Ю. В. Косолапов, **Е. С. Чекунов** (Ростов-на-Дону, ЮФУ).
Применение $\mathcal{F}$-метрики в симметричных кодовых криптосистемах.

Задача теоретического и экспериментального исследования методов защиты информации, основанных на теории помехоустойчивого кодирования, является актуальной [1]–[3]. Интерес к использованию помехоустойчивых кодов, в частности, обусловлен возможностью построения комплексных методов защиты. Такие методы защиты, например, построены и исследованы в [1], [4], где кодовое зашумление одновременно применяется для защиты информации от *частичной* технической утечки и внешних помех. Для защиты информации от *полной* технической утечки конструктивно подходят симметричные кодовые криптосистемы [4], [5]. Одной из стойких симметричных кодовых криптосистем является криптосистема Стройка–Тилбурга [2], обладающая, однако, практическими ограничениями: большой объем ключа (порядка $(2n-k)|\mathbf{F}|^{n-k}$ элементов поля $\mathbf{F}$) и нет возможности одновременно бороться с помехами в канале. Поэтому актуальной является задача построения симметричных кодовых криптосистем без таких ограничений. В работе, представленной данным сообщением, строится симметричная криптосистема с использованием кодов в $\mathcal{F}$-метриках [3].

Пусть $G_{k\times n}$ — порождающая матрица кода C (над полем $\mathbf{F}$) в $\mathcal{F}$-метрике с $\mathcal{F}$-расстоянием $d_{\mathcal{F}}$; $D_{\mathcal{F}}$ — быстрый алгоритм декодирования кода C в $\mathcal{F}$-метрике, исправляющий до $t=\lfloor (d_{\mathcal{F}}-1)/2\rfloor$ $\mathcal{F}$-ошибок (см., например, [3]); $S_{k\times k}$ — случайная невырожденная матрица; $P_{n\times n}$ — случайная перестановочная матрица. Секретным ключом криптосистемы является четверка $K=(S_{k\times k}, G_{k\times n}, P_{n\times n}, D_{\mathcal{F}})$, объем K равен $k^2+n(k+1)$ элементов поля $\mathbf{F}$. Пусть $\overline{m}$ — информационное сообщение, $\overline{z}$ — вектор $\mathcal{F}$-ошибок, выбранный случайным образом так, чтобы выполнялось условие

$$w_{\mathcal{F}}(\overline{z})=t_1<t, \quad w_{\mathcal{H}}(\overline{z})\geqslant n/2, \tag{1}$$

где $w_{\mathcal{H}}(\overline{z}), w_{\mathcal{F}}(\overline{z})$ — вес Хэмминга и $\mathcal{F}$-вес вектора ошибок $\overline{z}$, соответственно.

Шифрование: $\overline{c}=\overline{m}\,S_{k\times k}\,G_{k\times n}\,P_{n\times n}+\overline{z}$.

Расшифрование: $\overline{y}=D_{\mathcal{F}}(\overline{c}\,P^{-1}_{n\times n})$, $\overline{m}=\overline{y}\,S^{-1}_{k\times k}$.

Стойкость предложенной криптосистемы к статистической атаке на шифрограмму, описанной в [2], основана на том, что к кодовому слову добавляется вектор $\overline{z}$, удовлетворяющий условию (1). Такие вектора ошибок можно генерировать в процессе шифрования и нет необходимости хранить, как это предполагается в оригинальной системе Стройка–Тилбуга. Частным случаем $\mathcal{F}$-метрик, для которых выполняется условие (1), являются ранговая $\mathcal{F}$-метрика и $\mathcal{F}$-метрика Вандермонда. Симметричная криптосистема на ранговых кодах, позволяющая одновременно бороться с полной технической утечкой и с ранговыми помехами, построена в [4]. В работе построена симметричная кодовая криптосистема на основе кодов в $\mathcal{F}$-метрике Вандермонда. Вопрос о применении криптосистемы в $\mathcal{F}$-метрике Вандермонда для одновременной борьбы с технической утечкой и помехами в настоящее время исследуется.

СПИСОК ЛИТЕРАТУРЫ

1. *Яковлев В. А.* Защита информации на основе кодового зашумления. СПб.: ВАС, 1993.
2. *Val Tilburg J.* Security-Analisys of a Class of Cryptosystems Based on Linear Error-Correcting Codes. Eindhoven: PTT Research, 1994, p. 198.
3. *Габидулин Э. М., Обернихин В. А.* Коды в $\mathcal{F}$-метрике Вандермонда и их применение. — Проблемы передачи информации, 2003, т. 39, № 2, с. 3–14.
4. *Косолапов Ю. В.* Способ защиты информации от технической утечки, основанный на применении кодового зашумления и кодовых криптосистем. Автореферат диссертации на соискание ученой степени канд. техн. наук. Ростов-на-Дону: ЮФУ, 2009, 24 с.

5. *Деундяк В. М.*, *Косолапов Ю. В.*, *Чекунов Е. С.* О реализации и применении модификации Стройка–Тилбурга шифросистем типа Мак–Элиса. — В сб.: Материалы международного Российско-Абхазского симпозиума «Уравнения смешанного типа и родственные проблемы анализа и информатики». Нальчик, 2009, с. 75-77.