DOI: 10.18372/2410-7840.19.12206
УДК 621.391

ИССЛЕДОВАНИЯ СВОЙСТВ ГИБРИДНЫХ КРИПТО-КОДОВЫХ КОНСТРУКЦИЙ

Сергей Евсеев, Сергей Остапов, Иван Белодед

Рассмотрены способы построения гибридных крипто-кодовых конструкций с ущербными кодами (ГККУК) на основе синтеза модифицированных несимметричных крипто-кодовых систем Мак-Элиса (МНККС) на эллиптических кодах (ЕС) с многоканальными криптографическими системами на ущербных кодах, протоколы обмена для обеспечения конфиденциальности в IP-сетях. Исследуются основные критерии криптосистем, а также теоретические основы снижения в 2 – 3 раза энергетической емкости предложенных МНККС Мак-Элиса с ЕС и гибридных конструкций МНККС с ущербными кодами за счет уменьшения мощности поля Галуа без снижения уровня криптостойкости гибридной криптосистемы в целом при их программной реализации. Получены результаты статистических исследований стойкости на основе пакета NIST STS 822.

Ключевые слова: *гибридные крипто-кодовые конструкции, модифицированная крипто-кодовая система Мак-Элиса, ущербные коды, модифицированные эллиптические коды.*

Введение. Развитие информационно-коммуникационных 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 [1]. 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. Проведенные исследования [2]-[4] показали, что угрозы приобрели признаки гибридности и комплексирования, что приводит к появлению синергизма при их внедрении. В этих условиях одним из актуальных направлений обеспечения безопасности информационных потоков в ГСИ можно считать создание системы интегрированной защиты сетевых ресурсов на основе синтеза модифицированных несимметричных крипто-кодовых систем (МНККС) Мак-Элиса и Нидеррайтера на алгеброгеометрических кодах (АГК). В работе [6] рассматривалась двуключевая криптографическая система на основе модифицированной схемы Мак-Элиса. Суть модификации, в отличие от нашего случая, сводилась к использованию ошибки для кодирования информационных битов. Однако, основные усилия были направлены на ускорение работы с ключами, поскольку, как известно, большой размер ключевой информации являются одним из основных недостатков схемы Мак-Элиса. Представление публичного ключа в виде (*row echelon form*) позволило ускорить время обработки ключевой информации в 5 – 10 раз. В работе [7] указано, что существенным недостатком данных криптосистем является большой объем ключевых данных, что существенно затрудняет их практическую реализацию. Для снижения ключевых данных в работе [8] рассматриваются механизмы уменьшения длины кодового слова без уменьшения исправляющей способности кода, что позволяет уменьшить энергетические затраты на практическую реализацию криптосистем без снижения уровня криптостойкости. Перспективным направлением использования НККС Мак-Элиса и Нидеррайтера является их использование в синтезе с системами многоканальной криптографии на ущербных кодах. В работах [9, 10] под ущербными кодами понимается циклический алгоритм получения ущербных текстов, который заключается в случайной замене битового представления каждого символа исходного текста кортежем меньшего или равного числа бит с последующей конкатенацией. Полученные при нанесении ущерба исходному тексту ущерб и ущербный текст для усиления криптостойкости

предлагается в [9, 10] шифровать симметричным криптоалгоритмом и передавать различными каналами. Применение синтезированных гибридных крипто-кодовых конструкций НККС Мак-Элиса с системой многоканальной криптографии на ущербных кодах позволяет одним механизмом интегрировано обеспечить требуемые уровни показателей достоверности, безопасности и оперативности при обработке и передаче конфиденциальной информации по открытым каналам ГСИ [5]-[10].

Исходя из актуальности, *целью* данной работы является исследование способов построения гибридных крипто-кодовых конструкций на ущербных кодах (ГККУК) на основе МНККС Мак-Элиса на эллиптических кодах (ЕС), сравнительный анализ свойств МНККС на АГК с ГККУК. Проведение исследований энергетических затрат при их программной реализации, оценка статистических свойств их криптостойкости на основе пакета NIST STS822.

Анализ публикаций [5]-[7] подтверждают, что их применение обеспечивает быстродействие на уровне криптопреобразований симметричных блочных криптоалгоритмов (БСШ), доказуемую криптостойкость на основе теоретико-сложностной задачи декодирования случайного кода (применение теоретико-кодовой схемы Мак-Элиса на ЕС над полем $GF\ (2^{10})$ обеспечивает криптостойкость 10^{30}-10^{35} групповых операций), и достоверность на основе использования алгеброгеометрического кода (АГК) (обеспечивается $P_{ош}$ 10^{-9}-10^{-12}).

Однако существенным недостатком практического применения НККС Мак-Элиса являются большие объемы ключевых данных (для обеспечения требуемой криптостойкости необходимо построение системы в поле GF (2^{10}-2^{13})). В работе [5] авторами предложены способы модификации АГК на основе укорочения /удлинения кодового слова, что позволяет снизить энергетическою емкость практической реализации МНККС Мак-Элиса над полем GF (2^6-2^8) без снижения стойкости криптосистемы.

На основе синтеза МНККС Мак-Элиса на модифицированных АГК с системами многоканальной криптографии на ущербных кодах [9], [10] получены ГККУК, рассмотренные в работе [5]. Использование ущербных кодов позволяет уменьшить мощность поля GF (2^4-2^6) для построения модифицированных крипто-кодовых конструкций на основе МНККС Мак-Элиса на модифицированных (укороченных /удлиненных) эллиптических кодах (МЕС), сохранив при этом уровень криптостойкости полной НККС Мак-Элиса, за счет увеличения расстояния единственности ключа на основе полной совокупности энтропии ущербных текстов [11].

Способы построения гибридных крипто-кодовых конструкций на основе МНККС Мак-Элиса на ущербных кодах. 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, $|h|=x$, $x \le 1/2k$. 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: $n = 2\sqrt{q} + q + 1 - x$, $k \ge \alpha - x$, $d \ge n - \alpha$, $\alpha = 3 \cdot degF$.

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: $n = 2\sqrt{q} + q + 1 - x$, $k \ge n - \alpha$, $d \ge \alpha$, $\alpha = 3 \cdot degF$.

Утверждения 1, 2 позволяют формировать крипто-кодовую конструкцию 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 крипто-кодовую конструкцию с параметрами: $l_{K_+} = x\lceil \log_2(2\sqrt{q}+q+1) \rceil$; $l_l = (\alpha - x) \cdot m$; $R = (\alpha - x)/\left(2\sqrt{q} + q + 1 - x\right)$;

Утверждение 4. Укороченный эллиптический *(n, k, d)* код над $GF(2^m)$, построенный через отображения вида $\varphi: X \to P^{r-1}$, определяет модифицированную крипто-кодовую конструкцию с параметрами: размерность секретного ключа определяется выражением $l_{K_+} = x\lceil \log_2(2\sqrt{q}+q+1)\rceil$;

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

Для дальнейшего снижения затрат на программную реализацию предлагается использовать в МНККС Мак-Элиса ущербные коды. Протокол обмена с использованием ГККККУК на основе МККС Мак-Элиса на укороченных ЕС представлен на рис. 1.

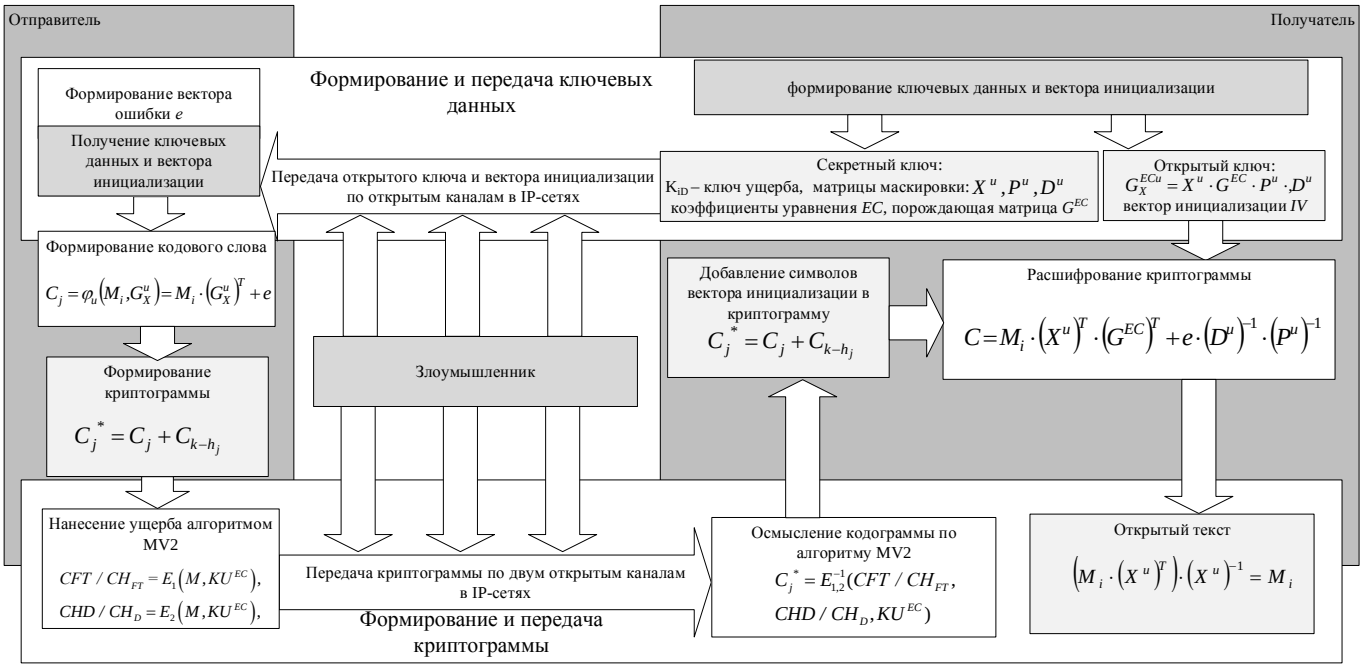

Рис. 1. Протокол обмена с использованием ГККККУК на основе МККС Мак-Элиса на укороченных МЕС

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, $|h| = x$, $x \le \frac{1}{2}\ 1/2k$ 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 5. 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: $k \ge \alpha - x + x_1$, $d \ge n - \alpha$, $\alpha = 3 \cdot degF$.

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 5, это символы множества h_1, которые полностью определяют модифицированный эллиптический *(n, k, d)*-код над *GF(q)*.

Утверждение 6. 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: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot degF$.

Следствие 2. Если известен вид эллиптической кривой (набор $a_1 \dots a_6$, $\forall a_i \in GF(q)$), 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 $a_1 \dots a_6$, $\forall a_i \in GF(q)$ однозначно задает вид эллиптической кривой и, соответственно, набор ее точек *EC(GF(q))*. По утверждению 6, 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)*. На рис. 2 представлен протокол обмена с использованием ГККККУК на основе МККС Мак-Элиса на удлиненных МЕС.

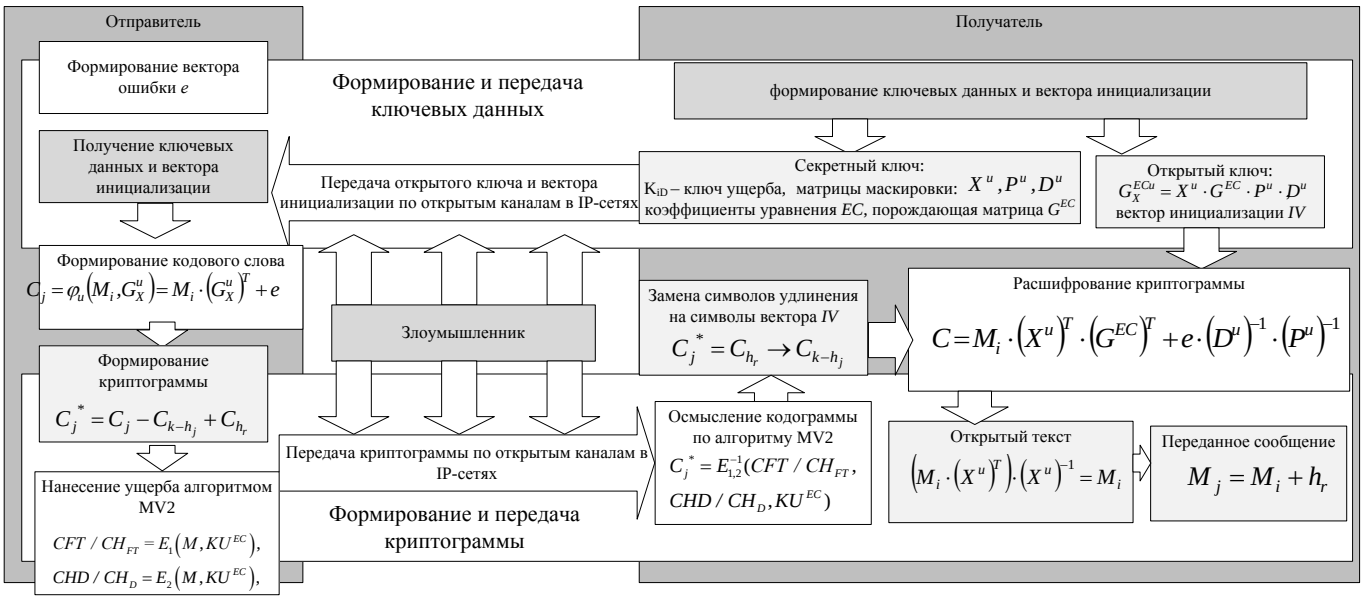

Рис. 2. Протокол обмена с использованием ГККККУК на основе МККС Мак-Элиса на удлиненных МЕС

Таким образом, синтез МНККС Мак-Элиса на МЕС позволяют строить ГККККУК с требуемым уровнем криптостойкости и уменьшенными показателями энергетической емкости, что существенно позволяет расширить спектр их применения для обеспечения услуг безопасности и достоверности информации. Проведем исследование свойств, предложенных КККУК, сравним с результатами НККС Мак-Элиса на ЕС, и МНККС Мак-Элиса на МЕС.

Исследование свойств НККС Мак-Элиса на ЕС и модифицированной НККС Мак-Элиса на МЕС. Проведем оценку параметров несимметричных теоретико-кодовых схем с использованием эллиптических кодов. Введем следующие обозначения:

l_I – длина информационной последовательности (блока), поступающей на вход теоретико-кодовой схемы (в битах); l_K – длина открытого ключа (в битах); l_{K+} – длина закрытого ключа (в битах); l_s – длина кодограммы (в битах); O_K – сложность формирования кодограммы (количество групповых операций); O_{SK} – сложность раскодирования кодограммы (количество групповых операций); O_{K+} – сложность решения задачи анализа (количество групповых операций); K_C – коэффициент сжатия остатка; K_f – коэффициент сжатия флага; s – количество отрезков ущербного текста; $u(n)$, $v(r)$ – положительные числа ключа ущерба; $z(m)$ – раунды ущерба; L_0 – длина исходного текста; L_{DT} – длина ущербного текста.

Для построения графиков были использованы условные сокращения (приставки): ukh/udh – гибридные КККУК с укороченными МЕС/гибридные КККУК с удлиненными МЕС; uk – МНККС с укороченными МЕС; ud – МНККС с удлиненными МЕС.

При расчетах параметров криптосистем были использованы поля Галуа: для ТКС Мак-Элиса – $GF(2^{10})$; для МНККС с укороченными/удлиненными МЕС – $GF(2^6)$; для гибридных КККУК – $GF(2^4)$.

Проведем сравнительный анализ параметров несимметричной теоретико-кодовой схемы (НТКС) Мак-Эллиса с использованием ЭК, с параметрами модифицированных МНККС Мак-Элиса на МЕС.

Для оценивания *длины информационной последовательности (в битах)*, поступающей на вход МНККС с алгебраическим (n, k, d)-кодом над $GF(2^m)$ используем выражения: – для НТКС на ЕС: $l_I = k \cdot m$; для МНККС на укороченных кодах МЕС: $l_I = 1/2k \cdot m$; для МНККС на удлиненных кодах МЕС: $l_I = k \cdot m$.

В табл. 1 и на рис. 3 представлены зависимости сложности формирования кодограммы от мощности поля.

Таблица 1

Зависимость сложности формирования криптограммы в различных $GF(2^m)$

$GF(2^m)$	R					
	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
3	31	87	242	603	817	968
4	76	340	760	980	2140	6282
5	335	872	2241	6121	8706	11461
6	582	2170	**6348**	**9830**	**10722**	**60760**
7	1023	6172	17092	61751	83000	210170
8	5237	10673	67016	105265	207422	605005
9	10563	50487	98765	510780	710920	1018079
10	**52704**	**103822**	497309	908243	4572881	5561379

Из приведенных данных видно, что сложность формирования криптограммы для выбранной мощности поля Галуа 2^6 на укороченных и удлиненных кодах значительно ниже (в 5 раз и более), чем в оригинальной реализации НТКС на ЕС. Соответственно, скорость формирования криптограммы существенно возрастет.

Для оценивания *Длина кодограммы* (в битах) используем выражения: для НТКС на ЕС: $l_s = n \cdot m$; для МНККС на укороченных МЕС: $l_S = \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m$; для МНККС на удлиненных МЕС: $l_S = (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times m$. В табл. 2 и на рис. 4 представлены зависимости сложности раскодирования кодограммы от мощности поля.

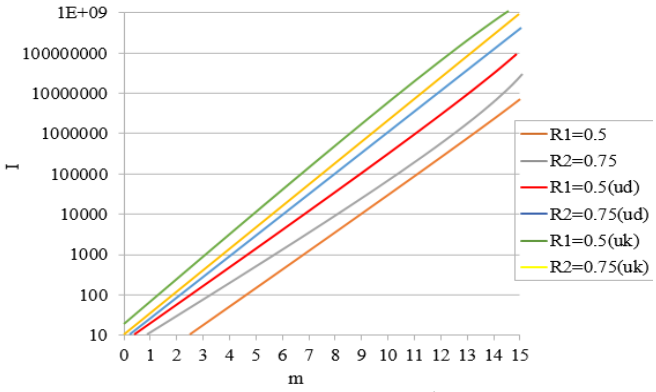

Рис. 3. Зависимость сложности формирования криптограммы в различных $GF(2^m)$

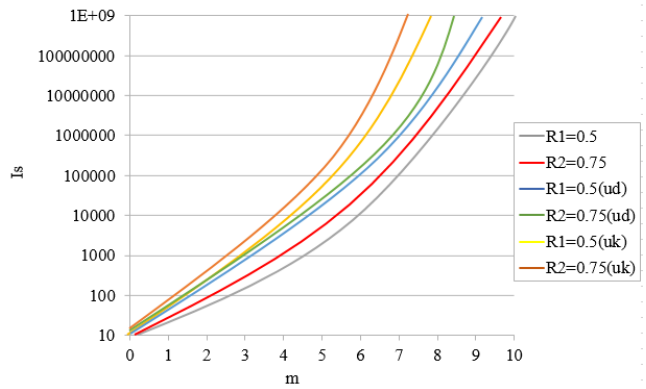

Рис. 4. Зависимость сложности раскодирования криптограммы в различных $GF(2^m)$

Анализ результатов расчетов также, как в случае формирования криптограммы, показывает существенный прирост скорости раскодирования при использовании укороченный и удлиненных МЕС.

Длина открытого ключа (в битах) определяется суммой элементов матрицы G_X^{EC} и задается выражениями: для НТКС на ЕС: $l_K = k \cdot n \cdot m$; – для МНККС на укороченных МЕС: $l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m$; для МНККС на удлиненных МЕС:

$$l_K = 1/2\,k \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m\,.$$

Длина закрытого ключа (в битах) определяется суммой элементов матриц X, P, D (в битах) и задается выражениями: для НТКС на ЕС: $l_{K+} = n^2 \cdot k^2 \cdot m$; для МНККС на укороченных МЕС: $l_{K_+} = 1/2\,k \left\lceil \log_2\left(2\sqrt{q} + q + 1\right) \right\rceil$, для МНККС на удлиненных МЕС:

$$l_{K_+} = \left(1/2\,k - 1/2\,k\right) \left\lceil \log_2\left(2\sqrt{q} + q + 1\right) \right\rceil .$$

В табл. 3 и на рис. 5 представлены зависимости сложности взлома на основе перестановочного декодирования от мощности поля.

Таблица 2

Зависимость сложности раскодирования криптограммы в различных *GF(2ᵐ)*

GF(2ᵐ)	*R*					
	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
1	43	57	78	81	82	96
2	67	98	456	457	457	556
3	120	640	1024	1168	1280	5127
4	680	2378	7672	8232	11028	23674
5	2092	7512	21073	42082	78634	277830
6	12397	61246	**103862**	**281472**	**760553**	**5220573**
7	127523	136495	642648	752018	4566721	19768512
8	1203984	1494284	3564898	3957812	12948312	52694229
9	10637991	12768954	54678128	67458242	92516734	102564872
10	**175645127**	**193648924**	1e+09	1e+09	1e+09	1e+09

Таблица 3

Зависимость сложности взлома в различных GF(2m)

GF(2ᵐ)	*R*					
	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
1	1.056	1.38	2.786	2.835	4.122	4.257
2	2.237	3.017	4.978	5.961	6.233	6.781
3	2.868	4.867	7.568	8.120	8.234	9.764
4	4.843	6.613	9.87	12.1	12.647	13.32
5	6.22	8.03	12.017	14.224	14.742	16.892
6	7.891	12.245	**14.983**	**17.483**	**18.767**	**19.76**
7	8.995	13.13	17.14	20.32	21.102	22.93
8	10.37	15.16	19.55	23.23	24.05	26.11
9	11.74	17.18	21.96	26.15	27.002	29.302
10	13.19	19.23	24.37	29.06	29.95	32.484

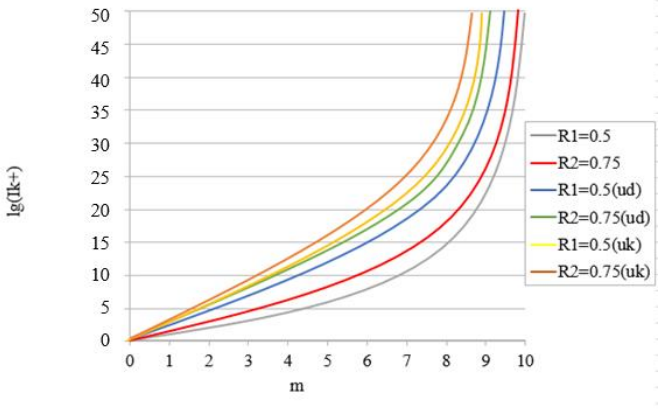

Рис. 5. Зависимость сложности взлома в различных *GF(2ᵐ)* (перестановочное декодирование)

Анализ рис. 5 показал, что уменьшение мощности поля до 2^6 не привело к существенному снижению сложности взлома криптограмм перестановочным декодированием. Совершенно очевидно, что такие результаты достигаются за счет применения универсального сжатия данных по алгоритму MV2.

Сложность формирования кодограммы оценивается выражениями:

– для НТКС на ЕС: при реализации систематического кодирования: $O_K = (r+1) \cdot n$; для несистематического кодирования: $O_K = (k+1) \cdot n$.

Для МНККС на укороченных МЕС: при реализации систематического кодирования: $O_K = (r+1)\times(2\sqrt{q}+q+1-1/2k)$, для несистематического кодирования: $O_K = (k+1)\times(2\sqrt{q}+q+1-1/2k)$. Для *МНККС* на удлиненных МЕС: при реализации систематического кодирования: $O_K = (r+1)\times(2\sqrt{q}+q+1-1/2k+1/2k)$, для несистематического кодирования: $O_K = (k+1)\times(2\sqrt{q}+q+1-1/2k+1/2k)$.

Сложность раскодирования кодограммы определяется выражениями: для НТКС на ЕС: $O_{SK} = 2\cdot n^2+k^2+4t^2+(t^2+t-2)^2/4$; для МНККС на укороченных МЕС:

$$O_{SK} = 2\left(2\sqrt{q}+q+1-1/2k\right)^2 + 1/2k^2+4t^2+\left(t^2+t-2\right)^2/4;$$

– для МНККС на удлиненных МЕС:

$$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)+ k^2+4t^2+\left(t^2+t-2\right)^2/4.$$

Сложность решения задачи анализа (декодирования) задаются выражениями: для НТКС на ЭК:

$O_{K+} = N_{покр} \cdot n \cdot r$, где $N_{покр} \geq \frac{C_n^{\rho \cdot t}}{C_{n-k}^{\rho \cdot t}} = \frac{n(n-1)...(n-\rho \cdot t-1)}{(n-k)(n-k-1)...(n-k-\rho \cdot t-1)}$, $t = \lfloor (d-1)/2 \rfloor$.

Потенциальная стойкость криптосистемы определяется величиной $\rho \times t$, а помехоустойчивость системы – $(1-\rho) \times t$. Для МНККС на укороченных кодах: $O_{K+} = N_{покр} \times (2\sqrt{q} + q + 1 - 1/2\,k) \times r$;

– для МНККС на удлиненных кодах: $O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - 1/2\,k + 1/2\,k\right) \times r$.

В табл. 4 и на рис. 6 представлена зависимости сложности взлома и сложности кодирования для различных скоростей ЕС (МЕС).

Таблица 4

Сводная диаграмма сложности взлома и сложности кодирования для различных скоростей ЕС

lg(ls)	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
1	4.75	12.1	15.6	18.23	19.12	19.82
2	10.52	21.76	32.47	35.67	38.63	39.18
3	18.22	33.17	43.75	51.61	56.88	58.03
4	21.42	51.75	59.43	72.81	78.92	80.52
5	38.77	61.09	68.26	87.32	94.91	104.56
6	54.13	78.37	**101.72**	**112.46**	**120.83**	**128.79**
7	82.14	83.72	156.75	164.72	182.39	189.74
8	165.84	179.13	223.64	231.57	276.27	287.33
9	358.33	371.09	421.97	428.63	459.81	476.52
10	**672.37**	**684.94**	716.41	722.26	783.46	794.28

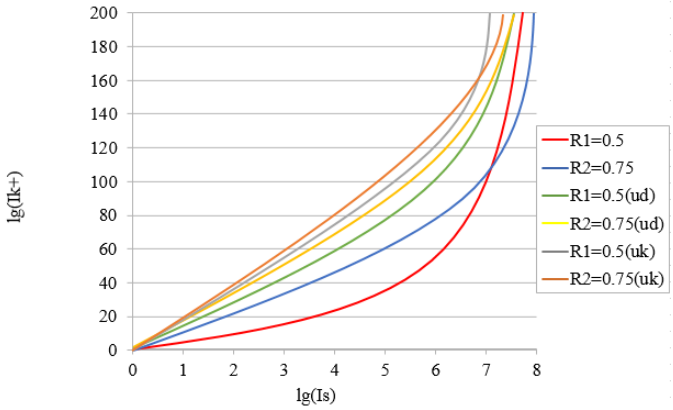

Рис. 6. Сводная диаграмма сложности взлома и сложности кодирования для различных скоростей ЕС (МЕС)

В табл. 5 и на рис. 7 представлены зависимости объема открытых ключевых данных для различных показателей стойкости.

Анализ представленных результатов табл. 4, 5, рис. 6, 7 ясно демонстрирует за счет чего получено возрастание относительной скорости передачи данных: объем ключевых данных в системах на укороченных/удлиненных кодах вдвое меньший обычной НККС.

В табл. 6 представлены результаты исследований емкостной характеристики при программной реализации от мощности поля.

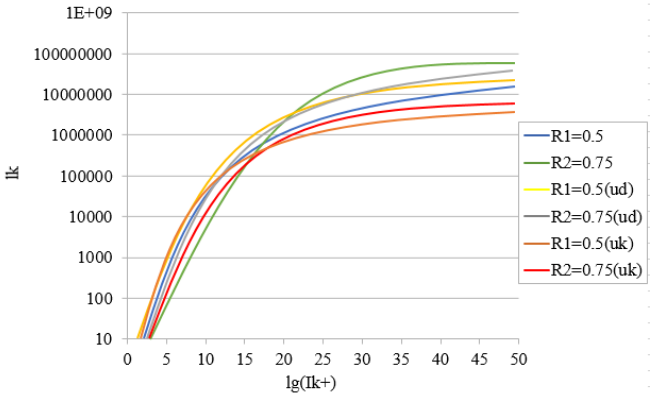

Рис. 7. Зависимости объема открытых ключевых данных для различных показателей стойкости

Таблица 5

Зависимости объема открытых ключевых данных для различных показателей стойкости

lg(lk+)	R					
	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
5	30	87	240	602	968	799
20	2278137	4351076	926137	987234	1034682	1897092
35	**12329538**	**14097276**	**4253109**	**5237688**	**6126273**	**6832018**
50	22541273	77520337	43076332	60122407	8602376	7027160

Таблица 6

Зависимость скорости программной реализации от мощности поля (количество групповых операций)

Криптосистемы	2^5	2^6	2^7	2^8	2^9	2^{10}
НККС MacElis на ЕС	10018042	18048068	32847145	47489784	63215578	**82467897**
МНККС MacElis на укороченных МЕС	10007947	**17787431**	28595014	44079433	61974253	79554764
МНККС MacElis на удлиненных МЕС	11156138	**18561228**	33210708	48297112	65171690	84051337

Результирующая таблица 6 показывает количество групповых операций программной реализации НККС в зависимости от мощности поля. Видно, что если для реализации НККС Мак-Элиса в поле 2^{10} необходимо $82{,}5*10^6$ групповых операций, то реализация МНККС на укороченных/удлиненных МЕС в поле 2^6 требует $17{,}7 – 18{,}6\times10^6$ групповых операций, т. е. в 4,5 раза меньше.

В работах [8, 9] 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 [9]. Как следствие, ущербный текст имеет длину меньшую длины исходного текста, и не имеет смысла исходного текста [9].

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.

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.

Криптографическими ущербными текстами называются тексты, полученные следующими способами [9]: 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.

Проведем **сравнительный анализ параметров МНККС Мак-Эллиса на МЕС (укороченных/удлиненных) и с параметрами ГККККУК на основе НМНККС Мак-Элиса на МЕС.** *Длина информационной последовательности* (в битах), поступающей на вход криптосистемы с УК определяется следующим выражением: для ГККККУК на укороченных кодах: $l_I = l_z^c + l_z^f$, где $l_z^c = K_c \times L + \frac{1}{K_f} \times s$ – длина ущербного текста; $l_z^f = L + u \times s$ – длина ущерба; $s = \left[\frac{L_0 - L_{DT}}{L_{DT}} \right]$ – количество отрезков ущербного текста, $K_C = 1 - K_f \approx 0{,}758$ – коэффициент сжатия остатка (ущербного текста) (при u = 8, v = 3, z = 5); $K_f = \frac{2 - 2^{v-u+1}}{u} \approx 0{,}242$ – коэффициент сжатия флага (ущерба) (при u = 8, v = 3, z = 5); $z = \frac{log\left(u \times L\right) - 7}{log\left(1/K_C\right)}$ – необходимое для рандомизации шифра MV2, количество допустимых раундов преобразования. *Для* ГККККУК на удлиненных *МЕС*: $l_I = 1/\ 2k \times m + l_z^c + l_z^f$.

В табл. 7 и на рис. 8 приведены результаты исследований сложности формирования криптограммы в различных *GF(2ᵐ)*.

Таблица 7

Зависимость сложности формирования криптограммы в различных $GF(2^m)$

$GF(2^m)$	R							
	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
3	242	603	817	968	643	780	923	998
4	760	980	2140	6282	**905**	**1085**	**1563**	**5125**
5	2241	6121	8706	11461	1863	2450	6137	8282
6	**6348**	**9830**	**10722**	**60760**	6273	7016	9183	10341
7	17092	61751	83000	210170	16582	15985	16563	16925
8	67016	105265	207422	605005	65278	65450	66137	68282
9	98765	510780	710920	1018079	95327	96037	97134	97841

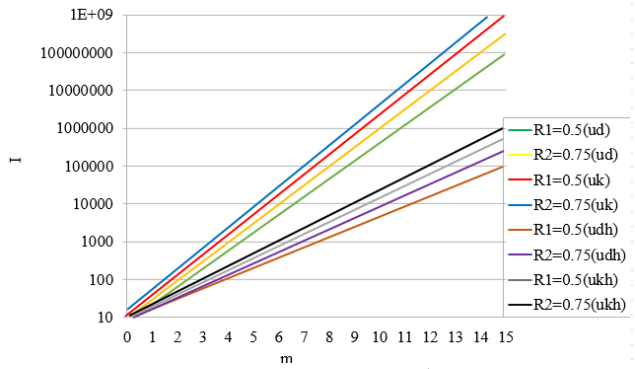

Рис. 8. Зависимость сложности формирования криптограммы в различных $GF(2^m)$

Длина кодограммы (в битах) определяется выражениями:

– для ГККККУК на укороченных МЕС:

$$l_S = (2\sqrt{q} + q + 1 - 1/2k) \times m;$$

– для ГККККУК на удлиненных МЕС:

$$l_S = (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times m.$$

В табл. 8 и на рис. 9 приведены результаты исследований сложности раскодирования криптограммы в различных $GF(2^m)$.

Таблица 8

Зависимость сложности раскодирования криптограммы в различных $GF(2^m)$

$GF(2^m)$	R							
	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
1	78	81	82	96	148	153	1568	1621
2	456	457	457	556	835	897	6112	9624
3	1024	1168	1280	5127	1240	1307	12283	14817
4	7672	8232	11028	23674	**5224**	**11937**	**34673**	**225017**
5	21073	42082	78634	277830	12348	25597	95088	1246572
6	**103862**	**281472**	**760553**	**5220573**	123548	127137	1316373	4383507

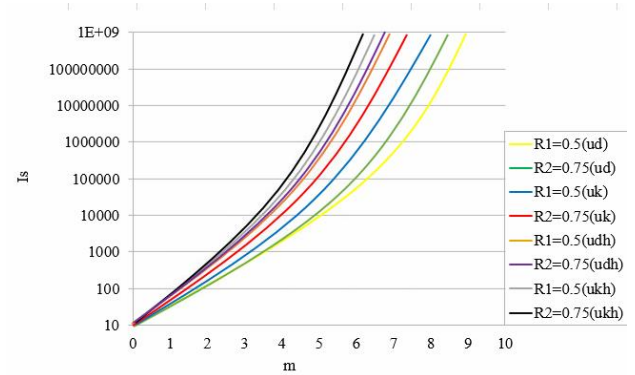

Рис. 9. Зависимость сложности раскодирования криптограммы в различных $GF(2^m)$

Анализ табл. 7, 8, рис. 8, 9 показал, что использование ущербных кодов и дальнейшее уменьшение мощности поля Галуа приводит к значительному уменьшению сложности формирования (примерно в 12 раз) и раскодирования (примерно в 20 раз) криптограммы.

Длина открытого ключа (в битах) определяется суммой элементов матрицы G_X^{EC} и задается выражениями: для ГККККУК на укороченных МЕС: $l_K = 1/2\,k \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m$; для ГККККУК на удлиненных МЕС: $l_K = 1/2\,k \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times m$.

Длина закрытого ключа (в битах) определяется суммой элементов матриц X, P, D (в битах) и задается выражениями: для ГККККУК на укороченных кодах: $l_{K_+} = 1/2\,k[\log_2 (2\sqrt{q} + q + 1)] + \left|F_u^v\right|$, где $\left|F_u^v\right| = 2^u!$ – мощность множества подстановочных преобразований; для ГККККУК на удлиненных кодах: $l_{K_+} = (1/2\,k - 1/2\,k)[\log_2 (2\sqrt{q} + q + 1)] + \left|F_u^v\right|$.

В табл. 9 и на рис. 10 приведены результаты исследований сложности взлома алгоритмом перестановочного декодирования в различных $GF(2^m)$.

Таблица 9

Зависимость сложности взлома ГККККУК над $GF(2^m)$

$GF(2^m)$	R							
	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
1	2.786	2.835	4.122	4.257	1.089	1.864	2.391	3.46
2	4.978	5.961	6.233	6.781	2.569	3.643	4.108	4.962
3	7.568	8.120	8.234	9.764	3.57	4.131	5.382	7.623
4	9.87	12.1	12.647	13.32	**4.92**	**5.817**	**6.836**	**8.972**
5	12.017	14.224	14.742	16.892	7.591	8.617	10.13	12.005
6	**14.983**	**17.483**	**18.767**	**19.76**	10.85	12.53	14.673	14.962

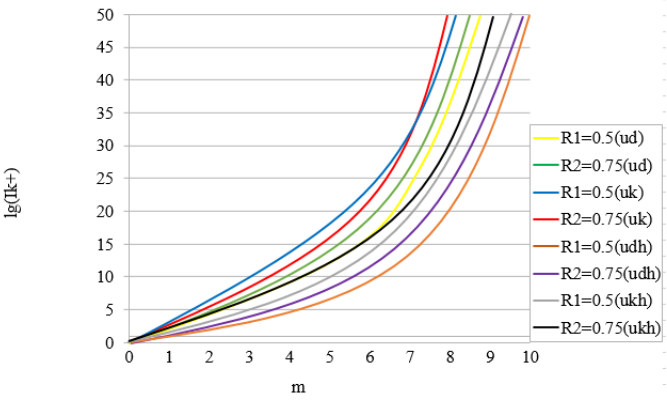

Рис. 10. Зависимость сложности взлома ГККККУК над $GF(2^m)$ (перестановочное декодирование)

Очевидным результатом снижения мощности поля является, как это демонстрируют таблица 9 и график на рис. 10, дальнейшее уменьшение сложности взлома, которая, как это показано дальнейшими статистическими тестами, вполне компенсируется универсальным алгоритмом сжатия MV2.

Сложность формирования кодограммы *определяется выражениями*: для ГККККУК на укороченных *МЕС*:

– при реализации систематического кодирования определяется выражением:

$$O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2\,k\right)+O\left(\frac{1-K_C^u}{K_f}\times L\right),$$

– для несистематического кодирования:

$$O_K = O_K = (k+1)\times(k+1)\times$$
$$\left(2\sqrt{q}+q+1-1/2\,k\right)+O\left(\frac{1-K_C^u}{K_f}\times L\right)$$

Для ГККККУК на удлиненных МЕС:

– при реализации систематического кодирования определяется выражением:

$$O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2\,k+1/2\,k\right)$$
$$+O\left(\frac{1-K_C^u}{K_f}\times L\right),$$

– для несистематического кодирования:

$$O_K = (k+1)\times\left(2\sqrt{q}+q+1-1/2\,k+1/2\,k\right)$$
$$+O\left(\frac{1-K_C^u}{K_f}\times L\right).$$

Сложность раскодирования кодограммы определяется выражениями:

– для ГККККУК на укороченных МЕС:

$$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2\,k\right)^2+1/2k^2+$$
$$4t^2+\left(t^2+t-2\right)^2/4+O\left(\frac{\alpha-z\times\log k}{\left|K_z^c\times L\right|}\right);$$

– для ГККККУК на удлиненных МЕС:

$$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2\,k+1/2\,k\right)^2+k^2+4t^2+$$
$$\left(t^2+t-2\right)^2/4+O\left(\frac{\alpha-z\times\log k}{\left|K_z^c\times L\right|}\right).$$

Сложность решения задачи анализа (декодирования) определим выражениями:

– для ГККККУК на укороченных МЕС:

$$O_{K+} = N_{покр}\times\left(2\sqrt{q}+q+1-1/2\,k\right)\times r+N_{F\ или}\left(N_K\right),$$

где $N_F \approx \frac{K_C^{\,z}}{2^{1-K_C^{\,z+1}}}\times|F|$, K_C=97/128, $|F|$ – суммарная длина выходных флагов (ущербов) (бит) – при известном злоумышленнику остатке (ущербном тексте) и заданных флагах (ущербах), при неизвестном ключе – $N_K \approx 2^{1190\times z}$, $z = 16$;

– для ГККККУК на удлиненных МЕС:

$$O_{K+} = N_{покр}\times\left(2\sqrt{q}+q+1-1/2\,k+1/2\,k\right)\times$$
$$r+N_{F\ или}\left(N_K\right).$$

В табл. 10 и на рис. 11 приведены результаты исследований сложности взлома и сложности кодирования для различных скоростей R в различных $GF(2^m)$. В табл. 11 приведены результаты исследований зависимости объема открытых ключевых данных ГККККУК на МЕС для различных показателей стойкости.

В табл. 12 представлены результаты исследований емкостной характеристики при программной реализации от мощности поля.

Таблица 10

Сложность взлома и сложности кодирования для различных скоростей R

$\lg(l_s)$	R							
	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
1	15.6	18.23	19.12	19.82	7.21	9.17	12.54	14.56
2	32.47	35.67	38.63	39.18	21.46	23.72	27.48	29.82
3	43.75	51.61	56.88	58.03	31.68	33.83	37.38	38.43
4	59.43	72.81	78.92	80.52	**41.72**	**42.27**	**47.48**	**58.23**
5	68.26	87.32	94.91	104.56	56.63	58.91	62.86	66.53
6	**101.72**	**112.46**	**120.83**	**128.79**	72.32	74.79	89.5	97.71

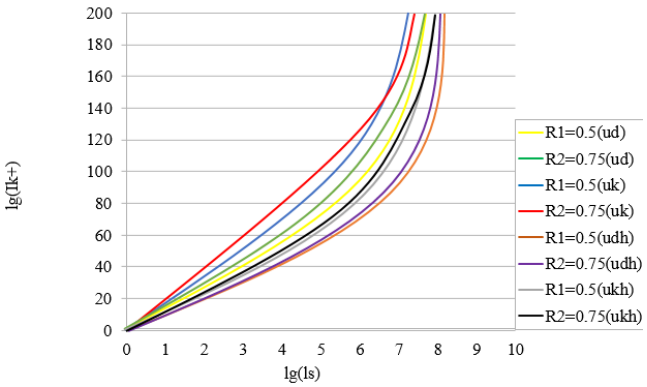

Рис. 11. Сводная диаграмма сложности взлома и сложности кодирования ГККККУК для различных скоростей МЕС

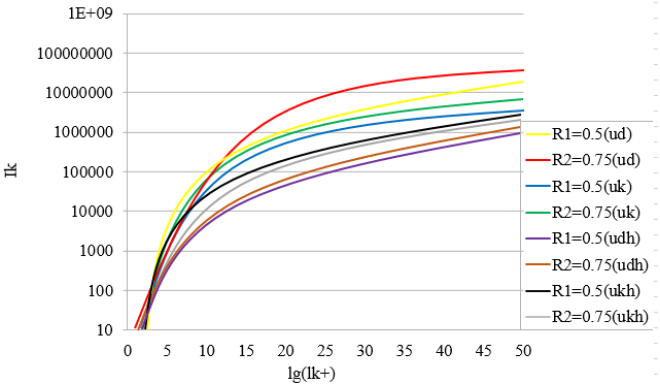

Рис. 12. Зависимости объема открытых ключевых данных ГККККУК для различных показателей стойкости

Таблица 11

Зависимости объема открытых ключевых данных ГККККУК для различных показателей стойкости

$\lg(l_{k+})$	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
5	240	602	968	799	812	827	853	898
20	926137	987234	1034682	1897092	87531	95019	312560	402843
35	**4253109**	**5237688**	**6126273**	**6832018**	**421108**	**650389**	**957648**	**1121732**
50	43076332	60122407	8602376	7027160	1032562	2340561	3867228	4218394

Таблица 12

Зависимость скорости программной реализации от мощности поля (количество групповых операций)

	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
MacElis на укороченных МЕС	8293075	10007947	**17787431**	28595014	44079433	61974253	79554764
MacElis на удлиненных МЕС	8506422	11156138	**18561228**	33210708	48297112	65171690	84051337
ГККККУК на МНККС MacElis на удлиненных МЕС	**5612316**	7900315	14892945	25565274	42279183	58963778	76564173
ГККККУК на МНККС MacElis на укороченных МЕС	**5942627**	7905257	14682411	25595014	42116327	58468143	75474764

Как и при исследовании МНККС получили существенное уменьшение открытых ключевых данных для ГККККУК, что и приводит к суммарному увеличению относительной скорости передачи.

Естественным продолжением наших исследований, очевидно, должно быть тестирование статистических характеристик предложенных крипто-кодовых конструкций с целью получения объективных традиционных данных о крипто-стойкости.

Для проведения статистических исследований стойкости исследуемых криптосистем воспользуемся пакетом NIST STS 822 [11]. Результаты исследований представлены в табл. 13.

Таблица 13 продемонстрировала, что несмотря на уменьшение мощности поля Галуа до $GF(2^6)$ для МНККС и $GF(2^4)$ для ГККККУК, статистические характеристики таких крипто-кодовых конструкций оказались, как минимум, не хуже традиционных НККС Мак-Элиса на $GF(2^{10})$. Все криптосистемы прошли 100% тестов НИСТ, причем наилучший результат показала ГККККУК на укороченных МЕС: 155 из 189 тестов пройдено на уровне 0,99, что составляет 82% от всего количества тестов. При этом традиционная НККС Мак-Элиса на $GF(2^{10})$ показала 149 тестов на уровне 0,99.

Таблица 13

Результаты исследований статистической безопасности

Алгоритм	Количество тестов, в которых тестирование прошли более 99% последовательностей	Количество тестов, в которых тестирование прошли более 96% последовательностей	Количество тестов, в которых тестирование прошли менее 96% последовательностей
НККС MacElis	149 (78,83%)	189 (100%)	0 (0%)
МНККС MacElis на укороченных МЕС	151 (79,89%)	189 (100%)	0 (0%)
МНККС MacElis на удлиненных МЕС	152 (80,42%)	189 (100%)	0 (0%)
ГККККУК на МНККС MacElis на удлиненных МЕС	153 (80,95%)	189 (100%)	0 (0%)
ГККККУК на МНККС MacElis на укороченных МЕС	155 (82 %)	189 (100%)	0 (0%)

Выводы:

Выполненные исследования крипто-кодовых конструкций на основе НККС Мак-Элиса позволяют сделать следующие выводы:

1. Исследованы методы увеличения скорости крипто-кодовых конструкций на основе НКС Мак-Элиса, заключающиеся в уменьшении мощности поля Галуа до *GF* (2^6) – *GF* (2^4), увеличении/уменьшении длины МЕС и внесении ущерба.

2. Достигнуто существенное увеличение быстродействия систем (как минимум в 20 раз по скорости формирования криптограммы), что позволяет использовать обычную персональную вычислительную технику для криптографической защиты информации такими системами.

3. Внесение ущерба, использование универсального алгоритма сжатия MV2 позволяет достичь, как минимум, равных показателей криптостойкости при уменьшении мощности поля Галуа, сокращении объемов ключевой информации, о чем свидетельствуют статистические тесты в среде NIST STS 822. Наилучшие статистические характеристики продемонстрировали гибридные крипто-кодовые конструкции на ущербных кодах (на укороченных МЕС – *GF*(2^4)), превышающие характеристики НККС Мак-Элиса на *GF* (2^{10}) примерно на 4%.

ЛИТЕРАТУРА

[1]. ISO 9000:2015(en) Quality management systems – Fundamentals and vocabulary [Electronic resource]. Access: https://www.iso.org/obp/ui/ # iso: std: iso: 9000:ed-4:v1:en.

[2]. CISCO: Кибератаки на индустриальные системы усиливаются, а доверие к имеющимся системам защиты падает. [Электронный ресурс]. Режим доступа: https: // www. cisco. com / c / ru _ ru/ about/ press/press-releases/2016/01-21a.html.

[3]. Rise of IoT Botnets Showcases Cybercriminals' Ability to Find New Avenues of Attack. [Электронный ресурс]. Режим доступа: http: // storage. pardot. com / 44731/127332/Cybercrime_Trends_Report___2016 _Year_in_Review__1_.pdf.

[4]. Исследование HP: Средний годовой ущерб от кибератак вырос до 15 млн долл. на организацию. [Электронный ресурс]. Режим доступа: http: // www. connect-wit.ru/issledovanie-hp-crednij-godovoj-ushherb-ot-kiberatak-vyros-do-15-mln-doll-na-organizatsiyu.html.

[5]. Х. Рзаев, Г. Искендерзаде, Ф. Самедов, З. Иманова, Ж. Джамалова, "Математические модели крипто-кодовых средств защиты информации на основе ТКС", *Защита информации: сборник научных трудов НАУ,* вып. 23, С. 24-26, 2016.

[6]. B. Biswas and N. Sendrier, "McEliece Cryptosystem Implementation: Theory and Practice", *PQCrypto 2008, Springer-Verlag Berlin Heidelberg 2008,* LNCS 5299, pp. 47–62, 2008.

[7]. В. Дудыкевич, Б. Томашевский, С. Евсеев, "Аналіз методів захисту інформації доказової стійкості з використанням секретних систем на алгебраїчних блокових кодах", *Науково-технічний журнал «Інформаційна безпека».* №2 (2), с. 17-26, 2009.

[8]. Р. Блейхут, *Теория и практика кодов, контролирующих ошибки: пер. с англ.*, М.: Мир, 1986.

[9]. V. Mishhenko, Ju. Vilanskij, *Ushherbnye teksty i mnogokanal'naja kriptografija*, Jenciklopediks., 2007, 292 p.

[10]. V. Mishhenko, Ju. Vilanskij, V. Lepin, "Kriptograficheskij algoritm MV 2", 2006, 177 p.

[11]. A. Rukhin, J. Soto, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", *NIST Special Publication 800-22*, 09.2000.

REFERENCES

[1]. ISO 9000:2015(en) Quality management systems – Fundamentals and vocabulary [Electronic resource]. Access: https://www.iso.org/obp/ui/ # iso: std: iso: 9000:ed-4:v1:en.

[2]. CISCO: Kiberataki na industrial'nye sistemy usilivajutsja, a doverie k imejushhimsja sistemam zashhity padaet. [Electronic resource]. Access: https: // www. cisco. com / c / ru _ ru/ about/ press/press-releases/2016/01-21a.html.

[3]. Rise of IoT Botnets Showcases Cybercriminals' Ability to Find New Avenues of Attack. [Electronic resource]. Access: http:// storage. pardot. com/ 44731/ 127332/ Cybercrime_Trends_Report___2016_Year_in_Review__1_.pdf.

[4]. Issledovanie HP: Srednij godovoj ushherb ot kiberatak vyros do 15 mln doll. na organizaciju. [Electronic resource]. Access: http:// www. connect - wit. ru/ issledovanie-hp-crednij-godovoj-ushherb-ot-kiberatak-vyros-do-15-mln-doll-na-organizatsiyu. html.

[5]. H. Rzaev, G. Iskenderzade, F. Samedov, Z. Imanova, Zh. Dzhamalova, "Matematicheskie modeli kriptokodovyh sredstv zashhity informacii na osnove TKS", *Zashhita informacii: sbornik nauchnyh trudov NAU*, vol. 23, pp. 24-26, 2016.

[6]. B. Biswas, N. Sendrier, "McEliece Cryptosystem Implementation: Theory and Practice", *PQCrypto 2008, Springer-Verlag Berlin Heidelberg 2008, LNCS 5299*, pp. 47-62, 2008.

[7]. V. Dudykevich, B. Tomashevskij, S. Evseev, "Analiz metodiv zahistu informaciï dokazovoï stijkosti z vikoristannjam sekretnih sistem na algebraïchnih blokovih kodah", *Naukovo-tehnichnij zhurnal «Informacijna bezpeka»,* no. 2 (2). Lugans'k, pp. 17-26, 2009.

[8]. R. Blejhut, *Teorija i praktika kodov, kontrolirujushhih oshibki: per. s angl.*, M.: Mir, 1986.

[9]. V. Mishhenko, Ju. Vilanskij, *Ushherbnye teksty i mnogokanal'naja kriptografija*, Jenciklopediks., 2007, 292 p.

[10]. V. Mishhenko, Ju. Vilanskij, V. Lepin, *Kriptograficheskij algoritm MV 2*, 2006, 177 p.

[11]. A. Rukhin, J. Soto, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 09.2000.

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ГІБРИДНИХ КРИПТО-КОДОВИХ КОНСТРУКЦІЙ

Розглянуто способи побудови гібридних крипто-кодових конструкцій з збитковими кодами (ГККК3К) на основі синтезу модифікованих несиметричних крипто-кодових систем Мак-Еліса (МНККС) на еліптичних кодах (ЕС) з багатоканальними криптографічними системами на збиткових кодах, протоколи обміну для забезпечення конфіденційності в IP-мережі. Досліджуються основні критерії криптосистем, а також теоретичні основи зниження в 2 - 3 рази енергетичної ємності запропонованих МНККС Мак-Еліса з МЕС і гібридних конструкцій МНККС з збитковими кодами за рахунок зменшення потужності поля Галуа без зниження рівня криптостійкості гібридної криптосистеми в цілому при їх програмної реалізації. Отримано результати статистичних досліджень стійкості на основі пакету NIST STS 822.

Ключові слова: гібридні крипто-кодові конструкції, модифікована крипто-кодова система Мак-Еліса, ущербні коди, модифіковані еліптичні коди.

RESEARCH OF THE PROPERTIES OF HYBRID CRYPTO-CODE CONSTRUCTIONS

The methods for constructing hybrid crypto-code constructions with defective codes (GKKKUK) based on the synthesis of modified non-symmetric crypto-code systems McEliece (MNCCS) on elliptic codes (EC) with multichannel cryptographic systems on defective codes, exchange protocols for securing confidentiality in IP networks. The basic criteria of cryptosystems are investigated. Theoretical bases of decrease in 2 - 3 times power capacity of MNCCS McEliece with EC and hybrid designs of MNCCS with defective codes due to reduction of power of the Galois field. The required level of cryptographic strength of the hybrid cryptosystem as a whole is provided for their software implementation. The results of statistical stability studies based on the NIST STS 822 package are obtained.

Keywords: hybrid crypto-code designs, modified McAllis crypto-code system, maladaptive codes, modified elliptic codes.

Евсеев Сергей Петрович, кандидат технических наук, старший научный сотрудник, доцент кафедры информационных систем Харьковского национального экономического университета имени Семена Кузнеца.
E-mail: Serhii.Yevseiev@hneu.net

Євсеєв Сергій Петрович, кандидат технічних наук, старший науковий співробітник, доцент кафедри інформаційних систем Харківського національного економічного університету імені Семена Кузнеця.

Yevseiev Sergiy, PhD, Senior Researcher, Associate Professor of the Information Systems Department of the Kharkov National Economic University named after Semen Kuznets.

Остапов Сергей Эдуардович, доктор физико-математических наук, профессор, заведующий кафедрой программного обеспечения компьютерных систем, Черновицкий национальный университет им. Юрия Федьковича.
E-mail: sergey.ostapov@gmail.com

Остапов Сергій Едуардович, доктор фізико-математичних наук, професор, завідувач кафедрою програмного забезпечення комп'ютерних систем, Чернівецький національний університет імені Юрія Федьковича.

Ostapov Segiy, Doctor of Sciences (Physics and Mathematics), Professor, Head of the Computer Systems Software Department of the Chernivtsi National University named after Yuri Fedkovich.

Белодед Иван Викторович, магистр, студент Харьковского национального экономического университета имени Семена Кузнеца.
E-mail: bilodid.vanya@gmail.com

Білодід Іван Вікторович, магістр, студент Харківського національного економічного університету імені Семена Кузнеця.

Bilodid Ivan, student of the Kharkiv National University of Economics named after Semen Kuznets.