УДК 004.056.55

А.А. КУЗНЕЦОВ, д-р техн. наук, А.И. ПУШКАРЕВ,
И.И. СВАТОВСКИЙ, канд. техн. наук, А.В. ШЕВЦОВ

НЕСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ НА АЛГЕБРАИЧЕСКИХ КОДАХ ДЛЯ ПОСТКВАНТОВОГО ПЕРИОДА

Введение

Математической основой современных несимметричных криптосистем являются такие двухключевые конструкции, в которых задача поиска секретного ключа (private key) по известному открытому ключу (public key) связана с решением известной и очень сложной математической задачи (факторизации, дискретного логарифмирования и пр.) [1 – 3]. С появлением квантовых вычислений, основанных на принципах квантовой механики, в частности на принципе суперпозиции и явлении квантовой запутанности, скорость решения некоторых математических задач значительно возрастает [4]. Существуют квантовые алгоритмы, (алгоритмы Дойча и Йожи, Саймона, Гровера, Шора и другие), выполнение которых занимает гораздо меньше времени, чем выполнение любого вероятностного классического алгоритма [5 – 11]. Алгоритм Шора позволяет найти за конечное время все простые множители больших чисел или решить задачу дискретного логарифмирования и, как следствие, найти секретный ключ соответствующего асимметричного криптоалгоритма (например, в криптосистеме RSA) [10]. Следовательно, разработка и теоретическое обоснование новых криптографических алгоритмов, в том числе алгоритмов несимметричного шифрования и электронной цифровой подписи (ЭЦП), в которых сложность поиска секретного параметра по известному открытому ключу остается высокой даже с учетом возможного применения квантовых вычислений (т.е. для постквантового периода), является важной научной задачей [12 – 14].

Перспективным направлением в развитии постквантовой криптографии (Post-Quantum Cryptography) являются кодовые криптосистемы (Code-Based Cryptography), построение которых основано на использовании алгебраических кодов, замаскированных под код общего положения (случайный код, полный код) [14, 29]. В русскоязычной литературе подобные алгоритмы получили название теоретико-кодовых схем [22], или крипто-кодовых преобразований [23]. Кодовые криптосистемы позволяют реализовать относительно быстрое (в сравнении, например, с криптосистемами RSA, ECC и пр.) криптографическое преобразование данных, а также реализовать дополнительный контроль возникающих ошибок [23]. В работах [14, 29 – 31] показано, что криптокодовые преобразования остаются стойкими даже в случае использования квантовых вычислений.

На сегодняшний день известны различные криптографические примитивы, основанные на использовании алгебраических кодов: алгоритмы несимметричного [15, 16, 18, 20] и симметричного [17] шифрования, генераторы псевдослучайных последовательностей [24], протоколы доказательства с нулевым разглашением (Zero-knowledge proof) [27], схемы ЭЦП [29, 30], идентификации [31, 32] и пр. Это позволяет на основе единого математического и программного обеспечения реализовать широкий спектр эффективных механизмов криптографической защиты информации. И хотя известны также и вычислительно эффективные атаки на отдельные варианты теоретико-кодовых схем [19, 33 – 36], базовая конструкция [15], предложенная около 40 лет назад, остается стойкой ко всем известным методам криптоанализа, что в исторической ретроспективе подтверждает надежность и перспективность крипто-кодовых преобразований, особенно в контексте построения эффективных постквантовых алгоритмов криптографической защиты [37].

Цель работы – обзор известных несимметричных криптосистем на алгебраических кодах, в том числе схем формирования и проверки ЭЦП (Code-Based Signatures), исследование современного состояния, существующих противоречий и перспектив практического применения на постквантовый период.

Алгебраические коды для несимметричных криптосистем

Рассмотрим векторное пространство V_n как множество n-последовательностей с элементами из конечного поля $GF(q)$ с покомпонентным сложением и умножением на скаляр. *Линейный* (n,k,d) *код* V_k над $GF(q)$ есть подпространство в V_n, т.е. непустое множество n-последовательностей (*кодовых слов*) с элементами из $GF(q)$, где k – размерность линейного подпространства, d – минимальный вес Хемминга (число ненулевых элементов) $w_h(c)$ произвольного ненулевого кодового слова c кода V_k: $d = \min\limits_{\forall c \in V_k, c \neq 0} w_h(c)$. Ввиду линейности подпространства V_k набор весов различных ненулевых кодовых слов совпадает с набором расстояний по Хеммингу между различными кодовыми словами, т.е. d называют также *минимальным кодовым расстоянием* по Хеммингу кода V_k. Величину $R = \frac{k}{n}$ называют *относительной скоростью кода*, а $\delta = \frac{d}{n}$ *– относительным минимальным кодовым расстоянием*.

Линейный код V_k (как линейное подпространство в V_n) задается набором базисных (линейно независимых) векторов

$$(g_{0,0}, g_{0,1}, ..., g_{0,n-1}),$$
$$(g_{1,0}, g_{1,1}, ..., g_{1,n-1}),$$
$$\dots$$
$$(g_{k-1,0}, g_{k-1,1}, ..., g_{k-1,n-1}),$$

которые обычно представляются в матричном виде через порождающую матрицу

$$G = \begin{pmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{pmatrix}$$

ранга $rank(G) = k$ и размерности $k \times n$.

Произвольное кодовое слово $c = (c_0, c_1, ..., c_{n-1})$ кода V_k есть линейная комбинация строк из матрицы G. Кодирование заключается в сопоставлении каждого *информационного слова* $i = (i_0, i_1, ..., i_{k-1})$ с символами из $GF(q)$ некоторому кодовому слову $(c_0, c_1, ..., c_{n-1})$. Наиболее простой способ кодирования задается выражением $c = iG$.

Линейное подпространство, отождествляющее код V_k, имеет ортогональное дополнение (обозначим его U_{n-k}). Базис подпространства U_{n-k} задается векторами

$$(h_{0,0}, h_{0,1}, ..., h_{0,n-1}),$$
$$(h_{1,0}, h_{1,1}, ..., h_{1,n-1}),$$
$$\dots$$
$$(h_{n-k-1,0}, h_{n-k-1,1}, ..., h_{n-k-1,n-1})$$

и обычно представляется в матричном виде через проверочную матрицу

$$H = \begin{pmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{pmatrix}$$

ранга $rank(H) = n - k$ и размерности $(n-k) \times n$.

Условие ортогональности векторов из V_k и U_{n-k} в матричном виде записывается как $GH^T = 0$, где под нулем понимается нулевая матрица размерности $k \times (n-k)$.

Основной целью избыточного кодирования информации является контроль (обнаружение и исправление) ошибок, произошедших при передаче сообщения по каналу с шумами [38 – 40]. Для контроля ошибок кодирующее устройство вносит избыточность (проверочную часть длины $r = n - k$) в передаваемые данные. На приемной стороне, анализируя свойства проверочной части и ее соответствие передаваемым данным, декодер уменьшает влияние ошибок, возникших при передаче.

Обозначим вектор ошибок, воздействующий на передаваемое кодовое слово c, как n-последовательность $e = (e_0, e_1, ..., e_{n-1})$ с элементами из $GF(q)$. Искаженное кодовое слово обозначим вектором $c^* = c + e = (c_0 + e_0, c_1 + e_1, ..., c_{n-1} + e_{n-1})$.

Синдромом в теории кодирования называют вектор $s = (s_0, s_1, ..., s_{n-k-1})$ с элементами из $GF(q)$, который характеризует воздействие вектора ошибок на произвольное кодовое слово:

$$s = c^* H^T = cH^T + eH^T = eH^T,$$

т.е. значение вектора s зависит только от вектора ошибок $e = (e_0, e_1, ..., e_{n-1})$ и не зависит от выбранного кодового слова $c = (c_0, c_1, ..., c_{n-1})$.

Следует отметить, что при больших n и k задача поиска вектора e по ненулевому синдрому s для случайно выбранного в пространстве V_n линейного кода V_k является *чрезвычайно сложной математической задачей*. В общем случае эта задача относится к классу NP-сложных [37]. Однако для *алгебраических кодов*, со специфической структурой матриц G и H, декодирование (задача поиска вектора ошибок e и/или восстановление безошибочного кодового слова c) является *полиномиально разрешимой задачей*. К таким кодам относят: коды Рида – Соломона и их обобщения [38 – 40], а также различные ограничения указанных конструкций на произвольное подполе [40].

Определение 1 [38 – 40]. Пусть $X = (X_0, X_1, ..., X_{n-1})$ вектор над $GF(q^m)$, причем все X_i – различные элементы $GF(q^m)$. Пусть также $B = (B_0, B_1, ..., B_{n-1})$ – вектор над $GF(q^m)$ с необязательно различными B_i элементами $GF(q^m)$. Тогда (n, k, d) обобщенный код Рида – Соломона $\text{ОРС}_k(X, h)$ состоит из всех векторов вида

$$(B_0 \cdot F(X_0), B_1 \cdot F(X_1), ..., B_{n-1} \cdot F(X_{n-1})),$$

где $F(x)$ – любой многочлен с коэффициентами из $GF(q^m)$, степень которого не превосходит k. Код ОРС является МДР кодом, его проверочная матрица $\text{ОРС}_k(X, h)$:

$$H = \begin{pmatrix} Y_0 & Y_1 & ... & Y_{n-1} \\ X_1 \cdot Y_0 & X_2 \cdot Y_1 & ... & X_{n-1} \cdot Y_{n-1} \\ X_1^2 \cdot Y_0 & X_2^2 \cdot Y_1 & ... & X_{n-1}^2 \cdot Y_{n-1} \\ ... & ... & ... & ... \\ X_1^{n-k-1} \cdot Y_0 & X_2^{n-k-1} \cdot Y_1 & ... & X_{n-1}^{n-k-1} \cdot Y_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & ... & 1 \\ X_1 & X_2 & ... & X_{n-1} \\ X_1^2 & X_2^2 & ... & X_{n-1}^2 \\ ... & ... & ... & ... \\ X_1^{n-k-1} & X_2^{n-k-1} & ... & X_{n-1}^{n-k-1} \end{pmatrix} \cdot \begin{pmatrix} Y_0 & 0 & ... & 0 \\ 0 & Y_1 & ... & 0 \\ 0 & 0 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & Y_{n-1} \end{pmatrix},$$

где вектор $Y = (Y_0, Y_1, ..., Y_{n-1})$ такой, что $\forall Y_i \in GF(q^m)$, $Y_i \neq 0$ и дуальным к $\text{ОРС}_k(X, B)$ является $\text{ОРС}_{n-k}(X, Y)$.

Через ограничение ОРС на подполе вводится класс т.н. альтернантных кодов [38 – 40].

Определение 2 [38 – 40]. Альтернантный (n, k, d) код $A(X, B)$ состоит из всех слов кода $\text{ОРС}_k(X, B)$ таких, что их компоненты лежат в поле $GF(q)$. Другими словами, $A(X, B)$ равен ограничению кода $\text{ОРС}_k(X, B)$ на подполе $GF(q)$, т.е. он состоит из всех векторов c над $GF(q)$, для которых выполняется равенство $cH^T = 0$, где H – проверочная матрица $\text{ОРС}_k(X, B)$. По-

рождающая матрица $A(X, B)$ может быть получена заменой каждого элемента матрицы H соответствующим вектор-столбцом длины m над $GF(q)$.

Параметры кода $A(X, B)$ связаны соотношением: $n - mr \le k \le n - r$; $d \ge r + 1$, причем доказано [38 – 40], что среди большого числа всех возможных альтернантных кодов при фиксированном n и k найдутся такие коды, параметры которых лежат выше кодовых границ (1) и (2). Одним из частных случаев $A(X, B)$ являются коды Гоппы [42, 43].

Определение 3 [40]. Альтернантный (n, k, d) код Гоппы $\Gamma(L, G)$ над $GF(q)$ состоит из всех векторов $c = (c_1, c_2, \ldots, c_n)$ таких, что

$$R_c(x) \equiv 0 \bmod G(x),\ R_c(x) = \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i},$$

где $G(x)$ – многочлен с коэффициентами из $GF(q^m)$ (многочлен Гоппы), $L = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ – подмножество элементов из $GF(q^m)$ таких, что $G(\alpha_i) \ne 0\ \forall \alpha_i \in L$.

Многочлен $x - \alpha_i$ в кольце многочленов по модулю $G(x)$ имеет обратный многочлен:

$$(x - \alpha_i)^{-1} = -\frac{G(x) - G(\alpha_i)}{x - \alpha_i} G^{-1}(\alpha_i).$$

Следовательно, вектор $c = (c_1, c_2, \ldots, c_n)$ принадлежит коду Гоппы $\Gamma(L, G)$ только если

$$\sum_{i=1}^{n} c_i \frac{G(x) - G(\alpha_i)}{x - \alpha_i} G^{-1}(\alpha_i) = 0.$$

Если $G(x) = \sum_{i=0}^{r} g_i x^i$, где $g_i \in GF(q^m)$ и $g_r \ne 0$, то

$$\frac{G(x) - G(\alpha_i)}{x - \alpha_i} = g_r(x^{r-1} + x^{r-2}\alpha_i + \ldots + \alpha_i^{r-1}) + g_{r-1}(x^{r-2}\alpha_i + \ldots + \alpha_i^{r-1}) + \ldots + g_2(x + \alpha_i) + g_1.$$

Приравнивая нулю все коэффициенты при x^{r-1}, x^{r-2}, …, 1, получим, что условие $cH^T = 0$ выполнится только если проверочная матрица

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \ldots & \alpha_n^{r-1} \end{pmatrix} \begin{pmatrix} G^{-1}(\alpha_1) & 0 & \ldots & 0 \\ 0 & G^{-1}(\alpha_2) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & G^{-1}(\alpha_n) \end{pmatrix} = \begin{pmatrix} G^{-1}(\alpha_1) & G^{-1}(\alpha_2) & \ldots & G^{-1}(\alpha_n) \\ \alpha_1 G^{-1}(\alpha_1) & \alpha_2 G^{-1}(\alpha_2) & \ldots & \alpha_n G^{-1}(\alpha_n) \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{r-1} G^{-1}(\alpha_1) & \alpha_2^{r-1} G^{-1}(\alpha_2) & \ldots & \alpha_n^{r-1} G^{-1}(\alpha_n) \end{pmatrix}$$

также задает (n, k, d) код Гоппы $\Gamma(L, G)$ над $GF(q)$.

Последнее выражение при $Y = (Y_1, Y_2, \ldots, Y_n)$, $Y_1 = G^{-1}(\alpha_1)$, $Y_2 = G^{-1}(\alpha_2)$, …, $Y_n = G^{-1}(\alpha_n)$ эквивалентно матрице H для ОРС. Проверочную матрицу $\Gamma(L, G)$ над $GF(q)$ с элементами из $GF(q)$ можно получить путем представления каждого элемента из $GF(q^m)$ вектор-столбцом длины m символов из $GF(q)$. Справедлива следующая оценка.

Теорема [40, 42, 43]. Параметры (n, k, d) кода Гоппы $\Gamma(L, G)$ связаны соотношениями

$$n = /L/,\ k \ge n - mr,\ r = deg\ G(x),\ d \ge r + 1.$$

Для сепарабельных (когда многочлен $G(x)$ не имеет кратных корней ни в одном расширении поля) двоичных кодов Гоппы эти соотношения примут вид

$$n = 2^m,\ k \ge n - mr,\ r = deg\ G(x),\ d \ge 2r + 1. \quad (1)$$

Таким образом, при соответствующем выборе вектора-шаблона $Y = (Y_1, Y_2, \ldots, Y_n)$ удается построить блоковые коды с высокими конструктивными характеристиками, причем количество таких кодов задается количеством соответствующих шаблонов (или многочленов $G(x)$ в случае кодов Гоппы) [40, 42, 43]. Это свойство рассмотренных кодовых конструкций широко используется при решении различных инженерных задач как в области повышения помехоустойчивости передачи информации, так и для криптографической защиты. В частности, несимметричные криптосистемы доказуемой стойкости (provable security), построенные

на кодах Гоппы, помимо высокой скорости и возможности совмещать контроль ошибок с защитой от несанкционированного ознакомления [15 – 22], остаются стойкими даже на постквантовый период [28].

Несимметричное шифрование на основе кодов (теоретико-кодовые схемы)

Первой и наиболее изученной схемой несимметричного шифрования, основанной на использовании алгебраических блоковых кодов, является предложенная в 1978 году криптосистема Мак-Элиса (McEliece) [15]. Она обладает неоспоримыми преимуществами: высокой скоростью криптографического преобразования, а также возможностью совмещать контроль ошибок с защитой от несанкционированного ознакомления [15 – 22]. Кроме того, подобные (крипто-кодовые) преобразования остаются стойкими даже в случае использования квантовых вычислений [28].

Криптосистема Мак-Элиса. Открытым ключом в схеме Мак-Элиса является матрица

$$G_X = X \cdot G \cdot P \cdot D, \tag{2}$$

где G – порождающая матрица алгебраического (n,k,d) кода над $GF(q)$ (в оригинальной статье [15] предлагалось использовать рассмотренный выше двоичный код Гоппы), X – невырожденная $k \times k$ матрица с элементами из $GF(q)$, P и D – перестановочная и диагональная $n \times n$ матрицы (для двоичных кодов используется только матрица P).

Матрицы X, P и D являются секретным ключом, который маскирует используемый алгебраический блоковый код под случайный код (код общего положения), т.е. открытый ключ G_X представляется злоумышленнику как случайно сформированная порождающая матрица некоторого линейного кода, для которого неизвестен алгоритм быстрого декодирования. Напротив, уполномоченный пользователь, знающий секретный ключ (матрицы X, P и D), может снять действие маскирующих матриц и воспользоваться быстрым алгоритмом декодирования алгебраического кода с порождающей матрицей G.

Криптограмма представляет собой вектор длины n, который вычисляется по правилу

$$c_X^* = I \cdot G_X + e, \tag{3}$$

где вектор $c_X = I \cdot G_X$ является кодовым словом замаскированного кода, т.е. c_X принадлежит (n,k,d) коду с порождающей матрицей G_X, I – k-разрядный информационный вектор над $GF(q)$, вектор e – секретный вектор ошибок веса $w_h(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Вектор e следует рассматривать как одноразовый сеансовый секретный ключ, его вес определяет сложность декодирования искаженного кодового слова (криптограммы) c_X^*. Злоумышленнику необходимо декодировать кодограмму c_X^*, используя известную ему порождающую матрицу G_X. Однако декодирование случайного кода (при соответствующих параметрах n,k,q и $w_h(e)$) вычислительно недостижимо. Не зная матрицы X, P и D, злоумышленник не может восстановить матрицу G и воспользоваться алгоритмом декодирования полиномиальной сложности. Из этих соображений величину $w_h(e)$ следует максимизировать. Например, при $w_h(e) = t$ сложность декодирования будет максимальной, что обеспечит наивысший уровень стойкости кодовой криптосистемы для заданных параметров n,k,q.

Для уполномоченного пользователя (знающего секретный ключ) декодирование – полиномиально разрешимая задача. Действительно, легитимный пользователь, получив вектор c_X^*, строит вектор $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$. Матрица $\Lambda = PD$ сохраняет вес и расстояние по Хеммингу, т.е. для любых кодовых слов c и c' выполняются равенства:

$$w_h(c) = w_h(c \cdot \Lambda), \; w_h(c,c') = w_h(c \cdot \Lambda, c' \cdot \Lambda).$$

Это означает, что вектор $\vec{c}^{*}$ является искаженным не более чем в t разрядах кодовым словом алгебраического кода с порождающей матрицей G и его можно декодировать быстрым алгоритмом полиномиальной сложности [19].

Уполномоченный пользователь, используя алгоритмом полиномиальной сложности, декодирует вектор $\vec{c}^{*} = I' \cdot G + e'$, т.е. находит I'. Затем он вычисляет k-разрядный информационный вектор $I = I' X^{-1}$.

Таким образом, в криптосистеме Мак-Элиса основным средством маскировки линейного блокового (n, k, d) кода под линейный случайный код (код общего положения) являются матрицы X, P, D. Дополнительным секретным параметром, который можно использовать в случае кодов Гоппы, является многочлен Гоппы $G(x)$, или, в более широком смысле, вектор $Y = (Y_0, Y_1, \ldots, Y_{n-1})$ в случае альтернантных кодов. Изменение шаблона не снижает конструктивных кодовых характеристик, т.е. с точки зрения криптографического преобразования не приведет к снижению безопасности. Однако знание вектора-шаблона $Y = (Y_0, Y_1, \ldots, Y_{n-1})$ (или многочлена $G(x)$) является необходимым для правильного декодирования информационного сообщения, т.е. для корректного расшифрования на приемной стороне.

Опубликовано большое число различных атак на крипто-кодовые схемы защиты информации [19, 33 – 36], некоторые из которых оказались достаточно эффективными относительно отдельных вариантов кодовых криптосистем. Однако базовая конструкция [15], предложенная около 40 лет назад, остается стойкой ко всем известным методам криптоанализа, в том числе и в случае использования квантовых вычислительных систем.

Наиболее естественным направлением в развитии методов криптоанализа кодовой схемы Мак-Элиса является использование неалгебраических методов декодирования. Действительно, если существует вычислительно эффективный способ декодирования кодового слова (3) только по известной порождающей матрице (2), тогда информационное сообщение I может быть эффективно восстановлено и без знания секретного ключа (матриц X, P и D).

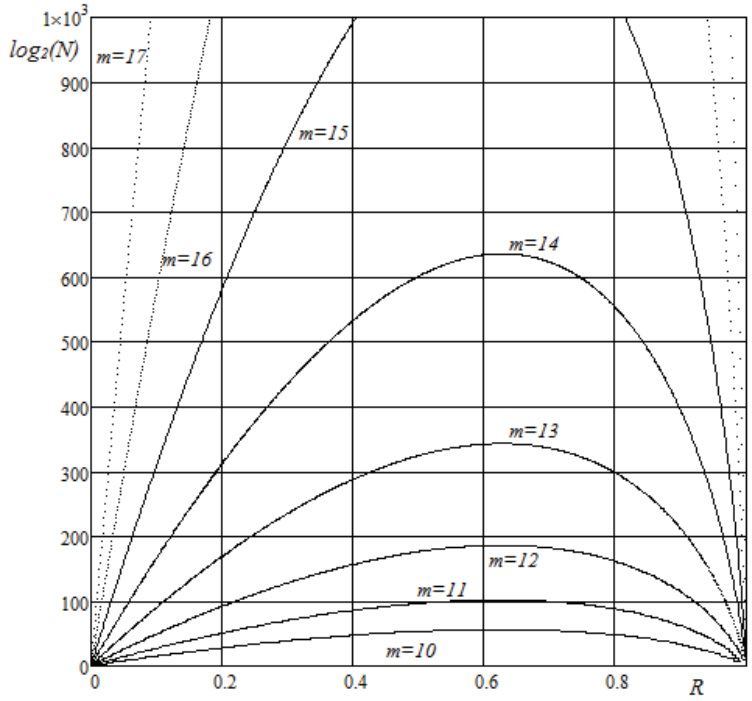
Среди универсальных методов декодирования линейных блоковых кодов, заданных произвольной порождающей матрицей, особое место занимают перестановочные алгоритмы [38 – 40]. Основная идея такого декодирования состоит в использовании различных наборов информационных множеств. Представим порождающую матрицу (2) в каноническом виде. При этом единичные вектора-столбцы могут быть выбраны произвольно с соответствующим формированием единичных подматриц и систематическим размещением k символов информационного множества. Оставшиеся $(n-k)$ символов однозначно вычисляются по элементам информационного множества. Позиции этих $(n-k)$ символов задают размещение единичных вектор-столбцов соответствующей проверочной матрицы. Если выбрать размещение $(n-k)$ единичных вектор-столбцов таким образом, чтобы они покрыли все t позиций ненулевых элементов вектора ошибок e, тогда кодовое слово, вычисленное по k символам информационного множества, не будет содержать ошибок, т.е. слово (3) можно декодировать даже без знания специальной алгебраической структуры порождающей (проверочной) матрицы используемого алгебраического кода.

Таким образом, при реализации перестановочного декодирования конкретная комбинация ошибок будет исправлена, только если удастся найти такое информационное множество, которое целиком содержит эту комбинацию. Такое множество, являющееся кровельной комбинацией ошибок, и набор проверочных множеств, которые покрывают все наборы ошибок данного типа, называют покрытием [38]. Задача декодера состоит в том, чтобы найти проверочное множество, которое покрывает неизвестную комбинацию ошибок. Рассмотрим границы для количества кровельных множеств. Предположим, что с помощью (n, k, d) кода исправляются все комбинации из t или меньшего количества ошибок. Рассмотрим комбинацию только из t кратных ошибок, так как все ошибки меньшей кратности будут покрыты. Общее количество комбинаций ошибок во всех n позициях равно C_n^t. Поскольку объем кровельного

множества равен $n - k$, максимальное количество комбинаций ошибок, которые могут быть покрыты данным множеством, равно C_{n-k}^{t}. Наименьшее количество множеств, которые могут исправить все комбинации из t ошибок, ограничивается выражением [38]:

$$N \geq \frac{C_n^t}{C_{n-k}^t} = \frac{n!(n-k-t)!}{(n-t)!(n-k)!}. \quad (4)$$

На рисунке приведены зависимости наименьшего числа кровельных множеств, которые потребуются для исправления всех комбинаций из t ошибок произвольного линейного блокового кода. Зависимости не учитывают вычислительную сложность формирования слов-кандидатов, вычисляемых по выбранной конфигурации информационного множества (реальная стойкость будет еще выше). Оценки N приведены в логарифмическом масштабе в зависимости от относительной скорости кодирования $R = k/n$ и рассчитаны для параметров (1).



Как следует из приведенных на рисунке зависимостей, наибольшую стойкость схема Мак-Элиса обеспечивает при использовании кодов с относительной скоростью $R \approx 2/3$, что согласуется с выводами большинства исследований [28]. В табл. 1 приведены параметры некоторых схем с кодами Гоппы и $R \approx 2/3$, оценки стойкости к атаке перестановочного декодирования, оценки вычислительной сложности кодирования (зашифрования) и декодирования (расшифрования), а также аналогичные оценки для несимметричного шифрования RSA.

Для криптосистемы Мак-Элиса значения в табл. 1 оценивались следующим образом. Размер открытого ключа оценивался как число двоичных элементов матрицы G_X – kn бит. Размер закрытого ключа оценивался как как число элементов матрицы X (k^2 бит) плюс число элементов, необходимых для хранения правила перестановки ($n \log_2 n$ бит). Сложность шифрования оценивалась как максимальное число операций, которые необходимо выполнить для формирования кодового слова посредством матричного вычисления выражения (3). Для двоичного (n, k, d) кода это соответствует $k \cdot n$ двоичным операциям. Сложность расшифрования оценивалась как число двоичных операций, которые необходимо выполнить для декодирования кодового слова с ошибками. Сложность алгебраического декодирования двоичных кодов Гоппы оценивалась как $t^2 \cdot m^3$ двоичных операций [29 – 32].

Таблица 1

Параметры	Уровень стойкости (без учета квантового криптоанализа)			
	Достаточный (2^{80} ... 2^{128})	Высокий (2^{192} ... 2^{256})		Сверхвысокий ($> 2^{512}$)
Криптосистема Мак-Элиса				
Параметры (*n, k, d*)	(2048, 1300, 137)	(4096, 2584, 253)		(16384, 10322, 867)
Размер секретного ключа, бит	1 712 528	6 726 208		106 773 060
Размер открытого ключа, бит	2 662 400	10 584 064		169 115 648
Сложность шифрования, битовых операций	$2{,}6\cdot10^6$	$1{,}1\cdot10^7$		$1{,}7\cdot10^8$
Сложность расшифрования, битовых операций	$6{,}2\cdot10^6$	$2{,}7\cdot10^7$		$5{,}1\cdot10^8$
Оценка стойкости (эквивалентная длина ключа симметричного шифра), log_2N	102	186		636
Оценка стойкости к квантовому криптоанализу, бит	**49**	**91**		**310**
Криптосистема RSA				
Размер модуля и открытого (закрытого) ключа, бит	2 048	7 680	15360	
Сложность шифрования (расшифрования), битовых операций	$3{,}2\cdot10^9$	$1{,}7\cdot10^{11}$	$1{,}4\cdot10^{12}$	
Оценка стойкости (эквивалентная длина ключа симметричного шифра), бит	112	192	256	
Оценка стойкости к квантовому криптоанализу, бит	**40**	**41**	**44**	

Оценка стойкости криптосистемы Мак-Элиса к квантовому криптоанализу проведена в [46, 47]. В частности, в [47] приводится оценка числа итераций для декодирования квантовым алгоритмом Гровера (Grover's algorithm). Эта оценка имеет вид

$$C^{\frac{n}{2\log n}},\ C=\frac{1}{(1-R)^{1-R}}, \tag{5}$$

где $R = k / n$ – относительная скорость используемого кода.

Значения в табл. 1 рассчитаны по соотношению (5). На практике оценка (5) снижает стойкость криптосистемы – примерно в два раза уменьшается эквивалентная длина ключа, что вполне ожидаемо для надежных постквантовых алгоритмов (как и для большинства симметричных шифров).

Для криптосистемы RSA значения в табл. 1 оценивались следующим образом. Скорость криптопреобразования (шифрования и расшифрования) оценивалась как сложность модульного возведения в степень. В работе [48, с. 613] показано, что в общем случае для *l*-битных чисел операция модульного возведения в степень требует порядка $\frac{3}{2}l^3$ двоичных операций. Пусть *p* и *q* – два *l*-битных простых числа, модуль преобразования RSA (общесистемный параметр) *n* = *pq* (2*l*-битное число), а открытым (секретным) ключом являются 2*l*-битные числа *e* и *d*. Тогда сложность модульного возведения в степень при шифровании (расшифровании) потребует $\frac{3}{2}(2l)^3 = 12l^3$ операций. Более эффективным является последовательное вычисление возведения в степень по модулям (*p* – *1*) и (*q* – *1*) соответственно. Такой алгоритм потребует в два раза большее число операций, однако в связи с уменьшением размерности модулей общее число операций сократится. Сложность преобразования составит $2\frac{3}{2}l^3 = 3l^3$ и значения, приведенные в табл. 1, соответствуют этой оценке. Размер модуля и соответству-

ющая оценка стойкости (как эквивалентная длина ключа симметричного шифра) указана в работе [49]. Оценки объема квантовых ресурсов, необходимых для решения некоторых асимметричных криптографический задач с помощью алгоритма Шора, при различных параметрах этих задач, и сравнение их со сложностью решения переборной задачи при поиске ключа симметричного шифра приведены в [50]. В частности, для m-битного числа дается оценка $4m^3$ временной сложности квантового алгоритма факторизации Шора и значения, приведенные в табл. 1, соответствуют этой оценке.

Следует обратить внимание на высокую скорость криптографического преобразования в схеме Мак-Элиса, которая на 3-5 порядков превосходит скорость шифрования в системе RSA (при сопоставимых показателях стойкости).

Вторым важным преимуществом схемы Мак-Элиса является возможность совмещать криптографичское преобразование с контролем возникающих ошибок. Действительно, если при формировании криптограммы (2) использовать случайный вектор ошибок e, веса $w(e) < t$, тогда появляется возможность одновременно с криптографическим преобразованием данных контролировать ошибки в пределах исправляющей способности. Уменьшение веса вектора e снизит криптографическую стойкость схемы Мак-Элиса, однако повысит помехоустойчивость передачи данных, т.е. в такой «гибридной» схеме изменяя $w(e)$ можно адаптивно реагировать на потребность в соответствующих услугах безопасности. Обозначим долю веса вектора ошибок вектора e, приходящегося на искусственное внесение при формировании криптограммы (см. выражение (2)) символом $\rho = w(e)/t$. Тогда стойкость криптосистемы, построенная на алгебраических кодах, будет определяться функцией от величины $\rho \cdot t$, а обеспечиваемая помехоустойчивость передаваемых криптограмм – функцией от величины $(1-\rho)\cdot t$.

Третье и, очевидно, одно из важнейших положительных свойств криптосистемы Мак-Элиса состоит в высокой устойчивости к квантовому криптоанализу. По сравнению с другими несимметричными криптосистемами, например с RSA, сложность квантового криптоанализа кодовой криптосистемы с увеличением ее параметров возрастает очень быстро. Фактически сложность криптоанализа при использовании квантовых алгоритмов сопоставима с решением переборных задач поиска эквивалентных ключей симметричных шифров. Данные в табл. 1 наглядно подтверждают эту тенденцию.

Основными недостатками рассмотренной кодовой криптосистемы являются огромные объемы ключевых данных (десятки мегабит), а также снижение относительной скорости передачи информации (наибольшая стойкость криптосистемы достигается при относительной скорости кодирования $R = k/n \approx 2/3$).

Криптосистема Нидеррайтера. Альтернативным примером криптосистем на кодах является схема Нидеррайтера, впервые предложенная в [16]. Открытым ключом в этой криптосистеме есть матрица

$$H_X = X \cdot H \cdot P \cdot D, \tag{6}$$

где H – проверочная матрица алгебраического (n,k,d) кода над $GF(q)$ (в оригинальной статье [16] предлагалось использовать обобщенные коды Рида – Соломона), X – невырожденная $(n-k)\times(n-k)$ матрица с элементами из $GF(q)$, P и D – перестановочная и диагональная $n \times n$ матрицы (для двоичных кодов используется только матрица P).

Матрицы X, P и D (как и для криптосистемы Мак-Элиса) являются секретным ключом, который маскирует используемый алгебраический блоковый код под случайный код (код общего положения), т.е. открытый ключ (6) представляется злоумышленнику как случайно сформированная проверочная матрица некоторого линейного кода, для которого неизвестен алгоритм быстрого декодирования. Напротив, уполномоченный пользователь, знающий секретный ключ (матрицы X, P и D), может снять действие маскирующих матриц и воспользоваться быстрым алгоритмом декодирования алгебраического кода с проверочной матрицей H.

Криптограмма s_X представляет собой вектор длины $(n-k)$:

$$s_X = e \cdot H_X^T, \qquad (7)$$

где вектор e – вектор длины n и веса $w_h(e) \le t$, который несет конфиденциальную информацию (информационное сообщение, подлежащее зашифрованию). Наибольшая стойкость обеспечивается при $w_h(e) = t$.

Для расшифрования криптограммы s_X выполняются следующие действия [19]. Уполномоченный пользователь (имеющий секретный ключ) находит одно из q^k решений выражения $s_X = c_X^* \cdot H_X^T$. Найденное решение – кодовое слово с ошибками $c_X^* = I \cdot G_X + e$. Далее, как и в схеме Мак-Элиса, 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.

Расшифрование s_X может быть выполнено и по следующей схеме [14]. Сперва заметим, что выражение (7) можно переписать в виде $s_X{}^T = H_X \cdot e^T$. В этом случае, уполномоченный пользователь (имеющий матрицы X, P и D) для расшифрования криптограммы вычисляет вектор $s_X^{*T} = X^{-1} \cdot s_X{}^T = X^{-1} \cdot H_X \cdot e^T = H \cdot P \cdot D \cdot e^T = H \cdot \bar{e}^T$, значение которого зависит от вектора $\bar{e}^T = P \cdot D \cdot e^T$.

Вектор $s_X^{*T} = H \cdot \bar{e}^T$ представляет собой синдром, вычисленный по проверочной матрице H алгебраического (n,k,d) кода, т.е. алгоритм быстрого (алгебраического) декодирования позволяет найти вектор $\bar{e}^T$, после чего уполномоченный пользователь снимает действие матриц маскирования P, D и находит вектор

$$e^T = D^{-1} \cdot P^{-1} \cdot \bar{e}^T = D^{-1} \cdot P^{-1} \cdot P \cdot D \cdot e^T.$$

Таким образом, в криптосистеме Нидеррайтера основным средством маскировки линейного кода под случайный код являются (как и в криптосистеме Мак-Элиса) матрицы *X, P, D*. Если использовать коды Гоппы, тогда многочлен *G(x)* может выступать дополнительным секретным параметром.

В работе [19] показано, что стойкости криптосистем Мак-Элиса и Ниддерайтера эквивалентны и эффективную атаку на одну из схем можно легко трансформировать в атаку на другую схему. В этом смысле оценки стойкости из табл. 1 справедливы и по отношению к криптосистеме Ниддерайтера. Другие характеристики этих криптосистем (скорость криптопреобразования, объемы ключей) также сопоставимы.

Очевидным преимуществом теоретико-кодовой схемы Нидеррайтера по сравнению с криптосистемой Мак-Элиса является потенциально бóльшая относительная скорость передачи данных. Действительно, относительная скорость в криптосистеме Мак-Элиса определяется относительной скоростью используемого (n,k,d) кода, т.е. $R = k/n$, причем наибольшая стойкость достигается при $R = k/n \approx 2/3$ (см. рисунок). Информационное сообщение в системе Нидеррайтера сначала преобразуется в равновесную последовательность e длины n и веса $w_h(e) \le t$, а затем умножается на проверочную матрицу как в (7). Положим $w_h(e) = t$ (в этом случае будет обеспечена максимальная стойкость криптосистемы для заданных (n,k,d) параметров кода). Тогда максимальное число бит информационных данных, которые можно зашифровать в системе Нидеррайтера при использовании двоичного (n,k,d) кода, будет определяться выражением $l_{\inf} = \lfloor \log_2 C_n^t \rfloor$, где $\lfloor x \rfloor$ – наибольшее целое число, меньшее x. Криптограмма (7) представляет собой синдромный вектор длины $n - k$, т.е. относительная скорость передачи данных в криптосистеме Нидеррайтера (для двоичных кодов) будет опре-

деляться выражением: $R^* = l_{\inf} / (n-k)$. Эта формула легко обобщается на случай недвоичных кодов с основанием q:

$$R^* = \frac{\left\lfloor \log_q \left((q-1)^t \frac{n!}{t!(n-t)!} \right) \right\rfloor}{n-k}. \quad (8)$$

Если предположить, что информационная последовательность будет преобразовываться во все возможные векторы e длины n и веса $0 \le w_h(e) \le t$, тогда:

$$R^* = \frac{\left\lfloor \log_q \left(\sum_{i=0}^{t} (q-1)^i \frac{n!}{i!(n-i)!} \right) \right\rfloor}{n-k}. \quad (9)$$

Выражение (9) достигает максимума для так называемых *совершенных кодов* (perfect codes), кодовые (n,k,d) параметры которых удовлетворяют верхней границе Хемминга для мощности (числа кодовых слов) $A_q(n,d)$ линейного q-ичного кода [38 – 40]:

$$A_q(n,d) \le \frac{q^n}{\sum_{i=0}^{t} (q-1)^i \frac{n!}{i!(n-i)!}}. \quad (10)$$

Мощность линейного (n,k,d) кода над $GF(q)$ равна q^k, следовательно из (10) следует ограничение на число информационных символов кода

$$k \le n - \log_q \left(\sum_{i=0}^{t} (q-1)^i \frac{n!}{i!(n-i)!} \right).$$

Если параметры (n,k,d) кода удовлетворяют верхней границе Хемминга, тогда

$$\log_q \left(\sum_{i=0}^{t} (q-1)^i \frac{n!}{i!(n-i)!} \right) = n-k, \quad (11)$$

что после подстановки в (9) дает $R^* = 1$, т.е. относительная скорость максимальна и криптограмма в схеме Нидеррайтера не будет содержать избыточных символов.

В качестве примера приведем совершенный двоичный (q = 2) код Хемминга, исправляющий одну ошибку (t = 1). Он определен для любого положительного целого $m > 2$ и имеет кодовые параметры $(n = 2^m - 1, k = 2^m - m - 1, d = 3)$ [38 – 40].

Очевидно, что для этих значений

$$\sum_{i=0}^{t} \frac{n!}{i!(n-i)!} = 2^m, \; n-k = m$$

и относительная скорость (9) равна 1.

Другим примером является совершенный двоичный код Голея (perfect binary Golay code) с параметрами (n = 23, k = 12, d = 7) [38 – 40]. Для этих значений имеем

$$\sum_{i=0}^{t} \frac{n!}{i!(n-i)!} = 2048, \; n-k = 12,$$

т.е. относительная скорость (9) также равна 1.

В [53 – 54] показано, что любой нетривиальный совершенный код имеет параметры кода Хэмминга или кода Голея, т.е. достижение $R^* = 1$ ограничивается только этими конструкциями. Большинство других кодов, в том числе и коды Гоппы, обладают конструктивными (n,k,d) параметрами, лежащими существенно ниже верхней границы (10) (реальные дистанционные характеристики кодов Гоппы выше). Например, для кода Гоппы с параметрами n = 1024, k = 524, t = 50 (использован в авторском варианте [15] схемы Мак-Элиса) относительная скорость шифрования (8) в схеме Нидеррайтера $R^* \approx 0{,}57$, что незначительно выше по сравнению со скоростью $R \approx 0{,}51$ в схеме МакЭлиса. С увеличением длины кода кон-

структивные параметры кодов Гоппы ухудшаются, что приводит к снижению скорости. Эту тенденцию наглядно демонстрируют результаты расчетов в табл. 2, в которой приводятся оценки относительной скорости при использовании кодов с параметрами из табл. 1.

Таблица 2

Кодовые (n,k,d) параметры	Конструктивные кодовые характеристики			
	(1024, 524, 101)	(2048, 1300, 137)	(4096, 2584, 253)	(16384, 10322, 867)
Схема Мак-Элиса	$\approx 0{,}51$	$\approx 0{,}63$	$\approx 0{,}63$	$\approx 0{,}63$
Схема Нидеррайтера	$\approx 0{,}57$	$\approx 0{,}57$	$\approx 0{,}53$	$\approx 0{,}48$

Очевидно, что с увеличением длины кода Гоппы скорость (8), (9) для схемы Нидеррайтера снижается и не превосходит относительной скорости кодирования $R = k/n$. В авторской статье [16] в схеме Нидеррайтера предлагалось использовать обобщенные коды Рида – Соломона, их (n,k,d) параметры связаны соотношением $d = n - k + 1$, т.е. удовлетворяют верхней границе Синлгтона [38 – 40]. Тогда, например, для $q = 1024$ расширенный код Рида – Соломона будет иметь параметры (1024, 524, 501) и оценка (8) дает относительную скорость для схемы Нидеррайтера $R^* \approx 0{,}66$, что на 30 % выше по сравнению с $R \approx 0{,}51$ для схемы Мак-Элиса. Однако в работе [19] предложена эффективная атака на криптосистемы с обобщенными кодами Рида – Соломона, т.е. применение этого класса кодов несостоятельно. Таким образом, стойкие ко всем известным атакам криптосистемы Мак-Элиса и Нидеррайтера на двоичных кодах Гоппы сравнимы по относительной скорости передачи данных.

Электронная цифровая подпись на основе кодов

Первый известный алгоритм формирования и проверки ЭЦП с использованием алгебраических кодов основан на криптосистеме Нидеррайтера и был представлен Courtois, Finiasz и Sendrier в [29]. Оценка стойкости этой схемы (названной по инициалам ее изобретателей – CFS) против подделки подписи сводится к оценке сложности решения задачи синдромного декодирования. Знание секретного ключа позволяет декодеру решить эту задачу для некоторой доли случайных кодовых слов.

В алгоритме CFS реализован принцип, который заключается в многократном хешировании документа, рандомизированного счетчиком битовой длины *r*, пока не будет получен правильно выделенный синдром. Подписавшийся использует свой секретный ключ для определения соответствующего вектора ошибок. Вместе с текущим значением счетчика этот вектор ошибок используется в качестве подписи.

Реализация схемы CFS для формирования и проверки ЭЦП осуществляется в соответствии со следующими алгоритмами.

1. *Системные параметры*: m, $t \in N$;

2. *Генерация ключа*: генерация пары ключей как в криптосистеме Нидеррайтера на основе использования алгебраического кода из класса ($n = 2^m$, $k = n - mt$, $2t + 1$) двоичных неприводимых кодов Гоппы (см. раздел 1), для которого порождаются следующие матрицы:

- матрица H : $(n - k) \times n$ – проверочная матрица алгебраического кода с исправляющей способностью t ошибок,
- матрица X : $(n - k) \times (n - k)$ – случайная обратимая матрица,
- матрица P : $n \times n$ – случайная матрица перестановок.

Следует отметить, что диагональная матрица D используется лишь для недвоичных кодов и в данном (двоичном) случае матрица D для генерации пары ключей не требуется.

Открытый ключ: матрица $H_X = X \cdot H \cdot P$ и число t (исправляющая способность кода).

Секретный ключ: матрицы X, P и быстрый (полиномиальной сложности) алгоритм декодирования алгебраического кода.

Алгоритм декодирования позволяет по введенной синдромной последовательности $s=(s_0,s_1,...,s_{n-k-1})$ в случае успеха декодирования найти вектор ошибок $e=(e_0,e_1,...,e_{n-1})$ и кодовое слово $c=(c_0,c_1,...,c_{n-1})$. В противном случае (если декодирование не удалось) алгоритм выдает отказ в обработке синдрома $s=(s_0,s_1,...,s_{n-k-1})$, т.е. по такой последовательности алгоритм не может найти вектор ошибок $e=(e_0,e_1,...,e_{n-1})$ и кодовое слово $c=(c_0,c_1,...,c_{n-1})$.

3. *Формирование подписи*

Вход:

1) h – функция хеширования, которая применяется к входным данным x (аргументу функции) произвольной длины. Результатом хеширования является хеш-код $h(x)$ длины $n-k$ бит;

2) Быстрый (полиномиальной сложности) алгоритм декодирования алгебраического кода, который применяется к синдромной последовательности $s=(s_0,s_1,...,s_{n-k-1})$. Предполагается, что в результате выполнения алгоритма декодирования возможны две ситуации:

- если декодирование успешно – выводится найденный вектор ошибок $e=(e_0,e_1,...,e_{n-1})$, который соответствует вектору $s=(s_0,s_1,...,s_{n-k-1})$;

- если декодирование не успешно – выдается сообщение о невозможности найти вектор ошибок $e=(e_0,e_1,...,e_{n-1})$ для введенного вектора $s=(s_0,s_1,...,s_{n-k-1})$;

3) Открытый текст M, для которого необходимо сформировать ЭЦП по схеме CFS.

Выход:

ЭЦП по схеме CFS Y для открытого текста M.

Алгоритм формирования ЭЦП по схеме CFS

Шаг 1. Хеширование открытого текста M, т.е. вычисление хеш-кода $h(M)$. Присваивание переменной i значения $i=1$;

Шаг 2. Вычисление хеш-кода $h(h(M)\|i)$, где $h(M)\|i$ – конкатенация (объединение) значений $h(M)$ и i, представленных в виде битовых последовательностей;

Шаг 3. Значение $h(h(M)\|i)$ интерпретируется как синдромная последовательность $s_X=(s_0,s_1,...,s_{n-k-1})$, вычисленная для некоторого (произвольного) кодового слова и вектора ошибок $e=(e_0,e_1,...,e_{n-1})$, т.е. предполагается выполнение равенства (7*) для соответствующего открытого ключа $H_X=X\cdot H\cdot P$;

Шаг 4. Вычисление значение вектора

$$s_X^{*T}=X^{-1}\cdot s_X{}^T \ ,$$

который (как предполагается) представляет собой синдром, вычисленный по проверочной матрице H алгебраического (n,k,d) кода, т.е. предполагается, что

$$s_X^{*T}=X^{-1}\cdot s_X{}^T=X^{-1}\cdot H_X\cdot e^T=H\cdot P\cdot e^T=H\cdot\overline{e}^T$$

и алгоритм быстрого декодирования позволит найти вектор $\overline{e}^T=P\cdot e^T$;

Шаг 5. Для синдромной последовательности s_X^* реализуется выполнение быстрого алгоритма декодирования:

- если декодирование успешно – выводится найденный вектор ошибок $\overline{e}^T=P\cdot e^T$, который соответствует вектору s_X^*;

- если декодирование не успешно – выдается сообщение о невозможности найти вектор ошибок $\overline{e}^T=P\cdot e^T$ для введенного вектора s_X^*. Присваивание переменной i значения $i=i+1$ и переход на Шаг 2;

Шаг 6. Вычисление вектора

$$e^T = P^{-1} \cdot \overline{e}^T = P^{-1} \cdot P \cdot e^T;$$

Шаг 7. Формирование ЭЦП по схеме CFS $Y = (e, i)$ для открытого текста M.

Таким образом, в результате выполнения рассмотренного алгоритма формирования ЭЦП по схеме CFS вычисляется такое наименьшее положительное целое число i, для которого значение $h(h(M)\|i)$, интерпретируемое как синдромная последовательность $s_X = (s_0, s_1, ..., s_{n-k-1})$, соответствует вектору ошибок $e = (e_0, e_1, ..., e_{n-1})$, т.е. формально запишем:

$$Y = (e, i) : H_X \cdot e^T = \left(h(h(M)\|i)\right)^T. \quad (12)$$

Задача вычисления вектора $e = (e_0, e_1, ..., e_{n-1})$ по известному вектору $h(h(M)\|i)$ сопряжена с решением задачи декодирования (n, k, d) кода:

- для уполномоченного пользователя (знающего секретный ключ) – это вычислительно простая задача (полиномиальной сложности);
- для злоумышленника (знающего только открытый ключ) – это вычислительно сложная задача декодирования случайного кода (относящаяся к классу сложности NP-полных задач).

Для верификации (проверки правильности ЭЦП $Y = (e, i)$ сообщения M) необходимо убедиться в том, является ли результат хеширования $h(h(M)\|i)$ синдромной последовательностью, вычисленной по вектору $e = (e_0, e_1, ..., e_{n-1})$ (который интерпретируется как вектор ошибок).

4. *Верификация*

Ввод:

1) Открытый ключ (матрица $H_X = X \cdot H \cdot P$ и число *t*);

2) Функция хеширования *h*;

3) ЭЦП $Y = (e, i)$;

4) Открытый текст M.

Выход:

решение о *правильности* или *неправильности* ЭЦП;

Алгоритм верификации (алгоритм проверки ЭПЦ по схеме CFS):

Шаг 1. Вычисление вектора

$$(s'_X)^T = H_X \cdot e^T;$$

Шаг 2. Вычисление вектора

$$(s''_X)^T = h(h(M)\|i);$$

Шаг 3. Принятие решение о *правильности* или *неправильности* ЭЦП:

- если $s'_X = s''_X$, тогда принимается решение о *правильности* ЭЦП;
- если $s'_X \neq s''_X$, тогда принимается решение о *неправильности* ЭЦП.

Оценим конструктивные характеристики схемы CFS при формировании ЭЦП с использованием двоичных блоковых (n, k, d) кодов.

Сложность формирования и проверки ЭЦП. Корректное использование рассмотренной схемы подписи CFS предполагает успешное декодирование на шаге 5 алгоритма формирование ЭЦП. Оценим среднее число попыток декодирования (среднее число выполнений шага 5 алгоритма формирования ЭЦП).

Для двоичного блокового (n,k,d) кода любая конфигурация из $t=\left\lfloor \frac{d-1}{2} \right\rfloor$ и меньше ошибок может быть гарантированно исправлена и соответствует, таким образом, уникальной синдромной последовательности. Следовательно, количество синдромных последовательностей, которые гарантированно будут корректно обработаны алгоритмом декодирования и приведут к успеху на шаге 5 алгоритма формирования ЭЦП, определяется выражением $N=\sum_{i=0}^{t} C_n^i$. Синдромная последовательность имеет длину $n-k$, и общее количество всех возможных таких последовательностей равно 2^{n-k}. Тогда, если принять предположение о равновероятности формирования хеш-кодов $h(h(M)\|i)$ на втором шаге алгоритма формирования ЭЦП, вероятность успеха декодирования для единичной попытки на шаге 5 будет определяться выражением

$$P_{у.д.}=\frac{\sum_{i=0}^{t} C_n^i}{2^{n-k}}. \qquad (13)$$

Если воспользоваться аппроксимацией [30] $\sum_{i=0}^{t} C_n^i=\frac{n^t}{t!}$, то для рассмотренных выше двоичных сепарабельных кодов Гоппы с параметрами (1) выражение (15) примет вид

$$P_{у.д.}=\frac{\sum_{i=0}^{t} C_n^i}{2^{n-k}}=\frac{\frac{n^t}{t!}}{n^t}=\frac{1}{t!}. \qquad (14)$$

Таким образом, успех в декодировании (на шаге 5 алгоритма формирования ЭЦП) будет достигнут при реализации в среднем после $t!$ попыток. Каждая попытка требует $t^2\cdot m^3$ двоичных операций [30], т.е. среднее число битовых операций, которые необходимо затратить для формирования ЭЦП по схеме CFS, определяется как

$$N_{ф.п.}=t^2\cdot m^3\cdot t!. \qquad (15)$$

Заметим, что в формуле (15) не учтены затраты на формирование хеш-кодов (шаги 2 и 3 алгоритма формирования ЭЦП), а также не учтены затраты на снятие действия матрицы маскирования $s_X^{*T}=X^{-1}\cdot s_X{}^T$ (на шаге 4 алгоритма).

Для проверки (верификации) ЭЦП $Y=(e,i)$, сформированной для сообщения M, необходимо вычислить хеш-код $h(h(M)\|i)$ и сравнить его с результатом произведения $H_X\cdot e^T$. Если не учитывать сложность хеширования, тогда сложность проверки ЭЦП будет определятся выражением

$$N_{п.п.}=(n-k)\cdot n=m\cdot t\cdot 2^m \qquad (16)$$

(потребуется $(n-k)\cdot n$ битовых операций умножения и сложения для вычисления $H_X\cdot e^T$).

Стойкость ЭЦП по схеме CFS. В основе построения схемы ЭЦП CFS лежит использование несимметричной криптосистемы Нидеррайтера, стойкость которой (как количество кровельных множеств, при которых перестановочное декодирование позволит исправить все комбинации из t ошибок без знания секретного ключа) определяется выражением (4). В то же время для формирования ложной подписи $Y'=(e',i')$ подделанного сообщения M' злоумышленнику необходимо не только реализовать декодирование случайного кода, а выполнить это декодирование в среднем $t!$ раз (как и уполномоченному пользователю), т.е. найти такое наименьшее положительное целое число i, для которого выполнится равенство (12). С учетом последнего замечания выражение для оценки стойкости ЭЦП по схеме CFS запишем в виде

$$N_c \geq t!\frac{C_n^t}{C_{n-k}^t} = t!\frac{n!(n-k-t)!}{(n-t)!(n-k)!} = t!\frac{2^m!(mt-t)!}{(2^m-t)!(mt)!}. \quad (17)$$

Для оценки стойкости ЭЦП к квантовому криптоанализу воспользуемся формулой (5), которая устанавливает число итераций для декодирования случайного кода квантовым алгоритмом Гровера. Такое декодирование необходимо выполнить в среднем $t!$ раз. Если предположить, что квантовый алгоритм, предназначенный для решения переборных задач, может быть использован для переборного поиска числа i и потребует в среднем $\frac{\pi}{4}\sqrt{t!}$ попыток, тогда выражение для оценки стойкости ЭЦП по схеме CFS к атакам квантового криптоанализа примет вид

$$N_{с.к.} \geq \frac{\pi}{4}\sqrt{t!}\left(\frac{1}{(1-R)^{1-R}}\right)^{\frac{n}{2\log n}} = \frac{\pi}{4}\sqrt{t!}\left(\left(1-\frac{k}{n}\right)^{\frac{k}{n}-1}\right)^{\frac{n}{2\log n}} = \frac{\pi}{4}\sqrt{t!}\left(1-\frac{k}{n}\right)^{\frac{k-n}{2\log n}} = \frac{\pi}{4}\sqrt{t!}\left(\frac{m\cdot t}{2^m}\right)^{-t/2}. \quad (18)$$

Длина ЭЦП по схеме CFS. Цифровая подпись $Y=(e,i)$ состоит из двух частей: двоичного вектора e длиной n бит и целого числа i, которое может принимать значение в диапазоне $0,1,..,2^{n-k}-1$. Таким образом, битовая длина ЭЦП (записанной в виде последовательности (e,i)) будет определяться выражением

$$l_{ЭЦП} = 2\cdot n - k = 2^m + m\cdot t. \quad (19)$$

Следует отметить, что n-битный вектор e не может принимать все 2^n значений. Этот вектор интерпретируется в схеме CFS как битовый вектор ошибок, который может быть исправлен с использованием двоичного блокового (n,k,d) кода, т.е. вес Хемминга вектора e не может превышать исправляющей способности кода:

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

Следовательно, количество всех допустимых векторов e (как элемента ЭЦП по схеме CFS) определяется выражением $N_{w(e)\leq t} = \sum_{i=0}^{t} C_n^i$ и вектор e может быть преобразован в безызбыточную последовательность e^* длины $\left\lceil \log_2(N_{w(e)\leq t}) \right\rceil$ бит.

С учетом безызбыточного кодирования вектора e^* выражение (19) перепишем в виде

$$l_{ЭЦП}^* = \left\lceil \log_2\left(\sum_{i=0}^{t} C_n^i\right)\right\rceil + n - k = \left\lceil \log_2\left(\sum_{i=0}^{t} C_{2^m}^i\right)\right\rceil + m\cdot t.$$

Используя выражение (10) для верхней границы Хемминга, последнюю формулу можем переписать в виде

$$l_{ЭЦП}^* \leq \left\lceil \log_2\left(2^{n-k}\right)\right\rceil + n - k = 2\cdot m\cdot t. \quad (19^*)$$

Для формирования ЭЦП в сжатом виде $Y=(e^*,i)$ следует использовать методы равновесного кодирования, изложенные, например, в [14, 52].

Объем ключевых данных, используемых в схеме CFS, определяется объемом ключевых данных несимметричной теоретико-кодовой схемы Нидеррайтера. Запишем в явном виде эти выражения:

- битовая длина открытого ключа (число двоичных ячеек матрицы $H_X = X\cdot H\cdot P$)

$$l_{о.к.} = (n-k)\cdot n = n^2 - kn = m\cdot t\cdot 2^m; \quad (20)$$

- битовая длина закрытого ключа (число двоичных ячеек матрицы X плюс битовая длина n целых чисел в диапазоне $0,1,..,n-1$ для указания правила заполнения матрицы P)

$$l_{з.к.} = (n-k)^2 + n \cdot \lceil \log_2 n \rceil = (m \cdot t)^2 + 2^m \cdot m . \quad (21)$$

В статье [29] рассмотрены примеры ЭЦП с $t \in \{8,9,10\}$ и $m \in \{11,12,...,17\}$, оценки характеристик (15) – (21) для этих параметров приведены в табл. 3. В последних строках таблицы приведены параметры схемы CFS, устойчивой к квантовым атакам.

Таблица 3

m	t	$N_{ф.п.}$	$N_{п.п.}$	N_c	$N_{с.к.}$	$l_{ЭЦП}$*	$l_{о.к.}$	$l_{з.к.}$
11	8	$2^{31.7}$	$2^{17.5}$	$2^{52,1}$	$2^{25,5}$	176	$2^{17.5}$	$2^{14.9}$
	9	$2^{35.2}$	$2^{17.6}$	$2^{58,3}$	$2^{26.4}$	198	$2^{17.6}$	$2^{15.0}$
	10	$2^{38.8}$	$2^{17.8}$	$2^{64,6}$	$2^{31.6}$	220	$2^{17.8}$	$2^{15.1}$
12	8	$2^{32.1}$	$2^{18.6}$	$2^{59,0}$	$2^{29.0}$	192	$2^{18.6}$	$2^{15.8}$
	9	$2^{35.6}$	$2^{18.8}$	$2^{66,2}$	$2^{29.9}$	216	$2^{18.8}$	$2^{15.9}$
	10	$2^{39.2}$	$2^{18.9}$	$2^{73,3}$	$2^{36.0}$	240	$2^{18.9}$	$2^{16.0}$
13	8	$2^{32.4}$	$2^{19.7}$	$2^{66,0}$	$2^{32.5}$	208	$2^{19.7}$	$2^{16.8}$
	9	$2^{35.9}$	$2^{19.9}$	2^{74}	$2^{33.4}$	234	$2^{19.9}$	$2^{16.9}$
	10	$2^{39.5}$	$2^{20.0}$	$2^{82,1}$	$2^{40.4}$	260	$2^{20.0}$	$2^{16.9}$
14	8	$2^{32.7}$	$2^{20.8}$	$2^{73,2}$	$2^{36.1}$	224	$2^{20.8}$	$2^{17.9}$
	9	$2^{36.2}$	$2^{21.0}$	$2^{82,1}$	$2^{37.0}$	252	$2^{21.0}$	$2^{17.9}$
	10	$2^{39.9}$	$2^{21.1}$	$2^{90,9}$	$2^{44.9}$	280	$2^{21.1}$	$2^{17.9}$
15	8	$2^{33.0}$	$2^{21.9}$	$2^{80,4}$	$2^{39.7}$	240	$2^{21.9}$	$2^{18.9}$
	9	$2^{36.5}$	$2^{22.1}$	$2^{90,2}$	$2^{40.6}$	270	$2^{22.1}$	$2^{19.0}$
	10	$2^{40.2}$	$2^{22.2}$	$2^{99,9}$	$2^{49.4}$	300	$2^{22.2}$	$2^{19.0}$
16	8	$2^{33.3}$	$2^{23.0}$	$2^{87,6}$	$2^{43.3}$	256	$2^{23.0}$	$2^{20.0}$
	9	$2^{36.8}$	$2^{23.2}$	$2^{98,3}$	$2^{44.2}$	288	$2^{23.2}$	$2^{20.0}$
	10	$2^{40.4}$	$2^{23.3}$	$2^{108,9}$	$2^{53.9}$	320	$2^{23.3}$	$2^{20.0}$
17	8	$2^{33.6}$	$2^{24.1}$	$2^{94,9}$	$2^{47.0}$	272	$2^{24.1}$	$2^{21.1}$
	9	$2^{37.1}$	$2^{24.3}$	$2^{106,5}$	$2^{47.9}$	306	$2^{24.3}$	$2^{21.1}$
	10	$2^{40.7}$	$2^{24.4}$	$2^{118,1}$	$2^{58,5}$	340	$2^{24.4}$	$2^{21.1}$
24	9	$2^{38.6}$	$2^{31.8}$	$2^{165,0}$	$2^{82,0}$	432	$2^{31.8}$	$2^{28.6}$
	10	$2^{42.2}$	$2^{31.9}$	$2^{183,0}$	$2^{91,0}$	480	$2^{31.9}$	$2^{28.6}$
	11	2^{46}	$2^{32.0}$	$2^{201,1}$	$2^{100,0}$	528	$2^{32.0}$	$2^{28.6}$
28	10	$2^{42.9}$	$2^{36.1}$	$2^{220,7}$	$2^{109.9}$	560	$2^{36.1}$	$2^{32.8}$
	11	$2^{46.6}$	$2^{36.3}$	$2^{242,5}$	$2^{110.9}$	616	$2^{36.3}$	$2^{32.8}$
	12	$2^{50.4}$	$2^{36.4}$	$2^{264,14}$	$2^{131.7}$	672	$2^{36.4}$	$2^{32.8}$

Анализируя данные табл. 3, следует отметить высокую стойкость ЭЦП по схеме CFS, которая, как и ожидалось, является и остается высокой к атакам квантового криптоанализа. Использование квантовых вычислений приводит к квадратичному снижению стойкости схемы CFS, т.е. сложность криптоанализа сопоставима с решением переборных задач поиска эквивалентных ключей симметричных шифров. По сравнению, например, с криптосистемой RSA (см. табл. 1), наблюдается очень быстрый рост стойкости.

В то же время очевидным недостатком схемы CFS является высокая сложность формирования ЭЦП. Даже для невысоких (по современным представлениям) уровней стойкости 2^{80} … 2^{90} формирование ЭЦП потребует порядка 10^9 … 10^{10} битовых операций. При этом, как следует из данных табл. 3, сложность формирования ЭЦП с рекомендованными авторами [29] параметрами двоичных кодов Гоппы, от 2^{14} до 2^{16} раз превышает сложность проверки (верификации) ЭЦП. Это объясняется большим числом попыток декодирования на шаге 5 алгоритма формирования ЭЦП, которые необходимо выполнить для нахождения такого положительного целого числа i, для которого выполнялось бы равенство (12). Отметим, что

сложность формирования ЭЦП снижается по мере улучшения кодовых соотношений используемого (n,k,d) кода и для совершенного кода, удовлетворяющего верхней кодовой границе Хемминга (10) оценка (13) примет вид $P_{у.д.}=1$. Тогда каждая попытка декодирования (для произвольного значения i) на шаге 5 алгоритма формирования ЭЦП приводила бы к успеху и не нужно было бы использовать параметр i. Однако построение длинных двоичных кодов (в том числе и сепарабельных кодов Гоппы), близких по своим кодовым соотношениям к верхней границе Хемминга, является открытой проблемой теории помехоустойчивого кодирования, которая в контексте развития схемы CFS приобретает особую актуальность.

Еще один недостаток схемы CFS, не отмеченный ранее в других работах, состоит в возможности быстрой подделки подписи $Y=(e,i)$ используя кодовые слова применяемого (n,k,d) кода. Действительно, если выбрать произвольное кодовое слово $c=(c_0,c_1,...,c_{n-1})$ используемого (n,k,d) кода с проверочной матрицей H_X, тогда очевидное равенство $H_X\cdot c^T=0$ приведет возможности гарантированно подделать подпись $Y_n=(e+c,i)$, причем равенство (12) будет также выполняться:

$$Y_n=(e+c,i):H_X\cdot(e+c)^T=H_X\cdot e^T+H_X\cdot c^T=H_X\cdot c^T=\left(h(h(M)\|i)\right)^T.$$

Для защиты от такой примитивной подделки в алгоритм верификации ЭЦП $Y=(e,i)$ необходимо добавить обязательную проверку веса Хемминга вектора e, т.е. шаг 3 необходимо переписать в виде:

Шаг 3. Принятие решение о *правильности* или *неправильности* ЭЦП:

- если $s'_X=s''_X$ и $w(e)\le t$ тогда принимается решение о *правильности* ЭЦП;
- если $s'_X\ne s''_X$ и (или) $w(e)>t$ тогда принимается решение о *неправильности* ЭЦП.

Указанное замечание может быть косвенно реализовано через применение алгоритма равновесного кодирования [14]. Так при формировании ЭЦП в сжатом виде $Y=(e^*,i)$ число всех возможных значений вектора e^* не превосходит $2^{m\cdot t}$, т.е. часть подделанного ЭЦП – вектор $e+c$ – не будет корректно преобразован в безызбыточную последовательность, и наоборот. Однако при такой организации схемы CFS для защиты от подделки подписи в алгоритм равновесного кодирования, например в алгоритм 2.2 [14, с. 99], необходимо внести возможность отказа в обработке с выдачей сообщения о некорректности введенных данных.

Выводы

Несимметричные криптосистемы на основе алгебраических блоковых кодов были предложены около 40 лет назад и воспринимались тогда большинством исследователей как некое экзотическое и малоприменимое направление в криптографии. Очевидные недостатки (огромные объемы ключевых данных и снижение относительной скорости передачи) в течение длительного времени сдерживали их дальнейшее развитие и практическое использование.

И только в последние годы, когда стало понятно, что многие существующие, стандартизированные и широко используемые на практике криптоалгоритмы могут оказаться беззащитными против атак квантового криптоанализа, кодовые криптосистемы получили заслуженное внимание исследователей. Декодирование случайного кода – чрезвычайно сложная вычислительная задача, и переборный поиск при ее решении, вероятно, является лучшим из известных вариантов. Квантовые алгоритмы ускоряют этот процесс, что снижает временные затраты криптоанализа, но это снижение не является критичным (примерно в два раза уменьшается эквивалентная длина ключа). Фактически следует признать, что кодовые криптосистемы являются реальной альтернативой современным несимметричным криптосистемам (RSA,

ECC, или других) в части построения надежных постквантовых алгоритмов. Приведенные в работе расчеты наглядно подтверждают этот вывод. Кроме того, особенности построения кодовых схем позволяют одновременно с криптозащитой реализовать дополнительную услугу контроля возникающих ошибок, что, безусловно, представляет интерес для их применения в телекоммуникационных системах специального назначения.

Для практического применения кодовых криптосистем необходимо решить (или смириться с их существованием) несколько конструктивных проблем и наиболее очевидная из них – огромные объемы ключевых данных. В связи с возможностью использования квантовых вычислительных систем эти объемы придется значительно увеличить (примерно в четыре раза). Например, для рассмотренных в статье вариантов объемы ключей достигают сотен мегабит и пока не представляется возможным их уменьшить без снижения стойкости криптосистемы. Ключи в кодовых схемах – это генераторные (порождающие и/или проверочные) матрицы линейного кода, которые должны выглядеть для злоумышленника как случайный набор линейно независимых векторов. Сжать или каким-то образом уменьшить этот набор без снижения стойкости не представляется возможным.

Очевидным недостатком схемы ЭЦП CFS является высокая сложность формирования подписи. Это объясняется большим числом попыток декодирования при формировании ЭЦП. По мере улучшения кодовых соотношений сложность формирования ЭЦП снижается и для совершенного кода, удовлетворяющего верхней кодовой границе Хемминга, достигается оптимальное значение. Таким образом, построение длинных двоичных кодов (в том числе и сепарабельных кодов Гоппы), близких по своим кодовым соотношениям к верхней границе Хемминга в контексте развития схемы CFS, приобретает особую актуальность. Повышение вычислительной эффективности схем формирования и проверка ЭЦП на основе кодов, оценка стойкости к современным методам криптоанализа являются перспективным направлением дальнейших исследований.

Список литературы: 1. *Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.* Handbook of Applied Cryptography – CRC Press, 1997. – 794 p. 2. *Standards* catalogue. 2016.URL:http://www.iso.org/iso/iso_catalogue catalogue_tc/ catalogue_detail.htm? csnumber=18199 3. *Arto Salomaa*. Public-Key Cryptography, Second, Enlarged Edition. – Springer-Verlag, Berlin, Heidelberg, New York, 1996. – x+271 pp. 4. *Nigel Smart*. Cryptography: An Introduction (3rd Edition). – 432 pp. https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf 5. *David Deutsch and Richard Jozsa.* Rapid solutions of problems by quantum computation // Proceedings of The Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 439, no. 1907. – 1992. – P. 553-558. 6. *Cleve R., Ekert A., Macchiavello C., Mosca M.* Quantum algorithms revisited // Proceedings of The Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 454, no. 1969. – 1998. – P. 339-354. 7. *Simon D. R*. On the power of quantum computation // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium. – P. 116-123. 8. *Grover L.* A fast quantum mechanical algorithm for database search // Proceedings of the 28th annual ACM symposium on the theory of computing (STOC, 96). ACM Press, New York. – 1996. – P. 212–219. 9. *Grover L.* A framework for fast quantum mechanical algorithms // Proceedings of the 13th annual ACM symposium on theory of computing (STOC' 98). ACM Press, New York. – 1998. – P. 53–62. 10. *Shor P. W*. Algorithms for quantum computation: discrete logarithms and factoring // Foundations of Computer Science : Conference Publications. – 1994. – P. 124-134. 11. *Shor P. W.* Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science: Conference Publications. – 1997. – P. 1484-1509. 12. *Neal Koblitz and Alfred J.* Menezes. A Riddle Wrapped in an Enigma. https://eprint.iacr.org/2015/1018.pdf 13. *Committee* on National Security Systems, Use of public standards for the secure sharing of information among national security systems, Advisory Memorandum 02-15, July 2015. https://cryptome.org/2015/08/CNSS_Advisory_Memo_02-15.pdf 14. *Bernstein, Daniel J., Buchmann, Johannes, and Dahmen, Erik.* Post-Quantum Cryptography. – 2009, Springer-Verlag, Berlin-Heidleberg. – 245 p. 15. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, Jet Propulsion Lab., Pasadena, CA, January-February, 1978. P. 114-116. 16. *Niederreiter H.* Knapsack-type cryptosystems and algebraic coding theory // Problem Control and Inform Theory. – 1986. – V. 15. – P. 19-34. 17. *T. R. N. Rao and K. H. Nam*. Private-key algebraic-coded cryptosystem. Advances in Cryptology –

CRYPTO 86, New York. – NY: Springer. – P. 35–48. 18. *Yu. V. Stasev, A. A. Kuznetsov.* Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes // Cybernetics and Systems Analysis, Volume 41, Issue 3, May 2005, Pages 354 – 363. 19. *Сидельников В.М.* Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22 с. 20. *Сидельников В.М., Шестаков С.О.* О системе шифрования, построенной на основе обобщенных кодов Рида – Соломона // Дискретная математика. – 1992. – Т.4., №3. – С.57-63. 21. *Gorbenko I.D., Zamula A.A., Semenko Ye.A*. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. – Volume 75, 2016 Issue 2. pages 169-178. 22. *Кузнецов А.А.* Исследование эффективности криптосистем на алгебраических блоковых кодах // Системи обробки інформації. – Харків : ХУ ПС. – 2005 – Вип. 4. – С. 202 –206. 23. *Кузнецов А.А.* Исследование помехоустойчивости и криптостойкости теоретико-кодовых схем // Моделювання та інформаційні технології. – Київ: НАНУ. – 2005. – №33. – С. 81-84. 24. *Fisher Jean-Dernard , Jacques Stern.* An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding / Jean-Dernard Fisher , Stern Jacques // EUROCRYPT'96 Proceeding, LNCS 1070. P. 245 – 255. 25. *Oliynykov R., Gorbenko I., Dolgov V., Kaidalov D.* Improvement for distinguisher efficiency of the 3-round Feistel network and a random permutation // Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS'2011, 2011, pp 743 – 746. 26. *Gaborit, P., Laudaroux, C., and Sendrier, N.* Synd: a very fast code-based cipher stream with a security reduction. In IEEE Conference, ISIT'07, pages 186–190. 27. *Kirill Morozov, Tsuyoshi Takagi*. Zero-Knowledge Protocols for the McEliece Encryption // Information Security and Privacy Volume 7372 of the series Lecture Notes in Computer Science pp 180-193. 28. *Gorbenko, I.D., Dolgov, V.I.,Rublinetskii, V.I.,Korovkin, K.V.* Methods of Information Protection in Communications Systems and Methods of Their Cryptoanalysis // Telecommunications and Radio Engineering. – Volume 52, 1998 Issue 4. pages 89-96. 29. *Courtois, N., Finiasz, M., and N.Sendrier*: How to achieve a McEliece-based digital signature scheme. In Advances in Cryptology – ASIACRYPT 2001, volume 2248, pages 157–174. 30. *Finiasz, M.* Parallel-CFS: Strengthening the CFS McEliece-based signature scheme. In Biryukov, A., Gong, G., Stinson, D., eds.: Selected Areas in Cryptography. Volume 6544 of LNCS., Springer (2010). – 159 -170. 31. *Stern, J.* A new identification scheme based on syndrome decoding. In Advances in Cryptology – CRYPTO'93, volume 773 of LNCS. Springer Verlag (1994). 32. *Veron, P.* Improved identification schemes based on error-correcting codes. Appl. Algebra Eng. Commun. Comput., 8(1):57–69 (1996). 33. *Anne Canteaut and Nicolas Sendrier*. Cryptanalysis of the original McEliece cryptosystem. In Kazuo Ohta and Dingyi Pei, editors, Advances in cryptology— ASIACRYPT'98, volume 1514 of Lecture Notes in Computer Science, pages 187– 199. 34. *Vladimir M. Sidelnikov and Sergey O. Shestakov*. On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Mathematics and Applications, 1992. – 439-444. 35. *Minder L., Shokrollahi A.* Cryptanalysis of the Sidelnikov Cryptosystem // Advances in Cryptology – EUROCRYPT 2007: 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007. Proceedings – Springer Berlin Heidelberg, 2007. – P. 347-360. 36. *Daniel J. Bernstein and Tanja Lange and Christiane Peters.* Attacking and defending the McEliece cryptosystem. https://cr.yp.to/codes/mceliece-20080807.pdf 37. *E. Berlekamp, R. McEliece, H. van Tilborg*. On the Inherent Intractability of Certain Coding Problems // IEEE Transactions on Information Theory, vol. IT-24, No. 3, May 1978. – P. 384-386. 38. *Clark G.C., Cain J.B.* Error-Correction Coding for Digital Communications. – Springer, 1981, – 432 p. 39. *Blahut R. E.* Theory and Practice of Error Control Codes. – Addison Wesley Publishing Company, Inc., Reading, Massachusetts, 1983, 1983. – 500 p. 40. *F. J. MacWilliams and N. J. A. Sloane*. The theory of error-correcting codes. – North-Holland, Amsterdam, New York, Oxford, 1977, – 762 pp. 41. *Claude E. Shannon*. Communication in the Presence of Noise. Proceedings of the IRE, vol. 37, no. 1, pp. 10–21, Jan. 1949. 42. *Гонна В. Д.* Новый класс линейных корректирующих кодов // Проблемы передачи информации. – 1970. – Т. 6, вып.3. – С. 24-30. 43. *Гонна В. Д.* На неприводимых кодах достигается пропускная способность ДСК // Проблемы передачи информации. – 1974. – Т.10, вып. 1. – С. 111–112. 44. *National* Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard", November 2001: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf 45. *A New* Encryption Standard of Ukraine: The Kalyna Block Cipher. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. https://eprint.iacr.org/2015/650.pdf 46. *Raphael Overbeck, Nicolas Sendrier* Code-based cryptography. In: Daniel J. Bernstein, et al. (eds). First International Workshop on Post-quantum Cryptography, PQ Crypto 2006, Leuven, The Netherland, May 23-26, 2006. Selected papers, pp. 95-145. 47. *D. J. Bernstein.* Grover vs. McEliece. In N. Sendrier, editor, Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Pro-

ceedings, volume 6061 of Lecture Notes in Computer Science, pages 73–80. Springer, 2010. 48. *A. Menezes, P. van Oorschot, S. Vanstone*. Chapter 14. Efficient Implementation // Handbook of Applied Cryptography. – CRC-Press, 1996. – 816 p. 49. *Kerry Maletsky*. RSA vs ECC Comparison for Embedded Systems. White Paper. Atmel Corporation – 2015. – 5p. http://www.atmel.com/images/atmel-8951-cryptoauth-rsa-ecc-comparison-embedded-systems-whitepaper.pdf 50. *John Proos and Christof Zalka.* Shor's discrete logarithm quantum algorithm for elliptic curves. arXiv.quant-ph/0301141 v2, 2004. 51. *Ziatdinov M.* Using frequency analysis and Grover's algorithm to implement known ciphertext attack on symmetric ciphers // Lobachevskii Journal of Mathematics. – 2013. – Vol.34 N4. – P. 313-315. 52. *Метод* недвійкового рівновагового кодування / В. Б. Дудикевич, О. О. Кузнєцов, Б. П. Томашевський // Сучасний захист інформації. – 2010. – № 3. – С. 57-68. http://nbuv.gov.ua/UJRN/szi_2010_3_10 53. *Tietavainen A., Perko A.* There are no unknown perfect binary codes. – Annales Universitatis Turkuensis. – Ser. A, I 148, 3-10[6], 1971. 54. *Lint van J. H.* Nonexistence theorems for perfect error-correcting codes. – Computers in Algebra and Number Theory. – Vol. IV [6], 1971.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 15.09.2016