УДК 004.056.55

А.А. КУЗНЕЦОВ, д-р техн. наук, А.И. ПУШКАРЕВ, А.С. КИЯН

АЛГОРИТМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ АЛГЕБРАИЧЕСКОГО КОДИРОВАНИЯ

Введение

Электронная цифровая подпись (ЭЦП) является цифровым эквивалентом подписи (печати, штампа и пр.), наличие которого в сообщении позволяет с высокой точностью определить источник сообщения (документа) и юридически доказать, что, с определенной вероятностью, только он мог создать и подписать этот документ [1 – 3].

Для формирования ЭЦП на сегодняшний день используются криптографические механизмы и протоколы [4 – 10], в которых задача поиска секретного ключа по известному открытому ключу связана с решением известной и чрезвычайно сложной математической задачи (например, факторизации, дискретного логарифмирования, дискретного логарифмирования в группе точек эллиптической кривой) [1 – 3]. Однако квантовые вычисления позволяют существенно ускорить решение многих математических задач [11 – 20], в том числе лежащих в основе современных алгоритмов ЭЦП [20]. Например, алгоритм Шора (Shor) позволяет найти за приемлемое время все простые множители в системе RSA, т.е. найти секретный ключ и/или подделать ЭЦП без знания секретного ключа [16].

Появление квантовых компьютеров анонсировано на ближайшие 10 – 15 лет [21, 22]. По этой причине Национальный Институт Стандартов и Технологий (NIST) США в конце 2016 г. объявил открытый конкурс (http://csrc.nist.gov/groups/ST/post-quantum-crypto/) с целью принятия в течение пяти-семи лет новых постквантовых криптостандартов [22]. В этом смысле разработка, исследование и обоснование рекомендаций по практическому использованию новых криптосистем, устойчивых к квантовому криптоанализу, т.е. на постквантовый период (Post-Quantum Cryptography), имеет особую актуальность и востребованность [20 – 22].

Одно из направлений в развитии постквантовой криптографии основывается на использовании алгебраических блоковых кодов (Code-based Cryptography) [20, 21, 23 – 31]. При этом обеспечивается высокая скорость криптографического преобразования, стойкость к классическому и квантовому криптоанализу, а также возможность дополнительного контроля возникающих ошибок [28 – 30].

В основе построения кодовых криптосистем лежит использование специальных маскирующих матриц, которые выступают в качестве секретного ключа и, по предположению, надежно скрывают алгебраическую структуру кода [26]. Злоумышленник, не зная секретного ключа, не может воспользоваться алгебраическим алгоритмом декодирования (полиномиальной сложности) и вынужден декодировать кодовое слово, решая NP-сложную задачу [32].

В данной статье рассматриваются наиболее известные кодовые криптосистемы Мак-Элиса и Нидеррайтера [23, 24], а также схема CFS (Courtois, Finiasz, Sendrier) [31] для формирования и проверки ЭЦП. Предлагается новая схема ЭЦП с использованием алгебраических кодов, приводятся сравнительные оценки эффективности по различным показателям (стойкость, сложность формирования и проверки ЭЦП, объемы ключевых данных, длина подписи и пр.).

Кодовые криптосистемы Мак-Элиса и Нидеррайтера

В 1978 г. Мак-Элисом (McEliece) была предложена первая криптосистема на алгебраических блоковых кодах [23]. В ее основе лежит маскирование быстрого правила декодирования посредством матричного умножения порождающей матрицы алгебраического блокового кода на случайные невырожденные матрицы (секретный ключ). Полученный результат (открытый ключ) представляет собой порождающую матрицу, имеющую вид случайно выбран-

ных линейно независимых векторов. Злоумышленник, имеющий только открытый ключ, вынужден использовать сложный алгоритм неалгебраического декодирования (NP-полная задача). Уполномоченный пользователь, знающий секретный ключ, снимает действие маскирования и применяет быстрый алгебраический алгоритм декодирования (полиномиально разрешимая задача).

Введем необходимые обозначения и определения.

Зафиксируем конечное поле $GF(q)$. Пусть G – порождающая матрица алгебраического (n,k,d) кода над $GF(q)$ (в оригинальной статье предлагалось использовать двоичные сепарабельные коды Гоппы), X – невырожденная $k\times k$ матрица с элементами из $GF(q)$, P и D – перестановочная и диагональная $n\times n$ матрицы, соответственно (для двоичных кодов используется только матрица P). Матрица

$$G_X = X\cdot G\cdot P\cdot D$$

является открытым ключом, маскирующие матрицы X, P и D являются секретным ключом. Криптограммой является искаженное ошибкой e кодовое слово

$$c_X^* = I\cdot G_X + e, \tag{1}$$

причем вес Хемминга вектора ошибок $w_h(e)$ удовлетворяет ограничению

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

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 $GF(q)$. 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 $w_h(e)=t$ обеспечивается наивысший уровень стойкости кодовой криптосистемы для заданных параметров n,k,q. Уполномоченный пользователь, получив вектор c_X^*, строит вектор $\bar{c}^* = c_X^*\cdot D^{-1}\cdot P^{-1}$. Используя алгоритм полиномиальной сложности, он декодирует вектор $\bar{c}^* = I'\cdot G + e'$, т.е. находит I'. Затем он вычисляет k-разрядный информационный вектор $I = I'X^{-1}$.

Другим важным примером кодовых криптосистем является схема Нидеррайтера (Niederreiter) [24]. Открытым ключом в этой криптосистеме есть матрица

$$H_X = X\cdot H\cdot P\cdot D,$$

где H – проверочная матрица алгебраического (n,k,d) кода над $GF(q)$ (в оригинальной статье 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 H_X 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 $(n-k)$ и вычисляется по правилу

$$s_X = e\cdot H_X^T, \tag{2}$$

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 – суть 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 [20]. Сперва заметим, что выражение (2) можно переписать в виде

$$s_X{}^T = H_X \cdot e^T . \qquad (3)$$

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

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

В работах [33 – 38] исследованы свойства кодовых криптосистем Мак-Элиса и Нидеррайтера, приведены оценки стойкости, в том числе к квантовому криптоанализу, показано, что относительная скорость передачи данных для наиболее важных с прикладной точки зрения случаев существенно ниже единицы. Предложена новая криптосистема, которая позволяет существенно (на 30 – 40 %) повысить относительную скорость передачи информации.

ЭЦП на основе алгебраических кодов

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

В **схеме CFS** для формирования ЭЦП реализуется многократное хеширование информационного сообщения, рандомизированного счетчиком битовой длины r, до тех пор, пока не будет получен правильно выделенный (допускающий декодирование) синдром. Уполномоченный пользователь использует 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 [31].

1. Генерация общесистемных параметров: выбираются положительные целые числа m, t.

2. Генерация ключа: формируются пары ключей как в криптосистеме Нидеррайтера на основе алгебраического кода из класса ($n = 2^m$, $k = n - mt$, $2t + 1$) двоичных кодов Гоппы. Для этого формируются:

– 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;

Открытым ключом является матрица $H_X = X \cdot H \cdot P$ и число t (исправляющая способность кода).

Секретным ключом являются матрицы H, X и P, а также связанный с матрицей H 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 [20, 31]

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 (3) 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^*. В этом случае переменной i присваивается значение $i = i + 1$ и осуществляется 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:

$$Y = (e, i) : H_X \cdot e^T = h(h(M)\|i)^T. \quad (4)$$

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 ЭЦП по схеме CFS) [20, 31]

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.

В работах [34, 39 – 41] приведены оценки конструктивных характеристик схемы CFS, исследована эффективность криптосистемы по показателям стойкости, сложности формирования и проверки ЭЦП, объемам ключевых данных, длине подписи и пр. Выявлен существенный недостаток схемы CFS, не отмеченный ранее в других работах, который состоит в возможности быстрой подделки подписи $Y = (e, i)$ используя кодовые слова применяемого (n, k, d) кода. Обоснованы рекомендации для защиты от такой подделки. В частности, 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 $s'_X \neq s''_X$ и (или) $w(e) > t$ тогда принимается решение о *неправильности* ЭЦП.

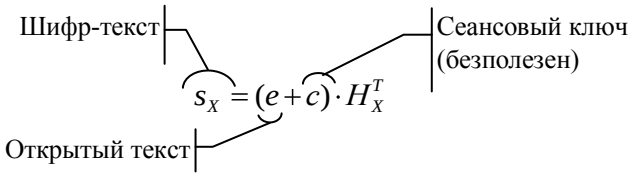
Дополнительная проверка веса Хемминга вектора e позволяет защититься от подделки подписи на основе добавления произвольного кодового слова.

Рассмотренная схема ЭЦП CFS основана на использовании кодовой криптосистемы Нидеррайтера. С момента публикации авторской статьи [31] (т.е. уже более 15 лет) предполагается, что это единственный возможный вариант ЭЦП на алгебраических кодах [20]. В данной работе предлагается новая схема ЭЦП, которая построена на использовании кодовой криптосистемы Мак-Элиса. По своим основным параметрам (стойкости, длине ключа и длине подписи) она сопоставима со схемой ЭЦП CFS.

Предлагаемая схема формирования и проверки ЭЦП. Для наглядной демонстрации принципов построения схемы CFS и предлагаемой схемы ЭЦП на рис. 1 приведены основные аналитические соотношения, связывающие открытый и шифр-текст в кодовых криптосистемах Мак-Элиса и Нидеррайтера, а также их интерпретации, используемые для формирования и проверки подписи.

В криптосистеме Нидеррайтера [24] информационное сообщение в виде равновесной последовательности e умножается на открытый ключ – матрицу H_X, что в теории кодирования эквивалентно нахождению синдрома s_X, который однозначно определяется вектором e. Уполномоченный пользователь, знающий секретные матрицы X и P в $H_X = X \cdot H \cdot P$, сможет применить быстрый (полиномиальной сложности) алгоритм декодирования для нахождения вектора e. Без знания матриц X и P неуполномоченный пользователь вынужден использовать сложный алгоритм декодирования случайного кода, для которого достаточно использовать матрицу H_X. Таким образом, в схеме Нидеррайтера для реализации асимметричного шифрования используется т.н. «односторонняя функция», кода вычислить s_X по известным H_X и e вычислительно легко (полиномиальная сложность), а найти e по известным H_X и s_X чрезвычайно сложно (NP-полная задача).

Криптосистема Нидеррайтера:

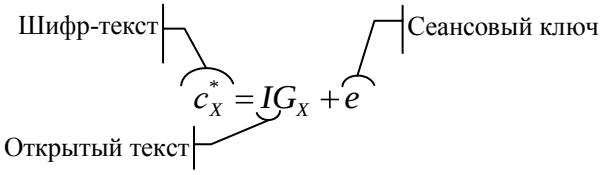


Односторонняя функция:

– для вычисления s_X (синдромной последовательности) по известному e требуется алгоритм полиномиальной сложности;

– для вычисления e по известному s_X (без знания алгебраической структуры кода) требуется алгоритм декодирования случайного кода (NP-сложная задача);

Криптосистема Мак-Элиса:



Односторонняя функция:

– для вычисления c_X^* (кодового слова со случайно сформированной ошибкой) по известным I и e требуется алгоритм полиномиальной сложности;

– для вычисления I и (или) e по известному c_X^* (без знания алгебраической структуры кода) требуется алгоритм декодирования случайного кода (NP-сложная задача);

CFS-схема ЭЦП:

Хеш-образ $s_X = h(h(M)\|i)$, вычисленный по подписываемому сообщению M и значению счетчика i, интерпретируется как синдромная последовательность;

Зная секретный ключ (алгебраическую структуру кода), уполномоченный пользователь использует алгоритм полиномиальной сложности для быстрого нахождения вектора e. Если декодирование не успешно, тогда выбирается другое значение счетчика i и процедура повторяется;

Найденные значения e и i являются частями ЭЦП $Y = (e, i)$ сообщения M. При этом обязательно выполняется равенство:

$$Y = (e, i) : H_X \cdot e^T = h(h(M)\|i)^T,$$

которое лежит в основе процедуры проверки (верификации) ЭЦП.

Предлагаемая схема ЭЦП:

Хеш-образ $c_X^* = h(h(M)\|i)$, вычисленный по подписываемому сообщению M и значению счетчика i, интерпретируется как кодовое слово со случайно сформированной ошибкой;

Зная секретный ключ (алгебраическую структуру кода) уполномоченный пользователь использует алгоритм полиномиальной сложности для быстрого нахождения векторов I и e. Если декодирование не успешно, тогда выбирается другое значение счетчика i и процедура повторяется;

Найденные значения I, e и i являются частями ЭЦП $Y = (I, e, i)$ сообщения M. При этом обязательно выполняется равенство:

$$Y = (I, e, i) : IG_X + e = h(h(M)\|i),$$

которое лежит в основе процедуры проверки (верификации) ЭЦП.

Рис. 1. Кодовые криптосистемы и схемы ЭЦП на их основе

В схеме ЭЦП CFS [31] используется односторонняя функция из схемы Нидеррайтера, но только для формирования и проверки ЭЦП. Для этого подписываемое информационное сообщение M (его сжатый образ) непосредственно связывается со значением синдрома s_X и только уполномоченный пользователь, знающий секретные матрицы X и P в $H_X = X \cdot H \cdot P$, сможет применить быстрый (полиномиальной сложности) алгоритм декодирования для нахождения вектора e. Этот найденный вектор совместно со вспомогательной информацией (значение счетчика i) и составляют подпись $Y = (e, i)$ сообщения M. Для проверки (верификации) подписи достаточно владеть открытым ключом (матрицей H_X) – для этого достаточно вычислить синдром s_X и сравнить его с сжатым образом информационного сообщения. Таким образом, для формирования и проверки ЭЦП используется односторонняя функция из схемы Нидеррайтера: вычислить s_X по известным H_X и e (проверить ЭЦП) вычислительно легко (полиномиальная сложность), а найти e по известным H_X и s_X (сформировать ЭЦП) чрезвычайно сложно (NP-полная задача).

В криптосистеме Мак-Элиса [23] информационное сообщение M рассматривается как информационный вектор I, подлежащий избыточному кодированию. Кодовое слово вычисляется через произведение $c_X = I \cdot G_X$, где порождающая матрица $G_X = X \cdot G \cdot P$ представляет собой открытый ключ, а матрицы X и P – секретный (закрытый) ключ. Шифрограмма $c_X^* = I \cdot G_X + e$ представляет собой кодовое слово c_X с добавленным к нему случайным вектором ошибки e. Уполномоченный пользователь, знающий секретные матрицы X и P в $G_X = X \cdot G \cdot P$, сможет применить быстрый (полиномиальной сложности) алгоритм декодирования для нахождения векторов I и e. Без знания матриц X и P неуполномоченный пользователь вынужден использовать сложный алгоритм декодирования случайного кода, для которого достаточно использовать лишь матрицу G_X. Таким образом, в схеме Мак-Элиса для реализации асимметричного шифрования используется следующая одностороння функция: вычислить c_X^* по известным G_X, I и e вычислительно легко (полиномиальная сложность), а найти I и e по известным G_X и c_X^* чрезвычайно сложно (NP-полная задача).

Предлагаемая схема формирования и проверки ЭЦП использует одностороннюю функцию из схемы Мак-Элиса. Для этого подписываемое информационное сообщение M (его сжатый образ) непосредственно связывается со значением c_X^* и только уполномоченный пользователь, знающий секретные матрицы X и P в $G_X = X \cdot G \cdot P$, сможет применить быстрый (полиномиальной сложности) алгоритм декодирования для нахождения векторов I и e. Эти векторы совместно со вспомогательной информацией (значение счетчика i) составляют подпись $Y = (I, e, i)$ сообщения M. Для проверки (верификации) подписи достаточно владеть открытым ключом (матрицей G_X) – для этого достаточно вычислить c_X^* и сравнить его с сжатым образом информационного сообщения. Таким образом, вычислить c_X^* по известным G_X, I и e (проверить ЭЦП) вычислительно легко (полиномиальная сложность), а найти I и e по известным G_X и c_X^* (сформировать ЭЦП) чрезвычайно сложно (NP-полная задача).

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

1. Генерация общесистемных параметров: выбираются положительные целые числа m, t.

2. Генерация ключа: формируются пары ключей как в криптосистеме Нидеррайтера на основе алгебраического кода из класса $(n, k, d = 2t + 1)$ кодов. В частном случае может использоваться код из класса $(n = 2^m, k = n - mt, 2t + 1)$ двоичных кодов Гоппы.

Для этого формируются:

– матрица $G: k \times n$ – порождающая матрица алгебраического кода с исправляющей способностью t ошибок,

– матрица $X: k \times k$ – случайная обратимая матрица,

– матрица $P: n \times n$ – случайная матрица перестановок.

В случае применения недвоичных кодов используется также матрица $D: n \times n$ – случайная диагональная матрица. Если код двоичный, тогда под D в дальнейшем будем понимать единичную матрицу.

Открытым ключом является матрица $G_X = X \cdot G \cdot P \cdot D$ и число t (исправляющая способность кода).

Секретным ключом являются матрицы G, X, P и D, а также связанный с матрицей G быстрый (полиномиальной сложности) алгоритм декодирования алгебраического кода.

Алгоритм декодирования позволяет по введенному кодовому слову с ошибками $c^*_X = (c^*_0, c^*_1, ..., c^*_{n-1})$ в случае успеха декодирования найти вектор ошибок $e = (e_0, e_1, ..., e_{n-1})$ и вектор $I = (I_0, I_1, ..., I_{k-1})$, причем $c^*_X = I \cdot G_X + e$. В противном случае (если декодирование не удалось) алгоритм выдает отказ в декодировании вектора $c^*_X = (c^*_0, c^*_1, ..., c^*_{n-1})$, т.е. по такой последовательности алгоритм не может найти вектор ошибок $e = (e_0, e_1, ..., e_{n-1})$ и вектор $I = (I_0, I_1, ..., I_{k-1})$.

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 кодовых символов (для двоичных кодов – n бит);

2. Быстрый (полиномиальной сложности) алгоритм декодирования алгебраического кода, который применяется к кодовому слову с ошибками $c^*_X = (c^*_0, c^*_1, ..., c^*_{n-1})$. Предполагается, что в результате выполнения алгоритма декодирования возможны две ситуации:

– если декодирование успешно – выводятся векторы $e = (e_0, e_1, ..., e_{n-1})$ и $I = (I_0, I_1, ..., I_{k-1})$, которые соответствует вектору $c^*_X = (c^*_0, c^*_1, ..., c^*_{n-1})$;

– если декодирование не успешно – выдается сообщение о невозможности найти векторы $e = (e_0, e_1, ..., e_{n-1})$ и $I = (I_0, I_1, ..., I_{k-1})$ для введенного вектора $c^*_X = (c^*_0, c^*_1, ..., c^*_{n-1})$;

3. Открытый текст M, для которого необходимо сформировать ЭЦП.

Выход:

ЭЦП Y для открытого текста M.

Предлагаемый алгоритм формирования ЭЦП

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 двух последовательностей;

Шаг 3. Значение $h(h(M)\|i)$ интерпретируется как кодовое слово с ошибками $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$, вычисленное для некоторых $I = (I_0, I_1, ..., I_{k-1})$ и $e = (e_0, e_1, ..., e_{n-1})$, причем $c = IG_X$, $c_X^* = c + e$, т.е. предполагается выполнение равенства (19) для соответствующего открытого ключа $G_X = X \cdot H \cdot P \cdot D$;

Шаг 4. Вычисление значения вектора

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1},$$

который (как предполагается) представляет собой искаженное не более чем в t разрядах кодовое слово алгебраического (n, k, d) кода с порождающей матрицей G и его можно декодировать быстрым алгоритмом полиномиальной сложности, т.е. предполагается, что

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1} = (I \cdot G_X + e) \cdot D^{-1} \cdot P^{-1} = (I \cdot X \cdot H \cdot P \cdot D + e) \cdot D^{-1} \cdot P^{-1} = I \cdot X \cdot H + e \cdot D^{-1} \cdot P^{-1}$$

и алгоритм быстрого декодирования позволит найти вектор $I' = I \cdot X$ посредством декодирования слова $\bar{c}^* = I' \cdot G + e'$, $e' = e \cdot D^{-1} \cdot P^{-1}$;

Шаг 5. Для слова $\bar{c}^* = I' \cdot G + e'$ реализуется выполнение быстрого алгоритма декодирования:

– если декодирование успешно – выводятся найденные векторы $I' = I \cdot X$ и $e' = e \cdot D^{-1} \cdot P^{-1}$, которые соответствует вектору $\bar{c}^* = I' \cdot G + e'$;

– если декодирование не успешно – выдается сообщение о невозможности найти векторы $I' = I \cdot X$ и $e' = e \cdot D^{-1} \cdot P^{-1}$ для введенного вектора $\bar{c}^*$. Присваивание переменной i значения $i = i + 1$ и переход на Шаг 2;

Шаг 6. Вычисление векторов

$$I = I' X^{-1} \text{ и } e = e' \cdot D \cdot P;$$

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

Таким образом, в результате выполнения рассмотренного алгоритма формирования ЭЦП, вычисляется такое наименьшее положительное целое число i, для которого значение $h(h(M)\|i)$, интерпретируемое как кодовое слово с ошибками c_X^*, соответствует кодовому слову $c = IG_X$ и вектору ошибок e, т.е. формально запишем:

$$Y = (I, e, i) : IG_X + e = h(h(M)\|i) \ . \qquad (5)$$

Задача вычисления векторов I и e 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 $Y = (I, e, i)$ сообщения M) необходимо убедиться в том, является ли результат хеширования $h(h(M)\|i)$ кодовым словом с ошибками c_X^*, вычисленным по векторам I и e.

4. Верификация

Ввод:

1. Открытый ключ (матрица $G_X = X \cdot H \cdot P \cdot D$ и число t);

2. Функция хеширования h;

3. ЭЦП $Y = (I, e, i)$;

4. Открытый текст M.
Выход:
решение о *правильности* или *неправильности* ЭЦП.

Предлагаемый алгоритм верификации (алгоритм проверки ЭПЦ)

Шаг 1. Вычисление вектора

$$c_X^{*}{}' = IG_X + e;$$

Шаг 2. Вычисление вектора

$$c_X^{*}{}'' = h(h(M)\|i);$$

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

– если $c_X^{*}{}' = c_X^{*}{}''$ и $w(e) \le t$ тогда принимается решение о *правильности* ЭЦП;

– если $c_X^{*}{}' \ne c_X^{*}{}''$ и (или) $w(e) > t$ тогда принимается решение о *неправильности* ЭЦП.

Отметим, что предлагаемая процедура верификации защищена от быстрой подделки подписи $Y = (I, e, i)$ на основе добавления произвольного кодового слова применяемого (n, k, d) кода (предложена и подробно рассмотрена в работе [34]). Так, если выбрать произвольное кодовое слово $\hat{c}$ используемого (n, k, d) кода с порождающей матрицей G_X, тогда можно попытаться подделать подпись $Y = (I, e + \hat{c}, i)$. Однако равенство (5) не будет выполняться:

$$Y = (I, e + \hat{c}, i) : IG_X + e + \hat{c} \ne h(h(M)\|i) \ .$$

Это очевидное преимущество предлагаемой схемы ЭЦП дополнительно усилено введенной проверкой веса вектора e, которая предназначена для защиты от других гипотетических атак (например, одновременной подделки и вектора I и вектора e).

Оценим конструктивные характеристики предлагаемой схемы формирования и проверки ЭЦП с использованием алгебраических кодов. При оценке будем предполагать, что используются двоичные сепарабельные коды Гоппы с параметрами [42, 43]:

$$n = 2^m, k = n - mt, t = deg\, G(x), d \ge 2t + 1, \qquad (6)$$

где $G(x)$ – многочлен Гоппы, $deg\, G(x)$ – степень многочлена $G(x)$.

Сложность формирования и проверки ЭЦП. Наиболее затратной частью алгоритма формирования ЭЦП является Шаг 5, на котором выполняется многократная попытка декодирования до достижения успеха. Оценим вероятность успеха декодирования, покажем, что сложность формирования ЭЦП предлагаемым способом сопоставима со схемой CFS [31].

При использовании (n, k, d) кода над $GF(q)$ на вход декодера поступает кодовое слово с ошибками

$$\bar{c}^{*} = I' \cdot G + e'$$

длины n символов из $GF(q)$, причем k-символьный вектор I' может принимать одно из q^k значений, а вектор e' – одно из

$$N = \sum_{i=0}^{t} (q-1)^i C_n^i, \ C_n^i = \frac{n!}{i!(n-i)!}$$

значений (т.к. $w(e') \le t$). Следовательно, число возможных значений вектора $\bar{c}^{*}$ равно $q^k \cdot N$, а общее число возможных n-символьных векторов с элементами из $GF(q)$ определяется как q^n. Тогда вероятность успеха декодирования для единичной попытки на шаге 5:

$$P_{у.д.} = \frac{q^k \cdot \sum_{i=0}^{t} (q-1)^i C_n^i}{q^n} = \frac{\sum_{i=0}^{t} (q-1)^i C_n^i}{q^{n-k}}, \quad (7)$$

что для двоичного случая

$$P_{у.д.} = \frac{\sum_{i=0}^{t} C_n^i}{2^{n-k}} \quad (8)$$

совпадает с аналогичным выражением из [31, с. 163]. При этом, по мере улучшения кодовых соотношений сложность формирования ЭЦП снижается. Так, для совершенного линейного (n,k,d) кода над $GF(q)$, удовлетворяющего верхней кодовой границе Хемминга [44]

$$q^k \le \frac{q^n}{\sum_{i=0}^{t} (q-1)^i C_n^i}, \quad (9)$$

вероятность успеха декодирования будет равна единице.

С учетом кодовых соотношений (6) для двоичных кодов Гоппы и аппроксимации [31]

$$\sum_{i=0}^{t} C_n^i = \frac{n^t}{t!}$$

оценка (8) примет вид

$$P_{у.д.} = \frac{\sum_{i=0}^{t} C_n^i}{2^{n-k}} = \frac{\frac{n^t}{t!}}{n^t} = \frac{1}{t!}, \quad (10)$$

что совпадает с аналогичным выражением из [31, с. 163] для схемы ЭЦП CFS.

Таким образом, успех в декодировании (на шаге 5 алгоритма формирования ЭЦП) будет достигнут при реализации в среднем после $t!$ попыток. Для двоичных кодов Гоппы каждая попытка требует $t^2 \cdot m^3$ двоичных операций [20, 31], т.е. среднее число битовых операций, которые необходимо затратить для формирования ЭЦП как по схеме CFS, так и по предлагаемой схеме, определяется как

$$N_{ф.п.} = t^2 \cdot m^3 \cdot t!. \quad (11)$$

В (11) не учтены затраты на формирование хеш-кодов (шаги 2 и 3 алгоритма формирования ЭЦП), а также операции с матрицами маскирования X и P (на шагах 4 и 6 алгоритма).

Для проверки (верификации) ЭЦП $Y = (I,e,i)$ необходимо вычислить хеш-код $h(h(M)\|i)$ и сравнить его с результатом вычисления $IG_X + e$. Если не учитывать сложность хеширования, тогда сложность проверки ЭЦП будет определяться выражением

$$N_{п.п.} = k \cdot n = m \cdot t \cdot 2^m. \quad (12)$$

Стойкость ЭЦП. В работе [26] показано, что стойкость несимметричных криптосистем Мак-Элиса и Нидеррайтера эквивалентна. Если принять предположение о тождественности оценок стойкости соответствующих ЭЦП (по схеме CFS и по предлагаемой схеме), тогда следует использовать формулы (17) и (18) из работы [34].

Длина ЭЦП. Цифровая подпись $Y = (I,e,i)$ состоит из трех частей: вектора I длиной k бит, вектора e длиной n бит и целого числа i, которое может принимать значение в диапазоне $0,1,..,q^{n-k}-1$ (после q^{n-k} попыток будет гарантирован успех в декодировании на Шаге 5 алгоритма формирования ЭЦП). Таким образом, при использовании двоичных кодов битовая длина ЭЦП (записанной в виде последовательности (I,e,i)) будет определяться выражением

$$l_{ЭЦП} = 2 \cdot n = 2^{m+1}. \quad (13)$$

При этом вектор e может быть преобразован в безызбыточную последовательность e^* длины $\lceil \log_2(N_{w(e)\le t}) \rceil$ бит. С учетом безызбыточного кодирования вектора e^* выражение (13) для длины ЭЦП $Y = (I, e^*, i)$ перепишем в виде

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

Используя выражение (9) для верхней границы Хемминга получим:

$$l_{ЭЦП}^* \le \left\lceil \log_2 \; 2^{n-k} \right\rceil + n = m \cdot t + 2^m . \qquad (14)$$

m	t	Криптосистема Нидеррайтера (ЭЦП по схеме CFS)			Криптосистема Мак-Элиса (ЭЦП по предложенной схеме)		
		$l_{ЭЦП}^*$	$l_{о.к.}$	$l_{з.к.}$	$l_{ЭЦП}^*$	$l_{о.к.}$	$l_{з.к.}$
10	10	200	102400	20240	1124	946176	864016
	20	400	204800	50240	1224	843776	689216
	30	600	307200	100240	1324	741376	534416
	40	800	409600	170240	1424	638976	399616
	50	1000	512000	260240	1524	536576	284816
	60	1200	614400	370240	1624	434176	190016
	70	1400	716800	500240	1724	331776	115216
	80	1600	819200	650240	1824	229376	60416
	90	1800	921600	820240	1924	126976	25616
	100	2000	1024000	1010240	2024	24576	10816
12	20	480	983040	106752	4336	15794176	14917888
	40	960	1966080	279552	4576	14811136	13124608
	60	1440	2949120	567552	4816	13828096	11446528
	80	1920	3932160	970752	5056	12845056	9883648
	100	2400	4915200	1489152	5296	11862016	8435968
	120	2880	5898240	2122752	5536	10878976	7103488
	140	3360	6881280	2871552	5776	9895936	5886208
	160	3840	7864320	3735552	6016	8912896	4784128
	180	4320	8847360	4714752	6256	7929856	3797248
	200	4800	9830400	5809152	6496	6946816	2925568
14	50	1400	11468800	719376	17084	256966656	246217232
	100	2800	22937600	2189376	17784	245497856	224749632
	150	4200	34406400	4639376	18484	234029056	204262032
	200	5600	45875200	8069376	19184	222560256	184754432
	250	7000	57344000	12479376	19884	211091456	166226832
	300	8400	68812800	17869376	20584	199622656	148679232
	350	9800	80281600	24239376	21284	188153856	132111632
	400	11200	91750400	31589376	21984	176685056	116524032
	450	12600	103219200	39919376	22684	165216256	101916432
	500	14000	114688000	49229376	23384	153747456	88288832
	550	15400	126156800	59519376	24084	142278656	75641232
	600	16800	137625600	70789376	24784	130809856	63973632
	650	18200	149094400	83039376	25484	119341056	53286032
	700	19600	160563200	96269376	26184	107872256	43578432

Объем ключевых данных в предлагаемой схеме определяется объемом ключевых данных несимметричной криптосистемы Мак-Элиса. Для двоичных кодов имеем:

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

$$l_{о.к.} = k \cdot n = (2^m - m \cdot t) \cdot 2^m; \quad (15)$$

- 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)

$$l_{з.к.} = k^2 + n \cdot \lceil \log_2 n \rceil = (2^m - m \cdot t)^2 + 2^m \cdot m. \quad (16)$$

Таким образом, основные конструктивные характеристики предлагаемой схемы формирования и проверки ЭЦП сопоставимы с характеристиками ЭЦП по схеме CFS [34]. При этом для высокоскоростных кодов (с $R = \frac{k}{n} > \frac{1}{2}$) объем ключевых данных схемы Нидеррайтера меньше, чем у схемы Мак-Элиса, а для низкоскоростных (с $R = \frac{k}{n} < \frac{1}{2}$) – наоборот, меньший объем ключей имеет схема Мак-Элиса. Схемы ЭЦП (предлагаемая и CFS) наследуют это свойство. Ввиду добавления в ЭЦП $Y = (I, e, i)$ вектора I битовая длина подписи больше, по сравнению со схемой CFS, на $2^m - m \cdot t$ бит. В остальном при оценке параметров предлагаемой схемы ЭЦП следует ориентироваться на данные [34, табл. 3].

В таблице приведены оценки длин ключей и длин подписей для схемы CFS (с использованием криптосистемы Нидеррайтера) и по предлагаемой схеме (с использованием криптосистемы Мак-Элиса). Для оценки параметров использовались конструктивные кодовые соотношения (6) для двоичных сепарабельных кодов Гоппы.

Выводы

Кодовые криптосистемы рассматриваются на сегодняшний день как реальная альтернатива в построении надежных постквантовых алгоритмов криптографической защиты информации [21, 22]. Исследование стойкости, быстродействия и возможности эффективной программно-аппаратной реализации таких криптосистем представляет важную и актуальную научно-техническую проблему, непосредственно связанную с обеспечением услуг информационной безопасности в условиях использования квантовых вычислительных систем и алгоритмов.

В статье рассмотрены кодовые криптосистемы Мак-Элиса и Нидеррайтера, а также алгоритмы формирования и проверки ЭЦП на их основе. В частности, с использованием криптопреобразований по схеме Мак-Элиса была предложена новая схема ЭЦП, которая по своим основным параметрам (стойкости, длине ключей и длине подписей) сопоставима с уже известной схемой CFS. Основное отличие предложенной схемы ЭЦП состоит в способе формирования подписи: информационная последовательность (ее сжатый образ) интерпретируется не как синдром кодового слова (как в схеме CFS), а как искаженное ошибками кодовое слово. Уполномоченный пользователь формирует ЭЦП в результате быстрого (полиномиальной сложности) декодирования. Неуполномоченный пользователь (не знающий правило маскирования алгебраического кода) для подделки подписи вынужден декодировать случайный код, решая NP-полную задачу. Проверка подписи осуществляется посредством матричного умножения элементов подписи с проверкой полученного результата. Предложенная схема ЭЦП защищена от быстрой подделки подписи на основе добавления произвольного кодового слова применяемого кода (эта атака предложена и подробно рассмотрена в работе [34]). Указанное преимущество дополнительно усилено введенной проверкой веса Хемминга, которая предназначена для защиты от других гипотетических атак (например, одновременной подделки нескольких элементов подписи).

Проблемным вопросом практического применения ЭЦП на алгебраических кодах остается чрезвычайно высокая сложность формирования подписи. Ввиду того, что реальные кодовые характеристики при большой длине кода значительно уступают верхним кодовым границам, сложность формирования ЭЦП растет как факториал от исправляющей способности кода. Фактически, это означает, что с увеличением исправляющей способности практическое использование таких ЭЦП вычислительно недостижимо. Однако для совершенных кодов (удовлетворяющих верхней кодовой границе Хемминга) сложность формирования ЭЦП минимальна, она определяется сложностью быстрого декодирования используемого алгебраического кода. В этом смысле поиск кодов, удовлетворяющих верхним кодовым границам, приобретает особую актуальность.

Другим возможным направлением снижения сложности формирования ЭЦП является совершенствование самой схемы формирования подписи. Это направление представляется особенно актуальным при условии использования уже известных кодовых конструкций, например двоичных сепарабельных кодов Гоппы.

Список литературы: 1. *Alfred, J. Menezes, Paul C. van Oorschot, Scott, A.* Vanstone. Handbook of Applied Cryptography – CRC Press, 1997. – 794 p. 2. *Горбенко, І.Д., Горбенко, Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування : підручник для вищих навч. закладів. – Харків : Форт, 2013. – 880 с. 3. *Nigel Smart*. Cryptography: An Introduction (3rd Edition). – 432 pp. https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf 4. *ISO/IEC 9796-2:2010* "Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms". 5. *ISO/IEC 9796-3:2006* "Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms". 6. *ISO/IEC 14888-1:2008* "Information technology – Security techniques – Digital signatures with appendix – Part 1: General". 7. *ISO/IEC 14888-2:2008* "Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms". 8. *ISO/IEC 14888-3:2006* "Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms". 9. *ISO/IEC 15946-1:2008* "Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General". 10. *ISO/IEC 15946-5:2009* "Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation". 11. *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. 12. *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. 13. *Simon, D. R.* On the power of quantum computation // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium. – P. 116-123. 14. *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. 15. *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. 16. *Shor, P. W*. Algorithms for quantum computation: discrete logarithms and factoring // Foundations of Computer Science : Conference Publications. – 1994. – P. 124-134. 17. *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. 18. *Neal Koblitz* and *Alfred J. Menezes*. A Riddle Wrapped in an Enigma. https://eprint.iacr.org/2015/1018.pdf 19. *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. 20. *Bernstein, Daniel J., Buchmann, Johannes, and Dahmen, Erik.* Post-Quantum Cryptography. – 2009, Springer-Verlag, Berlin-Heidleberg. – 245 p. 21. *Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone*. NISTIR 8105. Report on Post-Quantum Cryptography. National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf. 22. *Dustin Moody*. Post Quantum Cryptography: NIST's Plan for the Future. National Institute of Standards and Technology. http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/pqcrypto-2016-presentation.pdf. 23. *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. 24. *Niederreiter, H.* Knapsack-type cryptosystems and algebraic coding theory // Problem Control and Inform Theory, 1986, v. 15. P. 19-34.

25. *Stasev, Yu. V., Kuznetsov, A. A.* 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. 26. *Сидельников, В.М.* Криптография и теория кодирования // Материалы конф. «Московский университет и развитие криптографии в России». – Москва : МГУ, 2002. – 22 с. 27. *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. 28. Кузнецов, А.А. Алгебраическая теория блоковых кодов и ее приложения в криптографии // Перша міжнар. наук. конф. 25–27 травня 2005р. „Теорія та методи обробки сигналів". Тези доповідей. – К. : НАУ. – 2005. – С. 6 – 8. 29. *Кузнецов, А.А.* Исследование эффективности криптосистем на алгебраических блоковых кодах // Системи обробки інформації. – Харків : ХУПС, 2005 – Вип. 4. – С. 202 –206. 30. *Кузнецов, А.А.* Исследование помехоустойчивости и криптостойкости теоретико-кодовых схем // Моделювання та інформаційні технології. – Київ : НАНУ, 2005. – №33. – С. 81-84. 31. *Courtois, N., Finiasz, M., and N.Sendrier* How to achieve a McEliece-based digital signature scheme // Advances in Cryptology – ASIACRYPT 2001, volume 2248, pages 157–174. 32. *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. 33. *Кузнецов, А., Пушкарев, А., Кавун, С., Калашников, В.* Несимметричные криптосистемы на основе алгебраического кодирования: современное состояние, существующие противоречия и перспективы практического использования на постквантовый период // Computer science and cybersecurity. – Kharkiv : V.N. Karazin Kharkiv National University, 2016. – Issue 3(3) 2016. – P. 36-60. 34. *Кузнецов, А.А., Пушкарев, А.И., Сватовский, И.И., Шевцов, А.В.* Несимметричные криптосистемы на алгебраических кодах для пост-квантового периода // Радиотехника. – 2016. – Вып. 186. – С. 70-90. 35. *Кузнецов, О., Пушкарьов, А., Шевцов, О., Кузнецова, Т.* Несиметричне криптографічне перетворення з використанням алгебраїчних блокових кодів // Захист інформації. – Київ : Нац. авіаційний ун-т, 2016. – Т. 18, №4, жовтень-грудень 2016. – С. 269-275. 36. *Кузнецов, О.О., Пушкарьов, А.І., Шевцов, О.В, Кузнецова, Т.Ю.* Несиметричне криптоперетворення з використанням алгебраїчних блокових кодів // Актуальні задачі та досягнення у галузі кібербезпеки: матеріали Всеукр. наук.-практ. конф., 23–25 листопада 2016 року. – Кропивницький : КНТУ, 2016. – С. 124-127. 37. *Кузнецов О.О., Пушкарьов А.І., Шевцов О.В., Кузнецова Т.Ю.* Несиметричні крипто-кодові системи захисту інформації // 71-а наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів : матеріали конф. (6-8 грудня 2016 р.) – Одеса : ОНАЗ, 2016. – 84-87 с. 38. *Кузнецов, О.О., Пушкарьов, А.І., Сватовський, І.І., Шевцов, А.В., Кузнецова, Т.Ю.* Несиметричні криптосистеми на алгебраїчних блокових кодах // Актуальні питання забезпечення кібербезпеки та захисту інформації: тези доповідей учасників III Міжнар. наук.-практ. конф., 22-25 лютого 2017 р. – К. : Вид-во Європейського ун-ту, 2017. – С. 108-112. 39. *Кузнецов, А.А., Сватовский, И.И., Шевцов, А.В.* Схемы электронной цифровой подписи на основе помехоустойчивых кодов // Труды науч.-техн. конф. с международным участием «Компьютерное моделирование в наукоемких технологиях», 26-31 мая 2016 г. – Харьков : ХНУ имени В.Н. Каразина, 2016. – С. 191-193. 40. *Кузнецов, А., Сватовский, И., Шевцов, А.* Электронная цифровая подпись на алгебраических кодах для постквантового периода // Матеріали V-ї міжнар. наук.-техн. конф. "Захист інформації і безпека інформаційних систем", 2-3 червня 2016 р. – Львів : НУ "Львівська політехніка", 2016. – С. 122-123. 41. *Кузнецов, А.А., Сватовский, И.И., Шевцов, А.В.* Алгоритми цифрового підпису для постквантового періоду із застосування алгебраїчних кодів: сучасний стан, існуючі протиріччя та перспективи практичного застосування // Безпека інформації в інформаційно-телекомунікаційних системах : Матеріали міжнар. наук.-практ. конф. Вип. 18, 25-26 травня 2016 р. – К. : Державна служба спеціального зв'язку та захисту інформації України, 2016 – С. 17. 42. *Гоппа, В. Д.* Новый класс линейных корректирующих кодов // Проблемы передачи информации. – 1970. – Т. 6, вып. 3. – С. 24–30. 43. *Гоппа, В. Д.* На неприводимых кодах достигается пропускная способность ДСК // Проблемы передачи информации. – 1974. – Т. 10, вып. 1. – С. 111–112. 44. *MacWilliams, F. J. and Sloane,N. J.* A. The theory of error-correcting codes. – North-Holland, Amsterdam, New York, Oxford, 1977. – 762 pp.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 11.04.2017