 Научная статья

DOI: 10.18287/2541-7525-2021-27-1-62-73

УДК 519.7

Дата: поступления статьи: 11.12.2020
после рецензирования: 20.01.2021
принятия статьи: 28.02.2021

С.М. Рацеев
Ульяновский государственный университет,
г. Ульяновск, Российская Федерация
E-mail: ratseevsm@mail.ru. ORCID: https://orcid.org/0000-0003-4995-9418
О.И. Череватенко
Ульяновский государственный педагогический университет
имени И.Н. Ульянова, г. Ульяновск, Российская Федерация
E-mail: choi2008@mail.ru. ORCID: https://orcid.org/0000-0003-3931-9425
В.А. Чернявская
Ульяновский государственный педагогический университет
имени И.Н. Ульянова, г. Ульяновск, Российская Федерация
E-mail: vera.chernya@yandex.ru. ORCID: https://orcid.org/0000-0001-9875-2232

О НЕКОТОРЫХ КРИПТОСИСТЕМАХ, ОСНОВАННЫХ НА АЛГЕБРАИЧЕСКИХ КОДАХ

АННОТАЦИЯ

В 1978 г. Мак-Элис построил первую кодовую криптосистему с открытым ключом, которая основана на применении помехоустойчивых кодов. При этом эффективные атаки на секретные ключи этой криптосистемы до сих пор не найдены. В работе приводятся описания классической и модернизированной криптосистем Мак-Элиса и Нидеррайтера, а также примеры их практического применения на основе кодов Гоппы с использованием алгоритма Паттерсона. Также приводятся алгоритмы двухшаговых протоколов аутентификации с нулевым разглашением на основе кодовых криптосистем.

Ключевые слова: криптосистема Мак-Элиса; помехоустойчивые коды; коды Гоппы; декодирование кода.

Цитирование. Рацеев С.М., Череватенко О.И., Чернявская В.А. О некоторых криптосистемах, основанных на алгебраических кодах // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 27, № 1. С. 62–73. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-62-73.

Информация о конфликте интересов: авторы и рецензенты заявляют об отсутствии конфликта интересов.

Сергей Михайлович Рацеев — доктор физико-математических наук, доцент, профессор кафедры информационной безопасности и теории управления, Ульяновский государственный университет, 432017, Российская Федерация, г. Ульяновск, ул. Льва Толстого, 42.

Ольга Ивановна Череватенко — кандидат физико-математических наук, доцент, доцент кафедры высшей математики, Ульяновский государственный педагогический университет имени И.Н. Ульянова, 432071, Российская Федерация, г. Ульяновск, пл. Ленина, 4/5.

Вера Алексеевна Чернявская — студент кафедры информационной безопасности и теории управления, Ульяновский государственный университет, 432017, Российская Федерация, г. Ульяновск, ул. Льва Толстого, 42.

Введение

В 1978 г. Мак-Элисом предложена первая криптосистема, основанная на алгебраических блоковых кодах [1]. В ее основе лежит маскировка быстрого алгоритма декодирования посредством умножения исходной порождающей матрицы G на случайную невырожденную матрицу, которая, в частности, является секретным ключом криптосистемы. Полученный результат (открытый ключ) представляет собой порождающую матрицу, имеющую вид случайно выбранных линейно независимых векторов. Злоумышленник, имеющий только открытый ключ, вынужден использовать сложный алгоритм неалгебраического декодирования (NP-полная задача). Законный пользователь, знающий секретный ключ, снимает действие маскировки и применяет быстрый алгебраический алгоритм декодирования (полиномиально разрешимая задача). Данная криптосистема на данный момент остается криптостойкой, так как нет ни одного эффективного алгоритма нахождения секретного ключа. Более того, данная криптосистема является одним из претендентов на официальную постквантовую криптосистему [2].

Криптосистема Мак-Элиса при использовании кодов Гоппы считается криптостойкой. Для декодирования кодов Гоппы хорошо известен алгоритм Паттерсона [3]. Но он применим только для двоичных кодов Гоппы. При этом заметим, что любой алгоритм декодирования обобщенных кодов Рида — Соломона можно применить и для кодов Гоппы над любым полем. Для обобщенных кодов Рида — Соломона и кодов Гоппы подобные алгоритмы рассматривались в работах [4–7].

1. Криптосистема Мак-Элиса

Классическая криптосистема. Пусть G — порождающая матрица $[n, k, d]$-кода над $GF(q)$, исправляющего t и менее ошибок (в оригинальной статье предлагается использовать двоичные сепарабельные коды Гоппы), C — невырожденная матрица порядка k над полем $GF(q)$, P и D — перестановочная и диагональная матрицы порядка n соответственно (для двоичных кодов матрица D не используется).

Матрица $\widetilde{G} = C \cdot G \cdot P \cdot D$ является открытым ключом абонента A, как и параметры n, k, t. Маскирующие матрицы C, P, D и порождающая матрица G являются секретным ключом абонента A. В силу того, что матрицы C, P, D невырождены, матрица $\widetilde{G}$ является порождающей матрицей эквивалентного кода. Предположим, что абонент B хочет передать абоненту A сообщение x длины k с компонентами из $GF(q)$. Алгоритм шифрования, предложенный Мак-Элисом, выглядит следующим образом.

1. Случайным равновероятным образом генерируется вектор ошибок e длины n над $GF(q)$ веса не более t.
2. Абонент B вычисляет шифрованное сообщение $y = x\widetilde{G} + e$, которое по открытому каналу связи передает абоненту A.

Вектор ошибок e, генерируемый на первом шаге, является случайным параметром шифра, который значительно усложняет криптоанализ. При $wt(e) = t$ сложность дешифрования будет максимальной. Также заметим, что при каждом таком шифровании вектор e должен генерироваться заново. Для расшифрования сообщения абонент A совершает следующие действия.

1. Умножение полученного вектора на матрицу $(PD)^{-1}$: $\widetilde{y} = yD^{-1}P^{-1}$. При этом $\widetilde{y} = yD^{-1}P^{-1} = xCG + \widetilde{e} = \widetilde{x}G + \widetilde{e}$, где $\widetilde{x} = xC$, $wt(\widetilde{e}) = wt(e)$.
2. Декодирование вектора $\widetilde{x}$ на основе вектора $\widetilde{y}$, т. е. получение вектора $\widetilde{x} = xC$.
3. Нахождение исходного сообщения x путем умножения вектора $\widetilde{x}$ на C^{-1}: $x = \widetilde{x}C^{-1}$.

Замечание 1. Пусть G и H — порождающая и проверочная матрицы некоторого линейного кода, C и D — невырожденные квадратные матрицы подходящих размеров (для вычисления CG, DH). Порождающие матрицы CG и G задают один и тот же линейный код, так как $GH^T = O$, тогда и только тогда, когда $CGH^T = O$. Аналогично проверочные матрицы H и DH задают один и тот же линейный код. Это значит, что для декодирования вектора $\widetilde{x}$ на втором шаге приведенного выше алгоритма применяется проверочная матрица H (если она необходима), соответствующая матрице G.

Модернизированная криптосистема. Для того чтобы уменьшить объем параметров криптосистемы Мак-Элиса, имеется модернизированная версия данной криптосистемы [8], которая использует порождающую матрицу G в канонической форме: $G = (I_k, Q_{k\times(n-k)})$. В этом случае вместо хранения $k \times n$ элементов достаточно хранить только матрицу Q размера $k \times (n - k)$. Более того, для

алгоритмов кодирования и декодирования требуется меньшее число операций. Также вместо матриц C, P, D в качестве секретного ключа хранится только перестановка элементов множества L и многочлен $G(x)$ кода $\Gamma(L, G)$.

Как утверждается в работе [8], криптостойкость модернизированной версии эквивалентна криптостойкости классической версии криптосистемы Мак-Элиса. Итак, сначала вычисляется открытый ключ G криптосистемы на основе параметров q, m, n, r.

1. Случайным образом генерируется многочлен $G(x)$ степени r над полем $GF(q^m)$ (например, можно сгенерировать неприводимый многочлен).

2. Случайным образом выбираются n элементов поля $GF(q^m)$, не являющиеся корнями многочлена $G(x)$, которые определяют множество L. Если $G(x)$ неприводим, то можно взять любые различные n элементов поля $GF(q^m)$.

3. Вычисляется проверочная матрица H' над полем $GF(q^m)$ размера $r \times n$ на основе L и $G(x)$, $r = \deg G(x)$.

4. С помощью элементарных преобразований строк матрица H' приводится к систематическому виду CH' (некоторые столбцы такой матрицы образуют единичную матрицу, а невырожденная матрица C является произведением соответствующих матриц элементарных преобразований), а затем с помощью перестановки столбцов приводится к виду $H = (Q^T_{(n-k)\times k}, I_{n-k})$, т. е. матрица CH' справа умножается на перестановочную матрицу P: $H = CH'P$. К множеству L применяется такая же перестановка (обозначение L оставим прежним).

5. На основе матрицы H вычисляется порождающая матрица G в канонической форме: $G = (I_k, Q_{k\times(n-k)})$.

В итоге матрица G является открытым ключом криптосистемы. Как видно из алгоритма, для получения H требуется некоторая невырожденная матрица C и перестановочная матрица P. Заметим, что если $n = q^m$, то $L = GF(q^m)$. Также в качестве $G(x)$ чаще всего выбирают неприводимый многочлен над $GF(q^m)$. Множество L для данной криптосистемы является случайным и держится в секрете. Алгоритм шифрования в модернизированной версии не отличатся от классической, разве что на него требуется меньшее число операций. Для того чтобы абоненту B передать абоненту A сообщение x длины k с компонентами из $GF(q)$, требуется выполнить следующие шаги.

1. Абонент B случайным равновероятным образом генерирует вектор ошибок e длины n над $GF(q)$ веса не более t.

2. Абонент B получает шифрованное сообщение $y = xG + e = x(I, Q) + e = (x, xQ) + e$, которое по открытому каналу связи передает абоненту A.

Для расшифрования сообщения абонент A совершает следующие действия.

1. По вектору y вычисляется синдромный вектор S (синдромный многочлен $S(x)$).

2. С помощью алгоритма декодирования полиномиальной сложности находится вектор e веса не более t, который имеет синдром S.

3. После этого вычисляется кодовый вектор $u = y - e$, из которого извлекается сообщение x (из первых k позиций вектора u).

Есть несколько оснований для использования кодов Гоппы в криптосистеме Мак-Элиса: 1) существуют быстрые алгоритмы полиномиальной сложности декодирования кодов Гоппы; 2) код Гоппы легко генерировать, но очень сложно обнаружить «замаскированный» код Гоппы; 3) код Гоппы можно построить с помощью любого неприводимого многочлена над $GF(2^m)$, при этом порождающая матрица кода будет иметь «почти случайный» вид.

Заметим, что для любой фиксированной длины n существует «очень много» различных кодов Гоппы. Пусть $N(q, s, r)$ — число неэквивалентных неприводимых кодов Гоппы над полем $GF(q)$ длины q^s и степени r многочлена $G(x)$. Точной формулы для $N(q, s, r)$ пока неизвестно. В работе [9] приводятся верхние границы для $N(q, s, r)$, которые являются точными для некоторых небольших значений параметров. Например, число двоичных неприводимых кодов Гоппы длины $n = 128$ и степенью неприводимого многочлена $r = 10$ оценивается сверху числом $N(2, 7, 10) = 1037499670492467 > 10^{15}$. А для числа $N(2, 7, 15)$ (т. е. для кодов той же длины 128 с неприводимым многочленом $G(x)$ степени 15) уже выполнено равенство $N(2, 7, 15) = 2376547806952061120164378 1 > 2 \cdot 10^{25}$. Если увеличить длину

кодов до $n = 4096$ (чтобы обеспечивался должный уровень криптостойкости системы Мак-Элиса), то для данной границы уже при $r = 7$ получаем $N(2, 12, 7) = 13728607731106143 > 10^{16}$.

Заметим, что криптосистема Мак-Элиса требует очень большого объема памяти для своих параметров. Для примера, чтобы добиться 80-битной криптостойкости, для алгоритма RSA необходим 1024-битный ключ, при этом для криптосистемы Мак-Элиса требуется ключ размера не менее 450 кбит для достижения той же степени криптостойкости.

Пример 1 (классическая криптосистема Мак-Элиса). Рассмотрим расширение поля $GF(2) \subset GF(2^4)$. Пусть поле $GF(2^4)$ строится на основе примитивного многочлена $p(x) = x^4 + x + 1$, α — примитивный элемент поля $GF(2^4)$:

$$\begin{array}{llllllllllllll}
\alpha^0 = & 1 & & & & = & 1000, & \alpha^1 = & & \alpha & & & = & 0100,\\
\alpha^2 = & & & \alpha^2 & & = & 0010, & \alpha^3 = & & & & \alpha^3 & = & 0001,\\
\alpha^4 = & 1 & +\alpha & & & = & 1100, & \alpha^5 = & & \alpha & +\alpha^2 & & = & 0110,\\
\alpha^6 = & & & \alpha^2 & +\alpha^3 & = & 0011, & \alpha^7 = & 1 & +\alpha & & +\alpha^3 & = & 1101,\\
\alpha^8 = & 1 & & +\alpha^2 & & = & 1010, & \alpha^9 = & & \alpha & & +\alpha^3 & = & 0101,\\
\alpha^{10} = & 1 & +\alpha & +\alpha^2 & & = & 1110, & \alpha^{11} = & & \alpha & +\alpha^2 & +\alpha^3 & = & 0111,\\
\alpha^{12} = & 1 & +\alpha & +\alpha^2 & +\alpha^3 & = & 1111, & \alpha^{13} = & 1 & & +\alpha^2 & +\alpha^3 & = & 1011,\\
\alpha^{14} = & 1 & & & +\alpha^3 & = & 1001, & \alpha^{15} = & 1 & & & & = & 1000.
\end{array}$$

Пусть $L = GF(2^4) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$, $G(x) = x^2 + x + \alpha^3$. Так как след элемента α^3 в поле $GF(2^4)$ не равен нулю, то многочлен $G(x)$ в этом поле не имеет корней. Поэтому из неприводимости $G(x)$ над $GF(2^4)$ следует, что код $\Gamma(L, G)$ является сепарабельным, т. е. он исправляет до двух ошибок. Проверочная матрица H кода $\Gamma(L, G)$ примет такой вид:

$$H = \begin{pmatrix} G(0)^{-1} & G(1)^{-1} & G(\alpha)^{-1} & \ldots & G(\alpha^{14})^{-1} \\ 0G(0)^{-1} & 1G(1)^{-1} & \alpha G(\alpha)^{-1} & \ldots & \alpha^{14}G(\alpha^{14})^{-1} \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^{12} & \alpha^{12} & \alpha^4 & \alpha^3 & \alpha^9 & \alpha^4 & \alpha & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^6 & \alpha & \alpha^2 & \alpha^2 & \alpha^8 & \alpha^9 \\ 0 & \alpha^{12} & \alpha^5 & \alpha^5 & \alpha^{12} & \alpha^8 & \alpha^6 & \alpha^{14} & \alpha^{13} & \alpha^{11} & 1 & \alpha^{11} & \alpha^{13} & \alpha^{14} & \alpha^6 & \alpha^8 \end{pmatrix} =$$

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

Так как все строки матрицы H линейно независимы, то $n - k = 8$, $k = 8$. Выписав построчно фундаментальную систему решений системы однородных линейных уравнений $HX = O$, находим порождающую матрицу кода $\Gamma(L, G)$:

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

Абонент A генерирует невырожденную матрицу C и перестановочную матрицу P:

$$C = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}, \quad C^{-1} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$P = \begin{pmatrix} e_{\sigma(0)} \\ e_{\sigma(1)} \\ \dots \\ e_{\sigma(15)} \end{pmatrix} = \begin{pmatrix} 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \end{pmatrix},$$

$$\sigma = \begin{pmatrix} 0&1&2&3&4&5&6&7&8&9&10&11&12&13&14&15 \\ 4&10&13&9&0&7&15&3&14&11&5&1&8&2&12&6 \end{pmatrix},$$

где σ — подстановка на множестве $\{0, 1, \dots, 15\}$ (строки и столбцы нумеруем с нуля). После этого абонент A вычисляет матрицу:

$$\widetilde{G} = CGP = \begin{pmatrix} 0&0&0&1&1&0&1&0&0&1&1&1&0&1&1&0 \\ 0&0&0&0&1&0&1&0&0&1&1&0&0&0&0&1 \\ 0&0&1&0&1&0&0&0&0&0&1&0&1&1&0&1 \\ 0&0&0&1&0&1&0&1&1&0&1&1&1&0&1&0 \\ 1&0&0&1&0&1&1&0&1&1&0&1&0&1&1&1 \\ 0&1&1&0&0&0&1&1&0&1&1&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0&1&0&0&0&1&0&1&1 \\ 1&1&1&0&1&0&0&1&0&1&0&0&1&1&1&1 \end{pmatrix}.$$

Параметры $n = 16,\ k = 8,\ t = 2$ и матрица $\widetilde{G}$ являются открытым ключом абонента A.

Предположим, что абонент B хочет передать абоненту A сообщение $x = (0, 1, 1, 1, 0, 0, 1, 1)$, которое нужно предварительно зашифровать на открытом ключе абонента A. Абонент B генерирует вектор ошибок веса два и вычисляет:

$$y = x\widetilde{G} + (0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0) =$$

$$= (1,1,0,0,0,1,1,1,0,0,1,1,0,0,1,0).$$

Сообщение y передается абоненту A по открытому каналу связи. Для расшифрования сообщения y абонент A проделывает следующие действия. Сначала вектор y умножается на $P^{-1} = P^T$:

$$\widetilde{y} = yP^{-1} = (0,1,0,0,1,1,0,0,1,1,1,1,0,0,0,1),$$

т. е. элементы в векторе y переставляются в соответствии с перестановкой σ. Для декодирования $\widetilde{y}$ применим алгоритм Паттерсона (см. [3; 4]). По вектору $\widetilde{y}$ вычисляется синдромный многочлен

$$S(x) \equiv \sum_{i=0}^{15} \frac{\widetilde{y}_i}{x - \alpha_i} \equiv \frac{1}{x-1} + \frac{1}{x-\alpha^3} + \frac{1}{x-\alpha^4} + \frac{1}{x-\alpha^7} +$$

$$+ \frac{1}{x-\alpha^8} + \frac{1}{x-\alpha^9} + \frac{1}{x-\alpha^{10}} + \frac{1}{x-\alpha^{14}} \equiv \alpha^9 + \alpha^5 x \pmod{G(x)}.$$

Вычисляется $T(x) \equiv (\alpha^9 + \alpha^5 x)^{-1} \equiv 1 + \alpha^{14} x \pmod{G(x)}$.

Учитывая, что $s(x) \equiv \sqrt{x} \equiv \alpha^9 + x \pmod{G(x)}$, вычисляется $p(x)$:

$$p(x) \equiv \sqrt{T(x) + x} \equiv \sqrt{1 + \alpha^3 x} \equiv$$

$$\equiv (1)^8 + (\alpha^3)^8(\alpha^9 + x) \equiv \alpha^{14} + \alpha^9 x \pmod{G(x)}.$$

Полагается $r = \deg G(x) = 2,\ r_{-1}(x) = G(x),\ r_0(x) = p(x),\ v_{-1}(x) = 0,\ v_0(x) = 1$. При $j = 0$ выполнено:

$$\deg r_{-1}(x) = 2 > \frac{r}{2}, \quad \deg r_0(x) = \frac{r}{2},$$

поэтому с точностью до константы $\sigma(x) = r_0^2(x) + x v_0(x) = \alpha^{13} + x + \alpha^3 x^2$.

Корнями многочлена $\sigma(x)$ являются $X_1 = \alpha^4 = \alpha_5$, $X_2 = \alpha^6 = \alpha_7$, поэтому ошибки в векторе $\widetilde{y}$ содержатся на 5-й и 7-й позициях. После исправления двух ошибок в векторе $\widetilde{y}$ новый вектор примет вид

$$\overline{y} = (0,1,0,0,1,0,0,1,1,1,1,1,0,0,0,1) = xCG = \widetilde{x}G.$$

Так как столбцы матрицы G с номерами 7, 9–15 (нумеруя с нуля) образуют единичную матрицу, то из вектора $\overline{y}$ извлекаем вектор $\widetilde{x} = (1,1,1,1,0,0,0,1)$. Осталось вычислить:

$$x = \widetilde{x}C^{-1} = (0,1,1,1,0,0,1,1).$$

2. Криптосистема Нидеррайтера

Другим важным примером кодовых криптосистем является схема Нидеррайтера [10]. Открытым ключом в этой криптосистеме являются параметры n, k, t и матрица $\widetilde{H} = CHPD$, где H — проверочная матрица алгебраического $[n,k,d]$-кода над $GF(q)$ (в оригинальной статье предлагалось использовать обобщенные коды Рида — Соломона, но такой вариант взломан), C — невырожденная матрица порядка $n-k$ над полем $GF(q)$, P и D — перестановочная и диагональная матрицы порядка n соответственно (для двоичных кодов матрица D не используется). Маскирующие матрицы C, P, D и проверочная матрица H являются секретным ключом абонента A.

Предположим, что абонент B хочет передать абоненту A сообщение e длины n над $GF(q)$ веса не более t, т. е. сообщения в этом случае не являются кодовыми словами, а представляют собой всевозможные векторы ошибок, которые этот код в состоянии исправлять (как помещать открытые тесты в векторы-ошибок см., напр., [11]). Шифрованное сообщение длины $n-k$ получается следующим образом: $y = e\widetilde{H}^T$.

При этом наибольшая стойкость будет при $wt(e) = t$. Для расшифрования сообщения абонент A совершает следующие действия.

1. Абонент A умножает полученный вектор на $(C^T)^{-1}$:

$$S = y(C^T)^{-1} = eDP^T H^T C^T (C^T)^{-1} = eDP^T H^T = \widetilde{e}H^T,$$

где $\widetilde{e} = eDP^T$, $wt(\widetilde{e}) = wt(e)$.

2. В смежном классе с синдромом S теперь с помощью алгоритма декодирования вычисляется вектор ошибок $\widetilde{e}$ (здесь можно применить любой алгоритм декодирования, который по синдромному вектору находит вектор ошибок: алгоритм Сугиямы, Берлекэмпа — Месси и т. д.).

3. Нахождение исходного сообщения e путем умножения вектора $\widetilde{e}$ на PD^{-1}: $e = \widetilde{e}PD^{-1}$.

Заметим, что на втором шаге алгоритма расшифрования вычисляется вектор ошибок по синдромному вектору, а не по искаженному вектору.

Приведем также модификацию алгоритма расшифрования сообщения $y = e\widetilde{H}^T$.

1. Умножение полученного вектора y на $(C^T)^{-1}$:

$$S = y(C^T)^{-1} = eDP^T H^T = \widetilde{e}H^T,$$

где $\widetilde{e} = eDP^T$, $wt(\widetilde{e}) = wt(e)$.

2. Нахождение какого-либо вектора $\widetilde{x}$, который является решением относительно x уравнения $S = xH^T$ (т. е. $\widetilde{e}$ и $\widetilde{x}$ имеют одинаковые синдромы и поэтому принадлежат одному смежному классу, причем $u = \widetilde{x} - \widetilde{e}$ — кодовое слово, поэтому $\widetilde{x} = u + \widetilde{e}$. Следовательно, $\widetilde{x}$ является вектором вида $\widetilde{x} = iG + \widetilde{e}$ для некоторого неизвестного информационного вектора i).

3. Нахождение вектора ошибок $\widetilde{e}$ с помощью алгоритма декодирования, примененного для вектора $\widetilde{x}$.

4. Нахождение исходного сообщения e путем умножения вектора $\widetilde{e}$ на PD^{-1}: $e = \widetilde{e}PD^{-1}$.

Заметим, что $S = xH^T$ — синдромный вектор и что $\widetilde{e}$ является одним из решений уравнения $S = xH^T$ относительно x. Нахождение какого-либо решения этого уравнения является простой задачей, так как это система из $n-k$ линейных уравнений с n неизвестными. Но нахождение из всех решений вектора минимального веса является очень сложной задачей.

Если использовать коды Гоппы, то многочлен $G(x)$ может выступать дополнительным секретным параметром.

Теорема 1 ([12]). Пусть H — двоичная матрица размера $(n-k)\times n$, $S = eH^T$ — ненулевой синдромный вектор, $wt(e) \leqslant t$. Тогда нахождение двоичного вектора e веса не более t с синдромом S является NP-полной задачей.

В работе [13] показано, что стойкости криптосистем Мак-Элиса и Нидеррайтера эквивалентны, поэтому любую эффективную атаку на одну из схем можно легко преобразовать в атаку на другую схему.

Для криптосистемы Нидеррайтера также имеется модернизированный вариант (с использованием кодов $\Gamma(L,G)$) для уменьшения объема хранимой информации. Алгоритм выработки открытого ключа H для модернизированной криптосистемы имеет следующий вид.

1. Случайным образом генерируется многочлен $G(x)$ степени r над полем $GF(q^m)$ (например, можно сгенерировать неприводимый многочлен).
2. Случайным образом выбираются n элементов поля $GF(q^m)$, не являющиеся корнями многочлена $G(x)$, которые определяют множество L. Если $G(x)$ неприводим, то можно взять любые различные n элементов поля $GF(q^m)$.
3. Вычисляется проверочная матрица H' размера $r\times n$ на основе L и $G(x)$.
4. С помощью элементарных преобразований строк и перестановки столбцов матрица H' приводится к каноническому виду $H = CH'P = (Q^T_{(n-k)\times k}, I_{n-k})$. L также умножается на P справа.
5. На основе матрицы H вычисляется порождающая матрица G в канонической форме: $G = (I_k, Q_{k\times(n-k)})$.

Шифрование сообщения в модернизированной криптосистеме совпадает с классической версией $y = eH^T$, разве что необходимо выполнить меньшее число операций. Для расшифрования сообщения необходимо выполнить следующие действия.

1. Вычисляется $S = y(C^T)^{-1} = eP^TH'^T = \widetilde{e}H'^T$, где $\widetilde{e} = eP^T$, $wt(\widetilde{e}) = wt(e)$.
2. С помощью алгоритма декодирования по синдромному вектору S находится вектор $\widetilde{e}$, после чего вычисляется $e = \widetilde{e}P$.

Пример 2 (классическая криптосистема Нидеррайтера). Рассмотрим, как и в примере 1, расширение $GF(2)\subset GF(2^4)$, $L = GF(2^4) = \{0,1,\alpha,\alpha^2,\ldots,\alpha^{14}\}$, многочлен $G(x) = x^2+x+\alpha^3$, код $\Gamma(L,G)$ с проверочной матрицей H. Матрицы C и P возьмем из примера 1.

Абонент A вычисляет матрицу:

$$\widetilde{H} = CHP = \begin{pmatrix} 0&0&1&0&0&0&1&0&1&0&1&1&0&0&1&0\\ 1&1&1&1&0&0&0&0&1&0&1&1&1&0&1&1\\ 0&0&0&0&0&0&1&1&1&0&0&0&1&0&1&1\\ 1&0&0&1&1&0&1&0&1&1&1&1&1&1&1&0\\ 1&0&1&0&1&0&0&1&1&0&1&1&1&0&1&0\\ 0&1&1&1&0&1&0&1&1&0&0&1&1&0&0&0\\ 0&1&1&1&0&1&0&0&0&1&0&1&1&1&0&1\\ 1&0&0&0&1&1&0&1&1&1&1&1&1&0&0&1 \end{pmatrix}.$$

Параметры n, k, t и матрица $\widetilde{H}$ являются открытым ключом абонента A.

Абонент B помещает сообщение x в вектор ошибок e длины n веса не более $t=2$. Пусть

$$e = (0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0).$$

Абонент B шифрует сообщение e с помощью открытого ключа $\widetilde{H}$:

$$y = e\widetilde{H} = (0,0,0,1,0,1,1,1).$$

Шифрованное сообщение y передается по открытому каналу связи абоненту A.

Абонент A, получив сообщение y, расшифровывает его следующим образом. Сначала происходит умножение вектора y на матрицу $(C^T)^{-1} = (C^{-1})^T$:

$$S = y(C^T)^{-1} = (1,1,0,1,0,1,1,0).$$

Зафиксируем частное решение $\widetilde{x}$ системы уравнений $xH^T = S$:

$$\widetilde{x} = (0,0,0,0,1,1,1,0,0,0,0,0,0,0,0,0).$$

После применения к вектору $\widetilde{x}$ алгоритма декодирования, например алгоритма Паттерсона:

$$S(x) \equiv \alpha^{13} + \alpha^7 x, \quad T(x) \equiv S^{-1}(x) \equiv \alpha^{14} + \alpha x,$$

$$p(x) \equiv \sqrt{T(x) + x} \equiv \alpha^8 + \alpha^2 x,$$

$$\sigma(x) = r_0^2(x) + x v_0^2(x) = \alpha + x + \alpha^4 x, \;\; X_1 = 1 = \alpha_1, \;\; X_2 = \alpha^{12} = \alpha_{13},$$

получаем вектор ошибок $\widetilde{e}$:

$$\widetilde{e} = (0,1,0,0,0,0,0,0,0,0,0,0,0,1,0,0).$$

Для нахождения вектора e осталось вычислить:

$$e = \widetilde{e}P = (0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0).$$

3. Современная кодовая криптосистема

Рассмотрим современную кодовую криптосистему [14; 15] на основе кодов Гоппы, которая использует идеи крипосистем Мак-Элиса и Нидеррайтера.

Генерация ключа. Абонент A производит следующую последовательность действий.

1. Генерация случайным образом неприводимого многочлена $G(x) \in GF(2^m)$ степени $r = t$.

2. Случайным образом выбирается множество $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ различных элементов поля $GF(2^m)$.

3. Вычисляется проверочная матрица H' размера $r \times n$ на основе множества L и многочлена $G(x)$: $(H')_{ij} = \alpha_j^{i-1} G(\alpha_j)^{-1}$.

4. Пусть $\beta_1, \ldots, \beta_m$ — базис пространства $GF(2^m)$ над $GF(2)$ (например, если α — примитивный элемент поля $GF(2^m)$, то можно взять $\beta_i = \alpha^{i-1}$, $i = 1, \ldots, m$). Каждый элемент матрицы H' заменяется двоичным вектором-столбцом длины m с компонентами из поля $GF(2)$, где данный столбец является координатным столбцом элемента матрицы H' в базисе $\beta_1, \ldots, \beta_m$. Тем самым получим двоичную матрицу $\widetilde{H}$ размера $rm \times n$ над $GF(2)$.

5. С помощью элементарных преобразований строк матрица $\widetilde{H}$ приводится к систематическому виду $H = (I_{n-k}, Q_{(n-k),k})$. Если это невозможно, то происходит переход в шаг 1.

После таких манипуляций открытым ключом абонента A являются n, k, t, $H = (I_{n-k}, Q)$. Секретным ключом являются параметры L и $G(x)$ неприводимого (следовательно, сепарабельного) кода Гоппы $\Gamma(L, G)$ длины n и размерности $k = n - mr$.

Шифрование сообщения. Пусть h — некоторая хеш-функция (например, с длиной свертки 256), e — двоичный открытый текст веса t. Алгоритм шифрования абонентом B сообщения e на основе открытого ключа абонента B имеет следующий вид.

1. Вычисление двоичного вектора $c_0 = eH^T = e(I_{n-k}, Q)^T$ длины mr.

2. Вычисление значения хеш-функции от e: $c_1 = h(e)$.

Шифрованным сообщением будет являться пара (c_0, c_1).

Расшифрование сообщения. После получения сообщения (c_0, c_1) для его расшифрования абонент A проделывает следующие шаги.

1. Вектор c_0 дополняется $k = n - rm$ нулями до длины n: $v = (c_0, 0, \ldots, 0)$.

2. С помощью алгоритма декодирования находится (единственный) кодовый вектор $u \in \Gamma(L, G)$, находящийся на расстоянии Хэмминга до вектора v не более t, т. е. $d(u, v) \leqslant t$ (ниже приводится этому обоснование).

3. Вычисляется вектор $\widetilde{e} = v - u$.

4. Если $wt(\widetilde{e}) = t$, $\widetilde{e}H^T = c_0$ и $h(\widetilde{e}) = c_1$, то $e = \widetilde{e}$ — исходный открытый текст.

Заметим, что на втором шаге алгоритма расшифрования синдром вектора v совпадает с c_0: $vH^T = c_0$. Действительно, $vH^T = v(I_{n-k}, Q_{(n-k),k})^T = v \begin{pmatrix} I_{n-k} \\ Q^T_{k,(n-k)} \end{pmatrix} = c_0$. Поэтому векторы e и v имеют одинаковые синдромы, значит, принадлежат одному смежному классу. Следовательно, искомый кодовый вектор равен $u = v - e$.

Замечание 2. Алгоритмы шифрования и расшифрования можно модернизировать следующим образом. Пусть x — исходный двоичный открытый текст, длина которого совпадает с длиной сверок хеш-функции h. Генерируется случайный двоичный вектор (ошибок) e длины n веса t, вычисляются $c_0 = eH^T$, $c_1 = h(e)$, $y = x \oplus c_1$. Шифрованным сообщением будет являться пара (c_0, y). Для расшифрования производятся следующие действия: $v = (c_0, 0, \ldots, 0)$, находится кодовый вектор $u \in \Gamma(L, G)$ со свойством $d(u, v) \leqslant t$, вычисляются $e = v - u$, $c_1 = h(e)$. Тогда $x = y \oplus c_1$.

4. Протоколы аутентификации на основе кодовых криптосистем

Построение протоколов аутентификации с нулевым разглашением можно реализовать, используя известные алгоритмы открытого шифрования. В качестве секретной информации, которой владеет доказывающая сторона A, будет использоваться секретный ключ x асимметричного шифра. Пусть D_x — алгоритм расшифрования на секретном ключе x, E_y — алгоритм шифрования на открытом ключе y. Проверяющая сторона шифрует некоторое сообщение M на открытом ключе y и передает криптограмму $C = E_y(M)$ абоненту A. Абонент A демонстрирует владение секретной информацией x тем, что расшифровывает сообщение своим секретным ключом: $M = D_x(C)$ и передает сообщение M проверяющей стороне B. Для проверяющей стороны B это не несет никакой дополнительной информации о секретном ключе x, так как у B до этого было то же самое сообщение M. При этом при построении протоколов с нулевым разглашением знания нужен некоторый механизм, который позволит владельцу секретного ключа (доказывающему A) до передачи восстановленного сообщения M проверяющему B убедиться в том, что последнее уже известно проверяющему B.

В качестве такого механизма могут использоваться алгоритмы хеширования (хеш-функции). Данный механизм используется в протоколах с нулевым разглашением, описанных в стандарте [16].

В стандарте [16] регламентируется формирование запроса в виде пары значений (C, H), где C — шифртекст, полученный путем шифрования некоторого сообщения M по открытому ключу доказывающего A, и H — значение хеш-функции, вычисленное от сообщения M с использованием некоторой хеш-функции h: $H = h(M)$. Получая запрос (C, H), доказывающий имеет возможность убедиться в том, что восстановленное им из шифртекста C сообщение M известно проверяющему. Для этого достаточно вычислить значение хеш-функции от восстановленного сообщения и сравнить его со значением второго элемента запроса.

В соответствии с [16] двухшаговый протокол с нулевым разглашением знания включает следующие шаги.

1. Проверяющий B выбирает произвольное сообщение M и, используя алгоритм открытого шифрования E_y и открытый ключ y доказывающего, зашифровывает сообщение M: $C = E_y(M)$. Затем, используя хеш-функцию h, вычисляет значение хеш-функции от : $H = h(M)$. После этого он отправляет доказывающему A пару значений (C, H) в качестве своего запроса.

2. Доказывающий A расшифровывает криптограмму C, используя свой личный секретный ключ x, в результате чего получает сообщение $\widetilde{M} = D_x(C)$. Затем он вычисляет значение хеш-функции от $\widetilde{M}$: $\widetilde{H} = h(\widetilde{M})$, сравнивает значения $\widetilde{H}$ и H, если $\widetilde{H} = H$, то отправляет проверяющему значение $\widetilde{M}$ в качестве своего ответа.

3. Если выполнено равенство $\widetilde{M} = M$, то проверяющий B принимает доказательство; если равенство не выполнено, то отвергает.

Протокол аутентификации на основе классической криптосистемы Мак-Элиса. Абонент A фиксирует порождающую матрицу G некоторого $[n, k, d]$-кода над $GF(q)$, исправляющего t и менее ошибок, невырожденную матрицу S порядка k над полем $GF(q)$, перестановочную и диагональную матрицы P и D порядка n.

Матрица $\widetilde{G} = SGPD$ является открытым ключом абонента A, как и параметры n, k, t. Маскирующие матрицы S, P, D и порождающая матрица G являются секретным ключом абонента A.

Протокол аутентификации имеет следующий вид.

1. Проверяющий B генерирует случайное сообщение M длины k с компонентами из $GF(q)$, а также вектор ошибок e длины n над $GF(q)$ веса не более t. Вычисляет $C = M\widetilde{G} + e$, $H = h(M)$ и отправляет доказывающему A пару значений (C, H).

2. Доказывающий A вычисляет $C' = CD^{-1}P^{-1}$, декодирует вектор M' на основе вектора C', вычисляет $\widetilde{M} = M'S^{-1}$, вычисляет $\widetilde{H} = h(\widetilde{M})$. Если $\widetilde{H} = H$, то отправляет проверяющему значение $\widetilde{M}$ в качестве своего ответа.

3. После этого проверяющий B проверяет равенство $\widetilde{M} = M$.

Аналогичным образом можно использовать любую кодовую криптосистему в качестве основы для протокола аутентификации.

Выводы

Рассмотренная в работе тема является актуальной, так как затрагивает вопрос существования постквантовых криптосистем с открытым ключом. Приведены некоторые вариации кодовых криптосистем, включая некоторые современные модификации на основе кодов Гоппы. Приводится пример декодирования кода Гоппы на основе алгоритма Паттерсона. Также в работе предложен вариант протокола аутентификации на основе кодовых криптосистем. Представленный протокол имеет нулевое разглашение знания.

Литература

[1] McEliece R.J. A Public-Key Cryptosystem Based On Algebraic Coding Theory // DSN Progress Report. 1978. Vol. 42–44. P. 114–116.

[2] Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology. Internal Report 8240. January, 2019. 27 p. DOI: http://doi.org/10.6028/NIST.IR.8240.

[3] Patterson N.J. The algebraic decoding of Goppa codes // IEEE Transactions on Information Theory. 1975. Vol. 21, №. 2. P. 203–207. DOI: https://doi.org/10.1109/TIT.1975.1055350.

[4] Рацеев С.М. Об алгоритмах декодирования кодов Гоппы // Челяб. физ.-матем. журн. 2020. Т. 5, № 3. С. 327–341. DOI: https://doi.org/10.47475/2500-0101-2020-15307.

[5] Рацеев С.М., Череватенко О.И. О простом алгоритме декодировании кодов БЧХ, кодов Рида — Соломона и кодов Гоппы // Вестник СибГУТИ. 2020. № 3 (51). С. 3–14. URL: https://www.elibrary.ru/item.asp?id=44408789; http://vestnik.sibsutis.ru/showpapper.php?act=showpapper&id=950

[6] Рацеев С.М., Череватенко О.И. Об алгоритмах декодирования обобщенных кодов Рида — Соломона // Системы и средства информатики. 2020. Т. 30, № 4. С. 83–94. DOI: https://doi.org/10.14357/08696527200408.

[7] Рацеев С.М., Череватенко О.И. Об алгоритмах декодирования обобщенных кодов Рида — Соломона на случай ошибок и стираний // Вестник Самарского университета. Естественнонаучная серия. 2020. Т. 26, № 3. С. 17–29. DOI: https://doi.org/10.18287/2541-7525-2020-26-3-17-29.

[8] Bhaskar Biswas, Nicolas Sendrier. McEliece Cryptosystem Implementation: Theory and Practice // Buchmann J., Ding J. (eds.) Post-Quantum Cryptography. PQCrypto 2008. Lecture Notes in Computer Science. Vol. 5299. Springer, Berlin; Heidelberg, 2008. DOI: https://doi.org/10.1007/978-3-540-88403-3_4.

[9] Fitzpatrick P., Ryan J.A. Counting irreducible Goppa codes. Conference: Workshop on Coding and Cryptography (WCC). Versaille, France. Volume: 2003. March, 2003. URL: https://www.researchgate.net/publication/276265397_Counting_irreducible_Goppa_codes.

[10] Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problems of Control and Information Theory. 1986. Vol. 15, № 2. P. 159–166.

[11] Bernstein Daniel J., Buchmann Johannes, Dahmen Erik (eds.) Post-Quantum Cryptography. Berlin, Heidelberg: Springer-Verlag, 2009. DOI: http://dx.doi.org/10.1007/978-3-540-88702-7_4.

[12] Berlekamp E., McEliece R.J., Tilborg H. Van. On the inherent intractability of certain coding // IEEE Transactions on Information Theory. 1978. Vol. IT-24, № 3. P. 384–386. DOI: https://doi.org/10.1109/TIT.1978.1055873.

[13] Сидельников В.М. Криптография и теория кодирования // Московский университет и развитие криптографии в России: материалы конференции. Москва: МГУ, 2002. 22 с.

[14] Wang W., Szefer J., Niederhagen R. FPGA-based key generator for the niederreiter cryptosystem using binary Goppa codes. In: Fischer W., Homma N. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2017 // CHES 2017. Lecture Notes in Computer Science. Vol. 10529. P. 253–274. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-66787-4_13.

[15] Bernstein D., Chou T., Lange T., Maurich I., Misoczki R., Niederhagen R., Persichetti E., Peters C., Schwabe P., Sendrier N., Szefer J., Wang W. Classic McEliece: conservative code-based cryptography. Project documentation. URL: https://classic.mceliece.org/nist/mceliece-20190331.pdf, свободный. Яз. англ. (дата обращения: 02.12.2020).

[16] ISO/IEC 9798-5:2009(E) «Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge technique». URL: https://www.iso.org/standard/50456.html.

Scientific article

DOI: 10.18287/2541-7525-2021-27-1-62-73

Submited: 11.12.2020
Revised: 20.01.2021
Accepted: 28.02.2021

S.M. Ratseev
Ulyanovsk State University, Ulyanovsk, Russian Federation
E-mail: ratseevsm@mail.ru. ORCID: https://orcid.org/0000-0003-4995-9418
O.I. Cherevatenko
Ulyanovsk State University of Education, Ulyanovsk, Russian Federation
E-mail: chai@pisem.net. ORCID: https://orcid.org/0000-0003-3931-9425
V.A. Chernyavskaya
Ulyanovsk State University, Ulyanovsk, Russian Federation
E-mail: vera.chernya@yandex.ru. ORCID: https://orcid.org/0000-0001-9875-2232

ON SOME CRYPTOSYSTEMS BASED ON ALGEBRAIC CODES

ABSTRACT

In 1978 McEliece built the first public key cryptosystem based on error-correcting codes. At the same time, effective attacks on the secret keys of this cryptosystem have not yet been found. The work describes the classical and modernized cryptosystems of McEliece and Niederreiter, also examples of their practical application based on Goppa codes using the Patterson algorithm. Also the algorithms of two-step authentication protocols with zero disclosure based on error-correcting codes are given.

Key words: McEliece cryptosystem; error-correcting codes; Goppa codes; code decoding.

Citation. Ratseev S.M., Cherevatenko O.I., Chernyavskaya V.A. On some cryptosystems based on algebraic codes. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2021, vol. 27, no. 1, pp. 62–73. DOI: http://doi.org/10.18287/2541-7525-2021-27-1-62-73. (In Russ.)

Information about the conflict of interests: authors and reviewers declare no conflict of interests.

Sergey Mihaylovich Ratseev — Doctor of Physical and Mathematical Sciences, associate professor, Department of Information Security and Control Theory, Ulyanovsk State University, 42, Leo Tolstoy Street, Ulyanovsk, 432017, Russian Federation.

Olga Ivanovna Cherevatenko — Candidate of Physical and Matheatical Sciences, associate professor, Department of Higher Mathematics, Ulyanovsk State University of Education, 4/5, Lenin Square, Ulyanovsk, 432063, Russian Federation.

Vera Alekseevna Chernyavskaya — student of the Department of Information Security and Control Theory, Ulyanovsk State University, 42, Leo Tolstoy Street, Ulyanovsk, 432017, Russian Federation.

References

[1] McEliece R.J. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *DSN Progress Report*, 1978, no. 42–44, pp. 114–116.

[2] Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology. Internal Report 8240. January, 2019, 27 p. DOI: https://doi.org/10.6028/NIST.IR.8240

[3] Patterson N.J. The algebraic decoding of Goppa codes. *IEEE Transactions on Information Theory*, 1975, vol. 21, no. 2, pp. 203–207. DOI: https://doi.org/10.1109/TIT.1975.1055350.

[4] Ratseev S.M. On decoding algorithms for Goppa codes. *Chelyabinskiy Fiziko-Matematicheskiy Zhurnal = Chelyabinsk Physical and Mathematical Journal*, 2020, vol. 5, no. 3, pp. 327–341. DOI: https://doi.org/10.47475/2500-0101-2020-15307. (In Russ.)

[5] Ratseev S.M., Cherevatenko O.I. On a simple algorithm for decoding BCH codes, Reed-Solomon codes, and Goppa codes. *Vestnik SibGUTI*, 2020, № 3 (51), pp. 3–14. Available at: https://www.elibrary.ru/item.asp?id=44408789; http://vestnik.sibsutis.ru/showpapper.php?act=showpapper&id=950. (In Russ.)

[6] Ratseev S.M., Cherevatenko O.I. On decoding algorithms for generalized Reed-Solomon codes. *Sistemy i Sredstva Informatiki* = Systems and Means of Informatics, 2020, vol. 30, issue 4, pp. 83–94. DOI: https://doi.org/10.14357/08696527200408. (In Russ.)

[7] Ratseev S.M., Cherevatenko O.I. On decoding algorithms for generalized Reed-Solomon codes with errors and erasures. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2020, vol. 26, no. 3, pp. 17–29. DOI: https://doi.org/10.18287/2541-7525-2020-26-3-17-29. (In Russ.)

[8] Bhaskar Biswas, Nicolas Sendrier. McEliece Cryptosystem Implementation: Theory and Practice. In: Buchmann J., Ding J. (eds.) *Post-Quantum Cryptography. PQCrypto 2008. Lecture Notes in Computer Science*, 2008, vol 5299, pp. 47–62. Springer, Berlin; Heidelberg. DOI: https://doi.org/10.1007/978-3-540-88403-3_4.

[9] Fitzpatrick P., Ryan J.A. Counting irreducible Goppa codes. *Workshop on Coding and Cryptography (WCC).* At: Versaille, France. Voleume: 2003. Available at: https://www.researchgate.net/publication/276265397_Counting_irreducible_Goppa_codes.

[10] Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 1986, vol. 15, no. 2, pp. 159–166.

[11] Bernstein Daniel J.; Buchmann Johannes; Dahmen Erik (eds.) Post-Quantum Cryptography. Berlin; Heidelberg: Springer-Verlag, 2009, pp. 95–145. DOI: http://dx.doi.org/10.1007/978-3-540-88702-7_4.

[12] Berlekamp E., McEliece R.J., Tilborg H. Van. On the inherent intractability of certain coding. *IEEE Transactions on Information Theory*, 1978, vol. IT-24, no. 3, May 1978, pp. 384–386. DOI: https://doi.org/10.1109/TIT.1978.1055873.

[13] Sidelnikov V.M. Cryptography and coding theory. In: *Materials of the conference «Moscow State University and Development of Cryptography in Russia»*. Moscow: MGU, 2002, 22 p. (In Russ.)

[14] Wang W., Szefer J., Niederhagen R. FPGA-based key generator for the niederreiter cryptosystem using binary Goppa codes. In: Fischer W., Homma N. (eds.) *Cryptographic Hardware and Embedded Systems – CHES 2017*. CHES 2017. Lecture Notes in Computer Science, 2017, vol. 10529, pp. 253–274. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-66787-4_13.

[15] Bernstein D., Chou T., Lange T., Maurich I., Misoczki R., Niederhagen R., Persichetti E., Peters C., Schwabe P., Sendrier N., Szefer J., Wang W. Classic McEliece: conservative code-based cryptography. Project documentation. Available at: https://classic.mceliece.org/nist/mceliece-20190331.pdf (accessed: 02.12.2020).

[16] ISO/IEC 9798-5:2009(E) Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge technique. Available at: https://www.iso.org/standard/50456.html.