УДК 512.624.5 **DOI** 10.15622/sp.18.2.504-530

А.А. Молдовян, Н.А. Молдовян

НОВЫЕ ФОРМЫ СКРЫТОЙ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФИРОВАНИЯ

Молдовян А.А., Молдовян Н.А. **Новые формы скрытой задачи дискретного логарифмирования.**

Аннотация. Предлагаются новые варианты задачи дискретного логарифмирования в скрытой группе, которая представляет интерес для построения постквантовых криптографических протоколов и алгоритмов. Данная задача формулируется над конечными ассоциативными алгебрами с некоммутативной операцией умножения. В известном варианте указанная задача определяется как суперпозиция операций возведения в степень и автоморфного отображения алгебры, представляющей собой конечное некоммутативное кольцо с глобальной двухсторонней единицей, и называется конгруэнц логарифмированием. Ранее было показано, что последняя задача, заданная в конечной алгебре кватернионов, сводится к задаче дискретного логарифмирования в конечном поле, которое является расширением простого поля, над которым задана конечная алгебра кватернионов, и дальнейшие исследования задачи конгруэнц логарифмирования как примитива постквантовых криптосхем следует проводить в направлении поиска новых ее носителей, для которых такое сведение окажется вычислительно нереализуемым. Представлен ряд новых конечных ассоциативных алгебр, обладающих существенно различающимися свойствами в сравнении с алгеброй кватернионов, в частности в них отсутствует глобальная двухсторонняя единица. Это отличие потребовало новой формулировки задачи дискретного логарифмирования в скрытой группе, отличной от варианта конгруэнц логарифмирования. Предложено несколько вариантов такой формулировки, в которых используются локальные единицы различных типов. Рассматриваются левые, правые и двухсторонние локальные единицы, в качестве которых выступают обратимые и необратимые элементы алгебры. Предложены два общих способа построения конечных ассоциативных алгебр с некоммутативным умножением. Первый способ относится к заданию алгебр, имеющих произвольное натуральное значение размерности $m > 1$, второй — к заданию алгебр произвольных четных размерностей. Впервые разработаны алгоритмы цифровой подписи, основанные на вычислительной трудности задачи дискретного логарифмирования в скрытой группе.

Ключевые слова: криптография, шифры с открытым ключом, постквантовые криптосхемы, задача дискретного логарифмирования, конгруэнц логарифмирование, коммутативные шифры, открытое шифрование, цифровая подпись.

1. Введение. Для обеспечения информационной безопасности современных компьютерных технологий широкое практическое применение нашли криптографические алгоритмы и протоколы [1-2], в том числе двухключевые шифры (криптосхемы с открытым ключом), основанные на вычислительной трудности задачи факторизации чисел специального вида [3] и задачи дискретного логарифмирования (ЗДЛ) [4]. Приемлемый уровень стойкости криптосхем, основанных на этих задачах, определяется тем, что наиболее эффективные алгоритмы их решения, известные в настоящее время

и реализуемые с помощью существующей вычислительной техники, имеют субэкспоненциальную (задача факторизации и ЗДЛ в конечных полях) или экспоненциальную сложность (ЗДЛна эллиптической кривой специального вида).

Значительный прогресс в развитии квантовых вычислений[5,6] обусловил достаточно высокую степень актуальности вопроса оценки вычислительной сложности решения ЗДЛ и задачи факторизации на квантовом компьютере. Исследования, выполненные в данном направлении, показали, что обе рассматриваемые задачи имеют полиномиальную сложность в модели квантовых вычислений [7-9]. Данные результаты и прогнозируемое появления в ближайшее десятилетие практически действующих квантовых вычислителей[10], которые способны эффективно решать задачу взлома существующих криптографических алгоритмов и протоколов, основанных на ЗДЛ и задаче факторизации, обусловливают высокую степень актуальности проблемы создания арсенала протоколов электронной цифровой подписи (ЭЦП), открытого распределения ключей и открытого шифрования, которые были бы удобными для практического применения и стойкими к атакам с использованием квантовых компьютеров.

Алгоритмы симметричной криптографии (шифры с разделяемым секретным ключом), например, блочные и поточные шифры, по мнению специалистов, останутся стойкими к криптоанализу с использованием квантовых вычислителей. Однако для обеспечения достаточно высокой стойкости алгоритмов и протоколов криптографии с открытым ключом, в основу последних требуется положить вычислительно трудные задачи, обладающие сверхполиномиальной вычислительной сложностью при их решении с использованием как обычных, так и квантовых компьютеров. Создание практичных алгоритмов и протоколов постквантовой асимметричной (двухключевой) криптографии связан с поиском новых вычислительно трудных задач, пригодных для использования в качестве примитивов криптосхем с открытым ключом.

Откликом на такой вызов стали объявление Национальным институтом стандартов и технологий (НИСТ; National Institute of Standards and Technology, NIST) конкурса на разработку постквантовых криптосхем с открытым ключом[10] и появление регулярно проводимых тематических конференций по проблематике постквантовой криптографии [11].

Для построения постквантовых двухключевых криптосхем ранее было предложено использовать задачу поиска сопрягающего элемента в некоммутативных группах переплетения (braidgroups)[12,13],

называемых также группами кос. Эта идея привлекла внимание исследователей и была использована для построения алгоритмов открытого шифрования, протоколов открытого согласования секретного ключа и электронной цифровой подписи (ЭЦП). Однако в критических публикациях было показано, что в этом подходе имеются принципиальные трудности, связанные с тем, что задача поиска сопрягающего элемента сводится к решению систем линейных уравнений [14]. Последнее ставит под сомнение безопасность многочисленных двухключевых криптосхем, основанных на вычислительной сложности задачи поиска сопрягающего элемента в группах переплетения [15,16].

Более перспективным представляется подход к построению постквантовых криптосхем с открытым ключом, состоящий в комбинировании ЗДЛ с задачей поиска сопрягающего элемента, и приводящий к так называемой ЗДЛ в циклической группе, скрытой в конечной некоммутативной ассоциативной алгебре (КНАА) [17, 18]. Вычислительная сложность последней задачи (называемой также скрытой ЗДЛ) является сверхполиномиальной при ее решении на обычных вычислительных машинах. Однако в работах [17, 19, 20] были предложены полиномиальные алгоритмы сведения скрытой ЗДЛ, заданной над предложенными в [21-23] конечными алгебрами и представленной в известной на тот момент форме (названной конгруэнц логарифмированием), к ЗДЛ в конечном поле. В связи с этим была поставлена задача поиска новых носителей задачи конгруэнц логарифмирования (ЗКЛ) [17, 19], использование которых позволило бы устранить полиномиальную сводимость к ЗДЛ в конечном поле и обеспечить тем самым сверхполиномиальную сложность ЗКЛ при ее решении на квантовом компьютере, то есть потенциальную возможность разработки постквантовых криптосхем на основе ЗКЛ.

Задача построения алгоритмов и протоколов ЭЦП на основе скрытой ЗДЛ до настоящего момента не была решена. Это связано с тем, что ЗКЛ удобна для построения на ее базе протоколов открытого согласования ключа и алгоритмов открытого и коммутативного шифрования, но неочевидно как ее использовать для построения протокола цифровой подписи.

В настоящей работе решается задача поиска новых КНАА, заданных над простым конечным полем $GF(p)$ и обладающих существенно отличающимися свойствами от известных КНАА, и предлагаются новые варианты задания ЗДЛ в скрытой группе, существенно отличающиеся от ЗКЛ. Также описываются два унифицированных способа задания КНАА больших размерностей, которые позволяют построить два различных подкласса КНАА, включающих алгебры больших размерностей. Первый

способ позволяет построить КНАА произвольных размерностей $m \geq 1$, а второй — КНАА произвольных четных размерностей $m \geq 2$. На основе предложенных новых форм задания ЗДЛ в скрытой группе разработаны постквантовые алгоритмы ЭЦП.

2. Конечные некоммутативные ассоциативные алгебры. Рассмотрим конечное векторное пространство размерности m, заданное над простым полем $GF(p)$. Произвольный элемент этого пространства (вектор) V можно представить в виде упорядоченного набора m элементов конечного поля $GF(p)$: $V = (a, b,\ldots, q)$, а также в виде $V = a\mathbf{e} \oplus b\mathbf{i} \oplus\ldots\oplus q\mathbf{v}$, где $\mathbf{e}$, $\mathbf{i}$ и $\mathbf{v}$ — формальные базисные векторы. В последнем выражении слагаемые $a\mathbf{e}$, $b\mathbf{i}$ и $q\mathbf{v}$ обозначают однокомпонентные векторы $(a, 0, \ldots, 0)$, $(0, b, 0,\ldots, 0)$ и $(0, \ldots, 0, q)$, соответственно, и называются компонентами вектора V. Операция сложения векторов V и $V' = (a', b',\ldots, q')$, для которой примем обозначение $\oplus$, определяется как сложение всех одноименных координат:

$$V \oplus V' = \left(a, b,..., q\right) \oplus \left(a', b',..., q'\right) = \\ = \left(a + a', b + b,... q + q'\right),$$

где знак «+» обозначает операцию сложения в поле $GF(p)$.

Определим операцию умножения двух векторов $V = a\mathbf{e} \oplus b\mathbf{i} \oplus\ldots\oplus q\mathbf{v}$ и $X = x\mathbf{e} \oplus y\mathbf{i} \oplus\ldots\oplus w\mathbf{v}$ (обозначаемую знаком $\circ$) как перемножение каждой компоненты первого операнда с каждой компонентой второго операнда, то есть по следующей формуле:

$$V \circ X = \left(a\mathrm{e} \oplus b\mathrm{i} \oplus ... \oplus q\mathrm{v}\right) \circ \left(x\mathrm{e} \oplus y\mathrm{i} \oplus ... \oplus w\mathrm{v}\right) = \\ = ax\left(\mathrm{e} \circ \mathrm{e}\right) \oplus ay\left(\mathrm{e} \circ \mathrm{i}\right) \oplus ... \oplus aw\left(\mathrm{e} \circ \mathrm{v}\right) \oplus \\ \oplus bx\left(\mathrm{i} \circ \mathrm{e}\right) \oplus by\left(\mathrm{i} \circ \mathrm{i}\right) \oplus ... \oplus bw\left(\mathrm{i} \circ \mathrm{v}\right) \oplus ... \\ ... \oplus qx\left(\mathrm{v} \circ \mathrm{e}\right) \oplus qy\left(\mathrm{v} \circ \mathrm{i}\right) \oplus ... \oplus qw\left(\mathrm{v} \circ \mathrm{v}\right),$$

где координаты рассматриваемых однокомпонентных векторов перемножаются как элементы поля $GF(p)$, а произведение пары формальных базисных векторов в каждом слагаемом заменяется на некоторый однокомпонентный вектор, значение которого выбирается по так называемой таблице умножения формальных базисных векторов (ТУФБВ) [23, 24]. Координаты таких однокомпонентных векторов, отличные от единицы поля $GF(p)$, называются структурными коэффициентами. Если последний равен единице, то однокомпонентный вектор обозначается в виде соответствующего базисного вектора. После выполнения указанной за-

мены в правой части последнего выражения каждое слагаемое представляет собой однокомпонентный вектор. Сумма однокомпонентных векторов с одинаковым формальным базисным вектором равна некоторому другому однокомпонентному вектору с тем же базисным вектором. В общем случае это дает сумму m однокомпонентных векторов вида $a''\mathbf{e} \oplus b''\mathbf{i} \oplus \ldots \oplus q''\mathbf{v}$, то есть вектор $V'' = (a'', b'', \ldots, q'')$.

Определенная таким способом операция умножения пары m-мерных векторов является замкнутой в конечном множестве всевозможных векторов размерности m. Рассмотренное конечное векторное пространство с описанной операцией умножения называется конечной m-мерной алгеброй. Если операция умножения в конечной алгебре является ассоциативной и некоммутативной, то последняя называется КНАА.

Для фиксированных значений размерности конечной алгебры и характеристики поля $GF(p)$ путем разработки соответствующих конкретных ТУФБВ можно задать конечные алгебры различных типов, например, представляющие собой конечные расширенные поля $GF(p^m)$, коммутативные кольца [24, 25] и некоммутативные кольца [21-23] с глобальной двухсторонней единицей, алгебры без глобальной единицы [24]. В качестве носителей ЗДЛ в скрытой группе представляют интерес КНАА, которые в частных случаях могут представлять собой конечные некоммутативные кольца с глобальной двухсторонней единицей. Примером последних являются конечная алгебра кватернионов [24] и 8-мерная КНАА, предложенная в [21]. В литературе описано сравнительно малое число примеров КНАА, в связи с чем представляет интерес разработка унифицированных способов их построения для случаев различных размерностей.

В настоящей работе предлагается следующее обобщение ТУФБВ, использованной в [24] для построения 2-мерных КНАА. Для задания m-мерных алгебр при произвольном натуральном значении $m \geq 2$ может быть использована ТУФБВ общего вида, представленного как таблица 1, в которой формальные базисные векторы обозначены как $\mathbf{e}_i$, $i = 0, 1, \ldots, m-1$, а структурные коэффициенты — как μ_i. В данной таблице в каждой ячейке i-ой строке содержится формальный базисный вектор $\mathbf{e}_i$, а в каждой ячейке j-го столбца структурный коэффициент равен μ_j.Результат умножения $\mathbf{e}_i \circ \mathbf{e}_j$ указан в ячейке, расположенной на пересечении i-ой строки и j-го столбца таблицы. Благодаря такому устройству ТУФБВ произведение двух формальных базисных векторов определяется по следующей простой формуле:

$$\mathrm{e}_i \circ \mathrm{e}_j = \mu_j \mathrm{e}_i. \qquad (1)$$

Используя (1), легко показать, что при умножении произвольных трех формальных базисных векторов выполняется свойство ассоциативности:

$$\left\{\left(\mathrm{e}_i \circ \mathrm{e}_j\right) \circ \mathrm{e}_k = \mu_j \mu_k \circ \mathrm{e}_i;\ \ \mathrm{e}_i \circ \left(\mathrm{e}_j \circ \mathrm{e}_k\right) = \mu_j \mu_k \circ \mathrm{e}_i\right\} \Rightarrow$$
$$\Rightarrow \left(\mathrm{e}_i \circ \mathrm{e}_j\right) \circ \mathrm{e}_k = \mathrm{e}_i \circ \left(\mathrm{e}_j \circ \mathrm{e}_k\right).$$

С учетом определения операции умножения векторов из последней формулы следует, что она обладает свойством ассоциативности. Таким образом, таблица 1 задает общий способ построения КНАА произвольной размерности.

Таблица 1. Таблица умножения формальных базисных векторов, задающая некоммутативную ассоциативную операцию умножения векторов произвольной размерности ($\mu_i \in GF(p)$, $i = 0, 1, \ldots, m-1$)

∘	$\mathbf{e}_0$	$\mathbf{e}_1$	…	$\mathbf{e}_i$	…	$\mathbf{e}_j$	…	$\mathbf{e}_k$	…	$\mathbf{e}_{m-1}$
$\mathbf{e}_0$	$\mu_0\mathbf{e}_0$	$\mu_1\mathbf{e}_0$	…	$\mu_i\mathbf{e}_0$	…	$\mu_j\mathbf{e}_0$	…	$\mu_k\mathbf{e}_0$	…	$\mu_{m-1}\mathbf{e}_0$
$\mathbf{e}_1$	$\mu_0\mathbf{e}_1$	$\mu_1\mathbf{e}_1$	…	$\mu_i\mathbf{e}_1$	…	$\mu_j\mathbf{e}_1$	…	$\mu_k\mathbf{e}_1$	…	$\mu_{m-1}\mathbf{e}_1$
…	…	…	…	…	…	…	…	…	…	…
$\mathbf{e}_i$	$\mu_0\mathbf{e}_i$	$\mu_1\mathbf{e}_i$	…	$\mu_i\mathbf{e}_i$	…	$\mu_j\mathbf{e}_i$	…	$\mu_k\mathbf{e}_i$	…	$\mu_{m-1}\mathbf{e}_i$
…	…	…	…	…	…	…	…	…	…	…
$\mathbf{e}_j$	$\mu_0\mathbf{e}_j$	$\mu_1\mathbf{e}_j$	…	$\mu_i\mathbf{e}_j$	…	$\mu_j\mathbf{e}_j$	…	$\mu_k\mathbf{e}_j$	…	$\mu_{m-1}\mathbf{e}_j$
…	…	…	…	…	…	…	…	…	…	…
$\mathbf{e}_k$	$\mu_0\mathbf{e}_k$	$\mu_1\mathbf{e}_k$	…	$\mu_i\mathbf{e}_k$	…	$\mu_j\mathbf{e}_k$	…	$\mu_k\mathbf{e}_k$	…	$\mu_{m-1}\mathbf{e}_k$
…	…	…	…	…	…	…	…	…	…	…
$\mathbf{e}_{m-1}$	$\mu_0\mathbf{e}_{m-1}$	$\mu_1\mathbf{e}_{m-1}$	…	$\mu_i\mathbf{e}_{m-1}$	…	$\mu_j\mathbf{e}_{m-1}$	…	$\mu_k\mathbf{e}_{m-1}$	…	$\mu_{m-1}\mathbf{e}_{m-1}$

Другой предлагаемый унифицированный способ построения КНАА состоит в задании ТУФБВ, определяющей ассоциативную операцию умножения векторов произвольной четной размерности, по следующей ей формуле:

$$\mathrm{e}_i \circ \mathrm{e}_j = \begin{cases} \mathrm{e}_i, & \text{если } (i+j) \bmod 2 = 0; \\ \mathrm{e}_{m-1-i}, & \text{если } (i+j) \bmod 2 = 1. \end{cases} \qquad (2)$$

Формула (2) задает ассоциативную операцию умножения векторов для произвольного четного значения размерности. Действительно, рассмотрим три произвольных m-мерных вектора:

$$A = \sum_{i=0}^{m-1} a_i \mathrm{e}_i,\ B = \sum_{j=0}^{m-1} b_j \mathrm{e}_j \ \text{ и } \ C = \sum_{k=0}^{m-1} c_k \mathrm{e}_k.$$

В соответствии с определением операции умножения векторов получаем следующие соотношения:

$$\left(A \circ B\right) \circ C = \sum_{i,j,k=0}^{m-1} a_i b_j c_k \left(\mathrm{e}_i \circ \mathrm{e}_j\right) \circ \mathrm{e}_k;$$

$$A \circ \left(B \circ C\right) = \sum_{i,j,k=0}^{m-1} a_i b_j c_k \mathrm{e}_i \circ \left(\mathrm{e}_j \circ \mathrm{e}_k\right).$$

Легко показать, что при четном значении m из выражения (2) следует, что при всех возможных значениях тройки индексов (i, j, k)имеет место равенство $\left(\mathrm{e}_i \circ \mathrm{e}_j\right) \circ \mathrm{e}_k = \mathrm{e}_i \circ \left(\mathrm{e}_j \circ \mathrm{e}_k\right)$. Следовательно, выполняется соотношение $\left(A \circ B\right) \circ C = A \circ \left(B \circ C\right)$. Последнее означает, что операция умножения векторов, определенная по формуле (2), является ассоциативной.

Формула (2) описывает ТУФБВ для произвольного четного значения размерности m.В ячейках таблицы общего вида присутствуют только формальные базисные векторы, то есть однокомпонентные векторы с единичным значением координаты. После составления конкретной ТУФБВ для некоторого фиксированного четного значения размерности, можно перейти к этапу нахождения различных вариантов расстановки (распределения) структурных коэффициентов, при которых свойство ассоциативности операции умножения сохраняется. Таким способом составлена таблица 2 для случая задания 4-мерной алгебры, свойства которой описываются в следующем разделе. При использовании ТУФБВ, в которой распределение формальных базисных векторов по ячейкам таблицы зафиксировано, выбором различных распределений структурных коэффициентов и их значений можно задавать различные варианты операции умножения векторов, придающие существенно различные свойства некоммутативным алгебрам, которые заданы прификсированных значениях размерности и характеристики поля $GF(p)$.

В следующих разделах приводятся результаты изучения конкретных КНАА, причем существенное внимание уделено описанию единичных элементов следующих типов: локальных, глобальных, левосторонних, правосторонних и двухсторонних. Интерес к изучению единиц различного вида определяется тем, что их наличие и возможность выбора единичных элементов алгебры используется для задания новых форм скрытой ЗДЛ и построения постквантовых криптосхем.

Задание ЗДЛ в скрытой группе, содержащейся в некоторой КНАА, в качестве криптографического примитива предполагает нали-

чие большого числа циклических групп, имеющих достаточно большое значение порядка. При этом в криптосхемах, основанных на этой задаче, предполагается выполнение операции возведения векторов в целочисленную степень большой разрядности (от 160 до 512 бит в зависимости от задаваемого уровня стойкости). Для выполнения такой операции для больших значений степени используется алгоритм быстрого возведения в степень, основанный на процедуре последовательного возведения в квадрат.

При построении криптосхем с использованием различных форм скрытой ЗДЛ требуется реализовать модифицированную версию алгоритма быстрого возведения в степень, для которой нет необходимости задавать значение единичного вектора, поскольку его вид изменяется в зависимости от выбора КНАА конкретного вида, от типа используемых единичных элементов и от выбора циклических групп, в которых выполняются вычисления в рамках разрабатываемой криптосхемы.

Данная версия алгоритма быстрого возведения в степень играет значительную роль при выполнении экспериментальных исследований свойств разрабатываемых КНАА. С ее помощью возможно нахождение глобальных и локальных двухсторонних единичных элементов без предварительного вывода математических формул, описывающих координаты единичных элементов.

3. Задание 4-мерной КНАА с параметризуемым умножением. Рассмотрим КНАА размерности 4, которая является кольцом с параметризуемой операцией умножения, различные модификации которой являются взаимно ассоциативными. Умножение векторов задается по ТУФБВ, представленной в виде таблицы 2. Различные модификации операции умножения задаются различными наборами фиксируемых значений структурных коэффициентов μ и λ.

Пусть даны векторы V, W, U и две различные модификации операции умножения $\circ$ и $*$. Под взаимной ассоциативностью операций $\circ$ и $*$ понимается выполнимость следующего соотношения:

$$(V \circ W) * U = V \circ (W * U). \tag{3}$$

Используя определение операции умножения, легко показать, что для КНАА, заданной рассматриваемой ТУФБВ, любые две модификации умножения являются взаимно ассоциативными. Рассмотренные в литературе конечные алгебры не обладают данным свойством, которое представляет самостоятельный интерес для использования в криптографических алгоритмах.

Таблица 2. Строение ТУФБВ для задания КНАА, являющейся кольцом с параметризуемой операцией умножения ($\mu, \lambda \in GF(p)$; $\mu \neq \lambda$)

∘	**e**	**i**	**j**	**k**
e	**e**	μ**k**	μ**e**	**k**
i	**j**	λ**i**	λ**j**	**i**
j	**j**	μ**i**	μ**j**	**i**
k	**e**	λ**k**	λ**e**	**k**

При условии $\lambda \neq \mu$ умножение 4-мерных векторов, выполняемое по таблице 1, задает КНАА, являющуюся конечным кольцом с глобальной единицей, равной вектору:

$$E = \left(\frac{\lambda}{\lambda - \mu}, \frac{1}{\lambda - \mu}, \frac{1}{\mu - \lambda}, \frac{\mu}{\lambda - \mu} \right). \tag{4}$$

В этом кольце обратимы все векторы $V = (a, b, c, d)$, координаты которых удовлетворяют условию $dc - ab \neq 0$. Если имеет место $dc - ab = 0$, то вектор V необратим. Из последнего условия легко найти число необратимых векторов, которое равно $p^3 + p^2 - p$, и значение порядка некоммутативной мультипликативной группы кольца:

$$\Omega = p^4 - \left(p^3 + p^2 - p \right) = p\left(p - 1 \right)\left(p^2 - 1 \right).$$

Для множества необратимых векторов N можно ввести понятие локальных единиц. Если выполняется соотношение $E_{(} \circ N = N$, то вектор $E_{(}$ называется левой локальной единицей, а если $N \circ E_{)} = N$, то вектор $E_{)}$ называется правой локальной единицей для вектора N. В случае выполнимости соотношений $E_{(N)} \circ N = N$ и $N \circ E_{(N)} = N$ вектор $E_{(N)}$ называется двухсторонней локальной единицей для вектора N. Фиксированному необратимому вектору $N = (a, b, c, d)$ соответствует множество различных локальных единиц каждого вида. Множество левых локальных единиц описывается формулой:

$$E_{(} = \left(x, y, z, w \right) = \left(i, \frac{c}{a + \lambda c} - \frac{a + \mu c}{a + \lambda c} j,\ j, \frac{a}{a + \lambda c} - \frac{a + \mu c}{a + \lambda c} i \right), \tag{5}$$

где $i, j = 0, 1, 2, \ldots, p - 1$. В это множество входят необратимые и обратимые элементы рассматриваемого некоммутативного кольца, вклю-

чая глобальную единицу (4). Множество необратимых левых локальных единиц является подмножеством множества (5) и описывается формулой:

$$E'_{(} = (x, y, z, w) = \left(i, \frac{c}{a+\lambda c} - \frac{a+\mu c}{a+\lambda c} \cdot \frac{c}{a} i;\ \frac{c}{a} i;\ \frac{a}{a+\lambda c} - \frac{a+\mu c}{a+\lambda c} i \right), \tag{6}$$

где $i = 0, 1, 2, \ldots, p-1$.

Множество правых локальных единиц вектора N описывается формулой:

$$E_{)} = (x, y, z, w) = \left(\frac{c}{b+c} - \frac{\lambda b+\mu c}{b+c} k, h, k,\ \frac{b}{b+c} - \frac{\lambda b+\mu c}{b+c} h \right), \tag{7}$$

где $h, k = 0, 1, 2, \ldots, p-1$. Множество необратимых правых локальных единиц вектора N описывается формулой:

$$E'_{(} = (x, y, z, w) = \left(\frac{c}{b+c} - \frac{\lambda b+\mu c}{b+c} \cdot \frac{c}{b} h,\ h,\ \frac{c}{b} h,\ \frac{b}{b+c} - \frac{\lambda b+\mu c}{b+c} h \right), \tag{8}$$

где $h = 0, 1, 2, \ldots, p-1$.Множество двухсторонних локальных единиц представляет собой пересечение множеств (5) и (7) и описывается формулой:

$$E_{()} = (x, y, z, w) = \left(\frac{c}{b+c} - \frac{\lambda b+\mu c}{b+c} k,\ \ \frac{c}{a+\lambda c} - \frac{a+\mu c}{a+\lambda c} k, \right.$$
$$\left. k,\ \ \frac{ab+\mu c^2}{(b+c)(a+\lambda c)} - \frac{(a+\mu c)(\lambda b+\mu c)}{(b+c)(a+\lambda c)} k \right), \tag{9}$$

где $k = 0, 1, 2, \ldots, p-1$.В последнем множестве присутствует единственный необратимый вектор, содержащийся одновременно в множествах (6) и (8) и соответствующий значению:

$$k = k_0 = \frac{c^2}{ab + ac + \mu c^2 + \lambda bc} = \frac{c}{d + a + \mu c + \lambda b}. \tag{10}$$

Легко показать, что локальные единицы вектора N являются соответствующими локальными единицами для вектора N^uпри произвольном натуральном значении степени u. Учитывая конечность рассматриваемого кольца, можно показать, что при некотором значении

степени $u = \omega$ имеет место $N^{\omega} = E'_{(N)}$, где $E'_{(N)}$ двухсторонняя локальная единица вектора N, значение которой может быть вычислено по (9) при значении k_0, задаваемом формулой (10). Таким образом, всевозможные степени необратимого вектора N порождают циклическую группу порядка ω с единицей $E'_{(N)}$, что может быть использовано для задания ЗДЛ в скрытой подгруппе, отличной от ЗКЛ.

4. Задание ЗДЛ в скрытой группе необратимых векторов. Пусть в КНАА, рассмотренной в разделе 3, даны обратимый вектор Q и необратимый вектор N, такие, что выполняется неравенство $Q \circ N \neq N \circ Q$. Выберем некоторое произвольное достаточно большое натуральное число u и вычислим вектор F по формуле:

$$F = Q^{q-u} \circ E_{(N)}, \tag{11}$$

где $E_{(N)}$ — некоторый элемент множества (9), q — порядок вектора Q.

Зададим вычисление открытого ключа Y по формуле:

$$Y = Q^{u-t} \circ F \circ N^{x} \circ Q^{t}, \tag{12}$$

где пара случайно выбираемых чисел t и x являются личным секретным ключом владельца открытого ключа Y. Некоторый другой пользователь выбирает секретный ключ в виде пары случайных чисел t' и x' и вычисляет свой открытый ключ:

$$Y = Q^{u-t} \circ F \circ N^{x} \circ Q^{t}.$$

Первый и второй, обменявшись своими открытыми ключами, имеют возможность вычислить общее секретное значение в виде вектора Z по следующим двум формулам:

$$Z = Q^{u-t'} \circ Y^{x'} \circ Q^{t'}; \; Z = Q^{u-t} \circ Y'^{x} \circ Q^{t}. \tag{13}$$

То, что каждая из двух последних формул задает вычисление одного и того же значения, легко доказывается с учетом соотношения (11) и следующего достаточно очевидного равенства:

$$\left(Q^{u-t} \circ F \circ N \circ Q^{t}\right)^{x} = Q^{u-t} \circ F \circ N^{x} \circ Q^{t}.$$

Формулы (12) и (13) задают схему открытого согласования секретного ключа, стойкость которой определяется вычислительной сложность нахождения пары значений t и x по известным параметрам

Y, *Q*, *N*, *F* и *u*. При известном значении *t*нахождение *x* составит ЗДЛ в группе, генерируемой элементом:

$$G = Q^{u-t} \circ F \circ N \circ Q^t.$$

Вычисление двух неизвестных значений *t* и *x*из (12) определяет ЗДЛ в скрытой группе. Последняя задача имеет существенные отличия от ЗКЛ, которая задается формулой:

$$Y = Q^{q-t} \circ G^x \circ Q^t, \tag{14}$$

где *Q* и *G* — пара неперестановочных обратимых элемента конечного некоммутативного кольца; *t*и *x* — неизвестные натуральные значения.

Сравнение показывает, что ЗДЛ в скрытой группе, задаваемая по формуле (12) является более гибкой в плане большего числа задаваемых параметров.

Специфичным для формулы (12) является возможность произвольного выбора степени *u*и локальной двухсторонней единицы, который определяет значение вектора *F*, вычисляемого по формуле (11). Следует заметить, что криптосхема, задаваемая формулами (11), (12) и (13), работает корректно, если в (11) вместо двухсторонней локальной единицы $E_{(N)}$ взять произвольную левую или правую локальную единицу из множеств (5) или (7) соответственно.

Симметричным по отношению к рассмотренному является вариант задания ЗДЛ в скрытой группе по следующим двум формулам:

$$F = E_{(;)} \circ Q^{q-u}, \tag{11′}$$

где $E_{(;)}$ — некоторая локальная единица (левая, правая или двусторонняя); при этом в качестве $E_{(;)}$ можно брать как обратимый, так и необратимый элемент относительно глобальной единицы (4); и

$$Y = Q^{u-t} \circ N^x \circ F \circ Q^t. \tag{12′}$$

Самостоятельное значение имеет способ задания ЗДЛ в скрытой группе по следующим двум формулам:

$$F_1 = Q^{q-u} \circ F_2^{-1} \circ E_{(;)}, \tag{15}$$

где F_2 — произвольно выбираемый обратимый элемент конечного некоммутативного кольца;

$$Y = Q^{u-t} \circ F_1 \circ N^x \circ F_2 \circ Q^t. \tag{16}$$

Используя формулу (15), легко показать, что справедливо следующее соотношение:

$$Q^{u-t} \circ F_1 \circ N^x \circ F_2 \circ Q^t = \left(Q^{u-t} \circ F_1 \circ N \circ F_2 \circ Q^t\right)^x. \quad (17)$$

Пара элементов F_1 и F_2 может быть получена также выбором в качестве F_1 произвольного обратимого элемента и последующим вычислением значения F_2 по формуле:

$$F_2 = E_{(;)} \circ F_1^{-1} \circ Q^{q-u}.$$

В криптосхемах, задаваемых парой формул (11′) и (12′) и парой формул (15) и (16), согласование общего секретного ключа Z по открытому каналу выполняется также по формулам (13).

5. Задание ЗДЛ в скрытой группе алгебры без единицы. В разделе 4 предложены новые варианты задания ЗДЛ в скрытой группе КНАА, являющейся конечным некоммутативным кольцом. В представленных вариантах используется наличие глобальной единицы, относительно которой рассматривается обратимость (и необратимость) элементов КНАА, например, алгебры, представленной в разделе 3.

Для КНАА, не содержащих глобальной двухсторонней единицы, указанные способы задания ЗДЛ в скрытой группе не могут быть применены. Примерами КНАА последнего типа являются ассоциативные алгебры с операцией умножения векторов, задаваемой по ТУФБВ, представленной в таблице 1, для случаев размерности векторного пространства $m = 2$ [24]и$m = 3, 4, 5$.Можно предположить, что для случая произвольной размерности КНАА с операцией умножения определяемой по таблице 1 глобальная двухсторонняя единица отсутствует. Простое строение данной ТУФБВ позволяет предположить, что могут быть получены общие формулы для произвольного значения размерности m, описывающие единичные элементы и делители нуля в КНАА с операцией умножения, заданной по таблице 1, однако это представляется самостоятельной задачей.

Рассмотрение КНАА без глобальной двусторонней единицы в качестве носителя ЗДЛ в скрытой группе предполагает использование другого подхода, в котором не требуется применение обратимых элементов. Потенциальная возможность применения таких КНАА в качестве носителей ЗДЛ в скрытой группе связана с существованием двухсторонних локальных единиц, с которыми связаны подмножества элементов алгебры, которые образуют циклические группы. Например, в

трехмерной алгебре, заданной таблицей 1 для случая значений структурных коэффициентов $\mu_1 = \mu_2 = \mu_3 = 1$ множество правых локальных единиц для элемента $N = (a, b, c)$, координаты которого удовлетворяют условию $a + b + c \neq 0$, описывается формулой:

$$E_{)} = (x, y, z) = (i, j, 1 - i - j),$$

где $i, j = 0, 1, 2, \ldots, p - 1$. Это множество правых единиц является глобальным в том смысле, что входящие в него правые единицы действуют как таковые на всевозможные элементы N, удовлетворяющие указанному условию. Элементу $N = (a, b, c)$ соответствует единственная левая локальная единица, которая совпадает с единственной двухсторонней локальной единицей:

$$E_{(} = E_{()} = (x, y, z) = \left(\frac{a}{a+b+c}, \frac{b}{a+b+c}, \frac{c}{a+b+c} \right). \tag{18}$$

Всевозможные степени элемента N образуют циклическую группу с единицей (18).

Другим примером является 4-мерная КНАА с операцией умножения, определяемой по таблице 3. В данной алгебре существуют локальные единицы только для векторов$N = (a, b, c, d)$, координаты которых удовлетворяют соотношению $ac = bd$. Множество правых локальных единиц вектора N описывается формулой:

$$E_{)} = (x, y, z, w) = \left(i, j, \frac{b}{\mu a + \lambda b} - j, \frac{a}{\mu a + \lambda b} - i \right), \tag{19}$$

где $i, j = 0, 1, 2, \ldots, p - 1$, а множество левых локальных единиц — формулой:

$$E_{(} = (x, y, z, w) = \left(k, \ \frac{a}{\lambda(a+d)} - \frac{\mu}{\lambda} k, \ h, \ \frac{d}{\mu(a+d)} - \frac{\lambda}{\mu} h \right), \tag{20}$$

где $k, h = 0, 1, 2, \ldots, p - 1$.

Множество локальных двухсторонних единиц для Nопределяется пересечением множеств (19) и (20), что дает следующую формулу:

$$E_{(N)} = \left(k, \frac{a}{\lambda(a+d)} - \frac{\mu}{\lambda} k, \frac{b}{\mu a + \lambda b} - \frac{a}{\lambda(a+d)} + \frac{\mu}{\lambda} k, \frac{a}{\mu a + \lambda b} - k \right), \tag{21}$$

где $k = 0, 1, 2, \ldots, p - 1$.

Таблица 3. Правило умножения формальных базисных векторов в 4-мерной КНАА без глобальной единицы (μ, λ ∈ *GF*(*p*); μ ≠ λ)

∘	**:e**	**:i**	**:j**	**:k**
:e	**:μe**	**:μi**	**:μi**	**:μe**
:i	**:λe**	**λi**	**λi**	**λe**
:j	**:λk**	**λj**	**λj**	**λk**
:k	**:μk**	**μj**	**μj**	**μk**

В множестве (21) содержится только один элемент $E_{(N)} = (a', b', c', d')$, координаты которого удовлетворяют условию $a'c' = b'd'$. Этот элемент является единицей циклической группы, которую порождают всевозможные степени *N*, и его координаты могут быть вычислены по формуле (21) при значении:

$$k = k_0 = \frac{a^2}{(a+d)(\mu a + \lambda b)}. \qquad (21')$$

Таким образом, вычисление двухсторонней локальной единицы $E_{(N)}$ может быть выполнено по формуле (21) или путем возведения элемента *N* в степень, кратную порядку циклической группы, генерируемой всевозможными степенями *N*. Это может быть проиллюстрировано следующим вычислительным экспериментом, выполненным для 4-мерного вектора:

$$N = (908829491, 124888084499, 18949746053, 676148046414381)$$

при значениях p = 1108878614179151; μ = 257; λ = 13:

$$N^{p-1} = (1016120000861220,\ 58254033235670,\ 20300751201639,\ 697158116826006).$$

Вычисление по формуле (21) дает значение k_0 = 1016120000861220, подстановка которого в (21) дает следующее:

$$E_{(N)} = N^{p-1}.$$

Элемент $E_{(N)} = (a', b', c', d')$ является правой единицей подмножества КНАА, которое описывается формулой:

$$V_N = V \circ E_{(N)}, \qquad (22)$$

где V пробегает все элементы КНАА. Элемент $E_{(N)}$ является левой единицей подмножества КНАА, которое описывается формулой:

$$V'_N = E_{(N)} \circ V.$$

Ни в одном из двух последних подмножеств КНАА элемент $E_{(N)}$не является двухсторонней единицей для всех элементов подмножества. Каждое из этих подмножеств замкнуто относительно операции умножения. В подмножестве (22) можно задать автоморфизм относительно операции умножения, описываемый формулой:

$$\psi_{N,t}(V_N) = N^{\eta-t} \circ V_N \circ N^t, \tag{23}$$

где η — порядок циклической группы, генерируемой степенями элемента N. Действительно, для произвольных двух элементов V_{N1} и V_{N2} множества (22) выполняются соотношения:

$$\begin{aligned}\psi_{N,t}\left(V_{N1} \circ V_{N2}\right) &= N^{\eta-t} \circ (V_{N1} \circ V_{N2}) \circ N^t = \\ &= N^{\eta-t} \circ \left(V_{N1} \circ E_{(N)} \circ V_{N2}\right) \circ N^t = \\ &= \left(N^{\eta-t} \circ V_{N1} \circ N^t\right) \circ \left(N^{\eta-t} \circ V_{N2} \circ N^t\right) = \\ &= \psi_{N,t}\left(V_{N1}\right) \circ \psi_{N,t}\left(V_{N2}\right).\end{aligned}$$

В силу указанного автоморфизма имеет место следующая формула:

$$\left(N^{\eta-t} \circ V_N \circ N^t\right)^x = N^{\eta-t} \circ V_N^x \circ N^t, \tag{24}$$

которая может быть использована для построения криптосхемы открытого согласования общего секретного ключа, в которой формирование открытого ключа Yпо секретному ключу (x, t) выполняется по формуле:

$$Y = N^{\eta-t} \circ V_N^x \circ N^t, \tag{25}$$

где N, $V_{(N)}$ и η — параметры криптосхемы, а вычисление общего секретного ключа — по формулам:

$$Z = N^{\eta-t} \circ Y'^x \circ N^t, Z = N^{\eta-t'} \circ Y^{x'} \circ N^{t'}. \tag{26}$$

Формула (25) определяет еще один вариант задания ЗДЛ в скрытой группе, который отличается от ЗКЛ тем, что его носителем является КНАА без глобальной единицы. При выборе параметров N и $V_{(N)}$следует выполнить естественное требование, состоящее в выполнении неравенства $N \circ V_{(N)} \neq V_{(N)} \circ N$.

Для рассматриваемой в разделе 5 КНАА был сформулирован ряд положений, касающихся векторов вида $N = (a, b, c, d)$,где $ac = bd$. Число таких векторов равно $p^3 + p^2 - p$. Возникает естественный вопрос об остальных $p^4 - (p^3 + p^2 - p)$ векторов вида $V = (a', b', c', d')$, где $a'c' \neq b'd'$. Данная 4-мерная КНАА является весьма своеобразной и векторы последнего вида при умножении «самоустраняются», то есть умножение двух векторов произвольного вида дает в результате вектор первого типа. Можно сказать, что операция умножения обладает сжимающим свойством.

6. Постквантовые алгоритмы цифровой подписи. Интерес к использованию ЗДЛ в скрытой группе для построения схем электронной цифровой подписи (ЭЦП) связан с актуальностью разработки алгоритмов ЭЦП, стойких к атакам с использованием гипотетического квантового компьютера. Однако для выполнения такой разработки требуется использование новых форм задания указанной вычислительно трудной задачи. В данном разделе предлагаются новые формы задания ЗДЛ в скрытой группе, позволяющие реализовать построение алгоритмов ЭЦП с использованием вычислений в КНАА.

При задании скрытой ЗДЛ над алгеброй с глобальной двухсторонней единицей существенным моментом является использование необратимых элементов в качестве генератора скрытой циклической группы. Для необратимых векторов существует большое число локальных единиц различного типа, например, описываемых формулами (5) и (7) в случае 4-мерной КНАА из раздела 3, задаваемой с помощью таблицы 2. Зададим формирование личного секретного ключа подписанта в соответствии со следующей процедурой:

1. Выбрать случайный необратимый вектор N, локальный порядок которого равен достаточно большому простому числу η.

2. Выбрать случайные векторы E_1, E_2 и E_3из множества локальных единиц, соответствующих вектору N(в качестве E_1 и E_2 выбираются обратимые векторы).

3. Сгенерировать обратимый вектор G, такой, что имеет место неравенство $N \circ G \neq G \circ N$, и вычислить следующие векторы:

$$U = E_1 \circ G^{-1};\ H = U^{-1} \circ E_2; T = E_3 \circ H^{-1}. \qquad (27)$$

4. Сгенерировать случайное число $x < \eta$.

Следует отметить, что вычисляемый на шаге 3 вектор U является обратимым элементом как произведение двух обратимых элементов, поэтому существует обратное к нему значение U^{-1}, используемое при вычислении вектора H. Последний также обратим, и существует обратное к нему значение H^{-1}, которое используется при вычислении вектора T. Нахождение обратных значений выполняется путем решения соответствующих систем из четырех линейных уравнений.

Личный секретный ключ подписанта представляет собой целое число x и тройку векторов N, G и T.Открытый ключ подписанта представляет собой пару векторов Y и Q, вычисляемых по следующим двум формулам:

$$Y = G \circ N^x \circ U; Q = H \circ N \circ T. \tag{28}$$

Вычисляемые векторы Y и Qпринадлежат различным циклическим группам, содержащимся в используемой КНАА, но связаны они с одной и той же замаскированной циклической группой, генерируемой всевозможными степенями необратимого вектора N. Скрытая ЗДЛ состоит в вычислении значения x по известным 4-мерным векторам Y и Q, которые принадлежат разным циклическим группам, содержащимся в используемой КНАА.

Процедура генерации ЭЦП к некоторому заданному электронному документу M выполняется следующим образом:

1. Сгенерировать случайное число $k < \eta$.

2. Вычислить вектор $W = G \circ N^k \circ T$.

3. Вычислить первый элемент ЭЦП в виде двоичного числа $e = F_h(M, W)$, где F_h — некоторая специфицированная хэш-функция.

4. Вычислить второй элемент ЭЦП в виде двоичного числа s:

$$s = k - ex \bmod \eta.$$

Процедура проверки подлинности ЭЦП (e, s) к документу M выполняется по открытому ключу (Y, Q) следующим образом:

1. Вычислить вектор:

$$\tilde{W} = Y^e \circ Q^s.$$

2. Вычислить двоичное число $\tilde{e} = F_h\left(M, \tilde{W}\right)$.

3. Сравнить значения $\tilde{e}$ и e. Если $\tilde{e} = e$, то подпись (e, s) является подлинной. В противном случае подпись отклоняется.

Вычисление значения подписи выполняется с учетом операций возведения в степень в циклической группе, задаваемой вектором N, а проверка подлинности цифровой подписи осуществляется с помощью операций возведения в степень в двух других циклических группах, а именно в конечных группах, порождаемых векторами Y и Q, представляющих собой элементы открытого ключа. В связи с этим корректность предложенной схемы подписи не является очевидной, что делает целесообразным рассмотрение формального доказательства ее корректности. Последнее выполняется путем подстановки значения ЭЦП (e, s) на выходе процедуры генерации подписи на вход процедуры проверки подлинности ЭЦП. С учетом формул (28) и справедливости соотношений $U \circ G = E_1$, $U \circ H = E_2$ и $T \circ H = E_3$, вытекающих из (27), такая подстановка дает следующее:

$$\tilde{W} = Y^e \circ Q^s = \left(G \circ N^x \circ U\right)^e \circ \left(H \circ N \circ T\right)^s =$$

$$= G \circ \left(N^x \circ E_1\right)^{e-1} \circ N^x \circ U \circ H \circ \left(N \circ E_3\right)^{s-1} \circ N \circ T =$$

$$= G \circ \left(N^x\right)^{e-1} \circ N^x \circ E_2 \circ \left(N\right)^{s-1} \circ N \circ T = G \circ N^{ex} \circ E_2 \circ N^s \circ T =$$

$$= G \circ N^{ex+s} \circ T = G \circ N^{ex+(k-ex)} \circ T = G \circ N^k \circ T =$$

$$= W \;\Rightarrow\; \tilde{e} = F_h\left(M, \tilde{W}\right) = F_h\left(M, W\right) = e\,.$$

В представленной схеме ЭЦП процедура проверки подписи состоит в выполнении операций над векторами, принадлежащими двум различным циклическим группам КНАА. При этом при вычислении подписи используется связь элементов Y и Q открытого ключа с одной и той же циклической группой, которая скрыта для всех, кроме владельца открытого ключа. В предположении, что потенциальному атакующему известны значения G, U, H и T (это дает возможность вычислить значения N и N^x), для подделки подписи ему потребуется найти число x, то есть решить задачу дискретного логарифмирования в циклической группе, генерируемой вектором N. При использовании гипотетического квантового вычислительного устройства последняя задача может быть решена за полиномиальное время. Однако, атакующему известны только векторы Y и Q, поэтому возможность применения квантового компьютера для взлома предложенной схемы ЭЦП связана со сведением используемой ЗДЛ в скрытой группе к ЗДЛ в явно заданной циклической группе. В настоящее время этот вопрос является мало изученным и потребуется выполнение дополнительных исследований со стороны независимых исследователей, чтобы получить достаточную экспертную

оценку стойкости предложенной схемы ЭЦП к атакам с использованием квантового вычислительного устройства.

Использование необратимого вектора N в описанной схеме ЭЦП связано с предотвращением потенциальных атак, основанных на гомоморфном отображении КНАА в поле $GF(p)$,которые рассмотрены в [21].

Другая новая форма задания скрытой ЗДЛ может быть сформулирована для случая использования КНАА без глобальной двухсторонней единицы (см. раздел 5) следующим образом:

1. Выбрать случайный вектор $N = (a, b, c, d)$ большого простого порядка η, удовлетворяющий условию $ac = bd$.

2. Сформировать случайные векторыU,G, T, H и L, такие, что выполняются условия $U \circ G = E_1$, $T \circ H = E_2$ и $U \circ L \circ H = E_3$, где E_1, E_2 и E_3 — локальные единицы произвольных типов.

3. Сгенерировать случайное число $x < \eta$.

Личный секретный ключ подписанта представляет собой целое число x и тройку векторов N, G, и T.Открытый ключ подписанта представляет собой тройку векторов Y, Qи L,в которой первые два вычисляются по формулам (28).Постквантовая схема ЭЦП описывается следующими двумя алгоритмами.

Алгоритм генерации ЭЦП к некоторому заданному электронному документу M:

1. Сгенерировать случайное число $k < \eta$.

2. Вычислить вектор $W = G \circ N^k \circ T$.

3. Вычислить первый e и второй элементы ЭЦП по формулам $e = F_h(M, W)$ и $s = k - ex \bmod \eta$.

Алгоритм проверки подлинности ЭЦП (e, s) к документу M:

1.Вычислить вектор $\tilde{W} = Y^e \circ L \circ Q^s$.

2. Вычислить значение $\tilde{e} = F_h(M, \tilde{W})$.

3. Если $\tilde{e} = e$, то подпись (e, s) признается подлинной. В противном случае подпись отклоняется.

Доказательство корректности работы второй схемы ЭЦП выполняется следующим образом:

$$\tilde{W} = Y^e \circ L \circ Q^s = \left(G \circ N^x \circ U\right)^e \circ L \circ \left(H \circ N \circ T\right)^s =$$

$$= G \circ N^{ex} \circ U \circ L \circ H \circ N^s \circ T = G \circ N^{ex} \circ E_3 \circ N^s \circ T =$$

$$= G \circ N^{ex+s} \circ T = G \circ N^{ex+(k-ex)} \circ T = G \circ N^k \circ T =$$

$$= W \quad \Rightarrow \quad \tilde{e} = e\,.$$

Предложенные формы задания ЗДЛ в скрытой группе и алгоритмы ЭЦП на их основе заслуживают внимания криптографов, поскольку при подтверждении их стойкости к квантовым атакам устраняются недостатки (большой размер подписи и открытого ключа, ограниченное число документов, которые могут быть подписаны при регистрации одного открытого ключа), присущие постквантовым схемам ЭЦП, предложенным в рамках конкурса НИСТ по разработке постквантовых криптосхем с открытым ключом.

Представляет интерес рассмотрение возможности разработки на основе предложенных схем ЭЦП протоколов слепой цифровой подписи по аналогии с протоколами слепой подписи, основанными на ЗДЛ и описанными в работах[24, 25].

7. Заключение. В данной статье предложены две новые 4-мерные КНАА и общий способ построения КНАА произвольной размерности $m \geq 2$. Одна из предложенных алгебр является кольцом с глобальной двухсторонней единицей и представляет интерес в качестве нового носителя ЗКЛ. Для этой алгебры предложены два новых варианта задания ЗДЛ в скрытой группе, отличные от ЗКЛ. Вторая четырехмерная алгебра не содержит глобальной двухсторонней единицы и для нее предложен третий вариант ЗДЛ в скрытой группе. Другие две новые формы задания скрытой ЗДЛ предложены и использованы для построения постквантовых алгоритмов ЭЦП.

Алгоритмы ЭЦП, основанные на вычислительной трудности скрытой ЗДЛ, разработаны впервые. Предложенные КНАА и новые формы задания скрытой ЗДЛ представляют существенный интерес для разработки протоколов открытого согласования общего секретного ключа, коммутативного шифрования и ЭЦП, стойких к атакам с использованием квантовых вычислителей.

Рассмотренные ТУФБВ могут быть применены также и для задания КНАА над конечными полями, отличными от $GF(p)$, в частности над полями $GF(2^s)$. При этом в последнем случае самостоятельный интерес представляет использование в качестве степени расширения двоичного поля s простого числа, равного степени Мерсенна, за счет чего можно добиться формирования конечных циклических групп, (являющихся подмножествами задаваемых КНАА), которые обладают простым значением порядка. Для данного варианта построения КНАА применимы все предложенные варианты задания ЗДЛ в скрытой подгруппе.

Скрытая ЗДЛ представляется перспективной в качестве кандидата на универсальный постквантовый криптографический примитив, на основе которого могут быть разработаны постквантовые двухключевые алгоритмы и протоколы различного типа.

Литература

1. *Sirwan A., Majeed N.* New Algorithm for Wireless Network Communication Security // International Journal on Cryptography and Information Security. 2016. vol. 6. no. 3/4. pp. 1–8.
2. *Feng Y., Yang G., Liu. J.K.* A new public remote integrity checking scheme with user and data privacy // International Journal of Applied Cryptography. 2017. vol. 3. no 3. pp. 196–209.
3. *Chiou S.Y.* Novel Digital Signature Schemes based on Factoring and Discrete Logarithms // International Journal of Security and Its Applications. 2016. vol. 10. no. 3. pp. 295–310.
4. *Poulakis D.* A variant of Digital Signature Algorithm // Designs, Codes and Cryptography. 2009. vol. 51. no. 1. pp. 99–104.
5. *Yan S.Y.* Quantum Computational Number Theory // Springer. 2015. 252 p.
6. *Yan S.Y.* Quantum Attacks on Public-Key Cryptosystems // Springer. 2014. 207 p.
7. *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.
8. *Smolin J.A., Smith G., Vargo A.* Oversimplifying quantum factoring // Nature. 2013. vol. 499. no. 7457. pp. 163–165.
9. *Hamdi S.M., Zuhori S.T., Ffiroz M., Biprodip P.* A Compare between Shor's quantum factoring algorithm and General Number Field Sieve // 2014 International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT). 2014. pp. 1–6.
10. 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: 06.03.2018).
11. *Verma G.K.* A Proxy Blind Signature Scheme over Braid Groups // International Journal of Network Security. 2009. vol. 9. no 3. pp. 214–217.
12. *Hiranvanichakorn P.* Provably Authenticated Group Key Agreement based on Braid Groups − The Dynamic Case // International Journal of Network Security. 2017. vol. 19. no. 4. pp. 517−527.
13. *Myasnikov A., Shpilrain V., Ushakov A.* A Practical Attack on a Braid Group Based Cryptographic Protocol // Annual International Cryptology Conference. 2005. vol. 3621. pp. 86−96.
14. *Chaturvedi A., Lal S.* An Authenticated Key Agreement Protocol Using Conjugacy Problem in Braid Groups // International Journal of Network Security. 2008. vol. 6. no. 2. pp. 181–184.
15. *Verma G.K.* Probable Security Proof of a Blind Signature Scheme over Braid Groups // International Journal of Network Security. 2011. vol. 12. no. 2. pp. 118−120.
16. *Kuzmin A.S. et al.* Cryptographic Algorithms on Groups and Algebras // Journal of Mathematical Sciences. 2017. vol. 223. no. 5. pp. 629−641.
17. *Moldovyan D.N., Moldovyan N.A., Shcherbacov V.A.* Non-commutative finite associative algebras of 3-dimensional vectors // Quasigroups and related systems. 2018. vol. 26. no. 1. pp. 109−120.
18. *Кузьмин А.С. и др.* Криптографические алгоритмы на группах и алгебрах // Фундаментальная и прикладная математика. 2015. Т. 20. № 1. С. 205−222.
19. *Глухов М.М.* К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах // Математические вопросы криптографии. 2010. Т. 1. № 4. С. 5−22.
20. *Moldovyan D.N., Moldovyan N.A.* Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms // Quasigroups and Related Systems. 2010. vol. 18. pp. 177−186.

21. *Moldovyan D.N., Moldovyan N.A.* A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols // International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. 2010. vol. 6258. pp. 183−194.
22. *Moldovyan D.N.* Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. vol. 18. pp. 165−176.
23. *Moldovyan A.A., Moldovyan N.A., Shcherbacov. V.A.* Non-commutative finite associative algebras of 2-dimension vectors // Computer Science Journal of Moldova. 2017. vol. 25. no. 3(75). pp. 344−356.
24. *Camenisch J.L., Piveteau J.-M., Stadler M.A.* Blind Signatures Based on the Discrete Logarithm Problem //Workshop on the Theory and Application of Cryptographic Techniques. 1994. pp. 428–432.
25. *Pointcheval D., Stern J.* Security Arguments for Digital Signatures and Blind Signatures // Journal of Cryptology. 2000. vol. 13. no. 3. pp. 361−396.

Молдовян Александр Андреевич — д-р техн. наук, профессор, главный научный сотрудник, лаборатория кибербезопасности и постквантовых криптосистем, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: компьютерная безопасность, криптография, безопасность компьютерных сетей, управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома. Число научных публикаций — 200. maa1305@yandex.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Российская Федерация; р.т.: +7(812)328–5185.

Молдовян Николай Андреевич — д-р техн. наук, профессор, главный научный сотрудник, лаборатория кибербезопасности и постквантовых криптосистем, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: компьютерная безопасность, криптография, симметричные и асимметричные криптосистемы, электронная цифровая подпись, аутентификация, блочные шифры, псевдовероятностные шифры. Число научных публикаций — 250. nmold@mail.ru; 39, 14-я линия В.О., 199178, Санкт-Петербург, Российская Федерация; р.т.: +7(812)328–5185.

Поддержка исследований. Работа выполнена при частичной финансовой поддержке РФФИ (проект № 18-07-00932-а).

DOI 10.15622/sp.18.2.504-530

A.A. MOLDOVYAN, N.A. MOLDOVYAN

NEW FORMS OF DEFINING THE HIDDEN DISCRETE LOGARITHM PROBLEM

Moldovyan A.A., Moldovyan N.A. **New Forms of Defining the Hidden Discrete Logarithm Problem.**

Abstract. Novel variants of defining the discrete logarithm problem in a hidden group, which represents interest for constructing post-quantum cryptographic protocols and algorithms, are proposed. This problem is formulated over finite associative algebras with non-commutative multiplication operation. In the known variant this problem, called congruent logarithm, is formulated as superposition of exponentiation operation and automorphic mapping of the algebra that is a finite non-commutative ring. As it has been shown before, congruent logarithm problem defined in the finite quaternion algebra can be reduced to discrete logarithm in the finite field that is an extension of the field over which the quaternion algebra is defined. Therefore further reseaches of the congruent logarithm problem as primitive of the post-quantum cryptoschemes should be carried out in direction of finding new carriers. This paper presents novel associative algebras possessing significantly different properties than quaternion algebra, in particular they contain no global unit. This difference demanded a new definition of the discrete logarithm problem in a hidden group, which is different from the congruent logarithm. Several variants of such definition, in which the notion of the local unite is used, are proposed. Right, left, and bi-side local unites are considered. Two general methods for constructing the finite associative algebras with non-commutative multiplication operation are proposed. The first method relates to defining the algebras having dimension value equal to a natural number $m > 1$, and the second one relates to defining the algebras having arbitrary even dimensions. For the first time, the digital signature algorithms based on computational difficulty of the discrete logarithm problem in a hidden group have been proposed.

Keywords: Cryptography, Public-Key Ciphers, Post-Quantum Cryptoschemes, Discrete Logarithm Problem, Congruence Logarithm, Commutative Ciphers, Public Encryption, Digital Signature.

Moldovyan Alexandr Andreevich — Ph.D., Dr. Sci., Professor, Chief Researcher of Laboratory of Information Systems Security, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: computer security, cryptography, network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems; The number of publications — about 200. maa1305@yandex.ru, http://www.spiiras.nw.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328–5185.

Moldovyan Nikolay Andreevich — Ph.D., Professor, Chief Researcher of Laboratory of Information Systems Security, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: computer security, cryptography, symmetric and asymmetric cryptosystems, digital signature, authentication, block ciphers, pseudo-probabilistic ciphers. The number of publications — more 250. nmod@mail.ru, http://www.spiiras.nw.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328–5185.

Acknowledgements. This research is supported by the Russian Foundation for Basic Research (project No. 18-07-00932-a).

References

1. Sirwan A., Majeed N. New Algorithm for Wireless Network Communication Security. *International Journal on Cryptography and Information Security.* 2016. vol. 6. no. 3/4. pp. 1–8.
2. Feng Y., Yang G., Liu. J.K. A new public remote integrity checking scheme with user and data privacy. *International Journal of Applied Cryptography*. 2017. vol. 3. no 3. pp. 196–209.
3. Chiou S.Y. Novel Digital Signature Schemes based on Factoring and Discrete Logarithms. *International Journal of Security and Its Applications.* 2016. vol. 10. no. 3. pp. 295–310.
4. Poulakis D. A variant of Digital Signature Algorithm. *Designs, Codes and Cryptography*. 2009. vol. 51. no. 1. pp. 99–104.
5. Yan S.Y. Quantum Computational Number Theory. Springer. 2015. 252 p.
6. Yan S.Y. Quantum Attacks on Public-Key Cryptosystems. Springer. 2014. 207 p.
7. 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.
8. Smolin J.A., Smith G., Vargo A. Oversimplifying quantum factoring. *Nature*. 2013. vol. 499. no. 7457. pp. 163–165.
9. Hamdi S.M., Zuhori S.T., Ffiroz M., Biprodip P. A Compare between Shor's quantum factoring algorithm and General Number Field Sieve. 2014 International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT). 2014. pp. 1–6.
10. Federal Register. The Daily Journal of the United States Government. Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (accessed: 06.03.2018).
11. Verma G.K. A Proxy Blind Signature Scheme over Braid Groups. *International Journal of Network Security.* 2009. vol. 9. no 3. pp. 214–217.
12. Hiranvanichakorn P. Provably Authenticated Group Key Agreement based on Braid Groups − The Dynamic Case. *International Journal of Network Security*. 2017. vol. 19. no. 4. pp. 517−527.
13. Myasnikov A., Shpilrain V., Ushakov A. A Practical Attack on a Braid Group Based Cryptographic Protocol. Annual International Cryptology Conference. 2005. vol. 3621. pp. 86−96.
14. Chaturvedi A., Lal S. An Authenticated Key Agreement Protocol Using Conjugacy Problem in Braid Groups. *International Journal of Network Security*. 2008. vol. 6. no. 2. pp. 181–184.
15. Verma G.K. Probable Security Proof of a Blind Signature Scheme over Braid Groups. *International Journal of Network Security.* 2011. vol. 12. no. 2. pp. 118−120.
16. Kuzmin A.S. et al. Cryptographic Algorithms on Groups and Algebras. *Journal of Mathematical Sciences.* 2017. vol. 223. no. 5. pp. 629−641.
17. Moldovyan D.N., Moldovyan N.A., Shcherbacov V.A. Non-commutative finite associative algebras of 3-dimensional vectors. *Quasigroups and related systems.* 2018. vol. 26. no. 1. pp. 109−120.
18. Kuzmin A.S. et al. [Cryptographic Algorithms on Groups and Algebras]. *Fundamentalinaya i prikladnaya matematika – Fundumental and applied mathematics*. 2015. Issue 20. vol. 1. pp. 205−222. (In Russ.).
19. Glukhov M.M. [On analysis of some public key distribution systems based on non-abelian groups]. *Matematicheskie voprosy kriptografii – Mathematical Items of Cryptography.* 2010. Issue 1. vol. 4. pp. 5−22. (In Russ.).
20. Moldovyan D.N., Moldovyan N.A. Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms. *Quasigroups and Related Systems*. 2010. vol. 18. pp. 177−186.

21. Moldovyan D.N., Moldovyan N.A. A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols. International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. 2010. vol. 6258. pp. 183−194.
22. Moldovyan D.N. Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes. *Quasigroups and Related Systems.* 2010. vol. 18. pp. 165−176.
23. Moldovyan A.A., Moldovyan N.A., Shcherbacov. V.A. Non-commutative finite associative algebras of 2-dimension vectors. *Computer Science Journal of Moldova*. 2017. vol. 25. no. 3(75). pp. 344−356.
24. Camenisch J.L., Piveteau J.-M., Stadler M.A. Blind Signatures Based on the Discrete Logarithm Problem. Workshop on the Theory and Application of Cryptographic Techniques. 1994. pp. 428–432.
25. Pointcheval D., Stern J. Security Arguments for Digital Signatures and Blind Signatures. *Journal of Cryptology*. 2000. vol. 13. no. 3. pp. 361−396.