УДК 512.552.18+003.26 **DOI** 10.15622/ia.24.6.9

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

РАНДОМИЗАЦИЯ В ПОСТКВАНТОВЫХ АЛГОРИТМАХ ЭЦП С СЕКРЕТНОЙ ГРУППОЙ

Молдовян А.А., Молдовян Д.Н., Костина А.А. **Рандомизация в постквантовых алгоритмах ЭЦП с секретной группой.**

Аннотация. В области постквантовой двухключевой криптографии значительный интерес представляет разработка практичных алгебраических схем электронной цифровой подписи (ЭЦП) с секретной группой, стойкость которых базируется на вычислительной сложности решения систем степенных уравнений с многими неизвестными. В качестве алгебраического носителя в таких криптосхемах используются ассоциативные некоммутативные конечные алгебры (АНКА). Специфическим моментом, связанным с обеспечением стойкости к атакам на основе известных подписей при разработке схем ЭЦП данного типа, является наличие проблемы совершенствования механизма рандомизации подгоночного элемента цифровой подписи, представляющего собой вектор S, многократно входящий в уравнение верификации в качестве множителя. Известное решение этой проблемы на основе вычисления S в зависимости от двух векторов, выбираемых случайным образом из двух коммутативных секретных групп, таких, что элементы одной из них некоммутативны с элементами другой, при использовании в проверочном уравнении значения хеш-функции от S приводит к увеличению размера ЭЦП, обусловленного необходимостью задания двух вспомогательных подгоночных элементов подписи. В статье предлагается новый механизм рандомизации подписи, отличающийся вычислением значения S в зависимости от двух векторов, выбираемых случайным образом из одной коммутативной секретной группы. Предложенный механизм обеспечивает приемлемый уровень стойкости к атакам на основе известных подписей и может быть положен в основу разработки схем ЭЦП с одним уравнением верификации и одним вспомогательным подгоночным элементом подписи. Разработан новый алгебраический алгоритм ЭЦП, представляющий интерес как прототип практичного постквантового стандарта ЭЦП. Даны оценки его параметров при реализации на четырехмерных АНКА и на алгебре матриц 3×3, заданных над простым конечным полем.

Ключевые слова: постквантовая криптография, многомерная криптография, алгоритм ЭЦП, рандомизация ЭЦП, криптоалгоритм на конечных алгебрах, криптосхема на некоммутативных алгебрах, секретная группа.

1. Введение. Исследования в области разработки двухключевых криптографических алгоритмов, стойких к криптоанализу с использованием квантовых компьютеров, имеют высокую степень актуальности [1, 2]. Это обусловлено ожидаемым появлением в ближайшем будущем практически доступных квантовых вычислителей, для которых известны полиномиальные по времени алгоритмы решения как задачи факторизации (ЗФ), так и задачи дискретного логарифмирования (ЗДЛ) [3, 4]. Проблема разработки практичных постквантовых криптографических алгоритмов является текущим вызовом в области прикладной криптографии, поскольку на

практике наиболее широко применяемые алгоритмы открытого согласования секретного ключа, открытого шифрования и электронной цифровой подписи (ЭЦП) основаны на ЗДЛ и/или ЗФ. Действительно, появление практически доступного многокубитного квантового вычислителя будет означать необходимость обновления арсенала используемых на практике криптографических двухключевых алгоритмов. Для обеспечения постквантовой стойкости разрабатываемые криптографические алгоритмы и протоколы должны базироваться на использовании вычислительной трудности задач, для которых неизвестны и предположительно не будут найдены эффективные (полиномиальные) алгоритмы их решения на квантовом компьютере. В этом направлении разработано большое число криптоалгоритмов, относящихся к различным типам, например, к криптосхемам на группах [5], на кодах, исправляющих ошибки [6, 7], на алгебраических решетках [8, 9], на трудно обратимых функциях [10] и на булевых функциях [11].

Значительное внимание со стороны криптографического сообщества уделяется разработке и криптоанализу постквантовых алгоритмов открытого шифрования, открытого согласования ключа и ЭЦП, базирующихся на трудно обратимых нелинейных отображениях с секретной лазейкой [12 – 15]. Стойкость алгоритмов данного типа определяется вычислительной сложностью решения больших систем степенных уравнений (БССУ), обычно квадратных и в отдельных случаях уравнений третьей и более высокой степени, с многими неизвестными. Это направление известно с 1988 г. как “multivariate cryptography” (далее будем использовать термин многомерная криптография) и в его рамках разработано большое число алгоритмов, которые достаточно детально проанализированы, а многие из них прошли несколько этапов совершенствования. Однако в известных разработках, относящихся к многомерной криптографии так и не был устранен существенный прикладной недостаток, связанный с непрактично большим размером открытого ключа (от десятков Кбайт до нескольких Мбайт для различных уровней стойкости от 2^{80} до 2^{256}). В частности, непрактичность алгоритмов ЭЦП с таким размером открытого ключа связана с его распечаткой на бумажном носителе, который подписывается создателем (владельцем) этого ключа и хранится в удостоверяющем центре.

Недавно предложенная в работах [16, 17] парадигма построения алгоритмов многомерной криптографии, использующая задание трудно обратимых отображений с секретной лазейкой как операции экспоненциирования в конечных векторных полях с секретной

модификацией, потенциально позволяет уменьшить размер открытого ключа в 10 раз и более. Однако, и в этом случае длина открытого ключа остается непрактично большой.

В статьях [18, 19] предложена концепция построения алгоритмов многомерной криптографии, относящихся к новому типу – алгебраическим алгоритмам ЭЦП с секретной группой, стойкость которых основана на вычислительной сложности решения БССУ. В криптоалгоритмах этого типа в качестве алгебраического носителя используются ассоциативные некоммутативные конечные алгебры (АНКА), включая как частный случай алгебры матриц. Достоинством постквантовых алгоритмов ЭЦП данного типа является сочетание сравнительно малых размеров открытого ключа и цифровой подписи по сравнению с известными. Их особенностью является использование подгоночного элемента подписи в виде вектора **S**, используемого в качестве множителя, входящего в проверочное уравнение два и более раза. При этом вектор **S** вычисляется в зависимости от предварительно генерируемого рандомизирующего элемента подписи *e*.

В отличие от рандомизированных алгоритмов ЭЦП, стойкость которых основана на вычислительной трудности решения ЗДЛ, в алгоритмах ЭЦП с секретной группой при фиксированном секретном ключе подгоночный элемент потенциально принимает значения из существенно ограниченного подмножества элементов алгебраического носителя. Несмотря на уникальность упомянутого подмножества, возникают предпосылки для реализации атак на основе известных подписей, которые состоят в вычислении элементов секретного ключа по некоторому набору известных подписей. Действительно, в работе [20] было показано, что механизм рандомизации элемента **S**, используемый в алгоритмах [18, 19], является недостаточным для обеспечения стойкости к указанной атаке по причине вычисления значения **S** в зависимости от случайного вектора, выбираемого из ограниченного подмножества элементов АНКА (а именно, из секретной группы, порядок которой существенно меньше порядка алгебраического носителя).

Предложенный в [20] способ совершенствования механизма рандомизации ЭЦП требует использования удвоенного уравнения верификации подписи. Последнее обусловливает значительное снижение производительности процедуры проверки подлинности ЭЦП, а также появление предпосылок специальных атак типа подделка подписи. Способ совершенствования механизма рандомизации ЭЦП, дающий возможность использовать в процедуре верификации только одно проверочное уравнение с многократным

вхождением вектора **S** разработан в статье [21], в которой вычисление подгоночного элемента подписи **S** задается в зависимости от двух взаимно некоммутативных векторов, выбираемых случайным образом из двух секретных коммутативных групп. В работах [21, 22] рассмотрены перспективные варианты проверочных уравнений, в которых используется дополнительный прием предотвращения атак на основе решения проверочного уравнения относительно неизвестного вектора **S**, состоящий в задании в проверочном уравнении операции возведения в степень $\rho = \Phi(\mathbf{S})$, где $\Phi(\cdot)$ – некоторая специфицированная хеш-функция. Этот прием представляется эффективным для обозначенной цели, однако в алгоритмах ЭЦП с двумя секретными группами требуется использования двух дополнительных подгоночных элементов подписи, что приводит к увеличению размера ЭЦП.

В настоящей статье предлагается новый механизм рандомизации в алгебраических алгоритмах ЭЦП с одной секретной коммутативной группой и одним проверочным уравнением, обеспечивающий возможность использовать только один дополнительный подгоночный элемент подписи в схемах ЭЦП с проверочным уравнением, включающем значение хеш-функции $\Phi(\mathbf{S})$ в качестве дополнительного механизма защиты от атак, состоящим в решении проверочного уравнения относительно неизвестного вектора **S**. Новым в разработанном способе является то, что вычисление вектора **S** выполняется в зависимости от случайного выбора двух векторов **G** и **H** из секретной коммутативной группы, которые служат левым и правым множителями относительно некоторого фиксированного секретного вектора **V**, не принадлежащего секретной группе и некоммутативного с **G** и **H**. Благодаря использованию одной секретной коммутативной группы, обеспечивается возможность использования только одного дополнительного подгоночного элемента подписи, что приводит к уменьшению размера ЭЦП при заданном уровне стойкости.

2. Алгебраические носители алгоритма. Для постквантовых алгоритмов ЭЦП с векторным проверочным уравнением, включающим подгоночный элемент ЭЦП **S** в качестве множителя, принципиальным является обеспечение стойкости к атакам, основанным на решении указанного уравнения относительно неизвестного вектора **S**. Для реализации этого требования в работах [21, 22] используется многократное вхождение **S** в уравнение верификации, причем таким образом, что некоторая группа множителей, включающая **S**, возводится в достаточно большую степень, благодаря чему сведение

решения проверочного уравнения к решению системы скалярных степенных уравнений с координатами **S** в качестве неизвестных вычислительно неосуществимо.

Этот прием обусловливает наличие в уравнении верификации ЭЦП операций возведения в степень достаточно большого размера, что приводит к необходимости использования алгоритма быстрого возведения в степень, корректность работы которого базируется на свойстве ассоциативности операции умножения. Таким образом, в качестве носителя алгоритмов ЭЦП, основанных на вычислительной трудности решения БССУ, следует рассматривать конечные алгебраические структуры с ассоциативным умножением, в частности АНКА, в том числе, конечные алгебры матриц.

Для формирования АНКА интерес представляет способ задания в конечном векторном пространстве дополнительной операции – операции векторного умножения, обладающей свойствами замкнутости, ассоциативности и дистрибутивности слева и справа относительно операции сложения векторов. Например, операция умножения может быть определена следующим образом. Пусть конечное m-мерное векторное пространство задано над полем $GF(p)$, где p –простое число. Векторы **V** этого пространства записываются 1) в виде упорядоченного набора значений из $GF(p)$: $\mathbf{V} = (v_0, v_1, \ldots, v_{m-1})$, где $v_i \in GF(p)$ – координаты вектора; или 2) в виде суммы его компонент: $\mathbf{V} = \sum_{i=0}^{m-1} v_i \mathbf{e}_i$, где $\mathbf{e}_i$ – базисные векторы; $v_i\mathbf{e}_i$ –компоненты вектора. Естественным представляется задание результата операции умножения векторов **V** и $\mathbf{U} = \sum_{j=0}^{m-1} u_j \mathbf{e}_j$ по правилу перемножения каждой компоненты вектора **V** с каждой компонентой вектора **U**, а именно, по следующей формуле:

$$\mathbf{VU} = \sum_{i,j=0}^{m-1} v_i u_j \left(\mathbf{e}_i \mathbf{e}_j\right), \tag{1}$$

в которой требуется выполнить замену каждого произведения вида $\mathbf{e}_i\mathbf{e}_j$ некоторым базисным вектором или однокомпонентным вектором $\lambda\mathbf{e}_k$ (значение $\lambda \neq 1$ называется структурной константой). Аналогичным путем может быть задана конечная алгебра над различными расширениями простого поля $GF(p)$, в том числе над полями $GF(2^s)$, элементами которых являются двоичные многочлены степени не выше $s-1$, при различных степенях расширения s. Для разработки

алгебраических алгоритмов ЭЦП с секретной группой наиболее интересными для использования в качестве алгебраических носителей представляются АНКА, заданные над простыми полями $GF(p)$ и над полями характеристики два, т. е. расширениями двоичного поля $GF(2)$.

Для выполнения m^2 замен в формуле (1) составляется некоторая таблица умножения базисных векторов (ТУБВ). Обычно полагается, что левый множитель в произведении $\mathbf{e}_i\mathbf{e}_j$ указывает строку, а правый – столбец, на пересечении которых имеем ячейку, содержащую нужный для выполнения замены базисный вектор $\mathbf{e}_k$ или однокомпонентный вектор $\lambda\mathbf{e}_t$. На самом деле в ячейках ТУБВ можно записывать произвольные многокомпонентные векторы. Формула (1) обеспечивает свойства замкнутости и дистрибутивности умножения относительно операции сложения векторов и в этом случае. Однако задача составления ТУБВ, задающей ассоциативное некоммутативное умножение векторов, значительно упрощается, если в ячейках ТУБВ указывать только базисные и/или однокомпонентные векторы.

Известны унифицированные способы задания АНКА произвольных четных размерностей $m \geq 6$ [23] и $m \geq 2$ [24]. Алгебра квадратных матриц размерности $n \times n$, заданных над конечными полями (например, над простым полем $GF(p)$ или над расширением двоичного поля $GF(2^s)$), может быть рассмотрена как АНКА размерности $m = n^2$ с умножением, определенным по прореженным ТУБВ специального вида, составленным в соответствии с правилами матричного умножения. Для случаев алгебр матриц 2×2 и 3×3 такие ТУБВ показаны как таблицы 1 и 2 соответственно. Для разработки алгебраических алгоритмов ЭЦП с секретной группой, стойкость которых основана на вычислительной сложности решения БССУ, существенный интерес имеет также использование конечных алгебр матриц размеров 5×5 и 7×7 в качестве алгебраического носителя. Потенциально последние два варианта могут обеспечить более высокий уровень стойкости при приемлемом снижении производительности процедур генерации и верификации ЭЦП. Однако применение последних двух вариантов алгебраического носителя в данной работе не рассматривается.

Задание АНКА по прореженным (с большой долей ячеек с нулевой структурной константой) ТУБВ представляет интерес, поскольку при фиксированном значении размерности вычислительная сложность операции векторного умножения существенно меньше по сравнению со случаем использования ТУБВ без нулевых структурных констант.

Таблица 1. Трактовка умножения матриц 2×2 $||a_{ij}||$ как умножения четырехмерных векторов $A = (a_0, a_1, a_2, a_3)$, где $a_0 = a_{11}$; $a_1 = a_{12}$;$a_2 = a_{21}$; $a_3 = a_{22}$

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

Таблица 2. Трактовка умножения матриц 3×3 $||a_{ij}||$ как умножения девятимерных векторов $A = (a_0, a_1, \ldots, a_8)$, где $a_0 = a_{11}$; $a_1 = a_{12}$; $a_2 = a_{13}$; $a_3 = a_{21}$; $a_4 = a_{22}$; $a_5 = a_{23}$; $a_6 = a_{31}$; $a_7 = a_{32}$; $a_8 = a_{33}$

×	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	0	0	0	0	0	0
$\mathbf{e}_1$	0	0	0	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	0	0	0
$\mathbf{e}_2$	0	0	0	0	0	0	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	0	0	0	0	0	0
$\mathbf{e}_4$	0	0	0	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	0	0	0
$\mathbf{e}_5$	0	0	0	0	0	0	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_6$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	0	0	0	0	0	0
$\mathbf{e}_7$	0	0	0	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	0	0	0
$\mathbf{e}_8$	0	0	0	0	0	0	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$

В алгоритмах ЭЦП со скрытой (секретной) группой секретный и открытый ключи генерируются в виде наборов обратимых векторов, в которых каждый элемент открытого ключа вычисляется как произведение нескольких секретных векторов (элементов секретного ключа). Часть таких произведений включают в качестве множителей обратные значения последних. Это обстоятельство обусловливает использование (в качестве алгебраического носителя алгоритма ЭЦП) АНКА с глобальной двухсторонней единицей, обозначаемой как вектор **E**, вид которого определяется ТУББ. Способ [23] позволяет задать АНКА с глобальной двухсторонней единицей для произвольных четных размерностей $m \geq 6$. Унифицированный способ [24] позволяет задать АНКА с множеством глобальных односторонних единиц для различных четных значений размерности и только для случая $m = 4$ найдена возможность включения в ТУББ структурных констант, выбором значений которых обеспечивается наличие глобальной двухсторонней единицы (таблица 3).

Вычисление вектора $\mathbf{V}^{-1}$, обратного по отношению к вектору **V**, осуществляется путем решения системы линейных скалярных уравнений, к которой сводится векторное уравнение **XV** = **E** с неизвестным вектором **X**. Обычно в рассматриваемых алгебраических алгоритмах ЭЦП вычислительная сложность нахождения обратного вектора этим путем многократно меньше сложности операции возведения векторов в степень, выполняемой в АНКА.

С учетом определенной операции умножения векторов, предлагаемый способ рандомизации можно выразить следующей формулой:

$$\mathbf{S} = \mathbf{DGVHF}, \qquad (2)$$

где **G** и **H** – векторы, выбираемые случайным образом из секретной коммутативной группы; **D**, **V** и **F** – фиксированные секретные векторы (некоммутативные с векторами **G** и **H**).

Таблица 3. Задание операции умножения в четырехмерных АНКА с глобальной двухсторонней единицей (структурные константы λ и ε удовлетворяют неравенству$\lambda\varepsilon \neq 1$)

×	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\varepsilon\mathbf{e}_3$	$\varepsilon\mathbf{e}_0$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\lambda\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\varepsilon\mathbf{e}_1$	$\varepsilon\mathbf{e}_2$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\lambda\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_3$

3. Строение четырехмерных АНКА заданных над полями четной характеристики. При разработке алгебраических алгоритмов ЭЦП с секретной коммутативной группой, а также при выполнении их криптоанализа, важным является знание декомпозиции АНКА на множество коммутативных подалгебр. Этот вопрос достаточно подробно изучен в статьях [25, 26] для различных типов четырехмерных АНКА, заданных над простыми полями $GF(p)$ нечетной характеристики, и показана общность строения таких алгебр. В связи с предполагаемым использованием четырехмерных АНКА, заданных по таблице 1 и таблице 3 над полями четной характеристики $GF(2^s)$, авторами было изучено их строение с точки зрения декомпозиции на коммутативные подалгебры. При этом была использована методика изучения, апробированная в [25, 26]. В результате выполненного исследования была установлена общность

строения для изученных двух случаев, которая характеризуется следующими основными моментами:

1. Четырехмерная АНКА, определенная над полем $GF(2^s)$, включает $\eta = 2^{2s} + 2^s + 1$ коммутативных подалгебр, каждая из которых имеет порядок, равный 2^{2s}, и включает все скалярные векторы (т.е. векторы вида $\mathbf{L} = \alpha\mathbf{E}$, где $\alpha \in GF(2^s)$).

2. Существуют ровно три типа коммутативных подалгебр порядка 2^{2s}:

2.1. Подалгебры первого типа, содержащие мультипликативную группу, имеющую циклическое строение и порядок, равный $\Omega_1 = 2^{2s} - 1$. Число подалгебр первого типа равно $\eta_1 = 2^{s-1}(2^s - 1)$.

2.2. Подалгебры второго типа, включающие мультипликативную группу порядка $\Omega_2 = (2^s - 1)^2$, которая порождается минимальной системой образующих, включающей два вектора порядка, равного $2^s - 1$. Число подалгебр второго типа равно $\eta_2 = 2^{s-1}(2^s + 1)$.

2.3. Подалгебры третьего типа, содержащие мультипликативную группу, имеющую циклическое строение и порядок, равный $\Omega_3 = 2^s(2^s - 1)$. Число подалгебр третьего типа равно $\eta_3 = 2^s + 1$.

3. Координаты каждого из векторов $\mathbf{V} = (v_0, v_1, v_2, v_3)$ заданной подалгебры могут быть выражены через координаты любого нескалярного вектора $\mathbf{C} = (c_0, c_1, c_2, c_3)$, принадлежащего заданной подалгебре (ее представителя), и уникальную пару скалярных переменных $d, h \in GF(p)$. Вид выражения, описывающего координаты v_0, v_1, v_2 и v_3 зависит от ТУБВ, по которой задается АНКА, и от типа заданной подалгебры. В случае АНКА, заданной по таблице 1, для подалгебр первого и второго типов получена следующая формула:

$$\mathbf{V} = (v_0, v_1, v_2, v_3) = (d, h, c_2c_1^{-1}h, d + (c_3 + c_0)c_1^{-1}h). \quad (3)$$

Возможность описания коммутативной подалгебры по координатам ее представителя и две скалярные переменные имеет существенное значение при выполнении криптоанализа алгебраических алгоритмов ЭЦП, основанных на вычислительной сложности решения БССУ.

С учетом применения АНКА, заданных над полями $GF(2^s)$, в качестве алгебраического носителя разрабатываемого алгоритма ЭЦП и полученных результатов можно заметить, что степень расширения s следует выбирать с учетом получения минимального числа простых

делителей малого размера для чисел $2^s - 1$ и $2^s + 1$. Действительно последние два числа задают возможные порядки ω элементов рассматриваемых алгебр, в том числе и векторов, содержащихся в секретной коммутативной группе, а при вычислении подписи в типовых алгебраических алгоритмах ЭЦП имеет место ситуация, когда требуется вычислить обратное значение по модулю ω для случайных чисел. Последнее возможно только для чисел взаимно простых с ω. Если условие взаимной простоты не будет выполняться, то ряд шагов процедуры генерации подписи потребуется повторить при других значениях параметров рандомизации. Вероятность таких повторов может быть снижена до приемлемо малого значения, если задавать простое значение ω или значение ω, содержащее только делители достаточно большого размера (более 10 бит). В таблице 4 представлены приемлемые значения степени расширения полей $GF(2^s)$.

С учетом строения четырехмерных АНКА, заданных над полем $GF(2^s)$, и разложений чисел $2^s - 1$ и $2^s + 1$ (для всех приемлемых степеней расширения s число $2^s + 1$ делится на 3) видно, что в качестве секретной коммутативной группы целесообразно использовать мультипликативную группу подалгебры первого или второго типов. Для первого случая генерируется случайный вектор $\mathbf{J}_1$ порядка $\omega_1 = (2^{2s} - 1)/3$, выполняя следующие три шага:

1. Сгенерировать случайный вектор $\mathbf{V}$ и вычислить вектор $\mathbf{W} = \mathbf{V}^3$.

2. Для каждого простого делителя d числа ω_1 вычислить натуральное число $\sigma = \omega_1/d$ и проверить выполнимость неравенства $\mathbf{W}^\sigma \neq \mathbf{E}$. Если хотя бы для одного нетривиального делителя d имеет место равенство $\mathbf{W}^\sigma = \mathbf{E}$, то перейти к шагу 1.

3. Взять вектор $\mathbf{W}$ в качестве вектора $\mathbf{J}_1$, имеющего порядок ω_1.

С учетом того, что число подалгебр первого типа равно $\eta_1 = 2^{s-1}(2^s - 1)$, легко установить, что цикл, включающий первые два шага, в среднем будет выполняться ≈2 раза. Выбор случайных векторов $\mathbf{G}$ из секретной группы осуществляется путем генерации случайного натурального числа $k < \omega_1$ и вычисления вектора $\mathbf{G} = \mathbf{J}_1^k$.

Чтобы задать в качестве секретной коммутативной группы мультипликативную группу подалгебры второго типа, генерируется нескалярный случайный вектор $\mathbf{J}_2$ порядка $\omega_2 = 2^s - 1$, выполняя следующие три шага:

1. Сгенерировать случайный нескалярный вектор $\mathbf{V}$.

2. Для каждого простого делителя d числа ω_2 вычислить натуральное число $\sigma = \omega_2/d$ и проверить выполнимость неравенства $\mathbf{V}^{\sigma} \neq \mathbf{E}$. Если хотя бы для одного нетривиального делителя d имеет место равенство $\mathbf{V}^{\sigma} = \mathbf{E}$, то перейти к шагу 1.

3. Взять вектор $\mathbf{W}$ в качестве вектора $\mathbf{J}_2$, имеющего порядок ω_2.

С учетом того, что число подалгебр второго типа равно $\eta_2 = 2^{s-1}(2^s + 1)$, легко установить, что цикл, включающий первые два шага, в среднем будет выполняться ≈ 2 раза. Выбор случайных векторов $\mathbf{G}$ из секретной группы осуществляется путем генерации двоичного многочлена α, являющегося примитивным элементом поля $GF(2^s)$, и случайных натуральных чисел $t < \omega_2$ и $u < \omega_2$ с последующим вычислением вектора $\mathbf{G} = \alpha^t \mathbf{J}_2^k$ (заметим, что фиксированное значение α может использоваться для случайного выбора многих различных векторов).

Таблица 4. Приемлемые значения степени расширения s для задания четырехмерных АНКА над полями $GF(2^s)$

Степень s	Число простых делителей (и их размер, бит)	
	для значения $2^s - 1$	для значения $(2^s + 1)/3$
61	1 (61)	1 (60)
67	2 (28 и 40)	2 (23 и 43)
71	3 (18, 26 и 28)	2 (26 и 44)
79	3 (12, 28 и 41)	1 (78)
101	2 (43 и 59)	1 (100)
103	2 (32 и 72)	2 (39 и 63)
109	2 (30 и 80)	2 (27 и 81)
127	1 (127)	1 (126)
137	2 (65 и 73)	4 (11, 14, 55 и 57)
139	2 (43 и 97)	2 (23 и 116)
149	2 (67 и 83)	4 (11, 20, 26 и 93)
181	4 (16, 21, 23 и 123)	3 (11, 25 и 144)
193	3 (24, 76 и 94)	4 (13, 26, 71 и 84)
197	2 (13 и 185)	2 (98 и 98)
199	2 (38 и 162)	1 (198)
211	3 (14, 66 и 132)	5 (13, 24, 33, 38 и105)
223	6 (15, 18, 21, 22, 71 и 79)	2 (38 и 184)
227	2 (55 и 173)	3 (19, 62 и 146)
229	4 (21, 25, 56 и 129)	2 (25 и 204)
241	2 (25 и 217)	3 (12, 88 и 142)
257	3 (49, 80 и 129)	2 (69 и 187)

4. Атака на основе известных подписей. Алгебраические алгоритмы ЭЦП, стойкость которых базируется на вычислительной сложности решения БССУ, относятся к недетерминированным схемам ЭЦП. Используемый в них механизм рандомизации подписи оставляет принципиальную возможность вычисления элементов секретного ключа, входящих в формулу для вычисления подгоночного элемента подписи **S**. Это означает, что при разработке алгоритмов такого типа требуется выполнить оценку стойкости к атакам на основе известных подписей. Если вычислительная сложность такой атаки достаточно высока, то рандомизацию ЭЦП можно считать достаточно полной [22]. Способ выполнения оценки сложности атаки на основе известных подписей рассматривается в работе [22]. Применяя этот способ к алгоритму ЭЦП, использующему рандомизацию подписи по формуле (2), получаем следующую модель атаки.

При наличии z известных подписей имеем z векторных уравнений, в каждом из которых присутствуют фиксированные неизвестные векторные значения **D**, **V** и **F** (элементы секретного ключа) и уникальные неизвестные **G** и **H**, выбираемые случайным образом из коммутативной секретной группы. Тот факт, что выбор уникальных неизвестных осуществляется из существенно ограниченного множества элементов АНКА, используемой в качестве алгебраического носителя, обусловливает недостаточность рандомизации элемента подписи **S**. При наличии некоторого набора известных подписей вычисление фиксированных секретных векторов **D**, **V** и **F** может быть в принципе выполнено путем сведения решения системы из z векторных степенных уравнений к решению системы из $4z$ скалярных степенных уравнений. При этом выбор каждого из случайных векторов **G** и **H** потенциально может быть описан через $\mu < m$ скалярных неизвестных (уникальных для каждой известной подписи), если задан некоторый нескалярный вектор **C** из секретной коммутативной группы.

Пусть имеются известные подписи с подгоночными элементами $\mathbf{S}_i$, где $i = 1, 2, \ldots, z$, причем $\mathbf{S}_i$ вычислено по паре уникальных значений $\mathbf{G}_i$ и $\mathbf{H}_i$ из секретной группы. Рассматривая вектор $\mathbf{G}_1$ в качестве представителя секретной группы каждый из случайных векторов $\mathbf{G}_i$ для $i = 2, 3, \ldots, z$ и векторов $\mathbf{H}_i$ для $i = 1, 2, \ldots, z$ может быть описан через μ скалярных неизвестных. С учетом этого, по z известным подписям можно записать zm скалярных уравнений с $4m$ фиксированными скалярными неизвестными (которыми являются координаты секретных векторов **D**, **V**, **F** и координаты неизвестного представителя секретной группы $\mathbf{G}_1$) и $\mu + 2\mu(z - 1)$ уникальными

скалярными неизвестными. С увеличением значения z число уравнений растет быстрее, чем число неизвестных. Натуральное значение z_0, удовлетворяющее уравнению

$$z_0 m = 4m + \mu + 2\mu(z_0 - 1), \tag{4}$$

может быть принято за число необходимых для выполнения атаки известных подписей, а сложность решения системы из $z_0 m$ степенных уравнений в поле $GF(p)$ с $z_0 m$ неизвестными – за стойкость алгоритма ЭЦП с механизмом рандомизации по формуле (2).

Значение μ зависит от размерности используемого алгебраического носителя и от декомпозиции последнего на коммутативные подалгебры. Строение ряда четырехмерных АНКА с глобальной двухсторонней единицей (в том числе алгебры матриц 2×2), заданных над $GF(p)$, с точки зрения декомпозиции на коммутативные подалгебры порядка p^2 хорошо изучено, показана общность их строения и получены формулы, включающие две скалярные переменные и описывающие по координатам заданного представителя подалгебры все содержащиеся в ней векторы [25].

С учетом результатов выполненного исследования строения четырехмерных АНКА, заданных по таблице 1 и таблице 3 над полями четной характеристики $GF(2^s)$, легко видеть, что и в этом случае имеется возможность описать выбор вектора из заданной подалгебры по координатам представителя последней и двум скалярным переменным, принимающих значения в $GF(2^s)$.

Таким образом, при использовании в качестве алгебраического носителя конечных алгебр, заданных по таблицам 1 и 3, в рассмотренной модели атаки следует принять значение $\mu = 2$, при котором условие (4) не выполняется ни при каких значениях z_0. С учетом существенной неоднозначности получаемых решений можно принять вывод, что при применении четырехмерных АНКА с глобальной двухсторонней единицей формула (2) обеспечивает достаточно полную рандомизацию подписи.

Строение девятимерной АНКА, заданной по таблице 2, может быть исследовано по способу, примененному в работе [25]. Это составляет задачу независимого рассмотрения, однако получение значения μ для этого случая представляется уместным. Все элементы коммутативной подалгебры, содержащей нескалярный девятимерный вектор $\mathbf{C}$, могут быть найдены как решения системы из девяти скалярных линейных уравнений, соответствующей векторному уравнению $\mathbf{CX} = \mathbf{XC}$. Главный определитель системы скалярных

уравнений имеет ранг 6, т.е. пространство решений имеет размерность три и, следовательно, описывается по координатам вектора **C** формулой, включающей три скалярные переменные, т.е. имеем $\mu = 3$. При $m = 9$ и $\mu = 3$ уравнение (4) имеет решение $z_0 = 11$, что в рамках атаки на основе известных подписей соответствует решению системы из 99 степенных уравнений в поле $GF(p)$. Для лучших известных алгоритмов решения систем степенных уравнений оценка сложности решения этой задачи при числе уравнений, равном 99, составляет не менее 2^{256} даже в полях сравнительно малого порядка, а именно в полях $GF(256)$ [13]. Таким образом, при использовании конечной алгебры матриц 3×3 в качестве алгебраического носителя алгоритмы ЭЦП с рандомизацией подписи по формуле (2) также обеспечивают высокий уровень стойкости к атаке на основе известных подписей.

5. Разработанный алгоритм ЭЦП. Решение уравнений с многократным вхождением неизвестной, заданных в конечной некоммутативной алгебре может быть выполнено путем сведения к системе скалярных степенных уравнений, если неизвестный вектор (или некоторое выражение, куда он входит) возводится в сравнительно малую степень. В случае степени, имеющей разрядность 32 бит и более, это представляет собой вычислительно трудную задачу. Задание в проверочном уравнении хотя бы одной операции возведения в степень большой разрядности является приемом обеспечения стойкости к атакам, связанным с решением проверочного уравнения относительно подгоночного элемента подписи **S** как неизвестной. Другим приемом достижения такой цели является использование в проверочном уравнении операции возведения в степень, зависящую от значения **S** (например, вычисляемую как хеш-функция от **S**), в результате чего проверочное уравнение приобретает вид экспоненциального уравнения.

В разработанном алгебраическом алгоритме ЭЦП используются оба указанных приема, обеспечивая высокую стойкость к указанным атакам. При этом предполагается использование алгебраических носителей различных типов:

1. четырехмерных АНКА, заданных по таблице 1 над простым полем $GF(p)$ при 128-битном простом порядке p;

2. четырехмерных АНКА, заданных по таблице 1 или таблице 3 над расширением двоичного поля $GF(2^s)$ при степени $s = 127$, которая обеспечивает наличие в разложениях чисел $2^s + 1$ и $2^s - 1$ только достаточно больших простых делителей за исключением числа 3, которое является делителем числа $2^s + 1$ при натуральных

значениях s, соответствующих приемлемому разложению значения $2^s - 1$;

3. девятимерной АНКА (алгебры матриц 3×3), заданной по таблице 2 над простым полем $GF(p)$ при 64-битном простом порядке p.

При использовании четырехмерной АНКА, заданной над полем $GF(p)$, в качестве порядка поля используется простое число вида $p = 2q + 1$, где q – 127-битное простое число. Генерация такого числа p выполняется методом подбора 127-битных простых значений q до тех пор, пока вычисленное по указанной формуле число p не будет простым. В качестве секретной группы берется подгруппа мультипликативной группы коммутативной подалгебры третьего типа. Для задания секретной группы генерируется случайный вектор (элемент секретного ключа) $\mathbf{J}$, порядок которого равен числу $\omega = pq$, по следующему алгоритму:

1. Выбрать случайные элементы h и d поля $GF(p)$, такие, что h имеет порядок q, а d отличен от нуля и единицы.

2. Сгенерировать случайный вектор $\mathbf{V}$ и вычислить вектор $\mathbf{J} = \mathbf{V}\mathbf{J}'\mathbf{V}^{-1}$, где вектор $\mathbf{J}' = (h, d, 0, h)$ имеет порядок $\omega = pq$ (действительно, легко показать, что $\mathbf{J}'^{\omega} = \mathbf{E}$,$\mathbf{J}'^{p} \neq \mathbf{E}$ и $\mathbf{J}'^{q} \neq \mathbf{E}$).

3. Взять вектор $\mathbf{J}$ в качестве элемента секретного ключа.

При использовании четырехмерной АНКА, заданной над полем $GF(2^s)$, берется значение $s = 127$, при котором имеем:

$2^s - 1 =$ 170141183460469231731687303715884105727 – 127-битное простое число;

$(2^s + 1)/3 =$ 56713727820156410577229101238628035243 –126-битное простое число.

В качестве секретной группы задается подгруппа мультипликативной группы коммутативной подалгебры первого типа. Для этого генерируется случайный вектор $\mathbf{J}$ порядка $\omega = (2^{2s} - 1)/3$, равного произведению двух простых чисел длины 126 и 127 бит. Вектор $\mathbf{J}$ используется как генератор секретной циклической группы.

При использовании в качестве алгебраического носителя девятимерной АНКА, заданной по таблице 2 над полем $GF(p)$, используется 64-битое простое вида$p = 2q + 1$, где q –простое число, при этом p таково, что число $r = p^2 + p + 1$ является простым. При этом генератором секретной группы служит вектор $\mathbf{J}$ порядка $\omega = r$. Примеры подходящих простых значений p представлены в таблице 5 (где знак «\\» обозначает перенос записи числа в следующую строку). Простое p, соответствующее приведенным двум формулам, формируется путем многократной (в среднем не более 10^3 раз для разрядности p до 96 бит) генерации различных простых 63-битных

чисел q и проверкой на простоту чисел p и r, вычисляемых по двум указанным выше формулам.

Таблица 5. Примеры подходящих значений p (для различных значений разрядности) и соответствующие простые делители порядка ω

Значение p (длина в битах)	Простые делители ω (и их длина, бит)	
	q	r
959171755463 (40)	479585877731 (39)	9200104564789322\\ 42099833 (80)
25271244599\\ 5463 (48)	12635622299\\ 7731 (47)	6386358036101005597\\ 7462579833 (96)
36802238809\\ 418339 (56)	1840111940\\ 4709169 (55)	1354404781385457398\\ 845650318937261 (111)
133147932671\\ 28944783 (64)	1769732813521\\ 900658699 (63)	177283719746382279559\\ 337772146191861873 (128)
5021288074440\\ 707076923 (72)	2510644037220\\ 353538461 (71)	1252781692502456964370\\ 7613109378931741442601 (144)
12045013962879\\ 22323235223 (80)	60225069814396116 1617611 (79)	14508236136595544966\\ 3567914846118052214 37\\ 11094953 (160)
431629884442508\\ 29318249230143 (96)	21581494222125414 659124615071 (95)	1863043571438530627066\\ 0787533384672970059 00\\ 409930429030593 (191)
2669778488756826071 8840929163053897581 9 (128)	13348892443784\\ 130359420464581\\ 5269487909 (127)	7127717179028682076320171 49\\ 7774134208043365636618092703\\ 461567797650400569658 1 (256)
8966932799355719\\ 59062298173795513\\ 824251385322239 (160)	4483466399677\\ 8597953114908\\ 68977569121256\\ 92661119 (159)	8040588382816140172 99\\ 346720056488863119472\\ 580173974350750961605 5\\ 251382109146283579 33\\ 457253295361 (319)

В разработанном алгоритме ЭЦП в качестве секретного ключа служат натуральные числа u, w, x, y, z, каждое из которых меньше значения ω, и набор попарно некоммутативных обратимых векторов **A**, **B**, **D**, **F**, **J** и **V**, генерируемых случайным образом, причем значение z является взаимно простым с ω и порядок вектора **J** равен ω. Открытый ключ представляет собой набор из девяти векторов (**U**, **Y**, **Z**, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$, $\mathbf{T}_5$, $\mathbf{T}_6$), которые вычисляются по следующим формулам:

$$\mathbf{U} = \mathbf{D}\mathbf{J}^{z}\mathbf{D}^{-1},\ \mathbf{Y} = \mathbf{A}\mathbf{J}\mathbf{A}^{-1},\ \mathbf{Z} = \mathbf{B}^{-1}\mathbf{J}^{-1}\mathbf{B}, \tag{5}$$

$$\mathbf{T}_1 = \mathbf{A}\mathbf{J}^{u}\mathbf{D}^{-1},\ \mathbf{T}_2 = \mathbf{F}^{-1}\mathbf{J}^{y}\mathbf{V}^{-1}\mathbf{A}^{-1},\ \mathbf{T}_3 = \mathbf{F}^{-1}\mathbf{J}^{x}\mathbf{V}^{-1}\mathbf{A}^{-1}, \tag{6}$$

$$\mathbf{T}_4 = \mathbf{AVJ}^{w}\mathbf{V}^{-1}\mathbf{B},\ \mathbf{T}_5 = \mathbf{B}^{-1}\mathbf{VJ}^{z}\mathbf{F},\ \mathbf{T}_6 = \mathbf{DJ}^{-u}\mathbf{B}. \quad (7)$$

Длина секретного (открытого) ключа составляет ≈540 (580) и ≈550 (650) байт в случае реализации алгоритма на четырехмерных и девятимерных АНКА соответственно.

Процедура формирования ЭЦП к документу M осуществляется с использованием секретного ключа и включает следующую последовательность шагов:

1. Сгенерировать случайные натуральные числа k и t ($1 < k < \omega$; $1 < t < \omega$) и вычислить рандомизирующий вектор (вектор-фиксатор)

$$\mathbf{R} = \mathbf{AJ}^{k}\mathbf{VJ}^{t}\mathbf{V}^{-1}\mathbf{B}. \quad (8)$$

2. Используя 512-битную коллизионно стойкую хеш-функцию Ф, вычислить рандомизирующий элемент подписи в виде 512-битного хеш-значения $e = e_1 \| e_2 = \Phi(M \| \mathbf{R})$, представленного в виде конкатенации двух 256-битных строк, представляющих числа e_1 и e_2. Если наибольший общий делитель чисел $e_1 - e_2 + 1$ и ω не равен единице, то перейти к шагу 1 (вероятность этого пренебрежимо мала (менее 2^{-60}), поэтому эта теоретическая возможность практически не влияет на среднюю производительность процедуры вычисления ЭЦП).

3. Вычислить натуральные значения n и d:

$$n = -e_1 - u \bmod \omega,\quad d = \frac{t - ze_2 - xe_1 - w - y}{e_1 - e_2 + 1} \bmod \omega. \quad (9)$$

4. Вычислить подгоночный элемент подписи в виде вектора $\mathbf{S}$ по формуле

$$\mathbf{S} = \mathbf{DJ}^{n}\mathbf{VJ}^{d}\mathbf{F}. \quad (10)$$

5. Вычислить значение хеш-функции $\Phi(\mathbf{S})$ и натуральное число $\rho = \Phi(\mathbf{S}) \bmod \omega$.

6. Вычислить вспомогательный подгоночный элемент подписи в виде натурального числа σ по формуле

$$\sigma = z^{-1}(k - \rho - u - n) \bmod \omega. \quad (11)$$

7. Выдать тройку значений $(e, \sigma, \mathbf{S})$ в качестве сгенерированной ЭЦП.

Вычислительная сложность процедуры генерации ЭЦП определяется главным образом четырьмя операциями экспоненциирования, выполняемыми в АНКА, используемой в качестве алгебраического носителя. В случае реализации алгоритма на четырехмерной и девятимерной АНКА указанная сложность равна ≈12300 и ≈15500 операций умножения в конечном поле, над которым задана АНКА, соответственно. Размер подписи равен 160 (168) байт в случае реализации алгоритма на четырехмерных (девятимерных) АНКА.

Процедура верификации ЭЦП $(e, \sigma, \mathbf{S})$ к документу M выполняется с использованием открытого ключа по следующему алгоритму:

1. Вычислить значение $\rho = \Phi(\mathbf{S}) \bmod \omega$ и контрольный вектор $\mathbf{R}'$ по формуле

$$\mathbf{R}' = \mathbf{Y}^{\rho}\mathbf{T}_1\mathbf{U}^{\sigma}\mathbf{S}\mathbf{T}_2\left(\mathbf{Y}^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{T}_3\right)^{e_1}\mathbf{T}_4\left(\mathbf{T}_5\mathbf{S}^{-1}\mathbf{T}_6\mathbf{Z}^{e_1}\right)^{e_2}. \qquad (12)$$

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

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

Вычислительная сложность процедуры верификации ЭЦП определяется шестью операциями возведения в степень, выполняемыми в АНКА, используемой в качестве алгебраического носителя. В случае реализации алгоритма на четырехмерной и девятимерной АНКА трудоемкость равна ≈18500 и ≈23300 операций умножения в конечном поле, над которым задана АНКА, соответственно.

Корректность работы предложенного алгоритма доказывается как факт того, что подпись $(e, \sigma, \mathbf{S})$, вычисленная в соответствии с процедурой генерации подписи, верифицируется как подлинная ЭЦП. Действительно, с учетом формул (5)–(11) и хорошо известного равенства $(\mathbf{X}\mathbf{J}\mathbf{X}^{-1})^{x} = \mathbf{X}\mathbf{J}^{x}\mathbf{X}^{-1}$ из проверочного уравнения (12) получаем:

$$\mathbf{R}' = \left(\mathbf{AJA}^{-1}\right)^{\rho}\mathbf{AJ}^{u}\mathbf{D}^{-1}\left(\mathbf{DJ}^{z}\mathbf{D}^{-1}\right)^{\sigma}\left(\mathbf{DJ}^{n}\mathbf{VJ}^{d}\mathbf{F}\right)\mathbf{F}^{-1}\mathbf{J}^{y}\mathbf{V}^{-1}\mathbf{A}^{-1}\times$$

$$\times\left[\left(\mathbf{AJA}^{-1}\right)^{e_1}\mathbf{AJ}^{u}\mathbf{D}^{-1}\left(\mathbf{DJ}^{n}\mathbf{VJ}^{d}\mathbf{F}\right)\mathbf{F}^{-1}\mathbf{J}^{x}\mathbf{V}^{-1}\mathbf{A}^{-1}\right]^{e_1}\mathbf{AVJ}^{w}\mathbf{V}^{-1}\mathbf{B}\times$$

$$\times\left[\mathbf{B}^{-1}\mathbf{VJ}^{z}\mathbf{F}\left(\mathbf{F}^{-1}\mathbf{J}^{-d}\mathbf{V}^{-1}\mathbf{J}^{-n}\mathbf{D}^{-1}\right)\mathbf{DJ}^{-u}\mathbf{B}\left(\mathbf{B}^{-1}\mathbf{J}^{-1}\mathbf{B}\right)^{e_1}\right]^{e_2} =$$

$$= \mathbf{AJ}^{\rho+u+z\sigma+n}\mathbf{VJ}^{d+y}\mathbf{V}^{-1}\mathbf{A}^{-1}\left(\mathbf{AJ}^{e_1+u+n}\mathbf{VJ}^{d+x}\mathbf{V}^{-1}\mathbf{A}^{-1}\right)^{e_1}\mathbf{AVJ}^{w}\mathbf{V}^{-1}\mathbf{B}\times$$

$$\times\left(\mathbf{B}^{-1}\mathbf{VJ}^{z-d}\mathbf{V}^{-1}\mathbf{J}^{-n-u-e_1}\mathbf{B}\right)^{e_2} = \mathbf{AJ}^{\rho+u+z\sigma+n}\mathbf{VJ}^{d+y}\mathbf{V}^{-1}\mathbf{A}^{-1}\times$$

$$\times\left(\mathbf{AJ}^{0}\mathbf{VJ}^{d+x}\mathbf{V}^{-1}\mathbf{A}^{-1}\right)^{e_1}\mathbf{AVJ}^{w}\mathbf{V}^{-1}\mathbf{B}\left(\mathbf{B}^{-1}\mathbf{VJ}^{z-d}\mathbf{V}^{-1}\mathbf{J}^{0}\mathbf{B}\right)^{e_2} =$$

$$= \mathbf{AJ}^{\rho+u+z\sigma+n}\mathbf{VJ}^{d+y}\mathbf{V}^{-1}\mathbf{A}^{-1}\left(\mathbf{AVJ}^{d+x}\mathbf{V}^{-1}\mathbf{A}^{-1}\right)^{e_1}\mathbf{AVJ}^{w}\mathbf{V}^{-1}\mathbf{B}\times$$

$$\times\left(\mathbf{B}^{-1}\mathbf{VJ}^{z-d}\mathbf{V}^{-1}\mathbf{B}\right)^{e_2} =$$

$$= \mathbf{AJ}^{\rho+u+(k-\rho-u-n)+n}\mathbf{VJ}^{d+y+e_1(d+x)+w+e_2(z-d)}\mathbf{V}^{-1}\mathbf{B} =$$

$$= \mathbf{AJ}^{k}\mathbf{VJ}^{d(1+e_1-e_2)+y+e_1x+w+e_2z}\mathbf{V}^{-1}\mathbf{B} = \mathbf{AJ}^{k}\mathbf{VJ}^{t}\mathbf{V}^{-1}\mathbf{B} = \mathbf{R}.$$

С учетом полученного равенства $\mathbf{R} = \mathbf{R}'$ имеем $e' = \Phi(M\|\mathbf{R}') = \Phi(M\|\mathbf{R}) = e$, т. е. корректно вычисленная подпись проходит процедуру верификации как подлинная ЭЦП.

6. Обсуждение. Постквантовая стойкость разработанного алгоритма ЭЦП обеспечивается тем, что она базируется на вычислительной сложности решения БССУ, для чего квантовый компьютер не является эффективным. Атака, состоящая в решении системы уравнений, связывающих координаты векторов, составляющих открытый ключ, с координатами секретных векторов, являющихся элементами секретного ключа, называется прямой атакой. Такая система записывается по формулам (5), (6) и (7), представляя каждое степенное векторное уравнение в виде системы из m скалярных уравнений. При $m = 4$ ($m = 9$) имеем 36 (81) скалярных уравнений второй и более высоких степеней.

С учетом того, что секретные векторы **A**, **B**, **D**, **F**, **J** и **V** в случае четырехмерных АНКА задают 24 скалярных неизвестных, а координаты каждого из неизвестных векторов $\mathbf{J}^{u}$,$\mathbf{J}^{w}$, $\mathbf{J}^{x}$, $\mathbf{J}^{y}$ и $\mathbf{J}^{z}$ могут быть представлен через координаты представителя секретной группы **J** и две уникальных скалярных неизвестных, то в системе из 36 степенных

уравнений имеются 34 скалярные неизвестные (система является переопределенной, но она имеет хотя бы одно решение по построению).

В случае девятимерных векторов координаты каждого из неизвестных векторов $\mathbf{J}^u$,$\mathbf{J}^w$, $\mathbf{J}^x$, $\mathbf{J}^y$ и $\mathbf{J}^z$ могут быть представлен через координаты представителя секретной группы $\mathbf{J}$ и три уникальных скалярных неизвестных, то в системе из 81 степенного уравнения имеются 69 скалярных неизвестных. Используя оценки трудоемкости решения больших систем степенных уравнений [13] при равенстве числа уравнений и неизвестных для случаев $m = 4$ и $m = 9$ получаем оценки уровня стойкости к прямой атаке $>2^{100}$ и $>2^{192}$ соответственно. Стойкость к атакам на основе известных подписей превышает уровень стойкости к прямой атаке, что позволяет сделать вывод о достаточной полноте рандомизации подписи, обеспечиваемой в разработанном алгоритме.

Подделка подписи к документу M' для разработанного алгебраического алгоритма ЭЦП теоретически может быть выполнена путем генерации случайного обратимого вектора $\mathbf{R}'$, выбора случайного значения σ и вычисления значения $e = e_1 \| e_2 = \Phi(M' \| \mathbf{R}')$ с последующим решением проверочного уравнения относительно вектора $\mathbf{S}$ как неизвестной. Действительно, если решение проверочного уравнения будет найдено, то легко видеть, что подпись $(e, \sigma, \mathbf{S})$, сгенерированная таким путем пройдет проверочную процедуру как подлинная подпись. Однако в разработанном алгоритме используются два различных механизма задания вычислительной невозможности решения уравнения верификации относительно неизвестного значения подгоночного элемента подписи $\mathbf{S}$.

Если атаку по подделке подписи попытаться выполнить путем генерации случайного обратимого вектора $\mathbf{R}'$, выбора случайного вектора $\mathbf{S}$ и вычисления значений $\rho = \Phi(\mathbf{S}) \bmod \omega$ и $e = e_1 \| e_2 = \Phi(M' \| \mathbf{R}')$ с последующим решением проверочного уравнения относительно натурального значения σ как неизвестной, то легко показать, что решение возникающего на последнем шаге уравнения существует с пренебрежимо малой вероятностью, не более 2^{-127}. Действительно, относительно неизвестной $\mathbf{U}^\sigma$ рассматриваемое уравнение имеет единственное решение $\mathbf{N}$, которое попадает в коммутативную подалгебру, содержащую элемент открытого ключа $\mathbf{U}$ с вероятностью $1/\eta_1 \approx 2^{-255}$ $(1/\eta_2 \approx 2^{-255})$, если $\mathbf{U}$ принадлежит подалгебре первого (второго) типа, или с вероятностью $1/\eta_3 \approx 2^{-127}$, если $\mathbf{U}$ принадлежит подалгебре третьего типа. При этом вероятность того, что при формировании открытого ключа будет реализовано последнее событие равна $p^{-1} \approx 2^{-128}$.

Предложенный механизм рандомизации ЭЦП, так же как и его аналог [21], обеспечивает уровень стойкости к атакам на основе известных подписей не менее уровня стойкости к прямым атакам. При одинаковой стойкости к прямым атакам, равной 2^{192}, вычислительная сложность процедура генерации (верификации) разработанного алгоритма ЭЦП равна ≈15500 (≈23300) умножений в поле $GF(p)$, что меньше соответствующих значений алгоритма ЭЦП [21], равных ≈36000 (≈55000) умножений в поле $GF(p)$. При этом размер ЭЦП в разработанном алгоритме составляет 168 байт, что на 19,2% меньше размера подписи, равного 208 байт, в алгоритме [21].

9. Заключение. Предложенный новый механизм рандомизации в алгебраических схемах ЭЦП с секретной группой, стойкость которых базируется на вычислительной сложности решения БССУ, обеспечивает стойкость к атаке на основе известных подписей, превышающую стойкость к прямой атаке (устранение основной предпосылки для потенциальной уязвимости к атаке на основе известных подписей) и позволяет уменьшить размер подписи для заданного уровня стойкости. На основе указанного способа разработан новый алгоритм ЭЦП, представляющий интерес как практичная постквантовая криптосхема. Элементы техники его построения представляют интерес для разработки прототипа алгебраического постквантового стандарта ЭЦП, относящегося к многомерной криптографии. Для повышения уровня стойкости представляет интерес реализация алгебраических алгоритмов данного типа на АНКА больших размерностей, в том числе на алгебрах матриц 5×5 и 7×7, заданных над простыми конечными полями $GF(p)$ с 32-битным порядком p, а также над полями $GF(2^s)$ со значениями $s = 16–64$, однако это представляет задачу самостоятельного исследования.

Становление нового направления в области постквантовой криптографии, связанного с разработкой алгебраических алгоритмов цифровой подписи стало возможным благодаря вниманию и поддержке выдающегося ученого в области информатики, информационных технологий и теории управления, д.т.н, члена-корр. РАН, заслуженного деятеля науки и техники РФ Юсупова Рафаэля Мидхатовича многих инициативных начинаний сотрудников СПИИРАН, работающих в области криптографии. В сердцах авторов и его ближайших коллег благодарная память об этом останется навсегда.

Литература

1. Saarinen M.J., Smith-Tone D. Post-Quantum Cryptography. 15-th International Conference, PQCrypto 2024, Oxford, UK, 2024, Proceedings Part I // Lecture Notes in Computer Science. Springer, Cham, 2024. 434 p. DOI: 10.1007/978-3-031-62743-9.

2. Johansson T., Smith-Tone D. Post-Quantum Cryptography. 14-th International Conference, PQCrypto 2023, College Park, MD, USA, Proceedings // Lecture Notes in Computer Science. Springer, Cham, 2023. 714 p. DOI: 10.1007/978-3-031-40003-2.
3. Yan S.Y. Quantum Computational Number Theory. Springer. 2015. 252 p. DOI: 10.1007/978-3-319-25823-2.
4. Yan S.Y. Quantum Attacks on Public-Key Cryptosystems. Springer. 2014. 207 p. DOI: 10.1007/978-1-4419-7722-9.
5. Battarbee C., Kahrobaei D., Perret L., Shahandashti S.F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures // Post-Quantum Cryptography. PQCrypto 2023. Lecture Notes in Computer Science. Springer, Cham, 2023. vol. 14154. DOI: 10.1007/978-3-031-40003-2_5.
6. Alamelou Q., Blazy O., Cauchie S., Gaborit P. A code-based group signature scheme // Designs, Codes and Cryptography. 2017. vol. 82. pp. 469–493. DOI: 10.1007/s10623-016-0276-6.
7. Kosolapov Y.V., Turchenko O.Y. On the construction of a semantically secure modification of the McEliece cryptosystem // Prikladnaya Diskretnaya Matematika. 2019. no. 45. pp. 33−43. DOI: 10.17223/20710410/45/4.
8. Gärtner J. NTWE: A Natural Combination of NTRU and LWE // Post-Quantum Cryptography. PQCrypto 2023. Lecture Notes in Computer Science, Springer, Cham, 2023. vol. 14154. DOI: 10.1007/978-3-031-40003-2_12.
9. Lysakov I.V. Solving some cryptanalytic problems for lattice-based cryptosystems with quantum annealing method // Matematicheskie Voprosy Kriptografii [Mathematical Aspects of Cryptography]. 2023. vol. 14. no. 2. pp. 111–122. DOI: 10.4213/mvk441.
10. Hamlin B., Song F. Quantum Security of Hash Functions and Property-Preservation of Iterated Hashing. Post-Quantum Cryptography. PQCrypto 2019. Lecture Notes in Computer Science. Springer, Cham, 2019. vol. 11505. pp. 329–349. DOI: 10.1007/978-3-030-25510-7_18.
11. Agibalov G.P. ElGamal cryptosystems on Boolean functions // Prikladnaya Diskretnaya Matematika. 2018. no. 42. pp. 57–65. DOI: 10.17223/20710410/42/4.
12. Shuaiting Q., Wenbao H., Yifa Li, Luyao J. Construction of Extended Multivariate Public Key Cryptosystems // International Journal of Network Security. 2016. vol. 18. no. 1. pp. 60–67.
13. Ding J., Petzoldt A. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. vol. 15. no. 4. pp. 28–36.
14. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York, NY, 2020. vol. 80. pp. 7–23. DOI: 10.1007/978-1-0716-0987-3_2.
15. Cartor R., Cartor M., Lewis M., Smith-Tone D. IPRainbow // Post-Quantum Cryptography. Lecture Notes in Computer Science. Springer, Cham, 2022. vol. 13512. pp. 170–184. DOI: 10.1007/978-3-031-17234-2_9.
16. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. no. 3(103). pp. 80–89. DOI: 10.56415/basm.y2023.i3.p80.
17. Moldovyan N.A. Parameterized method for specifying vector finite fields of arbitrary dimensions // Quasigroups and related systems. 2024. vol. 32. no. 2. pp. 299–312. DOI: 10.56415/qrs.v32.21.
18. 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: 10.56415/qrs.v30.24.
19. Moldovyan D.N. A new type of digital signature algorithms with a hidden group // Computer Science Journal of Moldova. 2023. vol. 31. no. 1(91). pp. 111–124. DOI: 10.56415/csjm.v31.06.

20. Молдовян А.А., Молдовян Д.Н., Молдовян Н.А. Постквантовые двухключевые криптосхемы на конечных алгебрах // Информатика и автоматизация. 2024. Т. 23. № 4. С. 1246–1276. DOI: 10.15622/ia.23.4.12.
21. Молдовян Н.А, Петренко А.С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2024. № 6(64). С. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
22. Молдовян Н.А, Петренко А.С. Типовые уравнения верификации в схемах ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2025. № 3(67). С. 45–54. DOI: 10.21681/2311-3456-2025-3-XX-XX. (в печати)
23. Moldovyan N.A. Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and Related Systems. 2018. vol. 26. no. 2. pp. 263–270.
24. 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 and Computer Software (Bulletin SUSU MMCS). 2019. vol. 12. no. 1. pp. 66–81. DOI: 10.14529/mmp190106.
25. 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. DOI: 10.56415/qrs.v30.11.
26. Duong M.T., Moldovyan A.A., Moldovyan D.N., Nguyen M.H., Do B.T. Structure of quaternion-type algebras and a post-quantum signature algorithm // International Journal of Electrical and Computer Engineering (IJECE). 2025. vol. 15. no. 3. pp. 2965–2976. DOI: 10.11591/ijece.v15i3.pp2965-2976.

Молдовян Александр Андреевич — д-р техн. наук, профессор, главный научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН). Область научных интересов: криптография, постквантовые криптоалгоритмы с открытым ключом, электронная цифровая подпись, криптографические протоколы, компьютерная безопасность. Число научных публикаций — 200. maa1305@yandex.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-7181.

Молдовян Дмитрий Николаевич — канд. техн. наук, доцент кафедры, кафедра информационных систем, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ». Область научных интересов: криптография, постквантовые двухключевые криптоалгоритмы на алгебрах и нелинейных отображениях, цифровая подпись, информационная безопасность. Число научных публикаций — 100. mdn.spectr@mail.ru; улица Профессора Попова, 5, 197022, Санкт-Петербург, Россия; р.т.: +7(812)234-2772.

Костина Анна Александровна — научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН). Область научных интересов: криптосхемы с открытым ключом, электронная цифровая подпись, криптографические протоколы, информационная безопасность. Число научных публикаций — 40. to.ann@inbox.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-7181.

Поддержка исследований. Работа выполнена при финансовой поддержке РНФ: проект № 24-21-00225.

DOI 10.15622/ia.24.6.9

A. MOLDOVYAN, D. MOLDOVYAN, A. KOSTINA

RANDOMIZATION IN POST-QUANTUM DIGITAL SIGNATURE ALGORITHMS WITH A SECRET GROUP

Moldovyan A., Moldovyan D., Kostina A. **Randomization in Post-Quantum Digital Signature Algorithms with a Secret Group.**

Abstract. In the field of post-quantum public-key cryptography, a direction of development of practical algebraic signature algorithms with a secret group is of particular interest, the security of which is based on the computational difficulty of solving large systems of power equations. As an algebraic carrier of such algorithms, finite non-commutative associative algebras (FNAA) are used. A specific point related to ensuring security against attacks based on known signatures when developing digital signature schemes of this type is the presence of the problem of improving the randomization mechanism of the fitting element of the digital signature, which is a vector S, repeatedly included in the verification equation as a multiplier. A well-known solution to this problem based on the use of two commutative secret groups, such that the elements of one of them are non-commutative with the elements of the other, when using the hash function value from S in the verification equation leads to an increase in the size of the digital signature, due to the need to specify two auxiliary fitting signature elements. The article proposes a new mechanism for signature randomization, which is distinguished by calculating the value of S depending on two vectors randomly selected from one commutative secret group. The proposed mechanism provides an acceptable security level against attacks based on known signatures and can be used as a basis for developing digital signature schemes with one verification equation and one auxiliary fitting signature element. A new algebraic algorithm has been developed that is of interest as a prototype of a practical post-quantum digital signature standard. Estimates of its parameters are given when using FNAA and the algebra of 3×3 matrices defined over a finite field as an algebraic support.

Keywords: post-quantum cryptography, multivariate cryptography, digital signature algorithm, signature randomization, cryptoalgorithm on finite algebras, cryptoalgorithm on non-commutative algebras, secret group.

References

1. Saarinen M.J., Smith-Tone D. Post-Quantum Cryptography. 15-th International Conference, PQCrypto 2024, Oxford, UK, 2024, Proceedings Part I. Lecture Notes in Computer Science. Springer, Cham, 2024. 434 p. DOI: 10.1007/978-3-031-62743-9.
2. Johansson T., Smith-Tone D. Post-Quantum Cryptography. 14-th International Conference, PQCrypto 2023, College Park, MD, USA, Proceedings. Lecture Notes in Computer Science. Springer, Cham, 2023. 714 p. DOI: 10.1007/978-3-031-40003-2.
3. Yan S.Y. Quantum Computational Number Theory. Springer. 2015. 252 p. DOI: 10.1007/978-3-319-25823-2.
4. Yan S.Y. Quantum Attacks on Public-Key Cryptosystems. Springer. 2014. 207 p. DOI: 10.1007/978-1-4419-7722-9.
5. Battarbee C., Kahrobaei D., Perret L., Shahandashti S.F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures. Post-Quantum Cryptography. PQCrypto 2023. Lecture Notes in Computer Science. Springer, Cham, 2023. vol. 14154. DOI: 10.1007/978-3-031-40003-2_5.
6. Alamelou Q., Blazy O., Cauchie S., Gaborit P. A code-based group signature scheme. Designs, Codes and Cryptography. 2017. vol. 82. pp. 469–493. DOI: 10.1007/s10623-016-0276-6.

7. Kosolapov Y.V., Turchenko O.Y. On the construction of a semantically secure modification of the McEliece cryptosystem. Prikladnaya Diskretnaya Matematika. 2019. no. 45. pp. 33–43. DOI: 10.17223/20710410/45/4.
8. Gärtner J. NTWE: A Natural Combination of NTRU and LWE. Post-Quantum Cryptography. PQCrypto 2023. Lecture Notes in Computer Science, Springer, Cham, 2023. vol. 14154. DOI: 10.1007/978-3-031-40003-2_12.
9. Lysakov I.V. Solving some cryptanalytic problems for lattice-based cryptosystems with quantum annealing method. Matematicheskie Voprosy Kriptografii [Mathematical Aspects of Cryptography]. 2023. vol. 14. no. 2. pp. 111–122. DOI: 10.4213/mvk441.
10. Hamlin B., Song F. Quantum Security of Hash Functions and Property-Preservation of Iterated Hashing. Post-Quantum Cryptography. PQCrypto 2019. Lecture Notes in Computer Science. Springer, Cham, 2019. vol. 11505. pp. 329–349. DOI: 10.1007/978-3-030-25510-7_18.
11. Agibalov G.P. ElGamal cryptosystems on Boolean functions. Prikladnaya Diskretnaya Matematika. 2018. no. 42. pp. 57–65. DOI: 10.17223/20710410/42/4.
12. Shuaiting Q., Wenbao H., Yifa Li, Luyao J. Construction of Extended Multivariate Public Key Cryptosystems. International Journal of Network Security. 2016. vol. 18. no. 1. pp. 60–67.
13. Ding J., Petzoldt A. Current State of Multivariate Cryptography. IEEE Security and Privacy Magazine. 2017. vol. 15. no. 4. pp. 28–36.
14. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography. Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York, NY, 2020. vol. 80. pp. 7–23. DOI: 10.1007/978-1-0716-0987-3_2.
15. Cartor R., Cartor M., Lewis M., Smith-Tone D. IPRainbow. Post-Quantum Cryptography. Lecture Notes in Computer Science. Springer, Cham, 2022. vol. 13512. pp. 170–184. DOI: 10.1007/978-3-031-17234-2_9.
16. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms. Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. no. 3(103). pp. 80–89. DOI: 10.56415/basm.y2023.i3.p80.
17. Moldovyan N.A. Parameterized method for specifying vector finite fields of arbitrary dimensions. Quasigroups and related systems. 2024. vol. 32. no. 2. pp. 299–312. DOI: 10.56415/qrs.v32.21.
18. 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: 10.56415/qrs.v30.24.
19. Moldovyan D.N. A new type of digital signature algorithms with a hidden group. Computer Science Journal of Moldova. 2023. vol. 31. no. 1(91). pp. 111–124. DOI: 10.56415/csjm.v31.06.
20. Moldovyan A., Moldovyan D., Moldovyan N. [Post-quantum public-key cryptoschemes on finite algebras]. Informatics and Automation. 2024. vol. 23(4). pp. 1246–1276. DOI: 10.15622/ia.23.4.12. (In Russ.).
21. Moldovyan N.A., Petrenko A.S. [Algebraic signature algorithm with two hidden groups]. Voprosy kiberbezopasnosti – Cibersecurity questions. 2024. no. 6(64). pp. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107. (In Russ.).
22. Moldovyan N.A., Petrenko A.S. [Typical verification equations in algebraic signature schemes with two hidden groups]. Voprosy kiberbezopasnosti – Cibersecurity questions. 2025. no 3(67). pp. 45–54. DOI: 10.21681/2311-3456-2025-3-XX-XX. (in print). (In Russ.).
23. Moldovyan N.A. Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions. Quasigroups and Related Systems. 2018. vol. 26. no. 2. pp. 263–270.

24. 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 and Computer Software (Bulletin SUSU MMCS). 2019. vol. 12. no. 1. pp. 66–81. DOI: 10.14529/mmp190106.
25. 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. DOI: 10.56415/qrs.v30.11.
26. Duong M.T., Moldovyan A.A., Moldovyan D.N., Nguyen M.H., Do B.T. Structure of quaternion-type algebras and a post-quantum signature algorithm. International Journal of Electrical and Computer Engineering (IJECE). 2025. vol. 15. no. 3. pp. 2965–2976. DOI: 10.11591/ijece.v15i3.pp2965-2976.

Moldovyan Alexander — Ph.D., Dr.Sci., Professor, Chief researcher, Laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: cryptography, post-quantum public-key cryptoalgorithms, digital signature, cryptographic protocols, computer security. The number of publications — 200. maa1305@yandex.ru; 39, 14-th Line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-7181.

Moldovyan Dmitriy — Ph.D., Associate professor of the department, Department of information systems, Saint Petersburg Electrotechnical University «LETI». Research interests: cryptography, post-quantum public-key cryptoalgorithms on algebras and on non-linear mappings, digital signature, information security. The number of publications — 100. mdn.spectr@mail.ru; 5, Professor Popov St., 197022, St. Petersburg, Russia; office phone: +7(812)234-2772.

Kostina Anna — Researcher, Laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: public-key cryptoschemes, digital signature algorithms, cryptographic protocols, information security. The number of publications — 40. to.ann@inbox.ru; 39, 14-th Line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-7181.

Acknowledgements. This research is supported by RSF (project No. 24-21-00225).