УДК 621.391

А.А. КУЗНЕЦОВ

Харьковский университет Воздушных Сил им. И. Кожедуба, Украина

НЕСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ДОКАЗУЕМОЙ СТОЙКОСТИ НА АЛГЕБРАИЧЕСКИХ БЛОКОВЫХ КОДАХ

Исследуются несимметричные криптосистемы доказуемой стойкости на алгебраических блоковых кодах. Разрабатывается математический аппарат криптографических преобразований с использованием алгебраических блоковых кодов.

несимметричная криптосистема, алгебраический блоковый код, доказуемая стойкость, декодирование, криптографические преобразования, криптограмма

Постановка проблемы в общем виде и анализ литературы

Перспективным направлением в развитии теории защиты информации является разработка и исследование несимметричных криптографических систем доказуемой стойкости [1 – 3].

Модель доказуемой стойкости основана на сведении задачи бесключевого чтения к решению некоторой хорошо изученной теоретико-сложностной задачи, например, к дискретному логарифмированию или факторизации [2]. Практическое использование средств защиты доказуемой стойкости, наряду с теоретически обоснованной моделью безопасности, сопряжено с возможностью применения инфраструктуры открытых ключей [2]. В тоже время проблема построения эффективных криптосистем остается острой и актуальной. Связано это, в первую очередь, с высокой сложностью реализации известных несимметричных криптоалгоритмов [1, 2]. Перспективным направлением в этом смысле являются криптосистемы на алгебраических блоковых кодах [3 – 5].

Построение несимметричных криптографических средств защиты информации на алгебраических блоковых кодах сопряжено с маскированием быстрого правила декодирования, т.е. со сведением задачи бесключевого чтения открытого текста к решению неуполномоченным пользователем теоретико-сложностной задачи декодирования случайного кода [5]. Эффективным средством маскирования быстрого правила декодирования являются маскирующие матричные отображения, порождающие большие ансамбли линейных блоковых кодов с сохранением весового спектра и фиксированных кодовых соотношений [6].

Целью данной статьи является математическая формализация процессов прямого и обратного преобразования (шифрования и расшифрования), разработка математического аппарата криптографических преобразований, оценка сложности их реализации.

1. Математический аппарат быстрых криптографических преобразований с использованием алгебраических блоковых кодов

Математические основы современной криптографии заложены в работах известного американского ученого К. Шеннона [7], который впервые ввел абстрактное определение секретной системы и математически формализовал процесс криптографического преобразования информации. В классическое формальное определение криптосистемы входят следующие множества:

– множество открытых текстов $M = \{M_1, M_2, ..., M_m\}$;

– множество криптограмм $E = \{E_1, E_2, ..., E_m\}$,

– множество прямых отображений $\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_s\}$, параметризированных соответствующими

ключами: $\varphi_i : M \xrightarrow{K_i} E$;

– множество обратных отображений $\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_s^{-1}\}$, параметризированных соответствующими ключами: $\varphi_i^{-1} : E \xrightarrow{K_i^*} M$;

– множество ключей прямых отображений $\{K_1, K_2, \ldots, K_s\}$;

– множество ключей обратных отображений $K^* = \{K_1^*, K_2^*, \ldots, K_s^*\}$.

Если при этом $K \neq K^*$, то система асимметрична (несимметрична).

Дадим формальное определение несимметричных криптосистем на алгебраических блоковых кодах, формализуем процесс прямого и обратного криптографического преобразования (шифрования и расшифрования).

Несимметричная криптосистема 1-го типа, построенная на алгебраическом блоковом (n, k, d) коде C над $GF(q)$, формально задается совокупностью следующих множеств:

– множество открытых текстов

$$M = \{M_1, M_2, \ldots, M_q k\}, \text{ где } M_i = (I_0, I_1, \ldots, I_{k-1}),$$
$$\forall I_j \in GF(q);$$

– множество криптограмм

$$E = \{E_1, E_2, \ldots, E_q k\},$$

где $E_i = (c^*_{X_0}, c^*_{X_1}, \ldots, c^*_{X_{n-1}})$, $\forall c^*_{X_j} \in GF(q)$;

– множество прямых отображений

$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_s\}$, где $\varphi_i: M \to E$, $i = 1, 2, \ldots, s$;

– множество обратных отображений

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_s^{-1}\},$$

где $\varphi_i^{-1}: E \to M$, $i = 1, 2, \ldots, s$;

– множество ключей, параметризирующих прямые отображения

$$K = \{K_1, K_2, \ldots, K_s\} = \{G_X^1, G_X^2, \ldots, G_X^s\},$$

т.е. $\varphi_i : M \xrightarrow{K_i} E$;

– множество ключей, параметризирующих обратные отображения

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

т.е. $\varphi_i^{-1} : E \xrightarrow{K_i^*} M$,

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

В рассматриваемой несимметричной криптосистеме алгебраический (n, k, d) код C с быстрым алгоритмом декодирования маскируется под случайный (n, k, d) код C^* посредством умножения генераторной матрицы G кода C на хранящиеся в секрете маскирующие матрицы X^i, P^i и D^i:

$$G^i_X = X^i \cdot G \cdot P^i \cdot D^i. \qquad (1)$$

Не зная правила маскировки, т.е. конкретного набора матриц $\{X,P,D\}_i$, противник вынужден использовать сложный алгоритм декодирования случайного кода. Напротив, уполномоченный пользователь, знающий правило маскировки, может воспользоваться быстрым алгоритмом декодирования алгебраического кода.

Исходными данными при описании несимметричной криптосистемы 1-го типа является алгебраический блоковый (n, k, d) код C над $GF(q)$ и маскирующие матричные отображения, заданные множеством матриц $\{X,P,D\}_i$. Рассмотрим процесс формирования криптограммы E_i, исследуем эффективные пути его реализации с позиции алгебраических методов теории блоковых кодов.

Под прямым отображением $\varphi_i : M \xrightarrow{K_i} E$ в криптосистеме 1-го типа понимается процедура кодирования замаскированным алгебраическим кодом с добавлением к нему случайного вектора ошибки (с весом ошибки меньшей или равной исправляющей способности кода):

$$E_j = (c^*_{X_0}, c^*_{X_1}, \ldots, c^*_{X_{n-1}}) = M_j \cdot G^i_X + e =$$
$$= (I_0, I_1, \ldots, I_{k-1}) \cdot \begin{pmatrix} g_{X_{0,0}} & g_{X_{0,1}} & \cdots & g_{X_{0,n-1}} \\ g_{X_{1,0}} & g_{X_{1,1}} & \cdots & g_{X_{1,n-1}} \\ \cdots & \cdots & \cdots & \cdots \\ g_{X_{k-1,0}} & g_{X_{k-1,1}} & \cdots & g_{X_{k-1,n-1}} \end{pmatrix} + (2)$$
$$+ (e_0, e_1, \ldots, e_{n-1}),$$

где $g_{X_{l,m}}$ – элементы порождающей матрицы G^i_X замаскированного (n, k, d) кода C^* над $GF(q)$;

$e = (e_0, e_1, \ldots, e_{n-1})$ – случайный вектор ошибок

над $GF(q)$,

$$w(e_i) \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor .$$

Таким образом, криптограмма $E_j = (c^*_{X_0}, c^*_{X_1}, ..., c^*_{X_{n-1}})$, сформированная в криптосистеме 1-го типа, представляет собой кодовое слово замаскированного матричными отображениями (n, k, d) кода C^* над $GF(q)$ со случайно внесенным вектором ошибок, т.е.:

$$E_j = c_X + e = (c^*_{X_0}, c^*_{X_1}, ..., c^*_{X_{n-1}}),$$

где $c^*_{X_l} = c_{X_l} + e_l$, c_X – кодовое слово (n, k, d) кода C^* над $GF(q)$, $c_X = (c_{X_0}, c_{X_1}, ..., c_{X_{n-1}})$.

Принимая во внимание то обстоятельство, что ключевые матрицы $\{X, P, D\}_i$ в выражении (1) сформированы случайно и независимо, порождающая матрица G^i_X в общем случае не обладает какой либо специальной структурой, облегчающей вычисление криптограммы (2). В тоже время сложность формирования криптограммы как функция размера задачи растет полиномиально от параметров кода (подробная оценка сложности реализации рассматриваемых криптосистем проведена ниже).

Рассмотрим процесс расшифрования криптограммы E_i, исследуем эффективные пути его реализации с позиции алгебраических методов теории блоковых кодов.

Под обратным отображением $\varphi_i^{-1} : E \xrightarrow{K_i^*} M$ в несимметричной криптосистеме 1-го типа понимается процесс декодирования кодового слова с ошибками замаскированного кода C^*. Для его реализации необходимо выполнить следующие действия:

– снять действие матриц маскирования $\{P, D\}_i$ с криптограммы E_j:

$$E_j \cdot D^{-1} \cdot P^{-1} = E_j \cdot \Lambda^{-1} =$$

$$= (c^*_{X_0}, c^*_{X_1}, ..., c^*_{X_{n-1}}) \cdot \begin{pmatrix} \lambda'_{0,0} & \lambda'_{0,1} & ... & \lambda'_{0,n-1} \\ \lambda'_{1,0} & \lambda'_{1,1} & ... & \lambda'_{1,n-1} \\ ... & ... & ... & ... \\ \lambda'_{n-1,0} & \lambda'_{n-1,1} & ... & \lambda'_{n-1,n-1} \end{pmatrix} = \quad (3)$$

$$= (\bar{c}^*_0, \bar{c}^*_1, ..., \bar{c}^*_{n-1}),$$

где $\lambda'_{l,m}$ – элементы матрицы Λ^{-1} – обратной к унипотентной матрице $\Lambda = P \cdot D$;

– декодировать полученную последовательность $(\bar{c}^*_0, \bar{c}^*_1, ..., \bar{c}^*_{n-1})$ – кодовое слово с ошибками алгебраического (n, k, d) кода C над $GF(q)$:

$$(\bar{c}^*_0, \bar{c}^*_1, ..., \bar{c}^*_{n-1}) \to (\bar{c}_0, \bar{c}_1, ..., \bar{c}_{n-1}),$$

где во введенных выше обозначениях $\bar{c}^*_l = \bar{c}_l + e$;

– выделить информационную часть в кодовом слове $(\bar{c}_0, \bar{c}_1, ..., \bar{c}_{n-1})$:

$$(\bar{c}_0, \bar{c}_1, ..., \bar{c}_{n-1}) \to (\bar{I}_0, \bar{I}_1, ..., \bar{I}_{k-1});$$

– снять действие матрицы маскирования $\{X\}_i$ с полученной последовательности:

$$(I_0, I_1, ..., I_{k-1}) = (\bar{I}_0, \bar{I}_1, ..., \bar{I}_{n-1}) \cdot X^{-1} =$$

$$= (\bar{I}_0, \bar{I}_1, ..., \bar{I}_{n-1}) \cdot \begin{pmatrix} x'_{0,0} & x'_{0,1} & ... & x'_{0,k-1} \\ x'_{1,0} & x'_{1,1} & ... & x'_{1,k-1} \\ ... & ... & ... & ... \\ x'_{k-1,0} & x'_{k-1,1} & ... & x'_{k-1,k-1} \end{pmatrix},$$

где $x'_{l,m}$ – элементы матрицы X^{-1} – обратной к маскирующей матрице X.

Процедуры снятия действия матриц маскирования $\{X, P, D\}_i$ заключаются в умножении соответствующих векторов на обратные матрицы $\{X^{-1}, P^{-1}, D^{-1}\}_i$ и реализуются алгоритмами с полиномиальной сложности. Процедура декодирования последовательности, т.е. отображение

$$(\bar{c}^*_0, \bar{c}^*_1, ..., \bar{c}^*_{n-1}) \to (\bar{c}_0, \bar{c}_1, ..., \bar{c}_{n-1})$$

для алгебраических блоковых кодов так же реализуется алгоритмами полиномиальной сложности. Выделение информационной части в кодовом слове $(\bar{c}_0, \bar{c}_1, ..., \bar{c}_{n-1})$ для систематического способа кодирования состоит в считывании информационных символов с заранее определенных позиций в кодовом слове. Для несистематического способа кодирования выделение информационной части предполагает выполнение операции, полиномиальной сложности.

Таким образом, процесс расшифрования криптограммы E_i в рассматриваемой несимметричной

криптосистеме реализуем алгоритмами полиномиальной сложности. Как будет показано ниже, сложность криптографических преобразований сопоставима с блочно-симметричными криптоалгоритмами.

Формирование криптограммы в несимметричной криптосистеме 1-го типа реализуется через кодирование информационного вектора кодовым словом замаскированного кода. Стойкость к бесключевому чтению основана на трудоемкости его декодирования, т.е. нахождения специально вносимого вектора ошибок. Другими словами, вектор ошибок *e* в выражении (2) играет роль одноразового сеансового ключа, скрывающего информационную посылку $M_j = (I_1, I_2, ..., I_k)$. Изменив назначение векторов *e* и M_j, получим крипоситстему со следующими свойствами.

Несимметричная криптосистема 2-го типа, *построенная на алгебраическом блоковом (n, k, d)* коде *C* над *GF*(*q*), формально задается совокупностью следующих множеств:

– множество открытых текстов

$M = \{M_1, M_2, ..., M_\mu\}$, где $M_i = (e_0, e_1, ..., e_{n-1})$,

$$\forall e_j \in GF(q),\ w(M_i) \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor;$$

– множество криптограмм

$E = \{E_1, E_2, ..., E_\mu\}$, где $E_i = (c^*_{X_0}, c^*_{X_1}, ..., c^*_{X_{n-1}})$,

$$\forall c^*_{X_j} \in GF(q);$$

– множество прямых отображений

$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_s\}$, где $\varphi_i: M \to E$, $i = 1, 2, \ldots, s$;

– множество обратных отображений

$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_s^{-1}\}$, где $\varphi_i^{-1}: E \to M$, $i = 1, 2, \ldots, s$;

– множество ключей, параметризирующих прямые отображения

$$K = \{K_1, K_2, ..., K_s\} = \{G_X^1, G_X^2, ..., G_X^s\},$$ т.е.

$$\varphi_i : M \xrightarrow{K_i} E;$$

– множество ключей, параметризирующих обратные отображения

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

$$\text{т.е. } \varphi_i^{-1} : E \xrightarrow{K_i^*} M,$$

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

Исходными данными при описании несимметричной криптосистемы 2-го типа так же является алгебраический блоковый (*n, k, d*) код *C* над *GF*(*q*) и маскирующие матричные отображения, заданные множеством матриц $\{X,P,D\}_i$. Основное отличие состоит в процедуре формирования криптограммы E_i, которая соответствует добавлению случайно сформированного кодового слова $c_X = (c_{X_0}, c_{X_1}, ..., c_{X_{n-1}})$ замаскированного (*n, k, d*) кода *C** над *GF*(*q*) к информационной равновесной посылке $e = (e_0, e_1, ..., e_{n-1})$. Для общего случая

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

Формализуем прямое отображение $\varphi_i : M \xrightarrow{K_i} E$ в криптосистеме 2-го типа посредством следующего выражения:

$$E_j = (c^*_{X_0}, c^*_{X_1}, ..., c^*_{X_{n-1}}) = (I_0, I_1, ..., I_{k-1}) \cdot G_X^i + M_j =$$

$$= (I_0, I_1, ..., I_{k-1}) \cdot \begin{pmatrix} g_{X_{0,0}} & g_{X_{0,1}} & \cdots & g_{X_{0,n-1}} \\ g_{X_{1,0}} & g_{X_{1,1}} & \cdots & g_{X_{1,n-1}} \\ \cdots & \cdots & \cdots & \cdots \\ g_{X_{k-1,0}} & g_{X_{k-1,1}} & \cdots & g_{X_{k-1,n-1}} \end{pmatrix} + \quad (4)$$

$$+ (e_0, e_1, ..., e_{n-1}),$$

где $g_{X_{l,m}}$ – элементы порождающей матрицы G_X^i замаскированного (*n, k, d*) кода *C** над *GF*(*q*), $(I_0, I_1, ..., I_{k-1})$ – случайный вектор над *GF*(*q*),

$$w(e_i) \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor.$$

Таким образом, криптограмма

$$E_j = (c^*_{X_0}, c^*_{X_1}, ..., c^*_{X_{n-1}}),$$

сформированная в криптосистеме 2-го типа, представляет собой случайно сформированное кодовое слово замаскированного матричными отображениями (*n, k, d*) кода *C** над *GF*(*q*) с добавленным к нему информационным вектором $e = (e_0, e_1, ..., e_{n-1})$, т.е.:

$$E_j = c_X + M_j = (c^*_{X_0}, c^*_{X_1}, ..., c^*_{X_{n-1}}),$$

где $c^*_{X_l} = c_{X_l} + e_l$, c_X – кодовое слово (*n, k, d*) кода *C** над *GF*(*q*),

$$c_X = (c_{X_0}, c_{X_1}, ..., c_{X_{n-1}}).$$

Очевидно, как и для рассмотренной выше криптосистемы 1-го типа, сложность формирования криптограммы как функция размера задачи растет полиномиально от параметров кода (подробная оценка сложности реализации рассматриваемых криптосистем проведена ниже).

Оценим мощность множества открытых текстов $M = \{M_1, M_2, ..., M_\mu\}$. По определению, в качестве открытого текста используются вектора

$$M_i = (e_0, e_1, ..., e_{n-1}), \forall e_j \in GF(q),$$

$$w(M_i) \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor.$$

Число векторов веса $w(M_i) = t$ длины n символов из $GF(q)$ определяется выражением

$$\mu = (q-1)^t \cdot C_n^i. \qquad (5)$$

Обобщая приведенное выражение на случай $w(M_i) \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor$, получим:

$$\mu = \sum_{i=0}^{t} (q-1)^t \cdot C_n^i, \qquad (6)$$

случай $i = 0$ соответствует нулевой последовательности.

Под обратным отображением $\varphi_i^{-1} : E \xrightarrow{K_i^*} M$ в несимметричной криптосистеме 2-го типа понимается процесс декодирования кодового слова с ошибками замаскированного кода C^*. Для его реализации необходимо выполнить следующие действия:

– снять действие матриц маскирования $\{P, D\}_i$ с криптограммы E_j (см. выражение (3));

– декодировать полученную последовательность $(\overline{c}_0^*, \overline{c}_1^*, ..., \overline{c}_{n-1}^*)$ – кодовое слово с ошибками алгебраического (n, k, d) кода C над $GF(q)$;

– найденный вектор ошибок $e = (e_0, e_1, ..., e_{n-1})$ – равновесная информационная посылка.

Очевидно, что для выполнения обратного отображения (расшифрования) в криптосистеме 2-го типа требуется меньшее число операций, которые так же реализуются алгоритмами полиномиальной сложности. Кроме того, как будет показано ниже, при фиксированной относительной скорости передачи сообщений криптосистема 2-го типа обладает существенным преимуществом в стойкости к бесключевому чтению.

Рассмотренные выше криптосистемы позволяют помимо криптографического преобразования информационных сообщений интегрировано решать задачи помехоустойчивого кодирования. Действительно, если вес вектора $e = (e_0, e_1, ..., e_{n-1})$, выполняющего функции случайно сформированного сеансового ключа для криптосистемы 1-го типа и функции информационного вектора для криптосистемы 2-го типа, строго меньше исправляющей способности (n, k, d) кода над $GF(q)$, т.е.

$$w(e_i) < t = \left\lfloor \frac{(d-1)}{2} \right\rfloor,$$

то на приемной стороне при расшифровании криптограммы

$$E_j = c_X + M_j = (c_{X_0}^*, c_{X_1}^*, ..., c_{X_{n-1}}^*)$$

появляется возможность исправлять $t - w(e_i)$ случайно возникших при передаче ошибок.

Если $\rho = w(e) / t$ – доля исправляющей способности (n, k, d) кода, приходящегося на искусственное внесение при формировании криптограммы, то потенциальная стойкость криптосистемы к бесключевому чтению определяется величиной $\rho \cdot t$, а обеспечиваемая помехоустойчивость передаваемых криптограмм определяться величиной $(1 - \rho) \cdot t$.

Таким образом, несимметричные криптосистемы 1-го и 2-го типа позволяют выполнять быстрое несимметричное криптографическое преобразование информации и исправлять случайно возникающие ошибки.

Следует отметить, что современные протоколы передачи сообщений для контроля возникающих ошибок предполагают использование режима обнаружения с автоматическим переспросом. Эффективным средством интегрированного решения задач контроля ошибок в каналах с переспросом и быстрого криптографического преобразования информации являются криптосистемы 3-го типа.

Несимметричная криптосистема 3-го типа, построенная на алгебраическом блоковом (*n, k, d*) коде *C* над *GF*(*q*), формально задается совокупностью следующих множеств:

– множество открытых текстов

$M = \{M_1, M_2, \ldots, M_\mu\}$, где $M_i = (e_0, e_1, \ldots, e_{n-1})$,

$$\forall e_j \in GF(q),\ w(M_i) \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor;$$

– множество криптограмм

$$E = \{E_1, E_2, \ldots, E_\mu\}, \text{ где}$$

$$E_i = (S_{X_0}, S_{X_1}, \ldots, S_{X_{n-k-1}}),\ \forall S_{X_j} \in GF(q);$$

– множество прямых отображений

$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_s\}$, где $\varphi_i: M \to E$, $i = 1, 2, \ldots, s$;

– множество обратных отображений

$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_s^{-1}\}$, где $\varphi_i^{-1}: E \to M$, $i = 1, 2, \ldots, s$;

– множество ключей, параметризирующих прямые отображения

$$K = \{K_1, K_2, \ldots, K_s\} = \{H_X^1, H_X^2, \ldots, H_X^s\},$$

$$\text{т.е. } \varphi_i : M \xrightarrow{K_i} E;$$

– множество ключей, параметризирующих обратные отображения

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

$$\text{т.е. } \varphi_i^{-1} : E \xrightarrow{K_i^*} M,$$

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

Исходными данными при описании несимметричной криптосистемы 3-го типа является алгебраический блоковый (*n, k, d)* код *C* над *GF*(*q*) и маскирующие матричные отображения, заданные множеством матриц $\{X,P,D\}_i$. Основное отличие от рассмотренных выше криптосистем состоит в процедуре формирования криптограммы E_i, которая соответствует синдромной последовательности, полученной посредством умножения равновесного информационного вектора $M_i = (e_0, e_1, \ldots, e_{n-1})$ на проверочную матрицу H_X^i замаскированного (*n, k, d*) кода *C** над *GF*(*q*). Для общего случая

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

Формализуем прямое отображение $\varphi_i : M \xrightarrow{K_i} E$ в криптосистеме 3-го типа посредством следующего выражения:

$$\begin{aligned} E_j &= (S_{X_0}, S_{X_1}, \ldots, S_{X_{n-k-1}}) = M_j \cdot H_X^i = \\ &= (e_0, e_1, \ldots, e_{n-1}) \times \\ &\times \begin{pmatrix} h_{X_{0,0}} & h_{X_{0,1}} & \ldots & h_{X_{0,n-1}} \\ h_{X_{1,0}} & h_{X_{1,1}} & \ldots & h_{X_{1,n-1}} \\ \ldots & \ldots & \ldots & \ldots \\ h_{X_{k-1,0}} & h_{X_{k-1,1}} & \ldots & h_{X_{k-1,n-1}} \end{pmatrix}, \end{aligned} \quad (7)$$

где $h_{X_{l,m}}$ – элементы проверочной матрицы H_X^i замаскированного (*n, k, d*) кода *C** над *GF*(*q*), $(e_0, e_1, \ldots, e_{n-1})$ – информационный вектор над *GF*(*q*),

$$w(e_i) \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor.$$

Сложность формирования криптограммы при этом, как функция размера задачи, растет полиномиально от параметров кода (подробная оценка сложности реализации рассматриваемых криптосистем проведена ниже).

Под обратным отображением $\varphi_i^{-1} : E \xrightarrow{K_i^*} M$ в несимметричной криптосистеме 3-го типа понимается процесс декодирования кодового слова замаскированного кода *C** по известной синдромной последовательности $(S_{X_0}, S_{X_1}, \ldots, S_{X_{n-k-1}})$. Для его реализации необходимо выполнить следующие действия:

– найти одно (любое) из q^k решений выражения $S_X = c_X^* \cdot H_X^T$;

– снять действие матриц маскирования $\{P,D\}_i$ с вектора c_X^*:

$$\begin{aligned} c_X^* \cdot D^{-1} \cdot P^{-1} &= c_X^* \cdot \Lambda^{-1} = \\ = (c_{X_0}^*, c_{X_1}^*, \ldots, c_{X_{n-1}}^*) &\cdot \begin{pmatrix} \lambda'_{0,0} & \lambda'_{0,1} & \ldots & \lambda'_{0,n-1} \\ \lambda'_{1,0} & \lambda'_{1,1} & \ldots & \lambda'_{1,n-1} \\ \ldots & \ldots & \ldots & \ldots \\ \lambda'_{n-1,0} & \lambda'_{n-1,1} & \ldots & \lambda'_{n-1,n-1} \end{pmatrix} = \\ &= (\bar{c}_0^*, \bar{c}_1^*, \ldots, \bar{c}_{n-1}^*), \end{aligned}$$

где $\lambda'_{l,m}$ – элементы матрицы Λ^{-1} – обратной к унипотентной матрице $\Lambda = P \cdot D$;

– декодировать полученную последовательность $(\overline{c}_0^*, \overline{c}_1^*, ..., \overline{c}_{n-1}^*)$ – кодовое слово с ошибками алгебраического (n, k, d) кода C над $GF(q)$, вычисление вектора ошибок $e' = (e'_0, e'_1, ..., e'_{n-1}) = e \cdot D^{-1} \cdot P^{-1}$;

– вычисление вектора $e = e' \cdot P \cdot D$. Найденный вектор ошибок $e = (e_0, e_1, ..., e_{n-1})$ – равновесная информационная посылка.

Выполнение обратного отображения (расшифрования) во многом совпадает с расшифрованием криптограммы в криптосистеме 2-го типа. В тоже время как будет показано ниже, криптосистема 3-го типа обладает существенным преимуществом в относительной скорости передачи. Кроме того, рассмотренная криптосистема позволяет помимо криптографического преобразования информационных сообщений интегрировано решать задачи помехоустойчивого кодирования. Для этого следует использовать, например, методы равновесного кодирования при подготовке вектора $e = (e_0, e_1, ..., e_{n-1})$, выполняющего функции информационной посылки.

Оценим сложность реализации прямого и обратного криптографического преобразования (шифрования и расшифрования) в рассмотренных выше криптосистемах. Введем следующие обозначения: I_K – сложность формирования криптограммы (шифрования); I_{SK} – сложность расшифрования.

Формирование криптограммы для криптосистем 1-го и 2-го типа соответствует вычислению кодового слова замаскированного кода с последующим добавлением случайного вектора ошибок. Если замаскированный код задан порождающей матрицей G, в общем случае в несистематическом виде, то для формирования кодового слова достаточно умножить информационный вектор длины k символов на матрицу G. Сложность реализации этой процедуры составит $k \cdot n$ операций сложения и умножения над конечным полем, т.е. для несистематического способа кодирования имеем:

$$I_K = k \cdot n. \qquad (8)$$

Если замаскированный код задан проверочной матрицей H, в общем случае в несистематическом виде, то для формирования кодового слова необходимо вычислить проверочные символы и поместить их на соответствующие место в кодовом слове. Эта процедура соответствует систематическому правилу кодирования, сложность ее реализации составит $r \cdot n$ операций сложения и умножения над конечным полем, т.е.:

$$I_K = r \cdot n. \qquad (9)$$

Сложность расшифрования определяется сложностью алгебраического алгоритма декодирования алгебраического блокового кода. Для кодов Боуза-Чоудхури-Хоквингема (БЧХ), кодов Рида-Соломона (РС) и их обобщений, альтернантных кодов и их подклассов, локализация ошибок сводится к решению системы линейных уравнений от t неизвестных, где t – исправляющая способность соответствующего кода [8, 9], следовательно, запишем:

$$I_{SK} = t^2. \qquad (10)$$

Для алгеброгеометрических кодов имеем [10]:

$$I_{SK} = t^4. \qquad (11)$$

Сложность реализации прямого и обратного криптографического преобразования в криптосистемах 3-го типа определяются аналогично.

2. Исследование особенностей обмена сообщениями в разработанных криптосистемах

Разработанный математический аппарат быстрых криптографических преобразований основан на использовании свойств замаскированных алгебраических блоковых кодов и в качестве основных операторов использует преобразования помехоустойчивого кодирования. Рассмотрим схему передачи сообщений в несимметричной криптосистеме с использованием алгебраических блоковых кодов.

Схема передачи сообщений в криптосистемах 1-го и 2-го типа представлена на рис. 1. Передача криптограммы предваряется следующими операциями.

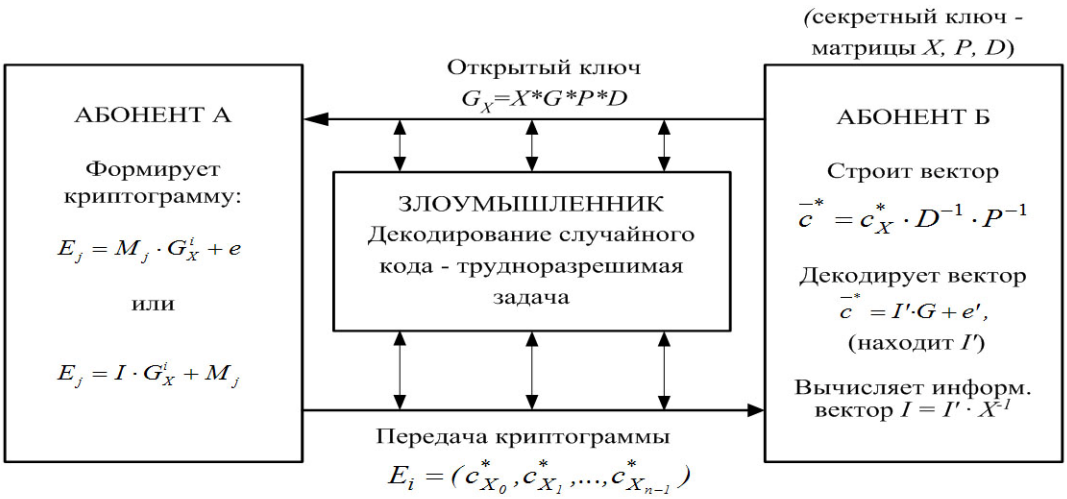

Рис. 1. Схема передачи сообщений в несимметричной криптосистеме 1-го и 2-го типа

Абонент Б случайно, равновероятно, независимо от других абонентов формирует матрицы *X, P, D* и хранит их в секрете (закрытый ключ). Вычисляет матрицу $G_X = X \cdot G \cdot P \cdot D$ и публикует ее как открытый (общедоступный) ключ. Абонент А для отправки секретного сообщения формирует криптограмму. Для криптосистемы 1-го типа криптограмма формируется по выражению (2), для криптосистемы 2-го типа – по выражению (4). Криптограмму может сформировать (зашифровать отправляемую информацию) любой пользователь, знающий публичный (общедоступный) ключ – матрицу G^i_X, (см. выражение (1)). Злоумышленник, не зная секретного ключа абонента Б – набора матриц $\{X,P,D\}_i$, не сможет вскрыть содержимое криптограммы (прочесть информационное сообщение), для него декодирование – трудноразрешимая задача (экспоненциальной сложности). Напротив, абонент Б декодирует криптограмму по алгоритмам полиномиальной сложности.

Схема передачи сообщений в криптосистеме 3-го типа представлена на рис. 2.

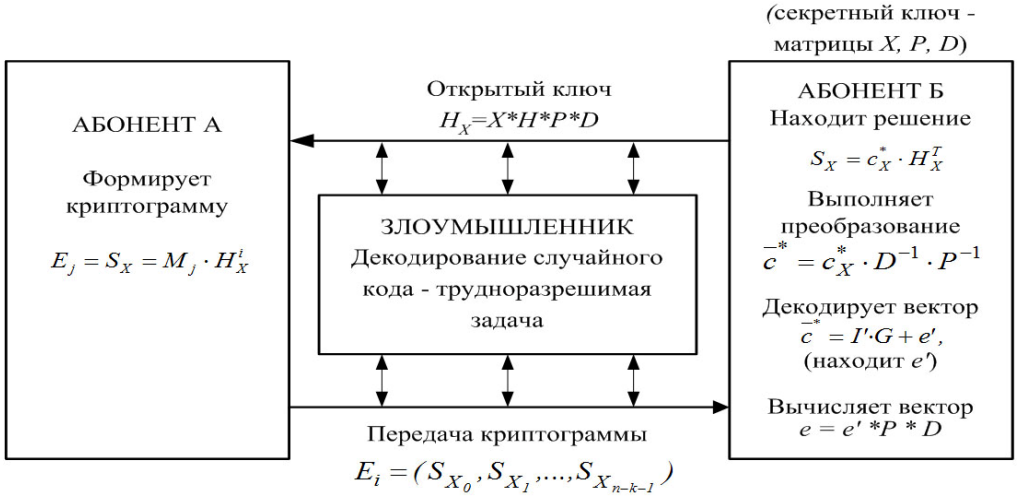

Рис. 2. Схема передачи сообщений в несимметричной криптосистеме 3-го типа

Передача криптограммы в криптосистеме 3-го типа предваряется такиими операциями. Абонент Б случайно, равновероятно, независимо от других абонентов формирует матрицы *X, P, D* и хранит их в секрете (закрытый ключ), вычисляет матрицу $H_X = X \cdot G \cdot H \cdot D$ и публикует ее как открытый (общедоступный) ключ.

Абонент А для отправки секретного сообщения *e* формирует криптограмму $S_X = e \cdot H_X^T$. Ее может

сформировать (зашифровать отправляемую информацию) любой пользователь, знающий публичный (общедоступный) ключ. Злоумышленник, не зная секретного ключа абонента Б, не сможет вскрыть содержимое криптограммы (прочесть информационное сообщение), для него декодирование – трудноразрешимая задача (экспоненциальной сложности). Напротив, абонент Б декодирует криптограмму по алгоритмам полиномиальной сложности. Действительно, уполномоченный пользователь (имеющий секретный ключ) находит одно из q^k решений выражения $S_X = c_X^* \cdot H_X^T$. Найденное решение – суть кодовое слово с ошибками $c_X^* = I \cdot G_X + e$. Далее уполномоченный пользователь строит вектор $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$ и декодирует полученное слово. Однако, вместо восстановления информационного слова I', он вычисляет кодовое слово $c' = I' \cdot G$, а затем и вектор ошибок $e' = \bar{c}^* - c'$. На последнем шаге производится вычисление вектора $e = e' \cdot P \cdot D$, который несет конфиденциальную информацию.

Выводы

Таким образом, разработанный математический аппарат криптографических преобразований с использованием алгебраических блоковых кодов основан на использовании разработанных правил маскировки алгебраических блоковых кодов под случайный код и сведении задачи криптоанализа к теоретико-сложной задаче декодирования случайного кода и позволяет строить быстрые криптографические преобразования доказуемой стойкости. Сложность его реализации растет полиномиально от параметров кода и при соответствующей длине кода n сравним по сложности с блочно-симметричными криптоалгоритмами.

Кроме того, разработанные криптосистемы позволяют интегрировано обеспечивать криптографическое преобразование информации и помехоустойчивое кодирование как в режиме прямого исправления ошибок, так и в режиме обнаружения с автоматическим переспросом.

Литература

1. Саломаа А. Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995. – 318 с.

2. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. – April 19, 2004. – 836 p.

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

4. Rao T.R.N., Nam K.H. Private-key algebraic-coded cryptosystem. Advances in Cryptology – CRYPTO 86, New York. – NY: Springer. – P. 35-48.

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

6. Стасев Ю.В., Кузнецов А.А. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов // Кибернетика и системный анализ: Международный научно-теоретический журнал. – 2005. – № 3. – С. 47-57.

7. Шеннон К. Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – С. 333-402.

8. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

9. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.

10.Кузнецов А.А., Северинов А.В., Задворный Д.А. Лысенко В.Н. Алгебраическое декодирование кодов по кривым Эрмита // Вісник ХПІ. – Х.: НТУ “ХПІ”, 2003. – № 26. – С 95-102.

Поступила в редакцию 5.04.2007

Рецензент: д-р техн. наук, проф. И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков.