АЛГЕБРАИЧЕСКИЕ АЛГОРИТМЫ ЭЦП С ПОЛНОЙ РАНДОМИЗАЦИЕЙ ПОДПИСИ

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

DOI: 10.21681/2311-3456-2024-2-93-100

Цель работы: *устранение потенциального снижения стойкости алгоритмов ЭЦП на некоммутативных алгебрах с увеличением числа подписанных электронных документов.*

Метод исследования: *обеспечение полной рандомизации подписи путем включения в формулу генерации подгоночного элемента подписи случайного обратимого вектора как одного из множителей. Использование двух проверочных уравнений с вхождение одного и того же подгоночного элемента подписи. Формирование открытого ключа в виде набора векторов, вычисляемых в зависимости от векторов, содержащихся в скрытой (секретной) коммутативной группе конечной некоммутативной ассоциативной алгебры, используемой в качестве алгебраического носителя алгоритма ЭЦП.*

Результаты исследования: *показана ограниченность рандомизации подписи, приводящая к снижению стойкости при увеличении числа подписанных документов, в ранее предложенных алгебраических алгоритмах ЭЦП со скрытой группой, стойкость которых основана на вычислительной трудности решения большой системы степенных уравнений. Разработан способ обеспечения полной рандомизации подписи в алгебраических алгоритмах указанного типа. Показано, что результаты изучения строения конечных некоммутативных алгебр (с точки зрения декомпозиции на множество коммутативных подалгебр), используемых в качестве алгебраического носителя, имеют существенное значение как для выбора параметров разрабатываемого алгоритма ЭЦП, так и для оценки его стойкости. Разработан новый алгебраический алгоритм ЭЦП, представляющий интерес как практичная постквантовая криптосхема благодаря достаточно малым размерам открытого ключа и подписи.*

Научная и практическая значимость *результатов статьи состоит в разработке и апробации способа обеспечения полной рандомизации подписи и обоснования необходимости реализации последней в алгоритмах ЭЦП на некоммутативных ассоциативных алгебрах. Разработанный новый алгоритм ЭЦП является достаточно практичным и представляет интерес как прототип для разработки постквантовых алгоритмов ЭЦП, ориентированных на применение в условиях ограниченности доступных вычислительных ресурсов.*

Ключевые слова: *конечная некоммутативная алгебра; ассоциативная алгебра; вычислительно трудная задача; скрытая коммутативная группа; цифровая подпись; постквантовая криптография.*

ALGEBRAIC SIGNATURE ALGORITHMS WITH COMPLETE SIGNATURE RANDOMIZATION

Moldovyan A. A.[4], Moldovyan D. N.[5] and Kostina A. A.[6]

Purpose of work *is eliminating the potential decrease in the security of digital signature algorithms on non-commutative algebras with an increase in the number of signed electronic documents.*

Research methods *are i) ensuring complete randomization of the signature by including a random reversible vector as one of the multipliers in the formula for generating the fitting element of the signature; ii) using doubled verification equation; iii) formation of a public key in the form of a set of vectors calculated depending on the vectors*

1 Молдовян Александр Андреевич, доктор технических наук, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук. ORCID: https://orcid.org/0000-0001-5480-6016. Scopus Author ID: 6603413666. E-mail: maa1305@yandex.ru

2 Молдовян Дмитрий Николаевич, кандидат технических наук, научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 36634567300. E-mail: mdn.spectr@mail.ru

3 Костина Анна Александровна, научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук. ORCID: https://orcid.org/0009-0004-5784-7242. Scopus Author ID: 57218870628. E-mail: to.ann@inbox.ru

4 Alexander 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. ORCID: https://orcid.org/0000-0001-5480-6016. Scopus Author ID: 6603413666. E-mail: maa1305@yandex.ru

5 Dmitriy N. Moldovyan, Ph.D. (in Tech.) researcher of laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 36634567300. E-mail: mdn.spectr@mail.ru

6 Anna A. Kostina, researcher of laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: https://orcid.org/0009-0004-5784-7242. Scopus Author ID: 57218870628. E-mail: to.ann@inbox.ru

contained in the hidden (secret) commutative group of a finite non-commutative associative algebra used as an algebraic carrier of the digital signature algorithm.

***Results of the study**. Limited signature randomization, leading to a decrease in security with an increase in the number of signed documents, is shown for previously proposed algebraic digital signature algorithms with a hidden group, the security of which is based on the computational difficulty of solving a large system of power equations. A method has been developed to ensure complete randomization of the signature in algebraic algorithms of the said type. It is shown that the results of studying the structure of finite non-commutative algebras (from the point of view of decomposition into a set of commutative subalgebras) used as an algebraic carrier are essential both for the choice of parameters of the developed digital signature algorithm and for the estimating its stability. A new algebraic digital signature algorithm has been developed, which is of interest as a practical post-quantum crypto-scheme, due to the rather small sizes of the public key and signature.*

***Practical relevance:** The significance of the results of the article lies in the development and testing of a method for ensuring complete signature randomization and the justification of the need to implement the latter in digital signature algorithms on non-commutative associative algebras. The developed new digital signature algorithm is quite practical and is of interest as a prototype for the development of post-quantum digital signature algorithms, oriented for use in conditions of limited available computing resources.*

***Keywords:** finite non-commutative algebra; associative algebra; computationally difficult problem; hidden commutative group; digital signature; post-quantum cryptography.*

Введение

Разработке постквантовых криптографических алгоритмов с открытым ключом, включая алгоритмы электронной цифровой подписи (ЭЦП), мировое криптографическое сообщество уделяет значительное внимание [1, 2]. Стойкость постквантовых криптоалгоритмов должна базироваться на вычислительной трудности задач, отличных от задачи дискретного логарифмирования (ЗДЛ) и задачи факторизации (ЗФ), поскольку для ЗДЛ и ЗФ известны полиномиальные алгоритмы их решения на квантовом компьютере.

Известны постквантовые двухключевые алгоритмы на группах [3], кодах [4, 5], алгебраических решетках [6, 7], хеш-функциях [8], булевых функциях [9], трудно обратимых отображениях [10, 11] и некоммутативных алгебрах [12, 13]. Обращают на себя внимание алгоритмы, основанные на трудно обратимых нелинейных отображениях с секретной лазейкой. Алгоритмы такого типа разрабатываются и исследуются более 35 лет многочисленными исследователями из разных стран [14, 15]. Широкий интерес к ним связан с тем, что их стойкость базируется на вычислительной трудности решения систем многих степенных уравнений с многими неизвестными [16], т. е. на задаче, для решения которой квантовый компьютер не является эффективным. Последнее означает, что стойкость этих алгоритмов к атакам с использованием обычных компьютеров обеспечивает стойкость и к квантовым атакам.

Типичные алгоритмы ЭЦП на трудно обратимых отображениях, например, Rainbow [17], Oil and Vinegar [18] и др. обладают малым размером подписи, однако, им характерен существенный с практической точки зрения недостаток – чрезмерно большой размер открытого ключа. Недавно предложенная новая парадигма [19] разработки алгоритмов на отображениях потенциально позволяет достигнуть уменьшения размера открытого ключа в 10 раз и более, однако, конкретные постквантовые алгоритмы на основе концепции [19] на настоящий момент не были предложены.

Сочетание сравнительно малых размеров подписи и открытого ключа характерно для алгебраических алгоритмов со скрытой группой [12, 20], стойкость которых также основана на вычислительной сложности решения больших систем степенных уравнений.

Постановка цели исследования

Специфической особенностью алгебраических алгоритмов, предложенных в [12, 20], является формирование ЭЦП в виде пары значений $(e, \mathbf{S})$, где e – натуральное число, играющее роль рандомизирующего параметра, и $\mathbf{S}$ – вектор, играющий роль подгоночного элемента подписи и вычисляемый в зависимости от значения e. При этом в проверочное уравнение вектор $\mathbf{S}$ входит два или более раз, что предотвращает его использование также и в качестве подгоночного элемента в атаках типа фальсификация подписи (вычисление подписи без знания секретного ключа). Для вычисления требуемого значения $\mathbf{S}$ по секретному ключу предварительно в зависимости от e вычисляются целочисленные степени n и d, а затем сам вектор $\mathbf{S}$ по следующей формуле:

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{A}^{-1}, \qquad (1)$$

где векторы $\mathbf{A}$, $\mathbf{B}$, $\mathbf{G}$ и $\mathbf{H}$ являются элементами секретного ключа, причем $\mathbf{G}$ и $\mathbf{H}$ есть элементы скрытой

коммутативной группы. Благодаря механизму рандомизации подгоночный элемент каждой подписи связан с уникальным вектором, равным значению $\mathbf{G}^n\mathbf{H}^d$, однако, последний всегда принадлежит скрытой группе, порядок которой много меньше порядка конечной некоммутативной ассоциативной алгебры (КНАА), используемой в качестве алгебраического носителя алгоритма ЭЦП. Таким образом, последнее показывает, что в алгоритмах [12, 20] обеспечивается неполная рандомизация, т.е. подгоночный элемент $\mathbf{S}$ может пробегать только малую долю значений КНАА.

Это определяет актуальность рассмотрения 1) задачи об оценке вычислительной сложности потенциально возможной атаки, направленной на вычисление секретных значений $\mathbf{A}$ и $\mathbf{B}$ и некоторого представителя $\mathbf{J}$ скрытой группы, а также 2) задачи разработки способа обеспечения полной рандомизации в алгебраических алгоритмах, основанных на сложности решения большой системы степенных уравнений. Настоящая статья посвящена решению обозначенных двух задач, причем решение второй направлено на достижение цели устранения потенциального снижения стойкости с увеличением числа подписанных электронных документов.

1. Используемые алгебраические носители

Определение в конечном m-мерном векторном пространстве (например, заданным над простым конечным полем $GF(p)$ замкнутой операции умножения, являющейся дистрибутивной слева и справа относительно операции сложения, приводит к заданию конечной m-мерной алгебры. Операция умножения векторов $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ и $\mathbf{B} = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$, где $\mathbf{e}_i$ – формальные базисные векторы, может быть определена формулой:

$$\mathbf{AB} = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j (\mathbf{e}_i \mathbf{e}_j) \qquad (2)$$

где каждое из всевозможных произведений пар базисных векторов заменяется на некоторый однокомпонентный вектор $\lambda\mathbf{e}_k$ по правилу, задаваемому некоторой таблицей умножения базисных векторов (ТУБВ): произведение $(\mathbf{e}_i \mathbf{e}_j)$ заменяется на содержимое ячейки, находящейся на пересечение i-й строки и j-го столбца.

Легко заметить, что таким образом заданное умножение обладает свойствами замкнутости и двухсторонней дистрибутивности. В алгебраических алгоритмах ЭЦП со срытой группой используется операция возведения в степень большого размера, что требует использования алгоритма быстрого возведения в степень, который применим в случае ассоциативного умножения. Поэтому в таких алгоритмах в качестве алгебраического носителя используются конечные ассоциативные алгебры, в частности КНАА различных четных размерностей. Например, в случае алгоритмов [12, 20] используются КНАА размерностей $m = 4$ и $m = 6$.

Использование четырехмерных КНАА представляет интерес, благодаря тому, что 1) они могут быть заданы по прореженным ТУБВ, для которых в формуле (2) половина слагаемых равна нулю, что существенно уменьшает вычислительную сложность операции умножений, и 2) их строение с точки зрения декомпозиции на коммутативные подалгебры достаточно хорошо изучено и показана их общность строения независим от вида ТУБВ, по которой задано умножение [13, 20, 21]. Для дальнейшего важны следующие два общих свойства:

1. В четырехмерной КНАА содержатся $\approx p^2/2$ коммутативных подалгебр порядка p^2, мультипликативная группа Γ которых имеет порядок $(p - 1)^2$ и двухмерное циклическое строение (порождается базисом, включающим два вектора порядка $p - 1$).
2. Все элементы коммутативной алгебры, содержащей конкретную группу Γ, могут быть описаны как множество векторов $\mathbf{V}$, координаты которых вычисляются по координатам некоторого вектора $\mathbf{J}$, содержащегося в Γ и отличного от скалярного вектора, в зависимости от пары скалярных переменных $g,h \in GF(p)$. При этом каждая из четырех координат векторов $\mathbf{V}$ выражается многочленом первой степени от переменных g и k с фиксированными коэффициентами, зависящими от координат вектора $\mathbf{J}$.

С учетом свойства (2) выбор z неизвестных векторов из скрытой группы связан с $4 + 2(z - 1)$ скалярными неизвестными (четыре скалярных неизвестных задают неизвестный вектор $\mathbf{J}$, а каждый из оставшихся $z - 1$ неизвестных векторов описывается через координаты вектора $\mathbf{J}$ и две уникальные скалярные неизвестные).

2. Атака на основе известных подписей

В алгебраических алгоритмах ЭЦП [12, 20] подгоночный элемент $\mathbf{S}_i$ некоторой i-й подписи вычисляется по формуле (1). При этом по i-й подписи и уравнению верификации ЭЦП может быть вычислен вектор-фиксатор $\mathbf{R}_i$, генерируемый по случайно выбираемым натуральным значениям $k < p - 1$ и $t < p - 1$ по формуле

$$\mathbf{R} = \mathbf{F}\mathbf{G}^k\mathbf{H}^t\mathbf{F}^{-1}, \qquad (3)$$

где вектор $\mathbf{F}$ является элементом секретного ключа (в частном случае $\mathbf{F}$ равен секретному элементу $\mathbf{A}$ из формулы (1)). Это означает, что с каждой подлинной подписью связаны два векторных степенных

уравнения. С учетом возможности задания любого элемента из скрытой группы по координатам фиксированного ее представителя $\mathbf{J}$ и двух скалярных переменных $g,h \in GF(p)$ пара векторных уравнений (2) и (3) для каждой i-й подписи сводится к восьми скалярным степенным уравнениям с фиксированными неизвестными координатами векторов $\mathbf{A}$, $\mathbf{B}$ и $\mathbf{F}$ (12 скалярных неизвестных при $\mathbf{A} \neq \mathbf{F}$ и 8 скалярных неизвестных при $\mathbf{A} = \mathbf{F}$), четырьмя фиксированными неизвестными координатами вектора $\mathbf{J}$ и четырьмя уникальными скалярными неизвестными $g_{i\mathrm{S}}$, $h_{i\mathrm{S}}$ (задают выбор случайного элемента $\mathbf{G}^n\mathbf{H}^d$ из скрытой группы в формуле (1)) и $g_{i\mathrm{R}}$, $h_{i\mathrm{R}}$ (задают выбор случайного элемента $\mathbf{G}^k\mathbf{H}^t$ из скрытой группы в формуле (3)).

С учетом перечисленного для u подлинных подписей получаем систему из $24u$ скалярных уравнений с $16 + 4u$ (или $12 + 4u$) скалярными неизвестными при $\mathbf{A} \neq \mathbf{F}$ (при $\mathbf{A} = \mathbf{F}$). Из условия равенства числа уравнений и числа неизвестных

$$8u = 16 + 4u, \text{ (при } \mathbf{A} \neq \mathbf{F})$$
$$8u = 12 + 4u, \text{ (при } \mathbf{A} = \mathbf{F})$$

получаем следующее ожидаемое число подписей нужных для вычисления секретных векторов $\mathbf{A}$, $\mathbf{B}$ и $\mathbf{F}$ независимо от значений других элементов секретного ключа: $u = 4$ (при $\mathbf{A} = \mathbf{F}$) и $u = 3$ (при $\mathbf{A} = \mathbf{F}$). При этом в первом (во втором) случае решается система из 32 (24) степенных уравнений в поле $GF(p)$. Если задать независимое вычисление секретного вектора $\mathbf{F}$ по системе скалярных уравнений, составленных только по формуле (3), то аналогичным путем получим уравнение $4u = 8 + 2u$, из которого имеем значение $u = 4$, определяющее систему из 16 скалярных уравнений. Это существенно меньше числа скалярных уравнений в системах уравнений, полученных в [12, 20] по формулам, связывающим элементы секретного и открытого ключей.

Достаточно легко предложить модификацию алгоритмов [12, 20] с вычислением вектора фиксатора по формуле

$$\mathbf{R} = \mathbf{F}\mathbf{G}^k\mathbf{H}^t\mathbf{N}^{-1}, \quad (4)$$

в которой секретные векторы $\mathbf{F}$ и $\mathbf{N} \neq \mathbf{F}$ отличны от секретных векторов $\mathbf{A}$ и $\mathbf{B}$. Этом случае получим $u = 5$ и число совместно решаемых уравнений, равное 40. Однако вычисление неизвестных $\mathbf{F}$ и $\mathbf{N}$ можно отделить от вычисления неизвестных $\mathbf{A}$ и $\mathbf{B}$, т.е. составить систему уравнений только по формуле (6) или только по формуле (1). В обоих случаях это дает такое уравнение для вычисления значения u:

$$4u = 12 + 2u. \quad (5)$$

Из уравнения (5) получаем $u = 6$ и число совместно решаемых скалярных степенных уравнений, равное 24, что существенно меньше числа уравнений в системах, полученных в [12, 20] из формул, связывающих элементы секретного ключа с элементами открытого ключа.

Таким образом, для исходных алгоритмов [12, 20] и для предложенного способа их модификации выполнение независимого вычисления секретных векторов по известным подписям существенно снижают оценки стойкости, полученные в [12, 20]. Это означает, что неполная рандомизация подписи в алгоритмах [12, 20] приводит к снижению уровня ожидаемой стойкости, поэтому для устранения атак на основе известных подписей в первую очередь следует рассмотреть возможность такого модифицирования алгебраических алгоритмов со скрытой группой, при котором обеспечивается полная рандомизация подписи.

3. Способ задания полной рандомизации подписи в алгебраических алгоритмах, основанных на трудности решения больших систем уравнений

Обеспечение полной рандомизации можно связать с заданием формулы генерации подгоночного элемента подписи, включающей случайный обратимый вектор $\mathbf{V}$, выбираемый из случайных коммутативных подалгебр, т. е. принимающий значения из всей мультипликативной группы КНАА, используемой в качестве алгебраического носителя. Представляет интерес задание такой формулы в следующем виде:

$$\mathbf{S} = \mathbf{D}\mathbf{G}^n\mathbf{H}^d\mathbf{V}, \quad (6)$$

где $\mathbf{D}$ – секретный вектор (элемент секретного ключа). Из-за наличия случайного множителя $\mathbf{V}$, который в общем случае неперестановочен с векторами из скрытой группы становится необходимым отказаться от многократного вхождения подгоночного элемента подписи в уравнение верификации подписи. Это означает, что следует предложить другой механизм защиты от так типа подделка подписи по открытому ключу с использованием вектора $\mathbf{S}$ в качестве подгоночного параметра подделки. В качестве такого механизма предлагается использование удвоенного проверочного уравнения, т. е. задание двух проверочных уравнений сходного типа, в каждое из которых вектор $\mathbf{S}$ входит только один раз.

После анализа ряда вариантов задания удвоенного проверочного уравнения с учетом возможных атак по подделке ЭЦП была найдена следующая пара связанных проверочных уравнений:

$$\mathbf{R}_1' = \mathbf{Y}_1^{e'}\mathbf{T}_1\mathbf{Z}_1^{es}\mathbf{U}_1\mathbf{S}\mathbf{Q}^{h'h};$$
$$\mathbf{R}_2' = \mathbf{Y}_2^{e'\sigma}\mathbf{T}_2\mathbf{Z}_2^{e}\mathbf{U}_2\mathbf{S}\mathbf{Q}^{h'\|h}, \quad (7)$$

где $\mathbf{Q}$ – вектор, являющийся общим параметром (так же как и используемая КНАА); $\mathbf{Y}_1$, $\mathbf{T}_1$, $\mathbf{Z}_1$, $\mathbf{U}_1$, $\mathbf{Y}_2$, $\mathbf{T}_2$, $\mathbf{Z}_2$ и $\mathbf{U}_2$ – элементы открытого ключа, вычисляемые как замаскированные элементы скрытой группы (выбирается случайный элемент скрытой группы и умножается слева и справа на секретные векторы); e' и e –натуральные значения вычисляемые как значение хеш-функции $e'||e = H(\mathbf{M}, \mathbf{R}_1, \mathbf{R}_2)$ от подписываемого документа с присоединенными к нему векторами-фиксаторами $\mathbf{R}_1$, и $\mathbf{R}_2$, предварительно сгенерированными по формулам, аналогичным (6); h' и h – натуральные значения вычисляемые как значение хеш-функции от подписываемого докумета $h'||h = H(M)$. Заметим, что использование различных множителей $\mathbf{Q}^{h'h}$ и $\mathbf{Q}^{h'||h}$ в первом и втором проверочных уравнениях связано обеспечение повышенной защищенности к атакам типа фальсификация ЭЦП.

Предполагается, что процедура формирования ЭЦП должна начинаться с вычисления значения хеш-функции $h'||h = H(M)$, после чего генерируются случайные натуральные значения k_1, t_1, k_2, t_2 и случайный вектор $\mathbf{V}$ и вычисляются случайные векторы-фиксаторы $\mathbf{R}_1$, и $\mathbf{R}_2$ по следующим двум формулам:

$$\mathbf{R}_1 = \mathbf{A}\mathbf{G}^{k_1}\mathbf{H}^{t_1}\mathbf{V}\mathbf{Q}^{h'h};$$
$$\mathbf{R}_2 = \mathbf{F}\mathbf{G}^{k_2}\mathbf{H}^{t_2}\mathbf{V}\mathbf{Q}^{h'||h}, \quad (8)$$

где $\mathbf{A}$ и $\mathbf{F}$ – секретные векторы.

Подгоночным элементом подписи является вектор $\mathbf{S}$, вычисляемый в зависимости от рандомизирующего элемента подписи $e'||e$ по формуле (7). Этот элемент связан с уникальным для каждой подписи значением $\mathbf{V}$, тем не менее накопление подписей с ростом числа подписанных документов должно дать принципиальную возможность вычисления секретных векторов $\mathbf{A}$ и $\mathbf{D}$, а также некоторого представителя $\mathbf{J}$ скрытой группы. Однако, благодаря заданию полной рандомизации подписи, можно ожидать, что вычислительная сложность этой задачи окажется выше, чем совместное вычисление элементов секретного ключа по большой системе степенных уравнений, составленных из формул, связывающих элементы открытого ключа с элементами секретного ключа. Если это окажется так, то предлагаемый механизм рандомизации достиг поставленной цели обеспечения высокого уровня защищенности от атак, использующих известные подписи, независимо от числа подписанных документов.

Дадим оценку числа подписей, при котором число уравнений, составленных по формулам (6) и (8), равно числу неизвестных, для случая использования четырехмерной КНАА в качестве алгебраического носителя криптосхемы. Заметим, что векторы $\mathbf{R}_1$ и $\mathbf{R}_2$, уникальные для каждой подписи, вычисляются из удвоенного проверочного уравнения, а множители $\mathbf{Q}^{h'h}$ и $\mathbf{Q}^{h}$ – по значению хеш-фукции от подписанного документа.

С каждой подлинной подписью связаны 12 скалярных уравнений с 16-ю фиксированными скалярными неизвестными (ими являются координаты секретных векторов $\mathbf{A}$, $\mathbf{D}$, $\mathbf{F}$ и некоторого представителя $\mathbf{J}$ скрытой группы) и с 10-ю уникальными неизвестными (ими являются координаты вектора $\mathbf{V}$ и три пары значений $g,h \in GF(p)$, задающих неизвестные векторы $\mathbf{G}^n\mathbf{H}^d$, $\mathbf{G}^{k_1}\mathbf{H}^{t_1}$ и $\mathbf{G}^{k_2}\mathbf{H}^{t_2}$, содержащиеся в скрытой группе, фиксированной вектором $\mathbf{J}$). Для u известных подписей получаем систему из $12u$ скалярных уравнений с 16 +$10u$ неизвестными, т. е. имеем уравнение

$$12u = 16 + 10u. \quad (9)$$

Из (9) получаем $u = 8$ и число уравнений в системе степенных уравнений, равное 96. При этом легко показать, что полная рандомизация подписи делает неэффективным раздельное (от вычисления вектора $\mathbf{D}$) вычисление секретных векторов $\mathbf{A}$ и $\mathbf{F}$, т. е. это не приводит к уменьшению числа совместно решаемых уравнений, при котором могут быть вычислены координаты части неизвестных секретных векторов. Полученную оценку можно считать общей для алгоритмов, построенных с использованием рассмотренного способа полной рандомизации подписи. Для сравнения с оценкой числа уравнений в системах, полученных по формулам, связывающим элементы секретного и открытого ключей, требуется рассмотрение конкретного алгебраического алгоритма, построенного с использованием предложенного способа рандомизации.

4. Алгоритм на основе предложенного способа полной рандомизации ЭЦП

В качестве алгебраического носителя будем использовать одну из известных четырехмерных КНАА, заданных над полем $GF(p)$, где простое $p = 2q + 1$ при 128-битном простом q, по прореженным ТУБВ, описанным, например, в работах [12, 13, 20, 21]. Можно ожидать, что использование КНАА с размерностями $m \geq 6$ может обеспечить более высокий уровень стойкости, однако, обоснование стойкости для этого случая потребует знание строения таких алгебр, которое на данный момент известно детально только для случая $m = 4$.

Будем полагать, что используемый алгебраический носитель и некоторый вектор $\mathbf{Q}$ порядка $p^2 - 1$ (можно показать, что векторов такого порядка существует в количестве $\approx p^4/4$) являются общими параметрами для всех пользователей схемы ЭЦП. Открытый ключ формируется в виде набора из 8 векторов $\mathbf{Y}_1$, $\mathbf{T}_1$, $\mathbf{Z}_1$, $\mathbf{U}_1$, $\mathbf{Y}_2$, $\mathbf{T}_2$, $\mathbf{Z}_2$ и $\mathbf{U}_2$ (с суммарным размером ≈ 512 байт) по следующему алгоритму:

1. Сгенерировать базис <**G**,**H**> (порядок каждого из векторов **G** и **H** равен q) скрытой группы порядка q^2, обладающей двухмерной цикличностью, для чего, например, можно воспользоваться алгоритмом из статьи [20].
2. Сгенерировать случайные обратимые векторы **A**, **B**, **F**, **N**, и **D**, принадлежащие разным коммутативным подалгебрам, отличным от подалгебры, содержащей скрытую группу.
3. Сгенерировать случайные натуральные числа $x < q$ и $w < q$ и вычислить векторы:

$$\mathbf{Y}_1 = \mathbf{AGHA}^{-1};\ \mathbf{Z}_1 = \mathbf{BH}^w\mathbf{B}^{-1};$$
$$\mathbf{T}_1 = \mathbf{AG}^3\mathbf{H}^5\mathbf{B}^{-1};\ \mathbf{U}_1 = \mathbf{BG}^5\mathbf{H}^3\mathbf{D}^{-1}; \quad (10)$$

$$\mathbf{Y}_2 = \mathbf{FG}^x\mathbf{F}^{-1};\ \mathbf{Z}_2 = \mathbf{NG}^2\mathbf{H}^7\mathbf{N}^{-1};$$
$$\mathbf{T}_2 = \mathbf{FG}^4\mathbf{H}^3\mathbf{N}^{-1} \text{ и } \mathbf{U}_2 = \mathbf{NG}^3\mathbf{H}^4\mathbf{D}^{-1}. \quad (11)$$

Числа x и w и векторы **A**, **B**, **D**, **F**, **G**, **H** и **N** являются элементами секретного ключа, имеющего общий размер ≈480 байт.

Алгоритм генерации ЭЦП использует некоторую специфицированную 256-битную хеш-функцию H и включает следующие шаги:

1. Вычислить хеш-значение от подписываемого документа M: $h'||h = H(M)$, где 256-битное хеш-значение представлено в виде конкатенации двух 128-битных натуральных чисел h' и h.
2. Сгенерировать случайные натуральные числа k_1, t_1, k_2, t_2 (не превосходящие числа q – 1) и случайный вектор **V**. Затем вычислить значения векторов-фиксаторов $\mathbf{R}_1$ и $\mathbf{R}_2$ по формулам (8).
3. Вычислить хеш-значение от документа M с присоединенными к нему векторами-фиксаторами $e'||e = H(M, \mathbf{R}_1, \mathbf{R}_2)$, где 256-битное хеш-значение представлено в виде конкатенации двух 128-битных натуральных чисел e' и e.
4. Вычислить степень n: $n = k_1 - e' - 8 \bmod q$.
5. Вычислить степень d: $d = t_2 - 7e - 7 \bmod q$.
6. Вычислить подгоночный элемент ЭЦП **S** по формуле (6).
7. Вычислить значение первого вспомогательного подгоночного элемента ЭЦП по формуле $s = w^{-1}e^{-1}(t_1 - t_2 - e' + 7e - 1) \bmod q$.
8. Вычислить значение второго вспомогательного подгоночного элемента ЭЦП по формуле $\sigma = x^{-1}e'^{-1}(k_2 - k_1 - 2e + e' + 1) \bmod q$.

Подписью к документу M является набор значений (e', e, s, σ, **S**) с общим размером ≈128 байт. Вычислительную сложность процедуры генерации ЭЦП можно приближенно оценить как 6 операций возведения в 128-битную степень в КНАА, используемой в качестве алгебраического носителя, и 2 операции возведения в 256-битную степень, что потребует выполнения ≈15400 операций умножения по модулю p.

Алгоритм верификации ЭЦП (e', e, s, σ, **S**) к документу M выполняется по открытому ключу и включает следующие шаги:

1. Вычислить хеш-значение от документа M: $h'||h = H(M)$.
2. Вычислить значения векторов $\mathbf{R}'_1$ и $\mathbf{R}'_2$ по формулам (7).
3. Вычислить хеш-значение от документа M с присоединенными к нему векторами $\mathbf{R}'_1$ и $\mathbf{R}'_2$: $\varepsilon'||\varepsilon = H(M, \mathbf{R}'_1, \mathbf{R}'_2)$, где 256-битное хеш-значение представлено в виде конкатенации двух 128-битных натуральных чисел ε' и ε.
4. Если одновременно выполняются равенства $\varepsilon' = e'$ и $\varepsilon = e$, то подпись принимается как подлинная, иначе подпись отвергается как ложная.

Вычислительную сложность процедуры проверки подлинности подписи можно приближенно оценить как 4 операции возведения в 128-битную степень в КНАА, используемой в качестве алгебраического носителя, и 2 операции возведения в 256-битную степень, что потребует выполнения ≈12300 операций умножения по модулю p. Корректность работы алгоритма ЭЦП означает, что корректно вычисленная подпись (e', e, s, σ, **S**) к документу M проходит процедуру верификации как подлинная ЭЦП.

Для доказательства корректности предложенного алгоритма ЭЦП вычисляем вектор $\mathbf{R}'_1$:

$$\mathbf{R}'_1 = (\mathbf{AGHA}^{-1})^{e'}\ \mathbf{AG}^3\mathbf{H}^5\mathbf{B}^{-1}\ (\mathbf{BH}^w\mathbf{B}^{-1})^{es} \times$$
$$\times\ \mathbf{BG}^5\mathbf{H}^3\mathbf{D}^{-1}\ (\mathbf{DG}^n\mathbf{H}^d\mathbf{V})\ \mathbf{Q}^{h'h} =$$
$$= \mathbf{AG}^{e' + n + 8}\mathbf{H}^{e' + xes + d + 8})\ \mathbf{VQ}^{h'h} = \mathbf{AG}^{e' + (k_1 - e' - 8) + 8} \times$$
$$\times\ \mathbf{H}^{e' + xe(x^{-1}e^{-1}\ (t_1 - t_2 - e' + 7e^{-1})) + d + 8}\ \mathbf{VQ}^{h'h} = \mathbf{AG}^{k_1}\ \mathbf{H}^{t_1}\ \mathbf{VQ}^{h'h} = \mathbf{R}_1;$$

Затем вычисляем вектор $\mathbf{R}'_2$ и значение $\varepsilon'||\varepsilon = H(M, \mathbf{R}'_1, \mathbf{R}'_2)$ и выполняем сравнение $\varepsilon'||\varepsilon$ со значением $e'||e = H(M, \mathbf{R}_1, \mathbf{R}_2)$:

$$\mathbf{R}'_2 = (\mathbf{FG}^x\mathbf{F}^{-1})^{e'\sigma}\ \mathbf{FG}^4\mathbf{H}^3\mathbf{N}^{-1}\ (\mathbf{NG}^2\mathbf{H}^7\mathbf{N}^{-1})^e \times$$
$$\times\ \mathbf{NG}^3\mathbf{H}^4\mathbf{D}^{-1}\ (\mathbf{DG}^n\mathbf{H}^d\mathbf{V})\ \mathbf{Q}^{h'h} =$$
$$= \mathbf{FG}^{xe'\sigma + 4 + 2e + 3 + n}\ \mathbf{H}^{3 + 7e + 4 + d}\ \mathbf{VQ}^{h'h} =$$
$$= \mathbf{AG}^{(k_2 - k_1 - 2e + e' + 1) + 4 + 2e + 3 + k_1 - e' - 8}\ \mathbf{H}^{3 + 7e + 4 + t_2 - 7e - 7}\ \mathbf{VQ}^{h'h} =$$
$$= \mathbf{FG}^{k_2}\mathbf{H}^{t_2}\mathbf{VQ}^{h'h} = \mathbf{R}_2;$$
$$\{\mathbf{R}'_1 = \mathbf{R}_1;\ \mathbf{R}'_2 = \mathbf{R}_2\} \Rightarrow \{\varepsilon' = e';\ \varepsilon = e\}.$$

Два последних равенства доказывают корректность разработанного алгоритма.

4. Обсуждение

В предложенном в разделе 3 алгоритме ЭЦП обеспечивается полная рандомизация подписи по способу, описанному в разделе 2. Этот способ существенно повышает сложность независимого вычисления отдельных секретных векторов (для рассматриваемого алгоритма это векторы **A**, **D** и **F**) при выполнении атаки на основе известных подлинных подписей, а именно, для успешного выполнения указанной атаки требуется решить систему

из 96 степенных уравнений с 96 неизвестными, заданную в поле $GF(p)$. Все секретные векторы, входящие в состав секретного ключа, могут быть вычислены из системы уравнений, составленной по формулам (10) и (11), связывающим элементы секретного ключа с элементами открытого ключа, и дополненной условием перестановочности неизвестных векторов, относящихся к скрытой группе. Обозначая неизвестные векторы из скрытой группы как $\mathbf{J}_0, \mathbf{J}_1, \ldots \mathbf{J}_7$, из формул (10) и (11) получаем следующую систему из 15 квадратных векторных уравнений:

$$\begin{cases} \mathbf{Y}_1\mathbf{A} = \mathbf{A}\mathbf{J}_0;\ \mathbf{Z}_1\mathbf{B} = \mathbf{B}\mathbf{J}_1;\ \mathbf{T}_1\mathbf{A} = \mathbf{B}\mathbf{J}_2;\ \mathbf{U}_1\mathbf{D} = \mathbf{B}\mathbf{J}_3; \\ \mathbf{Y}_2\mathbf{F} = \mathbf{F}\mathbf{J}_4;\ \mathbf{Z}_2\mathbf{N} = \mathbf{N}\mathbf{J}_5;\ \mathbf{T}_2\mathbf{N} = \mathbf{F}\mathbf{J}_6;\ \mathbf{U}_2\mathbf{D} = \mathbf{N}\mathbf{J}_7; \\ \mathbf{J}_0\mathbf{J}_1 = \mathbf{J}_1\mathbf{J}_0;\ \mathbf{J}_0\mathbf{J}_2 = \mathbf{J}_2\mathbf{J}_0;\ \mathbf{J}_0\mathbf{J}_3 = \mathbf{J}_3\mathbf{J}_0;\ \mathbf{J}_0\mathbf{J}_4 = \mathbf{J}_4\mathbf{J}_0; \\ \mathbf{J}_0\mathbf{J}_5 = \mathbf{J}_5\mathbf{J}_0;\ \mathbf{J}_0\mathbf{J}_6 = \mathbf{J}_6\mathbf{J}_0;\ \mathbf{J}_0\mathbf{J}_6 = \mathbf{J}_6\mathbf{J}_0 \end{cases} \quad (12)$$

где $\mathbf{J}_0 = \mathbf{GH}$; $\mathbf{J}_1 = \mathbf{H}^w$, $\mathbf{J}_2 = \mathbf{G}^3\mathbf{H}^5$; $\mathbf{J}_3 = \mathbf{G}^5\mathbf{H}^3$; $\mathbf{J}_4 = \mathbf{G}^x$; $\mathbf{J}_5 = \mathbf{G}^2\mathbf{H}^7$; $\mathbf{J}_6 = \mathbf{G}^4\mathbf{H}^3$; $\mathbf{J}_7 = \mathbf{G}^3\mathbf{H}^4$.

Заметим, что в этой системе последние 7 уравнений задают условие принадлежности неизвестных $\mathbf{J}_0, \mathbf{J}_1, \ldots \mathbf{J}_7$ одной и той же коммутативной подалгебре, содержащейся в КНАА, используемой в качестве алгебраического носителя. Поэтому при сведении системы (12) к системе скалярных степенных уравнений вектор $\mathbf{J}_0$ задаст 4 скалярных неизвестных, а каждый из векторов $\mathbf{J}_1, \mathbf{J}_2, \ldots \mathbf{J}_7$ задаст 2 скалярные неизвестные (поскольку его координаты выражаются через координаты вектора $\mathbf{J}_0$ и две переменные $g,h \in GF(p)$ [12, 13, 21]). При таком представлении неизвестных векторов $\mathbf{J}_1, \mathbf{J}_2, \ldots \mathbf{J}_7$ последние 7 векторных уравнений в системе (12) автоматически выполняются, т. е. их можно исключить, сводя систему (12) к системе из первых восьми уравнений. Последняя сводится к системе из 32 скалярных степенных уравнений с 38 скалярными неизвестными (24 скалярных неизвестных – это координаты векторов $\mathbf{A}$, $\mathbf{B}$, $\mathbf{F}$, $\mathbf{N}$, $\mathbf{D}$ и $\mathbf{J}$ и 14 скалярных неизвестных относятся к семи различным парам переменных $g,h \in GF(p)$.

Тот факт, что число скалярных неизвестных превышает число уравнений, показывает существование множества эквивалентных ключей, однако нахождение хотя бы одного из них связано с нахождением одного из решений системы (12). В целом вычислительную сложность прямой атаки, т. е. атаки, связанной с нахождением секретного ключа по открытому, можно оценить как сложность решения системы из 32 скалярных уравнений с 32 неизвестными в поле $GF(p)$ (шести скалярным неизвестным можно задать заранее фиксированные значения, а затем приступить к нахождению остальных неизвестных).

Учитывая, что атака с использованием известных подписей связана с решением системы из 96 уравнений с 96 неизвестными, можно сделать вывод, что предложенный способ рандомизации подписи достигает заявленную в статье цель.

Выводы

Показаны слабости механизма ограниченной рандомизации подписи, использованного в алгебраических алгоритмах со скрытой группой [12, 20], и предложен способ обеспечения полной рандомизации, реализованный в разработанном новом алгебраическом алгоритме ЭЦП, основанном на вычислительной сложности решения большой системы степенных уравнений в поле $GF(p)$ с 129-битной характеристикой p. Благодаря тому, что квантовый компьютер не эффективен для решения систем степенных уравнений, предложенный алгоритм представляет интерес как практичная постквантовая схема ЭЦП с достаточно малыми размерами подписи и открытого ключа. Разработанная схема подписи может быть реализована на КНАА размерности $m \geq 6$, что потенциально приведет к увеличению стойкости за счет увеличения размера системы степенных скалярных уравнений, связывающих открытый и секретный ключи. Однако, детальное рассмотрение этого вопроса, видимо, требует изучения строения таких КНАА, что представляет самостоятельную задачу.

Исследование выполнено за счет гранта Российского научного фонда № 24-21-00225, https://rscf.ru/project/24-21-00225/

Литература

1. *Post-Quantum Cryptography. 13th International Conference, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings // Lecture Notes in Computer Science. 2022. V. 13512. Springer, Cham.*
2. *Post-Quantum Cryptography. 14th International Conference, PQCrypto 2023, College Park, MD, USA, August 16–18, 2023, Proceedings // Lecture Notes in Computer Science. 2023. V. 14154. Springer, Cham.*
3. *Battarbee C., Kahrobaei D., Perret L., Shahandashti S. F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures // In: Johansson, T., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2023 / Lecture Notes in Computer Science, 2023. V. 14154. P. 113–138. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_5*
4. *Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. A code-based group signature scheme // Designs, Codes and Cryptography. 2017. V. 82. N. 1-2. P. 469–493. DOI: 10.1007/s10623-016-0276-6.*
5. *Kosolapov Y. V., Turchenko O. Y. On the construction of a semantically secure modification of the McEliece cryptosystem // Прикладная дискретная математика. 2019. № 45. С. 33–43. DOI: 10.17223/20710410/45/4.*

6. *Gärtner J. NTWE: A Natural Combination of NTRU and LWE // In: Johansson, T., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2023 / Lecture Notes in Computer Science, 2023, vol 14154, pp. 321–353. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_12*
7. *Lysakov I. V.. Solving some cryptanalytic problems for lattice-based cryptosystems with quantum annealing method // Математические вопросы криптографии, 2023. Т.14. Вып. 2. С. 111–122 DOI: 10.4213/mvk441*
8. *Hamlin B., Song F. Quantum Security of Hash Functions and Property-Preservation of Iterated Hashing // In: Ding, J., Steinwandt, R. (eds) Post-Quantum Cryptography. PQCrypto 2019 / Lecture Notes in Computer Science. 2019. V. 11505. P. 329–349. Springer, Cham. https://doi.org/10.1007/978-3-030-25510-7_18.*
9. *Agibalov G. P. ElGamal cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 42. P. 57–65. DOI: 10.17223/20710410/42/4.*
10. *Ding J., Petzoldt A., Schmidt D. S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_2*
11. *Shuaiting Q., Wenbao H., Yifa Li, Luyao J. Construction of Extended Multivariate Public Key Cryptosystems // International Journal of Network Security. 2016. V. 18. N. 1. P. 60–67.*
12. *Молдовян Д. Н., Молдовян А. А., Молдовян Н. А. Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // Вопросы кибербезопасности. 2022. № 1(47). С. 18–25. DOI: 10.21681/2311-3456-2022-1-18-25.*
13. *Moldovyan D. N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. Vol. 29. N.2(86). P. 206–226.*
14. *Ding J., Petzoldt A., Schmidt D. S. The Matsumoto-Imai Cryptosystem // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. P. 25–60. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_3*
15. *Ding J.,Petzoldt A. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. V. 15. N. 4. P. 28–36.*
16. *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*
17. *Cartor R., Cartor M., Lewis M., Smith-Tone D. IPRainbow // In: Cheon, J. H., Johansson, T. (eds) Post-Quantum Cryptography // Lecture Notes in Computer Science. 2022. V. 13512. P. 170–184. Springer, Cham. https://doi.org/10.1007/978-3-031-17234-2_9*
18. *Ding, J., Petzoldt, A., Schmidt, D. S. Oil and Vinegar // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. P. 89–151. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_5*
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. *Молдовян Д. Н., Молдовян А. А. Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2(48). С. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.*
21. *Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022. V. 30. N. 1. P. 133–140. https://doi.org/10.56415/qrs.v30.11*