Dinh H., Moore C., Russell A.* McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks. Режим доступа: https://dl.acm.org/citation.cfm?id=2033093
3. *Simon de Vries.* Achieving 128-Bit Security against Quantum Attacks in OpenVPN. 2016. p. 1–16. Режим доступа: https://essay.utwente.nl/.../2016-08-09%20msc%20thesis%
4. *Baldi M., Bianchi M., Chiaraluce F., et al.* Enhanced Public Key Security for the McEliece Cryptosystem. Режим Доступа: https://arxiv.org/abs/1108.2462
5. *Rossi M., Hamburg M., Hutter M., Marson M.E.* A Side-Channel Assisted Cryptanalytic Attack Against QcBits. Режим доступа: https://link.springer.com/chapter/10.1007/978-3-319-66787-4_1
6. *Грищук Р.В., Даник Ю.Г.* Основи кібербезпеки / За заг. ред. проф. Даника Ю.Г. Житомир : ЖНАЕУ, 2016.
7. *Евсеев С.* Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины / Науково-технічний журн. "Безпека інформації". 2016. Т. 22. № 3. С. 297–309.

8. *Zhang G., Cai S., Ma C., Zhang D.* Secure Error-Correcting (SEC) Schemes for Network Coding Through McEliece Cryptosystem. Режим доступа:
https://link.springer.com/article/10.1007/S10586-017-1294-5
9. *Zhang G., Cai S., Ma C., Zhang D.* Universal Secure Error-Correcting (SEC) Schemes for Network Coding via McEliece Cryptosystem Based on QC-LDPC Codes. Режим доступа:
https://link.springer.com/article/10.1007/s10586-017-1354-x
10. *Cho J.Y., Griesser H., Rafique D.* A McEliece-Based Key Exchange Protocol for Optical Communication Systems. Режим доступа:
https://link.springer.com/chapter/10.1007%2f978-3-319-59265-7_8
11. *Morozov K., Roy P.S., Sakurai K.* On Unconditionally Binding Code-Based Commitment Schemes. Режим доступа:
https://dl.acm.org/citation.cfm?id=3022327&dl=ACM&coll=DL
12. *Сидельников В.М.* О системе шифрования, построенной на основе обобщенных кодов Рида–Соломона // Дискретная математика. 1992. Т. 4. № 3. С. 57–63.
13. *Сидельников В.М.* Криптография и теория кодирования // Матер. конф. “Московский университет и развитие криптографии в России”. МГУ. 2002. С. 1–22.
14. *Рзаев Х.Н.* Разработка модифицированной несимметричной крипто-кодовой системы Мак-Элиса на укороченных эллиптических кодах // Восточно-евр. журн. передовых технологий. 2016. Т. 4. № 9 (82). С. 18–26.
15. *Рзаев Х.Н., Цыганенко А.С.* Анализ программной реализации метода недвоичного равновесного кодирования // Azərbaycan Texniki Universiteti, Elmi Əsərlər. 2016. Cild 1. № 1. Şəh. 107–112. Issn. 1815–1779.
16. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки / Пер. с англ. М.: Мир, 1986.
17. *Кларк Дж.-Мл., Кейн Дж.* Кодирование с исправлением ошибок в системах цифровой связи / Пер. с англ. под ред. Б.С. Цыбакова. М.: Радио и связь, 1987.
18. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
19. *Мутер В.М.* Основы помехоустойчивой телепередачи информации. Л.: Энергоатомиздат. Ленингр. отд-ние, 1990.
20. *Цыбаков Б.С., Гельфанд С.И.* Теория кодирования / Пер. с япон. Касами Т., Токура Н., Ивадари Е., Инагаки Я. М.: Мир, 1978.

Статья представлена к публикации членом редколлегии О.Н. Граничиным.

Поступила в редакцию 04.05.2016

После доработки 04.02.2017

Принята к публикации 08.11.2018