УДК 512.552.18+003.26 Вестник СПбГУ. Прикладная математика. Информатика... 2019. Т. 15. Вып. 2
MSC 16P10

Схема постквантовой электронной цифровой подписи на основе усиленной формы скрытой задачи дискретного логарифмирования

Н. А. Молдовян, И. К. Абросимов

Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Российская Федерация, 199178, Санкт-Петербург, 14-я линия В. О., 39

Для цитирования: *Молдовян Н. А., Абросимов И. К.* Схема постквантовой электронной цифровой подписи на основе усиленной формы скрытой задачи дискретного логарифмирования // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2019. Т. 15. Вып. 2. С. 212–220.
https://doi.org/10.21638/11702/spbu10.2019.205

Предложено построение схем цифровой подписи на основе вычислительно трудной скрытой задачи дискретного логарифмирования, заданной над конечными некоммутативными ассоциативными алгебрами. Рассмотрены модифицированная алгебра кватернионов и ее свойства как основа построения постквантовой схемы электронной цифровой подписи. Выведены формулы, описывающие множество локальных единиц, ассоциированных с заданным необратимым вектором модифицированной алгебры кватернионов. Сформулирована новая форма скрытой задачи дискретного логарифмирования и разработана схема цифровой подписи на основе этой задачи. Показана корректность предложенной схемы подписи.

Ключевые слова: постквантовая криптография, криптографический примитив, электронная подпись, конечная алгебра, некоммутативная ассоциативная алгебра.

Введение. Базой для криптографических преобразований, используемых для построения схем электронной цифровой подписи (ЭЦП), служат задачи факторизации и дискретного логарифмирования [1]. Безопасность применения данных схем учитывает то, что в настоящее время асимптотическая сложность наиболее эффективных алгоритмов решения этих задач для классических компьютеров — субэкспоненциальная. Предпринимаются попытки построения квантового компьютера, на котором такие задачи решаются значительно быстрее. В 1994 г. Шорр предложил алгоритм, позволяющий решить обе задачи за полиномиальное время [2]. Поэтому в случае появления квантового компьютера с достаточным числом кубитов можно будет быстро решать задачи факторизации и дискретного логарифмирования и основывающиеся на них криптосхемы окажутся нестойкими. Для сохранения всех возможных приложений криптографии с открытым ключом требуется нахождение новых вычислительно трудных задач, для решения которых как на классическом, так и на квантовом компьютерах существовали бы алгоритмы сверхполиномиальной сложности. Криптографические схемы, которые являются стойкими к атакам с применением квантового компьютера, и вычислительно трудные задачи, на которых они основаны, принято относить к постквантовой криптографии [3].

Нельзя утверждать, что создание квантового компьютера приведет к потере всех возможностей двухключевой криптографии, поскольку существует набор криптосистем, базирующихся на вычислительно трудных задачах, отличных от задач факторизации и дискретного логарифмирования. К постквантовым двухключевым криптографическим алгоритмам относятся [3] основанные на: 1) хэш-функциях; 2) кодах ис-

правления ошибок; 3) решетках; 4) многомерных квадратичных системах. Примерами этих криптосистем соответственно могут служить подпись Меркла [4], криптосистема Мак-Элиса [5], криптосистема NTRUEncrypt [6] и криптосистема на основе скрытых уравнений поля [7]. Однако они не вытеснили криптосистемы, базирующиеся на вычислительной трудности задач факторизации и дискретного логарифмирования, из-за недостаточной универсальности и больших длин ключа для обеспечения практических уровней безопасности (в частности, для 128-битовой стойкости в криптосистеме Мак-Элиса требуются ключи, размер которых порядка миллиона бит). Под недостаточной универсальностью криптосистемы здесь понимается то, что с ее помощью можно построить не все основные алгоритмы и протоколы двухключевой криптографии, а только какую-то их часть. Потому продолжается поиск новых вычислительно трудных задач, которые могут стать базой для постквантовых криптографических алгоритмов. По тематике постквантовой криптографии регулярно проводятся конференции [8]. Национальным институтом стандартов и технологий США был объявлен конкурс на разработку постквантовых криптоалгоритмов, которые базируются на новых вычислительно трудных задачах [9].

При поиске постквантовых криптографических примитивов значительное внимание уделяется некоммутативным алгебраическим структурам. Изучался вопрос о создании криптосхем, базирующихся на вычислительной трудности сопрягающего элемента в группах переплетений [10], однако в статье [11] были показаны сводимость этой задачи к задаче решения систем линейных уравнений и наличие принципиальных трудностей для обеспечения приемлемой стойкости. Более перспективным представляется использование задачи дискретного логарифмирования в скрытой циклической группе конечной ассоциативной алгебры с некоммутативной операцией умножения [12–15], называемой еще скрытой задачей дискретного логарифмирования. Но известная форма задания скрытой задачи дискретного логарифмирования позволяет разработать протокол открытого согласования ключа и алгоритм открытого шифрования [16], но не подходит для построения схем ЭЦП.

В настоящей работе предлагаются новая форма задания скрытой задачи дискретного логарифмирования и новая постквантовая схема ЭЦП. В качестве перспективного алгебраического носителя для предложенной вычислительно трудной задачи и схемы ЭЦП рассматривается конечная алгебра кватернионов, представленная в модифицированном виде, и исследуются ее свойства, применяемые для вычисления параметров схемы ЭЦП.

Постановка скрытой задачи дискретного логарифмирования и ее новая форма. В конечной некоммутативной группе Γ автоморным отображением является отображение, задаваемое формулой

$$\varphi_u(g) = u \circ g \circ u^{-1},$$

где $u \in \Gamma$ фиксирован; элемент g пробегает все элементы группы Γ.

Для построения криптосхем на основе конечных некоммутативных ассоциативных алгебр необходимо наличие взаимной коммутативности операций возведения в степень и сопряжения через элемент u:

$$\varphi_u(g^x) = (\varphi_u(g))^x.$$

Впервые задача скрытого дискретного логарифмирования была сформулирована следующим образом [13]: по заданным $y = u \circ g^x \circ u^{-1}$ и g требуется вычислить u и x.

Такая форма может быть использована для создания протоколов открытого распределения ключей и схем открытого шифрования. Новая форма задачи ориентирована на создание ЭЦП, так как в схеме ЭЦП возможно, чтобы каждый владелец открытого ключа мог применить свою циклическую группу. Генератором такой группы предлагается необратимый вектор конечной некоммутативной ассоциативной алгебры векторов. Как пример такой алгебры рассмотрим модифицированную алгебру кватернионов, заданную над простым конечным полем $\mathrm{GF}(p)$.

Операции в четырехмерных алгебрах. Пусть четырехмерные векторы заданы над полем $\mathrm{GF}(p)$, где p — простое число. Тогда каждый вектор $\bar{v} = (a, b, c, d)$ может быть записан в виде линейной комбинации базисных векторов $\bar{e}$, $\bar{i}$, $\bar{j}$, $\bar{k}$:

$$\bar{v} = a\bar{e} + b\bar{i} + c\bar{j} + d\bar{k}.$$

Операции сложения, вычитания и умножения на скаляр четырехмерных векторов осуществляются обычным образом — покоординатно:

$$\alpha\bar{v} \pm \beta\bar{w} = (\alpha a_1 \pm \beta a_2)\bar{e} + (\alpha b_1 \pm \beta b_2)\bar{i} + (\alpha c_1 \pm \beta c_2)\bar{j} + (\alpha d_1 \pm \beta d_2)\bar{k}.$$

На множестве четырехмерных векторов над конечным полем можно ввести операцию векторного умножения таким образом:

шаг 1 — представить каждый вектор-сомножитель как линейную комбинацию базисных векторов, коэффициенты которой являются координатами этого вектора:

$$\bar{v} \circ \bar{w} = (a_1\bar{e} + b_1\bar{i} + c_1\bar{j} + d_1\bar{k}) \circ (a_2\bar{e} + b_2\bar{i} + c_2\bar{j} + d_2\bar{k});$$

шаг 2 — перемножить получившиеся две линейные комбинации путем раскрытия скобок; в результате находим сумму произведений каждого слагаемого первой линейной комбинации на каждое слагаемое второй линейной комбинации:

$$\bar{v} \circ \bar{w} = a_1a_2(\bar{e} \circ \bar{e}) + a_1b_2(\bar{e} \circ \bar{i}) + \cdots + d_1d_2(\bar{k} \circ \bar{k});$$

шаг 3 — выполнить перемножение получившихся произведений базисных векторов согласно таблице умножения базисных векторов (ТУБВ).

ТУБВ устроена следующим образом. Строкам и столбцам ТУБВ соответствуют базисные векторы, а ячейкам — результат их перемножения, которым является некоторый базисный вектор, умноженный на структурную константу — элемент поля $\mathrm{GF}(p)$.

Таблица. **ТУБВ для модифицированной алгебры кватернионов**

$\circ$	$\bar{e}$	i	j	k
$\bar{e}$	$\bar{e}$	$\bar{i}$	$\bar{j}$	k
i	i	$-\varepsilon\bar{e}$	εk	$-j$
$\bar{j}$	$\bar{j}$	$-\varepsilon k$	$-\varepsilon\bar{e}$	$\bar{i}$
k	k	j	$-i$	$-\bar{e}$

Необратимые векторы модифицированной конечной алгебры кватернионов. В качестве алгебры, вычисления в которой реализуют описанную далее схему ЭЦП, возьмем модифицированную конечную алгебру кватернионов, задаваемую таблицей, где $\varepsilon \in \mathrm{GF}(p)$ — структурная константа, и рассмотрим ее свойства,

используемые при дальнейшем построении алгоритмов формирования и проверки ЭЦП. Для этого требуется установить, какой вектор является единицей алгебры и какому условию удовлетворяют необратимые векторы данной алгебры.

В общем случае единицы конечных некоммутативных ассоциативных алгебр имеют нетривиальный вид, который заведомо неочевиден. Кроме того, единицы бывают различных типов — правосторонние, левосторонние, локальные двухсторонние и т. п. [12]. Далее, для краткости правосторонние единицы будем называть правыми единицами, а левосторонними — левыми. Рассмотрим вывод единицы модифицированной алгебры кватернионов. Определим сначала множества правых и левых единиц, а затем их пересечение.

Обозначим E_r множество правых единиц, тогда для любого $\bar{e}_r \in E_r$ и $\bar{v}$ справедливо равенство $\bar{v} \circ \bar{e}_r = \bar{v}$.

Теорема. *Пусть* $\bar{v} = (a, b, c, d)$ *и* $\bar{e}_r = (x, y, z, w)$ *— правая единица, тогда координаты правой единицы ищутся как решение системы*

$$\begin{cases} ax - b\varepsilon y - c\varepsilon z - dw = a, \\ bx + ay - dz + cw = b, \\ cx + dy + az - bw = c, \\ dx - c\varepsilon y + b\varepsilon z + aw = d. \end{cases} \tag{1}$$

Доказательство. Обозначив $\bar{v} = (a, b, c, d)$ и $\bar{e}_r = (x, y, z, w)$, выполним перемножение векторов:

$$\begin{gathered} \bar{v} \circ \bar{e}_r = (a\bar{e} + b\bar{i} + c\bar{j} + d\bar{k}) \circ (x\bar{e} + y\bar{i} + z\bar{j} + w\bar{k}) = \\ = ax(\bar{e} \circ \bar{e}) + ay(\bar{e} \circ \bar{i}) + az(\bar{e} \circ \bar{j}) + aw(\bar{e} \circ \bar{k}) + \\ + bx(\bar{i} \circ \bar{e}) + by(\bar{i} \circ \bar{i}) + bz(\bar{i} \circ \bar{j}) + bw(\bar{i} \circ \bar{k}) + \\ + cx(\bar{j} \circ \bar{e}) + cy(\bar{j} \circ \bar{i}) + cz(\bar{j} \circ \bar{j}) + cw(\bar{j} \circ \bar{k}) + \\ + dx(\bar{k} \circ \bar{e}) + dy(\bar{k} \circ \bar{i}) + dz(\bar{k} \circ \bar{j}) + dw(\bar{k} \circ \bar{k}) = \\ = ax\bar{i} + ay\bar{i} + az\bar{j} + aw\bar{k} + bx\bar{i} - b\varepsilon y\bar{e} + b\varepsilon z\bar{k} - bw\bar{j} + \\ + cx\bar{j} - c\varepsilon y\bar{k} - c\varepsilon z\bar{e} + cw\bar{i} + dx\bar{k} + dy\bar{j} - dz\bar{i} - dw\bar{e} = \\ = (ax - b\varepsilon y - c\varepsilon z - dw)\bar{e} + (bx + ay - dz + cw)\bar{i} + \\ + (cx + dy + az - bw)\bar{j} + (dx - c\varepsilon y + b\varepsilon z + aw)\bar{k} \Rightarrow \\ \Rightarrow \bar{v} = (ax - b\varepsilon y - c\varepsilon z - dw)\bar{e} + (bx + ay - dz + cw)\bar{i} + \\ + (cx + dy + az - bw)\bar{j} + (dx - c\varepsilon y + b\varepsilon z + aw)\bar{k}. \end{gathered}$$

Согласно условию равенства векторов, это равенство равносильно системе (1), что и требовалось доказать.

Вычислим главный определитель системы (1)

$$\Delta = \begin{vmatrix} a & -b\varepsilon & -c\varepsilon & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c\varepsilon & b\varepsilon & a \end{vmatrix}. \tag{2}$$

Вспомогательные определители имеют вид $\Delta_x = \Delta$, $\Delta_y = \Delta_z = \Delta_w = 0$. Следовательно, учитывая (2), множество правых единиц состоит из одного вектора $(1, 0, 0, 0)$.

Проверим, что этот же вектор является левой единицей, а значит, и единицей алгебры:

$$(1,0,0,0)\circ(a,b,c,d) = a\bar{e} + b\bar{i} + c\bar{j} + d\bar{k}.$$

Таким образом, $(1,0,0,0)$ — единица модифицированной алгебры кватернионов. В случае, когда вектор (a,b,c,d) необратим, для его координат выполняется условие

$$a^2 = -d^2 + (b^2 + c^2)\varepsilon. \tag{3}$$

Процедуру генерации необратимого вектора можно описать следующим образом:

шаг 1 — сгенерировать $b, c, d \in \mathrm{GF}(p)$;

шаг 2 — проверить, что $-(d^2 + (b^2 + c^2)\varepsilon)$ является квадратичным вычетом (например, при помощи символа Лежандра), и если проверка завершилась неудачей, то перейти к шагу 1;

шаг 3 — вычислить $a = \sqrt{-(d^2 + (b^2 + c^2)\varepsilon)}$ в поле $\mathrm{GF}(p)$.

После выполнения процедуры генерации получаем искомый необратимый вектор $\bar{v} = (a,b,c,d)$.

Локальные единицы. Каждому необратимому вектору $\bar{v} = (a,b,c,d)$ можно сопоставить множества левых и правых локальных единиц. Построим множество $E_r(\bar{v})$ правых локальных единиц для вектора $\bar{v}$. Принимая во внимание, что $a = \sqrt{-(d^2 + (b^2 + c^2)\varepsilon)}$, находим, что главный определитель системы (1) обратится в нуль. Исключив с помощью системы компьютерной алгебры Wolfram Mathematica из расширенной матрицы системы (1) линейно зависимые строки (а именно, 3 и 4), имеем

$$\begin{cases} ax - b\varepsilon y - c\varepsilon z - dw = a, \\ bx + ay - dz + cw = b. \end{cases} \tag{4}$$

Домножим первую строку (4) на c и вторую на d, сложим и выразим в получившемся выражении z:

$$\begin{gathered}(ac+bd)x + (-bc\varepsilon + ad)y + (-c^2\varepsilon - d^2)z = ac + bd \Leftrightarrow \\ \Leftrightarrow z = \frac{(ac+bd-(ac+bd)x-(-bc\varepsilon+ad)y)}{-d^2-c^2\varepsilon} = \\ = \frac{-ac-bd+(ac+bd)x+(-bc\varepsilon+ad)y}{d^2+c^2\varepsilon}.\end{gathered}$$

Таким образом, z вычисляется по формуле

$$z = \frac{-ac-bd+(ac+bd)x+(-bc\varepsilon+ad)y}{d^2+c^2\varepsilon}. \tag{5}$$

Аналогично из системы (4) можно вывести для w:

$$w = \frac{bc\varepsilon - ad + (ad - bc\varepsilon)x + (-ac\varepsilon - bd\varepsilon)y}{d^2+c^2\varepsilon}. \tag{6}$$

Из (5) и (6) следует, что множество решений примет следующий вид:

$$E_r(\bar{v}) = \left\{ \frac{\bar{v}_0 + \bar{v}_1 t_1 + \bar{v}_2 t_2}{d^2+c^2\varepsilon} : t_1, t_2 \in \mathrm{GF}(p) \right\}, \tag{7}$$

где $\bar{v}_0 = (0, 0, -ac - bd, bc\varepsilon - ad)$; $\bar{v}_1 = (d^2 + c^2\varepsilon, 0, ac + bd, ad - bc\varepsilon)$; $\bar{v}_2 = (0, d^2 + c^2\varepsilon, ad - bc\varepsilon, -ac\varepsilon - bd\varepsilon)$; $\varepsilon \neq -d^2/c^2$.

Построим множество $E_l(\bar{v})$ левых локальных единиц вектора $\bar{v}$. Для этого определим решение векторного уравнения вида $\bar{e}_l \circ \bar{v} = \bar{v}$, где $\bar{e}_l$ — левая единица, которое равносильно следующей системе из четырех линейных уравнений:

$$\begin{cases} ax - b\varepsilon y - c\varepsilon z - dw = a, \\ bx + ay + dz - cw = b, \\ cx - dy + az + bw = c, \\ dx + c\varepsilon y - b\varepsilon z + aw = d. \end{cases} \tag{8}$$

Решив систему (8) с учетом условия (3), получим множество $E_l(\bar{v})$ левых локальных единиц для вектора $\bar{v}$:

$$E_l(\bar{v}) = \left\{ \frac{\bar{w}_0 + \bar{w}_1 t_1 + \bar{w}_2 t_2}{d^2 + c^2\varepsilon} : t_1, t_2 \in \mathrm{GF}(p) \right\}, \tag{9}$$

в котором $\bar{w}_0 = (0, 0, bd - ac, -bc\varepsilon - ad)$, $\bar{w}_1 = (d^2 + c^2\varepsilon, 0, ac - bd, ad + bc\varepsilon)$, $\bar{w}_2 = (0, d^2 + c^2\varepsilon, -ad - bc\varepsilon, -ac\varepsilon - bd\varepsilon)$, $\varepsilon \neq -d^2/c^2$.

Таким образом, для необратимых векторов модифицированной конечной алгебры кватернионов установлено существование множеств левых и правых локальных единиц, мощность каждого из них равна p^2. Этот факт и формулы (7) и (9), описывающие множества правых и левых локальных единиц, используются для задания новой формы скрытой задачи дискретного логарифмирования и построения на ее основе схемы ЭЦП.

ЭЦП над необратимыми векторами. Постановка усиленной формы скрытой задачи дискретного логарифмирования. Для построения схемы ЭЦП в скрытой конечной циклической группе примем в качестве аналога алгоритм ЭЦП Шнорра [17]. Для реализации повышенной скрытности группы, в которой предполагается выполнение базовой операции возведения в степень, зададим формирование открытого ключа в виде двух элементов алгебры $\bar{z}$ и $\bar{y}$, лежащих вне циклической группы, генерируемой степенями необратимого элемента $\bar{g}$, для которого в конечной некоммутативной ассоциативной алгебре с единицей $\bar{e}$ существуют большие множества локальных правых и левых единиц. При этом элементы $\bar{z}$ и $\bar{y}$ принадлежат разным конечным циклическим группам, но связаны с элементами $\bar{g}$ и $\bar{g}^x$ соответственно.

Процедура генерации открытого ключа состоит из семи шагов:

шаг 1 — выбрать большое (например, 512 бит) простое число p;

шаг 2 — выбрать случайный необратимый элемент $\bar{g}$ большого (не менее 256 бит) простого порядка q;

шаг 3 — выбрать случайные обратимые элементы $\bar{d}$ и $\bar{u}$ такие, что $\bar{g} \circ \bar{d} \neq \bar{d} \circ \bar{g}$, $\bar{g} \circ \bar{u} \neq \bar{u} \circ \bar{g}$, $\bar{u} \circ \bar{d} \neq \bar{d} \circ \bar{u}$;

шаг 4 — выбрать три числа: w, t, x;

шаг 5 — выбрать правую локальную единицу $\bar{e}_{\bar{g}}$ для элемента $\bar{g}$;

шаг 6 — вычислить элемент согласования $\bar{l} = \bar{d}^{-w} \circ \bar{e}_{\bar{g}} \circ \bar{u}^t$;

шаг 7 — вычислить открытый ключ $\bar{y} = \bar{d}^{-w} \circ \bar{g}^x \circ \bar{d}^w$ и $\bar{z} = \bar{u}^{-t} \circ \bar{g} \circ \bar{u}^t$.

Равенства, используемые для расчета открытого ключа, задают усиленную форму скрытой задачи дискретного логарифмирования. Эта задача формулируется следующим образом: по заданным $\bar{y} = \bar{d}^{-w} \circ \bar{g}^x \circ \bar{d}^w$, $\bar{z} = \bar{u}^{-t} \circ \bar{g} \circ \bar{u}^t$ и $\bar{l} = \bar{d}^{-w} \circ \bar{e}_{\bar{g}} \circ \bar{u}^t$ при неизвестных $\bar{d}$, $\bar{u}$, $\bar{g}$, $\bar{e}_{\bar{g}}$, w, t требуется определить x.

Процедура формирования подписи состоит в выполнении таких шагов:

шаг 1 — выбрать случайное число k;

шаг 2 — вычислить разовый открытый ключ $\bar{r} = \bar{d}^{-w} \circ \bar{g}^k \circ \bar{u}^t$;

шаг 3 — вычислить первый элемент подписи: $\bar{e} = F_H(\bar{m}||\bar{r})$, где $\bar{m}$ — вектор, представляющий подписываемое сообщение;

шаг 4 — вычислить второй элемент подписи: $s = k + ex \bmod q$.

Пара чисел (e, s) является подписью сообщения $\bar{m}$.

Процедура проверки подписи состоит в следующем:

шаг 1 — вычислить $\widetilde{r} = \bar{y}^{q-e} \circ \bar{l} \circ \bar{z}^s$;

шаг 2 — вычислить $\widetilde{e} = F_H(\bar{m}||\widetilde{r})$.

Если $\widetilde{e} = \bar{e}$, то подпись подлинная, иначе — поддельная.

Формальное доказательство корректности работы схемы ЭЦП можно выполнить путем подстановки правых частей формул для открытого ключа в формулу для $\widetilde{R}$:

$$\begin{gathered}\widetilde{r} = \bar{y}^{q-e} \circ \bar{l} \circ \bar{z}^s = (\bar{d}^{-w} \circ \bar{g}^x \circ \bar{d}^w)^{q-e} \circ (\bar{d}^{-w} \circ \bar{e}_{\bar{g}} \circ \bar{u}^t) \circ (\bar{u}^{-t} \circ \bar{g} \circ \bar{u}^t)^s = \\ = \bar{d}^{-w} \circ \bar{g}^{x(q-e)} \circ \bar{d}^w \circ \bar{d}^{-w} \circ \bar{e}_{\bar{g}} \circ \bar{u}^t \circ \bar{u}^{-t} \circ \bar{g}^s \circ \bar{u}^t = \\ = \bar{d}^{-w} \circ \bar{g}^{x(q-e)} \circ \bar{e} \circ \bar{e}_{\bar{g}} \circ \bar{e} \circ \bar{g}^s \circ \bar{u}^t = \bar{d}^{-w} \circ \bar{g}^{x(q-e)} \circ \bar{e}_{\bar{g}} \circ \bar{g}^s \circ \bar{u}^t = \\ = \bar{d}^{-w} \circ \bar{g}^{-ex+s} \circ \bar{u}^t = \bar{d}^{-w} \circ \bar{g}^k \circ \bar{u}^t = \bar{r}.\end{gathered}$$

Таким образом, ЭЦП работает корректно.

Существенное отличие построенной схемы ЭЦП от схемы Шнорра состоит в том, что в схеме Шнорра вычисления в процессе проверки подлинности ЭЦП выполняются в явно заданной циклической группе, а в предложенной схеме ведутся в двух разных циклических группах, причем каждая из них отлична от циклической группы, генерируемой необратимым элементом $\bar{g}$, который устанавливает связь между элементами открытого ключа $\bar{y}$ и $\bar{z}$. Благодаря такому отличию обеспечивается стойкость построенной схемы ЭЦП к квантовым атакам.

Заключение. Предложена новая форма скрытой задачи дискретного логарифмирования, ориентированная на построение протоколов ЭЦП. На основе такой задачи дана схема ЭЦП и сформулированы требования к конечной некоммутативной ассоциативной алгебре, реализующей данную схему. Одним из возможных носителей этой задачи служит модифицированная конечная алгебра кватернионов. Предложен алгоритм нахождения необратимых элементов и выведены формулы, описывающие множества левых и правых локальных единиц для заданного необратимого вектора. Упомянутые алгоритм и формулы позволяют вычислить требуемые параметры схемы подписи при использовании одним из ее носителей конечной модифицированной алгебры кватернионов.

Литература

1. *Menezes A. J., Van Oorschot P. C., Vanstone S. A.* Handbook of applied cryptography. Boca Raton, FL: CRC Press, 1997. 780 p.

2. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM Journal of Computing. 1997. Vol. 26. P. 1484–1509.

3. *Buchmann J., Dahmen E.* Post-quantum cryptography / ed. by D. J. Bernstein. Berlin; Heidelberg: Springer, 2009. 245 p.

4. *Merkle R. Ch.* Secrecy, authentication, and public key systems: technical report N 1979-1. Ctanford, 1979. 193 p.

5. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // DSN Progress Report 42–44. 1978. P. 114–116.

6. *Hoffstein J., Pipher J., Silverman J. H.* NTRU: A ring based public key cryptosystem // Algorithmic Number Theory (ANTS III). Portland, OR, June 1998 / ed. by J. P. Buhler. Berlin: Springer-Verlag, 1998. P. 267–288. (Lecture Notes in Computer Science, vol. 1423.)

7. *Courtois N.* The security of Hidden Field Equations (HFE) // Topics in Cryptology — CT-RSA 2001. Berlin; Heidelberg: Springer, 2001. P. 266–281. (Lecture Notes in Computer Science, vol. 2020.)

8. Post-quantum cryptography // 9th Intern. conference, PQCrypto 2018. Fort Lauderdale, FL, USA, April 9–11, 2018, Proceedings. Berlin; Heidelberg: Springer, 2018. (Lecture Notes in Computer Science, vol. 10786.)

9. Federal Register :: Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms // Federal Register. The Daily Journal of the United States Goverment. URL: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (дата обращения: 15.01.2019).

10. *Verma G. K.* A proxy blind signature scheme over braid groups // Intern. Journal of Network Security. 2009. Vol. 9, N 3. P. 214–217.

11. *Myasnikov A., Shpilrain V., Ushakov A.* A practical attack on a braid group based cryptographic protocol // Advances in Cryptology — CRYPTO'05. Berlin: Springer-Verlag, 2005. P. 86–96. (Lecture Notes in Computer Science, vol. 3621.)

12. *Moldovyan N. A., Moldovyan A. A.* Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem // Bulletin of the South Ural State University. Series Mathematical Modelling, Programming & Computer Software (Bulletin SUSU MMCS). 2019. Vol. 12, N 1. P. 66–81.

13. *Moldovyan D. N.* Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms // Quasigroups and Related Systems. 2010. Vol. 18, N 2. P. 165–176.

14. *Moldovyan D. N.* Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem // Computer Science Journal of Moldova. 2019. Vol. 27, N 1 (78). P. 56–72.

15. *Молдовян Д. Н., Молдовян Н. А.* Особенности строения групп векторов и синтез криптографических схем на их основе // Вестн. С.-Петерб. ун-та. Сер. 10. Прикладная математика. Информатика. Процессы управления. 2011. Вып. 4. С. 84–93.

16. *Молдовян Н. А., Абросимов И. К., Ковалева И. В.* Постквантовый протокол бесключевого шифрования // Вопросы защиты информации. 2017. № 3 (118). С. 3–13.

17. *Schnorr C. P.* Efficient signature generation by smart cards // Journal of Cryptology. 1991. Vol. 4, N 3. P. 161–174.

Статья поступила в редакцию 14 февраля 2019 г.
Статья принята к печати 15 марта 2019 г.

Контактная информация:

Молдовян Николай Андреевич — д-р техн. наук, проф., гл. науч. сотр.; nmold@mail.ru

Абросимов Иван Константинович — мл. науч. сотр.; ivnabr@yandex.ru

Post-quantum electronic digital signature scheme based on the enhanced form of the hidden discrete logarithm problem

N. A. Moldovyan, I. K. Abrosimov

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
39, 14 Line V. I., St. Petersburg, 199178, Russian Federation

For citation: Moldovyan N. A., Abrosimov I. K. Post-quantum electronic digital signature scheme based on the enhanced form of the hidden discrete logarithm problem. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2019, vol. 15, iss. 2, pp. 212–220. https://doi.org/10.21638/11702/spbu10.2019.205 (In Russian)

A digital signature scheme based on the computational difficulty of the hidden discrete logarithm problem defined in finite non-commutative associative algebras is proposed. The modified quaternion algebra and its properties are considered as the algebraic carrier of the introduced post-quantum digital signature scheme. Formulas describing the set of local units associated with a given non-invertible vector of a modified quaternion algebra are derived.

A new form of the hidden discrete logarithm problem has been formulated and a digital signature scheme has been developed on its base.

Keywords: post-quantum cryptography, cryptographic primitive, electronic signature, finite algebra, non-commutative associative algebra.

References

1. Menezes A. J., Van Oorschot P. C., Vanstone S. A. *Handbook of applied cryptography*. Boca Raton, CRC Press, 1997, 780 p.

2. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. *SIAM Journal of Computing*, 1997, vol. 26, pp. 1484–1509.

3. Buchmann J., Dahmen E. *Post-quantum cryptography*. Berlin, Heidelberg, Springer Press, 2009, 245 p.

4. Merkle R. Ch. *Secrecy, authentication, and public key systems*. Technical report no. 1979-1. Stanford, 1979, 193 p.

5. McEliece R. J. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report 42–44*, 1978, pp. 114–116.

6. Hoffstein J., Pipher J., Silverman J. H. NTRU: A ring based public key cryptosystem. *Algorithmic Number Theory (ANTS III)*. Portland, OR, June 1998. Berlin, Springer-Verlag Press, 1998, pp. 267–288. (Lecture Notes in Computer Science, vol. 1423.)

7. Courtois N. The security of Hidden Field Equations (HFE). *Topics in Cryptology — CT-RSA 2001*. Berlin, Heidelberg, Springer Press, 2001, pp. 266–281. (Lecture Notes in Computer Science, vol. 2020.)

8. Post-quantum cryptography. *9th Intern. conference, PQCrypto 2018*. Fort Lauderdale, FL, USA, April 9–11, 2018, Proceedings. Berlin, Heidelberg, Springer Press, 2018. (Lecture Notes in Computer Science, vol. 10786.)

9. Federal Register :: Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. *Federal Register. The Daily Journal of the United States Goverment*. Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (accessed: 15.01.2019).

10. Verma G. K. A proxy blind signature scheme over braid groups. *Intern. Journal of Network Security*, 2009, vol. 9, no. 3, pp. 214–217.

11. Myasnikov A., Shpilrain V., Ushakov A. A practical attack on a braid group based cryptographic protocol. *Advances in Cryptology — CRYPTO'05*. Berlin, Springer-Verlag Press, 2005, pp. 86–96. (Lecture Notes in Computer Science, vol. 3621.)

12. Moldovyan N. A., Moldovyan A. A. Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem. *Bulletin of the South Ural State University. Series Mathematical Modelling, Programming & Computer Software (Bulletin SUSU MMCS)*, 2019, vol. 12, no. 1, pp. 66–81.

13. Moldovyan D. N. Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms. *Quasigroups and Related Systems*, 2010, vol. 18, no. 2, pp. 165–176.

14. Moldovyan D. N. Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem. *Computer Science Journal of Moldova*, 2019, vol. 27, no. 1 (78), pp. 56–72.

15. Moldovyan D. N., Moldovyan N. A. Osobennosti stroeniya grupp vektorov i sintez kriptograficheskih shem na ih osnove [Features of the structure of groups of vectors and the synthesis of cryptographic schemes based on them]. *Vestnik of Saint Petersburg University. Series 10. Applied Mathematics. Computer Science. Control Processes*, 2011, iss. 4, pp. 84–93. (In Russian)

16. Moldovyan N. A., Abrosimov I. K., Kovaleva I. V. Postkvantovy'j protokol besklyuchevogo shifrovaniya [Post-quantum no-key encryption protocol]. *Voprosi zaschity informatsii* [*Information security issues*], 2017, no. 3 (118), pp. 3–13. (In Russian)

17. Schnorr C. P. Efficient signature generation by smart cards. *Journal of Cryptology*, 1991, vol. 4, no. 3, pp. 161–174.

Received: February 14, 2019.
Accepted: March 15, 2019.

A u t h o r's i n f o r m a t i o n:

Nikolai A. Moldovyan — Dr. Sci. in Technics, Professor, Chief Scientific Collaborate; nmold@mail.ru

Ivan K. Abrosimov — Junior Scientific Collaborate; ivnabr@yandex.ru