УДК 004.942

С.П. Евсеев

DOI: 10.30748/soi.2017.151.15

Харьковский национальный экономический университет им. С. Кузнеца, Харьков

ИСПОЛЬЗОВАНИЕ УЩЕРБНЫХ КОДОВ В КРИПТО-КОДОВЫХ СИСТЕМАХ

Рассматриваются общая конструкция несимметричных крипто-кодовых систем (НККС) на основе теоретико-кодовой схемы (ТКС) Мак-Элиса на алгеброгеометрических (АГК) на эллиптических кривых (эллиптических кодах, ЕС), позволяющих интегрировано (одним механизмом) обеспечивать требуемый уровень безопасности на основе теоретико-сложностной задачи – декодирования случайного кода (обеспечивается 10^{30}–10^{35} групповых операций, при мощности поля GF(2^{10}), оперативности – на уровне быстродействия криптопреобразований блочно-симметричных шифров (БСШ), достоверности – на основе алгеброгеометрических (помехоустойчивых m-ичных кодов) обеспечить $P_{ош}$ 10^{-9}–10^{-12}. Анализируются способы построения ущербных кодов, многоканальные протоколы обеспечения безопасности на основе НККС на ущербных кодах. Использование ущербных кодов позволяет увеличить быстродействие кодовых преобразований в НККС за счет уменьшения мощности поля GF (2^4–2^6), обеспечив требуемый уровень криптостойкости на основе увеличения полной энтропии ущербных кодов (увеличения расстояния единственности ключевых данных). Полученные результаты позволяют строить гибридные (комплексные) криптосистемы, обеспечивая основные показатели безопасности, оперативности и достоверности, предъявляемые к современным коммуникационным системам и сетям.

Ключевые слова: *несимметричная крипто-кодовая система, теоретико-кодовая схема, помехоустойчивые алгеброгеометрические коды, ущербные коды.*

Введение

Развитие телекоммуникационных технологий в глобальных системах Интернет (ГСИ) остро ставит вопрос повышения производительности из-за возрастающей структурной сложности и размерности современных сетей, характеризующихся множественными изменяющимися во времени информационными связями, а также потребности в увеличении уровня безопасности информационных потоков (БИП). Снижение производительности сетей связано с недостаточной защищенностью ИП на основе открытых протоколов HDLC, а также вследствие широкого использования слабозащищенных протоколов HTTP, SNMP, FTP, TCP/IP; участия в процессе обработки информации пользователей различных категорий, их непосредственного и одновременного доступа к системным ресурсам и процессам. Современная система технических средств защиты информации (ТСЗИ), включающая систему обнаружения, предотвращения атак и вторжений IPS/IDS, не может гарантировать обнаружение до 70 % информационных и кибератак, что периодически приводит к значительному возрастанию вредоносного трафика и несанкционированному доступу (НСД) к информационным ресурсам. В ТСЗИ доминирует использование стандартных аппаратно-программных (программных) средств защиты информации, на основе криптосистем, которые практически исчерпали свой потенциал относительно нейтрализации возможных киберугроз. Одновременно существенно возросли технические возможности инструментальных средств, привлекаемых злоумышленниками для получения НСД к ресурсам и сервисам ГСИ. В этих условиях одним из перспективных направлений обеспечения БИП можно считать создание системы интегрированной защиты сетевых ресурсов на основе несимметричных крипто-кодовых систем (НККС). Их применение позволяет одним механизмом интегрировано обеспечить требуемые уровни показателей достоверности, безопасности и оперативности при обработке и передаче конфиденциальной информации по открытым каналам ГСИ.

Анализ последних исследований [1 – 4] ***исследования и публикаций*** [5 – 9] подтверждают, что их применение обеспечивает быстродействие на уровне криптопреобразований симметричных блочных криптоалгоритмов (БСШ), доказуемую криптостойкость на основе теоретико-сложностной задачи декодирования случайного кода (обеспечивается 10^{30}–10^{35} групповых операций), и достоверность на основе использования алгеброгеометрического кода (АГК) (обеспечивается $P_{ош}$ 10^{-9}–10^{-12}).

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 стегаси-

стеме, 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. Существенным недостатком применения НККС Мак-Элиса являются большие объемы ключевых данных (для обеспечения требуемой криптостойкости необходимо построение системы в поле *GF* (2^{10}–2^{13})). Для уменьшения объемов ключевых данных (открытого ключа) в работе предлагается использовать ущербные коды, что позволяет уменьшить мощность поля GF (2^4–2^6), сохранив при этом уровень криптостойкости, за счет увеличения расстояния единственности ключа на основе полной совокупности энтропии ущербных текстов [1–2].

Целью статьи является теоретическое обоснование возможности использования ущербных кодов для построения гибридных (комплексных) криптосистем, на основе модифицированных несимметричных крипто-кодовых систем на модифицированных эллиптических кодах, что позволит обеспечить снижение энергетических затрат при их практической реализации.

Основной материал

1. Основные принципы построения крипто-кодовых систем.

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 [1–4; 10–17].

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). 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 [14–17].

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. Однако в работе [18] приводятся алгоритмы взлома НККС Мак-Элиса и Нидеррайтера, путем нахождения элементов порождающей (проверочной) матрицы.

Общая классификация крипто-кодовых систем (НККС) и услуги безопасности, обеспечивающиеся ними, представлена на рис. 1.

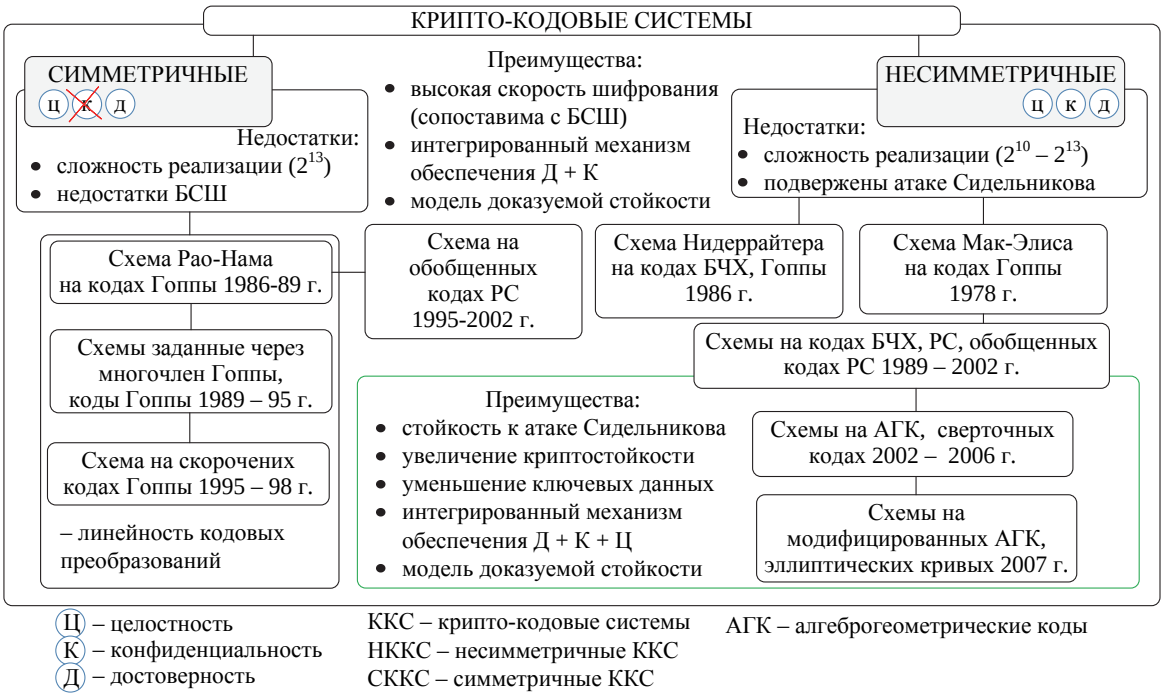


Рис. 1. Общая классификация крипто-кодовых систем

Одним из перспективных направлений в развитии алгебраической теории кодов являются методы алгеброгеометрического кодирования. Недвоичные алгебраические блоковые коды, построенные по алгебраическим кривым (алгеброгеометрические коды), обладают хорошими асимптотическими свойствами. Доказано, что при большой длине эти коды лежат выше границы Варшамова-Гилберта [14–18].

Зафиксируем конечное поле GF(q). Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве P^n над GF(q), g = g(X) – род кривой, X(GF(q)) – множество ее точек над конечным полем, N = X(GF(q)) – их число. Пусть C – класс дивизоров на X степени $\alpha > g - 1$. Тогда C определяет отображение $\varphi: X \to P^{k-1}$, где $k \geq \alpha - g + 1$. Набор $y_i = \varphi(x_i)$ задает код. Число точек в пересечении $\varphi(X)$ с гиперплоскостью равно α, т.е. $n - d \leq \alpha$. Эта конструкция позволяет строить коды с параметрами $k + d \geq n - g + 1$, длина n которых меньше либо равна числу точек на кривой X. При $2g < \alpha \leq n$ алгеброгеометрический код имеет параметры $(n, \alpha - g + 1, d)$, $d \geq n - \alpha$. Двойственный к нему код также является алгеброгеометрическим и имеет параметры $(n, n - \alpha + g - 1, d^{\perp})$, $d^{\perp} \geq \alpha - 2g + 2$. Конструктивные характеристики эллиптических кодов, построенных через отображение вида $\varphi: EC \to P^{k-1}$ над GF(q), $q = 2^m$, $m = \overline{2,6}$ приведены в табл. 1.

Таблица 1

Конструктивные кодовые характеристики эллиптических кодов, построенных через отображение $\varphi: EC \to pk^{-1}$ над gf(q), $q = 2^m$, $m = \overline{2,6}$

degF	α	(n, k, d)				
		GF(4)	GF(8)	GF(16)	GF(32)	GF(64)
1	3	9, 3, 6	14, 3, 11	25, 3, 22	44, 3, 41	81, 3, 78
2	6	9, 6, 3	14, 6, 8	25, 6, 19	44, 6, 38	81, 6, 75
3	9	–	14, 9, 5	25, 9, 16	44, 9, 35	81, 9, 72
4	12	–	14, 12, 2	25, 12, 13	44, 12, 32	81, 12, 69
5	15	–	–	25, 15, 10	44, 15, 29	81, 15, 66
6	18	–	–	25, 18, 7	44, 18, 26	81, 18, 63
7	21	–	–	25, 21, 4	44, 21, 23	81, 21, 60
8	24	–	–	–	44, 24, 20	81, 24, 57
9	27	–	–	–	44, 27, 17	81, 27, 54
10	30	–	–	–	44, 30, 14	81, 30, 51

Окончание табл. 1

degF	α	(n, k, d)				
		GF(4)	GF(8)	GF(16)	GF(32)	GF(64)
11	33	–	–	–	44, 33, 11	81, 33, 48
12	36	–	–	–	44, 36, 8	81, 36, 45
13	39	–	–	–	44, 39, 5	81, 39, 42
14	42	–	–	–	44, 42, 2	81, 42, 39
15	45	–	–	–	–	81, 45, 36
16	48	–	–	–	–	81, 48, 33
17	51	–	–	–	–	81, 51, 30
18	54	–	–	–	–	81, 54, 27
19	57	–	–	–	–	81, 57, 24
20	60	–	–	–	–	81, 60, 21
21	63	–	–	–	–	81, 63, 18
22	66	–	–	–	–	81, 66, 15
23	69	–	–	–	–	81, 69, 12
24	72	–	–	–	–	81, 72, 9
25	75	–	–	–	–	81, 75, 6
26	78	–	–	–	–	81, 78, 3

Дадим следующее определение алгеброгеометрического кода.

Определение 1 [2]. Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве P^n, т.е. совокупность решений однородного неприводимого алгебраического уравнения степени degX с коэффициентами из GF(q). Рассмотрим многообразия, соответствующие проективным гиперповерхностям, заданным в P^n уравнениями F=0, где F – однородные одночлены степени degF. Пусть $I(i_1, i_2, \ldots, i_n)$ – информационная последовательность. Алгеброгеометрический код по кривой X над GF(q) – это линейный код длины $n \le N$, кодовые слова $C(c_1, c_2, \ldots, c_n)$ которого задаются равенством

$$\sum_{i=0}^{k-1} i_j F_j(P_i) = c_i ,$$

где $P_i(X_i, Y_i, Z_i)$ – проективные точки кривой X, т.е. (X_i, Y_i, Z_i) – решения однородного алгебраического уравнения, задающие кривую X, $i = \overline{1,n}$; $F_j(P_i)$ – значения генераторных функций в точках кривой.

Это определение равносильно матричному представлению алгеброгеометрического кода:

$$G\,(i_0, i_1, ..., i_{k-1})^T = (c_0, c_1, ..., c_{n-1}) ,$$

где G – порождающая матрица размерности k×n, $k = \alpha - g + 1$, $\alpha = \deg X \cdot \deg F$.

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(P_0) & F_{k-1}(P_1) & ... & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k} .$$

Определение 2 [2]. Эллиптической кривой (EC) в аффинном пространстве A^2 над полем GF(q) называется гладкая кривая, заданная уравнением

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

или в P^2 заданная однородным уравнением

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3,$$

$a_i \in GF(q)$, род кривой g = 1.

Утверждение 1 [2]. Алгеброгеометрический (n, k, d) код по эллиптической кривой (эллиптический код) над GF(q) построенный через отображение вида $\varphi: EC \to P^{k-1}$ связан характеристиками $k + d \ge n$, причем:

$$n \le 2\sqrt{q} + q + 1 , \; k \ge \alpha, \; d \ge n - \alpha, \; \alpha = 3 \cdot \deg F.$$

Определение 3 [2]. Пусть X – гладкая проективная алгебраическая кривая в P^n, т.е. совокупность решений однородного неприводимого алгебраического уравнения степени degX с коэффициентами из GF(q), F – однородные одночлены степени degF. Алгеброгеометрический код по кривой X над GF(q) – это линейный код, состоящий из всех слов $(c_1, c_2, \ldots, c_n)$ длины $n \le N$, для которых выполняется равенство d + g – 1 уравнений

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0 ,$$

где $c_i \in GF(q)$, $d \ge \alpha - 2g + 2$, $\alpha = \deg X \cdot \deg F$.

Это определение равносильно матричному представлению алгеброгеометрического кода:

$$H\,(c_0, c_1, ..., c_{n-1})^T = 0 ,$$

где H – проверочная матрица кода размерности $r \times n$, $r = n - k = d + g - 2$

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{r-1}(P_0) & F_{r-1}(P_1) & ... & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r} .$$

Утверждение 2 [2]. Эллиптический (n, k, d) код над GF(q), построенный через отображение вида $\varphi: EC \to P^{r-1}$ связан характеристиками $k + d \geq n$, причем: $n \leq 2\sqrt{q} + q + 1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot degF$.

Определения 1 – 2 и результат утверждения 1 позволяют задать теоретико-кодовую схему Мак-Эллиса на основе эллиптических кодов следующим образом. Пусть G^{EC} – порождающая матрица эллиптического (n, k, d) кода над GF(q) вида

$$G^{EC} = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(P_0) & F_{k-1}(P_1) & ... & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}$$

и размерности k×n, $k = \alpha$, $\alpha = 3 \cdot degF$.

Пусть X – невырожденная k × k-матрица над GF(q), D – диагональная матрица с ненулевыми на диагонали элементами, P – перестановочная матрица размера n × n. Определим несимметричную крипто-кодовую систему Мак-Эллиса с эллиптическим кодом [11]:

– открытый ключ – матрица

$$G_X^{EC} = X \cdot G^{EC} \cdot P \cdot D,$$

– секретный (закрытый) ключ – матрицы X, P, D.

Закрытая информация (кодограмма) представляет собой вектор длины n и вычисляется по правилу

$$c_X^* = i \cdot G_X^{EC} + e,$$

где вектор $c_X = i \cdot G_X^{EC}$ принадлежит эллиптическому (n, k, d) коду с порождающей матрицей G_X^{EC}, i – k-разрядный информационный вектор, вектор e – секретный вектор ошибок веса ≤ t.

Чтобы задать несимметричную схему Нидеррайтера на эллиптических кодах воспользуемся другим определением алгеброгеометрического кода.

Определение 3 [1]. Пусть X – гладкая проективная алгебраическая кривая в P^n, т.е. совокупность решений однородного неприводимого алгебраического уравнения степени degX с коэффициентами из GF(q), F – однородные одночлены степени degF. Алгеброгеометрический код по кривой X над GF(q) – это линейный код, состоящий из всех слов $(c_1, c_2, \ldots, c_n)$ длины $n \leq N$, для которых выполняется равенство $d + g - 1$ уравнений

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0,$$

где $c_i \in GF(q)$, $d \geq \alpha - 2g + 2$, $\alpha = degX \cdot degF$.

Это определение равносильно матричному представлению алгеброгеометрического кода:

$$H\,(c_0, c_1, ..., c_{n-1})^T = 0,$$

где H – проверочная матрица кода размерности $r \times n$, $r = n - k = d + g - 2$

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{r-1}(P_0) & F_{r-1}(P_1) & ... & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}.$$

Определение 3 и результат утверждения 2 позволяют определить теоретико-кодовую схему Нидеррайтера на основе эллиптических кодов следующим образом. Пусть H^{EC} – проверочная матрица эллиптического (n, k, d) кода над GF(q) вида

$$H^{EC} = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{r-1}(P_0) & F_{r-1}(P_1) & ... & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}$$

и размерности r×n, $r = \alpha$, $\alpha = 3 \cdot degF$.

Пусть X – невырожденная k × k-матрица над GF(q), D – диагональная матрица с ненулевыми на диагонали элементами, P – перестановочная матрица размера n × n.

Определим несимметричную схему Нидеррайтера с эллиптическим кодом [12]:

– открытый ключ – матрица

$$H_X^{EC} = X \cdot H^{EC} \cdot P \cdot D,$$

– секретный (закрытый) ключ – матрицы X, P, D.

Закрытая информация (кодограмма) представляет собой вектор длины n и вычисляется по правилу

$$S_X = e \cdot \left(H_X^{EC} \right)^T,$$

где вектор e – вектор длины n и веса ≤ t, который несет конфиденциальную информацию (информационное сообщение, подлежащее закрытию).

Доказанные утверждения 1–2 и предложенные теоретико-кодовые схемы с эллиптическими кодами позволяют формировать кодограммы по несимметричному алгоритму, т.е. использовать открытый ключ для обмена закрытой информации.

Вместе с тем, проведенный в работе [1; 14] анализ программной реализации несимметричной крипто-кодовой системы на теоретико-кодовой схеме (ТКС) Мак-Элиса и Нидеррайтера показали на значительные сложности программной реализации, что существенно затрудняет использование НККС в протоколах открытых систем ГСИ.

Зависимость групповых операций реализации НККС от мощности поля приведена в табл. 2.

Таблица 2

Зависимость программной реализации от мощности поля

НККС MacElis	2^5	2^6	2^7	2^8	2^9	2^{10}
ЭК	10018042	18048068	32847145	47489784	63215578	82467897
укороченные ЭК	10007947	17787431	28595014	44079433	61974253	79554764
удлиненные ЭК	11156138	18561228	33210708	48297112	65171690	84051337

Для снижения энергозатрат криптопреобразований в НККС Мак-Элиса в работе [1] предлагается использовать модифицированные НККС (МККС) на модифицированных АГК на ЭК.

Наиболее простой и удобный способ модификации линейного блокового кода, не уменьшающий минимальное кодовое расстояние, состоит в укорочении его длины путем сокращения информационных символов. Пусть $I=(I_1, I_2, \ldots, I_k)$ – информационный вектор (n, k, d) блокового кода. Выберем подмножество h информационных символов, $|h|=x$, $x\leq 1/2k$. 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 3. 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 $\varphi: X\rightarrow P^{k-1}$, связан характеристиками k+d≥n, причем:

$$n = 2\sqrt{q} + q + 1 - x$$

$$k \geq \alpha - x,\ d \geq n - \alpha,\ \alpha = 3\cdot degF.$$

Утверждение 4. Укороченный эллиптический (n, k, d) код над GF(q), построенный через отображение вида $\varphi: X\rightarrow P^{r-1}$, связан характеристиками k+d≥n, причем:

$$n = 2\sqrt{q} + q + 1 - x$$

$$k \geq n - \alpha,\ d \geq \alpha,\ \alpha = 3\cdot degF.$$

Используя результат утверждений 3–4, зададим теоретико-кодовую схему на модифицированных эллиптических кодах, построенную через отображение вида $\varphi: X \rightarrow P^{k-1}$ и $\varphi: X \rightarrow P^{r-1}$. Справедливы следующие утверждения.

Утверждение 5. Укороченный эллиптический (n, k, d) код над $GF(2^m)$, построенный через отображения вида $\varphi: X\rightarrow P^{k-1}$, определяет модифицированную теоретико-кодовую схему с параметрами:

$$l_{K_+} = x\left\lceil \log_2\left(2\sqrt{q} + q + 1\right)\right\rceil;$$

$$l_I = (\alpha - x)\cdot m;$$

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

Утверждение 6. Укороченный эллиптический (n, k, d) код над $GF(2^m)$, построенный через отображения вида $\varphi: X\rightarrow P^{r-1}$, определяет модифицированную теоретико-кодовую схему с параметрами:

– размерность секретного ключа определяется выражением $l_{K_+} = x\left\lceil \log_2\left(2\sqrt{q} + q + 1\right)\right\rceil$;

– размерность информационного вектора (в битах):

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

– размерность кодограммы определяется выражением $l_S = \left(2\sqrt{q} + q + 1 - x\right)\times m$;

– относительная скорость передачи:

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

В работе [1] приведены формальное описание модифицированной несимметричной криптокодовой системы защиты информации на основе использования методов модификации и практические алгоритмы формирования кодограмм и их раскодирования в МНККС Мак-Элиса.

Для дальнейшего снижения затрат на программную реализацию в работе предлагается использовать в МНККС Мак-Элиса ущербные коды.

Второй способ модификации линейного блокового кода, который сохраняет минимальное кодовое расстояние и увеличивает количество передаваемых данных, состоит в удлинении его длины после формирования вектора инициализации, путем сокращения информационных символов. Пусть $I = (I_1, I_2, \ldots, I_k)$ – информационный вектор (n, k, d) блокового кода. Выберем подмножество h информационных символов, $|h| = x$, $x \leq 1/2k$ и сформируем вектор инициализации. Поместим в информационный вектор I в подмножество h нулей, т.е. $I_i = 0$, $\forall I_i \in h$. На остальных позициях вектора I поместим информационные символы. После в позиции вектора инициализации добавляем информационные символы. Для модификации (удлинения) эллиптических кодов будем использовать уменьшение набора точек кривой. Справедливо следующее утверждение.

Утверждение 7. 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. Зафиксируем подмножество $h_1 \subseteq h$, $|h_1| = x_1$. Пусть задан эллиптический (n, k, d) код над GF(q), построенный через отображение вида $\varphi: X \to P^{k-1}$. Тогда параметры удлиненного на x_1 символов из GF(q) эллиптического кода, построенного через отображение вида $\varphi:(X \cup h_1) \to P^{k-1}$, $n = 2\sqrt{q} + q + 1 - x + x_1$ будут связаны соотношениями: $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3 \cdot \text{degF}$.

Доказательство. Если $x_1 < x$, то удлинение кода на x_1 эквивалентно укорочению исходного кода на $x - x_1$. Подставив эти параметры в выражение $n = 2\sqrt{q} + q + 1 - x + x_1$, получим результат следствия 6. □

Следствие 1. Если известен вид эллиптической кривой (набор $a_1 \ldots a_6$, $\forall a_i \in GF(q)$), то подмножества h и h_1 полностью определяют модифицированные эллиптические (n, k, d) коды над GF(q), построенные через отображения вида: $\varphi: X \to P^{k-1}$ и $\varphi:(X \cup h_1) \to P^{k-1}$.

Доказательство. Набор коэффициентов $a_1 \ldots a_6$, $\forall a_i \in GF(q)$ однозначно задает вид эллиптической кривой и, соответственно, набор ее точек EC(GF(q)). Используя отображение вида $\varphi: EC \to P^M$ и результаты утверждений 1, 2, построим эллиптический (n, k, d) код над GF(q). Если известны символы удлинения, то построим удлиненные коды.

По утверждению 6, это символы множества h_1, которые полностью определяют модифицированный эллиптический (n, k, d) код над GF(q). □

Утверждение 8. Зафиксируем подмножество $h_1 \subseteq h$, $|h_1| = x_1$. Пусть задан эллиптический (n, k, d) код над GF(q), построенный через отображение вида $\varphi: X \to P^{r-1}$. Тогда параметры удлиненного на x_1 символов из GF(q) эллиптического кода, построенного через отображение вида $\varphi:(X \cup h_1) \to P^{r-1}$, будут связаны соотношениями: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot \text{degF}$.

Следствие 2. Если известен вид эллиптической кривой (набор $a_1 \ldots a_6$, $\forall a_i \in GF(q)$), то подмножества h и h_1 полностью определяют модифицированные эллиптические (n, k, d) коды над GF(q), построенные через отображения вида: $\varphi: X \to P^{r-1}$ и $\varphi:(X \cup h_1) \to P^{r-1}$.

Доказательство. Набор коэффициентов $a_1 \ldots a_6$, $\forall a_i \in GF(q)$ однозначно задает вид эллиптической кривой и, соответственно, набор ее точек EC(GF(q)). Используя отображение вида $\varphi: EC \to P^M$ и результаты утверждений 1 – 2, построим эллиптический (n, k, d) код над GF(q). Если известны символы удлинения, то построим удлиненные коды. По утверждению 7, это символы множеств h и h_1, которые полностью определяют модифицированный эллиптический (n, k, d) код над GF(q). □

Результаты утверждений 6, 7 и их следствия позволяют построить модифицированные (удлиненные в пределах $n \leq 2\sqrt{q} + q + 1$) эллиптические (n, k, d) коды над GF(q).

2. Основные принципы построения криптосистем на ущербных кодах.

В работах [19; 20] рассмотрены теоретические и практические основы построения ущербных кодов. Под *ущербным текстом понимается текст, полученный дальнейшей деформацией неизбыточных кодов букв.*

Таким образом, необходимым и достаточным условием ущербности текста с потерей смысла является сокращение длин кодов символов текста за пределами их избыточности. Как следствие, ущербный текст имеет длину меньшую длины исходного текста, и не имеет смысла исходного текста [19].

Теоретической основой построения ущербных текстов является удаление упорядоченности символов исходного текста и как следствие снижение избыточности символов языка в ущербном тексте.

При этом количество информации, выражающее эту упорядоченность, будет равно уменьшению энтропии текста по сравнению с максимально возможной величиной энтропии, соответствующей отсутствию упорядоченности в тексте вообще, т.е. равновероятному появлению любой буквы после любой предыдущей буквы. Методы вычисления информации, предложенные К. Шенноном, позволяют выявить соотношение количества предсказуемой (т.е. формируемой по определенным правилам) информации и количества той неожиданной информации, которую нельзя заранее предсказать.

Избыточность текста рассчитаем по формуле

$$B(M) = B_A L_0 = \left(\log N - \frac{H(M)}{L_0} \right) \times L_0 ,$$

где M – исходный текст;

B – избыточность языка ($B = R - r$, R – абсолютная энтропия языка ($R = \log N$, N – мощность алфавита, r – энтропия языка на один символ, $r = H(M) / L$, L – длина сообщения M в символах языка);

H(M) – энтропия (неопределенность) сообщения;

L_0 – длина сообщения M в символах языка со смыслом;

B_A – избыточность языка.

Для получения ущербного текста (FTC) и ущерба (DCH) используется метод “идеального” сжатия после выполнения m циклов механизма нанесения ущерба C_m [19; 20].

Количество циклов, необходимых для уменьшения длины исходного текста, равно:

$$m \rangle \frac{\log n - B_A}{\log \eta},$$

где n – мощность представления символа исходного текста;

B_A – избыточность языка;

η – количество раз уменьшения длины исходного текста в MV2 на каждом шаге (некоторый постоянный коэффициент).

Количественной мерой эффективности нанесения ущерба является степень разрушения смысла, равная разности энтропий ущербного текста и исходного текста на различных отрезках длины ущербного текста:

$$d = H(FTC) - \sum_{i=1}^{s} H(M_i)p_i, \quad \sum_{i=1}^{s} p_i = 1, \quad s = \left[\frac{L_0 - L_{FTC}}{L_{FTC}} \right],$$

где M_i – часть исходного текста, соответствующая i-му отрезку, p_i – ее вероятность, L_0 – длина M_i равна длине L_{FTC} – ущербного текста, s – количество отрезков. Для эргодичного источника символов исходного текста:

$$d_{max} = \log L_{FTC} - H(M_i).$$

На рис. 2 приведена структурная схема одного шага универсального механизма нанесения ущерба.

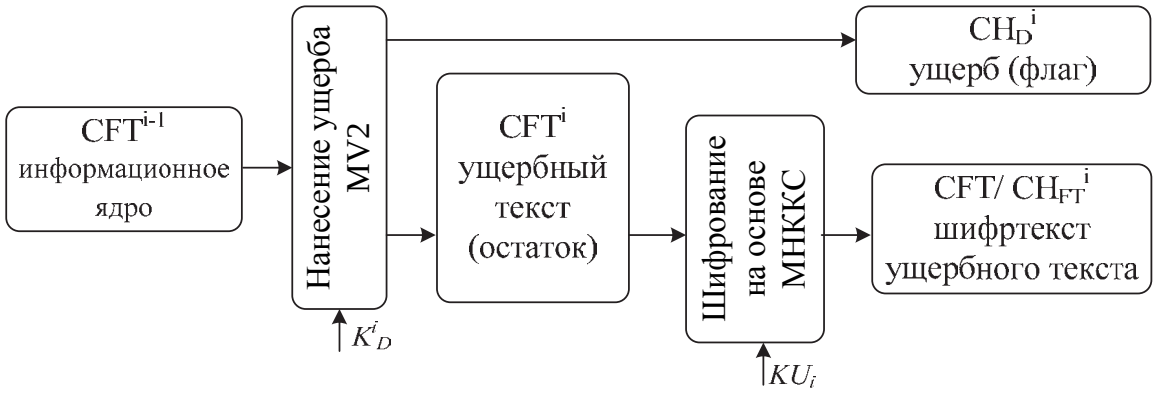


Рис. 2. Структурная схема одного шага универсального механизма нанесения ущерба

Под *информационным ядром* некоторого текста понимается ущербный текст CFT, полученный циклическим преобразованием универсального механизма нанесения ущерба C_m.

Универсальный механизм нанесения ущерба C_m может быть описан [19; 20]:

$$CFT / CH_{FT} = E_1\left(M, KU^{EC}\right),$$

$$CHD / CH_D = E_2\left(M, KU^{EC}\right),$$

$$M = E_{1,2}^{-1}(CFT / CH_{FT}, CHD / CH_D, KU^{EC}),$$

$$CFT / CH_{FT} = CFT / CH_{FT}^{i}, ..., CFT / CH_{FT}^{m},$$

где $KU^{EC} = \varphi(K_D^i, ..., K_D^m, KU_1^{EC}, ..., KU_m^{EC},$

$$CHD / CH_D = CHD / CH_D^i, ..., CHD / CH_D^m.$$

Таким образом, в результате имеем два шифртекста (ущерб (CH_D) и ущербный текст (FTC)), каждый из которых не имеет смысла ни в алфавите исходного текста, ни в алфавите шифртекста. Фактически шифртекст исходного сообщения (M) представляется в виде совокупности двух ущербных шифртекстов, каждый из которых в отдельности не может восстановить исходный текст.

Для восстановления исходной последовательности нет необходимости знать промежуточные ущербные последовательности. Необходимо знать только последнюю ущербную последовательность (последний ущербный текст после выполнения всех циклов) и все ущербы с правилами их нанесения.

Основные способы нанесения ущерба представлены на рис. 3, на рис. 4 приведены основные протоколы обеспечения услуг безопасности на основе использования ущербных кодов.

Криптографическими ущербными текстами называются тексты, полученные следующими способами [19]:

нанесением ущерба исходному тексту с последующим шифрованием ущербного текста и/или его ущербов;

нанесения ущерба шифртексту;

нанесения ущерба шифртексту ущербного текста и/или шифртексту ущербов.

Основным преимуществом в предлагаемых способах и протоколах обеспечения услуг безопасности на основе использования ущербных кодов является использование не БСШ, а МНККС Мак-Элиса и Нидеррайтера для обеспечения криптостойкости ущерба и/или ущербного текста.

Рис. 3. Основные способы нанесения ущерба

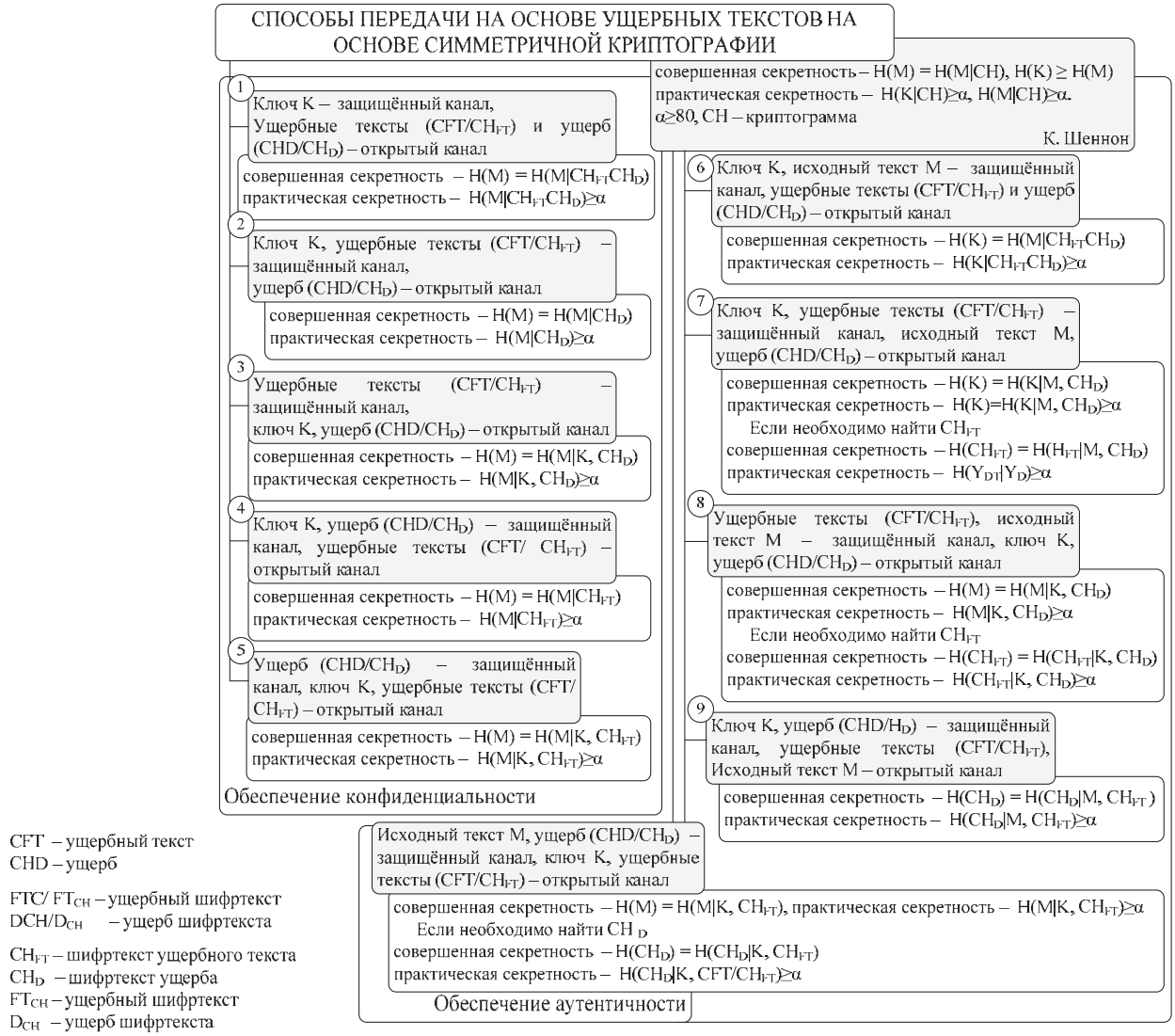


Рис. 4. Основные протоколы обеспечения услуг безопасности на основе использования ущербных кодов

Для оценки криптостойкости авторами [19; 20], предлагается использовать шенноновское понятие “расстояние единственности” шифра по открытому тексту – минимальное натуральное число L, при котором по известному шифртексту однозначно восстанавливается соответствующее сообщение, и “расстояние единственности” по ключу – минимальное натуральное число L, при котором по известному шифртексту однозначно определяется ключ шифрования.

Расстояние единственности для модели случайного шифра, для которого существует вероятность получить осмысленный текст при случайном и равновероятном выборе ключа K и попытке дешифрования шифртекста, при

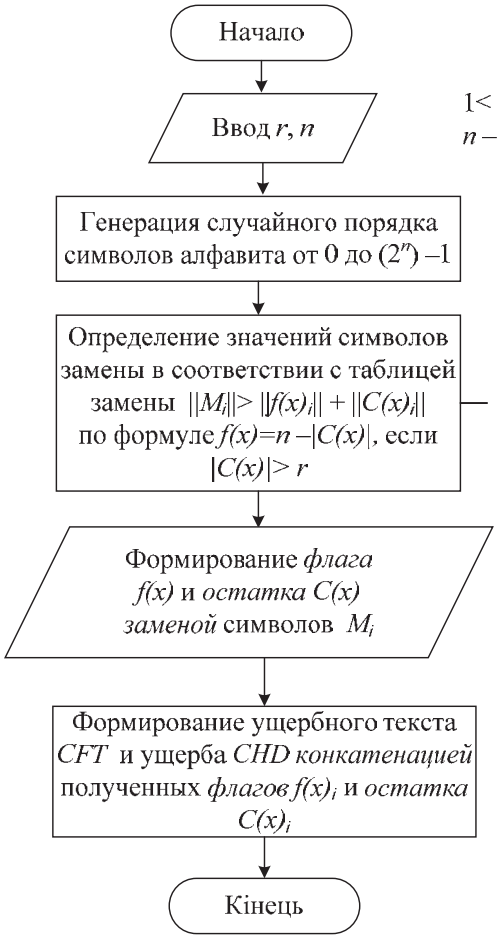
$$N_S = H(K)\frac{2^{HL}}{|I|^L} = 1:$$

$$L = U_0 = \frac{H(K)}{\log|I| - H} = \frac{H(K)}{B\log|I|},$$

где– избыточность исходного текста;

H – энтропия на букву осмысленного текста во входном алфавите I, |I| >2, 2^{HL} – приближенное значение числа осмысленных текстов.

В работах [19; 20] под ц*иклическим алгоритмом получения ущербных текстов* понимается универсальный механизм нанесения ущерба (C_m, где m – число циклов), который заключается в случайной замене битового представления каждого символа исходного текста кортежем меньшего или равного числа бит с последующей их конкатенацией. На рис. 5 приведен универсальный механизм нанесения ущерба (алгоритм MV2 (формирования ущербного текста)).



$1 < r < n$ – положительное целое число
n – мощность алфавита

Символ	Длина остатка	Остаток $C(x)$	Флаг $f(x)$
M_1	r	0^r	$0^{n-r-1}1$
M_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
M_{2^r+1}	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$M_{2^{n-1}-2^r}$	$n-2$	1^{n-2}	01
$M_{2^{n-1}-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$M_{2^n-2^r}$	$n-1$	1^{n-1}	1
$M_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…

CFT/ CH_{FT} – шифртекст ущербного текста
CHD/CH_D – шифртекст ущерба
FTC/ FT_{CH} – ущербный шифртекст
DCH/D_{CH} – ущерб шифртекста
$f(x)$ – флаг (ущерб)
$C(x)$ – остаток (ущербный код)

Рис. 5. Универсальный механизм нанесения ущерба (алгоритм MV2)

Область определения преобразования в алгоритме MV2 – множество $\{0, 1\}^n$ – рассматриваем как мощность алфавита некоторого семейства исходных текстов, с которым связано некоторое распределение вероятностей букв этого алфавита, а символы исходного текста – значения дискретного случайного элемента [19].

Пусть X – случайный дискретный элемент, принимающий значения $x_i \in \{0,1\}^n$ с вероятностями p_i и $T = (c, f) \in F_n^r$ – произвольное фиксированное преобразование MV2. Тогда для любого $y \in U_{r\,n-1}$ (некоторая двоичная строка из множества строк

переменной длины) и для любого $1 \le i \le |y|$ выполняется:

$$\#\left\{x \in \{0,1\}^n : c(x) = y\right\} = \#\left\{x \in \{0,1\}^n : c(x) = y^{(i)}\right\}.$$

Тогда независимо от распределения вероятностей случайного элемента X для энтропий случайных элементов FTC/FT_{CH} (ущербного шифртекста) и CHD (ущерба) выполняются равенства:

$$H(FTC / FT_{CH}) \le \log(2^n - 2^r),$$
$$H(CHD) \le \log(n - r + 1).$$

Таким образом, при равномерном распределении входов (флагов) алгоритма MV2 формируется равномерное распределение выхода (остатка):

$$P(c_k = 0 \,|\, 0 \le k \le |FTC / FT_{CH}|) = \frac{1}{2}.$$

Выводы

В работе впервые представлено теоретическое обоснование использования ущербных кодов в интегрированных механизмах обеспечения достоверности, безопасности и оперативности информационного трафика в протоколах открытых систем ГСИ, позволяющие строить гибридные (комплексные) криптосистемы. Основным отличием от известных гибридных систем является использование несимметричных крипто-кодовых систем вместо симметричных методов шифрования и использование систем на основе ущербных кодов для формирования многоканальной криптографии и/или увеличения криптостойкости за счет использования алгоритма MV2. Многоканальная криптография на основе МНККС Мак-Элиса и Нидеррайтера позволяет обеспечить основные услуги безопасности на основе комплексирования крипто-кодовых систем и систем на основе ущербных кодов, что позволяет обеспечить требуемые показатели стойкости, расширить услуги безопасности в открытых системах и многих практических приложениях ГСИ. Применение ущербных кодов в МНККС позволяет существенно снизить энергетические затраты на программную реализацию без снижения уровня криптостойкости.

Список литературы

1. Евсеев С.П. Анализ программной реализации прямого и обратного преобразования по методу недвоичного равновесного кодирования / С.П. Евсеев, Х.Н. Рзаев, А.С. Цыганенко // Науково-технічний журнал “Безпека інформації”. – Київ. – 2016. – Том. 22, № 2. – С. 196-203.

2. Евсеев С.П. Разработка модифицированной несимметричной крипто-кодовой системы Мак-Элиса на укороченных эллиптических кодах / С.П. Евсеев, О.Г. Король, Х.Н. Рзаев, З.Р. Иманова // Восточно-европейский журнал передовых технологий. – Харьков. – 2016. – Том 4. 9(82). – С. 18-26.

3. Евсеев С.П. Усовершенствование метода двухфакторной аутентификации на основе использования модифицированных крипто-кодовых схем / С.П. Евсеев, В.Г. Абдуллаев, Ж.Ф. Агазаде, В.С. Аббасова // Системи обробки інформації. – Х.: ХНУПС, 2016. – Вип. 9(146). – С. 132-145.

4. Evseev S.P. Developing of multi-factor au-thentication method based on Niederreiter-McEliece modi-fied crypto-code system / S.P. Evseev, G.P. Koc, E.V. Lekarev // Восточно-европейский журнал передовых технологий. – Харьков. – 2016. 6/4(84). – С. 11-23.

5. Transmission of Picturesque content with Code Base Cryptosystem [Электронный ресурс]. – Режим доступа: https://doaj.org/article/6714b60516cc4aa79e56d0c421febaf3.

6. Steganography application program using the ID3v2 in the MP3 audio file on mobile phone [Электронный ресурс]. – Режим доступа: https://doaj.org/article/707a6506be9e49698fd75323fcc1302c.

7. Space-Age Approach To Transmit Medical Image With Codebase Cryptosystem Over Noisy Channel [Электронный ресурс]. – Режим доступа: https://doaj.org/article/5c7da3a1e3ec4f83b552199034bd3241.

8. An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel [Электронный ресурс]. – Режим доступа: https://doaj.org/article/39a3ac65d5b24b348f069dfc82eb6248.

9. A Novel Approach For Information Security In Ad Hoc Networks Through Secure Key Management [Электронный ресурс]. – Режим доступа: https://doaj.org/article/378b88837cdf4cab9f8010a38a6aeb2b.

10. 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: сборник научных трудов НАУ. – К.: НАУ, 2016. – Вып. 23. – С. 24-26.

11. McEliece R.J. A Public-Key Criptosystem Based on Algebraic Theory / R.J. McEliece // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.

12. Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory / H. Niederreiter // Probl. Control and Inform. Theory. – 1986. –V.15. – P. 19-34.

13. Блейхут Р. Теория и практика кодов, контролирующих ошибки [Текст]: пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с.

14. Кларк Дж.-мл. Кодирование с исправлением ошибок в системах цифровой связи [Текст]: пер. с англ. / под ред. Б.С. Цыбакова / Кларк Дж.-мл. – М.: Радио и связь, 1987. – 392 с.

15. Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки [Текст] / Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн. – М.: Связь, 1979. – 744 с.

16. Мутер В.М. Основы помехоустойчивой телепередачи информации [Текст] / В.М. Мутер. – Л.: Энергоатомиздат. Ленингр. отд-ние, 1990. – 288 с.

17. Теория кодирования [Текст]: пер. с япон. / Т. Касами, Н. Токура, Е. Ивадари, Я. Инагаки / под ред. Б.С. Цыбакова и С.И. Гельфанда. – М.: Мир, 1978. – 576 с.

18. Сидельников В.М. Криптография и теория кодирования / В.М. Сидельников // Материалы конференции «Московский университет и развитие криптографии в России». – М.: МГУ. – 2002. – 22 с.

19. Мищенко В.А. Ущербные тексты и многоканальная криптография / В.А. Мищенко, Ю.В. Виланский. – Минск: Энциклопедикс, 2007. – 292 с.

20. Мищенко В.А. Криптографический алгоритм MV 2 / В.А. Мищенко, Ю.В. Виланский, В.В. Лепин. – Минск, 2006. – 177 с.

References

1. Evseev, S.P., Rzaev, H.N. and Cyganenko, A.S. (2016), "Analiz programmnoj realizacii prjamogo i obratnogo preobrazovanija po metodu nedvoichnogo ravnovesnogo kodirovanija" [Analysis of the software implementation of direct and inverse transformation using the non-binary equilibrium coding method], *Scientific and Technical Journal "Security of Information"*, Vol. 22, No. 2, Kiev, pp. 196-203.

2. Evseev, S.P., Korol', O.G., Rzaev, H.N. and Imanova, Z.R. (2016), "Razrabotka modificirovannoj nesimmetrichnoj kripto-kodovoj sistemy Mak-Jelisa na ukorochennyh jellipticheskih kodah" [Development of a modified asymmetric McElice crypto-code system on truncated elliptic codes], *East European Journal of Advanced Technologies*, Vol. 4. 9 (82), Kharkiv, pp. 18-26.

3. Evseev, S.P., Abdullaev, V.G., Agazade, Zh.F. and Abbasova, V.S. (2016), "Usovershenstvovanie metoda dvuhfaktornoj autentifikacii na osnove ispol'zovanija modificirovannyh kripto-kodovyh shem" [Improvement of the method of two-factor authentication based on the use of modified crypto-code schemes] Information Processing Systems, No. 9 (146), pp. 132-145.

4. Evseev, S.P., Koc, G.P. and Lekarev, E.V. (2016), "Developing of multi-factor au-thentication method based on Niederreiter-McEliece modi-fied crypto-code system" [Developing of the multi-factor au-thentication method based on the Niederreiter-McEliece modi-fied crypto-code system], *East European Journal of Advanced Technologies*, 6/4 (84), Kharkiv, pp. 11-23.

5. Transmission of Picturesque content with Code Base Cryptosystem, https://doaj.org/article/6714b60516cc4aa79e56d0c421fe.

6. Steganography application program using the ID3v2 in the MP3 audio file on mobile phone, https://doaj.org/article/707a6506be9e49698fd75323fc1.

7. Space-Age Approach To Transmit Medical Image With Codebase Cryptosystem Over Noisy Channel, https://doaj.org/article/5c7da3a1e3ec4f83b552199034bd.

8. An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel, https://doaj.org/article/39a3ac65d5b24b348f069dfc82eb.

9. A Novel Approach For Information Security In Ad Hoc Networks Through Secure Key Management, https://doaj.org/article/378b88837cdf4cab9f8010a38a6a.

10. Rzaev, H.N., Iskenderzade, G.G., Samedov, F.G., Imanova, Z.B. and Dzhamalova, Zh.S. (2016), "Matematicheskie modeli kripto-kodovyh sredstv zashhity informacii na osnove TKS" [Mathematical Models of Crypto-Code Means of Information Protection Based on TKS], *Protection of information: a collection of scientific works of NAU*, Issue. 23, NAU, Kiev, pp. 24-26.

11. McEliece, R.J. (1978), A Public-Key Criptosystem Based on Algebraic Theory, *DGN Progres Report 42-44*, January – February, Jet Propulsi on Lab. Pasadena, CA., pp. 114-116.

12. Niederreiter, H. (1986), Knapsack-Type Cryptosystems and Algebraic Coding Theory, *Probl. Control and Inform. Theory*, Vol. 15, pp. 19-34.

13. Bleikhut, R. (1986), *"Teorija i praktika kodov, kontrolirujushhih oshibki"* [*Theory and practice of codes that control errors*], Mir, Moscow, 576 p.

14. Clark, J.-m. (1987), "*Kodirovanie s ispravleniem oshibok v sistemah cifrovoj svjazi"* [*Coding with error correction in digital communication systems*], Radyo y sviaz, Moscow, 392 p.

15. McWilliams, F.J. and Sloan, N.J.A. (1979), *"Teorija kodov, ispravljajushhih oshibki"* [*Theory of Error Correcting Codes*], Sviaz, Moscow, 744 p.

16. Muter, V.M. (1990), "*Osnovy pomehoustojchivoj teleperedachi informacii"* [*Fundamentals of noise-proof telecasting of information*], Energoatomizdat, Leningr. Otd-tion, Leningrad, 288 p.

17. Kasami, T., Tokura, N., Iwadari, E. and Inagaki, J. (1978), *"Teorija kodirovanija"* [*Theory of coding*], Mir, Moscow, 576 p.

18. Sidelnikov, V.M. (2002), "Kriptografija i teorija kodirovanija" [Cryptography and coding theory], *Proceedings of the conference "Moscow University and the Development of Cryptography in Russia"*, Moscow State University, Moscow, 22 p.

19. Mishchenko, V.A. and Vilansky, Yu.V. (2007), "*Ushherbnye teksty i mnogokanal'naja kriptografija"* [*Damage texts and multichannel cryptography*], Encyclopedic, Minsk, 292 p.

20. Mishchenko V.A., Vilansky, Yu.V. and Lepin, V.V. (2006), *"Kriptograficheskij algoritm MV 2"* [*Cryptographic algorithm MV 2*]. Minsk, 177 p.

Поступила в редколлегию 07.08.2017
Одобрена к печати 19.10.2017

Відомості про автора:

Євсєєв Сергій Петрович
кандидат технічних наук старший науковий співробітник
доцент кафедри Харківського національного
економічного університету ім. С. Кузнеця,
Харків, Україна
https://orcid.org/0000-0003-1647-6444
e-mail: Serhii.Yevseiev@hneu.net

Information about the author:

Yevseiev Serhii
PhD Senior Research of
Simon Kuznets Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0003-1647-6444
e-mail: Serhii.Yevseiev@hneu.net

ВИКОРИСТАННЯ ЗБІТКОВИХ КОДІВ В КРИПТО-КОДОВИХ СИСТЕМАХ

С.П. Євсеєв

Розглядаються загальна конструкція несиметричних крипто-кодових систем (НККС) на основі теоретико-кодової схеми (ТКС) Мак-Еліса на алгеброгеометричних (АГК) на еліптичних кривих (еліптичних кодах, ЕС), що дозволяють інтегровано (одним механізмом) забезпечувати необхідний рівень безпеки на основі теоретико-сложностной завдання – декодування випадкового коду (забезпечується $10^{30} – 10^{35}$ групових операцій, при потужності поля GF (2^{10}), оперативності – на рівні швидкодії криптоперетворень блоково-симетричних шифрів (БСШ), вирогідності – на основі алгеброгеометричних (завадостійких m-ічних кодів) забезпечення $P_{пом}$ $10^{-9} – 10^{-12}$. Аналізуються способи побудови збиткових кодів, багатоканальні протоколи забезпечення безпеки на основі НККС на збиткових кодах. Використання збиткових кодів дозволяє збільшити швидкодію кодових перетворень в НККС за рахунок зменшення потужності поля GF (24 - 26), забезпечивши необхідний рівень криптостійкості на основі збільшення повної ентропії збиткових кодів (збільшення відстані єдиності ключових даних). Отримані результати дозволяють будувати гібридні (комплексні) криптосистеми, забезпечуючи основні показники безпеки, оперативності та достовірності, що пред'являються до сучасних комунікаційних систем і мереж.

Ключові слова: *несиметрична крипто-кодова система, теоретико-кодова схема, перешкодостійкі алгеброгеометріческіе коди, збіткові коди.*

THE USE OF DAMAGED CODES IN CRYPTO CODE SYSTEMS

S. Yevseiev

The article proves the urgency of studies on the construction of hybrid (complex) cryptosystems based on systems on defective codes and crypto-code structures, with considering the requirements for technical security facilities in open communication systems and networks (CSN). The development of computer systems in the era of high technology extends the functional range of their application in various areas of open corporate and global systems. However, their development contributes to the modernization of old and the emergence of new attacks, the development of cyber-attacks on the management systems of corporate and global systems. This puts forward new requirements to the basic information security requirements for the circulating CSN, without reducing the basic reliability (authenticity) and efficiency (throughput) parameters affecting the quality of service for subscribers of open corporate and global networks. To ensure the evitable quality of service requirements, the work analyzes the fundamentals of building crypto-code systems based on the modified McElis and Niederreiter theoretic-code schemes on modified algebra-geometric codes (elliptic codes, EC), which allow one to provide (with integrated) the required reliability and efficiency indicators Crypto-transformations (1030 - 1035 group operations are provided with stability, with field strength GF (2^{10}), efficiency - at the level of performance, crypto formations block-symmetric ciphers (BSC) reliability – based on Algebraic (m-ary error-correcting codes) provide Posh $10^{-9} – 10^{-12}$). A significant drawback in the practical implementation of these cryptosystems is the significant energy costs due to the need to build on GF (2^{10}). An analysis of the theoretical foundations of the use of multichannel systems on defective codes is carried out. The results obtained make it possible to construct hybrid (complex) cryptosystems based on McElis modified non-symmetric crypto-coded systems (MCCS) using defective codes, the main difference from the known approaches for constructing hybrid cryptosystems is the use of MCCS instead of symmetric cryptosystems with the further use of systems on defective codes. For the first time, the approach proposed in the work of the formation of hybrid cryptosystems based on the MCCS on the defective codes makes it possible to reduce the energy costs in their practical implementation on the basis of a reduction in power, the alphabet used.

Keywords*: asymmetric crypto-code system, the code-theoretic scheme, noise-resistant algebraic geometry codes, defective codes.*