УДК 512.552.18+003.26 **DOI** 10.15622/ia.23.4.12

А.А. Молдовян, Д.Н. Молдовян, Н.А. Молдовян

ПОСТКВАНТОВЫЕ ДВУХКЛЮЧЕВЫЕ КРИПТОСХЕМЫ НА КОНЕЧНЫХ АЛГЕБРАХ

Молдовян А.А., Молдовян Д.Н., Молдовян Н.А. **Постквантовые двухключевые криптосхемы на конечных алгебрах.**

Аннотация. Одним из направлений разработки практичных постквантовых криптографических алгоритмов с открытым ключом является использование конечных алгебр в качестве их алгебраического носителя. Рассматриваются два подхода в этом направлении: 1) построение алгоритмов электронной цифровой подписи со скрытой группой на некоммутативных ассоциативных алгебр и 2) построение алгоритмов многомерной криптографии с использованием операции экспоненцирования в векторном конечном поле (коммутативной алгебре, являющейся конечным полем) для задания нелинейного отображения с секретной лазейкой. Первый подход включает разработку криптосхем двух типов: основанных на вычислительной трудности а) скрытой задачи дискретного логарифмирования и б) решения большой системы квадратных уравнений. Для второго подхода возникают проблемы обеспечения полной рандомизации цифровой подписи и задания некоммутативных ассоциативных алгебр большой размерности. Обсуждаются способы решения данных проблем. Показана важность исследования строения конечных некоммутативных алгебр с точки зрения декомпозиции на множество коммутативных подалгебр. Другое направление использования конечных алгебр для разработки криптографических алгоритмов с открытым ключом связано с существенным (в 10 и более раз) уменьшением размера открытого ключа в алгоритмах многомерной криптографии. В нем возникает проблема разработки формализованных параметризуемых унифицированных способов задания векторных конечных полей больших размерностей (от 5 до 130) с достаточно большим числом потенциально реализуемых типов и модификаций (до 2^{500} и более), задаваемых различными наборами структурных констант, с помощью которых определяется операция умножения векторов. Предложены варианты указанных способов и топологий нелинейных отображений на векторных конечных полях различных размерностей. Показано, что использование отображений, задающих операцию экспоненцирования в векторных конечных полях, потенциально обеспечивает устранение основного недостатка известных алгоритмов многомерной криптографии, связанного с большим размером открытого ключа.

Ключевые слова: постквантовая криптография, многомерная криптография, конечная алгебра, некоммутативная алгебра, векторное конечное поле, нелинейные отображения.

1. Введение. Криптографические алгоритмы электронной цифровой подписи (ЭЦП), открытого шифрования и открытого согласования секретного ключа, основанные на вычислительной сложности задачи факторизации (ЗФ) и задачи дискретного логарифмирования (ЗДЛ), имеют достаточно широкое применение в современных информационных системах. В России и других ведущих странах мира действуют стандарты на криптографические алгоритмы с открытым ключом, основанные на ЗДЛ на эллиптической

кривой. Однако, достигнутый в последние годы значительный прогресс в области создания вычислителей нового типа, основанных на принципах квантовой механики, и ожидаемая возможность практической реализации квантовых алгоритмов решения ЗФ и ЗДЛ [1, 2], имеющих полиномиальную по времени вычислительную сложность, обусловили высокую степень актуальности проблемы разработки постквантовых криптографических алгоритмов с открытым ключом [3, 4], стойких к атакам с использованием как обычного, так и квантового компьютера. Откликом на данную проблему является проводимый с 1997 года по настоящее время всемирный конкурс по разработке проектов постквантовых стандартов на криптографические алгоритмы с открытым ключом [5].

Разработка постквантовых криптосхем (алгоритмов и протоколов) связана с использованием вычислительно трудных задач, для которых предположительно не будет найдено полиномиальных алгоритмов решения на гипотетическом квантовом компьютере. Предложены и апробированы различные задачи (отличные от ЗФ и ЗДЛ) в качестве основы для построения постквантовых криптосхем с открытым ключом. В качестве носителей последних, например, используются группы [6, 7], коды, исправляющие ошибки [8, 9], алгебраические решетки [10, 11], трудно обратимые [12] и булевы функции [13].

Одним из наиболее изученных и апробированных направлений разработки постквантовых криптосхем открытым ключом является многомерная криптография, основанная на трудно обратимых нелинейные отображения с секретной лазейкой [14, 15]. Однако существенным ограничением для практического применения ее алгоритмов является чрезмерно большой размер открытого ключа (от десятков Кбайт при 80-битном уровне стойкости до нескольких Мбайт при 256-битной стойкости) [16, 17]. Исключение составляет алгоритм [18], стойкость которого на настоящий момент мало изучена.

Недавно предложенная парадигма [19, 20] построения нелинейных отображений как операций экспоненциирования в конечных векторных полях потенциально позволяет уменьшить размер открытого ключа алгоритмов многомерной криптографии на один – два десятичных порядка при заданном уровне стойкости. Описанные варианты реализации таких нелинейных отображений используют конкретные векторные конечные поля размерности $m = 5,6,7$, заданные эвристически над полями нечетной [19] и четной [20] характеристики. При этом предполагается, что эвристический способ также может быть применен и для случаев

$m = 11–97$. Однако, этот способ затрудняет оптимизацию топологий нелинейных отображений, требующую иметь возможность параметризуемого задания векторных конечных полей с большим числом потенциально реализуемых модификаций при фиксированном значении размерности m. Это обусловливает важность задачи разработки формализованных унифицированных способов задания векторных конечных полей, представляющих собой частный случай конечных коммутативных ассоциативных алгебр, для развития парадигмы [19, 21].

Сравнительно новым подходом является построение постквантовых алгоритмов электронной цифровой подписи (ЭЦП) со скрытой группой на конечных некоммутативных ассоциативных алгебрах (КНАА) с использованием вычислительной трудности решения больших систем квадратных уравнений [21]. В настоящей статье показывается, что в известных криптосхемах последнего типа имеется проблема ограниченной рандимизации подписи, требующая использования КНАА сравнительно больших размерностей, и рассматривается способ обеспечения полной рандомизации подписи.

2. Алгебры и векторные поля. Элементами конечного m-мерного векторного пространства, заданного над конечным полем $GF(p^s)$, где p – четное или нечетное простое число; s – натуральное число, являются векторы A, представляемые в виде упорядоченного набора элементов поля: $A = (a_0, a_1, \ldots, a_{m-1})$, где $a_i \in GF(p^s)$ – координаты вектора, или в виде суммы его компонент: $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, где $\mathbf{e}_i$ – базисные векторы. В векторном пространстве заданы две стандартные операции: сложение векторов и умножение вектора на скаляр (скалярное умножение). Если дополнительно к этим двум операциям определить операцию векторного умножения, операндами которой являются два произвольных вектора, которая обладает свойствами замкнутости и дистрибутивности слева и справа относительно операции сложения, то получаем конечную m-мерную алгебру.

Естественным является задание результата операции умножения векторов $\mathbf{A} = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$ и $\mathbf{B} = \sum_{j=0}^{m-1} b_j \mathbf{e}_j$ по правилу перемножения каждой компоненты первого вектора с каждой компонентой второго вектора по следующей формуле:

$$\mathbf{AB} = \sum_{i,j=0}^{m-1} a_i b_j \left(\mathbf{e}_i \mathbf{e}_j\right),$$

в которой предполагается, что каждое произведение вида $\mathbf{e}_i\mathbf{e}_j$ должно быть заменено на некоторый базисный вектор или однокомпонентный вектор $\lambda\mathbf{e}_k$, где $\lambda \in GF(p)$ называется структурной константой. Для осуществления такой замены задается так называемая таблица умножения базисных векторов (ТУБВ), в ячейках которой при $\lambda = 1$ указывается базисный вектор $\mathbf{e}_k$. Для определенности будем полагать, что левый множитель в произведении $\mathbf{e}_i\mathbf{e}_j$ задает строку, а правый – столбец, пересечение которых указывает ячейку, содержащую однокомпонентный вектор $\lambda\mathbf{e}_k$. В общем случае можно задать замену $\mathbf{e}_i\mathbf{e}_j$ на многокомпонентный вектор с сохранением требуемых свойств замкнутости и дистрибутивности, однако в последнем случае проблематично разработать ТУБВ реализующие свойство ассоциативности. В рассматриваемых в данной статье приложениях интерес представляют ассоциативные алгебры. Для задания ассоциативной операции векторного умножения и обеспечения возможности унифицированного параметризуемого задания ТУБВ используется замена произведения $\mathbf{e}_i\mathbf{e}_j$ на однокомпонентный вектор.

Если ассоциативная операция векторного умножения (или просто операция умножения) является коммутативной (некоммутативной), то имеем конечную коммутативную (некоммутативную) ассоциативную алгебру (КК(Н)АА). Типовой вид ТУБВ [23], по которым могут быть заданы ККАА с глобальной двухсторонней единицей для случая произвольных размерностей $m \geq 2$ представлен в таблице 1 (с нумерацией базисных векторов от 1 до m).

Таблица 1 [23]. Общий вид ТУБВ (где $\psi = \tau^{-1}\varepsilon\lambda$) для задания векторных конечных полей $GF((p^s)^m)$ в виде m-мерных конечных алгебр над полем $GF(p^s)$

×	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	…	$\mathbf{e}_{m-1}$	$\mathbf{e}_m$
$:\mathbf{e}_1$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\mathbf{e}_4$	$\tau\mathbf{e}_5$	$\tau\ldots$	$\tau\mathbf{e}_{m-1}$	$\tau\mathbf{e}_m$
$:\mathbf{e}_2$	$:\tau\mathbf{e}_2$	$\varepsilon\mathbf{e}_3$	$\varepsilon\mathbf{e}_4$	$\varepsilon\mathbf{e}_5$	$\varepsilon\ldots$	$\varepsilon\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_m$	$\psi\mathbf{e}_1$
$:\mathbf{e}_3$	$\tau\mathbf{e}_3$	$\varepsilon\mathbf{e}_4$	$\varepsilon\mathbf{e}_5$	$\varepsilon\ldots$	$\varepsilon\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_m$	$\psi\mathbf{e}_1$	$\lambda\mathbf{e}_2$
$:\mathbf{e}_4$	$:\tau\mathbf{e}_4$	$\varepsilon\mathbf{e}_5$	$\varepsilon\ldots$	$\varepsilon\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_m$	$\psi\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$
$:\mathbf{e}_5$	$\tau\mathbf{e}_5$	$\varepsilon\ldots$	$\varepsilon\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_m$	$\psi\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$:\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$
…	$:\tau\ldots$	$\varepsilon\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_m$	$\psi\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$:\lambda\mathbf{e}_3$	$:\lambda\mathbf{e}_4$	$\lambda\ldots$
$\mathbf{e}_{m-1}$	$\tau\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_{m-1}$	$\psi\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$:\lambda\mathbf{e}_4$	$\lambda\ldots$	$\lambda\mathbf{e}_{m-2}$
$\mathbf{e}_m$	$\tau\mathbf{e}_m$	$\psi\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$:\lambda\mathbf{e}_3$	$:\lambda\mathbf{e}_4$	…	$\lambda\mathbf{e}_{m-2}$	$\lambda\mathbf{e}_{m-1}$

В статье [23] показано, что алгебры с операцией умножения, заданной по ТУБВ данного вида, при выполнении условия делимости числа $p^s - 1$ на значение m при многих различных наборах значений независимых структурных констант τ, ε и λ являются конечными полями $GF((p^s)^m)$, которые будем называть векторными конечными полями. Распределение структурной константы τ по ячейкам ТУБВ имеет отличительную специфику, которая состоит в том, что она присутствует в ряде ячеек как скалярный множитель τ^{-1}. В качестве критерия формирования векторного конечного поля для заданного набора значений структурных констант в [23] использовано существование вектора, имеющего порядок $p^{sm} - 1$. Количество различных наборов значений структурных констант, при которых образуется алгебра, являющаяся полем, определяет количество различных модификаций векторного поля $GF((p^s)^m)$, определяемого заданным фиксированным распределением базисных векторов по ячейкам ТУБВ.

Для применения в рамках парадигмы [19] для разработки алгоритмов многомерной криптографии предполагается использование случайно заданной модификации векторного конечного поля, формируемого по ТУБВ с известными распределениями базисных векторов и структурных констант, в качестве элемента секретного ключа. Это определяет интерес к обеспечению возможности задания большого числа различных модификаций поля $GF((p^s)^m)$, а значит – к поиску ТУБВ с достаточно большим числом распределений различных независимых структурных констант. Число различных модификаций векторного поля $GF((p^s)^m)$ можно оценить как $O((p^s - 1)^k)$, где $O(\cdot)$ – обозначение порядка; k – число независимых структурных констант. Значение k учитывает как константы, влияющие на формирование векторного поля, так и константы, которые не влияют на формирование поля $GF((p^s)^m)$ в том смысле, что изменение их значений при фиксированных значениях остальных констант не может привести к формированию векторного поля (если исходный набор значений констант не задавал формирование поля). Примером такого случая является константа τ в таблице 1.

Если для заданного значения размерности m найдено распределение базисных векторов в ТУБВ, обеспечивающее коммутативность и ассоциативность операции умножения, то при малых значениях m можно эвристически-интуитивным путем найти распределения структурных констант, при которых сохраняются указанные свойства векторного умножения. Однако при больших значениях m эвристический способ становится неэффективным,

за исключением малого числа типовых случаев, иллюстрируемых, например, распределениями структурных констант ε, λ и τ в таблице 1. Далее будут предложены формализованные унифицированные методы построения ТУБВ с параметризуемым заданием распределений базисных векторов и структурных констант. При этом для фиксированного распределения базисных векторов задаются $2(m-1)$ различных распределений независимых структурных констант.

Коммутативность операции умножения, задаваемой некоторой ТУБВ со структурными константами, является необходимым, но не достаточным требованием обеспечения возможности формирования векторного конечного поля. Например, ТУБВ, представленная как таблица 2 (задает алгебру с единицей $(0,0,0,\tau^{-1})$, не позволяет найти наборы значений констант δ, λ, μ, и τ, при которых формируется поле $GF((p^s)^m)$, в том числе и при выполнении условия $m|p^s-1$.

Таблица 2. Задание коммутативной операции умножение без возможности формирования векторного конечного поля

×	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\delta\lambda\tau\mathbf{e}_3$	$\delta\mathbf{e}_2$	$\lambda\mathbf{e}_1$	$\tau^{-1}\mathbf{e}_0$
$\mathbf{e}_1$	$\delta\mathbf{e}_2$	$\delta\mu\tau\mathbf{e}_3$	$\mu\mathbf{e}_0$	$\tau^{-1}\mathbf{e}_1$
$\mathbf{e}_2$	$\lambda\mathbf{e}_1$	$\mu\mathbf{e}_0$	$\lambda\mu\tau\mathbf{e}_3$	$\tau^{-1}\mathbf{e}_2$
$\mathbf{e}_3$	$\tau^{-1}\mathbf{e}_0$	$\tau^{-1}\mathbf{e}_1$	$\tau^{-1}\mathbf{e}_2$	$\tau^{-1}\mathbf{e}_3$

На данный момент нет теоретического критерия, по которому можно было бы установить возможность формирования векторных полей по заданной размерности и заданным распределениям базисных векторов и структурных констант в ТУБВ, определяющей коммутативную операцию умножения. В дальнейшем предполагается использование вычислительных экспериментов для ответа на этот вопрос.

Последние выполняются по следующему алгоритму:

1. Задается случайный набор значений структурных констант.
2. Осуществляется проверка наличия вектора, имеющего порядок $p^{sm}-1$, т.е. наличия примитивного элемента поля. Если для k случайных векторов были получены значения порядка менее $p^{sm}-1$, то перейти к шагу 3, иначе СТОП и вывести сообщение: «При текущем наборе значений структурных констант алгебра является полем $GF((p^s)^m)$)».
3. Если $i<t$, то сгенерировать новый случайный набор значений структурных констант прирастить счетчик $i \leftarrow i+1$ и перейти к шагу 2. В противном случае СТОП и вывести сообщение:

«При данных значениях m, p и s и данных распределениях базисных векторов и структурных констант векторное конечное поле $GF((p^s)^m))$ с вероятностью, близкой к 100%, не может быть сформировано».

Выводимое сообщение на шаге 2 (3) имеет нулевую (ненулевую) вероятность ошибки. Достаточно низкую вероятность ошибки вывода на шаге 3 можно обеспечить устанавливая сравнительно большие значения k и t, например, $k = t = 100$.

3. Алгоритмы ЭЦП со скрытой группой. Алгебраическими носителями алгоритмов ЭЦП со скрытой группой являются КНАА. С целью повышения производительности процедур генерации и верификации цифровой подписи могут использоваться прореженные ТУБВ. Примером последних является таблица 3. Для данного применения КНАА важным является знание их строения с точки зрения декомпозиции на множество коммутативных подалгебр. Изучение строения позволяет установить типы содержащихся в КНАА коммутативных мультипликативных групп и значения их порядка, а также получить формулы, описывающие все элементы коммутативной подалгебры по координатам некоторого ее представителя.

Для ряда четырехмерных КНАА, в том числе и алгебры, заданной по таблице 3 [22], строение детально изучено и установлена однотипность их строения. Последнее характеризуется следующими общими моментами:

1. Четырехмерная КНАА разбивается на $p^2 + p + 1$ коммутативных подалгебр порядка p^2, относящихся к трем различным типам и попарно пересекающихся строго в множестве скалярных векторов.

2. Подалгебры первого типа являются полями, изоморфными полю $GF(p^2)$, и их мультипликативная группа Γ_1 имеет циклическое строение и порядок, равный $\Omega_1 = p^2 - 1$.

3. Подалгебры второго типа содержат мультипликативную группу Γ_2 порядка $\Omega_2 = (p - 1)^2$, которая имеет двухмерное циклическое строение (т. е. базис Γ_2 включает два вектора одного и того же порядка $p - 1$).

4. Подалгебры третьего типа содержат циклическую мультипликативную группу Γ_3 порядка $\Omega_3 = p(p - 1)$.

Для числа подалгебр первого η_1, второго η_2 и третьего η_3 типов получены следующие формулы [22]:

$$\eta_1 = p(p - 1)/2; \quad (1)$$

$$\eta_2 = p(p+1)/2; \tag{2}$$

$$\eta_3 = p + 1. \tag{3}$$

Из формул (1), (2) и (3) видно, что наибольший интерес для задания скрытой группы, являющейся элементом секретного ключа, представляют мультипликативные группы коммутативных подалгебр первого и второго типов, поскольку их число примерно в p раз больше числа подалгебр третьего типа. Можно предположить, что указанные моменты строения имеют место для всех четырехмерных КНАА, однако формальное доказательство этого факта не получено. Изучение строения КНАА с размерностями $m \geq 6$ на данный момент остается открытым вопросом, который имеет существенную значимость для разработки алгоритмов ЭЦП на их основе.

Таблица 3. Задание четырехмерной КНАА по прореженной ТУБВ

×	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mu\mathbf{e}_0$	0	0	$\mu\mathbf{e}_3$
$\mathbf{e}_1$	0	$\delta\mathbf{e}_1$	$\delta\mathbf{e}_2$	0
$\mathbf{e}_2$	$\mu\mathbf{e}_2$	0	0	$\lambda\mu\mathbf{e}_1$
$\mathbf{e}_3$	0	$\delta\mathbf{e}_3$	$\delta\lambda\mathbf{e}_0$	0

Для генерации КНАА произвольных четных размерностей может быть применен унифицированный способ задания соответствующих ТУБВ, который характеризуется следующими двумя математическими формулами, описывающими вектор на пересечении i-й строки и j-го столбца:

$$\mathbf{e}_i\mathbf{e}_j = \begin{cases} \mathbf{e}_{i+j+d \bmod m} & (i \bmod 2 = 0); \\ \mathbf{e}_{i-j-d \bmod m} & (i \bmod 2 = 1,\ j \bmod 2 = 0); \\ \lambda\mathbf{e}_{i-j-d \bmod m} & (i \bmod 2 = 1,\ j \bmod 2 = 1). \end{cases} \tag{4}$$

$$\mathbf{e}_i\mathbf{e}_j = \begin{cases} \mathbf{e}_{i-j-d \bmod m} & (i \bmod 2 = 0,\ j \bmod 2 = 1); \\ \lambda\mathbf{e}_{i-j-d \bmod m} & (i \bmod 2 = 0,\ j \bmod 2 = 0); \\ \mathbf{e}_{i+j+d \bmod m} & (i \bmod 2 = 1). \end{cases} \tag{5}$$

В данном способе распределение базисных векторов является параметризуемым, т.е. зависит от выбранного значения параметра d

($0 \le d \le m - 1$) и его четности (для четных d используется формула (4), для нечетных d – формула (5)). Параметризация распределения структурных констант не реализуется, однако это не имеет существенного значения для построения схем ЭЦП со скрытой группой. Существенными представляются возможность формализованного задания КНАА произвольных четных размерностей и знание их строения. Ввиду отсутствия на данный момент результатов изучения строения КНАА для случая $m \ge 6$ можно применить подход, связанный с экспериментальным определением возможных значений порядка векторов.

Рассмотрим построение алгоритма ЭЦП со скрытой группой, основанного на вычислительной трудности скрытой задачи дискретного логарифмирования (СЗДЛ) в четырехмерной КНАА, заданной по таблице 3 над полем $GF(p)$, где простое $p = 2q + 1$ при 256-битном простом q. Определим формирование открытого ключа по следующему алгоритму:

1. Сгенерировать случайный базис $\langle \mathbf{G}, \mathbf{Q} \rangle$ (где $\mathbf{G}$ и $\mathbf{Q}$ – векторы порядка q) скрытой коммутативной группы $\Gamma_{\langle \mathbf{G},\mathbf{Q} \rangle}$ с двухмерной цикличностью ($\Gamma_{\langle \mathbf{G},\mathbf{Q} \rangle}$ – подгруппа группы типа Γ_2).
2. Сгенерировать случайные обратимые векторы $\mathbf{A}$ и $\mathbf{B}$ порядка $p^2 - 1$, такие, что $\mathbf{AB} \ne \mathbf{BA}$, и случайное натуральное число $x < q$.
3. Вычислить открытый ключ (размером 96 байт) в виде тройки 32-байтовых векторов $\mathbf{U}$, $\mathbf{Y}$ и $\mathbf{Z}$ по секретным значениям $\mathbf{G}$, $\mathbf{Q}$, $\mathbf{A}$, $\mathbf{B}$ и x, составляющим 136-байтовый секретный ключ:

$$\mathbf{U} = \mathbf{AG}^x\mathbf{B}^{-1};\ \mathbf{Y} = \mathbf{BGB}^{-1} \text{ и } \mathbf{Z} = \mathbf{BQA}^{-1}.$$

Алгоритм генерации ЭЦП к документу M использует 256-битную хэш-функцию f_H и включает следующие шаги:

1. Выбрать два случайных натуральных числа $k < q$ и $t < q$ и вычислить вектор $\mathbf{V} = \mathbf{AG}^k\mathbf{Q}^t\mathbf{A}^{-1}$ и первый элемент подписи в виде числа $e = f_H(M, \mathbf{V})$.
2. Вычислить второй элемент s ЭЦП как решение квадратного уравнения $es^2 - s + xt + t = k \bmod q$ с неизвестным s. Если это уравнение не имеет решений, то перейти к шагу 1.
3. Вычислить третий элемент d ЭЦП: $d = (s^{-1}t - 1) \bmod q$.
4. Верификация ЭЦП осуществляется с использованием открытого ключа ($\mathbf{U}$, $\mathbf{Y}$, $\mathbf{Z}$) по алгоритму:
   1. Вычислить вектор $\mathbf{V}'$:

$$\mathbf{V}' = \left(\mathrm{U} \circ \mathrm{Y}^{es} \circ \mathrm{Z} \circ \left(\mathrm{U} \circ \mathrm{Y} \circ \mathrm{Z}\right)^{d}\right)^{s}.$$

2. Если $e' = f_H(M, \mathbf{V}') = e$, то ЭЦП верна, иначе подпись ложная.

4. Второй тип схем ЭЦП со скрытой группой. Представляет интерес парадигма построения алгоритмов ЭЦП, основанных на трудности решения больших систем степенных уравнений и использующих векторное проверочное уравнение с многократным вхождением подписи. В некоммутативных алгебрах решение уравнений с многократным вхождением неизвестной и со случайными параметрами является вычислительно трудной задачей. Для того, чтобы владелец открытого ключа мог вычислить значение подписи, требуется специальным способом сформировать открытый ключ и соответствующим способом задать механизм рандомизации подписи. Основные моменты реализации алгоритмов указанного типа иллюстрируются следующей схемой ЭЦП, в которой алгебраическим носителем служит четырехмерная КНАА, использованная в алгоритме из предыдущего раздела.

Личный секретный ключ генерируется владельцем открытого ключа в виде четырех случайных векторов **A**, **B**, **G**, **H** и натурального числа x $(1 < x < q)$, где векторы **G** и **H** порядка q составляют базис <**G**, **H**> скрытой группы; **A** и **B** – обратимые векторы порядка $p^2 - 1$ или $(p-1)^2$, удовлетворяющие условиям $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BG} \neq \mathbf{GB}$.

Открытый ключ вычисляется в виде набора векторов **Y**, **Z** и **U** по следующим формулам:

$$\mathbf{Y} = \mathbf{AGB}, \mathbf{Z} = \mathbf{AG}^{x}\mathbf{B} \text{ и } \mathbf{U} = \mathbf{AHB}. \quad (6)$$

Процедура генерации ЭЦП к электронному документу M включает следующие шаги:

1. Выбрать случайные натуральные числа k и t $(1 < k < q;$ $1 < t < q)$ и вычислить рандомизирующий вектор-фиксатор:

$$\mathbf{R} = \mathbf{B}^{-1}\mathbf{G}^{k}\mathbf{H}^{t}\mathbf{B}. \quad (7)$$

2. Используя 512-битную коллизионно стойкую хэш-функцию f_H, вычислить 512-битный рандомизирующий элемент подписи в виде хэш-значения $e = e_1 \| e_2 = f_H(M \| \mathbf{R})$, представленного как конкатенация двух 256-битных чисел e_1 и e_2.

3. Вычислить натуральные значения n и d:

$$n = \frac{k - e_1 - e_1^2 - xe_1}{e_1\left(e_1 + e_2 + 1\right)} \bmod q;$$

$$d = \frac{t - e_1 e_2}{e_1\left(e_1 + e_2 + 1\right)} \bmod q\,.$$

4. Подгоночный элемент подписи вычисляется в виде четырехмерного вектора **S** по формуле:

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{A}^{-1}. \tag{8}$$

Процедура верификации ЭЦП выполняется по следующему алгоритму:

1. Вычислить контрольный четырехмерный вектор $\mathbf{R}'$ по формуле:

$$\mathbf{R}' = \left(\left(\mathbf{SY}\right)^{e_1}\mathbf{S}\left(\mathbf{US}\right)^{e_2}\mathbf{ZSY}\right)^{e_1}. \tag{9}$$

2. Вычислить значение хэш-функции $e' = f_H(M||\mathbf{R}')$.

3. Если $e' = e$, то ЭЦП признается подлинной, в противном случае подпись отклоняется как ложная.

Постквантовая стойкость этого алгоритма ЭЦП обеспечивается тем, что вычисление секретного ключа по открытому ключу требует нахождения решения системы из следующих пяти квадратных векторных уравнений с неизвестными **A**, $\mathbf{B}^{-1}$, **G**, $\mathbf{G}_x$ ($\mathbf{G}_x = \mathbf{G}^x$) и **H**:

$$\mathbf{YB}^{-1} = \mathbf{AG},\ \mathbf{ZB}^{-1} = \mathbf{AG}_x,\ \mathbf{UB}^{-1} = \mathbf{AH},\ \mathbf{GG}_x = \mathbf{G}_x\mathbf{G},\ \mathbf{GH} = \mathbf{HG}. \tag{10}$$

Система уравнений (10) сводится к системе из 20 квадратных уравнений с 20 неизвестными в поле $GF(p)$, порядок которого равен 257-битному простому числу. Однако оценка стойкости как вычислительной трудности решения системы (1) является достаточно прямолинейной. При более внимательном рассмотрении описанного алгоритма можно заметить, что в нем используется несколько ограниченный механизм рандомизации подписи, реализуемый формулами (7) и (8). Ограниченность заключается в том, что при

заданном фиксированном секретном ключе векторы $\mathbf{R}$ и $\mathbf{S}$ могут принимать только $\approx p^2$ различных значений из $\approx p^4$ обратимых векторных значений в КНАА, использованной в качестве алгебраического носителя.

Нетрудно заметить, что при наличии многих различных подписанных документов имеется много различных векторов $\mathbf{S}_i$, ($i = 1, 2, 3\ldots$) а также можно вычислить для каждого значения $\mathbf{S}_i$ соответствующее ему значение $\mathbf{R}_i$. Это позволяет построить систему уравнений с существенно меньшим числом векторных уравнений (и неизвестных) по сравнению с системой (10).

Легко видеть, что имея k подлинных подписей к некоторым документам, из проверочного уравнения (9) можно вычислить k рандомизирующих векторов $\mathbf{R}_i$, каждый из которых по формуле (7) задает уравнение с неизвестным вектором $\mathbf{B}$ и неизвестным вектором $\mathbf{Q}_i = \mathbf{G}^{k_i}\mathbf{H}^{t_i}$, принадлежащим скрытой группе. Последнее означает, что выбирая $\mathbf{Q}_1$ как неизвестный вектор с четырьмя неизвестными координатами, неизвестные $\mathbf{Q}_1$, $\mathbf{Q}_2$, … , $\mathbf{Q}_i$ являются связанными с вектором $\mathbf{Q}_1$, а именно, они выбираются из коммутативной подалгебры, представителем которой является вектор $\mathbf{Q}_1$. В работе [22] приводится формула, описывающая через координаты вектор $\mathbf{Q}_1$ и две скалярные переменные все p^2 векторов, принадлежащие указанной подалгебре. Таким образом, уравнение $\mathbf{R}_1 = \mathbf{B}^{-1}\mathbf{G}^{k_1}\mathbf{H}^{t_1}\mathbf{B}$ задает 8 неизвестных скалярных значений, а каждое из остальных $k-1$ уравнений вида $\mathbf{R}_i = \mathbf{B}^{-1}\mathbf{G}^{k_i}\mathbf{H}^{t_i}\mathbf{B}$ добавляет только две независимые скалярные неизвестные. В случае $k = 3$ имеем систему из 3 векторных квадратных уравнений, сводимую к системе из 12 скалярных кубических уравнений с 12 скалярными неизвестными, из которой можно определить координаты неизвестного вектора $\mathbf{B}$ и координаты одного из векторов, задающих скрытую группу.

С учетом результатов исследования строения использованной в качестве алгебраического носителя четырехмерной КНАА, а именно возможности использования формулы с двумя скалярными переменными, которая описывает все элементы подалгебры, содержащей скрытую группу, в системе (10) последние два векторных уравнения могут быть устранены добавлением условия, что неизвестные $\mathbf{G}_x$ и $\mathbf{H}$ принадлежат подалгебре, которая содержит неизвестный вектор $\mathbf{G}$. При преобразовании системы векторных уравнений в систему скалярных уравнений указанное условие даст 12 скалярных уравнений с 16 неизвестными скалярными значениями.

Если координаты вектора **B** известны, то число скалярных неизвестных уменьшается до 12.

Таким образом, неполная рандомизация потенциально может быть использована для существенного снижения сложности алгоритма взлома описанной схемы ЭЦП и актуальным является нахождение механизмов обеспечения полной рандомизации подписи, которые дадут возможность векторам **S** и **R** принимать все (или почти все) возможные обратимые значения в используемой КНАА. При этом в рассмотрении механизма такого снижения стойкости существенно использовались результаты исследования строения использованной КНАА. Это показывает, что последние важны не только для разработки алгоритмов ЭЦП со скрытой группой, но и для оценки стойкости.

Для обеспечения полной рандомизации подписи можно задать вычисление подгоночного элемента подписи по формуле:

$$\mathbf{S} = \mathbf{D}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{V}, \tag{11}$$

где **V** – случайный обратимый вектор. Однако это приводит к проблемам с использованием проверочных уравнений с многократным вхождением подгоночного элемента подписи **S**, которое является важным моментом стойкости к атакам с использованием **S** как подгоночного параметра алгоритма подделки ЭЦП. При применении формулы (11) для вычисления элемента подписи **S** вместо многократного вхождения **S** в проверочное уравнение можно использовать два различных проверочных уравнения с однократным вхождением **S**, например, таких:

$$\begin{aligned} \mathbf{R}_1' &= \mathbf{Y}_1^{e'}\mathbf{T}_1\mathbf{Z}_1^{es}\mathbf{U}_1\mathbf{S}, \\ \mathbf{R}_2' &= \mathbf{Y}_2^{e}\mathbf{T}_2\mathbf{Z}_2^{es}\mathbf{U}_2\mathbf{S}, \end{aligned} \tag{12}$$

где e и e' – рандомизирующие элементы подписи; $\mathbf{Y}_1$, $\mathbf{T}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{T}_2$, и $\mathbf{Z}_2$ – элементы открытого ключа, зависящие от секретного ключа (в виде набора векторов **A**, **B**, **D**, **N**, **P**, **G**, **H** и числа x) и вычисляемые по формулам:

$$\begin{aligned} &\mathbf{Y}_1 = \mathbf{A}\mathbf{G}^{x}\mathbf{A}^{-1};\ \mathbf{T}_1 = \mathbf{A}\mathbf{G}\mathbf{B}^{-1};\ \mathbf{Z}_1 = \mathbf{B}\mathbf{H}\mathbf{B}^{-1};\ \mathbf{U}_1 = \mathbf{B}\mathbf{G}\mathbf{D}^{-1}; \\ &\mathbf{Y}_2 = \mathbf{N}\mathbf{H}^{x}\mathbf{N}^{-1};\ \mathbf{T}_2 = \mathbf{N}\mathbf{H}\mathbf{P}^{-1};\ \mathbf{Z}_2 = \mathbf{P}\mathbf{G}\mathbf{P}^{-1};\ \mathbf{U}_2 = \mathbf{P}\mathbf{H}\mathbf{D}^{-1}, \end{aligned} \tag{13}$$

где $\mathbf{G}$ и $\mathbf{H}$ – векторы, образующие базис скрытой группы. При удвоенном проверочном уравнении (12) процедура генерации подписи в виде четверки значений (e, e', s, $\mathbf{S}$) включает следующие шаги:

1. Сгенерировать случайные натуральные числа k_1, k_2, t_1 и вычислить число $t_2 = t_1 + k_1 - k_2 \bmod q$. Затем сгенерировать случайный обратимый вектор $\mathbf{V}$ и вычислить векторы-фиксаторы $\mathbf{R}_1 = \mathbf{A}\mathbf{G}^{k_1+2}\mathbf{H}^{t_1}\mathbf{V}$ и $\mathbf{R}_2 = \mathbf{N}\mathbf{G}^{k_2}\mathbf{H}^{t_2+2}\mathbf{V}$.

2. Используя 512-битную хэш-функцию f_H, вычислить 512-битный рандомизирующий элемент подписи в виде хэш-значения $e\|e' = f_H(M\|\mathbf{R}_1\|\mathbf{R}_2)$, представленного как конкатенация двух 256-битных чисел e и e'.

3. Вычислить числа $n = k_1 - e'x \bmod q$; $d = t_2 - e'x \bmod q$ $s = e^{-1}(t_1 - t_2 + e'x) \bmod q$ и вектор $\mathbf{S} = \mathbf{D}\mathbf{G}^n\mathbf{H}^d\mathbf{V}$.

Корректность данной схемы ЭЦП легко доказывается, подавая на вход алгоритма верификации значения подписи, сформированной в соответствии с процедурой генерации подписи.

Заметим, что подгоночный элемент подписи $\mathbf{S}$ и каждый из векторов-фиксаторов $\mathbf{R}_1$ и $\mathbf{R}_2$ может принимать любое обратимое значение из КНАА, используемой в качестве алгебраического носителя. Тем не менее, по формулам (11) и (12) и известным подлинным подписям можно составить систему уравнений, по которой можно будет вычислить элементы секретного ключа $\mathbf{D}$ и $\mathbf{N}$, однако это не приводит к снижению стойкости по отношению к атаке, реализующей решение системы квадратных уравнений, составленной из формул (13), связывающих элементы открытого ключа с элементами секретного ключа.

Последнее обусловлено тем, что система, составленная по формулам по формулам (11) и (12), включает значительно больше уравнений за счет того, что каждая тройка уравнений, связанная с одной подписью включает дополнительное векторное неизвестное – уникальное значение вектора $\mathbf{V}$. Для получения оценки числа подписей, которые необходимы для составления системы кубичных скалярных уравнений, в которой число уравнений равно числу скалярных неизвестных, следует учесть, что каждая подпись задает следующие три векторных уравнения $\mathbf{S} = \mathbf{D}\mathbf{G}^n\mathbf{H}^d\mathbf{V}$, $\mathbf{R}_1' = \mathbf{A}\mathbf{G}^{k_1+2}\mathbf{H}^{t_1}\mathbf{V}$ и $\mathbf{R}_2' = \mathbf{N}\mathbf{G}^{k_2}\mathbf{H}^{t_2+2}\mathbf{V}$, где векторы $\mathbf{R}_1'$ и $\mathbf{R}_2'$ вычисляются по проверочным уравнениям (12).

Последние три уравнения представим в виде $\mathbf{S} = \mathbf{D}\mathbf{G}_1\mathbf{V}$, $\mathbf{R}_1' = \mathbf{A}\mathbf{G}_2\mathbf{V}$ и $\mathbf{R}_2' = \mathbf{N}\mathbf{G}_3\mathbf{V}$, где неизвестные векторы $\mathbf{G}_1 = \mathbf{G}^n\mathbf{H}^d$, $\mathbf{G}_2 = \mathbf{G}^{k_1+2}\mathbf{H}^{t_1}$ и $\mathbf{G}_3 = \mathbf{G}^{k_2}\mathbf{H}^{t_2+2}$ принадлежат скрытой группе и являются

уникальными неизвестными для каждой подписи, также как и векторная неизвестная $\mathbf{V} = (v_0, v_1, v_2, v_3)$. Принадлежность скрытой группе позволяет записать координаты каждого из векторов $\mathbf{G}_1$, $\mathbf{G}_2$ и $\mathbf{G}_3$ через координаты фиксированного вектора $\mathbf{G}_0$, принадлежащего скрытой группе, и пару скалярных неизвестных (формула (8) в [22]). Последнее определяет 6 уникальных скалярных неизвестных. С учетом уникальных скалярных неизвестных v_0, v_1, v_2 и v_3 устанавливаем, что каждая известная подпись задает 12 скалярных уравнений, 10 уникальных скалярных неизвестных. При этом 16 фиксированных неизвестных (координаты векторных неизвестных **A**, **D** и **N**) присутствуют в уравнениях, задаваемых каждой подписью. Для k известных подлинных подписей имеем систему из $12k$ скалярных уравнений, включающую $10k + 12$ скалярных неизвестных.

Решение уравнения $12k = 10k + 12$ дает значение $k = 6$ при котором число уравнений и число неизвестных равно 72, тогда как система скалярных кубических уравнений, составленная по формулам (13) включает всего 32 уравнения с 38 скалярными неизвестными (недоопределенность данной системы показывает, что имеются много различных решений, задающих класс эквивалентных секретных ключей).

5. Трудно обратимые отображения в векторных конечных полях. В алгоритмах многомерной криптографии открытый ключ P представляет собой трудно обратимое отображение (n-мерных векторов в u-мерное векторное пространство) с секретной лазейкой, заданное в виде набора из u многочленов второй или более высокой степени с коэффициентами и n переменными (координатами вектора-прообраза), принимающими значения в поле $GF(p^s)$. Значения многочленов задают координаты u-мерного вектора-образа. Шифрование по ключу P выполняется путем представления сообщения в виде n-мерного вектора **M** и вычисления u-мерного вектора-образа $\mathbf{C} = \mathrm{P}(\mathbf{M})$. Однозначность расшифровывания шифртекста **C** обеспечивается неравенством $u \geq n$.

Прямой атакой на алгоритмы такого типа является решение системы уравнений, задаваемой шифртекстом **C** и набором многочленов P. В настоящее время разработаны достаточно эффективные способы решения этой задачи [24]. В зависимости от требуемого уровня стойкости выбираются значения u, n и p^s. При этом вычислительная сложность прямой атаки W на основе лучших известных способов решения больших систем степенных уравнений экспоненциально зависит от числа уравнений и относительно слабо зависит от порядка поля $GF(p^s)$ в котором задана система. Таблица 4,

отражающая обобщающие результаты статьи [25], иллюстрирует этот факт для случая $u = n$.

Таблица 4. Минимальное число уравнений, обеспечивающее заданный уровень стойкости W к прямой атаке [25]

Порядок поля $GF(p^s)$	$W = 2^{80}$	$W = 2^{100}$	$W = 2^{128}$	$W = 2^{192}$	$W = 2^{256}$
$p^s = 16$	30	39	51	80	110
$p^s = 31$	28	36	48	75	103
$p^s = 256$	26	33	43	68	93

Для формирования открытого ключа P обычно составляется некоторый набор многочленов над полем $GF(p^s)$ малого порядка, задающий нелинейное отображение N, для которого легко задать процедуру, выполняющую обратное отображение N^{-1}. Последнее не может служить потайной лазейкой, поэтому для получения отображение, пригодного для использования в качестве P, выполняется маскирование N путем преобразования набора многочленов N в другой набор многочленов, описывающих суперпозицию N с одним или двумя линейными отображениями. Последние легко представимы в виде набора многочленов первой степени, поэтому результирующий набор многочленов P легко вычисляется и имеет ту же степень, что и многочлен N. При этом отображение P является трудно обратимым, если не знать строение P как суперпозиции, например, $\mathrm{P}(\mathbf{M}) = \mathrm{L}_2(\mathrm{N}(\mathrm{L}_1(\mathbf{M})))$ для случая двух маскирующих линейных отображений L_1 и L_2. Для последних легко вычисляются соответствующие обратные отображения L_1^{-1} и L_2^{-1}, а секретной лазейкой служит суперпозиция отображений $\mathrm{P}^{-1}(\mathbf{C}) = \mathrm{L}_1^{-1}(\mathrm{N}^{-1}(\mathrm{L}_2^{-1}(\mathbf{C}))) = \mathbf{M}$.

Атаки, связанные с использованием особенностей формирования открытого ключа P, например, с поиском эквивалентных представлений P в виде суперпозиции линейных отображений L_1' и L_2' и сравнительно легко обратимого отображения N′ называются структурными атаками. Различные варианты структурных атак на алгоритмы многомерной криптографии представлены в работах [25, 26]. Для обеспечения стойкости к структурным атакам маскирующие отображения L_1 и L_2 задаются наборами многочленов с достаточно большим числом слагаемых, что приводит к большим размерам открытого ключа.

Устранение этого недостатка в рамках парадигмы [19] обеспечивается тем, что нелинейное отображение задается

с использованием операций экспоненцирования в m-мерных векторных конечных полях $GF((p^s)^m)$. Последние являются конечными алгебрами, в которых указанные операции легко задаются наборами многочленов над полем $GF(p^s)$, над которым заданы сами алгебры. Обратной по отношению к операции экспоненцирования в поле $GF((p^s)^m)$ является операция извлечения корня соответствующей степени z и для многих случаев (которые легко могут быть заданы) выполняется как операция возведения в степень $Z = z^{-1} \bmod \Omega$, где $\Omega = p^{sm} - 1$ – порядок мультипликативной группы поля. Выполнение операции извлечения корня даже в случае малых степеней z вычислительно непредставима в виде набора многочленов, но может быть легко выполнена при знании всех параметров задания конкретной модификации векторного поля, в котором выполнялась соответствующая операция экспоненцирования.

В парадигме [19] предполагается такое задание набора многочленов открытого ключа P, из которого вычислительно трудно установит параметры задания (одного или многих) модификаций векторных конечных полей, использованных владельцем открытого ключа для задания нелинейного трудно обратимого отображения N. При этом обратное отображение N^{-1} легко реализуется посредством выполнения одного или многих операций извлечения корня в известных модификациях векторных конечных полей, а секретной лазейкой является знание указанных модификаций. В данном подходе структурные атаки связаны с вычислением параметров задания модификаций векторных конечных полей по многочленам открытого ключа. Структурные атаки данного типа оказываются связанными с решением больших систем степенных уравнений. В отличие от систем уравнений, решаемых в случае прямых атака, в случае указанных структурных атак уравнения содержат сравнительно мало слагаемых, однако число неизвестных и значения степеней значительно больше.

Для маскирования параметров задания векторных конечных полей достаточно использование линейных отображений, не приводящих к увеличению размера открытого ключа (например, перестановки координат преобразуемых векторов). При построении нелинейного отображения N при использовании нескольких операций экспоненцирования возможны различные структуры (топологии) отображения N, выбираемые в зависимости от параметров разрабатываемого криптографического алгоритма и параметров используемых векторных полей. Частные варианты топологий представлены в статьях [19, 20].

6. Формализованный способ задания векторных конечных полей с большим числом реализуемых модификаций. Рассмотрим унифицированный способ генерации ТУБВ, определяющих коммутативную ассоциативную операцию умножения m-мерных векторов для размерностей $m = 2^k - 1$, где k – натуральное число. В данном способе предполагается, что ТУБВ генерируется по следующей формуле, в которой индексы i и j трактуются как двоичные многочлены, представленные битовыми строками, двоичные значения которых равны числам i и j (номерам базисных векторов $1 \le i, j \le m$):

$$\mathbf{e}_i \mathbf{e}_j = \mathbf{e}_{ijd \bmod f(x)}, \tag{14}$$

где d – ненулевой двоичный многочлен не выше степени $k-1$; операция умножения двоичных многочленов i, j и d выполняется по модулю неприводимого двоичного многочлена $f(x)$ степени k, например, $f(x) = x^3 + x^2 + 1$ при $k = 3$. Параметр d задает вид распределения базисных векторов. Число различных значений d равно порядку мультипликативной группы поля $GF(2^k)$, а именно, значению $\Omega = 2^k - 1$, и формула (14) задает Ω различных распределений базисных векторов для фиксированного значения m.

Параметризация распределений структурных констант в ТУБВ, задаваемых формулой (14), может быть обеспечена внесением условий установки констант, приводящих к следующей унифицированной формуле с трехфакторной параметризацией (параметризации по значениям: размерности m, параметра d и параметра t):

$$\mathbf{e}_i \mathbf{e}_j = \begin{cases} \delta \mathbf{e}_{ijd \bmod f(x)}, & \text{если } \left(t\left(\widetilde{i} + \widetilde{d}\right) \bmod \Omega\right) + \left(t\left(\widetilde{j} + \widetilde{d}\right) \bmod \Omega\right) < \Omega \\ \lambda \mathbf{e}_{ijd \bmod f(x)}, & \text{если } \left(t\left(\widetilde{i} + \widetilde{d}\right) \bmod \Omega\right) + \left(t\left(\widetilde{j} + \widetilde{d}\right) \bmod \Omega\right) \ge \Omega \end{cases}, \tag{15}$$

где t – натуральное число ($1 \le t < \Omega$) задающее распределение независимых структурных констант δ и λ; $\widetilde{i}, \widetilde{j}, \widetilde{d}$ – индексы (дискретные логарифмы) двоичных многочленов i, j, d по модулю $f(x)$ при основании, равном одному из примитивных элементов поля $GF(2^k)$ с умножением по модулю $f(x)$. (Заметим, что при $t = \Omega$ задается тривиальное распределение структурной константы δ, состоящее в ее наличии в каждой клетке ТУБВ.)

Утверждение 1. Формула (14) для произвольных значений из области определения параметров d и k генерирует ТУБВ с коммутативной и ассоциативной операцией векторного умножения.

Доказательство. Свойство коммутативности непосредственно следует из коммутативности операции умножения в поле двоичных многочленов $GF(2^k)$. Докажем, что свойство ассоциативности тоже имеет место. Для произвольных трех векторов **A**, **B** и **C** в соответствии с определением операции векторного умножения имеем:

$$(\mathrm{AB})\mathrm{C} = \sum_{i,j,h=1}^{m} a_i b_j c_h \left(\mathrm{e}_i \mathrm{e}_j\right)\mathbf{e}_h; \quad \mathrm{A}(\mathrm{BC}) = \sum_{i,j,h=1}^{m} a_i b_j c_h \mathrm{e}_i \left(\mathrm{e}_j \mathrm{e}_h\right).$$

Следовательно, если для всевозможных троек базисных векторов $\mathbf{e}_i$, $\mathbf{e}_j$ и $\mathbf{e}_h$ выполняется равенство $(\mathbf{e}_i\mathbf{e}_j)\mathbf{e}_h = \mathbf{e}_i(\mathbf{e}_j\mathbf{e}_h)$, то векторное умножение ассоциативно, поскольку в этом случае имеем (**AB**)**C** = **A**(**BC**). В соответствии с формулой (14) получаем:

$$\begin{aligned}
&\left(\mathbf{e}_i \mathbf{e}_j\right)\mathbf{e}_h = \mathbf{e}_{ijd \bmod f(x)}\mathbf{e}_h = \mathbf{e}_{ijhd^2 \bmod f(x)};\\
&\mathbf{e}_i\left(\mathbf{e}_j \mathbf{e}_h\right) = \mathbf{e}_i \mathbf{e}_{jhd \bmod f(x)} = \mathbf{e}_{ijhd^2 \bmod f(x)} = \left(\mathbf{e}_i \mathbf{e}_j\right)\mathbf{e}_h.
\end{aligned}$$

Утверждение 2. Формула (15) для произвольных значений из области определения параметров d и k генерирует ТУБВ, задающую конечную алгебру с глобальной двухсторонней единицей $\mathbf{U} = (u_1, u_2, \ldots, u_\Omega)$, где все координаты равны нулю, кроме координаты $u_{d^{-1} \bmod f(x)} = \delta^{-1}$.

Доказательство. Умножая произвольный вектор **A** на **U**, легко показывается выполнимость равенств **AU** = **A** и **UA** = **A**.

Теорема. Формула (15) для произвольных значений из области определения параметров d, k и t генерирует ТУБВ, задающую коммутативную и ассоциативную операцию векторного умножения.

Доказательство. Свойство коммутативности дано в предыдущем доказательстве. С учетом доказанного утверждения 1 и формулы (15) имеем $(\mathbf{e}_i\mathbf{e}_j)\mathbf{e}_h = \psi_1\mathbf{e}_u$ и $\mathbf{e}_i(\mathbf{e}_j\mathbf{e}_h) = \psi_2\mathbf{e}_u$ при некотором двоичном многочлене u. Докажем, что во всех случаях имеем $\psi_1 = \psi_2$, т.е. свойство ассоциативности векторного умножения имеет место.

Определим переменные i', j' и h' следующим образом:

$$i' = t\left(\tilde{i} + \tilde{d}\right) \bmod \Omega; \quad j' = t\left(\tilde{j} + \tilde{d}\right) \bmod \Omega; \quad h' = t\left(\tilde{h} + \tilde{d}\right) \bmod \Omega.$$

Представим формулу (15) в следующем виде:

$$\mathbf{e}_i\mathbf{e}_j = \begin{cases} \delta\mathbf{e}_{ijd \bmod f(x)}, & \text{если } i'+j' < \Omega \\ \lambda\mathbf{e}_{ijd \bmod f(x)}, & \text{если } i'+j' \geq \Omega \end{cases}, \quad (16)$$

Можно легко показать, что умножение вектора $(\mathbf{e}_i\mathbf{e}_j)$ на базисный вектор $\mathbf{e}_h$ вносит структурную константу λ, если $(i'+j') \bmod \Omega + h' \geq \Omega$, или структурную константу δ, если $(i'+j') \bmod \Omega + h' < \Omega$. Умножение базисного вектора $\mathbf{e}_i$ на вектор $(\mathbf{e}_j\mathbf{e}_h)$ вносит структурную константу λ, если $i'+(j'+h') \bmod \Omega \geq \Omega$, или структурную константу δ, если $i'+(j'+h') \bmod \Omega < \Omega$.

Имеем следующие четыре случая.

Случай 1. Значения i', j' и h' удовлетворяют условию $i'+j'+h' < \Omega$. Тогда $i'+j' < \Omega$ и $j'+h' < \Omega$ и из (16) следует $\psi_1 = \delta^2$ и $\psi_2 = \delta^2 = \psi_1$.

Случай 2. Значения i', j' и h' удовлетворяют условиям $i'+j' < \Omega$ и $(i'+j') \bmod \Omega + h' \geq \Omega$. Тогда из (16) следует $\psi_1 = \delta\lambda$. Для вычисления ψ_2 рассмотрим подслучаи 2.1 и 2.2:

Подслучай 2.1. Имеет место неравенство $j'+h' < \Omega$ (произведение $\mathbf{e}_j\mathbf{e}_h$ дает множитель δ). Тогда имеем $i'+(j'+h') \bmod \Omega \geq \Omega$ (умножение $\mathbf{e}_i$ на $(\mathbf{e}_j\mathbf{e}_h)$ дает множитель λ) и $\psi_2 = \delta\lambda = \psi_1$.

Подслучай 2.2. Имеет место неравенство $j'+h' \geq \Omega$ (произведение $\mathbf{e}_j\mathbf{e}_h$ дает множитель λ). Тогда имеем $(j'+h') \bmod \Omega = j'+h'-\Omega$ и из условия $i'+j' < \Omega$ следует $i'+(j'+h') \bmod \Omega < \Omega$ (умножение $\mathbf{e}_i$ на $(\mathbf{e}_j\mathbf{e}_h)$ дает множитель δ) и $\psi_2 = \lambda\delta = \psi_1$.

Случай 3. Значения i', j' и h' удовлетворяют условиям $i'+j' \geq \Omega$ (произведение $\mathbf{e}_i\mathbf{e}_j$ вносит множитель λ) и $(i'+j') \bmod \Omega + h' < \Omega$ (умножение $\mathbf{e}_i\mathbf{e}_j$ на $\mathbf{e}_h$ дает множитель δ). Тогда $\psi_1 = \lambda\delta$. Для вычисления ψ_2 рассмотрим подслучаи 3.1 и 3.2:

Подслучай 3.1. Имеет место неравенство $j'+h' \geq \Omega$ (произведение $\mathbf{e}_j\mathbf{e}_h$ дает множитель λ). Тогда $i'+(j'+h') \bmod \Omega = i'+j'+h' \geq i'+j' \geq \Omega$ и умножение $\mathbf{e}_i$ на $(\mathbf{e}_j\mathbf{e}_h)$ дает множитель λ, т. е. $\psi_2 = \lambda\delta = \psi_1$.

Подслучай 3.2. Имеет место неравенство $j'+h' < \Omega$ (произведение $\mathbf{e}_j\mathbf{e}_h$ дает множитель δ). Тогда $i'+(j'+h') \bmod \Omega < \Omega$ (поскольку $i'+(j'+h') \bmod \Omega = i'+j'+h'-\Omega < j'+h' < \Omega$) и умножение $\mathbf{e}_i$ на $(\mathbf{e}_j\mathbf{e}_h)$ дает множитель δ, т. е. $\psi_2 = \lambda\delta = \psi_1$.

Случай 4. Значения i', j' и h' удовлетворяют условиям $i'+j' \geq \Omega$ и $(i'+j') \bmod \Omega + h' \geq \Omega$. Из этих двух условий следует $j'+h' \geq \Omega$, а с учетом (16) имеем $\psi_1 = \lambda^2$. С учетом неравенства $j'+h' \geq \Omega$ (умножение $\mathbf{e}_j$ на $\mathbf{e}_h$ дает множитель λ) легко показать $i'+(j'+h') \bmod \Omega = (i'+j') \bmod \Omega + h' \geq \Omega$, т. е. умножение $\mathbf{e}_i$ на $(\mathbf{e}_j\mathbf{e}_h)$ дает множитель λ и получаем $\psi_2 = \lambda^2 = \psi_1$.

Таким образом, для всех случаев и подслучаев выполняется равенство $\psi_1 = \psi_2$, т. е. рассматриваемая операция векторного умножения является ассоциативной.

Для фиксированных значений параметров m и d доказанная теорема позволяет найти $\Omega = m - 1$ различных распределений структурной константы λ и столько же различных распределений структурной константы δ (с независимыми значениями), задаваемых различными значениями параметра t. Значения констант, относящихся к различным распределениям, являются независимыми. Легко показать, что любое сочетание этих независимых структурных констант в единой ТУБВ сохраняет свойства коммутативности и ассоциативности операции умножения. С точки зрения возможности задания векторного конечного поля эти две константы имеют различное значение. Если для некоторых двух значений λ и δ конечная алгебра не является полем, то путем модифицирования значения λ можно добиться формирования векторного конечного поля. Однако, путем модифицирования значения δ при фиксированном исходом значении λ этого добиться нельзя.

Таким образом, доказанная теорема обеспечивает формальное параметризуемое задание $2m - 2$ (без учета константы с тривиальным распределением для случая $t = \Omega$) независимых структурных констант для значений размерности, представленных в таблице 5.

Таблица 5. Значения размерности, охватываемые предложенным способом параметрического задания распределений структурных констант

Размерность	7	15	31	63	127	255	511
Число констант	12	28	60	124	252	508	1020

7. Примеры построения ТУБВ. Рассмотрим варианты практического использования предложенного метода для случая размерности $m = 7$. Таблица 6 иллюстрирует случай задания полей $GF(p^7)$ в виде семимерных конечных алгебр при использовании ненулевых структурных констант η ($t = 1$), γ ($t = 2$), ρ($t = 3$), λ ($t = 4$), ε($t = 5$), μ ($t = 6$) в унифицированной формуле (15) с умножением

двоичных многочленов i, j и d по модулю неприводимого двоичного многочлена $x^3 + x^2 + 1$ (1101 – в представлении в виде битовой строки) и вычислении индексов номеров-многочленов i, j и d при основании индексов, равном многочлену $x^2 + 1$ (101). Экспериментально подтверждается существование векторных полей $GF(p^7)$ с глобальной двухсторонней единицей U=(0,0,0,0,0,0,1), заданных по таблице 6 над полем $GF(p)$ для $p = 29$ и $p = 211$ и различных наборов значений структурных констант.

Таблица 6. Задание семимерных векторных конечных полей с помощью базовых констант η, γ, ρ, λ, ε, и μ (константа Ψ = ηγρλεμ)

×	$\mathbf{e}_1$	$:\mathbf{e}_2$	$:\mathbf{e}_3$	$:\mathbf{e}_4$	$\mathbf{e}_5$	$:\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_1$	$\varepsilon\lambda\mu\mathbf{e}_5$	$\Psi\mathbf{e}_7$	$:\varepsilon\lambda\mu\mathbf{e}_2$	$\varepsilon\mu\rho\mathbf{e}_3$	$\varepsilon\mu\rho\mathbf{e}_6$	$\delta\lambda\mu\mathbf{e}_4$	$\mathbf{e}_1$
$:\mathbf{e}_2$	$\Psi\mathbf{e}_7$	$\delta\eta\rho\mathbf{e}_3$	$:\delta\lambda\eta\mathbf{e}_4$	$\varepsilon\eta\rho\mathbf{e}_6$	$\delta\eta\rho\mathbf{e}_1$	$\delta\lambda\eta\mathbf{e}_5$	$\mathbf{e}_2$
$:\mathbf{e}_3$	$:\varepsilon\lambda\mu\mathbf{e}_2$	$\delta\lambda\eta\mathbf{e}_4$	$\varepsilon\lambda\eta\mathbf{e}_6$	$\varepsilon\lambda\eta\mathbf{e}_5$	$\Psi\mathbf{e}_7$	$\delta\lambda\eta\mathbf{e}_1$	$\mathbf{e}_3$
$:\mathbf{e}_4$	$:\varepsilon\mu\rho\mathbf{e}_3$	$\varepsilon\eta\rho\mathbf{e}_6$	$\varepsilon\lambda\eta\mathbf{e}_5$	$\varepsilon\eta\rho\mathbf{e}_1$	$\varepsilon\mu\rho\mathbf{e}_2$	$\Psi\mathbf{e}_7$	$\mathbf{e}_4$
$\mathbf{e}_5$	$\varepsilon\mu\rho\mathbf{e}_6$	$\delta\eta\rho\mathbf{e}_1$	$\Psi\mathbf{e}_7$	$\varepsilon\mu\rho\mathbf{e}_2$	$\delta\mu\rho\mathbf{e}_4$	$\delta\mu\rho\mathbf{e}_3$	$\mathbf{e}_5$
$:\mathbf{e}_6$	$:\delta\lambda\mu\mathbf{e}_4$	$\delta\lambda\eta\mathbf{e}_5$	$\delta\lambda\eta\mathbf{e}_1$	$\Psi\mathbf{e}_7$	$:\delta\mu\rho\mathbf{e}_3$	$\delta\lambda\mu\mathbf{e}_2$	$\mathbf{e}_6$
$\mathbf{e}_7$	$\mathbf{e}_1$	$:\mathbf{e}_2$	$:\mathbf{e}_3$	$:\mathbf{e}_4$	$\mathbf{e}_5$	$:\mathbf{e}_6$	$\mathbf{e}_7$

Константы δ и λ, присутствующие в формуле (15) при фиксированном значении параметра t заполняют все ячейки ТУБВ, в каждой из которых присутствует либо δ, либо λ. При этом значение δ влияет на ненулевую координату глобальной двухсторонней единицы, но не влияет на формирование векторного поля (в том смысле, что, если для текущей пары значений δ и λ не сформировалось векторное конечное поле, то подбором значений δ этого добиться нельзя). Будем называть константу λ базовой, а δ – сопряженной к ней. В следующем примере константы, сопряженные с соответствующими базовыми константами, обозначены добавлением штриха.

Распределения сопряженных (по отношению к соответствующим константам из таблице 6) независимых структурных констант η' ($t = 1$), $\gamma'(t = 2)$, $\rho'(t = 3)$, $\lambda'(t = 4)$, $\varepsilon'(t = 5)$, $\mu'(t = 6)$ и эвристической константы τ представлены в таблице 7. Константа τ также не влияет на формирование векторного поля, но влияет на значение ненулевой координаты единичного вектора **U**:

$$u_{d^{-1} \bmod f(x)} = \Psi'^{-1}\tau^{-1}.$$

Найденное эвристическим путем распределение константы τ показывает, что формально задаваемое формулой (15) множество структурных констант может быть дополнено, расширяя множество потенциально реализуемых модификаций векторного конечного поля для фиксированного распределения базисных векторов. Для многих других значений размерности m и параметра d были найдены аналогичные распределения эвристических констант. С точки зрения увеличения числа различных модификаций векторного конечного поля, задаваемого по ТУБВ с фиксированным распределением базисных векторов представляет прикладной интерес эвристический поиск и других распределений дополнительных структурных констант. Однако он может служить только дополнением к разработанному формализованному методу параметризуемого задания различных распределений структурных констант.

Таблица 7. Распределения сопряженных структурных констант γ′, ε′, λ′, μ′, η′ и ρ′ (константа $\Psi' = \gamma'\varepsilon'\lambda'\mu'\eta'\rho'$)

×	$\mathbf{e}_1$	$:\mathbf{e}_2$	$:\mathbf{e}_3$	$:\mathbf{e}_4$	$\mathbf{e}_5$	$:\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_1$	$\delta'\eta'\rho'\mathbf{e}_5$	$\tau^{-1}\mathbf{e}_7$	$\delta'\eta'\rho'\mathbf{e}_2$	$\delta'\lambda'\eta'\mathbf{e}_3$	$\delta'\lambda'\eta'\mathbf{e}_6$	$\varepsilon'\eta'\rho'\mathbf{e}_4$	$\Psi'\tau\mathbf{e}_1$
$:\mathbf{e}_2$	$\tau^{-1}\mathbf{e}_7$	$\varepsilon'\lambda'\mu'\mathbf{e}_3$	$\varepsilon'\mu'\rho'\mathbf{e}_4$	$\delta'\lambda'\mu'\mathbf{e}_6$	$\varepsilon'\lambda'\mu'\mathbf{e}_1$	$\varepsilon'\mu'\rho'\mathbf{e}_5$	$\Psi'\tau\mathbf{e}_2$
$:\mathbf{e}_3$	$\delta'\eta'\rho'\mathbf{e}_2$	$\varepsilon'\mu'\rho'\mathbf{e}_4$	$\delta'\mu'\rho'\mathbf{e}_6$	$\delta'\mu'\rho'\mathbf{e}_5$	$\tau^{-1}\mathbf{e}_7$	$\varepsilon'\mu'\rho'\mathbf{e}_1$	$\Psi'\tau\mathbf{e}_3$
$:\mathbf{e}_4$	$\delta'\lambda'\eta'\mathbf{e}_3$	$\delta'\lambda'\mu'\mathbf{e}_6$	$\delta'\mu'\rho'\mathbf{e}_5$	$\delta'\lambda'\mu'\mathbf{e}_1$	$\delta'\lambda'\eta'\mathbf{e}_2$	$\tau^{-1}\mathbf{e}_7$	$\Psi'\tau\mathbf{e}_4$
$\mathbf{e}_5$	$\delta'\lambda'\eta'\mathbf{e}_6$	$\varepsilon'\lambda'\mu'\mathbf{e}_1$	$\tau^{-1}\mathbf{e}_7$	$\delta'\lambda'\eta'\mathbf{e}_2$	$\varepsilon'\lambda'\eta'\mathbf{e}_4$	$\varepsilon'\lambda'\eta'\mathbf{e}_3$	$\Psi'\tau\mathbf{e}_5$
$:\mathbf{e}_6$	$\varepsilon'\eta'\rho'\mathbf{e}_4$	$\varepsilon'\mu'\rho'\mathbf{e}_5$	$\varepsilon'\mu'\rho'\mathbf{e}_1$	$\tau^{-1}\mathbf{e}_7$	$\varepsilon'\lambda'\eta'\mathbf{e}_3$	$\varepsilon'\eta'\rho'\mathbf{e}_2$	$\Psi'\tau\mathbf{e}_6$
$\mathbf{e}_7$	$\Psi'\tau\mathbf{e}_1$	$:\Psi'\tau\mathbf{e}_2$	$\Psi'\tau\mathbf{e}_3$	$\Psi'\tau\mathbf{e}_4$	$\Psi'\tau\mathbf{e}_5$	$\Psi'\tau\mathbf{e}_6$	$\Psi'\tau\mathbf{e}_7$

8. Топологии нелинейного отображения. Предложенный метод формального параметризуемого задания многих распределений структурных констант при заданном распределении базисных векторов дает достаточно широкие возможности реализации нелинейного отображения N с секретной лазейкой (раздел 5). Простейшее строение (топология) представляет собой реализацию N в виде одной операции экспоненцирования в векторном конечном поле $GF((p^s)^n)$, заданной над полем $GF(p^s)$ набором многочленов, который вычисляется по ТУБВ, использованной для задания поля $GF((p^s)^n)$.

Для реализации такой тривиальной топологии представляет интерес использование полей $GF(p^s)$ четной характеристики, т.е. полей $GF(2^s)$ при различных степенях s. Это связано с тем, что в полях такой характеристики операции $\mathrm{N}(\mathbf{X}) = \mathbf{X}^i$ для значений степени i, равных

степеням числа 2, записываются набором степенных многочленов, каждый из которых включает всего одно слагаемое, а отображения вида $\mathrm{N}(\mathbf{X}) = \mathbf{X}^i\mathbf{X}^j$, которые непосредственно могут быть использованы в качестве открытого ключа P, – набором из n многочленов, каждый из которых включает не более n слагаемых [20]. В последнем случае имеем возможность предложить алгоритм шифрования, алгоритм ЭЦП или протокол открытого согласования общего секретного ключа с открытым ключом размера $\approx sn^2$ бит.

Такая тривиальная топология отображения N, например, может быть реализована для случая $n = 31$ (таблица 5), $s = 15$ и $\mathrm{N}(\mathbf{X}) = \mathbf{X}^{17}$, в котором реализуются условия делимости числа $2^s - 1$ на 31 (обеспечивает возможность задания векторного конечного поля) и неделимости $2^s - 1$ на 17 (обеспечивает однозначность извлечения корня степени 17 в поле $GF((2^{15})^{31})$). В такой реализации обеспечивается 80-битный уровень стойкости (таблица 4) при размере открытого ключа, равном ≈2 Кбайт.

Аналогичная реализация для случая $n = 127$ (таблица 5), $s = 14$ и $\mathrm{N}(\mathbf{X}) = \mathbf{X}^{257}$ обеспечивается 256-битный уровень стойкости (таблица 4) при размере P, равном ≈32 Кбайт. По сравнению с известным алгоритмом Rainbow [27] для такого же уровня стойкости имеем примерно 40-кратное уменьшение размера открытого ключа.

В случае реализации тривиальной топологии с заданием векторных конечных полей над полями нечетной характеристики p отображение N может быть задано в виде $\mathrm{N}(\mathbf{X}) = \mathbf{X}^2$ и $\mathrm{N}(\mathbf{X}) = \mathbf{X}^3$. В первом случае процедура расшифровывания шифртекста является неоднозначной и требуется разработка специального алгоритма извлечения квадратных корней, однако обеспечивается существенно меньший размер открытого ключа. Во втором случае всегда можно выбрать значение p, при котором извлечение корня третьей степени дает однозначный результат. Для этого следует выбрать простое p, такое, что $p - 1$ делится на 31, а число $p^{31} - 1$ не делится на 3 (например, $p = 311$), определяя возможность задания векторного конечного поля $GF(p^{31})$, в котором вычисление корня третьей степени осуществляется путем выполнения одной операции возведения в степень $z = 3^{-1} \bmod (p^{31} - 1)$: $\mathbf{X}^{1/3} = \mathbf{X}^z$. Однако использование отображения $\mathrm{N}(\mathbf{X}) = \mathbf{X}^3$ приводит к тому, что размер открытого ключа становится сравнительно большим, например, ≈30 Кбайт (≈2 Мбайт) при уровне стойкости 2^{80} (2^{256}).

Существенное уменьшение размера открытого ключа может быть достигнуто применением каскадной топологии, в которой входной вектор $\mathbf{X}$ разбивается на несколько подвекторов размерности

m и над каждым из них выполняется операции возведения в куб, перестановка всех n координат всех подвекторов и умножение новых значений подвекторов на секретные векторы размерности m (задает маскирующее линейное преобразование). В такой каскадной топологии при значениях $m = 7$ и $n = 70$ используются семимерные векторные конечные поля (в общем случае десять различных полей), заданные, например, над $GF(239)$, и обеспечивается ожидаемый уровень 192-битной стойкости при размере открытого ключа, равном ≈24 Кбайт. По сравнению с Rainbow [27] для такого же уровня стойкости имеем примерно 36-кратное уменьшение размера открытого ключа.

При реализации аналогичной каскадной топологии при значениях $m = 7$ и $n = 77$ с использованием поля четной характеристики $GF(64)$ 192-битная стойкости обеспечивается при размере открытого ключа, равном ≈3,8 Кбайт (226-кратное уменьшение размера P относительно Rainbow [27]).

Другие типы каскадных топологий для задания нелинейного отображения с секретной лазейкой на основе операций экспоненцирования в векторных конечных полях представлены в работах [19, 20].

9. Заключение. Конечные некоммутативные и коммутативные алгебры с ассоциативной операцией умножения представляют значительный интерес для разработки на их основе постквантовых двухключевых криптоалгоритмов. Первые служат алгебраическим носителем алгоритмов ЭЦП со скрытой группой, относящихся к двум различным типам, использующим вычислительную трудность двух различных задач: 1) скрытой ЗДЛ и 2) решения большой системы степенных уравнений. В алгоритмах второго типа возникает проблема обеспечения полной рандомизации подписи, для решения которой предложен способ, основанный на использовании приема удвоения уравнения верификации ЭЦП.

Алгебры второго типа представляют существенный интерес для построения криптоалгоритмов с открытым ключом, основанных на трудно обратимых отображениях с потайной лазейкой, предоставляя потенциальную возможность решения проблемы чрезвычайно большого размера открытого ключа в известных алгоритмах данного типа. Предложенный способ параметризуемого унифицированного задания векторных конечных полей решает проблему задания большого числа модификаций таких полей и обеспечивает возможность использования конкретной модификации или конкретного набора модификаций векторного конечного поля

в качестве элемента секретного ключа. Разработанный способ может служить прототипом для разработки других унифицированных способов задания векторных конечных полей с параметризацией распределения структурных констант с целью расширения множества значений размерности, для которых может быть формализован поиск распределений многих структурных констант. Однако это представляет самостоятельную исследовательскую задачу.

Литература

1. Ekert A., Jozsa R. Quantum computation and Shor's factoring algorithm // Reviews of Modern Physics. 1996. vol. 68. no. 3. pp. 733–752.
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. Post-Quantum Cryptography. Proceedings of the 13th International Conference, PQCrypto 2022 // Lecture Notes in Computer Science. 2022. vol. 13512.
4. Johansson T., Smith-Tone D. Post-Quantum Cryptography. Proceedings of the 14th International Conference, PQCrypto 2023 // Lecture Notes in Computer Science. 2023. vol. 14154.
5. Alagic G, Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Liu Y., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D., Apon D. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process // NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology. 2022. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934458 (дата обращения: 25.02.2024).
6. Han J., Zhuang J. DLP in semigroups: algorithms and lower bounds // J. Math. Cryptol. 2022. vol. 16. no. 1. pp. 278–288.
7. Battarbee C., Kahrobaei D., Perret L., Shahandashti S.F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures // Post-Quantum Cryptography. PQCrypto 2023. Lecture Notes in Computer Science. 2023. vol. 14154. pp. 113–138. DOI: 10.1007/978-3-031-40003-2_5.
8. Vysotskaya V.V., Chizhov I.V. The security of the code-based signature scheme based on the Stern identification protocol // Applied Discrete Mathematics. 2022. № 57. С. 67−90. DOI: 10.17223/20710410/57/5.
9. Kosolapov Y.V., Turchenko O.Y. On the construction of a semantically secure modification of the McEliece cryptosystem // Applied Discrete Mathematics. 2019. № 45. С. 33−43. DOI: 10.17223/20710410/45/4.
10. Gartner J. NTWE: A Natural Combination of NTRU and LWE // Post-Quantum Cryptography. PQCrypto 2023. Lecture Notes in Computer Science, 2023. vol. 14154. pp. 321–353. DOI: 10.1007/978-3-031-40003-2_12.
11. Lysakov I.V.. Solving some cryptanalytic problems for lattice-based cryptosystems with quantum annealing method // Mathematical Aspects of Cryptography. 2023. vol. 14. no. 2. pp. 111–122. DOI: 10.4213/mvk441.
12. Hamlin B., Song F. Quantum Security of Hash Functions and Property-Preservation of Iterated Hashing // Post-Quantum Cryptography. PQCrypto 2019 / Lecture Notes in Computer Science. 2019. vol. 11505. pp. 329–349. DOI: 10.1007/978-3-030-25510-7_18.
13. Agibalov G.P. ElGamal cryptosystems on Boolean functions / Applied Discrete Mathematics. 2018. № 42. С. 57−65. DOI: 10.17223/20710410/42/4.

14. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. vol. 80. DOI: 10.1007/978-1-0716-0987-3_2.
15. Debnath S., Kundu N., Mishra D., Choudhury T. Post-quantum digital signature scheme based on multivariate cubic problem // Journal of Information Security and Applications. 2020. vol. 53. DOI: 10.1016/j.jisa.2020.102512.
16. Ding J., Petzoldt A., Schmidt D.S. Oil and Vinegar // Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. vol. 80. pp. 89–151. Springer, New York. DOI: 10.1007/978-1-0716-0987-3_5.
17. Cartor R., Cartor M., Lewis M., Smith-Tone D. IPRainbow // Post-Quantum Cryptography. PQCrypto 2022. Lecture Notes in Computer Science. 2022. vol. 13512. pp. 170–184. DOI: 10.1007/978-3-031-17234-2_9.
18. Beullens W. MAYO: practical post-quantum signatures from oil-and-vinegar maps // Proceedings of the International Conference on Selected Areas in Cryptography (SAC 2021). Lecture Notes in Computer Science. 2022. vol. 13203. pp. 355–376.
19. Молдовян А.А., Молдовян Д.Н., Молдовян Н.А. Новый подход к разработке алгоритмов многомерной криптографии // Вопросы кибербезопасности. 2023. № 2(54). С. 52–64. DOI: 10.21681/2311-3456-2023-2-52-6.
20. Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. no. 1(94). pp. 46–60. DOI: 10.56415/csjm.v32.04.
21. Duong M.T., Moldovyan D.N., Do B.V., Nguyen M.H. Post-quantum signature algorithms on non-commutative algebras, using difficulty of solving systems of quadratic equations // Computer Standards and Interfaces. 2023, vol. 86. no. 103740. DOI: 10.1016/j.csi.2023.103740.
22. Moldovyan D.N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. vol. 29, no. 2(86). pp. 206–226.
23. Moldovyan N.A., Moldovyanu P.A. Vector Form of the Finite Fields GF(pm) // Bulletin of Academy of Sciences of Moldova. Mathematics. 2009. no. 3(61). pp. 57–63.
24. Ding J., Petzoldt A., Schmidt D.S. Solving Polynomial Systems // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. New York. 2020. vol. 80. pp. 185–248. DOI: 10.1007/978-1-0716-0987-3_8.
25. Ding J., Petzoldt A. Current State of Multivariate Cryptography // IEEE Security and Privacy. 2017. vol. 15. no. 4. pp. 28–36.
26. Qiao S., Han W., Li Y., Jiao L. Construction of Extended Multivariate Public Key Cryptosystems // International Journal of Network Security. 2016. vol. 18. no. 1. pp. 60–67.
27. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [on line] 2021. URL: https://www.pqcrainbow.org/ (дата обращения: 25.02.2024).

Молдовян Александр Андреевич — д-р техн. наук, профессор, главный научный сотрудник, лаборатория проблем компьютерной безопасности, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН). Область научных интересов: криптография, постквантовые криптоалгоритмы с открытым ключом, электронная цифровая подпись, криптографические протоколы, компьютерная безопасность. Число научных публикаций — 200. maa1305@yandex.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)333-3411.

Молдовян Дмитрий Николаевич — канд. техн. наук, доцент кафедры, кафедра информационных систем, Санкт-Петербургский государственный электротехнический

университет «ЛЭТИ». Область научных интересов: криптография, постквантовые двухключевые криптоалгоритмы на алгебрах и нелинейных отображениях, цифровая подпись, информационная безопасность. Число научных публикаций — 100. mdn.spectr@mail.ru; улица профессора Попова, 5, 199178, Санкт-Петербург, Россия; р.т.: +7(812)234-2772.

Молдовян Николай Андреевич — д-р техн. наук, профессор, главный научный сотрудник, лаборатория проблем компьютерной безопасности, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН). Область научных интересов: криптография, постквантовые криптоалгоритмы с открытым ключом, электронная цифровая подпись, блочные шифры, компьютерная безопасность. Число научных публикаций — 230. nmold@mail.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)333-3411.

Поддержка исследований. Работа выполнена при финансовой поддержке РНФ: проекты № 24-21-00225 (разделы 2, 3 и 4) и № 24-41-04006 (разделы 5, 6, 7 и 8).

DOI 10.15622/ia.23.4.12

A. MOLDOVYAN, D. MOLDOVYAN, N. MOLDOVYAN

POST-QUANTUM PUBLIC-KEY CRYPTOSCHEMES ON FINITE ALGEBRAS

Moldovyan A., Moldovyan D., Moldovyan N. **Post-Quantum Public-Key Cryptoschemes on Finite Algebras.**

Abstract. One direction in the development of practical post-quantum public-key cryptographic algorithms is the use of finite algebras as their algebraic carrier. Two approaches in this direction are considered: 1) construction of electronic digital signature algorithms with a hidden group on non-commutative associative algebras and 2) construction of multidimensional cryptography algorithms using the exponential operation in a vector finite field (in a commutative algebra, which is a finite field) to specify a nonlinear mapping with a secret trapdoor. The first approach involves the development of two types of cryptoschemes: those based on the computational difficulty of a) the hidden discrete logarithm problem and b) solving a large system of quadratic equations. For the second type, problems arise in ensuring complete randomization of the digital signature and specifying non-commutative associative algebras of large dimension. Ways to solve these problems are discussed. The importance of studying the structure of finite non-commutative algebras from the point of view of decomposition into a set of commutative subalgebras is shown. Another direction is aimed at a significant (10 or more times) reduction in the size of the public key in multivariate-cryptography algorithms and is associated with the problem of developing formalized, parameterizable, unified methods for specifying vector finite fields of large dimensions (from 5 to 130) with a sufficiently large number of potentially implementable types and modifications each type (up to 2^{500} or more). Variants of such methods and topologies of nonlinear mappings on finite vector fields of various dimensions are proposed. It is shown that the use of mappings that specify the exponential operation in vector finite fields potentially eliminates the main drawback of known multivariate-cryptography algorithms, which is associated with the large size of the public key.

Keywords: post-quantum cryptography, multivariate cryptography, finite algebra, non-commutative algebra, vector finite field, nonlinear mappings.

References

1. Ekert A., Jozsa R. Quantum computation and Shor's factoring algorithm. Reviews of Modern Physics. 1996. vol. 68. no. 3. pp. 733–752.
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. Post-Quantum Cryptography. Proceedings of the 13th International Conference, PQCrypto 2022. Lecture Notes in Computer Science. 2022. vol. 13512.
4. Johansson T., Smith-Tone D. Post-Quantum Cryptography. Proceedings of the 14th International Conference, PQCrypto 2023. Lecture Notes in Computer Science. 2023. vol. 14154.
5. Alagic G, Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Liu Y., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D., Apon D. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology. 2022. Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934458 (accessed: обращения: 25.02.2024).

6. Han J., Zhuang J. DLP in semigroups: algorithms and lower bounds. J. Math. Cryptol. 2022. vol. 16. no. 1. pp. 278–288.
7. Battarbee C., Kahrobaei D., Perret L., Shahandashti S.F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures. Post-Quantum Cryptography. PQCrypto 2023. Lecture Notes in Computer Science. 2023. vol. 14154. pp. 113–138. DOI: 10.1007/978-3-031-40003-2_5.
8. Vysotskaya V.V., Chizhov I.V. The security of the code-based signature scheme based on the Stern identification protocol. Applied Discrete Mathematics. 2022. № 57. C. 67−90. DOI: 10.17223/20710410/57/5.
9. Kosolapov Y.V., Turchenko O.Y. On the construction of a semantically secure modification of the McEliece cryptosystem. Applied Discrete Mathematics. 2019. № 45. C. 33−43. DOI: 10.17223/20710410/45/4.
10. Gartner J. NTWE: A Natural Combination of NTRU and LWE. Post-Quantum Cryptography. PQCrypto 2023. Lecture Notes in Computer Science, 2023. vol. 14154. pp. 321–353. DOI: 10.1007/978-3-031-40003-2_12.
11. Lysakov I.V. Solving some cryptanalytic problems for lattice-based cryptosystems with quantum annealing method. Mathematical Aspects of Cryptography. 2023. vol. 14. no. 2. pp. 111–122. DOI: 10.4213/mvk441.
12. Hamlin B., Song F. Quantum Security of Hash Functions and Property-Preservation of Iterated Hashing. Post-Quantum Cryptography. PQCrypto 2019 / Lecture Notes in Computer Science. 2019. vol. 11505. pp. 329–349. DOI: 10.1007/978-3-030-25510-7_18.
13. Agibalov G.P. ElGamal cryptosystems on Boolean functions. Applied Discrete Mathematics. 2018. № 42. C. 57−65. DOI: 10.17223/20710410/42/4.
14. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography. Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. vol. 80. DOI: 10.1007/978-1-0716-0987-3_2.
15. Debnath S., Kundu N., Mishra D., Choudhury T. Post-quantum digital signature scheme based on multivariate cubic problem. Journal of Information Security and Applications. 2020. vol. 53. DOI: 10.1016/j.jisa.2020.102512.
16. Ding J., Petzoldt A., Schmidt D.S. Oil and Vinegar. Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. vol. 80. pp. 89–151. Springer, New York. DOI: 10.1007/978-1-0716-0987-3_5.
17. Cartor R., Cartor M., Lewis M., Smith-Tone D. IPRainbow. Post-Quantum Cryptography. PQCrypto 2022. Lecture Notes in Computer Science. 2022. vol. 13512. pp. 170–184. DOI: 10.1007/978-3-031-17234-2_9.
18. Beullens W. MAYO: practical post-quantum signatures from oil-and-vinegar maps. Proceedings of the International Conference on Selected Areas in Cryptography (SAC 2021). Lecture Notes in Computer Science. 2022. vol. 13203. pp. 355–376.
19. Moldovyan A.A., Moldovyan D.N., Moldovyan N.A. A new approach to the development of multivariate cryptography algorithms. Voprosy kiberbezopasnosti – Cibersecurity questtions. 2023. no. 2(54). pp. 52–64. DOI: 10.21681/2311-3456-2023-2-52-6.
20. Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography. Computer Science Journal of Moldova. 2024. no. 1(94). pp. 46–60. DOI: 10.56415/csjm.v32.04.
21. Duong M.T., Moldovyan D.N., Do B.V., Nguyen M.H. Post-quantum signature algorithms on non-commutative algebras, using difficulty of solving systems of quadratic equations. Computer Standards and Interfaces. 2023, vol. 86. no. 103740. DOI: 10.1016/j.csi.2023.103740.

22. Moldovyan D.N. A practical digital signature scheme based on the hidden logarithm problem. Computer Science Journal of Moldova. 2021. vol. 29, no. 2(86). pp. 206–226.
23. Moldovyan N.A., Moldovyanu P.A. Vector Form of the Finite Fields GF(pm). Bulletin of Academy of Sciences of Moldova. Mathematics. 2009. no. 3(61). pp. 57–63.
24. Ding J., Petzoldt A., Schmidt D.S. Solving Polynomial Systems. In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. New York. 2020. vol. 80. pp. 185–248. DOI: 10.1007/978-1-0716-0987-3_8.
25. Ding J., Petzoldt A. Current State of Multivariate Cryptography. IEEE Security and Privacy. 2017. vol. 15. no. 4. pp. 28–36.
26. Qiao S., Han W., Li Y., Jiao L. Construction of Extended Multivariate Public Key Cryptosystems. International Journal of Network Security. 2016. vol. 18. no. 1. pp. 60–67.
27. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [on line] 2021. Available at: https://www.pqcrainbow.org/ (accessed: 25.02.2024).

Moldovyan Alexandr — Ph.D., Dr.Sci., Professor, Chief researcher, Laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: cryptography, post-quantum public-key cryptoalgorithms, digital signature, cryptographic protocols, computer security. The number of publications — 200. maa1305@yandex.ru; 39, 14-th Line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)333-3411.

Moldovyan Dmitriy — Ph.D., Associate professor of the department, Department of information systems, Saint Petersburg Electrotechnical University "LETI". Research interests: cryptography, post-quantum public-key cryptoalgorithms on algebras and on non-linear mappings, digital signature, information security. The number of publications — 100. mdn.spectr@mail.ru; 5, Professor Popov St., 199178, St. Petersburg, Russia; office phone: +7(812)234-2772.

Moldovyan Nikolay — Ph.D., Dr.Sci., Professor, Chief researcher, Laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: cryptography, post-quantum public-key cryptoalgorithms, digital signature, block ciphers, computer security. The number of publications — 230. nmold@mail.ru; 39, 14-th Line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)333-3411.

Acknowledgements. This research is supported by RFBR: projects #24-21-00225 (Sections 2, 3, and 4) and #24-41-04006 (Sections 5, 6, 7, and 8).