Раздел IV. Методы и средства криптографии и стеганографии

УДК 004.056.5

Ю.В. Косолапов, Е.С. Чекунов

СИММЕТРИЧНЫЕ КОДОВЫЕ КРИПТОСИСТЕМЫ НА ОСНОВЕ КОДОВ В Φ -МЕТРИКАХ

В работе с целью повышения стойкости симметричных кодовых криптосистем рассматриваются помехоустойчивые коды в Φ-метриках и строятся кодовые криптосистемы на кодах в ранговой Φ-метрике и Φ-метрике Вандермонда. Для криптосистемы в ранговой метрике получена оценка стойкости криатосистемы путем вычисления мощности множества искуственных ошибок, добавляемых при шифровании; для криптосистемы в метрике Вандермонда адаптирован алгоритм декодирования.

Симметричные кодовые криптосистемы; Φ-метрика.

Y.V. Kosolapov, E.S. Chekunov

SYMMETRIC CRYPTOSYSTEMS BASED ON ERROR CORRECTION CODES IN Φ-METRICS

In this paper the error correction codes in Φ-metric are considered for strengthing symmetric cryptosystems. Two cryptosystems on rank Φ-metric and Vandermonde Φ-metric are designed. The strength of the cryptosysem on rank codes is estimated and decoder for Vandermonde metric is adapted for corresponding symmetric cryptosystem.

Ssymmetric cryptosysmets based on error correction codes; Φ-metric.

Введение. В последние годы активно ведутся исследования в области построения методов защиты информации с использованием теории помехоустойчивого кодирования [1, 2]. Помехоустойчивые коды потенциально позволяют строить комплексные системы защиты, решающие одновременно как задачу защиты от помех, так и задачу защиты от несанкционированного воздействия. Эта особенность помехоустойчивых кодов может найти свое применение, например, в задаче защиты информации в каналах цифровой связи от технической утечки – несанкционированного чтения передаваемых данных. Помехоустойчивые коды уже успешно применяются в методах кодового зашумления для защиты от *частичной* утечки информации [3]. При этом в методах кодового зашумления возможна реализация одновременной защиты от помех и несанкционированного прослушивания [4]. Для защиты от *полной* утечки необходимо применение криптографических методов защиты. С точки зрения применения помехоустойчивых кодов, интерес представляют симметричные криптосистемы, так как могут быть построены на основе существующих в средствах связи помехоустойчивых кодеках [5, 4]. Отметим, что асимметричные кодовые криптосистемы не могут быть построены на основе существующих кодеков, так как в этом случае часть секретного ключа – кодек – является общеизвестной, что существенно снижает

стойкость криптосистем. Одной из наиболее стойких симметричных кодовых криптосистем является криптосистема Стройка–Тилбурга [6]. Однако она обладает принципиальными ограничениями – необходимо иметь достаточно большой объем памяти для хранения секретного ключа, а также нет возможности одновременно бороться с ошибками в канале. Первое ограничение связно с тем, что необходимо хранить предопределенную таблицу векторов ошибок большого веса и соответствующих синдромов (порядка $(2n-k)|F|^{n-k}$ элементов поля F), а второе ограничение связано с введением нелинейной функции в процедуру шифрования. Поэтому актуальной является задача построения таких симметричных кодовых криптосистем, у которых отсутствуют перечисленные выше ограничения.

Целью настоящей работы является построение симметричных кодовых криптосистем, позволяющих при стандартных параметрах помехоустойчивых кодеков противодействовать атаке методом статистического криптоанализа. Для этого ставится задача изучения помехоустойчивых кодов в специальной метрике – Φ-метрике – и построение кодовых криптосистем на соответсвующих кодах. В частности, в работе строятся две симметричные кодовые криптосистемы на основе кодов в ранговой Φ-метрике и Φ-метрике Вандермонда. Для криптосистемы в ранговой метрике получена оценка стойкости при стандартных параметрах кодеков, а для криптосистемы в Φ-метрике Вандермонда адаптирован декодер из [2].

Криптосистема Стройка–Тилбурга. Опишем оригинальную криптосистему Стройка-Тилбурга. Пусть $G_{k\times n}$ – порождающая матрица (n,k)-кода C над полем F и кодовым расстоянием Хэмминга $d=n-k+1$; D_C – быстрый алгоритм декодирования кода C, исправляющий до $t=\lfloor (d-1)/2 \rfloor$ ошибок; $F^n/C=\{\Xi_1;\Xi_2;..;\Xi_{2^{n-k}}\}$ – разбиение пространства F^n на классы эквивалентности по коду C; $S_{k\times k}$ – случайная невырожденная матрица; $P_{n\times n}$ – случайная перестановочная матрица; $H_{(n-k)\times n}$ – такая, что

$$S_{k\times k}\cdot G_{k\times n}\cdot P_{n\times n}\cdot H^{T}_{(n-k)\times n}=O_{k\times(n-k)},$$

где $O_{k\times(n-k)}$ – нулевая матрица; Z – подмножество F^n такое, что

$$\forall \bar{z}_i,\bar{z}_j\in Z,\bar{z}_i\neq\bar{z}_j:\bar{z}_i\in\Xi_r,\bar{z}_j\in\Xi_s\,|\,\Xi_r\neq\Xi_s;$$

$T=(\bar{z}\cdot H^{T}_{(n-k)\times n},\bar{z})\,|\,\bar{z}\in Z$ – синдромная таблица. Пусть f – нелинейная функция с областью определения $F^k\oplus F^n$ и областью значений F^k и пусть $f_{\bar{я}}=f(-,\bar{z})$. Будем предполагать, что: $\forall\bar{z}\in F^n\ \ \exists g_{\bar{z}}:F^k\to F^k\,|\ f(g_{\bar{z}}(\bar{y}),\bar{z})=\bar{y}$. Тогда $g_{\bar{z}}=f^{-1}_{\bar{z}}$. Пусть $K=(S_{k\times k},G_{k\times n},P_{n\times n},T,f_{\bar{z}}(\bar{x}))$ – секретный ключ криптосистемы. Сообщение $\bar{m}(\in F^n)$ зашифровывается по правилу:

$$\bar{c}=f_{\bar{z}}(\bar{m})\cdot S_{k\times k}\cdot G_{k\times n}\cdot P_{n\times n}+\bar{z},$$

где $\bar{z}$ выбирается случайно из Z. Для расшифрования принятого сообщения $\bar{c}$ по синдрому $\bar{c}\cdot H^{T}_{(n-k)\times n}$ из T находится $\bar{z}$, выполняется процедура декодирования $\bar{\alpha}=D_C((\bar{c}-\bar{z})\cdot P^{-1}_{n\times n})$ и вычисляется $\bar{m}=f^{-1}_{\bar{z}}(\bar{\alpha}\cdot S^{-1}_{k\times k})$.

Введение синдромной таблицы T и нелинейной функции $f_{\bar{z}}(\bar{x})$ [6] существенно осложняет криптоанализ этой криптосистемы при длине кода более 250 бит. Оригинальная схема Стройка–Тилбурга не использует корректирующей способности линейного кода и может применяться для борьбы с

несанкционированным съемом информации, в частности с полной технической утечкой, только в помехозащищенных каналах связи. В [5] построена схема реализации кодовой криптосистемы Стройка–Тилбурга на ранговых кодах и кодах Гоппы. В настоящей работе повышается стойкость криптосистем за счет перехода от хэмминговой метрики к Φ-метрике.

Φ-метрика. Φ-метрики – это метрики, основанные на проективных множествах. При определении Φ-метрики будем следовать работе [2]. Рассмотрим n-мерное векторное пространство F_q^n над полем Галуа F_q, $q = p^r$, r – простое. Пусть $\Phi = \{F_1, F_2, \ldots, F_N\}$ – любой набор подмножеств $F_i \subset F_q^n$ таких, что линейная оболочка $\Lambda\left(\bigcup_{i=1}^{N} F_i\right) = \Phi_q^n$. Под Φ-нормой (Φ-весом) w_Φ любого вектора $x \in F_q^n$ будем понимать мощность наименьшего набора подмножеств $\{F_i, i \in I\}$ из семейства Φ такого, что $x \in \Lambda\left(\bigcup_{i \in I} F_i\right)$. Φ-норма является метрикой в пространстве Φ_q^n. Φ-расстоянием между точками x и y назовем норму их разности $d_\Phi(x, y) = w_\Phi(x - y)$. Φ-метрика является обобщением метрики Хэмминга и ранговой метрики [2].

Рассмотрим произвольный код $C \subseteq \Phi_q^n$. Под Φ-расстоянием кода C будем понимать минимальное из Φ-расстояний различных ненулевых кодовых слов, т.е. $d_\Phi(C) = \min\{d_\Phi(x, y) \mid x, y \in C, x \neq y\}$. В качестве элементов F_i семейства Φ могут выступать векторы. В таком случае Φ-метрика называется проективной Φ-метрикой и ее элементы обозначаются через f_i, $\Phi = \{f_1, f_2, \ldots, f_N\}$. Для любого линейного (n, k)-кода C в проективной Φ-метрике выполняется граница Синглтона, т.е. $d_\Phi(C) \le n - k + 1$ [2]. Код, достигающий этой границы, будем называть кодом с максимальным Φ-расстоянием. Отметим, что в общем случае алгоритм быстрого декодирования линейных кодов в произвольной Φ-метрике неизвестен. Как правило, декодеры строятся для конкретных Φ-метрик. Так, в [2] построен код с максимальным Φ-расстоянием для специальной Φ-метрики, ассоциированной с матрицей Вандермонда.

Благодаря своим характеристикам, Φ-метрика нашла свое применение в кодовых криптосистемах. Так, в [2] предложена модификация асимметричной криптосистемы Нидеррайтера на основе кодов в Φ-метрике Вандермонда. Использование Φ-метрики позволяет усилить стойкость криптосистемы к атаке на ключ. В настоящей работе предлагается использование Φ-метрики для усиления стойкости симметричной кодовой криптосистемы к атаке на шифрограмму.

Симметричная кодовая криптосистема в Φ-метрике. Построим симметричную кодовую криптосистему для Φ-метрики в общем случае. Пусть $G_{k \times n}$ – порождающая матрица кода C над полем F в Φ-метрике с Φ-расстоянием d_Φ; D_Φ – быстрый алгоритм декодирования кода C в Φ-метрике, исправляющий до $t = \lfloor (d_\Phi - 1)/2 \rfloor$ Φ-ошибок; $S_{k \times k}$ – случайная невырожденная матрица; $P_{n \times n}$ – случайная перестановочная матрица. Секретным ключом криптосистемы является четверка

$$K = (S_{k \times k}, G_{k \times n}, P_{n \times n}, D_\Phi).$$

Пусть $\overline{m}$ – информационное сообщение, $\bar{z}$ – вектор Φ -ошибок, выбранный случайным образом так, чтобы выполнялось условие:

$$w_\Phi(\bar{z}) = t_1 < t, w_H(\bar{z}) \geq n(|F|-1)/|F|, \quad (1)$$

где $w_H(\bar{z})$ – вес Хэмминга вектора ошибок $\bar{z}$ над полем F. Тогда шифрование сообщения $\overline{m}$ выполняется по правилу:

$$\bar{c} = \overline{m} \cdot S_{k\times k} \cdot G_{k\times n} \cdot P_{n\times n} + \bar{z}.$$

Пусть криптограмма $\bar{c}$ передается по зашумленному каналу, в котором к криптограмме добавляется случайный вектор $\bar{e}$ Φ -веса не более $t - t_1$. Тогда для расшифрования принятого сообщения $\bar{c}' = \bar{c} + \bar{e}$ первоначально выполняется декодирование вектора $\bar{c}' \cdot P_{n\times n}^{-1}$: $\bar{y}' = D_\Phi(\bar{c}' \cdot P_{n\times n}^{-1})$, а затем вычисляется информационное сообщение $\overline{m} = \bar{y}' \cdot S_{k\times k}^{-1}$. Алгоритм расшифрования работает корректно. Действительно, принятый вектор $\bar{c}'$ имеет вид

$$\bar{c}' = \overline{m} \cdot S_{k\times k} \cdot G_{k\times n} \cdot P_{n\times n} + \bar{z} + \bar{e}.$$

Так как

$$d_\Phi(\bar{z} + \bar{e}) \leq d_\Phi(\bar{z}) + d_\Phi(\bar{e}) \leq t_1 + t - t_1 = t,$$

то алгоритм декодирования D_Φ корректно исправляет вектор ошибок $\bar{z} + \bar{e}$.

Стойкость предложенной криптосистемы к статистической, описанной в [6], основана на том, что к кодовому слову $\overline{m} \cdot S_{k\times k} \cdot G_{k\times n} \cdot P_{n\times n}$ добавляется вектор $\bar{z}$ веса Хэмминга не менее $n/2$, что является достаточным условием для противодействия атаке [6]. Размер секретного ключа K равен $k^2 + n(k+1)$ элементов поля Φ, где k^2 – размер скремблирующей матрицы $S_{k\times k}$, kn – размер кодовой матрицы $G_{k\times n}$, n – размер перестановки, соответствующей матрице $P_{n\times n}$. Обычно декодер D_Φ для кода в Φ -метрике легко определяется по кодеру, поэтому на размер ключа K декодер D_Φ не влияет.

Заметим, что метрика Хэмминга является частным случаем Φ -метрики [2], однако коды в хэмминговой метрике для построения стойких симметричных кодовых криптосистем не подходят, так как для таких кодов не выполняется условие (1). Поэтому для построения симметричных кодовых криптосистем должны быть использованы другие Φ -метрики. Далее рассматриваются конкретные Φ -метрики – ранговая метрика и метрика Вандермонда – и строятся кодовые криптосистемы на кодах в соответствующих метриках.

Криптосистема в ранговой Φ -метрике. Как отмечалось выше, криптосистема Стройка-Тилбурга обладает принципиальными ограничениями – большой объем секретного ключа и отсутствие возможности одновременно бороться с помехами в канале. Первое ограничение связно с тем, что необходимо хранить предопределенную синдромную таблицу T, размер которой составляет $(2n-k)\cdot|F|^{n-k}$ элементов поля F. Векторы ошибок $\bar{z}$ из T должны обладать тем свойством, что их вес Хэмминга над полем F должен быть не менее половины длины кодового слова. Наибольшая стойкость обеспечивается в случае, когда вес вектора ошибки удовлетворяет ограничению (1). Это ограничение не позволяет осуществить за приемлемое время атаку методом статистического криптоанализа на секретный ключ по выбранному открытому тексту [6]. Так как декодеры для кода C в Хэмминговой метрике не могут однозначно исправлять ошибки,

обладающие свойством (1), то такие ошибки необходимо хранить. Второе ограничение криптосистемы Стройка-Тилбурга – невозможность одновременно бороться с искажениями в канале – связано с тем, что для повышения стойкости криптосистемы введена нелинейная функция $f_{\bar{z}}$. В случае, если в криптосистеме Стройка–Тилбурга не использовать нелинейную функцию $f_{\bar{z}}$, то, как показано в [6], можно за $O(kn(n-k)2^{2(n-k)})$ операций в поле F осуществить успешную атаку на секретный ключ по выбранному открытому шифртексту.

В настоящей работе с целью построения симметричной кодовой криптосистемы предлагается использовать линейные коды в ранговой метрике – коды Габидулина [7]. Как показано в [2], ранговая метрика является Ф -метрикой. Опишем предлагаемую криптосистему. Пусть $\Gamma_{k\times n}$ – порождающая матрица кода Габидулина C с порождающим вектором $\bar{g}$ над полем F_{qN} (q - степень простого числа) и ранговым расстоянием $d = n-k+1$, $n \le N$; пусть $k = u+l$, $u,l \in N$; $D_{\bar{g}}$ – быстрый алгоритм декодирования кода Габидулина, исправляющий до $t = \lfloor (d-1)/2 \rfloor$ ранговых ошибок; $S_{u\times u}$ – случайная невырожденная матрица; $P_{n\times n}$ – случайная перестановочная матрица. Пусть $K = (S_{u\times u}, \Gamma_{k\times n}, P_{n\times n})$ – секретный ключ модифицированной криптосистемы. Пусть $\bar{m} \in F_{qN}^{u}$ – информационное сообщение, $\bar{v} \in F_{qN}^{l}$ – вектор, выбранный случайным образом, $\bar{z} \in F_{qN}^{n}$ – вектор ошибок, выбранный случайным образом так, что ранг этого вектора над полем F_q равен $t_1 (< t)$, и выполняется условие (1), тогда шифрование сообщения $\bar{m} (\in F_{qN}^{u})$ выполняется по правилу:

$$\bar{c} = (\bar{m} \cdot S_{u\times u} \,||\, \bar{v}) \cdot \Gamma_{k\times n} \cdot P_{n\times n} + \bar{z}.$$

Пусть криптограмма $\bar{c}$ передается по зашумленному каналу, в котором к криптограмме добавляется случайный вектор $\bar{e}$ ранга не более $t - t_1$. Для расшифрования вектора $\bar{c}' = \bar{c} + \bar{e}$ выполняется декодирование $\bar{b} = D_{\bar{g}}(\bar{c}' \times P_{n\times n}^{-1})$; далее вектор $\bar{b}$ представляется в виде $\bar{b} = \bar{b}_1 \,||\, \bar{b}_2$, где $\bar{b}_1 \in F_{qN}^{u}$, $\bar{b}_2 \in F_{qN}^{l}$, и вычисляется сообщение $\bar{m} = \bar{b}_1 \cdot S_{u\times u}^{-1}$. Принятый вектор $\bar{c}'$ имеет вид:

$$\bar{c}' = (\bar{m} \cdot S_{u\times u} \,||\, \bar{v}) \cdot \Gamma_{k\times n} \cdot P_{n\times n} + \bar{z} + \bar{e}.$$

Так как ранг вектора из F_{qN}^{n} над полем F_q является метрикой [7], то $r(\bar{z}+\bar{e} \,|\, q) \le r(\bar{z} \,|\, q) + r(\bar{e} \,|\, q) \le t_1 + t - t_1 = t$. Следовательно, алгоритм декодирования корректно исправляет вектор $\bar{z} + \bar{e}$.

В настоящей работе построен алгоритм генерации зашумляющих векторов $\bar{z}$, ранг которых не превосходит t_1, но при этом выполняется условие (1), достаточное для противодействия атаке методом статистического криптоанализа.

Вход: t_1 – ранговый вес вектора $\bar{z} \in F_{qN}^{n}$, $d (> t_1)$ – вес Хэмминга вектора $\bar{z}$.

Выход: вектор ошибок $\bar{z}$.

Шаг 1. Сгенерировать случайным образом t_1 линейно независимых векторов $\bar{a}_1,..,\bar{a}_{t_1} \in F_q^{t_1}$ длиной t_1 над полем F_q и $d-t_1$ ненулевых векторов $\bar{a}_{t_1+1},..,\bar{a}_d \in F_q^{t_1}$.

Шаг 2. Записать векторы $\bar{a}_1,..,\bar{a}_d$ по столбцам в виде $(t_1 \times d)$-матрицы над полем F_q: $M_{t_1 \times d} = (\bar{a}_i^T)_{i=1}^d$.

Шаг 3. Приписать справа к матрице $M_{t_1 \times (d)}$ нулевую матрицу размерностью $t_1 \times (n-d)$: $M'_{t_1 \times n} = M_{t_1 \times d} \mid O_{t_1 \times (n-d)}$, и далее снизу к $M'_{t_1 \times n}$ приписать $N - t_1$ строк, являющихся линейными комбинациями строк $M'_{t_1 \times n}$. В результате получим $A'_{N \times n}$;

Шаг 4. Искомая матрица $A(\bar{z})$ вычисляется как произведение матриц над полем F_q: $A(\bar{z}) = P^l_{N \times N} A'_{N \times n} P^r_{n \times n}$, где $P^l_{N \times N}$ и $P^r_{n \times n}$ – перестановочные матрицы. Матрица $A(\bar{z})$ – это представление вектора $\bar{z} \in F_{qN}^n$ в виде матрицы над полем F_q.

Конец алгоритма.

Для полей характеристики 2 получена оценка числа возможных зашумляющих векторов, прямо влияющая на стойкость криптосистемы.

Теорема. *Пусть* Z *– множество всех зашумляющих векторов, получаемых с помощью алгоритма генерирования векторов ранга* t_1 *и веса Хэмминга* $n(|F_{2N}|-1)/|F_{2N}|$ *над полем* F_{2N}, $K(t_1,2)$ *– число невырожденных квадратных матриц размерностью* $t_1 \times t_1$ *над полем* F_2, $L = \sum_{i=1}^{t_1} C_{t_1}^i$. *Тогда*

$$|Z| = K(t_1,2) C_{n-t_1}^{d-t_1} L^{d-t_1} (L+1)^{n-t_1}.$$

Доказательство. Как следует из условия теоремы, на первом шаге алгоритма невырожденную матрицу можно выбрать одним из $K(t_1,2)$ способов. Сгенерировать на $d-t_1$ ненулевых векторов длиной t_1 можно $C_{n-t_1}^{d-t_1} L^{d-t_1}$ способами, а число линейных комбинаций t_1 векторов определяется выражением $L = \sum_{i=1}^{t_1} C_{t_1}^i$. Тогда на третьем шаге имеется $(L+1)^{n-t_1}$ способов приписать линейные комбинации t_1 векторов. Таким образом,

$$|Z| = K(t_1,2) C_{n-t_1}^{d-t_1} L^{d-t_1} (L+1)^{n-t_1}. \quad \square$$

На практике для защиты от помех хорошими корректирующими свойствами обладают коды Габидулина над полями F_{2^16} и F_{2^32}. Для этих кодов получены оценки стойкости усовершенствованной криптосистемы Стройка–Тилбурга. Стойкость оценивалась по мощности множества зашумляющих векторов. Результаты оценки приведены в табл. 1 и 2. В первой строке каждой таблицы указан ранг искусственно добавляемой ошибки при шифровании (ранг вектора $\bar{z}$), а в первом столбце указан ранг естественной ошибки, которая может одновременно исправляться при расшифровании. Часть ячеек в таблицах не заполнены, что означает невозможность применения к модифицированной криптосистеме Стройка–Тилбурга соответсвующих соотношений ранга добавляемой искусственно ошибки и ранга естественной ошибки.

Таблица 1

Стойкость модифицированной криптосистемы над F_{2^16}

	1	2	3	4	5	6	7
0	4E+5	3,59E+16	1,66E+25	5,89E+32	3,24E+39	3,63E+45	9,20E+50
1	4E+5	3,59E+16	1,66E+25	5,89E+32	3,24E+39	3,63E+45	–
2	4E+5	3,59E+16	1,66E+25	5,89E+32	3,24E+39	–	–
3	4E+5	3,59E+16	1,66E+25	5,89E+32	–	–	–
4	4E+5	3,59E+16	1,66E+25	–	–	–	–
5	4E+5	3,59E+16	–	–	–	–	–
6	4E+5	–	–	–	–	–	–

Таблица 2

Стойкость модифицированной криптосистемы над полем F_{2^32}

	2	4	6	8	10	12	14
0	1,42E+34	1,66E+71	4,60E+103	1,80E+133	2,18E+160	9,77E+184	1,66E+207
1	1,42E+34	1,66E+71	4,60E+103	1,80E+133	2,18E+160	9,77E+184	1,66E+207
2	1,42E+34	1,66E+71	4,60E+103	1,80E+133	2,18E+160	9,77E+184	1,66E+207
3	1,42E+34	1,66E+71	4,60E+103	1,80E+133	2,18E+160	9,77E+184	–
4	1,42E+34	1,66E+71	4,60E+103	1,80E+133	2,18E+160	9,77E+184	–
5	1,42E+34	1,66E+71	4,60E+103	1,80E+133	2,18E+160	–	–
6	1,42E+34	1,66E+71	4,60E+103	1,80E+133	2,18E+160	–	–
7	1,42E+34	1,66E+71	4,60E+103	1,80E+133	–	–	–
8	1,42E+34	1,66E+71	4,60E+103	1,80E+133	–	–	–
9	1,42E+34	1,66E+71	4,60E+103	–	–	–	–
10	1,42E+34	1,66E+71	4,60E+103	–	–	–	–
11	1,42E+34	1,66E+71	–	–	–	–	–
12	1,42E+34	1,66E+71	–	–	–	–	–
13	1,42E+34	–	–	–	–	–	–
14	1,42E+34	–	–	–	–	–	–

Анализ стойкости модифицированной криптосистемы Стройка–Тилбурга по мощности множества зашумляющих векторов показывает, что, во-первых, стойкость системы растет как при увеличении ранга добавляемой ошибки, так и при увеличении мощности поля, над которым строятся ранговые коды, и, во-вторых, построенная криптосистема, обеспечивая высокую стойкость (начиная с ранга 3 добавляемой ошибки в случае поля F_{2^16} и ранга 2 в случае поля F_{2^32}), позволяет одновременно бороться с естественными помехами в канале. Эта особенность построенной кодовой криптосистемы дает возможность, например, строить комплексную защиту информации от полной технической утечки в зашумленных цифровых каналах связи с использованием элементной базы одного помехоустойчивого кодека.

Криптосистема в Ф-метрике Вандермонда. Рассмотрим специальную Ф-метрику, ассоциированную с матрицей Вандермонда. Для нее построен код с максимальным Ф-расстоянием и предложен быстрый алгоритм декодирования в [2], который сводится к задаче декодирования некоторого обобщенного кода Рида-Соломона. Кодовая криптосистема на основе кодов в Ф-метрике Вандермонда строится аналогично криптосистеме в ранговой Ф-метрике. Однако в отличие от последней, где декодер ранговых кодов не требует модификации, для криптосистемы в метрике Вандермонда не применим оригинальный декодер из [2]. Адаптируем декодер из [2] для построения симметричной криптосистемы на Ф-метрике Вандермонда.

Для изложения адаптированного алгоритма приведем определедение проективной Φ-метрики Вандермонда в соответствии с [2]. Рассмотрим обобщенную матрицу Вандермонда

$$F = \begin{pmatrix} u_1 & u_1x_1 & \dots & u_1x_1^{n-1} \\ u_2 & u_2x_2 & \dots & u_2x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ u_N & u_Nx_N & \dots & u_Nx_N^{n-1} \end{pmatrix},$$

где $n \le N, u_i \in \Phi_q \setminus \{0\}, x_i \in \Phi_q$ – различные, $i = 1 \dots N$. Возьмем в качестве элементов $f_1, f_2, \dots, f_N$, задающих проективную Φ-метрику Вандермонда строки матрицы F. Пусть линейный (n, k)-код X задается с помощью порождающей матрицы

$$G_{k\times n} = \begin{pmatrix} v_1 & v_1y_1 & \dots & v_1y_1^{n-1} \\ v_2 & v_2y_2 & \dots & v_2y_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ v_k & v_ky_k & \dots & v_ky_k^{n-1} \end{pmatrix},$$

где $v_i \in \Phi_q \setminus \{0\}$, а $y_i \in \Phi_q$ – различные, $i = 1 \dots k$. Кроме того, выберем y_i таким образом, чтобы они не совпадали ни с одним из x_j. В этом случае объединение матриц F и $G_{k\times n}$ также является обобщенной матрицей Вандермонда. Отметим, что размерность кода k должна удовлетворять соотношению $k + N < q$, поскольку максимально возможное число линейно независимых строк обобщенной матрицы Вандермонда над полем Φ_q равно q. В [2] доказано, что код X, задаваемый матрицей $G_{k\times n}$, является кодом с максимальным Φ-расстоянием $d_\Phi(X) = n - k + 1$. То есть код может исправлять вплоть до $t_\Phi = \lfloor n - k \rfloor / 2$ Φ-ошибок.

Пусть $\bar{c} = \bar{a}G + \bar{e} = \bar{g} + \bar{e}$, где $\bar{a}$ – информационный вектор, $\bar{g}$ – кодовый, а $\bar{e}$ – вектор Φ-ошибок. Причем Φ-вес вектора ошибки $\bar{e}$ не превосходит t_Φ. Тогда $\bar{e}$ можно представить в следующем виде: $\bar{e} = m_1f_1 + m_2f_2 + \dots + m_Nf_N$ так, что вес Хэмминга вектора $\bar{m} = (m_1, m_2, \dots, m_N)$ равен $w_H(\bar{m}) = t_\Phi$. Покажем, что в этом случае существует быстрый алгоритм декодирования. Рассмотрим конкатенацию матриц F, $G_{k\times n}$ следующего вида:

$$\begin{pmatrix} G_{k\times n} \\ F \end{pmatrix} = \begin{pmatrix} v_1 & v_1y_1 & \dots & v_1y_1^{n-1} \\ v_2 & v_2y_2 & \dots & v_2y_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ v_k & v_ky_k & \dots & v_ky_k^{n-1} \\ u_1 & u_1x_1 & \dots & u_1x_1^{n-1} \\ u_2 & u_2x_2 & \dots & u_2x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ u_N & u_Nx_N & \dots & u_Nx_N^{n-1} \end{pmatrix}. \qquad (2)$$

Выделим первые n строк в матрицу V. По построению матрица V является невырожденной, поэтому можно найти обратную V^{-1}. Умножим матрицу (2) на V^{-1}:

$$\begin{pmatrix} G_{k\times n} \\ F \end{pmatrix} V^{-1} = \begin{pmatrix} E_k & O \\ O & E_{n-k} \\ R_1 & R_2 \end{pmatrix}, \tag{3}$$

где E_p – единичная матрица порядка p. Матрица $(R_1\ R_2)$ является обобщенной матрицей Коши размером $(N-n+k)\times n$ с элементами вида $r_{ij} = \alpha_i\beta_j/(\mu_i - \nu_j)$, которые можно получить явно из леммы П.1 в [2]. Умножим вектор $\bar{c} = \bar{g} + \bar{e}$ на V^{-1} справа:

$$(\bar{g} + \bar{e})V^{-1} = (\bar{a}G_{k\times n} + \bar{m}F)V^{-1} = \tilde{g} + \bar{m}\tilde{F} = \tilde{g} + \tilde{e}.$$

Ввиду (3), последние $n-k$ компонент кодового вектора $\tilde{g}$ нулевые. Это позволяет определить $n-k$ компонент вектора $\tilde{e} = \bar{m}FV^{-1}$. Покажем что этого достаточно для восстановления всего вектора $\bar{m}$. Для этого необходимо решить систему уравнений $\bar{m}\tilde{F} = \tilde{e}$ или эквивалентную систему $\tilde{F}^{\tau}\bar{m}^{\tau} = \tilde{e}^{\tau}$:

$$\begin{pmatrix} O & R_1 \\ E_{n-k} & R_2 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_N \end{pmatrix} = \begin{pmatrix} * \\ \vdots \\ \tilde{e}_{N-n+k+1} \\ \vdots \\ \tilde{e}_N \end{pmatrix}. \tag{4}$$

Рассмотрим последние $n-k$ строк системы (4):

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & r_{1,1} & \cdots & r_{1,N-n+k} \\ 0 & 1 & \cdots & 0 & r_{2,1} & \cdots & r_{2,N-n+k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & r_{n-k,1} & \cdots & r_{n-k,N-n+k} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_N \end{pmatrix} = \begin{pmatrix} \hat{e}_1 \\ \hat{e}_2 \\ \vdots \\ \hat{e}_{n-k} \end{pmatrix},$$

где $\hat{e}_1 = \tilde{e}_{N-n+k+1}, \hat{e}_2 = \tilde{e}_{N-n+k+2}, \ldots, \hat{e}_{n-k} = \tilde{e}_N$. Матрица $H = (E_{n-k} \mid R_2)$ представляет собой конкатенацию единичной матрицы порядка $n-k$ и обобщенной матрицы Коши R_2. С помощью леммы П.2 из [2] умножением слева на подходящую квадратную невырожденную матрицу Φ порядка $n-k$ матрица H может быть преобразована к виду обобщенной матрицы Вандермонда $H' = (\Phi \mid \Phi R_2)$. Таким образом, система преобразуется к следующему виду:

$$H'm = \Phi \begin{pmatrix} \hat{e}_1 \\ \hat{e}_2 \\ \vdots \\ \hat{e}_{n-k} \end{pmatrix},$$

где правая часть и матрица H' известны. Поиск решения данной системы является задачей декодирования некоторого ОРС-кода C' с проверочной матрицей H'. Задача имеет единственное решение, если вес Хэмминга вектора $\overline{m}$ не превышает корректирующей способности кода t_Φ. Известны быстрые алгоритмы декодирования для ОРС-кодов [1]. Для определения вектора $\overline{m}$ и последующего вычисления векторов $\overline{e}$ и $\overline{g}$ достаточно применить один из известных быстрых алгоритмов декодирования обобщенных кодов Рида-Соломона.

Выводы. Повышение криптостойкости кодовых криптосистем возможно не только путем увеличения параметров кодеков и скремблирующих матриц, но и посредством перехода от метрики Хэмминга к другим метрикам, в частности к Φ-метрикам, для которых выполняется условие (1). Частным случаем Φ-метрик, для которых выполняется условие (1), являются ранговая Φ-метрика и Φ-метрика Вандермонда. Для этих метрик в настоящей работе построены симметричные кодовые криптосистемы. В частности, анализ показал, что при стандартных параметрах кодеков (например, для (16,8)- и (32,16)-кодов Габидулина) криптосистема в ранговой метрике обладает высокой стойкостью к статистическому криптоанализу. Кроме того, эта криптосистема может использоваться на практике для одновременной (за одну операцию) защиты как от несанкционированного чтения передаваемой информации, так и от «ранговых» помех, имеющих место, например, в системах многоканальной радиосвязи. Для криптосистемы в метрике Вандермонда адаптирован алгоритм быстрого декодирования из [2]. Вопрос о применении криптосистемы в Φ-метрике Вандермонда для одновременной борьбы с помехами и технической утечкой, а также уточнение стойкости этой криптосистемы к атаке методом статистического криптоанализа представляет интерес для дальнейшего исследования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Сидельников В.М.* Теория кодирования. – М.: Физматлит, 2008. – 324 с.
2. *Габидулин Э.М., Обернихин В.А.* Коды в Φ-метрике Вандермонда и их применение // Проблемы передачи информации. – 2003. – Т. 39, № 2. – С. 3-14.
3. *Яковлев В.А.* Защита информации на основе кодового зашумления / Под ред. В.И. Коржика. – СПб., 1993.
4. *Косолапов Ю.В.* Способ защиты информации от технической утечки, основанный на применении кодового зашумления и кодовых криптосистем: Автореф. дис. … канд. техн. наук. – Ростов-на-Дону. 2009. – 24 с.
5. *Деундяк В.М., Косолапов Ю.В., Чекунов Е.С.* О реализации и применении модификации Стройка-Тилбурга шифросистем типа Мак-Элиса // Материалы международного Российско-Абхазского симпозиума Уравнения смешанного типа и родственные проблемы анализа и информацтики. – Нальчик, 2009. – С. 75-77.
6. *Val Tilburg J.* Security-Analisys of a Class of Cryptosystems Based on Linear Error-Correcting Codes. Eindhoven: PTT Research, 1994. – 198 p.
7. *Габидулин Э.М.* Теория кодов с максимальным ранговым расстоянием // Проблемы передачи информации. – 1985. – Т. 21, № 1. – С. 1-12.

Косолапов Юрий Владимирович
Федеральное государственное образовательное учреждение высшего профессионального образования «Южный федеральный университет».
E-mail: itaim@mail.ru.
344090, г. Ростов-на-Дону, ул. Мильчакова, 8а.
Тел.: +79061833020

Чекунов Евгений Сергеевич
E-mail: echekunov@gmail.com.
Тел.: +79054782547.

Kosolapov Yury Vladimirovich
Federal State-Owned Educational Establishment of Higher Vocational Education «Southern Federal University».
E-mail: itaim@mail.ru.
8a, Milchakova street, Rostov-on-Don, 344090, Russia.
Phone: +79061833020.

Chekunov Evgeny Sergeevich
E-mail: echekunov@gmail.com.
Phone: +79054782547.

УДК 004.056.5

В.В. Мкртичян

СХЕМА СПЕЦИАЛЬНОГО ШИРОКОВЕЩАТЕЛЬНОГО ШИФРОВАНИЯ, ОСНОВАННАЯ НА НЕКОТОРЫХ КОНКАТЕНИРОВАННЫХ КОДАХ, И ИССЛЕДОВАНИЕ ГРАНИЦЫ ЕЕ ПРИМЕНЕНИЯ

Исследуется проблема защиты легально тиражируемой цифровой продукции от несанкционированного распространения. Строится математическая модель схемы специального широковещательного шифрования на основе обобщенных кодов Рида–Соломона конкатенированных с кодами Адамара и декодера Гурусвами–Судана. Разрабатывается программная реализация математической модели. Проводится исследование возможности ее применения в случае превышения допустимого числа членов коалиции злоумышленников.

Коды Рида–Соломона, конкатенированные коды; списочное декодирование; широковещательное шифрование; поиск злоумышленников.

V.V. Mkrtichan

BROADCAST ENCRYPTION SCHEME BASED ON SOME CONCATENATED CODES, RESEARCH OF BOUND OF THE SCHEME APPLYING

The problem of protecting legally replicated digital products from unauthorized distribution.ьConstruct a mathematical model of Skye special broadcast encryption scheme based on generalized Reed-Solomon concatenated with Hadamard codes and deco-dera Guruswami-Sudan.ьDeveloped software implementation of mathematical models.ьWe study its possible use in case of exceeding the allowable number of members of the coalition attackers.

Reed–Solomon codes; concatenated codes; list decoding; broadcast encryption; tracing traitors.

1. Введение и постановка задачи. В работе [1] рассмотрен перспективный способ защиты легально тиражируемой цифровой продукции от несанкционированного распространения, называемый схемой специального широковещательного шифрования (ССШШ). Известно, что злоумышленники, являющиеся легальными пользователями ССШШ, могут объединяться в коалиции и пытаться атаковать ССШШ. В [1] доказано, что для эффективного поиска всей коалиции или, по крайней мере, ее непустого подмножества можно применять обобщенный код Рида–Соломона (ОРС-код), специальным образом конкатенированный с кодом Адамара (КОРСА-код). При этом в качестве алгоритма декодирования предлагается использовать эффективный алгоритм списочного декодирования Гурусвами–Судана [2]. В [3] представлена математическая модель и теоретическое исследование эффективной ССШШ для ОРС-кода, в [4], [5] проведено экспериментальное исследование этой схемы. В [6] построена компьютерная модель списочного декодера Гурусвами–Судана для КОРСА-кода, выступающая наиболее сложным элементом