УДК 003.26
DOI: 10.52190/2073-2600_2022_1_31

Типовые проверочные уравнения в алгебраических алгоритмах ЭЦП со скрытой группой

Д. Н. Молдовян, канд. техн. наук
Санкт-Петербургский федеральный исследовательский центр РАН (СПб ФИЦ РАН)

Предложены типовые варианты задания проверочного уравнения в алгоритмах электронной цифровой подписи (ЭЦП) со скрытой группой, использующих в качестве алгебраического носителя конечные некоммутативные ассоциативные алгебры. Принципиальной особенностью алгоритмов данного типа является то, что подпись включает в качестве одного из элементов некоторый вектор, включаемый многократно в проверочное уравнение. Многократное включение этого элемента в проверочное уравнение определяет стойкость алгоритмов ЭЦП данного типа к подделке подписи и требует использования специального способа вычисления этого элемента по секретному ключу. Конкретный вид проверочного уравнения определяет формулы для вычисления элементов открытого ключа. Показано, что вычисление ЭЦП по секретному ключу может быть выполнено несколькими различными способами, но в обязательном порядке механизм рандомизации подписи включает операции возведения элементов скрытой группы в степени со случайными значениями.

Ключевые слова: информационная безопасность, цифровая подпись, постквантовая криптография, конечная ассоциативная алгебра, некоммутативная алгебра, скрытая группа.

Разработка практичных постквантовых алгоритмов электронной цифровой подписи остается актуальной задачей в области криптографии. Для ее решения представляется наиболее интересным способ, описанный в работах [1, 2], который является новым подходом к построению алгоритмов ЭЦП на конечных некоммутативных ассоциативных алгебрах (КНАА). В отличие от алгебраических алгоритмов, основанных на вычислительной трудности скрытой задачи дискретного логарифмирования (ЗДЛ) [3, 4], способ [1] задает построение алгоритмов ЭЦП, основанных на вычислительной трудности решения систем многих квадратных уравнений с многими неизвестными. Оба типа алгоритмов используют вычисления в скрытой (секретной) коммутативной группе и маскирующие операции в виде левых и правых умножений на векторы, которые являются неперестановочными с векторами, входящими в скрытую группу. Также общим является то, что базовыми операциями в алгоритмах указанных двух типов являются операции экспоненцирования (возведения в большую целочисленную степень).

При этом имеется принципиальное отличие, состоящее в том, что в алгоритмах второго типа ЭЦП в обязательном порядке включает некоторый специальным образом вычисляемый вектор **S** в качестве одного из своих элементов (или в качестве единственного элемента, т. е. в частном случае **S** может являться подписью), тогда как в алгоритмах первого типа использование вектора **S** в качестве элемента подписи является нетипичным. Использование вектора **S** в качестве элемента подписи предполагает, что он будет входить в проверочное уравнение, что создает предпосылки к потенциальной возможности его использования в качестве подгоночного параметра в атаках типа подделки подписи, т. е. вычисления подписи без использования секретного ключа. В алгоритмах ЭЦП, основанных на СЗДЛ, устранение таких атак обеспечивается удвоением проверочного уравнения [5, 6], а в алгоритмах, основанных на вычислительной трудности решения систем многих квадратичных уравнений, — многократным вхождением **S** в проверочное уравнение.

В [1, 2] представлены варианты проверочного уравнения с двумя вхождениями **S**. Поскольку число вхождений не связано с увеличением размера ЭЦП, но потенциально повышает стойкость к подделке подписи, представляет интерес рассмотрение схем ЭЦП, в проверочное уравнение которых вектор **S** входит три и более раз. Автор предлагает два варианта проверочных уравнений с $\beta \geq 3$ вхождениями вектора **S** и рассматривается вопрос о влиянии значения β на размер секретного и открытого ключей.

Используемый алгебраический носитель

В предлагаемых далее к рассмотрению постквантовых алгоритмах ЭЦП со скрытой группой предполагается, что в качестве алгебраическо-

Молдовян Дмитрий Николаевич, научный сотрудник.
E-mail: mdn.spectr@mail.ru

Статья поступила в редакцию 18 февраля 2022 г.

го носителя используется m-мерная КНАА со значением размерности $m \geq 4$, которая содержит глобальную двухстороннюю единицу и большое число коммутативных конечных групп в качестве подмножеств своих элементов. Другие типы КНАА, вероятно, тоже могут быть использованы для построения алгоритмов ЭЦП со скрытой группой, основанных на вычислительной трудности решения систем квадратных уравнений, однако это потребует разработки новых механизмов маскирования скрытой группы, что составляет самостоятельную задачу. Наличие глобальной единицы упрощает построение алгоритмов ЭЦП и предположительно дает возможность обеспечить более высокую производительность алгоритмов и меньшие размеры открытого ключа и подписи.

Известны различные варианты задания КНАА размерности $m = 6$ [7] и $m = 8$ [8]. Кроме того, известны унифицированные способы задания КНАА произвольной четной размерности [9]. Увеличение значения размерности m приводит к квадратичному увеличению числа умножений в конечном поле, над которым задана КНАА, для выполнения одного умножения некоторой пары векторов. Однако при этом имеется возможность уменьшить порядок указанного поля, поэтому вопрос выбора значения m заслуживает отдельного рассмотрения.

Для КНАА, используемых в качестве алгебраического носителя алгоритмов ЭЦП со скрытой группой, важным вопросом является изучение их строения с точки зрения декомпозиции на коммутативные подалгебры. Действительно, мультипликативная группа последних или некоторая ее подгруппа могут использоваться в качестве скрытой группы. В [10, 11] рассмотрены четырехмерные КНАА, заданные по прореженным таблицам умножения базисных векторов (ТУБВ), для которых полностью установлено их строение в упомянутом понимании. В частности, показано, что строение таких КНАА является сходным. Алгебра такого типа разбивается на множество $p^2 + p + 1$ коммутативных подалгебр порядка p^2, попарно пересекающихся строго в множестве скалярных векторов. При этом коммутативные подалгебры относятся к трем типам [10, 12] как содержащие мультипликативные группы:

- Γ_1 порядка

$$\Omega_1 = p^2 - 1, \qquad (1)$$

имеющую циклическое строение. Число таких подалгебр равно $\eta_1 = 2^{-1}p(p - 1)$;

- Γ_2 порядка

$$\Omega_2 = (p - 1)^2, \qquad (2)$$

имеющую двухмерное циклическое строение. Число подалгебр данного типа равно $\eta_2 = 2^{-1}p(p + 1)$;

- Γ_3 порядка

$$\Omega_3 = p(p - 1), \qquad (3)$$

имеющую циклическое строение. Число таких подалгебр равно $\eta_3 = p + 1$.

Таким образом, в данной работе предполагается использование четырехмерных КНАА [10], заданных по прореженным ТУБВ, как основного типа алгебраического носителя разработанных алгоритмов ЭЦП. Кроме того, что для указанных КНАА известно детальное строение, они обеспечивают возможность получения более высокой производительности процедур генерации и верификации ЭЦП, поскольку одна операция умножения векторов требует выполнения всего 8 операций умножения в конечном поле, что в два раза меньше по сравнению с использованием четырехмерных КНАА, заданных по "плотным" ТУБВ, например представленным в [4, 13].

Факторизация порядка скрытой группы не имеет критического влияния на стойкость алгоритмов ЭЦП, основанных на трудности решения систем многих квадратных уравнений. Однако используемый механизм вычисления элемента подписи **S** [1] таков, что при наличии делителей малого размера приводит к появлению существенной вероятности того, что процедуру генерации ЭЦП потребуется выполнять повторно (когда потребуется найти обратное значение из числа, которое не является взаимно простым с порядком скрытой группы). Для устранения таких повторов удобно задавать КНАА над простыми полями $GF(p)$ с простым значением $p = 2q + 1$, где q — тоже простое число. Действительно, это обеспечивает возможность задания скрытой группы порядка q^2 (являющейся подгруппой группы типа Γ_2) или порядка pq (являющейся подгруппой группы типа Γ_3). С учетом того что число подалгебр второго типа примерно в p раз больше, чем число подалгебр третьего типа, будем рассматривать в качестве основного варианта задание скрытой группы порядка q^2, которая обладает двухмерной цикличностью, т. е. порождается минимальной системой образующих (базисом), включающей два вектора, порядок каждого из которых равен q.

В последнем случае скрытая группа задается как вычисление пары векторов **G** и **H**, образующих базис $\langle \mathbf{G}, \mathbf{H} \rangle$ группы с двухмерной цикличностью. Для генерации базиса $\langle \mathbf{G}, \mathbf{H} \rangle$ в общем случае может быть использован следующий алгоритм.

Алгоритм генерации базиса $\langle \mathbf{G}, \mathbf{H} \rangle$.

1. Сгенерировать случайный обратимый вектор **R** и вычислить вектор $\mathbf{L} = \mathbf{R}^2$.

2. Если $\mathbf{L}^q = \mathbf{E}$, где **E** — вектор, являющийся глобальной двухсторонней единицей КНАА, ис-

пользумой в качестве алгебраического носителя, и $\mathbf{L} \neq \lambda\mathbf{E}$ для всех значений $\lambda \in GF(p)$ (т. е. если **L** не является скалярным вектором), то перейти к шагу 3, иначе перейти к шагу 1.

3. Сгенерировать случайное значение $\alpha \in GF(p)$, отличное от нуля и единицы поля $GF(p)$, такое, что β^2 также не равно единице поля $GF(p)$.

4. Сгенерировать случайное целое число k $(0 < k < q)$.

5. Вычислить вектор $\mathbf{H} = \alpha^2\mathbf{L}^k$.

6. Выдать в качестве базиса $\langle \mathbf{G}, \mathbf{H} \rangle$ случайной группы с двухмерной цикличностью два вектора: $\mathbf{G} = \mathbf{L}$ и **H**.

При q = 1443420272407352009010766274913970921515428178119 (160-битное простое число) имеем 161-битное простое число $p = 2q + 1$, предлагаемое для использования в качестве характеристики поля $GF(p)$, над которым задаются КНАА, служащие алгебраическим носителем рассматриваемых далее схем ЭЦП.

Схема ЭЦП со значением β = 3

Секретный ключ генерируется в виде набора четырехмерных векторов **A**, **B**, **D**, **F**, **G**, **H** и натуральных чисел x, w, i и j $(1 < x, w, i, j < q)$. Пара векторов **G** и **H** простого порядка q генерируется как базис $\langle \mathbf{G}, \mathbf{H} \rangle$ скрытой группы. В качестве векторов **A**, **B**, **D** и **F** генерируются случайные обратимые векторы, удовлетворяющие следующим условиям: $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AD} \neq \mathbf{DA}$, $\mathbf{AF} \neq \mathbf{FA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BD} \neq \mathbf{DB}$, $\mathbf{BF} \neq \mathbf{FB}$, $\mathbf{BG} \neq \mathbf{GB}$, $\mathbf{DF} \neq \mathbf{FD}$, $\mathbf{DG} \neq \mathbf{GD}$, $\mathbf{FG} \neq \mathbf{GF}$.

Открытый ключ вычисляется в виде набора четырехмерных векторов $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{Y}_3$ и $\mathbf{Z}_3$ по следующим формулам:

$$\mathbf{Y}_1 = \mathbf{AGB},\ \mathbf{Z}_1 = \mathbf{DHA}^{-1},\ \mathbf{Y}_2 = \mathbf{FH}_w\mathbf{B},$$
$$\mathbf{Z}_2 = \mathbf{DG}_x\mathbf{F}^{-1},\ \mathbf{Y}_3 = \mathbf{AH}_i\mathbf{D}^{-1} \text{ и } \mathbf{Z}_3 = \mathbf{B}^{-1}\mathbf{G}_j\mathbf{F}^{-1}. \quad (4)$$

Процедура генерации ЭЦП.

1. Сгенерировать случайные целые числа k и t, удовлетворяющие условиям $1 < k < q$ и $1 < t < q$, и вычислить вектор $\mathbf{R} = \mathbf{AG}^k\mathbf{H}^t\mathbf{F}^{-1}$.

2. Используя некоторую коллизионно стойкую 320-битную хэш-функцию f_H, вычислить значение $e = e_1 \| e_2 = f_H(M \| \mathbf{R})$, где M — подписываемый электронный документ, а хэш-значение e представлено как конкатенация двух 160-битных чисел e_1 и e_2.

3. Вычислить целочисленные значения n и d по следующим двум формулам:

$$n = \frac{k - e_1 - xe_2 - j}{e_1 + e_2 - 1} \bmod q; \quad (5)$$

$$d = \frac{t - e_1 - we_2 - i}{e_1 + e_2 - 1} \bmod q. \quad (6)$$

4. Вычислить четырехмерный вектор **S** по формуле

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{D}^{-1}. \quad (7)$$

Подписью является пара значений e (320-битное число) и вектор **S** (четыре 161-битных значения) с общим размером ≈121 байт. Основной вклад в вычислительную трудность процедуры генерации ЭЦП вносят четыре операции экспоненцирования четырехмерных векторов, которые можно оценить как 7680 умножений в поле $GF(p)$.

Процедура верификации ЭЦП.

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

$$\mathbf{R}_K = \left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^{e_1}\mathbf{Y}_3\mathbf{S}^{-1}\mathbf{Z}_3\left(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2\right)^{e_2} \quad (8)$$

с $\beta = 3$ вхождениями вектора **S** и двумя операциями возведения в степень.

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

3. Сравнить значения e_K и e. Если $e_K = e$, то ЭЦП признается подлинной, в противном случае $(e_K \neq e)$ — ложной.

Вычислительная сложность процедуры верификации ЭЦП определяется двумя операциями экспоненцирования четырехмерных векторов, и ее можно оценить как 3840 умножений в поле $GF(p)$.

Доказательство корректности схемы ЭЦП.

Схема ЭЦП работает корректно, если подпись, вычисленная по процедуре генерации ЭЦП, проходит процедуру верификации как подлинная ЭЦП. Действительно, с учетом формул (5)—(8) это демонстрируется следующим образом:

$$\mathbf{R}_K = \left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^{e_1}\mathbf{Y}_3\mathbf{S}^{-1}\mathbf{Z}_3\left(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2\right)^{e_2} =$$

$$= \begin{pmatrix}\mathbf{AGBB}^{-1}\mathbf{G}^n \times \\ \times\mathbf{H}^d\mathbf{D}^{-1}\mathbf{DHA}^{-1}\end{pmatrix}^{e_1}\mathbf{Y}_3\mathbf{S}^{-1}\mathbf{Z}_3\begin{pmatrix}\mathbf{FH}^w\mathbf{BB}^{-1}\mathbf{G}^n \times \\ \times\mathbf{H}^d\mathbf{D}^{-1}\mathbf{DG}^x\mathbf{F}^{-1}\end{pmatrix}^{e_1} =$$

$$= \left(\mathbf{AG}^{n+1}\mathbf{H}^{d+1}\mathbf{A}^{-1}\right)^{e_1}\left(\mathbf{Y}_3\mathbf{S}^{-1}\mathbf{Z}_3\right)\left(\mathbf{FH}^{w+d}\mathbf{G}^{n+x}\mathbf{F}^{-1}\right)^{e_2} =$$

$$= \mathbf{AG}^{ne_1+e_1}\mathbf{H}^{de_1+e_1}\mathbf{A}^{-1}\begin{pmatrix}\mathbf{AH}^i\mathbf{D}^{-1}\mathbf{DG}^{-n} \times \\ \times\mathbf{H}^{-d}\mathbf{BB}^{-1}\mathbf{G}^j\mathbf{F}^{-1}\end{pmatrix} \times$$

$$\times\mathbf{FH}^{we_2+de_2}\mathbf{G}^{ne_2+xe_2}\mathbf{F}^{-1} =$$

$$= \mathbf{AG}^{ne_1+e_1-n+j+ne_2+xe_2}\mathbf{H}^{de_1+e_1+i-d+we_2+de_2}\mathbf{F}^{-1} =$$

$$= \mathbf{AG}^{n(e_1+e_2-1)+e_1+xe_2+j}\mathbf{H}^{d(e_1+e_2-1)+e_1+we_2+i}\mathbf{F}^{-1} =$$

$$= \mathbf{AG}^{\frac{k-e_1-xe_2-j}{e_1+e_2-1}(e_1+e_2-1)+e_1+xe_2+j} \times$$

$$\times\mathbf{H}^{\frac{t-e_1-we_2-i}{e_1+e_2-1}(e_1+e_2-1)+e_1+we_2+i}\mathbf{F}^{-1} =$$

$$= \mathbf{AG}^k\mathbf{H}^t\mathbf{F}^{-1} = \mathbf{R} \Rightarrow f\left(M \| \mathbf{R}_K\right) = f\left(M \| \mathbf{R}\right) \Rightarrow e_K = e.$$

Постквантовая стойкость описанной схемы ЭЦП обеспечивается тем, что вычисление секретного ключа по открытому ключу связано с решением системы из 11 квадратных векторных уравнений (определяемых шестью формулами (4) и условием попарной перестановочности векторов **G**, **H**, $\mathbf{H}^w$, $\mathbf{G}^x$, $\mathbf{G}^j$ и $\mathbf{H}^i$) с 10 неизвестными (которыми являются четырехмерные векторы **A**, **B**, **D**, **F**, **G**, **H**, $\mathbf{H}^w$, $\mathbf{G}^x$, $\mathbf{G}^j$ и $\mathbf{H}^i$), заданной над использованной в качестве алгебраического носителя четырехмерной КНАА. Указанная система векторных уравнений сводится к системе из 44 квадратных уравнений с 40 неизвестными, заданной над полем $GF(p)$ со 161-битным значением порядка.

Заметим, что в данной схеме ЭЦП секретный ключ можно сформировать в виде набора **A**, **B**, **D**, **F**, **G**, **H**, $\mathbf{H}_w$, $\mathbf{G}_x$, $\mathbf{G}_j$ и $\mathbf{H}_i$, в котором векторы $\mathbf{H}_w$, $\mathbf{G}_x$, $\mathbf{G}_j$ и $\mathbf{H}_i$ выбираются случайным образом из скрытой группы, задаваемой базисом ⟨**G**, **H**⟩. При этом процедура верификации остается неизменной, однако процедура генерации ЭЦП приобретает вид следующего алгоритма.

1. Сгенерировать случайные целые числа k_1, k_2, k_3, k_4, k_5 и k_6 и вычислить вектор

$$\mathbf{R} = \mathbf{A}\mathbf{G}^{k_1}\mathbf{H}^{k_2}\mathbf{H}_w^{k_3}\mathbf{G}_x^{k_4}\mathbf{G}_j^{k_5}\mathbf{H}_i^{k_6}\mathbf{F}^{-1}. \qquad (9)$$

2. Вычислить значение $e = e_1 \| e_2 = f_H(M \| \mathbf{R})$.

3. Вычислить целочисленные значения n_i для $i = 1, 2, \ldots, 6$ по следующим формулам:

$$n_1 = \frac{k_1 - e_1}{e_1 + e_2 - 1} \bmod q; \quad n_2 = \frac{k_2 - e_1}{e_1 + e_2 - 1} \bmod q;$$

$$n_3 = \frac{k_3 - e_2}{e_1 + e_2 - 1} \bmod q; \quad n_4 = \frac{k_4 - e_2}{e_1 + e_2 - 1} \bmod q;$$

$$n_5 = \frac{k_5 - 1}{e_1 + e_2 - 1} \bmod q; \quad n_6 = \frac{k_6 - 1}{e_1 + e_2 - 1} \bmod q.$$

4. Вычислить четырехмерный вектор **S** по формуле

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{n_1}\mathbf{H}^{n_2}\mathbf{H}_w^{n_3}\mathbf{G}_x^{n_4}\mathbf{G}_j^{n_5}\mathbf{H}_i^{n_6}\mathbf{D}^{-1}. \qquad (10)$$

В модифицированной процедуре генерации ЭЦП выполняется 12 операций экспоненцирования, т. е. ее производительность в три раза меньше по сравнению с исходным вариантом этой процедуры. Видно, что предпочтительным является вычисление значений $\mathbf{H}_w$, $\mathbf{G}_x$, $\mathbf{G}_j$ и $\mathbf{H}_i$ по формулам $\mathbf{H}_w = \mathbf{H}^w$, $\mathbf{G}_x = \mathbf{G}^x$, $\mathbf{G}_j = \mathbf{G}^j$ и $\mathbf{H}_i = \mathbf{H}^i$. Из модифицированной версии процедуры генерации ЭЦП явно видно, что операции возведения векторов **G** и **H** в секретные степени при вычислении элементов открытого ключа используются как технический прием задания случайного выбора векторов из скрытой группы, который обеспечивает повышение производительности схемы ЭЦП.

Схема ЭЦП со значением β = 4

Секретный ключ генерируется в виде набора четырехмерных векторов **A**, **B**, **G** и натурального числа x ($1 < x < q$), где векторы **G** и **H** порядка q составляют базис ⟨**G**, **H**⟩ скрытой группы. В качестве векторов **A** и **B** генерируются случайные обратимые векторы, удовлетворяющие условиям $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BG} \neq \mathbf{GB}$.

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

$$\mathbf{Y} = \mathbf{AGB}, \ \mathbf{Z} = \mathbf{AG}^x\mathbf{B} \text{ и } \mathbf{U} = \mathbf{AHB}. \qquad (11)$$

Процедура генерации ЭЦП.

1. Сгенерировать случайные целые числа k и t ($1 < k < q$; $1 < t < q$) и вычислить четырехмерный вектор

$$\mathbf{R} = \mathbf{B}^{-1}\mathbf{G}^k\mathbf{H}^t\mathbf{B}. \qquad (12)$$

2. Используя 320-битную хэш-функцию f_H, вычислить значение $e = e_1 \| e_2 = f_H(M \| \mathbf{R})$, где M — подписываемый электронный документа, а хэш-значение e представлено как конкатенация двух 160-битных чисел e_1 и e_2.

3. Вычислить целочисленные значения n и d по следующим двум формулам:

$$n = \frac{k - e_1 - e_1^2 - xe_1}{e_1(e_1 + e_2 + 1)} \bmod q; \qquad (13)$$

$$d = \frac{t - e_1 e_2}{e_1(e_1 + e_2 + 1)} \bmod q. \qquad (14)$$

4. Вычислить подгоночный элемент ЭЦП в виде четырехмерного вектора **S** по формуле

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{A}^{-1}. \qquad (15)$$

Подписью является пара (e, **S**) с общим размером ≈121 байт. Основной вклад в вычислительную трудность процедуры генерации ЭЦП вносят четыре операции экспоненцирования четырехмерных векторов, из которых две выполняются при генерации вектора **R** и две — при вычислении вектора **S**.

Процедура верификации ЭЦП.

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

$$\mathbf{R}_K = \left((\mathbf{SY})^{e_1}\,\mathbf{S}(\mathbf{US})^{e_2}\,\mathbf{ZSY}\right)^{e_1} \qquad (16)$$

с β = 4 вхождениями вектора **S** и тремя операциями возведения в степень.

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

3. Сравнить значения e_K и e. Если $e_K = e$, то ЭЦП признается подлинной, иначе ($e_K \neq e$) — ложной.

Доказательство корректности схемы ЭЦП.

Корректность работы последней схемы ЭЦП показывается с учетом формул (11)–(16) следующим образом:

$$\mathbf{R}_K = \left((\mathbf{SY})^{e_1}\,\mathbf{S}(\mathbf{US})^{e_2}\,\mathbf{ZSY}\right)^{e_1} =$$

$$= \left(\left(\mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{GB}\right)^{e_1}\mathbf{S}\left(\mathbf{AHG}^{n}\mathbf{H}^{d}\mathbf{A}^{-1}\right)^{e_2}\mathbf{AG}^{x}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{A}^{-1}\mathbf{Y}\right)^{e_1} =$$

$$= \left(\mathbf{B}^{-1}\mathbf{G}^{ne_1+e_1}\mathbf{H}^{de_1}\mathbf{BSAG}^{ne_2}\mathbf{H}^{de_2+e_2}\mathbf{A}^{-1}\mathbf{AG}^{x+n}\mathbf{H}^{d}\mathbf{A}^{-1}\mathbf{Y}\right)^{e_1} =$$

$$= \left(\mathbf{B}^{-1}\mathbf{G}^{ne_1+e_1}\mathbf{H}^{de_1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{G}^{ne_2}\mathbf{H}^{de_2+e_2}\mathbf{G}^{x+n}\mathbf{H}^{d}\mathrm{GB}\right)^{e_1} =$$

$$= \left(\mathbf{B}^{-1}\mathbf{G}^{ne_1+n+ne_2+e_1+x+n+1}\mathbf{H}^{de_1+d+de_2+e_2+d}\mathbf{B}\right)^{e_1} =$$

$$= \left(\mathbf{B}^{-1}\mathbf{G}^{n(e_1+e_2+1)+e_1+x+1}\mathbf{H}^{d(e_1+e_2+1)+e_2}\mathbf{B}\right)^{e_1} =$$

$$= \mathbf{B}^{-1}\mathbf{G}^{ne_1(e_1+e_2+1)+e_1^2+xe_1+e_1}\mathbf{H}^{de_1(e_1+e_2+1)+e_1e_2}\mathbf{B} =$$

$$= \mathbf{B}^{-1}\mathbf{G}^{k}\mathbf{H}^{t}\mathbf{B} = \mathbf{R} \Rightarrow f\left(M \,\|\, \mathbf{R}_K\right) = f\left(M \,\|\, \mathbf{R}\right) \Rightarrow e_K = e.$$

Постквантовая стойкость представленной схемы ЭЦП обеспечивается тем, что вычисление секретного ключа по открытому ключу требует нахождения решения системы из следующих 5 квадратных векторных уравнений с 5 неизвестными, **A**, $\mathbf{B}^{-1}$, **G**, $\mathbf{G}_x$ и **H**:

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

Указанная система векторных уравнений сводится к системе из 20 квадратных уравнений с 20 неизвестными, заданной над полем $GF(p)$, порядок которого равен 161-битному простому числу.

Обсуждение

Известные алгоритмы ЭЦП и алгоритмы открытого распределения ключей и открытого шифрования, основанные на вычислительной сложности нахождения решений систем многих квадратных уравнений с многими неизвестными, относятся к так называемой многомерной криптографии [14, 15]. Предложенные в данной работе алгоритмы ЭЦП имеют общность с криптосхемами многомерной криптографии по используемой базовой вычислительно трудной задаче, которая определяет их постквантовую стойкость. По построению алгоритмы ЭЦП со скрытой группой существенно отличаются от двухключевых алгоритмов многомерной криптографии.

Существенно, что в предложенных схемах ЭЦП системы квадратных уравнений заданы над полем значительно большего порядка, чем в случае алгоритмов многомерной криптографии. Однако в последних число квадратных уравнений и число неизвестных составляет от 30 до 200, тогда как в первых число неизвестных равно 40 (в алгоритме со значением $\beta = 3$) и 20 (в алгоритме со значением $\beta = 4$). Меньшее число неизвестных компенсируется тем, что квадратные уравнения задаются над полем, размер порядка которого значительно больше (в 10 и более раз).

В [1] предложен неформальный показатель ψ уровня стойкости алгоритмов ЭЦП, основанных на вычислительной сложности решения систем многих квадратных уравнений, трактуемый как произведение двоичного логарифма от порядка поля, над которым задана система, и числа неизвестных. В соответствии с этим критерием предложенные два алгебраических алгоритма ЭЦП со скрытой группой обладают более высоким ожидаемым уровнем стойкости по сравнению с многими известными постквантовыми алгоритмами ЭЦП, относящимися к многомерной криптографии. Однако вопрос детального рассмотрения их стойкости к атакам различных типов является открытым.

Предложенные два алгоритма используют проверочные уравнения с различным числом β вхождений вектора **S**. Из построения алгоритмов видно, что с ростом значения β размер ЭЦП не изменяется, а размер открытого ключа больше зависит от формул, по которым вычисляются элементы открытого ключа в зависимости от элементов секретного ключа, чем от значения β.

Механизм многократного вхождения вектора **S** как подгоночного элемента подписи (элемента, вычисляемого в зависимости от рандомизирующего элемента e, определяемого значением вектора рандомизации **R**, таким способом, что для сгенерированной подписи выполняется проверочное уравнение) предназначен для предотвращения возможности использования **S** в качестве подгоночного значения также и при подделке подписи (атаки на алгоритм ЭЦП, связанные с попыткой вычисления правильной подписи без вычисления секретного ключа). Использование значения $\beta = 2$ представляется достаточным (при соответствующем построении алгоритма ЭЦП со скрытой группой) для достижения указанной цели. Однако разработка алгоритмов ЭЦП со значениями $\beta = 3$ и $\beta = 4$ также представляют интерес, поскольку при этом сохраняются достаточно высокая производительность и малые размеры подписи и открытого ключа и обеспечивается потенциально более высокий уровень защищенности от атак с использованием **S** в качестве подгоночного параметра алгоритма подделки ЭЦП.

Сравнение известных и предложенных постквантовых алгоритмов ЭЦП, использующих однотипную вычислительно трудную задачу, представлено в таблице, которая показывает, что вторые обладают преимуществами по некоторым параметрам.

Сравнение предложенных алгоритмов ЭЦП с известными алгоритмами, основанными на вычислительной сложности решения систем многих квадратичных уравнений

Алгоритм ЭЦП	Размер ЭЦП, байт	Размер открытого ключа, байт	Число квадратных уравнений (неизвестных)	Порядок поля, над которым заданы уравнения	Показатель ψ
[14]	—	—	27 (27)	2^{16}	432
Rainbow [16]	33	16065	27 (33)	2^8	264
QUARTZ [15]	16	72704	100 (107)	2^4	428
Rainbow [17] (3 разных версии)	66—204	>150000—>1900000	64 (96)—128 (204)	2^4, 31, 2^8	384—1632
[1] (β = 2)	160	512	28 (28)	$>2^{256}$	≈7168
Предложенный (β = 3)	121	483	36 (32)	$>2^{160}$	≈5120
Предложенный (β = 4)	121	242	20 (20)	$>2^{160}$	≈3200

Заключение

Увеличение числа вхождений элемента подписи **S** в проверочное уравнение расширяет вариативность разработки постквантовых алгебраических алгоритмов ЭЦП со скрытой группой при сохранении их преимуществ по производительности и размерам открытого ключа и подписи по сравнению с известными постквантовыми схемами ЭЦП. Представляет интерес использование проверочных уравнений в предложенных двух алгоритмах для разработки постквантовых алгебраических алгоритмов на КНАА, заданных над конечными полями характеристики два, что обеспечит снижение схемотехнической сложности реализации и повышение производительности. Однако это является вопросом отдельного рассмотрения. Также для будущих исследований представляется интересным и важным рассмотрение выбора параметров алгоритмов ЭЦП со скрытой группой при использовании в качестве их алгебраического носителя шестимерных и восьмимерных КНАА, заданных над простыми конечными полями $GF(p)$ и полями $GF(2^z)$.

Работа выполнена при частичной финансовой поддержке РФФИ (проект № 21-57-54001-Вьет_а) и бюджетной темы № FFZF-2022-0007.

Литература

1. *Молдовян А. А., Молдовян Н. А.; Молдовян Д. Н., Костина А. А.* Новый подход к разработке алгоритмов цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2021. № 4. С. 45—49. DOI: 0.52190/2073-2600_2021_4_45.

2. *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.

3. *Moldovyan N. A., Moldovyan A. A.* Finite Non-commutative Associative Algebras as Carriers of Hidden Discrete Logarithm Problem // Вестник ЮУрГУ. Сер. "Математическое моделирование и программирование". 2019. Т. 12. № 1. С. 66—81. DOI: 10.14529/mmp190106.

4. *Moldovyan A. A., Moldovyan N. A.* Post-quantum signature algorithms based on the hidden discrete logarithm problem // Computer Science J. Moldova. 2018. V. 26. № 3(78). P. 301—313.

5. *Молдовян А. А., Молдовян Н. А., Молдовян Д. Н., Фахутдинов Р. Ш.* Схемы цифровой подписи с удвоенным проверочным уравнением // Вопросы защиты информации. 2021. № 2. С. 30—36. DOI: 10.52190/2073-2600_2021_2_30.

6. *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. DOI: 10.21638/11701/spbu10.2020.410.

7. *Moldovyan D. N.* A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. V. 27. № 2. P. 293—308.

8. *Moldovyan D. N., Moldovyan A. A., Moldovyan N. A.* Digital signature scheme with doubled verification equation // Computer Science J. Moldova. 2020. V. 28. № 1(82). P. 80—103.

9. *Moldovyan N. A.* Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and Related Systems. 2018. V. 26. № 2. P. 263—270.

10. *Молдовян Д. Н.* Задание шестимерных алгебр как носителей криптосхем, основанных на скрытой задаче дискретного логарифмирования // Вопросы защиты информации. 2021. № 1. С. 26—32. DOI: 10.52190/2073-2600_2021_1_26.

11. *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. DOI: 10.21638/11701/spbu10.2021.303.

12. *Moldovyan D. N.* A practical digital signature scheme based on the hidden logarithm problem // Computer Science J. Moldova. 2021. V. 29. № 2(86). P. 206—226.

13. *Moldovyan N. A.* Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. № 2(93). P. 62—67.

14. *Shuaiting Q., Wenbao H., Yifa Li, Luyao J.* Construction of Extended Multivariate Public Key Cryptosystems // International J. Network Security. 2016. Vol. 18. № 1. P. 60—67.

15. *Jintai D., Dieter S.* Multivariable Public Key Cryptosystems [Электронный ресурс]. Режим доступа: https://eprint.iacr.org/2004/350.pdf (дата обращения: 15.02.2022).

16. *Ding J., Schmidt D.* Rainbow, a new multivariable polynomial signature scheme : Conference on Applied Cryptography and Network Security — ACNS 2005. Springer Lecture Notes in Computer Science. 2005. V. 3531. P. 164—175.

17. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [Электронный ресурс]. Режим доступа: https://www.pqcrainbow.org/ (дата обращения: 15.02.2022)

Typical verification equations in algebraic digital signature algorithms with a hidden group

D. N. Moldovyan
St. Petersburg Federal Research Center of the RAS (SPC RAS),
St. Petersburg, Russia

*Typical forms of the verification equation of the digital signature algorithms with a hidden group, which use finite non-commutative associative algebras as an algebraic support are proposed. The principal feature of the algorithms of this type is that the signature includes a certain vector **S** as one of its elements, which enters several times in the verification equation. The multiple entry of the vector **S** in the verification equation determines the security of the algorithms to the forging signature attacks that use the vector **S** as a fitting parameter. However the multiple entry requires the use of a special method for calculating the vector **S**, when using the secret key. The specific form of the verification equation determines the formulas for calculation of the public-key elements. It is shown that the calculation of the signature can be performed in several different ways, but in all cases the signature randomization mechanism includes exponentiations of the elements of the hidden group to the degrees with random values.*

Keywords: information security, digital signature, post-quantum cryptography, finite associative algebra, non-commutative algebra, hidden group.

Bibliography — 17 references. *Received February 18, 2022*