А. И. Терентьев (к. т. н., доцент)
Московский государственный технический университет гражданской авиации

МОДИФИЦИРОВАННАЯ КРИПТОСИСТЕМА МАК-ЭЛИСА НА ОСНОВЕ КОРРЕКТИРУЮЩЕГО ЧЛБ-КОДА

В настоящее время хорошо известны и широко применяются на практике асимметричные криптографические системы, основанные на математических задачах, связанных с вычислительной сложностью факторизации больших чисел, а также на логарифмировании в конечных полях и алгебраических структурах, определенных на множестве точек на эллиптических кривых.

Вместе с тем научный поиск новых принципов построения асимметричных криптографических систем представляется достаточно актуальным, несмотря на то что при первом рассмотрении многие гипотетические разработки, в том числе асимметричные криптосистемы, основанные на использовании свойств двоичных корректирующих кодов [1, 2, 6, 7, 10], и криптосистемы, основанные на числовых линейных блоковых корректирующих кодах (ЧЛБ-кодах) [8, 9], обладают рядом существенных недостатков, сдерживающих их практическую реализацию. Однако при определенных условиях, например вследствие дискредитации традиционных криптосистем посредством нахождения более эффективных методов решения математических задач, лежащих в их основе, эти криптосистемы могут представлять практический интерес.

В настоящее время наиболее известными асимметричными криптосистемами, основанными на использовании свойств корректирующих кодов, являются криптосистемы: Мак-Элиса на основе двоичных кодов Гоппы, Нидеррайтера на основе обобщенных кодов Рида—Соломона и Сидельникова на основе кодов Рида—Маллера [1, 2, 6, 7, 10]. В основу работы этих криптосистем положен, главным образом, принцип нарушения систематичности и структуры кодовых комбинаций используемых в них двоичных линейных блоковых корректирующих кодов с целью замаскировать эти коды под линейные коды без определенной структуры.

Попытки построения асимметричных криптосистем на основе двоичных (бинарных) корректирующих (контролирующих ошибки) кодов были обусловлены широкой известностью и изученностью этих кодов. Однако в случае использования для построения корректирующих кодов конечных полей всегда накладывается жесткое ограничение на мощность алфавита, что существенно ограничивает информационные возможности корректирующего кода и предопределяет его свойства, в том числе границы для кодового расстояния. В связи с этим, несмотря на доминирующее распространение двоичных кодов, продолжает развиваться научный поиск новых классов корректирующих кодов над бесконечными множествами элементов, которым будут присущи новые свойства и соответственно новые информационные возможности. К таким кодам относятся числовые линейные блоковые корректирующие коды над кольцом конечных десятичных дробей [9], являющиеся самым сильным обобщением всех известных корректирующих кодов по основанию системы счисления.

Учитывая изложенное, изучение асимметричных криптосистем, основанных на ЧЛБ-кодах, представляет определенный научный и практический интерес.

Рассмотрим метод модификации (обобщения) криптосистемы Мак-Элиса на случай использования корректирующего G2 ЧЛБ (n, k)-кода [8, 9].

Для построения модифицированной криптосистемы Мак-Элиса необходимо выбрать удовлетворяющий предварительно заданным требованиям криптостойкости системы G2 ЧЛБ (n, k)-код, исправляющий υ ошибок, для которого известен эффективный алгоритм декодирования.

Пусть G — порождающая матрица такого ЧЛБ-кода размерности $k \times n$ (т. е. $G_{k \times n}$). Для формирования открытого и закрытого ключей криптосистемы необходимо выполнить следующую последовательность действий:

1. Случайно выбрать числовую невырожденную матрицу S размерности $k \times k$ (т. е. $S_{k \times k}$).

2. Случайно выбрать матрицу перестановок P размерности $n \times n$ ($P_{n \times n}$).

3. Вычислить произведение матриц

$G_{E\ k \times n} = S_{k \times k}\ G_{k \times n}\ P_{n \times n}$.

Открытым ключом, по которому выполняется зашифрование, является пара (G_E, t).

Закрытым (секретным) ключом, по которому будет выполняться расшифрование, является тройка (S, G, P).

Для зашифрования сообщения M его необходимо представить в виде числового вектора m длины k и выбрать случайным образом вектор ошибок e длины n, содержащий не более t ненулевых элементов (чисел).

Криптограмма вычисляется как числовой вектор

$x = m\ G_E + e$.

Для расшифрования криптограммы x необходимо выполнить следующие действия:

1. Вычислить вектор

$x_1 = x\ P^{-1}$.

2. Используя алгоритм декодирования для выбранного ЧЛБ (n, k)-кода с порождающей матрицей G, получить вектор m_1 длины k.

3. Вычислить исходное сообщение

$m = m_1 S^{-1}$,

где S^{-1} — матрица, обратная к матрице S.

Таким образом, получен открытый текст M, представленный в виде числового вектора m длины k.

Обобщенная схема описанной модифицированной асимметричной криптосистемы Мак-Элиса на основе корректирующего ЧЛБ-кода представлена на рис. 1.

В целях обеспечения наглядности при иллюстрации основных этапов шифрования в асимметричной модифицированной криптосистеме Мак-Элиса, обобщенной на случай использования корректирующего G2 ЧЛБ (n, k)-кода, выберем короткий корректирующий G2 ЧЛБ (7, 4)-код с минимальным расстоянием Хэмминга $d = 3$, для которого далее приведем конкретные примеры всех этапов шифрования.

Пусть G2 ЧЛБ (7, 4)-код задан порождающей матрицей G [8, 9]:

$$G = \begin{pmatrix} 1\,0\,0\,0\,1\,1\,0 \\ 0\,1\,0\,0\,1\,0\,1 \\ 0\,0\,1\,0\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1 \end{pmatrix}.$$

Для формирования открытого и закрытого (секретного) ключей шифрования необходимо выполнить следующие действия.

Случайным образом выберем невырожденную матрицу S размерности $k \times k$ (т. е. $S_{k \times k}$):

$$S_{k \times k} = \begin{pmatrix} 5 & 7 & 6 & 5 \\ 7 & 10 & 8 & 7 \\ 6 & 8 & 10 & 9 \\ 5 & 7 & 9 & 10 \end{pmatrix},$$

имеющую обратную матрицу

$$S^{-1}{}_{k \times k} = \begin{pmatrix} 68 & -41 & -17 & 10 \\ -41 & 25 & 10 & -6 \\ -17 & 10 & 5 & -3 \\ 10 & -6 & -3 & 2 \end{pmatrix}.$$

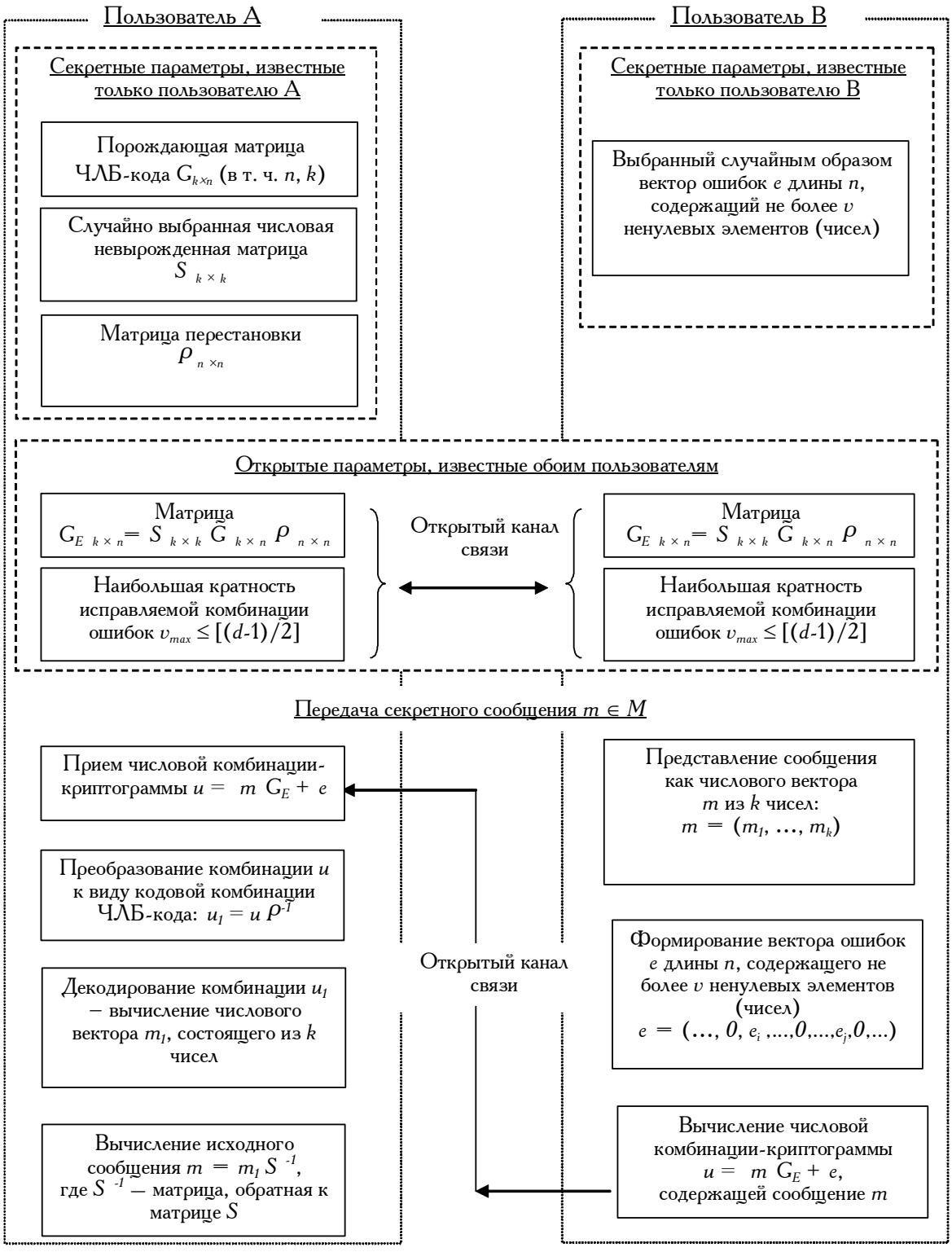

Рис. 1. Схема модифицированной асимметричной криптосистемы Мак-Элиса

Случайным образом выберем матрицу перестановок P размерности $n \times n$ (т. е. $P_{n \times n}$). Например:

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Соответственно, матрица обратной перестановки будет иметь вид:

$$P^{-1} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Вычислим произведение матриц $G_{E\ k \times n} = S_{k \times k}\, G_{k \times n}\, P_{n \times n}$.

$$G_{E\ k \times n} = \begin{pmatrix} 6 & 5 & 17 & 7 & 18 & 5 & 16 \\ 8 & 7 & 24 & 10 & 25 & 7 & 22 \\ 10 & 6 & 23 & 8 & 27 & 9 & 25 \\ 9 & 5 & 22 & 7 & 26 & 10 & 24 \end{pmatrix}.$$

Открытым ключом, по которому выполняется зашифрование, является пара (G_E, υ), где $\upsilon = 1$ для $G2$ ЧЛБ (7,4)-кода с $d = 3$.

Закрытым (секретным) ключом, по которому будет выполняться расшифрование, является тройка (S, G, P).

Для зашифрования сообщение M необходимо в виде числового вектора m длины k. Например:

$m = (2, 7, 4, 1)$.

Затем выбрать случайным образом числовой вектор ошибок e длины n, содержащий не более υ ненулевых элементов. Например,

$e = (0, 0, 0, 12, 0, 0, 0)$.

Криптограмма вычисляется как числовой вектор $u = m\ G_E + e$:

$u = (117, 88, 316, 123, 345, 105, 310) + (0, 0, 0, 12, 0, 0, 0) = (117, 88, 316, 135, 345, 105, 310)$.

Для расшифрования криптограммы u необходимо вычислить вектор

$u_1 = u\ P^{-1} = (88, 135, 117, 105, 316, 310, 345)$.

Затем, используя алгоритм декодирования для выбранного $G2$ ЧЛБ (7,4)-кода с порождающей матрицей G и соответственно формирующими суммами числового синдрома $s_ч$:

$s_{ч1} = \hat{a}_1 + \hat{a}_2 + \hat{a}_4 - \hat{b}_1$
$s_{ч2} = \hat{a}_1 + \hat{a}_3 + \hat{a}_4 - \hat{b}_2$
$s_{ч3} = \hat{a}_2 + \hat{a}_3 + \hat{a}_4 - \hat{b}_3$,

где $\hat{a}_1, \hat{a}_2, \hat{a}_3, \hat{a}_4, \hat{b}_1, \hat{b}_2, \hat{b}_3$ — элементы (числа) искаженной кодовой комбинации u_1, необходимо вычислить вектор m_1.

Для вектора $u_1 = u\ P^{-1} = (88, 135, 117, 105, 316, 310, 345)$ числовой и характеристический синдромы будут иметь вид:

$s_ч = (12, 0, 12)$ и $s_x = (1, 0, 1)$.

Таблица характеристических синдромов [8, 9] одиночных ошибок для выбранного $G2$ ЧЛБ (7,4)-кода имеет вид:

Искаж. число	Характеристический синдром		
	s_1	s_2	s_3
a_1	1	1	0
a_2	1	0	1
a_3	0	1	1
a_4	1	1	1
b_1	1	0	0
b_2	0	1	0
b_3	0	0	1

Согласно указанной таблице, искаженным является второй элемент вектора u_1, т. е. число 135. Абсолютная величина искажения равна 12. Таким образом, в результате декодирования получен вектор $m_1 = (88, 123, 117, 105)$.

Исходное сообщение m вычисляется следующим образом:

$m = m_1 S^{-1} = (2, 7, 4, 1)$, где S^{-1} — матрица, обратная к матрице S.

Таким образом, получен открытый текст M, представленный в виде числового вектора $m = (2, 7, 4, 1)$ длины k .

В заключение следует отметить, что асимметричные криптосистемы на основе двоичных корректирующих кодов не получили практического применения из-за большой длины открытого ключа зашифрования и значительной избыточности криптограммы (в 1,5 — 2,0 раза) по сравнению с исходным открытым текстом. Указанный недостаток не так очевиден в случае построения асимметричных криптосистем на основе ЧЛБ-кодов, поскольку при одинаковой корректирующей способности, особенно при использовании ЧЛБ-кодов с большим количеством информационных символов, они имеют существенно меньшую избыточность по сравнению со всеми известными корректирующими кодами с символами (элементами) из конечного алфавита.

СПИСОК ЛИТЕРАТУРЫ:

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии: Учебное пособие. М., 2001. — 480 с., илл.
2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М., 2002. — 816 с., илл.
3. *Иванов М. А.* Криптографические методы защиты информации в компьютерных системах и сетях. М., 2001. — 368 с.
4. *Молдовян А. А., Молдовян Н. А., Советов Б. Я.* Криптография. СПб., 2001. — 224 с., илл.
5. *Петров А. А.* Компьютерная безопасность. Криптографические методы защиты. М., 2000. — 448 с., илл.
6. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида—Маллера // Дискретная математика. 1994. Т. VI. № 2. С. 3—20.
7. *Сидельников В. М., Шестаков С. О.* О системе шифрования, построенной на основе обобщенных кодов Рида—Соломона // Дискретная математика. 1992. Т. IV. № 3. С. 57—63.
8. *Терентьев А. И.* Асимметричная криптографическая система на основе корректирующего ЧЛБ-кода с закрытой порождающей матрицей // Научный вестник МГТУ ГА. Сер. Информатика. Прикладная математика. 2002. № 55.
9. *Терентьев А. И.* Элементы теории и практики числовых линейных блоковых корректирующих кодов. М., 2000. — 204 с., илл.
10. *Чмора А. Л.* Современная прикладная криптография. М., 2001. — 256 с., илл.