Розглядаються загальна конструкція теоретико-кодових схем (ТКС), несиметрична крипто-кодова система (НККС) на основі ТКС Мак-Еліса на укорочених (модифікованих) еліптичних кодах. Пропонується математична модель НККС Мак-Еліса, алгоритми формування та розшифрування/розкодування криптограми/кодограми, аналізуються витрати на програмну реалізацію крипто-кодових засобів захисту інформації на основі ТКС Мак-Еліса

Ключові слова: несиметрична крипто-кодова система, теоретико-кодова схема, модифіковані перешкодостійкі коди

Рассматриваются общая конструкция теоретико-кодовых схем (ТКС), несимметричная крипто-кодовая система (НККС) на основе ТКС Мак-Элиса на укороченных (модифицированных) эллиптических кодах. Предлагается математическая модель НККС Мак-Элиса, алгоритмы формирования и расшифрования/раскодирования криптограммы/кодограммы, анализируются затраты на программную реализацию крипто-кодовых средств защиты информации на основе ТКС Мак-Элиса

Ключевые слова: несимметричная крипто-кодовая система, теоретико-кодовая схема, модифицированные помехоустойчивые коды

УДК 621.391
DOI: 10.15587/1729-4061.2016.75250

РАЗРАБОТКА МОДИФИЦИРОВАННОЙ НЕСИММЕТРИЧНОЙ КРИПТО-КОДОВОЙ СИСТЕМЫ МАК-ЭЛИСА НА УКОРОЧЕННЫХ ЭЛЛИПТИЧЕСКИХ КОДАХ

С. П. Евсеев
Кандидат технических наук,
доцент, старший научный сотрудник*
E-mail: serhii.yevseiev@m.hneu.edu.ua
Х. Н. Рзаев
Кандидат технических наук, доцент**
E-mail: xazail49@mail.ru
О. Г. Король
Кандидат технических наук, доцент*
E-mail: olha.korol@m.hneu.edu.ua
З. Б. Иманова
Ассистент**
E-mail: zarife1955@mail.ru
*Кафедра информационных систем
Харьковский национальный
экономический университет им. С. Кузнеца
пр. Науки, 9-А, г. Харьков, Украина, 61166
**Кафедра компьютерных технологий и программирования
Азербайджанский Государственный
Университет Нефти и Промышленности
пр. Азадлыг, 20, г. Баку, Азербайджан, AZ1010

1. Введение

Развитие телекоммуникационных систем во всех областях их применения выдвигает более жесткие требования к обеспечению надежности и безопасности всего цикла обработки данных. Для обеспечения данных критериев в телекоммуникационных системах используются программные/программно-аппаратные средства реализации методов помехоустойчивого кодирования (обеспечения достоверности) и методов криптографического преобразования информации (обеспечение безопасности: конфиденциальности, целостности и доступности), а также протоколы передачи данных на различных уровнях модели ISO/OSI. Перспективным направлением в развитии коммуникационных технологий и систем являются интегрированные механизмы, позволяющие в одной программной/программно-аппаратной реализации обеспечить требуемые показатели надежности и безопасности. С этой целью авторами предлагается использование модифицированной несимметричной крипто-кодовой системы на основе теоретико-кодовой схемы (ТКС) Мак-Элиса на укороченных эллиптических кодах. Такой подход обеспечивает требуемый уровень достоверности (надежности) передачи данных за счет использования методов помехоустойчивого кодирования, а применение несимметричной криптосистемы позволяет обеспечить требуемые показатели уровня криптостойкости.

2. Анализ литературных данных и постановка проблемы

Развитие коммуникационных технологий тесно связано с качеством представляемых услуг конечным пользователям системы и определяется показателями, предложенными в стандартах и рекомендациях Международного союза связи. Среди основных показателей качества обслуживания, рассмотренных в Рекомендациях МСЭ Е.800, особое значение уделяется коэффициенту готовности системы, который обеспечивает требуемый уровень надежности и безо-

пасности всего цикла обработки и хранения данных [1, 2]. Проведенный анализ в работе [3] показал, что быстрый рост числа пользователей и потребителей информации, расширение спектра предоставляемых телекоммуникационных услуг, возросшие объемы обрабатываемых данных приводят к ужесточению вероятностно-временных требований, предъявляемых к основным компонентам телекоммуникационных систем и сетей на всех этапах информационного обмена данными. Так, по данным [4] актуальность создания телекоммуникационных систем и сетей с защищенными каналами передачи данных в последние годы резко возросла. Возросли и требования к показателям безопасности передачи данных в телекоммуникационных системах и сетях, особенно в сетях специального назначения, в которых отказ в обслуживании или выход конкретных параметров качества за установленные пределы может привести к катастрофическим последствиям в финансовом секторе, промышленности, энергетическом комплексе и пр. Современные разработчики коммуникационных технологий вынуждены одновременно решать несколько задач одновременно и обеспечить не только безопасность передаваемой информации, но и оперативность передачи больших объемов данных. В работе [5] авторы предлагают использовать криптосистему Мак-Элиса в программном обеспечении Sequitur, которая позволяет интегрировано решать задачи быстродействия и безопасности при передаче конфиденциальной информации. В работе [6] криптосистему Мак-Элиса используют в качестве механизма обеспечения целостности в стегасистеме, которая обеспечивает хранение в файле MPEG Layer-III или MP3 информацию об исполнителе, текст песни и ее исполнение. Криптосистема используется для хранения как личного (закрытого) ключа, так и открытого в формате тег ID3v2. В работах [7, 8] предлагается использовать криптосистему Мак-Элиса для решения задач аутентификации (подлинности) и формирования цифровой подписи на основе теории алгебраического кодирования, а также для передачи конфиденциальной (медицинской информации). Авторы работы [9] предлагают использовать криптосистему Мак-Элиса в программном обеспечении Secure Key Management (SKM, фреймворк с высокой степенью масштабируемости по отношению к памяти), для генерации ключевых последовательностей и их распределения.

Для снижения затрат на передачу и обработку данных, обеспечению требуемых показателей достоверности и информационной скрытности (безопасности) предлагается использовать несимметричные крипто-кодовые системы на теоретико-кодовой схеме Мак-Элиса [10–12]. В работах [13, 14] рассмотрены основные принципы и математические модели построения несимметричных крипто-кодовых систем на основе теоретико-кодовых схем (ТКС) Мак-Элиса и Нидеррайтера на эллиптических кодах, позволяющих интегрировано обеспечить требуемые показатели достоверности информационной скрытности и оперативности при передаче данных в коммуникационных системах.

Вместе с тем, проведенный в работе [15] анализ программной реализации несимметричной крипто-кодовой системы на теоретико-кодовой схеме (ТКС) Нидеррайтера показал на значительные сложности реализации, что существенно затрудняет использование теоретико-кодовых схем для построения криптостойких несимметричных систем. В работе [16] рассмотрены новые подходы к взлому криптосистемы Мак-Элиса на основе рандомизированных сцепленных кодов. Разработка модифицированных крипто-кодовых систем с использованием модифицированных алгеброгеометрических кодов является перспективным направлением в решении данной научно-технической задачи.

3. Цели и задачи исследования

Целью работы является анализ общей конструкции построения теоретико-кодовых схем, как интегрированного механизма обеспечения достоверности, оперативности и безопасности в общем цикле обработки данных.

Для достижения цели рассмотрим следующие задачи:

– провести анализ общей структуры построения несимметричной крипто-кодовой системы (НККС), оценить эффективность и быстродействие по сравнению с симметричными и несимметричными криптоалгоритмами;

– рассмотреть математическую модель и основные алгоритмы преобразования информации в НККС Мак-Элиса на укороченных кодах;

– проанализировать затраты на программную реализацию крипто-кодовых средств защиты информации на основе ТКС Мак-Элиса.

4. Общая конструкция теоретико-кодовых схем, оценка их эффективности по сравнению с другими криптографическими методами

Рассмотрим общую конструкцию теоретико-кодовых схем. Зафиксируем конечное поле GF(q). Рассмотрим векторное пространство $GF^n(q)$ как множество n-последовательностей элементов из GF(q) с покомпонентным сложением и умножением на скаляр. Линейный (n, k, d) код C есть подпространство в $GF^n(q)$, т. е. непустое множество n-последовательностей (кодовых слов) над GF(q), k – размерность линейного подпространства, d – минимальное кодовое расстояние (минимальный вес ненулевого кодового слова).

Основной целью кодирования информации является контроль (обнаружение и исправление) ошибок, произошедших при передаче сообщения по каналу с шумами. Для контроля ошибок кодирующее устройство вносит избыточность (проверочную часть длины r, r=n–k) в передаваемые данные. На приемной стороне, анализируя свойства проверочной части и ее соответствие передаваемым данным, декодер уменьшает влияние ошибок, возникших при передаче.

Задача раскодирования может быть эффективно решена (с полиномиальной сложностью) для узкого класса кодов, например, помехоустойчивых кодов Боуза-Чоудхури-Хоквингема (БЧХ) и кодов Рида-Соломона. Одним из наиболее эффективных алгоритмов алгебраического декодирования кодов БЧХ является алгоритм Берлекемпа-Месси и его модификации (улучшения).

Известно [17–20], что алгоритм Берлекемпа-Месси содержит число реализации умножений, порядка t^2, или, формально, сложность алгоритма $O(t^2)$, где t – исправляющая способность кода, $t=\lfloor(d-1)/2\rfloor$. Для большого t используют ускоренный алгоритм Берлекемпа-Месси, позволяющий уменьшить вычислительную сложность алгоритма. Еще более эффективным, с точки зрения вычислительной сложности, является рекуррентный алгоритм Берлекемпа-Месси. Асимптотическая сложность декодирования кодов Рида-Соломона в этом случае не превосходит величины $O(n\log^2 n)$, причем очень близка к величине O(nlogn).

Декодирование произвольного линейного кода (кода общего положения) является весьма сложной вычислительной задачей, сложность ее решения растет экспоненциально. Так, для корреляционного декодирования произвольного (n, k, d) кода над GF(q) необходимо, в общем случае, сравнить принятую последовательность со всеми q^k кодовыми словами и выбрать ближайшее (в метрике Хемминга). Даже для небольших n, k, d и q задача корреляционного декодирования весьма трудоемка. Это положение лежит в основе всех криптосистем на алгебраических блоковых кодах. Маскируя код с быстрым алгоритмом декодирования (полиномиальной сложности) под произвольный (случайный) линейный код можно представить задачу декодирования для постороннего наблюдателя (возможного злоумышленника) как вычислительно сложную задачу (экспоненциальной сложности). Для уполномоченного пользователя криптосистемы (имеющего секретный ключ) декодирование – полиноминально разрешимая задача. Общая классификация теоретико-кодовых схем представлена на рис. 1.

Рис. 1. Общая классификация теоретико-кодовых схем

Для обеспечения безопасности в современных коммуникационных системах, как правило, используются симметричные и несимметричные криптоалгоритмы, обеспечивающие требуемый уровень криптостойкости. Как показывает проведенный анализ, применение теоретико-кодовых схем позволяет реализовать быстрое криптографическое преобразование с обеспечением доказуемой стойкости (табл. 1). Сложность их реализации сопоставима с симметричными криптоалгоритмами с блочно-симметричными шифрами (БСШ). Кроме того, их практическое использование позволяет применить инфраструктуру открытых ключей и строить интегрированные механизмы криптографического преобразования данных и канального кодирования для комплексного обеспечения безопасности и достоверности передачи данных.

В табл. 1. приведены результаты сравнительных исследований эффективности криптографических методов защиты информации при фиксированном уровне стойкости:

– среднем (сложность криптоанализа наилучшим известным алгоритмом не менее 2^{128} операций);

– высоком (сложность криптоанализа наилучшим известным алгоритмом не менее 2^{256} операций);

– сверхвысоком (сложность криптоанализа наилучшим известным алгоритмом не менее 2^{512} операций).

Таблица 1

Результаты сравнительных исследований эффективности криптографических методов защиты информации при фиксированном уровне стойкости

Методы криптографического преобразования	Модель безопасности	Длина ключевых данных, бит	Скорость шифрования, бит/с	Дополнительные функции
Блочные симметричные шифры	Практическая безопасность	128, 256, 512	10^6–10^9	Нет
Поточные симметричные шифры	Практическая безопасность	128, 256, 512	10^7–10^{10}	Нет
RSA-подобные криптоалгоритмы	Доказуемая безопасность	3248 (128), 15424 (256)	10^2–10^3	Нет
Несимметричные криптоалгоритмы на эллиптических кривых	Доказуемая безопасность	283 (128), 571 (256)	10^3–10^4	Нет
НККС	Доказуемая безопасность	$0{,}5\cdot10^6$ (128), $2\cdot10^6$ (256)	10^6–10^8	Контроль ошибок, обеспечение достоверности

Результаты оценки быстродействия алгоритмов преобразования информации в симметричных шифрах и НККС представлены на рис. 2.

Таким образом, как следует из приведенных результатов сравнительного анализа, несимметричные криптоалгоритмы с использованием теоретико-кодовых схем позволяют реализовать криптографическую защиту информации по технологии открытых ключей и обеспечить при этом скорость крипто-кодового преобразования информации со скоростью шифрования блочно-симметричных шифров. Кроме того, практическое использование теоретико-кодовых средств защиты информации позволяет на основе интеграции механизмов канального кодирования и шифрования комплексно обеспечить безопасность и достоверность передаваемых данных. Следовательно, применение теоретико-кодовых схем с одной стороны экономически выгоднее применения целого комплекса различных механизмов шифрования и канального кодирования, решающих отдельно взятые задачи, а с другой – наблюдается существенное снижение суммарных вычислительных затрат, приходящихся на единицу обрабатываемой и передаваемой информации, т. е. за счет снижения времени обработки повышается оперативность передачи данных. Рассмотрим математическую модель и основные алгоритмы в НККС Мак-Элиса.

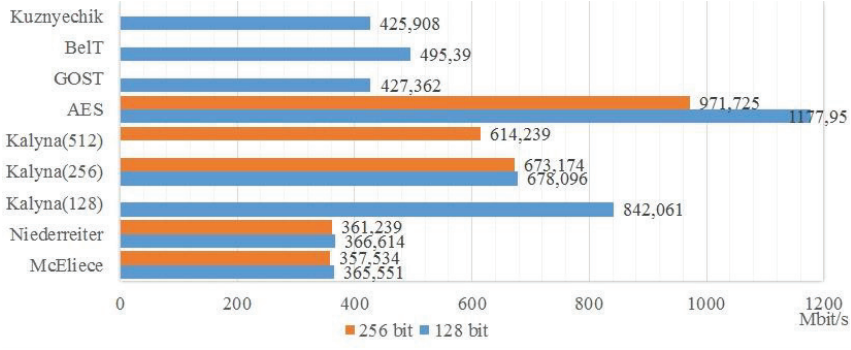


Рис. 2. Оценка быстродействия криптопреобразований в БСШ и НККС

5. Математическая модель и основные алгоритмы преобразования информации в предлагаемой системе Мак-Элиса на укороченных кодах

Известные способы модификации линейных блоковых кодов наиболее полно рассмотрены в [17–20]. На рис. 3 представлены наиболее распространенные способы модификации.

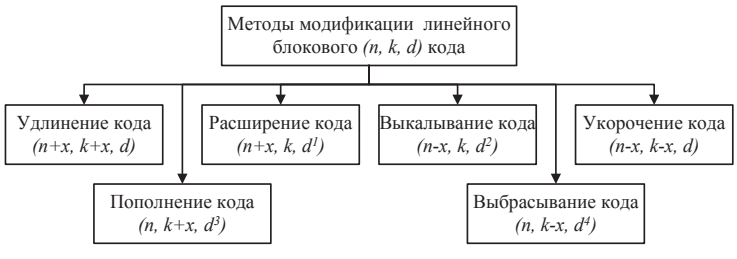


Рис. 3. Способы модификации линейных блоковых кодов

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 увеличении 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. Способы удлинения и укорочения линейных блоковых кодов не изменяют минимальное расстояние, и поэтому позволяют строить стойкие ко взлому несимметричные крипто-кодовые системы.

Наиболее простой и удобный способ модификации линейного блокового кода, не уменьшающий минимальное кодовое расстояние, состоит в укорочении его длины путем сокращения информационных символов. Пусть $I=(I_1, I_2, ..., I_k)$ – информационный вектор (n, k, d) блокового кода. Выберем подмножество h информационных символов, $|h|=x$, $x\le 1/2k$. Поместим в информационный вектор I в подмножество h нули, т. е. $I_i=0, \forall I_i\in h$. На остальных позициях вектора I поместим информационные символы. При кодировании информационного вектора символы множества h не участвуют (они нулевые) и их можно отбросить, а полученное кодовое слово будет короче на x кодовых символов. Для модификации (укорочения) эллиптических кодов будем использовать уменьшение набора точек кривой. Справедливо следующее утверждение.

Утверждение 1. Пусть EC – эллиптическая кривая над GF(q), g=g(EC) – род кривой, EC(GF(q)) – множество ее точек над конечным полем, N=EC(GF(q)) – их число. Пусть X и h – непересекающиеся подмножества точек, $X\cup h=EC(GF(q))$, $|h|=x$. Тогда укороченный эллиптический (n, k, d) код над GF(q), построенный через отображение вида $\varphi:X\to P^{k-1}$, связан характеристиками $k+d\ge n$, причем:

$$n=2\sqrt{q}+q+1-x,$$
$$k\ge\alpha-x, \qquad (1)$$
$$d\ge n-\alpha,\ \alpha=3\times degF.$$

Утверждение 2. Укороченный эллиптический (n, k, d) код над GF(q), построенный через отображение вида $\varphi:X\to P^{r-1}$, связан характеристиками $k+d\ge n$, причем:

$$n=2\sqrt{q}+q+1-x,$$
$$k\ge n-\alpha, \qquad (2)$$
$$d\ge\alpha,\ \alpha=3\times degF.$$

Используя результат утверждений 1, 2 зададим теоретико-кодовую схему на модифицированных эллиптических кодах, построенную через отображение вида $\varphi:X\to P^{k-1}$ и $\varphi:X\to P^{r-1}$. Справедливы следующие утверждения.

Утверждение 3. Укороченный эллиптический (n, k, d) код над $GF(2^m)$, построенный через отображения вида $\varphi:X\to P^{k-1}$, определяет модифицированную теоретико-кодовую схему с параметрами:

$$l_{K+}=x\cdot\left\lceil\log_2\left(2\sqrt{q}+q+1\right)\right\rceil; \qquad (3)$$
$$l_I=(\alpha-x)\cdot m; \qquad (4)$$
$$l_S=\left(2\sqrt{q}+q+1-x\right)\cdot m; \qquad (5)$$
$$R=(\alpha-x)/\left(2\sqrt{q}+q+1-x\right). \qquad (6)$$

Утверждение 4. Укороченный эллиптический (n, k, d) код над $GF(2^m)$, построенный через отображения

вида $\varphi: X \to P^{r-1}$, определяет модифицированную теоретико-кодовую схему с параметрами:

– размерность секретного ключа определяется выражением (3);

– размерность информационного вектора (в битах):

$$l_I = \left(2\sqrt{q} + q + 1 - \alpha\right) \cdot m; \quad (7)$$

– размерность кодограммы определяется выражением (5);

– относительная скорость передачи:

$$R = \left(2\sqrt{q} + q + 1 - \alpha\right) / \left(2\sqrt{q} + q + 1 - x\right). \quad (8)$$

Рассмотрим формальное описание модифицированной несимметричной крипто-кодовой системы защиты информации на основе использования методов модификации и практические алгоритмы формирования кодограмм и их раскодирования в разработанных теоретико-кодовых схемах.

Математическая модель НККС с использованием ТКС Мак-Элиса на основе укорочения (сокращения информационных символов) формально задается совокупностью следующих элементов [9]:

– множество открытых текстов

$$M = \{M_1, M_2, ..., M_{q^k}\},$$

где $M_i = \{I_0, I_{h_1}, .. I_{h_j}, I_{k-1}\}$, $\forall I_j \in GF(q)$, 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)

$$C = \{C_1, C_2, ..., C_{q^k}\},$$

где $C_i = (c^*_{X_0}, c^*_{h_1}, ..., c^*_{h_j}, c^*_{X_{n-1}})$, $\forall c^*_{X_j} \in GF(q)$;

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

$$\phi = \{\phi_1, \phi_2, ..., \phi_s\},$$

где $\phi_i : M \to C_{k-h_j}$, $i = 1, 2, ..., s$;

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

$$\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, ..., \phi_s^{-1}\},$$

где $\phi_i^{-1} : C_{k-h_j} \to M$, $i = 1, 2, ..., s$;

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

$$K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, ..., K_{s_{a_i}}\} = \{G_X^{EC_1}{}_{a_i}, G_X^{EC_2}{}_{a_i}, ..., G_X^{ECs}{}_{a_i}\},$$

где $G_X^{EC_1}{}_{a_i}$ – порождающая $n \times k$ матрица замаскированного под случайный код алгеброгеометрического блокового (n, k, d) кода с элементами из GF(q), т. е. $\phi_i : M \xrightarrow{K_{ia_i}} C_{k-h_j}$; $i = 1, 2, ..., s$; a_i – набор коэффициентов многочлена кривой $a_1 ... a_6$, $\forall a_i \in GF(q)$, однозначно задающий конкретный набор точек кривой из пространства P^2.

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

$$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, ..., \{X,P,D\}_s\},$$

$$\{X,P,D\}_i = \{X^i, P^i, D^i\},$$

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.

$$\phi_i^{-1} : C \xrightarrow{K_i^*} M, \; i = 1, 2, ..., s,$$

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

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 $C_i H^T = 0$, где H – проверочная матрица алгеброгеометрического блокового кода;

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

– h_j – информационные символы, равные нулю, $|h| = 1/2k$, 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 [8], обеспечивающий формирование открытого ключа уполномоченного пользователя:

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

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 $a_1 ... a_6$, $\forall a_i \in GF(q)$, однозначно задающих конкретный набор точек кривой из пространства P^2.

Формирование закрытого текста $C_j \in C_{k-h_j}$ по введенному открытому тексту $M_i \in M$ и заданному откры-

тому ключу $G_{X\ a_i}^{ECu}$, $u \in \{1,2,...,s\}$ осуществляется путем формирования кодового слова замаскированного кода с добавлением к нему случайно сформированного вектора $e=(e_0,e_1,...,e_{n-1})$:

$$C_j = \phi_u\left(M_i, G_X^u\right) = M_i \cdot \left(G_X^u\right)^T + e,$$

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

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

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

Для каждого формируемого закрытого текста $C_j \in C_{k-h_j}$ соответствующий вектор $e=(e_0,e_1,...,e_{n-1})$ 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, количество и места нулевых информационных символов может воспользоваться быстрым алгоритмом раскодирования алгеброгеометрического кода (полиномиальной сложности) для восстановления открытого текста [8]:

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

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:

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

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

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

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

раскодирует полученный вектор по алгоритму Берлекемпа-Месси [15]:

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

т. е. избавляется от второго слагаемого и от сомножителя $(G)^{ECT}$ в первом слагаемом в правой части равенства, после чего снимает действие матрицы маскирования X^u.

Для этого полученный результат раскодирования $M_i \cdot \left(X^u\right)^T$ следует умножить на $\left(X^u\right)^{-1}$: $\left(M_i \cdot \left(X^u\right)^T\right) \cdot \left(X^u\right)^{-1} =$ $= M_i$. Полученное решение – суть открытый текст M_i.

Рассмотрим практические алгоритмы формирования и расшифрования/раскодирования криптограммы/кодограммы в модифицированной несимметричной крипто-кодовой системе на основе ТКС Мак-Элиса на укороченных эллиптических кодах. На рис. 4 представлен алгоритм формирования криптограммы/кодограммы.

Рис. 4. Алгоритм формирования кодограммы в модифицированной НККС Мак-Элиса с укороченным модифицированным кодом

Алгоритм формирования кодограммы в модифицированной теоретико-кодовой схеме Мак-Элиса с укороченным модифицированным кодом зададим последовательностью следующих шагов:

Шаг 1. Зафиксируем конечное поле GF(q). Зафиксируем эллиптическую кривую $y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz+a_6z^3$ и набор ее точек EC(GF(q)):(P_1, P_2, ..., P_N) над GF(q). Зафиксируем подмножество точек h(GF(q)): (P_{x1}, P_{x2}, ..., P_{xx}), h⊆EC(GF(q)), |h|=x и храним его в секрете.

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

Шаг 3. По введенному информационному вектору I сформируем кодовое слово c. Если (n, k, d) код над GF(q) задан своей порождающей матрицей, то c=I×G.

Шаг 4. Сформируем случайный вектор ошибки e такой, что w(e)≤t, $t=\lfloor (d-1)/2 \rfloor$. Добавим сформированный вектор к кодовому слову, получим кодовое слово: c*=c+e.

Шаг 5. Сформируем кодограмму, путем удаления (укорочения) символов вектора инициализации: $c_X^*=c^*-IV$.

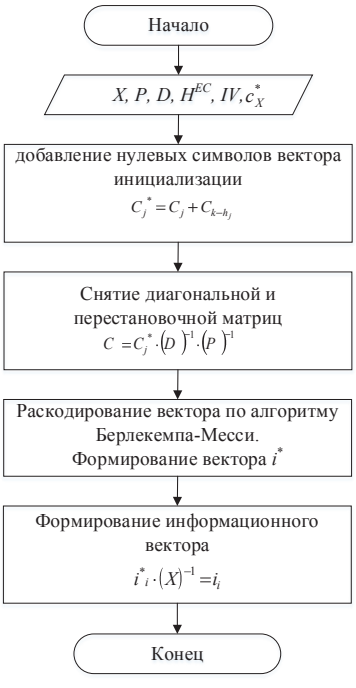
Алгоритм раскодирования кодограмм в модифицированных теоретико-кодовых схемах на эллиптических кодах зададим последовательностью следующих шагов.

Шаг 1. Ввод кодограммы, подлежащей раскодированию. Ввод закрытого ключа – порождающей и/или проверочной матрицы эллиптического кода.

Шаг 2. Кодограмма – суть кодовое слово с ошибками эллиптического кода. Вес вектора ошибок w(e)≤t. Раскодируем кодограмму – находим вектор ошибок.

Шаг 3. Формируем искомый информационный вектор.

Предложенный алгоритм раскодирования в модифицированной несимметричной крипто-кодовой системе с использованием ТКС Мак-Элиса с укороченным модифицированным кодом представлен на рис. 5.



Этап 1. Установка параметров кода, ввод личного ключа и кодограммы

X – невырожденная $k \times k$ матрица над $GF(q)$, P – перестановочная $n \times n$ матрица над $GF(q)$, D – диагональная $n \times n$ матрица над $GF(q)$, H^{EC} – проверочная $r \times n$ матрица эллиптического кода над $GF(q)$, a_i – набор коэффициентов многочлена кривой $a_1 \ldots a_6$, IV – вектор инициализации, IV= $|h|$ =½ k – элементы сокращения

Этап 2. Раскодирование кодограммы

Рис. 5. Алгоритм в модифицированной НККС Мак-Элиса с укороченным модифицированным кодом

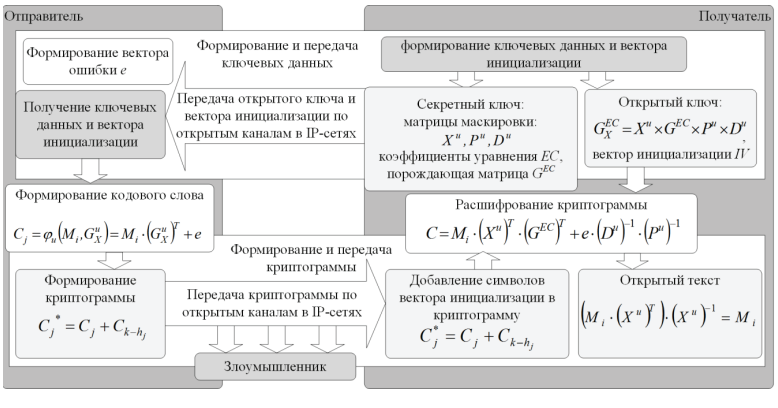


Рис. 6. Протокол обмена информацией в режиме реального времени с использованием модифицированной ТКС Мак-Элиса с укороченными ЕС

Основным этапом выполнения алгоритма раскодирования кодограмм в теоретико-кодовой схеме на эллиптических кодах является раскодирование принятой последовательности. При раскодировании кодограмм уполномоченному пользователю в теоретико-кодовых схемах на модифицированных эллиптических кодах следует учитывать параметры укороченных кодов.

Структурная схема протокола обмена информацией в режиме реального времени с использованием несимметричной криптосистемы на основе модифицированной ТКС Мак-Элиса с модифицированными (укороченными) эллиптическими кодами представлена на рис. 6.

Проведем исследование энергетических затрат на программную реализацию крипто-кодовых средств защиты информации на основе ТКС Мак-Элиса на модифицированных (укороченных) эллиптических кодах.

6. Оценка энергетических затрат на программную реализацию предлагаемой системы Мак-Элиса

Для оценки временных и скоростных показателей принято использовать единицу измерения cpb, где cpb (cycles per byte) – число тактов процессора, которое необходимо потратить для обработки 1 байта входящей информации.

Сложность алгоритма вычислим по выражению

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

где Utl – утилизация ядра процессора (%); Rate – пропускная способность алгоритма (байт/сек).

В табл. 2 приведены результаты исследований зависимости длины кодовой последовательности алгебро-геометрического кода в ТКС Мак-Элиса и Нидеррайтера от количества тактов процессора на выполнение элементарных операций в программной реализации крипто-кодовых систем.

Таблица 2

Результаты исследований зависимости длины кодовой последовательности кода в НККС Мак-Элиса и модифицированной НККС от количества тактов процессора

Длинна кодовой последовательности		MacElis на укороченных кодах			MacElis		
		10	100	1000	10	100	1000
Количество вызовов функций реализующих элементарные операции	Чтение символа	10 294 397	28 750 457	76 759 874	11 018 042	30 800 328	80 859 933
	Сравнение строк	3 406 921	9 246 748	25 478 498	3 663 356	10 199 898	26 364 634
	Конкатенация строк	1 705 544	5 045 748	12 379 422	1 834 983	5 125 564	13 415 329
Сумма		15 406 862	43 042 953	114 617 794	16 516 381	46 125 790	120 639 896
Длительность выполнения функций* в тактах процессора	Чтение символа	295 374	810 478	2 001 167	297 487	831 609	2 183 218
	Сравнение строк	178 814	531 379	1 248 684	197 821	550 794	1 423 690
	Конкатенация строк	544 990	1 328 114	3 586 486	544 990	1 522 293	3 984 353
Сумма		1 006 781	2 749 548	7 247 488	1 040 298	2 904 696	7 591 261
Длительность выполнения** в мсек		0,52	1,37	3,4	0,55	1,53	4

*Примечания: * – 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 системой 5 %*

В табл. 3 результаты исследований оценки временных и скоростных показателей процедур формирования и раскодирования информации в несимметричных крипто-кодовых системах на основе ТКС Мак-Элиса.

Таблица 3

Результаты исследований оценки временных и скоростных показателей процедур формирования и раскодирования информации

Показатели	Длина кодовой последовательности	Пропускная способность алгоритма, Rate (байт/сек)	Утилизация ядра процессора (%)	Сложность алгоритма, Per (cpb)
Количество вызовов функций, реализующих элементарные операции	100	46 125 790	56	61,5
	1000	120 639 896	56	62,0

Проведенный анализ табл. 2, 3 позволяет сделать вывод о значительных энергетических затратах при реализации несимметричных крипто-кодовых систем в протоколах коммуникационных систем и технологий, что значительно затрудняет их использование. Для устранения недостатка предлагается использовать модифицированные несимметричные крипто-кодовые схемы на основе использования модификации помехоустойчивых кодов, что обеспечивает снижение энергетических затрат и объемов ключевых данных пользователей за счет хранения данных о коэффициентах эллиптической кривой в аффинном пространстве для построения соответствующих матриц (закрытого и открытого ключей).

7. Выводы

1. Проанализирована общая структура построения несимметричных крипто-кодовых систем на основе ТКС Мак-Элиса, позволяющих интегрировано (одним устройством) обеспечить требуемые показатели по достоверности, оперативности и безопасности данных. Существенным недостатком НККС на основе ТКС Мак-Элиса является большой объем ключевых данных, что суживает их применение в различных областях коммуникационных систем (на сегодняшний день криптостойкость на уровне модели доказуемой стойкости обеспечивается при построении НККС в поле Галуа $GF(2^{13})$). Применение модифицированных (укороченных) эллиптических (алгебро-геометрических) кодов позволяет снизить объемы ключевых данных, сохраняя требования по криптостойкости НККС. Оценка быстродействия преобразования данных сопоставимо с быстродействием прямых и обратных криптопреобразований в современных БСШ, при этом обеспечивается криптостойкость на уровне несимметричных криптосистем (криптостойкость базируется на теоретико-сложностной задачи – декодирование случайного кода).

2. Предложенные математическая модель, практические алгоритмы шифрования/кодирования и расшифрования/раскодирования криптограммы/кодограммы в разработанной модифицированной крипто-кодовой системах на основе ТКС Мак-Элиса позволяет реализовать шифрование/расшифрование со скоростью симметричных криптосистем с БСШ. Сложность формирования кодограмм и их раскодирования определяется, соответственно, сложностью кодирования и раскодирования модифицированных (укороченных) эллиптических кодов и полиномиально зависит от длины кода и его исправляющей зависимости. Для 100 байт передаваемых данных сложность алгоритма Per составляет 61,5 cpb, а для 1000 байт – 62 cpb, что при значительном увеличении обрабатываемых данных практически не влияет на сложность алгоритма.

3. Передача ключевой последовательности при использовании модифицированной НККС Мак-Элиса

на основе укороченных кодов позволяет использовать открытые каналы связи коммуникационных систем для передачи конфиденциальной информации и интегрировано обеспечить требуемые показатели достоверности и оперативности всего цикла обработки информации.

Литература

1. Семенов, С. Г. Модели и методы управления сетевыми ресурсами в информационно-телекоммуникационных системах [Текст]: монография / С. Г. Семенов, А. А. Смирнов, Е. В. Мелешко. – Харьков: НТУ «ХПИ», 2011. – 212 с.
2. Рзаев, Х. Н. Анализ состояния и путей совершенствования протоколов безопасности современных телекоммуникационных сетей [Текст]: монография / Х. Н. Рзаев, О. Г. Король; под. ред. В. С. Пономаренко // Информационные технологии в управлении, образовании, науке и промышленности. – Х.: Издатель Рожко С. Г., 2016. – С. 217–234.
3. Телекоммуникационные услуги в мировой экономике [Электронный ресурс]. – Режим доступа: http://www.gumer.info/bibliotek_Buks/Econom/world_econom/30.php
4. Король, О. Г. Протоколы безопасности телекоммуникационных сетей [Текст] / О. Г. Король // Системи обробки інформації. – 2012. – № 6 (104). – С. 113–120.
5. Ojha, D. B. Transmission of Picturesque content with Code Base Cryptosystem [Text] / D. B. Ojha, A. Sharma, A. Dwivedi, B. Kumar, A. Kumar // International Journal of Computer Technology and Applications. – 2011. – Vol. 02, Issue 01. – P. 127–131. – Available at: https://doaj.org/article/6714b60516cc4aa79e56d0c421febaf3
6. Salman, A. G. Steganography application program using the ID3v2 in the MP3 audio file on mobile phone [Text] / A. G. Salman // Journal of Computer Science. – 2014. – Vol. 10, Issue 7. – P. 1249–1252. doi: 10.3844/jcssp.2014.1249.1252
7. Ojha, D. B. Space-Age Approach To Transmit Medical Image With Codebase Cryptosystem Over Noisy Channel [Text] / D. B. Ojha, A. Sharma, A. D. N. Pandey, A. Kumar // International Journal of Engineering Science and Technology. – 2010. – Vol. 2, Issue 12. – P. 7112–7117. – Available at: https://doaj.org/article/5c7da3a1e3ec4f83b552199034bd3241
8. Ojha, D. B. An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel [Text] / D. B. Ojha, A. Sharma // International Journal of Advanced Networking and Applications. – 2011. – Vol. 2, Issue 5. – P. 841–845. – Available at: https://doaj.org/article/39a3ac65d5b24b348f069dfc82eb6248
9. Jeeva, Y. C. A Novel Approach For Information Security In Ad Hoc Networks Through Secure Key Management [Text] / Y. C. Jeeva // Journal of Computer Science. – 2013. – Vol. 9, Issue 11. – P. 1556–1565. – Available at: https://doaj.org/article/378b88837cdf4cab9f8010a38a6aeb2b
10. McEliece, R. J. A Public-Key Criptosystem Based on Algebraic Theory [Text] / R. J. McEliece // DGN Progres Report 42-44. – Pasadena, C.A., 1978. – P. 114–116.
11. Niederreiter, H. Knapsack-Type Cryptosystems and Algebraic Coding Theory [Text] / H. Niederreiter // Problems of Control and Information Theory. – 1986. –Vol. 15, Issue 2. – P. 159–166.
12. Сидельников, В. М. Криптография и теория кодирования [Текст]: конференция / В. М. Сидельников // Московский университет и развитие криптографии в России. – М., 2002. – 22 с.
13. Евсеев, С. П. Исследование теоретико-кодовых схем для комплексного обеспечения безопасности и достоверности данных в информационных системах [Текст] / С. П. Евсеев, Б. П. Томашевский // Науковий вісник Чернівецького університету. Серія: Комп'ютерні системи та компоненти. – 2011. – Т. 2, Вип. 1. – С. 6–14.
14. Рзаев, Х. Н. Математические модели крипто-кодовых средств защиты информации на основе ТКС [Текст] / Х. Н. Рзаев, Г. Г. Искендерзаде, Ф. Г. Самедов, З. Б. Иманова, Ж. С. Джамалова // Защита информации. – К.: НАУ, 2016. – Вып. 23. – С. 24–26.
15. Рзаев, Х. Н. Анализ программной реализации метода недвоичного равновесного кодирования [Текст] / Х. Н. Рзаев, А. С. Цыганенко // Azərbaycan Texniki Unuversiteti, Elmi Əsərlər Cild. – 2016. – Issue 1. – P. 107–112.
16. Hamdi, O. On the Usage of Chained Codes in Cryptography [Text] / O. Hamdi // International Journal of Computer Science and Security. – 2010. – Vol. 3, Issue 6. – P. 482–490. – Available at: https://doaj.org/article/c0f40bdb1f6149f4ac107d44a95c9531
17. Блейхут, Р. Теория и практика кодов, контролирующих ошибки [Текст] / Р. Блейхут. – М.: Мир, 1986. – 576 с.
18. Кларк, Дж.-мл. Кодирование с исправлением ошибок в системах цифровой связи [Текст] / Кларк, Дж.-мл.; под ред. Б. С. Цыбакова. – М.: Радио и связь, 1987. – 392 с.
19. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки [Текст] / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М.: Связь, 1979. – 744 с.
20. Мутер, В. М. Основы помехоустойчивой телепередачи информации [Текст] / В. М. Мутер. – Л.: Энергоатомиздат. Ленингр. отд-ние, 1990. – 288 с.
21. Касами, Т. Теория кодирования [Текст] / Т. Касами, Н. Токура, Е. Ивадари, Я. Инагаки; под ред. Б. С. Цыбакова, С. И. Гельфанда. – М.: Мир, 1978. – 576 с.
22. Кузнецов, О. О. Захист інформації та економічна безпека підприємства [Текст]: монография / О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун. – Харків: Вид. ХНЕУ, 2008. – 360 с.