СПОСОБ УСИЛЕНИЯ РАНДОМИЗАЦИИ ПОДПИСИ В АЛГОРИТМАХ ЭЦП НА НЕКОММУТАТИВНЫХ АЛГЕБРАХ

Молдовян Д. Н.[1], Костина А. А.[2]

DOI: 10.21681/2311-3456-2024-4-71-81

Цель работы: *устранение уязвимости известных алгебраических алгоритмов ЭЦП с многократным вхождением подписи в проверочное уравнение к потенциальным атакам с использованием множества известных подписей.*

Метод исследования: *известные результаты по изучению строения четырехмерных конечных некоммутативных ассоциативных алгебр применяются для генерации параметров алгоритма ЭЦП. Устранение указанной в цели работы уязвимости реализуется путем усиления рандомизации подписи. Последняя обеспечивается за счет вычисления ЭЦП в зависимости от двух уникальных четырехмерных векторов, принадлежащим двум различным скрытым коммутативным группам четырехмерной некоммутативной алгебры, используемой в качестве алгебраического носителя. выполнение формального доказательства обеспечения почти полной рандомизации ЭЦП.*

Результаты исследования: *доказан ряд математических утверждений, лежащих в основе обоснования выбора параметров алгебраических алгоритмов ЭЦП, стойкость которых основана на вычислительной трудности решения больших систем степенных уравнений. Показано, что вычисление подписи в зависимости от двух уникальных векторов, выбираемых из различных коммутативных подалгебр, обеспечивает почти полную рандомизацию подписи, которая устраняет потенциальные атаки с использованием нескольких известных подписей, по отношению к которым являются уязвимыми известные алгебраические алгоритмы ЭЦП с многократным вхождением подписи в проверочное уравнение. На основе предложенного способа усиления рандомизации разработан алгебраический алгоритм ЭЦП, использующий в качестве алгебраического носителя четырехмерные конечные некоммутативные ассоциативные алгебры. В отличии от известных версий алгоритмов ЭЦП со скрытой группой и удвоенным проверочным уравнением используются две скрытые группы. Дана оценка стойкости к прямой атаке и к подделке подписи.*

Научная и практическая значимость *результатов статьи состоит в разработке и апробации способа усиления рандомизации подписи, перспективного для реализации на его основе практичных постквантовых алгоритмов ЭЦП, стойкость которых определяется вычислительной трудностью решения больших систем степенных уравнений. Предложен конкретный алгоритм такого типа, обладающий сравнительно малыми размерами подписи и открытого и секретного ключей.*

Ключевые слова: *конечная ассоциативная алгебра; некоммутативная алгебра; вычислительно трудная задача; скрытая группа; цифровая подпись; рандомизация цифровой подписи; постквантовая криптография*

A METHOD FOR STRENGTHENING SIGNATURE RANDOMIZATION IN SIGNATURE ALGORITHMS ON NON-COMMUTATIVE ALGEBRAS

Moldovyan D. N.[3], Kostina A. A.[4]

Purpose of work *is eliminating the vulnerability of well-known algebraic signature algorithms with multiple entry of the signature into the verification equation to potential attacks using a variety of well-known signatures.*

Research methods: *known results on the study of the structure of four-dimensional finite non-commutative associative algebras are used to generate parameters of the signature algorithm. The elimination of the said vulnerability is implemented*

1 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

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

3 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

4 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

by strengthening the randomization of the signature. The latter is provided by calculating the digital signature depending on two unique four-dimensional vectors belonging to two different hidden commutative groups of a four-dimensional non-commutative algebra used as an algebraic support. performing a formal proof of ensuring almost complete randomization of the EDS.

Results of the study: *a number of mathematical statements underlying the justification of the choice of parameters of algebraic signature algorithms, the security of which is based on the computational difficulty of solving large systems of power equations, are proved. It is shown that the calculation of the signature depending on two unique vectors selected from various commutative subalgebras provides almost complete randomization of the signature, which eliminates potential attacks using several known signatures, against which well-known algebraic algorithms of EDS with multiple entry of the signature into the verification equation are vulnerable. Based on the proposed method of randomization enhancement, an algebraic signature algorithm has been developed using four-dimensional finite non-commutative associative algebras as an algebraic support. Unlike the known versions of the signature algorithms with a hidden group and a doubled verification equation, two different hidden groups are used. The assessment of the security to the direct attack and to forging signature attack is given.*

Practical relevance: *the significance of the results of the article consists in the development of a method for enhancing signature randomization, which is attractive for the implementation of practical post-quantum signature algorithms based on it, the security of which being determined by the computational difficulty of solving large systems of power equations. A specific algorithm of this type is proposed, which has relatively small sizes of the signature and of the public and secret keys.*

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

Введение

Одной из актуальных проблем в области криптографии является разработка практичных постквантовых криптосхем с открытым ключом, в том числе алгоритмов электронной цифровой подписи (ЭЦП) [1, 2]. При построении постквантовых криптосхем должны быть использованы вычислительно сложные задачи, отличные от задач дискретного логарифмирования (ЗДЛ) и факторизации (ЗФ), для решения которых на квантовом компьютере известны полиномиальные алгоритмы[5]. Например, предложены постквантовые двухключевые криптосхемы на группах [3], алгебраических решетках [4], кодах [5], хеш-функциях [6], трудно обратимых отображениях с секретной лазейкой [7, 8] и некоммутативных алгебрах [9, 10].

Стойкость алгоритмов на трудно обратимых нелинейных отображениях основана на вычислительной сложности решения систем многих степенных уравнений (в частности, квадратных и кубических) с многими неизвестными, заданных в конечных полях сравнительно малого порядка [11, 12]. Применение квантового вычислителя для решения этой задачи не дает преимуществ по сравнению с использованием обычных компьютеров, что определяет интерес к ней как к постквантовому примитиву криптоалгоритмов с открытым ключом, в том числе алгоритмов ЭЦП. Последние обладают малым размером подписи и достаточно высокой производительностью при аппаратной и программной реализации, однако их существенным недостатком является чрезвычайно большой размер открытого ключа [13, 14]. Для устранения данного недостатка недавно предложена концепция задания трудно обратимого отображения как операции экспоненцирования в векторных конечных полях [15, 16]. Однако на настоящий момент не предложены конкретные алгоритмы ЭЦП, построенные в рамках этой концепции.

В статьях [17, 18] рассматривается подход к построению алгебраических алгоритмов ЭЦП со скрытой группой, стойкость которых базируется на трудности решения больших систем степенных уравнений в конечных полях, порядок которых имеет достаточно большой размер. Этот подход обеспечивает построение алгоритмов с малым размером подписи и открытого ключа, что делает его перспективным для разработки практичных постквантовых алгоритмов ЭЦП.

Формализация цели исследования

Общей особенностью алгоритмов ЭЦП со скрытой группой, разработанных в рамках парадигмы [17, 18] является использование проверочного уравнения с многократным вхождением подгоночного элемента подписи, представляющего собой некоторый вектор $\mathbf{S}$, вычисляемый в зависимости от рандомизирующего элемента подписи, представляющего собой натуральные число, вычисляемое в зависимости от случайных натуральных чисел, подписываемого документа и секретного ключа. В некоторых алгоритмах такого типа [19, 20] используются несколько рандомизирующих элементов подписи, но их конкатенация может быть рассмотрена как единый рандомизирующий элемент в виде натурального числа e. В статье [21] показано, что многократное вхождение элемента подписи $\mathbf{S}$ в качестве множителя уравнения проверки подлинности ЭЦП требует вычисления

5 Yan S. Y. Quantum Computational Number Theory. – Springer. 2015. – 252 p.

значения $\mathbf{S}$ по формуле $\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{A}^{-1}$ при фиксированных секретных векторных значениях $\mathbf{A}$, $\mathbf{B}$, $\mathbf{G}$ и $\mathbf{H}$, где $\mathbf{G}$ и $\mathbf{H}$ образуют базис скрытой коммутативной группы, и уникальных натуральных значениях n и d. Последние задают рандомизацию вектора $(\mathbf{G}^{n}\mathbf{H}^{d})$, который имеет уникальное значение для каждой вычисляемой подписи. Однако, число различных значений $(\mathbf{G}^{n}\mathbf{H}^{d})$ ограничено порядком скрытой группы, которая существенно меньше порядка мультипликативной группы алгебры, используемой в качестве алгебраического носителя. Это задает неустранимую неполноту рандомизации подписи в алгоритмах [17–20], которая, как показано в [21], приводит к снижению ожидаемого уровня стойкости.

Для устранения неполноты рандомизации в работе [21] предложен способ обеспечения полной рандомизации подписи в алгоритмах ЭЦП, стойкость которых основана на вычислительной сложности решения больших систем степенных уравнений. В способе [21] используется прием удвоения проверочного уравнений, вычисление подгоночного элемента подписи по формуле $\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{V}$, где $\mathbf{V}$ – случайный обратимый вектор. Последняя формула обеспечивает достаточную полноту рандомизации, однако для обеспечения стойкости к подделке подписи на основе известной подписи и использования вектора $\mathbf{S}$ в качестве подгоночного параметра атаки в каждом из двух проверочных уравнений используются два разных множителя, вычисляемые как различные 256-битные степени некоторого известного вектора $\mathbf{J}$. Такие же множители используются в процедуре генерации ЭЦП. Необходимость выполнения дополнительных операций экспоненцирования приводит к снижению производительности процедуры генерации (верификации) ЭЦП на 50% (40%).

В данной статье решается задача повышения производительности алгоритма ЭЦП с полной рандомизацией подписи путем разработки и использования нового способа обеспечения усиленной рандомизации подписи и векторных хеш-функций.

1. Свойства используемых алгебраических носителей

В разрабатываемой схеме ЭЦП в качестве алгебраического носителя предполагается использование конечных некоммутативных ассоциативных алгебр (КНАА) размерности $m \geq 4$, заданных над простым конечным полем $GF(p)$ по так называемым таблицам умножения базисных векторов (ТУБВ), с помощью которых определяется операция векторного умножения (умножение всевозможных пар векторов, результатом которого является вектор). Определение последней детально представлено в [21]. Вектор $\mathbf{V}$ будем обозначать в виде упорядоченного набора его координат (элементов поля $GF(p)$): $\mathbf{V} = (v_0, v_1, v_2, v_3)$.

Известны различные типы КНАА, например, включающие большое множество глобальных левосторонних [22] или большое множество глобальных правосторонних единиц [22, 23]. Далее будут рассматриваться КНАА, включающие глобальную двухстороннюю единицу, которая является единственной, хотя она может иметь достаточно разнообразный вид, определяемый ТУБВ, по которой задается операция векторного умножения. Известен способ унифицированного задания КНАА с глобальной двухсторонней единицей произвольных четных размерностей $m \geq 6$ [24]. Задание разнообразных четырехмерных КНАА с глобальной двухсторонней единицей представлено в работах [24, 25].

Для построения схемы ЭЦП и оценки ее стойкости важным является знание строения КНАА как декомпозиции на множество коммутативных подалгебр. В настоящее время строение КНАА достаточно хорошо изучено для случая размерности $m = 4$ [26, 27]. В связи с этим в разрабатываемом далее алгоритме ЭЦП в качестве его носителя предполагается использование четырехмерной КНАА с глобальной двухсторонней единицей. Исследования показали, что все такие КНАА имеют одинаковое строение, независимо от вида ТУБВ, по которой они задаются. Поэтому для использования в качестве алгебраического носителя предпочтительным является случай задания таких алгебр по прореженным ТУБВ, представленным, например, в [26, 27]. Этот выбор определяется тем, что для такого случая выполнение одной операции умножения векторов сводится к осуществлению всего 8 операций умножения в поле $GF(p)$, тогда как при использовании обычной ТУБВ потребуется выполнить 16 операций умножения в поле.

Результаты исследования строения различных четырехмерных КНАА с глобальной двухсторонней единицей [26–28] обобщаются следующим образом:

1. Множество четырехмерных векторов как элементов КНАА разбивается на $\eta = p^2 + p + 1$ коммутативных подалгебр порядка p^2, которые пересекаются строго в множестве скалярных векторов $\mathbf{L} = \alpha\mathbf{E}$, где $\mathbf{E}$ – единичный вектор (глобальная двухсторонняя единица) и $\alpha \in GF(p)$. Эти подалгебры будем называть K-подалгебрами.
2. Существуют три типа указанных подалгебр:
   2.1. Подалгебры, мультипликативная группа которых имеет циклическое строение и порядок $\Omega_1 = p^2 - 1$ (обозначим такую группу как $\Gamma 1$). Число таких K-подалгебр равно

$$\eta_1 = 2^{-1}p(p-1) \qquad (1)$$

   и каждая из них изоморфна полю $GF(p^2)$.

2.2. Подалгебры, мультипликативная группа которых (группа типа Γ2) имеет двухмерное циклическое строение (т. е. их базис включает два вектора одинакового порядка $p - 1$) и порядок $\Omega_2 = (p-1)^2$. Число таких K-подалгебр равно

$$\eta_2 = 2^{-1}p(p+1). \quad (2)$$

Каждая из подалгебр данного типа содержит $2p - 1$ необратимых векторов.

2.3. Подалгебры, мультипликативная группа которых (группа типа Γ3) имеет циклическое строение и порядок $\Omega_3 = p\,(p-1)$. Число таких K-подалгебр равно

$$\eta_3 = p + 1. \quad (3)$$

Каждая из подалгебр данного типа содержит p необратимых векторов.

3. Координаты каждого из векторов $\mathbf{V} = (v_0, v_1, v_2, v_3)$, принадлежащих заданной коммутативной подалгебре, могут быть вычислены по координатам некоторого фиксированного вектора $\mathbf{C} = (c_0, c_1, c_2, c_3)$, содержащегося в подалгебре и отличного от скалярного вектора, и по уникальной паре скалярных переменных $k,t \in GF(p)$. Вид формулы, описывающей координаты v_0, v_1, v_2 и v_3 зависит от ТУББВ, по которой задается КНАА, и от типа мультипликативной группы заданной подалгебры. Например, для мультипликативных групп типа Γ1 и Γ2 имеем следующую формулу [27]:

$$\mathbf{V} = (v_0, v_1, v_2, v_3) = (k, kc_1c_0^{-1}, t, t + k(c_3 - c_2)c_0^{-1}), \quad (4)$$

4. Порядок мультипликативной группы КНАА, заданной над полем $GF(p)$, равен

$$\Omega = p(p-1)\,(p^2-1). \quad (5)$$

Два вектора $\mathbf{A}$ и $\mathbf{B}$ будем называть перестановочными, если $\mathbf{AB} = \mathbf{BA}$, и неперестановочными, если $\mathbf{AB} \neq \mathbf{BA}$. Докажем несколько утверждений, которые используются в предлагаемом способе усиления рандомизации подписи и при построении приводимой далее схемы ЭЦП.

Утверждение 1. Пусть оба вектора $\mathbf{A}$ и $\mathbf{B}$ обратимы и $\mathbf{AB} \neq \mathbf{BA}$. Тогда из равенства $\mathbf{A}^i\mathbf{B}^j = \mathbf{A}^k\mathbf{B}^t$ следует $i \equiv k \bmod \omega_\mathbf{A}$ и $j \equiv t \bmod \omega_\mathbf{B}$, где $\omega_\mathbf{A}$ ($\omega_\mathbf{B}$) – порядок вектора $\mathbf{A}$ ($\mathbf{B}$).

Доказательство. $\{\mathbf{A}^i\mathbf{B}^j = \mathbf{A}^k\mathbf{B}^t\} \Rightarrow \{\mathbf{A}^{i-k}\mathbf{B}^{j-t} = \mathbf{E}\} \Rightarrow \{\mathbf{A}^{i-k} = \mathbf{E};\ \mathbf{B}^{j-t} = \mathbf{E}\} \Rightarrow \{i \equiv k \bmod \omega_\mathbf{A};\ j \equiv t \bmod \omega_\mathbf{B}\}$.

Утверждение 2. Пусть четырехмерные векторы $\mathbf{A}$ и $\mathbf{B}$ обратимы и $\mathbf{AB} \neq \mathbf{BA}$. Тогда: 1) из равенства $\mathbf{A}^i\mathbf{B} = \mathbf{A}^k\mathbf{B}$ следует $i \equiv k \bmod \omega_\mathbf{A}$; 2) если $i \neq k \bmod \omega_\mathbf{A}$, то $(\mathbf{A}^i\mathbf{B})(\mathbf{A}^k\mathbf{B}) \neq (\mathbf{A}^k\mathbf{B})(\mathbf{A}^i\mathbf{B})$.

Доказательство.

1. Первое положение следует непосредственно из доказанного утверждения 1. $\mathbf{A}^i\mathbf{B}^j = \mathbf{A}^k\mathbf{B}^t$

2. Предположим противное: $(\mathbf{A}^i\mathbf{B})(\mathbf{A}^k\mathbf{B}) = (\mathbf{A}^k\mathbf{B})(\mathbf{A}^i\mathbf{B})$. Тогда имеем $\mathbf{A}^i\mathbf{B}\,\mathbf{A}^k = \mathbf{A}^k\mathbf{B}\mathbf{A}^i \Rightarrow \mathbf{A}^{i-k}\mathbf{B} = \mathbf{B}\mathbf{A}^{i-k}$. Также очевидно, что $\mathbf{A}^{i-k}\mathbf{A} = \mathbf{A}\mathbf{A}^{i-k}$. Последние два равенства означают, что векторы $\mathbf{B}$ и $\mathbf{A}$ содержатся в K-подалгебре, содержащей вектор $\mathbf{A}^{i-k}$ (см. утверждения 2 и 3 в [26] или утв. 2 в [27]), откуда следует $\mathbf{AB} = \mathbf{BA}$, что противоречит условию $\mathbf{AB} \neq \mathbf{BA}$. Полученное противоречие доказывает положение 2.

Утверждение 3. Пусть векторы $\mathbf{A}$, $\mathbf{B}$ и $\mathbf{C}$ обратимы и отличны от скалярных векторов, причем $(\mathbf{AC})\mathbf{B} \neq \mathbf{B}(\mathbf{AC})$. Тогда из неравенства $i \neq k \bmod \omega_\mathbf{B}$, следует $(\mathbf{AB}^i\mathbf{C})(\mathbf{AB}^k\mathbf{C}) \neq (\mathbf{AB}^k\mathbf{C})(\mathbf{AB}^i\mathbf{C})$.

Доказательство. Предположим противное: $(\mathbf{AB}^i\mathbf{C})(\mathbf{AB}^k\mathbf{C}) = (\mathbf{AB}^k\mathbf{C})(\mathbf{AB}^i\mathbf{C})$. Тогда имеем $\mathbf{B}^i\mathbf{CAB}^k = \mathbf{B}^k\mathbf{CAB}^i \Rightarrow \mathbf{B}^{i-k}(\mathbf{CA}) = (\mathbf{CA})\mathbf{B}^{i-k}$. Последнее равенство означает, что векторы $\mathbf{B}^{i-k}$ и $(\mathbf{CA})$ содержатся в одной K-подалгебре. Очевидно, что векторы $\mathbf{B}^{i-k}$ и $\mathbf{B}$ содержатся в этой же подалгебре, из чего (см. утв. 2 и 3 в [26]) следует $(\mathbf{AC})\mathbf{B} = \mathbf{B}(\mathbf{AC})$, что противоречит условию $(\mathbf{AC})\mathbf{B} \neq \mathbf{B}(\mathbf{AC})$. Полученное противоречие доказывает утверждение 3.

Утверждение 4. Пусть векторы $\mathbf{A}$ и $\mathbf{B}$ обратимы и $\mathbf{AB} \neq \mathbf{BA}$. Тогда для всех пар натуральных значений i и k, таких, что $i \neq k \bmod \omega_\mathbf{B}$ векторы $\mathbf{AB}^i\mathbf{A}$ и $\mathbf{AB}^k\mathbf{A}$ принадлежат различным K-подалгебрам.

Доказательство. Справедливость утверждения 4 следует непосредственно из доказанного утверждения 3.

Утверждение 5. Пусть векторы $\mathbf{A}$, $\mathbf{B} \neq \mathbf{A}$ и $\mathbf{F}$ обратимы и отличны от скалярных векторов, причем $\mathbf{AB} = \mathbf{BA}$, $\mathbf{AF} \neq \mathbf{FA}$ и $\mathbf{BF} \neq \mathbf{FB}$. Тогда векторы $\mathbf{FA}$ и $\mathbf{FB}$ неперестановочны, т.е. $(\mathbf{FA})(\mathbf{FB}) \neq (\mathbf{FB})(\mathbf{FA})$.

Доказательство. Предположим противное: $(\mathbf{FA})(\mathbf{FB}) = (\mathbf{FB})(\mathbf{FA})$. Тогда имеем $\mathbf{AFB} = \mathbf{BFA} \Rightarrow \mathbf{B}^{-1}\mathbf{AF} = \mathbf{FAB}^{-1} \Rightarrow (\mathbf{B}^{-1}\mathbf{A})\mathbf{F} = \mathbf{F}(\mathbf{B}^{-1}\mathbf{A})$. Следовательно, векторы $\mathbf{F}$ и $(\mathbf{B}^{-1}\mathbf{A})$ принадлежат одной и той же K-подалгебре (см. утв. 2 и 3 в [26]). Вектор $\mathbf{A}$, очевидно, тоже принадлежит той же подалгебре, т. е. $\mathbf{AF} = \mathbf{FA}$, что противоречит условию $\mathbf{AF} \neq \mathbf{FA}$. Полученное противоречие доказывает утверждение 5.

Утверждение 6. Пусть дано разрешимое уравнение $\mathbf{A} = \mathbf{XBX}^{-1}$ с неизвестным вектором $\mathbf{X}$, где векторы $\mathbf{A}$ и $\mathbf{B} \neq \mathbf{A}$ обратимы и отличны от скалярных векторов. Тогда указанное уравнение имеет количество решений, равное порядку мультипликативной группы K-подалгебры, содержащей вектор $\mathbf{B}$, и каждое решение $\mathbf{X}_i$ принадлежит уникальной $\mathbf{K}$-подалгебре.

Доказательство. Разрешимость уравнения $\mathbf{A} = \mathbf{XBX}^{-1}$ означает существование некоторого

решения $\mathbf{X}_0$. Каждый обратимый вектор $\mathbf{V}$ K-подалгебры, содержащей вектор $\mathbf{B}$, задает уникальное решение $\mathbf{X} = \mathbf{X}_0\mathbf{V}$. Действительно, имеем $(\mathbf{X}_0\mathbf{V})\mathbf{B}(\mathbf{X}_0\mathbf{V})^{-1} = \mathbf{X}_0\mathbf{V}\mathbf{B}\mathbf{V}^{-1}\mathbf{X}_0^{-1} = \mathbf{X}_0\mathbf{B}\mathbf{V}\mathbf{V}^{-1}\mathbf{X}_0^{-1} = \mathbf{X}_0\mathbf{B}\mathbf{X}_0^{-1} = \mathbf{A}$. Таким образом, имеем столько уникальных решений, сколько имеется обратимых векторов в рассматриваемой K-подалгебре. Докажем, что других решений нет. Пусть имеется решение $\mathbf{X}_i$. Тогда имеем: $\{\mathbf{X}_i\mathbf{B}\mathbf{X}_i^{-1} = \mathbf{X}_0\mathbf{B}\mathbf{X}_0^{-1}\} \Rightarrow \{(\mathbf{X}_0^{-1}\mathbf{X}_i)\mathbf{B} = \mathbf{B}(\mathbf{X}_0^{-1}\mathbf{X}_i);\ \mathbf{X}_i = \mathbf{X}_0(\mathbf{X}_0^{-1}\mathbf{X}_i)\}$. Последние два равенства показывают, что любое решение $\mathbf{X}_i$ представимо в виде произведения решения $\mathbf{X}_0$ на вектор $(\mathbf{X}_0^{-1}\mathbf{X}_i)$, который перестановочен с $\mathbf{B}$, т. е. содержится в мультипликативной группе K-подалгебры, содержащей вектор $\mathbf{B}$.

Пусть имеются решения $\mathbf{X}_i$ и $\mathbf{X}_j \neq \mathbf{X}_i$. При фиксированном решении $\mathbf{X}_0$ имеем $\mathbf{X}_i = \mathbf{X}_0(\mathbf{X}_0^{-1}\mathbf{X}_i)$ и $\mathbf{X}_j = \mathbf{X}_0(\mathbf{X}_0^{-1}\mathbf{X}_j)$, где $\mathbf{X}_0^{-1}\mathbf{X}_i$ и $\mathbf{X}_0^{-1}\mathbf{X}_j$ принадлежат одной и той же K-подалгебре, а значит являются перестановочными. В силу утверждения 5 векторы $\mathbf{X}_i$ и $\mathbf{X}_j$ принадлежат разным K-подалгебрам, т. е. каждое решение содержится в уникальной K-подалгебре.

Утверждение 7. Пусть в уравнении $\mathbf{A} = \mathbf{X}\mathbf{G}\mathbf{X}^{-1}$ с неизвестными векторами $\mathbf{X}$ и $\mathbf{G}$ вектор $\mathbf{A}$ обратим и отличен от скалярного вектора, причем указанное уравнение имеет решения. Тогда решения с различными значениями переменной $\mathbf{G}$ не пересекаются по переменной $\mathbf{X}$.

Доказательство. Согласно утверждению 6 при фиксированном $\mathbf{G}$ имеется множество различных решений $(\mathbf{X}_i,\ \mathbf{G})$, отличающихся значениями $\mathbf{X}_i$. Пусть пары векторов $(\mathbf{X}_1,\ \mathbf{G}_1)$ и $(\mathbf{X}_2,\ \mathbf{G}_2)$ являются двумя различными решениями, в которых $\mathbf{G}_1 \neq \mathbf{G}_2$. Тогда предположение о равенстве $\mathrm{X}_1 = \mathrm{X}_2$ приводит к равенствам $\mathbf{X}_1\mathbf{G}_1\mathbf{X}_1^{-1} = \mathbf{X}_2\mathbf{G}_2\mathbf{X}_2^{-1}$ и $\mathbf{G}_1 = \mathbf{G}_2$, что противоречит условию $\mathbf{G}_1 \neq \mathbf{G}_2$.

Утверждение 8. Количество различных значений вектора $\mathbf{G}$, при которых уравнение $\mathbf{A} = \mathbf{X}\mathbf{G}\mathbf{X}^{-1}$ имеет решения равно $\approx p^2$, где $\mathbf{A}$ – обратимый вектор, отличный от скалярных векторов; p – порядок поля $GF(p)$, над которым задана четырехмерная КНАА с глобальной двухсторонней единицей.

Доказательство. Для каждого обратимого вектора $\mathbf{X}$ имеется некоторое $\mathbf{G} = \mathbf{X}^{-1}\mathbf{A}\mathbf{X}$. Согласно утверждению 6 при фиксированном $\mathbf{G}$ уравнение $\mathbf{A} = \mathbf{X}\mathbf{G}\mathbf{X}^{-1}$ имеет количество решений, равное порядку мультипликативной группы K-подалгебры, содержащей вектор $\mathbf{G}$, т.е. $\approx p^2$ различных значений $\mathbf{X}$, удовлетворяющих последнему уравнению. С учетом утверждения 7 и значения порядка мультипликативой группы КНАА, равного $\approx$p4, приходим к выводу, что формула $\mathbf{G} = \mathbf{X}^{-1}\mathbf{A}\mathbf{X}$ генерирует $\approx p^4/p^2 \approx p^2$ различных значений $\mathbf{G}$ при условии, что $\mathbf{X}$ пробегает все обратимые значения КНАА.

2. Способ усиления рандомизации

Для усиления рандомизации подписи в алгебраических алгоритмах со скрытой группой предлагается использование двух различных скрытых коммутативных групп, относящихся к разным K-подалгебрам, содержащих мультипликативную группу типа $\Gamma 1$. Пусть такие группы зафиксированы выбором двух обратимых неперестановочных векторов $\mathbf{G}$ и $\mathbf{P}$, порядок которых равен $\omega_\mathbf{G} = \omega_\mathbf{P} = p2 - 1$.Тогда в соответствии с утверждением 1 произведения всевозможных степеней векторов $\mathbf{G}$ и $\mathbf{P}$ пробегают $(p^2 - 1)^2 \approx p^4$ различных значений в четырехмерной КНАА, используемой в качестве алгебраического носителя. Действительно утверждение 1 показывает, что уникальной паре степеней $i \equiv k\ mod\ \omega_\mathbf{G}$ и $j \equiv t\ mod\ \omega_\mathrm{P}$ соответствует уникальный вектор $\mathbf{P}^j\mathbf{G}^i$.

С учетом этого предлагается следующая формула для вычисления подгоночного элемента подписи:

$$\mathbf{S} = \mathbf{D}\mathbf{P}^b\mathbf{G}^n\mathbf{F}^{-1}, \qquad (6)$$

где $\mathbf{D}$ и $\mathbf{F}$ – обратимые векторы, являющиеся элементами секретного ключа; натуральные числа $n < p^2 - 1$ и $b < p^2 - 1$ вычисляются в зависимости от рандомизирующих параметров ЭЦП. Поскольку секретные векторы $\mathbf{D}$ и $\mathbf{F}$ являются фиксированными, легко показать, что значения вектора $\mathbf{S}$ пробегают столько разных обратимых значений КНАА, сколько разных значений пробегает вектор $\mathbf{P}^b\mathbf{G}^n$, т. е. $\mathbf{S}$ потенциально принимает $\approx p^4$ различных значений. Этот способ существенно усиливает рандомизацию ЭЦП по сравнению с алгоритмами [17–20].

Атака, направленная на вычисление секретных векторов $\mathbf{D}$ и $\mathbf{F}$ по z известным подписям, предполагает составление системы скалярных уравнений, в которой число уравнений равно (или примерно равно) числу неизвестных. С учетом того, что вектор $\mathbf{P}^b\mathbf{G}^n$ принимает случайным образом почти все обратимые значения в КНАА, формулу (6) можно представить в виде $\mathbf{S} = \mathbf{D}\mathbf{V}\mathbf{F}^{-1}$, где $\mathbf{V}$ – уникальная векторная неизвестная, а $\mathbf{D}$ и $\mathbf{F}$ – фиксированные неизвестные, т.е. присутствующие в квадратном векторном уравнении, соответствующим каждой из z известных подписей. Таким образом, для z подписей имеем систему из z квадратных векторных уравнений с $z + 2$ векторными неизвестными. При любом числе подписей число неизвестных больше числа уравнений, однако, учитывая то, что уравнения не являются линейными можно предположить, что ограниченные решения могут быть вычислены, если число уравнений на 5% или 10% будет меньше числа неизвестных, т.е. для случая $z = 0{,}95(z + 2)$ или $z = 0{,}9(z + 2)$, соответственно, откуда получаем $z = 38$ или $z = 18$. При сведении системы векторных уравнений к системе скалярных уравнений получаем систему из 152 или

Таблица 1.

Минимальное число уравнений обеспечивающее вычислительную сложность W решения системы из z квадратных уравнений

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

72 квадратных уравнений в поле $GF(p)$ со 160 или 80 скалярными неизвестными, соответственно.

Показанный факт получения в ходе атаки на основе известных подписей систем уравнений, в которых число неизвестных существенно превышает число уравнений можно трактовать как формальное доказательство обеспечения предложенным способом почти полной рандомизации подписи.

В табл. 1 приведены оценки[6] вычислительной сложности решения систем из z квадратных уравнений, заданных в полях различного порядка. С учетом этих данных получаем оценку стойкости предложенного механизма усиленной рандомизации $W > 2^{192}$, что позволяет утверждать, что он не будет вносить слабости к атаке на основе известных подписей.

3. Алгоритм ЭЦП на основе разработанного способа усиленной рандомизации подписи

В качестве алгебраического носителя зададим одну из известных четырехмерных КНАА, заданных над простым конечным полем $GF(p)$ по прореженным ТУБВ [25, 27]. В качестве порядка возьмем простое число $p = 2q + 1$, такое, что q является 128-битным простым числом. В предложенном способе усиленной рандомизации подписи предполагается использование генераторов $\mathbf{G}$ и $\mathbf{P}$ двух разных скрытых циклических групп, которые не перестановочны между собой. Это определяет определенную специфику процедур формирования открытого ключа, а также генерации и верификации подписи, хотя использование приемов удвоения проверочного уравнения и задания элементов открытого ключа как замаскированных элементов скрытой группы остается, как и в алгоритме-аналоге из работы [21], в котором используется одна скрытая коммутативная группа.

В предлагаемом далее алгоритме используется условие необратимости векторов, конкретный вид которого зависит от ТУБВ, по которой определяется операция умножения в КНАА, поэтому далее предполагается, что используется прореженная ТУБВ, приводимая в [27] и определяющая следующее условие обратимости (необратимости) четырехмерных векторов $\mathbf{V} = (v_0, v_1, v_2, v_3)$:

$$\lambda v_0,\ v_1 \neq v_2 v_3 \quad (\lambda v_0,\ v_1 = v_2 v_3) \tag{7}$$

6 Ding J., Petzoldt A. Current State of Multivariate Cryptography. IEEE Security and Privacy Magazine. 2017, vol. 15, no. 4, pp. 28–36.

Формирование открытого ключа

Открытый ключ формируется в виде набора, включающего 32-байтное число ψ и 8 векторов $\mathbf{Y}_1$, $\mathbf{T}_1$, $\mathbf{Z}_1$, $\mathbf{L}_1$, $\mathbf{Y}_2$, $\mathbf{T}_2$, $\mathbf{Z}_2$, $\mathbf{L}_2$, $\mathbf{U}$ и $\mathbf{Q}$ (с суммарным размером ≈672 байт) по следующему алгоритму:

1. Сгенерировать векторы $\mathbf{G}$ и $\mathbf{P}$ порядка $p^2 - 1$, такие, что $\mathbf{GP} \neq \mathbf{PG}$.

2. Сгенерировать случайные обратимые векторы $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{K}$ и $\mathbf{N}$, принадлежащие разным K-подалгебрам, отличным от подалгебр, содержащих векторы $\mathbf{G}$ и $\mathbf{P}$. В результате получаем 8 секретных векторов $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{K}$, $\mathbf{N}$, $\mathbf{G}$, и $\mathbf{P}$, которые попарно неперестановочны и имеют общий размер ≈512 байт.

3. Сгенерировать случайные натуральные числа $x < p^2 - 1$, $u < p^2 - 1$ и $w < p^2 - 1$, причем x является взаимно простым с $p^2 - 1$. Затем вычислить значение $z = \psi^{-1} \bmod (p^2 - 1)$ следующие векторы:

$$\mathbf{Y}_1 = \mathbf{AGA}^{-1};\ \mathbf{T}_1 = \mathbf{AG}^u\mathbf{P}^w\mathbf{B}^{-1};\ \mathbf{Z}_1 = \mathbf{BPB}^{-1};$$
$$\mathbf{L}_1 = \mathbf{BP}^u\mathbf{D}^{-1};\ \mathbf{U} = \mathbf{DP}^x\mathbf{D}^{-1}; \tag{8}$$

$$\mathbf{Y}_2 = \mathbf{KG}^z\mathbf{K}^{-1};\ \mathbf{T}_2 = \mathbf{KG}^u\mathbf{P}^u\mathbf{N}^{-1};\ \mathbf{Z}_2 = \mathbf{NP}^z\mathbf{N}^{-1};$$
$$\mathbf{L}_2 = \mathbf{NP}^w\mathbf{D}^{-1};\ \mathbf{Q} = \mathbf{FG}^x\mathbf{F}^{-1}; \tag{9}$$

Натуральные 32-байтные числа x, u и w и векторы $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{G}$, $\mathbf{F}$, $\mathbf{K}$, $\mathbf{N}$ и $\mathbf{P}$ являются элементами секретного ключа, имеющего общий размер ≈608 байт.

Алгоритм генерации ЭЦП

Алгоритм вычисления ЭЦП к документу M включает следующие шаги:

1. Сгенерировать случайное натуральные число $k < p^2 - 1$ и вычислить значения векторов $\mathbf{R}_1$ и $\mathbf{R}_2$ по следующим формулам:

$$\mathbf{R}_1 = \mathbf{AG}^k\mathbf{F}^{-1},\ \mathbf{R}_2 = \mathbf{KG}^k\mathbf{F}^{-1}. \tag{10}$$

3. Вычислить хеш-значение от документа M с присоединенными к нему векторами $\mathbf{R}_1$ и $\mathbf{R}_2$: $e = e_1 \| e_2 = \mathrm{H}(\mathrm{M}, \mathbf{R}_1, \mathbf{R}_2)$, где 256-битное хеш-значение e представлено в виде конкатенации двух 128-битных натуральных чисел e_1 и e_2.

4. Сгенерировать случайное натуральное число $n < (p^2 - 1)$.

5. Вычислить степень b: $b = -(w + e + u + e_1e_2x) \bmod (p^2 - 1)$.

6. Вычислить подгоночный элемент ЭЦП **S** по формуле (6): $\mathbf{S} = \mathbf{DP}^b\mathbf{G}^n\mathbf{F}^{-1}$.

7. Вычислить вспомогательный рандомизирующий элемент ЭЦП σ по формуле $\sigma = H(\mathbf{S})$, т. е. σ является хеш-значением от подгоночного элемента **S**.

8. Вычислить вспомогательный подгоночный элемент в виде целого числа s по формуле $s = (k - \sigma - u - n)x^{-1} \bmod (p^2 - 1)$.

Подписью к документу M является тройка значений $(e_1||e_2,\ s,\ \mathbf{S})$ с общим размером ≈128 байт. Вычислительная сложность алгоритма генерации подписи примерно равна трем операциям возведения четырехмерных векторов в 256-битную степень или ≈9200 операций умножения в поле $GF(p)$.

Алгоритм верификации ЭЦП

Подпись $(e_1||e_2,\ s,\ \mathbf{S})$ к документу M выполняется по открытому ключу и включает следующие шаги:

1. Вычислить значения векторов $\mathbf{R}_1$ и $\mathbf{R}_2$ по следующим формулам:

$$\mathbf{R}_1' = \mathbf{Y}_1^{\sigma}\mathbf{T}_1\mathbf{Z}_1^{e}\mathbf{L}_1\mathbf{U}^{e_1e_2}\mathbf{SQ}^{s};$$
$$\mathbf{R}_2' = \mathbf{Y}_2'^{\sigma\psi}\mathbf{T}_2\mathbf{Z}_2^{e\psi}\mathbf{L}_2\mathbf{U}^{e_1e_2}\mathbf{SQ}^{s}. \qquad (11)$$

2. Вычислить хеш-функцию от документа M с присоединенными векторами $\mathbf{R}_1$ и $\mathbf{R}_2$: $\varepsilon_1||\varepsilon_2 = H(M, \mathbf{R}_1, \mathbf{R}_2)$, где 256-битное хеш-значение представлено в виде конкатенации двух 128-битных натуральных чисел ε_1 и ε_2.

3. Если выполняются равенства $\varepsilon_1 = e_1$ и $\varepsilon_2 = e_2$, то ЭЦП принимается как подлинная, иначе подпись отвергается как ложная.

Вычислительную сложность процедуры верификации ЭЦП можно грубо оценить как 4 операции возведения четырехмерных векторов в 256-битную степень, для чего надо осуществить ≈12300 операций умножения по модулю p. Покажем корректность работы предложенной схемы ЭЦП как то, что корректно сгенерированная ЭЦП $(e_1||e_2,\ \mathbf{S})$ проходит процедуру верификации как подлинная подпись к документу M.

Доказательство корректности схемы ЭЦП

По первому уравнению в формулах (11) вычисляем значение вектора $\mathbf{R}_1'$:

$$\mathbf{R}_1' = (\mathbf{AGA}^{-1})^{\sigma}\mathbf{AG}^{u}\mathbf{P}^{w}\mathbf{B}^{-1}(\mathbf{BPB}^{-1})^{e}\mathbf{BP}^{u}\mathbf{D}^{-1}(\mathbf{DP}^{x}\mathbf{D}^{-1})^{e_1e_2}$$
$$(\mathbf{DP}^{b}\mathbf{G}^{n}\mathbf{F}^{-1})\,(\mathbf{FG}^{x}\,\mathbf{F}^{-1})^{s} = \mathbf{AG}^{\sigma+u}\,\mathbf{P}^{w+e+u+xe_1e_2+b}\,\mathbf{G}^{n+xs}\,\mathbf{F}^{-1} =$$
$$= \mathbf{AG}^{\sigma+u}\,\mathbf{P}^{0}\,\mathbf{G}^{n+x(k-\sigma-u-n)\,x^{-1}}\,\mathbf{F}^{-1} = \mathbf{AG}^{\sigma+u}\,\mathbf{G}^{n+k-\sigma-u-n}\,\mathbf{F}^{-1} =$$
$$= \mathbf{AG}^{k}\,\mathbf{F}^{-1} = \mathbf{R}_1;$$

По второму уравнению (11) вычисляем значение вектора $\mathbf{R}_2'$ и значение $\varepsilon_1||\varepsilon_2 = H(M, \mathbf{R}_1', \mathbf{R}_2')$ и сравниваем $\varepsilon_1||\varepsilon_2$ со значением $e_1||e_2 = H(M, \mathbf{R}_1, \mathbf{R}_2)$:

$$\mathbf{R}_2' = (\mathbf{KG}^{z}\mathbf{K}^{-1})^{\sigma\psi}\,\mathbf{KG}^{u}\mathbf{P}^{u}\mathbf{N}^{-1}\,(\mathbf{NP}^{z}\mathbf{N}^{-1})^{e\psi}\,\mathbf{NP}^{w}\mathbf{D}^{-1}$$
$$(\mathbf{DP}^{x}\mathbf{D}^{-1})^{e_1e_2}\,(\mathbf{DP}^{b}\mathbf{G}^{n}\mathbf{F}^{-1})\,(\mathbf{FG}^{x}\mathbf{F}^{-1})^{s} =$$
$$= \mathbf{KG}^{z\sigma\psi+u}\mathbf{P}^{u+ze\psi+w+xe_1e_2+b}\,\mathbf{G}^{n+xs}\,\mathbf{F}^{-1} =$$
$$= \mathbf{KG}^{\sigma+u}\mathbf{P}^{0}\,\mathbf{G}^{n+x(k-\sigma-u-n)\,x^{-1}}\,\mathbf{F}^{-1} =$$
$$= \mathbf{KG}^{\sigma+u}\mathbf{G}^{n+k-\sigma-u-n}\mathbf{F}^{-1} = \mathbf{KG}^{k}\mathbf{F}^{-1} = \mathbf{R}_2;$$

Два последних равенства показывают, что проверяемая подпись прошла процедуру верификации как подлинная ЭЦП.

4. Обсуждение

Прямой атакой на предложенный алгоритм ЭЦП является вычисление секретного ключа по открытому. Поскольку каждый элемент открытого ключа зависит не от всех элементов открытого ключа, то актуальным является вопрос о вычислении секретного ключа по частям, т.е. можно ли свести решение системы квадратных векторных уравнений, составленной по формулам (8) и (9), к решению систем меньшего размера. Пара векторов $\mathbf{G}^u$ и $\mathbf{G}^x$ определяется вектором **G** и неизвестными u и x, поэтому их следует рассматривать как независимые неизвестные. Тройка векторов $\mathbf{P}^u$, $\mathbf{P}^x$ и $\mathbf{P}^w$ определяется вектором **P** и неизвестными u, x и w, поэтому их также следует рассматривать как самостоятельные неизвестные (иначе вместо системы степенных уравнений пришлось бы рассматривать систему, включающую степенные и экспоненциальные уравнения).

Также в качестве самостоятельных неизвестных следует рассматривать векторы $\mathbf{G}^z$ и $\mathbf{P}^z$. Однако при переходе от векторных уравнений к скалярным каждый из векторов $\mathbf{G}^u$, $\mathbf{G}^x$, $\mathbf{P}^u$, $\mathbf{P}^x$, $\mathbf{P}^w$, $\mathbf{G}^z$ и $\mathbf{P}^z$ будет привносить только две независимые скалярные неизвестные, поскольку его координаты могут быть выражены по формуле (4) через координаты вектора **G** (или вектора **P**) и две скалярные неизвестные $k,t \in GF(p)$. При этом степень скалярных уравнений увеличивается на единицу, однако это не так сильно влияет на сложность решения системы степенных уравнений, как число уравнений и неизвестных в системе уравнений, заданных в поле $GF(p)$.

Каждое из четырех векторных уравнений (8) включает две или три неизвестные и при переходе от одного уравнения к другому появляются два или три других неизвестных. Аналогичная ситуация имеет место и в векторных уравнениях (9). При переходе от одного из уравнений (8) к одному из уравнений (9) появляются, по крайней мере, две новые неизвестные, вовлекаемые в рассмотрение. Таким образом, система, включающая все 10 уравнений (8) и (9), не распадается на независимые системы с меньшим числом уравнений, т. е. вычисление неизвестных по частям предположительно не может быть реализовано.

Наиболее близкими к возможности раздельного вычисления неизвестных является система из пары уравнений $\mathbf{Y}_1 = \mathbf{AGA}^{-1}$ и $\mathbf{Y}_2 = \mathbf{KG}^{z}\mathbf{K}^{-1}$. Согласно утверждению 8, каждое из двух последних уравнений имеют $\approx p^2$ решений. Решения каждого из этих уравнений попадают в уникальные K-подалгебры.

Пусть $\mathbf{G}'$ и $\mathbf{G}''$ некоторые решения первого и второго уравнений соответственно, которые перестановочны (принадлежат одой K-подалгебре), т. е. $\mathbf{G}'\mathbf{G}'' = \mathbf{G}''\mathbf{G}'$. Возводя значение $\mathbf{G}'$ в степень z, можно проверить выполнимость условия $\mathbf{G}'^{z} = \mathbf{G}''$. Найдя пару значений $\mathbf{G}'$ и $\mathbf{G}''$, для которых выполняется последнее равенство, мы устанавливаем значение $\mathbf{G} = \mathbf{G}'$. Однако вычислительная трудоемкость процесса перебора составляет ≈2256 операций экспоненцирования. Кроме того, для установленных значений $\mathbf{G}$ для первого уравнения (и $\mathbf{G}^{z}$ для второго уравнения) имеются $\approx p^2$ решений, отличающихся значением вектора $\mathbf{A}$ (и $\mathbf{K}$).

Таким образом, для вычисления элементов секретного ключа по элементам открытого ключа предпочтительным с вычислительной точки зрения является решение системы уравнений следующего вида:

$$\begin{cases} \mathbf{Y}_1\mathbf{A} = \mathbf{AG};\ \mathbf{T}_1\mathbf{B} = \mathbf{AG}^{u}\mathbf{P}^{w};\ \mathbf{Z}_1\mathbf{B} = \mathbf{BP}; \\ \mathbf{L}_1\mathbf{D} = \mathbf{BP}^{u};\ \mathbf{Y}_2\mathbf{K} = \mathbf{KG}^{z};\ \mathbf{T}_2\mathbf{N} = \mathbf{KG}^{u}\mathbf{P}^{u}; \\ \mathbf{Z}_2\mathbf{N} = \mathbf{NP}^{z};\ \mathbf{L}_2\mathbf{D} = \mathbf{NP}^{w};\ \mathbf{UD} = \mathbf{DP}^{x};\ \mathbf{QF} = \mathbf{FG}^{x}.) \end{cases} \quad (12)$$

Эта система включает 10 степенных (квадратных и кубических) векторных уравнений с 15 неизвестными. При сведении решения этой системы векторных уравнений к системе скалярных уравнений координаты 8 неизвестных векторов задают 32 независимые скалярные неизвестные, а 7 векторных неизвестных ($\mathbf{G}^{u}$, $\mathbf{G}^{x}$, $\mathbf{P}^{u}$, $\mathbf{P}^{x}$, $\mathbf{P}^{w}$, $\mathbf{G}^{z}$ и $\mathbf{P}^{z}$) задают по две независимые скалярные неизвестные (координаты этих семи неизвестных выражаются по формуле (4) через координаты неизвестных $\mathbf{G}$ и $\mathbf{P}$ и пару скалярных значений $k,t \in GF(p)$.

Получаем систему из 40 степенных (квадратных, кубических и четвертой степени) скалярных уравнений с 46 скалярными неизвестными. Ожидаемая множественность решений показывает существование многих эквивалентных секретных ключей, однако нахождение одного из них можно оценить как вычислительную сложность решения системы из 40 степенных уравнений с 40 неизвестными (например, шести скалярным неизвестным присваиваем произвольные скалярные значения), заданной в поле $GF(p)$. С учетом данных табл. 1 и 129-битной разрядности p [11] получаем ожидаемую стойкость разработанного алгоритма к прямой атаке, равную $W > 2^{128}$.

В разработанном алгоритме ЭЦП реализован в полной мере предложенный в разделе 2 алгоритм усиленной рандомизации, поэтому его стойкость к атакам на основе известных подписей соответствует оценкам из раздела 2: $W > 2^{192}$.

Для получения более высокого уровня стойкости может быть использована реализация предложенного алгоритма на КНАА больших размерностей, например, $m = 6$ и $m = 10$ с ожидаемым уровнем стойкости (к прямой атаке и к подделке подписи) не менее 2192 и 2256 соответственно.

Сопоставление с алгоритмом-аналогом из статьи [21] представлено в табл. 2, из которой видно, что достоинство предложенного алгоритма состоит в более высокой производительности (на 66%). Несмотря на существенное уменьшение числа операций возведения в степень, осуществляемых в разработанном алгоритме, не было достигнуто более существенного увеличения производительности из-за того, что размер степени в нем увеличен в два раза по сравнению с алгоритмом из [21].

Для предложенного алгоритма является актуальным рассмотрение атаки по подделке подписи с использованием известных подлинных подписей. Определяющем в обеспечении стойкости к данной атаке является разнесение в проверочных уравнениях элементов открытого ключа $\mathbf{Y}_1$ (и $\mathbf{Y}_2$) и $\mathbf{U}$ по разные стороны от подгоночного элемента подписи $\mathbf{S}$ и использование вспомогательного рандомизирующего параметра σ, вычисляемого как хеш-функция от $\mathbf{S}$ (последнее требует использования вспомогательного подгоночного элемента s). Детальное рассмотрение этой атаки дает оценку стойкости $W \geq 2^{128}$ (решение системы уравнений (12) и последующее вычисление значения x (как дискретного логарифма в уравнении $(\mathbf{A}^{-1}\mathbf{Y}_1\mathbf{A})^{x} = \mathbf{F}^{-1}\mathbf{QF}$, после чего подделка подписи становится вычислительно выполнимой).

Таблица 2.

Сравнение с алгоритмом-аналогом из статьи [21]

Алгоритм	Размер открытого ключа, байт	Размер секретного ключа, байт	Размер подписи, байт	Производительность, отн. ед.	
				генерация	верификация
из статьи [23]	512	480	128	6,5	8,1
из раздела 3	672	608	128	10,8	8,1

Выводы

Предложен способ усиления рандомизации подписи в алгебраических алгоритмах ЭЦП со скрытой группой и разработан новый алгоритм, отличающийся использованием двух скрытых коммутативных групп, элементы которых не перестановочны между собой, благодаря чему обеспечивается достаточная полнота рандомизации подписи. Выполненный анализ стойкости W предложенного алгоритма к прямой атаке и к подделке подписи дал значение $W \geq 2^{128}$, которое приемлемо для многих применений. Представляет интерес реализация предложенного алгоритма на КНАА размерностей m = 6, 8 и 10, что потенциально обеспечивает существенное повышение уровня стойкости. Однако в этом случае для обоснования достигаемого уровня стойкости потребуется выполнение исследования строения таких алгебр, что представляет собой 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. *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*
5. *Kosolapov Y. V., Turchenko O. Y. On the construction of a semantically secure modification of the McEliece cryptosystem. Prikladnaya diskretnaya matematika [Applied discrete mathematics]. 2019, no. 45, pp. 33–43. DOI: 10.17223/20710410/45/4*
6. *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*
7. *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*
8. *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*
9. *Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix algebra // Вестник Санкт_петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т. 17. Вып. 3. С. 254–261. https://doi.org/10.21638/11701/spbu10.2021.303*
10. *Moldovyan N. A., Moldovyan A. A. Candidate for practical post-quantum signature scheme // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455–461. https://doi.org/10.21638/11701/spbu10.2020.410*
11. *Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2022. P. 1–17. DOI: 10.1049/ise2.12092*
12. *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*
13. *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*
14. *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*
15. *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*
16. *Moldovyan A. A., Moldovyan N. A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. V.32. N.1(94). P. 46–60. DOI: 10.56415/csjm.v32.04*
17. *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.*
18. *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.*
19. *Молдовян А. А., Молдовян Н. А. Алгоритмы ЭЦП на конечных некоммутативных алгебрах над полями характеристики два // Вопросы кибербезопасности. 2022. № 3(49). С. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68.*

20. *Moldovyan N. A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems. 2022. V. 30. N. 2(48). P. 287–298. DOI: https://doi.org/10.56415/qrs.v30.24*
21. *Молдовян А. А., Молдовян Д. Н., Костина А. А. Алгебраические алгоритмы ЭЦП с полной рандомизацией подписи // Вопросы кибербезопасности. 2024. № 2(60). С. 95–102. DOI: 10.21681/2311-3456-2024-2-95-102.*
22. *Moldovyan N. A., Moldovyan A. A. Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem // Вестник ЮУрГУ. Серия Математическое моделирование и программирование. 2019. Т. 12, № 1. С. 66–81. DOI: 10.14529/mmp190106*
23. *Moldovyan N. A. Finite Non-commutative Associative Algebras for Setting the Hidden Discrete Logarithm Problem and Post-quantum Cryptoschemes on Its Base // Bulletin of Academy of Sciences of Moldova. Mathematics. 2019. No. 1 (89). P. 71–78.*
24 *Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms with a hidden group and doubled verification equation. Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2023, no. 3, pp. 59–69. doi:10.31799/1684-8853-2023-3-59-69.*
25. *Moldovyan A. A., Moldovyan N. A. Post-quantum algebraic signature algorithms with a hidden group. Информационно-управляющие системы, 2023, no. 1(122), pp. 29–40. doi:10.31799/1684-8853-2023-1-29-40.*
26. *Moldovyan N. A., Moldovyan A. A. Structure of a 4-dimensional algebra and generating parameters of the hidden logarithm problem // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2022. Т. 18. Вып. 2. С. 209–217. https//doi.org/10.21638/11701/spbu10.2022.202*
27. *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, vol. 30, no. 1, pp. 133 – 140. https://doi.org/10.56415/qrs.v30.11*
28. *Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix algebra // Вестник Санкт_петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т. 17. Вып. 3. С. 254–261. https://doi.org/10.21638/11701/spbu10.2021.303*

References

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. 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, vol. 14154, pp. 113–138. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_5*
4. *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*
5. *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.*
6. *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, vol. 11505, pp. 329–349. Springer, Cham. https://doi.org/10.1007/978-3-030-25510-7_18*
7. *Ding J., Petzoldt A., Schmidt D. S. Multivariate Cryptography. In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020, vol.. 80. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_2*
8. *Ding J., Petzoldt A., Schmidt D. S. The Matsumoto-Imai Cryptosystem. In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020, vol. 80, pp. 25-60. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_3*
9. *Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix algebra. Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes, 2021, vol. 17, iss. 3, pp. 254–261. https://doi.org/10.21638/11701/spbu10.2021.303*
10. *Moldovyan N. A., Moldovyan A. A. Candidate for practical post-quantum signature scheme. Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes, 2020, vol. 16, iss. 4, pp. 455–461. https://doi.org/10.21638/11701/spbu10.2020.410*
11. *Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2022, pp. 1–17. DOI: 10.1049/ise2.12092*
12. *Ding J., Petzoldt A., Schmidt D.S. Solving Polynomial Systems. In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. New York. 2020, vol.. 80, pp. 185-248. https://doi.org/10.1007/978-1-0716-0987-3_8*
13. *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, vol. 13512, pp. 170–184. Springer, Cham. https://doi.org/10.1007/978-3-031-17234-2_9*
14. *Ding, J., Petzoldt, A., Schmidt, D.S. Oil and Vinegar. In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020, vol. 80, pp. 89-151. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_5*
15. *Moldovyan A.A., Moldovyan D.N., Moldovyan N.A. A new approach to the development of multidimensional cryptography algorithms. Voprosykiberbezopasnosti [Cibersecurity questtions]. 2023, no. 2(54), pp. 52–64. DOI:10.21681/2311-3456-2023-2-52-6.*
16. *Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. V.32. N.1(94). P. 46–60. DOI: 10.56415/csjm.v32.04*
17. *Moldovyan D.N., Moldovyan A.A., Moldovyan N.A. A new concept for designing post-quantum signature algorithms on non-commutative algebras. Voprosykiberbezopasnosti [Cibersecurity questtions]. 2022, no. 1(47), pp. 18–25. DOI: 10.21681/2311-3456-2022-1-18-25*
18. *Moldovyan D.N., Moldovyan A.A. Algebraic Signature Algorithms Based on Difficulty of Solving Systems of Equations. Voprosykiberbezopasnosti [Cibersecurity questtions]. 2022, no. 2(48), pp. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17*

19. *Moldovyan A. A., Moldovyan N. A. Signature algorithms on finite on non-commutative algebras over fields of characteristic two. Voprosykiberbezopasnosti [Cibersecurity questtions]. 2022, no. 3(49), pp. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68*
20. *Moldovyan N. A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems. 2022 vol. 30, no. 2(48), pp. 287–298. DOI: https://doi.org/10.56415/qrs.v30.24*
21. *Moldovyan A. A., Moldovyan D. N., Kostina A. A. Algebraic signature algorithms with complete signature randomization. Voprosy-kiberbezopasnosti [Cibersecurity questtions]. 2024, No. 2(60). P. 95–102. DOI: 10.21681/2311-3456-2024-2-95-102*
22. *Moldovyan N. A., Moldovyan A. A. Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem. Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software (Bulletin SUSU MMCS), 2019, vol. 12, no. 1, pp. 66–81. DOI: 10.14529/mmp190106*
23. *Moldovyan N. A. Finite Non-Commutative Associative Algebras for Setting the Hidden Discrete Logarithm Problem and Post-quantum Cryptoschemes on Its Base // Bulletin of Academy of Sciences of Moldova. Mathematics. 2019, no. 1 (89), pp. 71–78.*
24. *Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms with a hidden group and doubled verification equation. Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2023, no. 3, pp. 59–69. doi: 10.31799/1684-8853-2023-3-59-69*
25. *Moldovyan A. A., Moldovyan N. A. Post-quantum algebraic signature algorithms with a hidden group. Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2023, no. 1, pp. 29–40. doi:10.31799/1684-8853-2023-1-29-40.*
26. *Moldovyan N. A., Moldovyan A. A. Structure of a 4-dimensional algebra and generating parameters of the hidden logarithm problem Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes. 2022, vol. 18, iss. 2, pp. 209–217. https//doi.org/10.21638/11701/spbu10.2022.202*
27. *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, vol. 30, no. 1, pp. 133 – 140. https://doi.org/10.56415/qrs.v30.11*
28. *Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix algebra. Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes. 2021. V. 17. Iss. 3. P. 254–261. https://doi.org/10.21638/11701/spbu10.2021.303*