НОВЫЙ ПОДХОД К РАЗРАБОТКЕ АЛГОРИТМОВ МНОГОМЕРНОЙ КРИПТОГРАФИИ

Молдовян А.А.[1], Молдовян Д.Н.[2], Молдовян Н.А.[3]

Цель *работы: уменьшение размера открытого ключа двухключевых алгоритмов многомерной криптографии, основанных на вычислительной трудности решения систем многих степенных уравнений со многими неизвестными.*

Метод *исследования: использование нелинейных отображений, задаваемых в виде операций возведения в степень в конечных расширенных полях $GF(q^m)$, представленных в форме конечных алгебр. Последнее обеспечивает возможность выполнения операции возведения в степень в поле $GF(q^m)$ путем вычисления значений степенных многочленов над полем GF(q), задающих трудно обратимое нелинейное отображение векторного пространства над GF(q) с потайным ходом. Благодаря использованию нелинейных отображений данного типа обеспечивается возможность задания открытого ключа в алгоритмах многомерной криптографии в виде нелинейного отображения, реализуемого как вычисление значений набора многочленов третьей и шестой степени. При этом за счет использования маскирующих линейных отображений, не приводящих к увеличению числа слагаемых в многочленах, уменьшается размер открытого ключа по сравнению с известными алгоритмами-аналогами, в которых открытый ключ представлен набором многочленов второй и третьей степени. Предлагаемый подход потенциально расширяет области практического применения постквантовых алгоритмов открытого шифрования и электронной цифровой подписи, относящихся к многомерной криптографии, за счет существенного уменьшения размера открытого ключа.*

Результаты *исследования: сформулированы основные положения нового подхода к разработке алгоритмов многомерной криптографии Предложено задание трудно обратимых нелинейных отображений с потайным ходом в виде операций возведения во вторую и третью степень в конечных расширенных полях $GF(q^m)$, представленных в виде конечной алгебры. Дано обоснование задания открытого ключа в виде, включающем суперпозицию двух нелинейных отображений, выполняемых как вычисление набора многочленов второй и третьей степени, заданных над GF(q). Предложены приемы реализаций отображений указанного типа и рассмотрены конкретные варианты задания полей $GF(q^m)$ в форме конечных алгебр. Выполнена оценка размера открытого ключа в алгоритмах, разработанных в рамках нового подхода. при заданном уровне стойкости.*

Научная и практическая значимость *результатов статьи состоит в основных положениях нового способа построения алгоритмов многомерной криптографии, основанных на вычислительной трудности решения систем многих степенных уравнений со многими неизвестными и относящихся к постквантовым криптосхемам. Предлагаемый подход расширяет области практического применения постквантовых алгоритмов данного типа за счет существенного уменьшения размера открытого ключа, обеспечивающего предпосылки повышения производительности и уменьшения технических ресурсов для их реализации.*

Ключевые слова: *конечные поля; многочлены; отображения; нелинейные отображения; вычислительно трудная задача; многомерная криптография; открытое шифрование; цифровая подпись; постквантовая криптография.*

DOI:10.21681/2311-3456-2023-2-52-64

1 Молдовян Александр Андреевич, доктор технических наук, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. Orcid.org/0000-0001-5480-6016. E-mail: maa1305@yandex.ru

2 Молдовян Дмитрий Николаевич, кандидат технических наук, доцент Санкт-Петербургского государственного электротехнического университета ЛЭТИ, Санкт-Петербург, Россия. Orcid.org/0000-0002-4483-5048. E-mail: mdn.spectr@mail.ru

3 Молдовян Николай Андреевич, доктор технических наук, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. Orcid.org/0000-0002-4483-5048. E-mail: nmold@mail.ru

Введение

В настоящее время завершился третий раунд всемирного конкурса по разработке постквантовых стандартов на алгоритмы электронной цифровой подписи (ЭЦП) и открытого согласования ключа, проводимого под эгидой Национального института стандартов и технологий США (НИСТ) [1]. На данном этапе НИСТ определился с тремя алгоритмами CRYSTAL-Dilithium, FALCON (оба используют вычислительно трудные задачи в алгебраических решетках) и SPHINICS+ (основан на трудности обращения хэш-функции), выбранными в качестве основы для посткантовых стандартов ЭЦП [1]. Выбор алгоритмов открытого согласования ключа для стандартизации предполагается осуществить в ходе начавшегося четвертого раунда конкурса НИСТ. Несмотря на то, что выбор алгоритмов ЭЦП для стандартизации осуществлен, НИСТ объявил дополнительный набор заявок в номинации постквантовых ЭЦП, основанных не на структурированных алгебраических решетках и не на хэш-функциях [2]. Целью дополнительного набора заявок является выбор на четвертом этапе конкурса более практичного постквантового алгоритма ЭЦП для принятия постквантового стандарта широкого применения.

В области постквантовой криптографии имеется самостоятельное достаточно широкое направление, известное как многомерная криптография [3,4,5]. Алгоритмы открытого шифрования и алгоритмы ЭЦП, относящиеся к многомерной криптографии, основаны на вычислительной трудности решения систем из многих степенных уравнений (обычно квадратных и реже кубических) с многими неизвестными. Впервые алгоритмы данного типа предложены в 1988 г. За прошедшие 34 года разработок и исследований области многомерной криптографии предложен ряд постквантовых алгоритмов ЭЦП [6,7] и алгоритмов открытого шифрования [6,7]. К многомерной криптографии также относятся алгоритмы ЭЦП Rainbow [8,9] и GeMSS [10], участвовавшие в конкурсе НИСТ и выбранными в качестве финалиста и альтернативного алгоритма, соответственно, для рассмотрения на третьем раунде конкурса. Однако эти алгоритмы не были взяты для стандартизации, поскольку в них используется открытый ключ чрезмерно большого размера (от сотен байт до нескольких мегабайт для их разных модификаций, соответствующих различным уровням стойкости от 2^{128} до 2^{256}).

Появление большого числа алгоритмов многомерной криптографии и интерес к ним как к постквантовым двухключевым алгоритмам обусловили значительный интерес к разработке вычислительно эффективных алгоритмов решения систем многих степенных уравнений со многими неизвестными и к оценке сложности этих алгоритмов. Лучше известные в настоящее время алгоритмы решения таких систем основаны на так называемых алгоритмах F4[4] и F5[5] для вычисления базиса Гребнера и имеют вычислительную сложность, которая является экспоненциальной от числа уравнений и сравнительно слабо зависит от порядка поля в котором задается система степенных уравнений. Для наиболее типичных для алгоритмов многомерной криптографии случаев оценки приведены в работе [11] (см. табл. 1).

Типовое построение алгоритмов многомерной криптографии определяется механизмом формирования открытого ключа в виде множества *u* многочленов второй или третьей степени с коэффициентами и переменными, принимающими значения в поле

Таблица 1

Минимальное число уравнений обеспечивающее заданный уровень стойкости алгоритмов многомерной криптографии в случае равенства числа уравнений и неизвестных при задании системы квадратных уравнений в поле GF(q) [11]

W	2^{80}	2^{100}	2^{128}	2^{192}	2^{256}
q = 16	30	39	51	80	110
q = 31	28	36	48	75	103
q = 256	26	33	43	68	93

4 Faugere J.C., “A new efficient algorithm for computing Gröbner basis (F4)” Journal of Pure and Applied Algebra, vol. 139, pp. 61–88, 1999.

5 Faugre, J.-C.: A new efficient algorithm for computing Gröbner basis without reduction to zero (F5). In: Proceedings of the International Symposium on Symbolic and Algebraic Computation. 2002, pp. 75–83.

$GF(q)$, которые описывают нелинейное отображение $\mathcal{P}$ входных n-мерных векторов, заданных над полем $GF(q)$, в множество выходных u-мерных векторов с координатами в $GF(q)$. Однозначность процедуры расшифровывания имеет место при выполнении условия $u \geq n$. Значение u задает число уравнений в упомянутой системе равное u, а число неизвестных - значению n. При этом открытый ключ описывает трудно обратимое отображение, которое имеет секретную лазейку, известную владельцу (создателю) открытого ключа. С помощью этой лазейки владелец открытого ключа может выполнить отображение $\mathcal{P}^{-1}$ (обратное к $\mathcal{P}$), причем процедура обратного отображения может включать операции вне поля $GF(q)$.

Для формирования отображения $\mathcal{P}$, заданного набором степенных многочленов, разрабатывается достаточно простое нелинейное отображение $\mathcal{N}$, которое может быть представлено в виде набора степенных многочленов над $GF(q)$ и для которого можно найти обратное отображение $\mathcal{N}^{-1}$, причем $\mathcal{N}^{-1}$ вычислимо достаточно эффективно. Отображение $\mathcal{N}^{-1}$ является замаскированным в открытом ключе $\mathcal{P}$ за счет того, что $\mathcal{P}$ вычисляется как суперпозиция $\mathcal{N}$ и одного или двух линейных отображений $\mathcal{L}_1$ и $\mathcal{L}_2$, например, в соответствии с выражениями $\mathcal{P} = \mathcal{N}\cdot\mathcal{L}_1$, $\mathcal{P} = \mathcal{L}_2\bullet\mathcal{N}$ или $\mathcal{P} = \mathcal{L}_2\bullet\mathcal{N}\cdot\mathcal{L}_1$, где отображения $\mathcal{L}_1$ и $\mathcal{L}_2$ реализуются, например, как умножение входного вектора на невырожденную матрицу (заданную над полем $GF(q)$ и представляющую элемент секретного ключа) соответствующего размера.

Выбор отображения $\mathcal{N}$ представимого набором многочленов, значения которых определяют координаты выходного вектора (вектора-образа), задаваемыми координатами (значениями переменных в многочленах) входного вектора (отображаемого вектора, т. е. вектора-прообраза), обеспечивает возможность записать отображение $\mathcal{P}$ в виде набора многочленов, степень которых равна степени многочленов, задающих отображение $\mathcal{N}$. Благодаря маскирующим отображениям $\mathcal{L}_1$ и $\mathcal{L}_2$ по набору многочленов, задающих открытый ключ $\mathcal{P}$, без знания $\mathcal{N}$ вычислительно трудно выполнить отображение $\mathcal{P}^{-1}$. Однако осуществление отображений $\mathcal{L}_1$ и $\mathcal{L}_2$ приводит к значительному возрастанию числа слагаемых в многочленах, описывающих отображение к $\mathcal{P}$,

Алгоритм шифрования по ключу $\mathcal{P}$ (процедура открытого шифрования) осуществляется следующим образом:

1. Входное щифруемое сообщение рассматривается как n-мерный вектор $\mathbf{T} = (t_1, t_2, ..., t_n)$ с координатами в $GF(q)$.

2. Выходной текст (шифртекст) вычисляется как u-мерный вектор $\mathbf{C} = \mathcal{P}(\mathbf{T}) = (c_1, c_2, ..., c_u)$ с координатами в $GF(q)$.

Восстановление исходного текста **T** по шифртексту **C** осуществляется как нахождение прообраза вектора **C**:

$$\mathbf{T} = \mathcal{L}_1^{-1}(\mathcal{N}^{-1}(\mathcal{L}_2^{-1}(\mathbf{C}))) = \mathcal{L}_1^{-1}\bullet\mathcal{N}^{-1}\bullet\mathcal{L}_2^{-1}(\mathbf{C}).$$

Генерация ЭЦП к электронному документу D выполняется владельцем открытого ключа $\mathcal{P}$ по следующему алгоритму вычисления подписи:

1. Вычислить хэш-значение от документа D по формуле $H = f_H(D)$, где f_H – некоторая специфицированная коллизионно стойкая хэш-функция f_H (алгоритм вычисления которой входит в спецификацию алгоритма ЭЦП).

2. Представить хэш-значение H в виде вектора $\mathbf{H} = (h_1, h_2, ..., h_n)$ с координатами в поле $GF(q)$.

3. Вычислить ЭЦП в виде вектора **S** (прообраза вектора **H**): $\mathbf{S} = \mathrm{L}_1^{-1}\bullet\mathcal{N}^{-1}\bullet\mathcal{L}_2^{-1}(\mathbf{H})$.

Верификация подписи **S** выполняется по открытому ключу $\mathcal{P}$ в соответствии со следующей процедурой проверки подлинности ЭЦП:

1. Вычислить хэш-значение H от документа D: $H = f_H(D)$ и представить H в виде вектора **H**.

2. Вычислить вектор **H′** (образ вектора **S**): $\mathbf{H}' = \mathcal{P}(\mathbf{S})$.

3. Сравнить значения **H** и **H′**. При выполнении равенства $\mathbf{H} = \mathbf{H}'$ подпись считается правильной (подлинной), иначе – ложной.

Легко увидеть, что нахождение n-мерного вектора-прообраза по u-мерному вектору-образу может быть осуществлено, решая систему степенных уравнений, задаваемых открытым ключом $\mathcal{P}$ путем приравнивания значений многочленов к соответствующим координатам вектора-образа. Значения n координат вектора-прообраза будут найдены как решение системы из u степенных уравнений от n неизвестных.

Атаки, использующие алгоритмы решения системы многих степенных уравнений со многими неизвестными, называются прямыми атаками [12,13]. Разработаны также структурные атаки, использующие специфику построения алгоритмов многомерной криптографии [14,15]. Структурные атаки и их вычислительная эффективность в значительной степени зависят от строения преобразования $\mathcal{P}$. Значительное внимание исследователей было уделено оценке стойкости ряда алгоритмов многомерной криптографии к атакам по побочным каналам [16-19]. Рассмотрение атак последнего типа свидетельствует о мнении со стороны ряда специалистов о высокой вероятности

практического применения многомерных алгоритмов ЭЦП и открытого шифрования, несмотря на чрезмерно большие размеры открытого ключа для известных криптоалгоритмов данного типа при обеспечении требуемого уровня.

Постановка цели исследования

Целью данного исследования является сокращение размера открытого ключа в алгоритмах многомерной криптографии при заданном уровне стойкости, что обеспечит расширение областей их применения в постквантовую эру.

Для достижения этой цели решается задача задания параметризуемых нелинейных преобразований, реализуемых как операции возведения во вторую, третью и более высокую степень в полях $GF(q^m)$ при значении m, удовлетворяющим условию $1 < m \geq n$, допускающих вычисление результата выполнения указанной операции как вычисление значений набора многочленов над полем $GF(q)$. Для обеспечения последней возможности применяется задание поля $GF(q^m)$ в форме m-мерной конечной алгебры над полем $GF(q)$ по способу, впервые предложенному в работе [20]. Для расширения возможностей параметризации задаваемого нелинейного преобразования и использования параметров задания поля $GF(q^m)$ в качестве элементов секретного ключа рассматривается возможность задания полей $GF(q^m)$ с использованием различных таблиц умножения базисных векторов (ТУБВ) и различных распределений структурных констант в этих таблицах. Для задания достаточно большого ключевого пространства поля $GF(q^m)$ задаются по ТУБВ с m различными константами, имеющих уникальное распределение по ячейкам ТУБВ.

На основе указанного механизма задания нелинейных преобразований предлагается новая концепция разработки алгоритмов многомерной криптографии, состоящая в использовании возможности формирования открытого ключа в виде суперпозиции двух нелинейных отображений $\mathcal{N}_1$ и $\mathcal{N}_2$, реализуемых с использованием операций экспоненцирования в поле $GF(q^m)$, заданном в форме конечной алгебры, и обеспечивающих взаимное маскирование соответствующих обратных отображений $\mathcal{N}_1^{-1}$ и $\mathcal{N}_2^{-1}$. При этом выбирая, различные соотношения значений m, n и u, каждое из отображений $\mathcal{N}_1$ и $\mathcal{N}_2$ может быть реализовано как каскад из нескольких операций экспоненциирования, обеспечивая достаточную гибкость при выборе конкретных реализаций результирующего преобразования $\mathcal{P}$, задаваемого набором многочленов степени 4, 6 и 9. За счет повышения степени многочленов обеспечивается потенциальная возможность существенного уменьшения числа слагаемых в каждом из многочленов указанного набора при заданном уровне стойкости, приводящая к существенному уменьшению размера открытого ключа $\mathcal{P}$.

1. Задание конечных полей в форме конечных алгебр

В векторных пространствах определены операции сложения и скалярного умножения. Заданное над конечным полем $GF(p^z)$ характеристики p конечное m-мерное векторное пространство, в котором дополнительно определена операция *умножения всевозможных пар векторов, обладающая свойствами замкнутости и дистрибутивности слева и справа относительно операции сложения*, называется конечной m-мерной алгеброй. Произвольные два вектора **A** и **B** можно записать в виде суммы однокомпонентных векторов: $\mathbf{A} = \sum_{i=1}^{m} a_i \mathbf{e}_i$ и $\mathbf{B} = \sum_{j=1}^{m} b_j \mathbf{e}_j$, где $\mathbf{e}_i$ – *формальные базисные векторы*, и определить операцию умножения по следующей формуле:

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

где каждое из всевозможных произведений пар базисных векторов заменяется на некоторый базисный вектор $\mathbf{e}_k$ или на однокомпонентный вектор вида $\lambda\mathbf{e}_k$ (где координата λ называется структурной константой) по правилу, задаваемому некоторой ТУБВ.

В работе [20] впервые показано, что при выполнении определенных условий задания m-мерных конечных алгебр они представляют собой конечное поле $GF((p^z)^m)$ – расширение степени m поля $GF(p^z)$. Рассмотрим ТУБВ со структурными константами $\tau \in GF(p^z)$, $\varepsilon \in GF(p^z)$ и $\lambda \in GF(p^z)$, представленную как табл. 2, в которой в первой строке базисные векторы расположены в порядке возрастания их индексов и каждая последующая стока получена циклическим сдвигом влево предыдущей строки. На основе теоретического доказательств для случаев $m = 2$ и $m = 3$ при $\tau = 1$ и вычислительных экспериментов для размерностей $m \geq 4$ в [20] предложена следующая гипотеза:

> при выполнении делимости $m \mid (p^z - 1)$ и определения операции умножения по ТУБВ, представленной как табл. 2, существуют многочисленные тройки значений структурных констант τ, ε

Таблица 2

Формирование конечных полей вида $GF((p^z)^m)$ в виде m-мерных конечных алгебр, заданных над полем $GF(p^z)$, где $z \geq 1$.

×	e_1	e_2	e_3	e_4	e_5	…	e_{m-1}	e_m
e_1	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\mathbf{e}_4$	$\tau\mathbf{e}_5$	τ…	$\tau\mathbf{e}_{m-1}$	$\tau\mathbf{e}_m$
e_2	$\tau\mathbf{e}_2$	$\varepsilon\mathbf{e}_3$	$\varepsilon\mathbf{e}_4$	$\varepsilon\mathbf{e}_5$	ε…	$\varepsilon\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_m$	$\tau^{-1}\varepsilon\lambda\mathbf{e}_1$
e_3	$\tau\mathbf{e}_3$	$\varepsilon\mathbf{e}_4$	$\varepsilon\mathbf{e}_5$	ε…	$\varepsilon\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_m$	$\tau^{-1}\varepsilon\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$
e_4	$\tau\mathbf{e}_4$	$\varepsilon\mathbf{e}_5$	ε…	$\varepsilon\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_m$	$\tau^{-1}\varepsilon\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$
e_5	$\tau\mathbf{e}_5$	ε…	$\varepsilon\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_m$	$\tau^{-1}\varepsilon\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$
…	τ…	$\varepsilon\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_m$	$\tau^{-1}\varepsilon\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	λ…
$\mathbf{e}_{m-1}$	$\tau\mathbf{e}_{m-1}$	$\varepsilon\mathbf{e}_{m-1}$	$\tau^{-1}\varepsilon\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	λ…	$\lambda\mathbf{e}_{m-2}$
$\mathbf{e}_m$	$\tau\mathbf{e}_m$	$\tau^{-1}\varepsilon\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	…	$\lambda\mathbf{e}_{m-2}$	$\lambda\mathbf{e}_{m-1}$

и λ, при которых заданная *m*-мерная конечная алгебра является конечным полем $GF((p^z)^m)$.

Для случая при τ = 1 и при ε = 1 справедливость этой гипотезы легко устанавливается демонстрацией того, что рассматриваемая алгебра является изоморфной полю многочленов $GF((p^z)^m)$ с операцией умножения многочленов, заданных над $GF(p^z)$, по модулю неприводимого многочлена вида $x^m - \lambda$, где λ непредставим в виде *r*-й степени другого элемента поля $GF(p^z)$ для всех значений *r*, равных делителям числа *m*. Действительно, легко показать, что отображение многочленов вида $k_1 + k_2x + k_3x^2 + \ldots + k_mx^{m-1}$ в векторы вида $(k_1, k_2, k_3, \ldots k_m)$ является изоморфизмом, поскольку многочлен, полученный выполнением арифметического умножения произвольных двух многочленов степени не выше значения $m - 1$ и деления полученного произведения на неприводимый многочлен $x^m - \lambda$ отображается в вектор, являющийся результатом умножения *m*-мерных векторов, являющихся образами указанных двух многочленов.

Для рассматриваемых в настоящей работе приложений полей $GF((p^z)^m)$ в форме конечных алгебр (которые можно называть векторными полями) важным является установление других распределений структурных констант, не нарушающих свойства ассоциативности и коммутативности операции умножения. Для простых значений размерности *m* было установлено $m - 3$ дополнительных распределений структурных констант и найден алгоритм построения $m - 3$ дополнительных распределений. При этом для случайных фиксируемых значений $m - 1$ константы всегда можно экспериментально подобрать множество разных значений для *m*-ой константы, при которых формируемая алгебра является полем (этот факт экспериментально устанавливался нахождением элемента алгебры, имеющего порядок, равный значению $p^{zm} - 1$).

Примеры таких распределений иллюстрируются в табл. 3 ($m = 3$), табл. 4 ($m = 4$) , табл. 5 ($m = 5$) и табл. 6 ($m = 7$) при задании конечных *m*-мерных алгебр над конечными полями, в том числе над полями характеристики два. Интерес к заданию алгебр, являющихся полями, над конечными полями характеристики два связан с возможностью задания нелинейного биективного отображения $\mathcal{N}$ как операции возведения в квадрат в таких полях (число 2 не делит порядок мультипликативной группы поля характеристики два, что обеспечивает однозначность операции извлечения корня второй степени). При задании аналогичных алгебр над конечными полями нечетной характеристики такой возможности нет, поскольку в этом случае отображение, задаваемое возведением в квадрат не обладает свойством биективности. В случае нечетной характеристики поля биективные нелинейные отображения $\mathcal{N}$ могут быть заданы операциями возведения только в нечетную степень. Однако при несущественном дополнении схемы построения многомерных алгоритмов ЭЦП, открытого шифрования и открытого согласования ключа могут быть использованы нелинейные отображения, задаваемые операцией возведения в квадрат в векторных полях нечетной характеристики.

Очевидно, что при увеличении размера степени существенно возрастает размер открытого ключа, что с целью минимизации последнего определяет интерес к операциям возведения в квадрат и куб.

В отличие от случая задания полей $GF((2^z)^m)$ в виде конечных алгебр, когда такая возможность имеется

для ограниченного числа различных размерностей m (из-за необходимости выполнить условие делимости $m \mid p^z - 1$), поля $GF((p^z)^m)$ с нечетным значением характеристик могут быть заданы в форме конечных алгебр для произвольных значений размерности. Степень расширения $z = 20$ двоичного поля задает делимость числа $2^z - 1$ на 3, 5 и 11, т.е. над полем $GF(2^{20})$ могут быть заданы векторные поля $GF((2^{20})^3)$, $GF((2^{20})^5)$ и $GF((2^{20})^{11})$ путем задания операции векторного умножения по табл. 3, 5 и 6 соответственно (заметим, что операция возведения в куб в поле $GF((2^{20})^3)$ будет задавать небиективное нелинейное отображение, тогда как в полях $GF((2^{20})^5)$ и $GF((2^{20})^{11}$ – биективное).

Таблица 3.

Пример задания операции умножения в конечных полях $GF((2^{20})^3)$, имеющих вид трехмерных конечных алгебр над полем $GF(2^{20})$, с использованием трех структурных констант τ, ε, $\lambda \in GF(2^{20})$

×	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$
$\mathbf{e}_2$	$\tau\mathbf{e}_2$	$\varepsilon\mathbf{e}_3$	$\tau^{-1}\varepsilon\lambda\mathbf{e}_1$
$\mathbf{e}_3$	$\tau\mathbf{e}_3$	$\tau^{-1}\varepsilon\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$

Рассмотрим примеры задания нелинейного отображения $\mathcal{N}$ с использованием векторного поля $GF(p^4)$, заданного по табл. 4. Небиективное нелинейное отображение $\mathcal{N}(\mathbf{X}) = \mathbf{Y}$ четырехмерных векторов $\mathbf{X}$ может быть задано по формуле $\mathbf{Y} = \mathbf{X}^2$. Используя табл. 4 легко получить четыре многочлена над $GF(p)$, описывающие координаты вектора $\mathbf{Y}$ через координаты входного вектора $\mathbf{X}$.

$$\mathrm{Y} = (y_1, y_2, y_3, y_4) = \mathrm{X}^2 = (x_1, x_2, x_3, x_4)^2 :$$

$$\begin{cases} y_1 = \tau x_1^2 + 2\tau^{-1}\lambda\varepsilon\mu x_2 x_4 + \tau^{-1}\lambda\varepsilon x_3^2; \\ y_2 = 2\tau x_1 x_2 + 2\lambda x_3 x_4; \\ y_3 = 2\tau x_1 x_3 + \mu\varepsilon x_2^2 + \mu\lambda x_4^2; \\ y_4 = 2\tau x_1 x_4 + 2\varepsilon x_2 x_3. \end{cases}$$

Биективное нелинейное отображение $\mathcal{N}$ может быть задано по формуле $\mathbf{Y} = \mathbf{X}^3$. Используя табл. 4 легко получить четыре многочлена над $GF(p)$, описывающие координаты вектора $\mathbf{Y}$, являющегося образом входного вектора $\mathbf{X}$.

$$\mathrm{Y} = (y_1, y_2, y_3, y_4) = \mathrm{X}^3 = (x_1, x_2, x_3, x_4)^3 :$$

$$\begin{cases} y_1 = \tau x_1^3 + 6\lambda\varepsilon\mu x_1 x_2 x_4 + 3\lambda\varepsilon x_1 x_3^2 + \\ + 3\tau^{-1}\lambda\varepsilon^2\mu x_2^2 x_3 + 3\tau^{-1}\lambda^2\varepsilon\mu x_3 x_4^2; \\ y_2 = 3\tau^2 x_1^2 x_2 + 6\tau\lambda x_1 x_3 x_4 + 3\lambda\varepsilon\mu x_2^2 x_4 + \\ + 3\lambda\varepsilon x_2 x_3^2 + \mu\lambda^2 x_4^3; \\ y_3 = 3\tau^2 x_1^2 x_3 + 3\tau\mu\varepsilon x_1 x_2^2 + 3\tau\mu\lambda x_1 x_4^2 + \\ + 6\lambda\varepsilon\mu x_2 x_3 x_4 + \lambda\varepsilon x_3^3; \\ y_4 = 3\tau^2 x_1^2 x_4 + 6\tau\varepsilon x_1 x_2 x_3 + \\ + \mu\varepsilon^2 x_2^3 + 3\mu\varepsilon\lambda x_2 x_4^2 + 3\lambda\varepsilon x_3^2 x_4. \end{cases}$$

Если отображение $\mathbf{Y} = \mathcal{N}(\mathbf{X}) = \mathbf{X}^3$ задано последними четырьмя многочленами, то обратное отображение вектора может быть выполнено следующими двумя способами:

1) путем решения системы уравнений с неизвестными x_1, x_2, x_3 и x_4;

2) путем восстановления значений структурных констант (восстановление конкретной модификации векторного поля $GF(p^4)$ по заданным значениям коэффициентов многочленов.

Второй способ тоже реализуется как решение системы уравнений, которые определяются формулами, связывающими коэффициенты многочленов со значениями структурных констант, причем указанные формулы и вид таблицы умножения базисных векторов предполагаются известными. После восстановления векторного поля $GF(p^4)$ вычисление прообраза $\mathbf{X}$ по образу $\mathbf{Y}$ выполняется по формуле $\mathbf{X} = \mathcal{N}^{-1}(\mathbf{Y}) = \mathbf{X}^t$, где $t = 3^{-1} \bmod p^4 - 1$.

Таблица 4

Задание конечных полей $GF(p^4)$ в виде четырехмерных конечных алгебр над полем $GF(p)$ с использованием четырех структурных констант λ, ε, μ и λ

×	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$
$\mathbf{e}_1$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\mathbf{e}_4$
$\mathbf{e}_2$	$\tau\mathbf{e}_2$	$\mu\varepsilon\mathbf{e}_3$	$\varepsilon\mathbf{e}_4$	$\tau^{-1}\mu\lambda\varepsilon\mathbf{e}_1$
$\mathbf{e}_3$	$\tau\mathbf{e}_3$	$\varepsilon\mathbf{e}_4$	$\tau^{-1}\varepsilon\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$
$\mathbf{e}_4$	$\tau\mathbf{e}_4$	$\tau^{-1}\mu\varepsilon\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\mu\lambda\mathbf{e}_3$

Первый из указанных двух способов соответствует прямой атаке на криптоалгоритмы, разрабатываемые по предлагаемому в данной статье способу, а

Таблица 5

Задание пятимерных конечных алгебр над полем GF(p), являющихся векторными полями $GF(p^5)$, с использованием пяти ненулевых структурных констант τ, σ, ε, μ, λ ∈ GF(p)

×	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\mathbf{e}_4$	$\tau\mathbf{e}_5$
$\mathbf{e}_2$	$\tau\mathbf{e}_2$	$\mu\varepsilon\mathbf{e}_3$	$\sigma\varepsilon\mathbf{e}_4$	$\mu\varepsilon\mathbf{e}_5$	$\sigma\mu\tau^{-1}\varepsilon\lambda\mathbf{e}_1$
$\mathbf{e}_3$	$\tau\mathbf{e}_3$	$\sigma\varepsilon\mathbf{e}_4$	$\sigma\varepsilon\mathbf{e}_5$	$\sigma\mu\tau^{-1}\varepsilon\lambda\mathbf{e}_1$	$\sigma\lambda\mathbf{e}_2$
$\mathbf{e}_4$	$\tau\mathbf{e}_4$	$\mu\varepsilon\mathbf{e}_5$	$\sigma\mu\tau^{-1}\varepsilon\lambda\mathbf{e}_1$	$\mu\lambda\mathbf{e}_2$	$\mu\lambda\mathbf{e}_3$
$\mathbf{e}_5$	$\tau\mathbf{e}_5$	$\sigma\mu\tau^{-1}\varepsilon\lambda\mathbf{e}_1$	$\sigma\lambda\mathbf{e}_2$	$\mu\lambda\mathbf{e}_3$	$\sigma\lambda\mathbf{e}_4$

Таблица 6

Задание полей $GF(p^7)$ в виде семимерных конечных алгебр при использовании ненулевых структурных констант η, δ, ρ, λ, ε, μ и τ (коэффициент $\Psi = \eta\delta\rho\lambda\varepsilon\mu\tau^{-1}$)

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

второй – соответствует конкретному типу структурой атаки (структурными называются атаки, учитывающие определенную специфику построения алгоритма). Для задания высокой трудоемкости структурной атаки, связанной с восстановлением значений структурных констант, требуется, чтобы во втором способе решаемая система степенных уравнений содержала достаточно большое число неизвестных.

Задание пятимерного (семимерного) векторного поля над простым полем $GF(p^5)$ может быть задано по ТУБВ, представленной как табл. 5 (табл. 6). При этом в табл. 5 базисные векторы распределены стандартным способом, задаваемым табл. 1 для произвольных размерностей, а в табл. 6 – нестандартным (для фиксированного значения размерности $m > 3$ существуют различные варианты нестандартных распределений базисных векторов, для которых могут быть заданы конечные алгебры, являющиеся полями).

3. Криптоалгоритмы с заданием нелинейного отображения как операции возведения в степень в векторных полях

При реализации нелинейного отображения $\mathbf{Y} = \mathcal{N}(\mathbf{X}') = \mathbf{X}'^3$ с использованием m-мерного векторного поля при $m \geq 19$ (по аналогии с рассмотренным примером) и предварительном покоординатном умножении входного вектора $\mathbf{X}$ на вектор-ключ $\mathbf{K} = (k_1, k_2, \ldots, k_m)$, т. е. $\mathbf{X}' = (x_1k_1, x_2k_2, \ldots, x_mk_m)$, уже можно говорить о двухключевом криптоалгоритме, в котором открытым ключом является набор из m кубических многочленов, заданных набором коэффициентов, упорядоченных в лексикографическом порядке произведений троек переменных, к которым они относятся. Конкретная упорядоченная последовательность указанных троек входит в спецификацию криптоалгоритма и определяется видом ТУБВ, по которой задается векторное поле $GF(p^m)$. Секретным ключом является набор m значений структурных констант и m

Таблица 7

Размеры ключей в алгоритмах с открытым ключом вида $\mathcal{P} = \mathcal{N} \cdot \mathcal{L}$.

m ($n = m$)	длина p, бит	размер открытого ключа, Кбайт	размер секретного ключа, байт	Уровень стойкости к прямой атаке
19	16	< 15	≈80	2^{80}
29	16	< 50	≈120	2^{100}
43	8	< 80	≈90	2^{128}
71	8	< 360	≈150	2^{192}
97	8	< 920	≈200	2^{256}

координат вектора-ключа **K**. При m = 19 и 16-битном простом числе p будем иметь алгоритм с открытым (секретным) ключом размером не более 14000 (80) байт при ожидаемом уровне стойкости 2^{80} (см. табл. 1 с учетом неравенства $p >> 256$).

Легко видеть, что покоординатное перемножение векторов **K** и **X** представляет собой линейное преобразование $\mathcal{L}$ (использование которого не приводит к увеличению размера открытого ключа), а открытый ключ задает нелинейное преобразование $\mathcal{P}(\mathbf{X}) = (\mathcal{L}(\mathbf{X}))^3$ вида $\mathcal{P} = \mathcal{N} \cdot \mathcal{L}$. Для многомерных алгоритмов данного типа задание более высокого ожидаемого уровня стойкости требует существенного увеличения размерности m и связано с достаточно резким увеличением размера открытого ключа, что иллюстрируется в табл. 7.

Резкий рост размера открытого ключа обусловлен тем, что размерность входного (шифруемого) вектора равна размерности используемого векторного поля для задания нелинейного отображения $\mathcal{N}$ и определяет число кубических уравнений, входящих в единую систему, решение которой задает обратное отображение. При этом размер открытого ключа пропорционален третьей степени размерности m.

Для того, чтобы уменьшить размер открытого ключа при больших значениях стойкости, следует использовать векторные поля, размерность которых значительно меньше размерности входного вектора, т. е. n-мерный входной вектор трактовать как каскад из нескольких m-мерных векторов, преобразуемых независимо и с использованием разных наборов значений структурных констант. Для того, чтобы обеспечить влияние каждой координаты входного вектора на каждую координату вектора-образа, можно после первого нелинейного отображения выполнить перестановку координат полученного промежуточного n-мерного вектора (которая является линейным преобразованием и может быть обозначена как $\mathcal{L}_t$) и осуществить второе нелинейное преобразование аналогичного типа, но, возможно, с использованием векторных полей другой размерности.

Например, представляет интерес задание открытого ключа со структурой $\mathcal{P} = \mathcal{N}_2 \cdot \mathcal{L}_t \bullet \mathcal{N}_1 \bullet \mathcal{L}$ с нелинейными преобразованиями $\mathcal{N}_1$ и $\mathcal{N}_2$, из которых первое реализуется как каскад операций возведения в куб (параллельное возведение в куб нескольких векторов), а второе – как каскад операций возведения в квадрат.

При этом размерность последних задается как делитель размерности n (в случае отображения $\mathcal{N}_1$) или m (в случае отображения $\mathcal{N}_2$), а влияние каждой координаты входного вектора на все координаты выходного вектора обеспечивается применением линейного преобразования $\mathcal{L}_t$ в виде достаточно простой перестановки координат векторов на выходе операции $\mathcal{N}_1$, которая не приводит к увеличению числа слагаемых в полиномах открытого ключа и формирует набор входных векторов операции $\mathcal{N}_2$, таких, что каждый из них включает по одной координате из каждого выходного вектора операции $\mathcal{N}_1$.

Рассмотрим конкретный пример $n = u = 28$. Входной вектор $\mathbf{X} = (x_1, x_2, ..., x_{28})$ операции $\mathcal{N}_1$ представляем в виде каскада из 7 векторов: $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2, ..., \mathbf{X}_7)$, где четырехмерные векторы $\mathbf{X}_i = (x^{(i)}_1, x^{(i)}_2, ..., x^{(i)}_4)$, где i = 1, 2,..., 7, заданы над полем $GF(p)$. Нелинейное отображение $\mathcal{N}_1$ реализуется как возведение в куб (например, с использованием табл. 4) каждого из четырехмерных векторов $\mathbf{X}_i$. При этом формируется выходной вектор $\mathbf{Y} = (y_1, y_2, ..., y_{28})$, = $(\mathbf{Y}_1, \mathbf{Y}_2, ..., \mathbf{Y}_7)$, где $\mathbf{Y}_i = (y^{(i)}_1, y^{(i)}_2, ..., y^{(i)}_4)$ для i = 1, 2,..., 7. Линейное отображение $\mathcal{L}_t$ зададим как перестановку координат векторов $\mathbf{Y}_1, \mathbf{Y}_2, ..., \mathbf{Y}_7$, описываемую следующей формулой:

$$u^{(j)}_i = y^{(i)}_j,$$

где $u^{(j)}_i$ координаты каскада векторов $(\mathbf{U}_1, \mathbf{U}_2, ..., \mathbf{U}_4) = \mathbf{U} = (u_1, u_2, ..., u_{28})$, причем $\mathbf{U}_j = (u^{(j)}_1, u^{(j)}_2, ..., u^{(j)}_7)$ для j = 1, 2,..., 4. Нелинейное отображение $\mathcal{N}_2$ зададим как возведение в квадрат (например, с использова-

Таблица 8

Размеры ключей в алгоритмах с открытым ключом вида $\mathcal{P} = \mathcal{N}_2 \bullet \mathcal{L}_t \bullet \mathcal{N}_1 \bullet \mathcal{L}$,
(заданного в виде n степенных многочленов)

$n = m_1 \cdot m_2$	длина p, бит	размер открытого ключа, Кбайт	размер секретного ключа, байт	Уровень стойкости к прямой атаке
20=4×5	16	< 2,5	≈120	2^{80}
28=4×7	16	< 10	≈168	2^{100}
44=4·11	8	< 13	≈132	2^{128}
76=4·19	8	< 36	≈228	2^{192}
116=4·29	8	< 85	≈350	2^{256}

нием табл. 6) каждого из векторов $\mathbf{U}_j$, что формирует выходной вектор $\mathbf{Z} = (z_1, z_2, ..., z_{28}) = (\mathbf{Z}_1, \mathbf{Z}_2, ..., \mathbf{Z}_4)$, где $\mathbf{Z}_j = (z^{(j)}_1, z^{(j)}_2, ..., z^{(j)}_7)$ для $j = 1, 2,..., 4$.

В такой криптосхеме открытый ключ представляет собой 28 многочленов, каждый член которых представляет собой коэффициент умноженный на произведение некоторого набора шести переменных. С учетом того, что координаты векторов $\mathbf{U}_j$ описываются многочленами третьей степени, включающими 5 слагаемых, легко показать, что число слагаемых в каждом многочлене открытого ключа меньше значения 7×5^2, что дает размер открытого ключа менее $28 \times 7 \times 5^2 |p| = 4900|p|$, где $|p|$ – битовый размер характеристики поля $GF(p)$. При этом операции возведения векторов в третью степень выполняются по ТУБВ с уникальными наборами секретных констант, т.е. в рамках каждого их нелинейных $\mathcal{N}_2$ и $\mathcal{N}_1$ используются по 28 секретных значений структурных констант, а в рамках линейного преобразования $\mathcal{L}$, 28 секретных множителей, т. е размер секретного ключа составляет $84|p|$.

Аналогично рассмотренному варианту построения алгоритма с открытым ключом вида $\mathcal{P} = \mathcal{N}_2 \cdot \mathcal{L}_t \bullet \mathcal{N}_1 \cdot \mathcal{L}$, с использованием комбинирования каскада возведений в куб в векторном поле $GF(p^4)$ и каскада возведений в квадрат в поле $GF(p^7)$ можно, используя в рамках второго каскада возведение в квадрат в поле $GF(p^{m_2})$, построить алгоритмы с увеличенным размером входного вектора $n = 4 \cdot m_2$, где $m_2 = 11$, 19 и 29. Параметры получаемых таким способом алгоритмов многомерной криптографии представлены в табл. 8, в которой приведена ожидаемая стойкость к прямой атаке. Сложность атаки с вычислением значений структурных констант значительно выше, поскольку в последнем случае требуется решить систему степенных уравнений с числом неизвестных, равным $3n$, тогда как в прямой атаке решаемая системы уравнений шестой степени включает только n неизвестных.

При выполнении процедуры расшифровывания в алгоритмах с открытым ключом вида $\mathcal{P} = \mathcal{N}_2 \cdot \mathcal{L}_t \bullet \mathcal{N}_1 \cdot \mathcal{L}$, первой выполняемой операцией является нахождение квадратных корней в полях $GF(p)$. Из квадратичного вычета в поле $GF(p)$ существует два корня, для каждого из которых потребуется выполнить последующие операции расшифровывания ($\mathcal{L}_t^{-1}$, $\mathcal{N}_1^{-1}$ и $\mathcal{L}^{-1}$), в результате которых восстанавливается исходное сообщение. Это обстоятельство приводит к уменьшению производительности процедуры расшифровывания. Эта проблема может быть устранена при задании нелинейного отображения $\mathcal{N}_2$ в виде каскада операций возведения в куб. Однако это приводит к существенному увеличению размера открытого ключа.

При построении схемы ЭЦП процедура формирования подписи состоит в выполнении преобразования, обратного преобразованию $\mathcal{P}$, и также в качестве первой операции выполняется операция извлечения квадратно корня из значения хэш-функции $H = f_H(D) = H_1||H_2||H_3||H_4$, трактуемой как n-мерный вектор $\mathbf{H} = (\mathbf{H}_1, \mathbf{H}_2, \mathbf{H}_2, \mathbf{H}_4)$ в виде каскада из четырех m_2-мерных векторов. Для каждого из векторов $\mathbf{H}_1$, $\mathbf{H}_2$, $\mathbf{H}_2$ и $\mathbf{H}_4$ с вероятностью 0,5 корень не существует, поэтому в алгоритме ЭЦП следует предусмотреть генерацию четырех случайных 16-битных значений r_1, r_2, r_3, r_4, их присоединение к значениям H_1, H_2, H_3, H_4 и задание значения $\mathbf{H}_r = (\mathbf{H}_{r1}, \mathbf{H}_{r2}, \mathbf{H}_{r2}, \mathbf{H}_{r4})$ по значениям $H_1||r_1$, $H_2||r_2$, $H_3||r_3$, $H_4||r_4$. При этом на данном шаге в среднем потребуется опробовать 8 различных 16-битных значений, пока не будет получен вектор набор векторов $\mathbf{H}_{r1}$, $\mathbf{H}_{r2}$, $\mathbf{H}_{r2}$ и $\mathbf{H}_{r4}$, из каждого из которых существует квадратный корень в поле $GF(p^{m_2})$, что обе-

спечит возможность выполнения отображения $\mathcal{N}_2^{-1}$, а затем – $\mathcal{L}_t^{-1}$, $\mathcal{N}_1^{-1}$ и $\mathcal{L}^{-1}$, и получения значения подписи $\mathbf{S} = \mathcal{P}^{-1}(\mathbf{H}_r)$. Проверка ЭЦП состоит в выполнении преобразования $\mathbf{H}_r = \mathcal{P}(\mathbf{S})$, восстановления значений $H_1||r_1$, $H_2||r_2$, $H_3||r_3$, $H_4||r_4$, отбрасывания 16 правых битов в каждом из последних четырех значений и сравнении значения $H_1||H_2||H_3||H_4$ со значением хэш-функции, вычисленной от документа D.

3. Обсуждение

Предложенный способ построения алгоритмов многомерной криптографии с использовании конечных полей, задаваемых в форме конечных алгебр, представляет значительный практический интерес, поскольку позволяет существенно уменьшить размер открытого ключа по сравнению с известными аналогами при заданном уровне стойкости. Например, в алгоритмах ЭЦП Rainbow [8] и GeMSS [10] при уровне стойкости 2^{256} размер открытого (секретного) ключа составляет 1885 (1375) Кбайт и 3040 (76) Кбайт соответственно, тогда как для предложенного алгоритма второго типа имеем <85 (≈0,35) Кбайт. Для объективности надо отметить, что алгоритмы Rainbow и GeMSS прошли многостороннее исследование стойкости к различным видам атак и на данный момент имеющиеся оценки их стойкости являются признанными. Очевидно, что для предложенного алгоритма приведенные в табл. 8 оценки стойкости являются ожидаемыми и относятся только к модели прямой атаки. При появлении и детальном рассмотрении других атак могут потребоваться определенные модификации алгоритма, которые приведут к увеличению размера открытого ключа, однако при имеющемся отрыве по этому показателю можно ожидать, что предложенный алгоритм окажется более практичным и в модифицированном варианте.

Специфика строения алгоритмов предложенных двух типов такова, что основной структурной атакой на них является восстановление значений множества структурных констант, задающих конкретный вид полей, операции экспоненцирования в которых использованы в качестве нелинейного отображения. При этом восстановление структурных констант связано с решением системы многих степенных уравнений, в которые в качестве неизвестных входят произведения структурных констант и секретных координат вектора-ключа **K**. При этом число неизвестных в два (в первом типе) и три (во втором типе алгоритмов) раза больше, чем число неизвестных в прямой атаке. Поэтому данный вид структурной атаки ожидаемо имеет существенно более высокий уровень вычислительной сложности по сравнению с прямой атакой при использовании лучших известных алгоритмов решения систем многих степенных уравнений.

В алгоритме второго типа отображение $\mathcal{N}_1$ реализуется как каскад операций возведения в куб в поле $GF(p^{m_1})$, а отображение $\mathcal{N}_2$ –как каскад операций возведения в квадрат в поле $GF(p^{m_2})$, в результате чего формируется открытый ключ в виде набора многочленной шестой степени. Если оба нелинейных отображения реализовать как каскад операций возведения в квадрат (куб), то указанные многочлены будут иметь степень 4 (9), причем это приведет к уменьшению (увеличению) размера открытого ключа.

Идея использования векторных конечных полей при построении алгоритмов многомерной криптографии фактически порождает новую парадигму построения криптоалгоритмов такого типа. Предложенные два типа алгоритмов с одинаковой размерностью входных (n) и выходных (u = n) векторов являются только частными реализациями новой парадигмы построения алгоритмов многомерной криптографии. По аналогии могут быть легко построены алгоритмы для случая u > n. При этом для алгоритмов второго типа с открытым ключом вида $\mathcal{P} = \mathcal{N}_2 \bullet \mathcal{L}_t \bullet \mathcal{N}_1 \bullet \mathcal{L}$ имеются расширенные возможности по выбору степеней расширения векторных конечных полей, используемых для формирования отображения $\mathcal{N}_1$ и отображения $\mathcal{N}_2$, поскольку значение u можно использовать как подгоночный параметр, вычисляемый по формуле $u = m_1 m_2 > n$, а при переходе от выполнения отображения $\mathcal{N}_1$ к $\mathcal{N}_2$ необходимые u - n дополнительных координат формировать с использованием случайного выбора элементов поля $GF(p)$. Это приводит к построению вероятностного алгоритма открытого шифрования.

Также векторные конечные поля могут быть использованы в общепринятой схеме построения алгоритмов многомерной криптографии с центральным нелинейным отображением [3,11], т. е. с открытым ключом вида $\mathcal{P} = \mathcal{L}_2 \bullet \mathcal{N} \bullet \mathcal{L}_1$, где линейные отображения используются как маскирующие преобразования и выполняются как умножение на секретную матрицу, приводящее к существенному увеличению размера открытого ключа.

Выводы

Предложенный подход к построению алгоритмов многомерной криптографии предоставляет возможность существенного сокращения размера открытого ключа по сравнению с известными алгоритмами та-

кого типа при заданном уровне стойкости. При этом возрастает значение степени многочленов, составляющих открытый ключ, что представляет интерес для потенциального повышения стойкости к структурным атакам. Уменьшение размера открытого ключа обеспечивается применением линейных отображений, которые не приводят к увеличению числа слагаемых в многочленах открытого ключа.

В рамках предложенного подхода могут быть легко разработаны алгоритмы с заданием многочленов открытого ключа над полями, порядок которых (от 2^8 до 2^{32}) существенно превышает порядок полей, используемых в большинстве известных аналогах (от 4 до 2^8).

В рамках описанного подхода могут быть использованы конечные поля, заданные в виде конечных алгебр над полями нечетной и четной характеристики. Разработка конкретных алгоритмов, соответствующих второму случаю, представляется самостоятельной задачей отдельной работы.

Литература

1. Alagic G., Apon D., Cooper D. , Dang Q., Dang T., Kelsey J., Lichtinger, J. Yi-Kai Liu, Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NIST IR 8413, National Institute of Standards and Technology, July 2022, 99pp. [Электронный ресурс]. URL: https://doi.org/10.6028/NIST.IR.8413 (обращение 6 января 2023).
2. Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process. September 6, 2022, 99pp. [Электронный ресурс]. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf (обращение 6 января 2023).
3. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 7-23. https://doi.org/10.1007/978-1-0716-0987-3_2
4. Ding J., Petzoldt A., Schmidt D.S. The Matsumoto-Imai Cryptosystem // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 25-60. https://doi.org/10.1007/978-1-0716-0987-3_3
5. Ding J., Petzoldt A., Schmidt D.S. Hidden Field Equations // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 61-88 https://doi.org/10.1007/978-1-0716-0987-3_4
6. Ding J., Petzoldt A., Schmidt D.S. Oil and Vinegar // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 89-151. https://doi.org/10.1007/978-1-0716-0987-3_5
7. Ding J., Petzoldt A., Schmidt D.S. MQDSS // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 153-168. https://doi.org/10.1007/978-1-0716-0987-3_6
8. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [online] 2021. https://www.pqcrainbow.org/ (обращение 6 января 2023).
9. Hashimoto, Y. (2021). Recent Developments in Multivariate Public Key Cryptosystems // In: Takagi, T., Wakayama, M., Tanaka, K., Kunihiro, N., Kimoto, K., Ikematsu, Y. (eds) International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry. Springer, Singapore. 2021. V. 33. P. 209-229. https://doi.org/10.1007/978-981-15-5191-8_16
10. GeMSS: A Great Multivariate Short Signature, https://www-polsys.lip6.fr/Links/NIST/GeMSS.html (обращение 6 января 2023).
11. J. Ding, A. Petzoldt Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017, vol. 15, no. 4, pp. 28-36.
12. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate publickey cryptography // IET Information Security. 2022. P. 1-17. DOI:10.1049/ise2.12092
13. Ding J., Petzoldt A., Schmidt D.S. Solving Polynomial Systems. In: Multivariate Public Key Cryptosystems // Advances in Information Security. Springer. New York. 2020. V. 80. P. 185-248. https://doi.org/10.1007/978-1-0716-0987-3_8
14. Øygarden M., Smith-Tone, D., Verbel, J. On the Effect of Projection on Rank Attacks in Multivariate Cryptography // In: Cheon, J.H., Tillich, JP. (eds) Post-Quantum Cryptography. PQCrypto 2021. Lecture Notes in Computer Science. 2021. V. 12841. P.98-113. Springer, Cham. https://doi.org/10.1007/978-3-030-81293-5_6
15. Øygarden M., Felke P., Raddum H., Cid C. Cryptanalysis of the Multivariate Encryption Scheme EFLASH // Topics in Cryptology – CT-RSA 2020. Lecture Notes in Computer Science. 2020. V. 12006. P. 85-105.
16. Li W., Lu F., Zhao H. Power analysis attacks against QUAD // IAENG International Journal of Computer Science. 2019. V. 46. No. 1. P. 54–60.
17. Kr ̈amer J., Loiero M. Fault attacks on UOV and Rainbow // Constructive Side-Channel Analysis and Secure Design. Proceedings of the International Workshop on Constructive Side-Channel Analysis and Secure Design. Darmstadt, Germany, 2019. P. 193–214.
18. Park A., Shim K., Koo N., Han D. Side-channel attacks on post-quantum signature schemes based on multivariate quadratic equations // IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018. V. 2018. No 3. P. 500–523.
19. Park A, Kyung-Ah Shim, Namhun Koo, Dong-Guk Han. Side-Channel Attacks on Post-Quantum Signature Schemes based on Multivariate Quadratic Equations: Rainbow and UOV // IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018. V. 2018. No. 3. P. 500–523. DOI:10.46586/tches.v2018.i3.500-523
20. Moldovyan N.A., Moldovyanu P.A. Vector Form of the Finite Fields GF(p^m) // Bulletin of Academy of Sciences of Moldova. Mathematics. 2009. No 3 (61). P. 57-63.

A NEW APPROACH TO THE DEVELOPMENT OF MULTIDIMENSIONAL CRYPTOGRAPHY ALGORITHMS

Moldovyan A.A.[6], Moldovyan D.N.[7], and Moldovyan N.A.[8]

Purpose *of work is the reduction in the size of the public key of public-key algorithms of multivariate cryptography based on the computational difficulty of solving systems of many power equations with many unknowns.*

Research method *is use of non-linear mappings defined as exponentiation operations in finite extended fields $GF(q^m)$ represented in the form of finite algebras. The latter makes it possible to perform the exponentiation operation in the field $GF(q^m)$ by calculating the values of power polynomials over the field GF(q), which define a hardly reversible nonlinear mapping of the vector space over GF(q) with a secret trapdoor. Due to the use of nonlinear mappings of this type, it is possible to specify a public key in multidimensional cryptography algorithms in the form of a nonlinear mapping implemented as a calculation of the values of a set of polynomials of the third and sixth degree. At the same time, due to the use of masking linear mappings that do not lead to an increase in the number of terms in polynomials, the size of the public key is reduced in comparison with known analogue algorithms, in which the public key is represented by a set of polynomials of the second and third degrees. The proposed approach potentially expands the areas of practical application of post-quantum algorithms for public encryption and electronic digital signature, related to multidimensional cryptography, by significantly reducing the size of the public key.*

Results *of the study are the main provisions of a new approach to the development of algorithms of multidimensional cryptography are formulated. Hardly invertible nonlinear mappings with a secret trapdoor are proposed in the form of exponentiation operations to the second and third powers in finite extended fields $GF(q^m)$, represented in a form of a finite algebra. A rationale is given for specifying a public key in a form that includes a superposition of two non-linear mappings performed as a calculation of a set of second and third degree polynomials defined over GF(q). Techniques for implementing mappings of this type are proposed and specific options for specifying the fields $GF(q^m)$ in the form of finite algebras are considered. An estimate of the size of the public key in the algorithms developed within the framework of the new approach is made. at a given security level..*

Practical relevance *includes the developed main provisions of a new method for constructing multidimensional cryptography algorithms based on the computational difficulty of solving systems of many power equations with many unknowns and related to post-quantum cryptoschemes. The proposed approach expands the areas of practical application of post-quantum algorithms of this type by significantly reducing the size of the public key, which provides the prerequisites for improving performance and reducing technical resources for their implementation.*

Keywords: *finite fields; polynomials; mapping; non-linear mappings; computationally difficult problem; multivariate cryptography; public encryption; digital signature; post-quantum cryptography*

References

1. Alagic G., Apon D., Cooper D. , Dang Q., Dang T., Kelsey J., Lichtinger, J. Yi-Kai Liu, Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NIST IR 8413, National Institute of Standards and Technology, July 2022, 99 pp. [Jelektronnyj resurs]. URL: https://doi.org/10.6028/NIST.IR.8413 (obrashhenie 6 janvarja 2023).
2. Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process. September 6, 2022, 99pp. [Jelektronnyj resurs]. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf

6 Dmitriy N. Moldovyan, Dr.Sc. (in Tech.) associated professor, Saint Petersburg Electrotechnical University “LETI”, St. Petersburg, Russia. E-mail: mdn.spectr@mail.ru

7 Nikolay A. Moldovyan, Dr.Sc. (in Tech.) chief researcher of laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. Email: nmold@mail.ru

8 Nikolay A. Moldovyan, Dr.Sc. (in Tech.) chief researcher of laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. E mail: nmold@mail.ru

(obrashhenie 6 janvarja 2023).
3. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 7-23. https://doi.org/10.1007/978-1-0716-0987-3_2
4. Ding J., Petzoldt A., Schmidt D.S. The Matsumoto-Imai Cryptosystem // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 25-60. https://doi.org/10.1007/978-1-0716-0987-3_3
5. Ding J., Petzoldt A., Schmidt D.S. Hidden Field Equations // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 61-88 https://doi.org/10.1007/978-1-0716-0987-3_4
6. Ding J., Petzoldt A., Schmidt D.S. Oil and Vinegar // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 89-151. https://doi.org/10.1007/978-1-0716-0987-3_5
7. Ding J., Petzoldt A., Schmidt D.S. MQDSS // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 153-168. https://doi.org/10.1007/978-1-0716-0987-3_6
8. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [online] 2021. https://www.pqcrainbow.org/ (obrashhenie 6 janvarja 2023).
9. Hashimoto, Y. (2021). Recent Developments in Multivariate Public Key Cryptosystems // In: Takagi, T., Wakayama, M., Tanaka, K., Kunihiro, N., Kimoto, K., Ikematsu, Y. (eds) International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry. Springer, Singapore. 2021. V. 33. P. 209-229. https://doi.org/10.1007/978-981-15-5191-8_16
10. GeMSS: A Great Multivariate Short Signature, https://www-polsys.lip6.fr/Links/NIST/GeMSS.html (obrashhenie 6 janvarja 2023).
11. J. Ding, A. Petzoldt Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017, vol. 15, no. 4, pp. 28-36.
12. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate publickey cryptography // IET Information Security. 2022. P. 1-17. DOI:10.1049/ise2.12092
13. Ding J., Petzoldt A., Schmidt D.S. Solving Polynomial Systems. In: Multivariate Public Key Cryptosystems // Advances in Information Security. Springer. New York. 2020. V. 80. P. 185-248. https://doi.org/10.1007/978-1-0716-0987-3_8
14. Øygarden M., Smith-Tone, D., Verbel, J. On the Effect of Projection on Rank Attacks in Multivariate Cryptography // In: Cheon, J.H., Tillich, JP. (eds) Post-Quantum Cryptography. PQCrypto 2021. Lecture Notes in Computer Science. 2021. V. 12841. P.98-113. Springer, Cham. https://doi.org/10.1007/978-3-030-81293-5_6
15. 15. Øygarden M., Felke P., Raddum H., Cid C. Cryptanalysis of the Multivariate Encryption Scheme EFLASH // Topics in Cryptology – CT-RSA 2020. Lecture Notes in Computer Science. 2020. V. 12006. P. 85-105.
16. Li W., Lu F., Zhao H. Power analysis attacks against QUAD // IAENG International Journal of Computer Science. 2019. V. 46. No. 1. P. 54–60.
17. Kr¨amer J., Loiero M. Fault attacks on UOV and Rainbow // Constructive Side-Channel Analysis and Secure Design. Proceedings of the International Workshop on Constructive Side-Channel Analysis and Secure Design. Darmstadt, Germany, 2019. P. 193–214.
18. Park A., Shim K., Koo N., Han D. Side-channel attacks on post-quantum signature schemes based on multivariate quadratic equations // IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018. V. 2018. No 3. P. 500–523.
19. Park A, Kyung-Ah Shim, Namhun Koo, Dong-Guk Han. Side-Channel Attacks on Post-Quantum Signature Schemes based on Multivariate Quadratic Equations: Rainbow and UOV // IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018. V. 2018. No. 3. P. 500–523. DOI:10.46586/tches.v2018.i3.500-523
20. Moldovyan N.A., Moldovyanu P.A. Vector Form of the Finite Fields GF(p^m) // Bulletin of Academy of Sciences of Moldova. Mathematics. 2009. No 3 (61). P. 57-63.