УДК 003.26
doi:10.31799/1684-8853-2020-3-71-78

Научные статьи
Articles

Протоколы слепой цифровой подписи на основе скрытой задачи дискретного логарифмирования

Д. Н. Молдовян[а], *канд. техн. наук, научный сотрудник, orcid.org/0000-0001-5039-7198, mdn.spectr@mail.ru*
А. А. Молдовян[а], *доктор техн. наук, профессор, orcid.org/0000-0001-5480-6016*
Д. Ю. Гурьянов[б], *канд. техн. наук, доцент, orcid.org/0000-0002-2923-4965*
[а]*Санкт-Петербургский институт информатики и автоматизации РАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ*
[б]*Государственный университет морского и речного флота им. адмирала С. О. Макарова, Двинская ул., 5/7, Санкт-Петербург, 198035, РФ*

Введение: *существенный прогресс в развитии квантовых вычислений выдвинул проблему построения постквантовых двухключевых криптографических алгоритмов и протоколов, т. е. криптосхем, которые были бы стойкими к атакам с использованием квантовых компьютеров. На основе скрытой задачи дискретного логарифмирования разработаны практичные постквантовые схемы цифровой подписи. Представляет интерес разработка на ее основе постквантовых протоколов слепой подписи.* ***Цель:*** *разработка протоколов слепой подписи на основе вычислительной трудности скрытой задачи дискретного логарифмирования.* ***Метод:*** *применение ослепляющих множителей, которые вносятся клиентом в ходе протокола слепой подписи при передаче подписанту параметров, необходимых для формирования слепой подписи.* ***Результаты:*** *предложен способ внесения ослепляющих множителей двух типов, левых и правых, что обеспечивает возможность реализовать протоколы слепой подписи на основе алгоритмов цифровой подписи с проверочным уравнением, задаваемым в некоммутативных алгебраических структурах. С применением этого способа разработаны новые протоколы слепой подписи, основанные на вычислительной трудности скрытой задачи дискретного логарифмирования. В качестве алгебраического носителя разработанных протоколов использованы конечные некоммутативные ассоциативные алгебры двух типов: с глобальной двухсторонней единицей и с большим множеством глобальных левых единиц.* ***Практическая значимость:*** *предложенные протоколы обладают достаточно высокой производительностью и удобны для программной и аппаратной реализации.*

Ключевые слова *— постквантовые криптосхемы, компьютерная безопасность, защита информации, электронная цифровая подпись, слепая подпись, задача дискретного логарифмирования, некоммутативные ассоциативные алгебры, вычислительно сложная задача.*

Для цитирования: Молдовян Д. Н., Молдовян А. А., Гурьянов Д. Ю. Протоколы слепой цифровой подписи на основе скрытой задачи дискретного логарифмирования. *Информационно-управляющие системы*, 2020, № 3, с. 71–78. doi:10.31799/1684-8853-2020-3-71-78

For citation: Moldovyan D. N., Moldovyan A. A., Gurianov D. Yu. Blind signature protocols based on hidden discrete logarithm problem. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 3, pp. 71–78 (In Russian). doi:10.31799/1684-8853-2020-3-71-78

Введение

В связи с ожиданием появления в ближайшее десятилетие практически доступного квантового компьютера, для которого известны полиномиальные алгоритмы решения задачи факторизации [1, 2] и задачи дискретного логарифмирования (ЗДЛ) [3, 4], в последнее время активно ведутся исследования по разработке постквантовых двухключевых криптосхем [5–7], т. е. криптографических алгоритмов и протоколов с открытым ключом, которые являются вычислительно эффективными при их реализации на обычных компьютерах и имеют сверхполиномиальную стойкость к атакам с использованием квантовых компьютеров.

Одним из направлений в области постквантовой криптографии является разработка постквантовых двухключевых криптосхем на основе вычислительной трудности скрытой задачи дискретного логарифмирования (СЗДЛ) [8, 9]. Это направление представляет практический интерес не только для применения в постквантовую эру, но также и в настоящее время, поскольку криптосхемы данного типа имеют сравнительно высокую производительность и могут составить конкуренцию криптосхемам, основанным на вычислительной трудности ЗДЛ на эллиптической кривой.

В зависимости от типа разрабатываемой криптосистемы с открытым ключом применяются разные формы СЗДЛ. Различные версии протоколов согласования секретного ключа по открытому каналу, основанных на вычислительной трудности СЗДЛ, рассматриваются в работах [8–10]. Алгоритм открытого шифрования описан в [9], а схемы электронной цифровой подписи (ЭЦП) — в работах [11–13]. В ряде важных практических

приложений (например, системах тайного электронного голосования и электронных денег) уникальную роль играют протоколы слепой ЭЦП, позволяющие решать задачу обеспечения неотслеживаемости (анонимности) пользователей. В связи с этим значительный интерес представляет разработка протоколов слепой ЭЦП, основанных на вычислительной сложности СЗДЛ.

В данной статье представлены два протокола слепой цифровой подписи, разработанные с использованием известных схем ЭЦП, основанных на вычислительной сложности СЗДЛ. Для построения протоколов слепой подписи использован известный механизм [14, 15] внесения и удаления ослепляющих множителей в схемах ЭЦП, основанных на ЗДЛ в циклической конечной группе. Однако указанный механизм был модифицирован с учетом особенностей СЗДЛ, формулируемой в конечных некоммутативных ассоциативных алгебрах (КНАА). Новые внесенные элементы построения схемы слепой подписи связаны с тем, что один из двух используемых ослепляющих множителей играет роль левого операнда операции умножения, а второй — роль правого операнда.

Скрытая задача дискретного логарифмирования

Типовая ЗДЛ возникает при построении криптосхем с открытым ключом в конечных циклических группах простого порядка ω, в которых открытый ключ Y' вычисляется по формуле

$$Y' = G^x, \qquad (1)$$

где G — элемент, являющийся генератором группы и имеющий порядок ω; требуется вычислить неизвестное целое число $0 < x < \omega$, которое называется личным секретным ключом пользователя, являющегося владельцем открытого ключа Y', т. е. пользователя, который выбрал случайное число x и по нему вычислил значение Y'.

Для задания СЗДЛ требуется использовать конечные алгебраические структуры, в которых содержится очень большое число различных конечных циклических групп в качестве подмножеств ее элементов, причем эти подмножества не пересекаются. Например, СЗДЛ формулируется в конечных некоммутативных группах [7] и в КНАА [9, 13]. Отличие СЗДЛ, используемой для построения схем ЭЦП, от обычной ЗДЛ состоит в том, что открытый ключ формируется в виде элементов Y и Z из двух разных циклических групп, каждая из которых отлична от группы, генерируемой всевозможными степенями элемента G. При этом в качестве маскирующих операций, отображающих элементы Y' и G в элементы Y и Z, выбираются операции автоморфного [8] или гомоморфного [9, 12] отображения. Благодаря взаимной коммутативности таких маскирующих операций с операцией возведения в степень обеспечивается корректность процедуры проверки подлинности ЭЦП по открытому ключу (Y, Z) в случае, если схема ЭЦП в базовой циклической группе, генерируемой элементом G, работает корректно при использовании открытого ключа (Y', G). Изучение известных протоколов ЭЦП, основанных на вычислительной сложности СЗДЛ, показывает, что они представляют собой модифицированные версии протоколов ЭЦП, основанных на вычислительной сложности ЗДЛ и построенных в явно заданной конечной циклической группе простого порядка. При этом модифицирование состоит в маскировании элементов базовой циклической группы, в которой выполняется базовая операция возведения в степень достаточно большого размера, которая вносит основной вклад в обеспечение стойкости криптосхемы. Важной задачей, имеющей теоретическое и практическое значение, является исследование вычислительной сложности решения различных форм СЗДЛ. Существенным вкладом в этом направлении являются работы [16–18], выполненные для СЗДЛ, заданной в конечной алгебре кватернионов.

Типы алгебраических носителей схем ЭЦП на основе СЗДЛ

Задание КНАА

Рассмотрим m-мерное векторное пространство над конечным простым полем $GF(p)$, где p — простое число. Его элементами являются векторы, которые могут быть записаны в виде упорядоченных наборов элементов поля $GF(p)$, т. е. в виде $\mathbf{A} = (a_0, a_1, ..., a_{m-1})$, где a_i — координаты, или в виде всевозможных сумм однокомпонентных векторов, т. е. в виде $\mathbf{A} = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + ... + a_{m-1}\mathbf{e}_{m-1}$, где $\mathbf{e}_i$ — базисные векторы. В векторном пространстве определены операция сложения векторов и операция умножения вектора на скаляр. Векторное пространство с дополнительно определенной операцией векторного умножения ($\circ$), т. е. умножения произвольных двух векторов $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ и $\mathbf{B} = \sum_{i=0}^{m-1} b_i\mathbf{e}_i$, которая является дистрибутивной слева и справа относительно операции сложения, называется m-мерной алгеброй.

Операция векторного умножения с указанным свойством может быть задана по следующей формуле:

$$\mathbf{A} \circ \mathbf{B} = \sum_{j=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \mathbf{e}_i \circ \mathbf{e}_j, \qquad (2)$$

в которой предполагается подстановка вместо каждого произведения упорядоченных пар базисных векторов некоторого однокомпонентного вектора в соответствии с так называемой таблицей умножения базисных векторов. После такой подстановки правая часть формулы (2) в общем случае представляет собой m-мерный вектор, т. е. элемент рассматриваемого векторного пространства. При использовании таблиц умножения базисных векторов, задающих некоммутативную ассоциативную операцию умножения векторов, получаем КНАА.

Схема ЭЦП в КНАА с большим множеством глобальных левых единиц

В статье [19] описана схема ЭЦП, заданная в четырехмерной КНАА, содержащей p^2 глобальных левых единиц. Операция умножения в данной алгебре задана по таблице умножения базисных векторов (табл. 1). Множество глобальных левых единиц описывается формулой

$$\mathbf{L} = (l_0, l_1, l_2, l_3) = (d, h, 1-d, -h), \qquad (3)$$

где $d, h = 0, 1, \ldots, p-1$.

Каждая глобальная левая единица $\mathbf{L}$ задает гомоморфные отображения рассматриваемой алгебры следующих двух типов [19]. Операция гомоморфного отображения первого типа определяется по формуле

$$\varphi_{\mathbf{L}}(\mathbf{X}) = \mathbf{X} \circ \mathbf{L}, \qquad (4)$$

где переменная $\mathbf{X}$ пробегает все значения в алгебре. Операция гомоморфного отображения второго типа определяется по формуле

$$\psi_{\mathbf{L}}(\mathbf{X}) = \mathbf{B} \circ \mathbf{X} \circ \mathbf{A}, \qquad (5)$$

где фиксированные векторы $\mathbf{A}$ и $\mathbf{B}$ удовлетворяют условию $\mathbf{A} \circ \mathbf{B} = \mathbf{L}$ и переменная $\mathbf{X}$ пробегает все значения в алгебре. Прототипом схемы ЭЦП, основанной на вычислительной трудности СЗДЛ и предложенной в работе [19], является схема ЭЦП Шнорра [20]. В качестве характеристики конечного поля $GF(p)$, над которым задана КНАА, выбирается 256-битовое число вида $p = eq$, где e — небольшое четное число (например, имеющее разрядность от 2 до 16 бит) и q — простое число большого размера. Можно легко сгенерировать значение p такое, что структурный коэффициент $\mu = 2$ будет квадратичным невычетом по модулю p.

Процедура формирования открытого ключа описывается следующим образом.

1. Выбрать случайные четырехмерные векторы $\mathbf{A}$, $\mathbf{A}'$ и $\mathbf{N}$, всевозможные степени каждого из которых генерируют циклическую группу порядка q, причем указанные три вектора являются попарно не перестановочными.

2. Используя формулу (3), вычислить две случайные глобальные левые единицы $\mathbf{L}$ и $\mathbf{L}'$.

3. Вычислить вектор $\mathbf{B}'$ как решение уравнения $\mathbf{A}' \circ \mathbf{B}' = \mathbf{L}'$.

4. Вычислить вектор $\mathbf{B}$ как решение уравнения $\mathbf{A} \circ \mathbf{B} = \mathbf{L}$.

5. Вычислить порядок ω циклической группы, генерируемой вектором $\mathbf{B}'$.

6. Вычислить вектор $\mathbf{T}$ как решение уравнения $\mathbf{A} \circ \mathbf{T} = \mathbf{B}'^{\omega-1}$.

7. Сгенерировать равновероятное неотрицательное число $x < q$ и вычислить вектор $\mathbf{Y} = \mathbf{B} \circ \mathbf{N}^x \circ \mathbf{A} \circ \mathbf{L}$.

8. Вычислить вектор $\mathbf{Z} = \mathbf{B}' \circ \mathbf{N} \circ \mathbf{A}'$.

9. Взять векторы $\mathbf{Y}$, $\mathbf{Z}$ и $\mathbf{T}$ в качестве открытого ключа.

Отметим, что векторы $\mathbf{A}$, $\mathbf{A}'$, $\mathbf{B}$, $\mathbf{B}'$, $\mathbf{L}$, $\mathbf{L}'$, $\mathbf{N}$ и число x являются секретными элементами. Однако только значения $\mathbf{B}$, $\mathbf{A}'$, $\mathbf{N}$ и x являются элементами личного секретного ключа, поскольку только они нужны для вычисления ЭЦП.

Вычисление значения подписи выполняется по следующему алгоритму.

1. Выбрать случайное натуральное число $k < q$ и вычислить вектор $\mathbf{V} = \mathbf{B} \circ \mathbf{N}^k \circ \mathbf{A}'$.

2. Вычислить первый элемент ЭЦП $v = F_h(M, \mathbf{V})$, где F_h — некоторая специфицированная хэш-функция.

3. Вычислить второй элемент ЭЦП s: $s = k + xv \bmod q$.

Цифровой подписью к электронному документу M является пара чисел (v, s).

Процедура проверки подлинности подписи (v, s) включает следующие шаги.

1. Вычислить вектор $\mathbf{V}'$: $\mathbf{V}' = \mathbf{Y}^{-v} \circ \mathbf{T} \circ \mathbf{Z}^s$.

2. Вычислить значение хэш-функции v' от документа M, к которому присоединен вектор $\mathbf{V}'$: $v' = F_h(M, \mathbf{V}')$.

3. Если $v' = v$, то подпись (v, s) принимается как подлинная. В противном случае подпись отвергается.

■ ***Таблица 1***. Задание операции умножения в КНАА p^2 глобальных левых единиц [19], где μ — квадратичный невычет в $GF(p)$

■ ***Table 1***. Setting the operation of multiplication in KNAA p^2 global left units [19], where μ — is a quadratic non-residue in $GF(p)$

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mu\mathbf{e}_0$	$\mathbf{e}_3$	$\mu\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\mathbf{e}_1$	$\mu\mathbf{e}_0$	$\mathbf{e}_3$	$\mu\mathbf{e}_2$

Схема ЭЦП в КНАА с глобальной двухсторонней единицей

В работе [13] предложена схема ЭЦП, заданная в четырехмерной КНАА с глобальной двухсторонней единицей $\mathbf{E}$, в которой операция векторного умножения определена по таблице умножения базисных векторов (табл. 2). Рассмотрим некоторые результаты [13], используемые при построении указанной схемы ЭЦП.

Глобальная двухсторонняя единица $\mathbf{E}$ может быть вычислена по формуле

$$\mathbf{E}=\left(\frac{1}{\lambda-1}, \frac{1}{1-\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}\right). \quad (6)$$

Если для некоторых векторов $\mathbf{A}=(a_0, a_1, a_2, a_3)$ векторное уравнение вида $\mathbf{X}\circ\mathbf{A}=\mathbf{E}$ имеет единственное решение $\mathbf{X}=\mathbf{A}^{-1}$, то векторное уравнение $\mathbf{A}\circ\mathbf{X}=\mathbf{E}$ также имеет единственное решение $\mathbf{X}=\mathbf{A}^{-1}$. Вектор $\mathbf{A}^{-1}$ называется обратным по отношению к вектору $\mathbf{A}$. Признаком обратимости вектора $\mathbf{A}=(a_0, a_1, a_2, a_3)$ является неравенство вида

$$a_1a_2\neq a_0a_3. \quad (7)$$

Векторы $\mathbf{G}=(g_0, g_1, g_2, g_3)$, координаты которых удовлетворяют равенству $g_1g_2=g_0g_3$, являются необратимыми. Рассматриваемая алгебра включает некоторые подмножества элементов, которые действуют на некоторый фиксированный необратимый вектор $\mathbf{G}$ и всевозможные его степени $\mathbf{G}^k$ как локальные левые единицы. Также можно выделить множества локальных правых единиц.

Множество локальных левых единиц $\mathbf{L}$, соответствующих вектору $\mathbf{G}$, описывается формулой [13]

$$\mathbf{L}=(l_0, l_1, l_2, l_3)=$$
$$=\left(d, \frac{g_0-(\lambda g_0+g_2)d}{g_0+g_2}, h, \frac{g_2-(\lambda g_0+g_2)h}{g_0+g_2}\right), \quad (8)$$

■ ***Таблица 2***. Умножение базисных векторов в четырехмерной КНАА с глобальной двухсторонней единицей ($\lambda\neq 1$) [13]

■ ***Table 2***. Multiplication of basis vectors in four-dimensional KNAA with global two-sided unit ($\lambda\neq 1$) [13]

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_3$

где $d, h = 0, 1, ..., p-1$. Множество (8) локальных левых единиц содержит в себе p^2-p обратимых векторов и p необратимых векторов рассматриваемой алгебры.

Множество локальных правых единиц $\mathbf{R}$, соответствующих всевозможным натуральным степеням необратимого вектора $\mathbf{G}$, описывается формулой [13]

$$\mathbf{R}=(r_0, r_1, r_2, r_3)=$$
$$=\left(d, h, \frac{g_0-(\lambda g_0+g_1)d}{g_0+g_1}, \frac{g_1-(\lambda g_0+g_1)h}{g_0+g_1}\right), \quad (9)$$

где $d, h = 0, 1, ..., p-1$. В множестве (9) локальных правых единиц содержатся обратимые и необратимые векторы рассматриваемой КНАА. Количество первых равно p^2-p, а вторых — p.

Пересечение множеств (8) и (9) задает p различных двухсторонних локальных единиц для векторов вида $\mathbf{G}^k$ при произвольном натуральном числе $k\geq 1$, из которых необратимым элементом рассматриваемой КНАА является единственный вектор, обозначаемый как $\mathbf{E}_\mathbf{G}$ и представляющий собой единичный элемент циклической группы, генерируемой всевозможными степенями вектора $\mathbf{G}$. Значение локальной двухсторонней единицы $\mathbf{E}_\mathbf{G}$ можно найти по формуле $\mathbf{E}_\mathbf{G}=\mathbf{G}^\omega$, где ω — порядок вектора $\mathbf{G}$, являющийся делителем числа p^2-1. Из выражений (8) и (9) в статье [13] выводится следующее выражение, которое имеет значительно меньшую вычислительную сложность по сравнению с операцией возведения в степень ω:

$$\mathbf{E}_\mathbf{G}=\left(k, \frac{g_1}{g_0}k, \frac{g_0-(\lambda g_0+g_1)k}{g_0+g_1}, h, \frac{g_0g_1-(\lambda g_0+g_1)g_1k}{g_0^2+g_0g_1}\right), \quad (10)$$

где $k=g_0^2\left(\lambda g_0^2+g_0g_1+g_0g_2+g_1g_2\right)^{-1}$.

В качестве скрытой циклической группы, в которой выполняется базовая операция возведения в степень, схема ЭЦП [13] использует группу, генерируемую необратимым вектором $\mathbf{G}$. Легко видеть, что для произвольного обратимого вектора $\mathbf{R}$ из множества (9) локальных правых единиц и произвольного натурального значения k справедливо равенство $\mathbf{R}\circ\mathbf{G}^k=(\mathbf{R}\circ\mathbf{G})^k$. Взаимная коммутативность операции умножения слева на правую единицу и операции возведения в степень в базовой циклической группе позволяют использовать первую в качестве маскирующей операции при задании СЗДЛ.

Другой тип используемой маскирующей операции задается по формуле $\mathbf{Z}=\mathbf{R}'\circ\mathbf{G}\circ\mathbf{A}$, где

$\mathbf{R}'$ — обратимый вектор из множества локальных правых единиц (9); $\mathbf{A}$ — обратимый вектор, такой, что для некоторой локальной левой единицы $\mathbf{L}$ выполняется равенство $\mathbf{A} \circ \mathbf{R}' = \mathbf{L}$. Для любого натурального числа k выполняется условие взаимной коммутативности с операцией возведения в степень: $(\mathbf{R}' \circ \mathbf{G} \circ \mathbf{A})^k = \mathbf{R}' \circ \mathbf{G}^k \circ \mathbf{A}$.

В работе [13] предлагается следующая процедура формирования открытого ключа в виде пары четырехмерных векторов $(\mathbf{Y}, \mathbf{Z})$, использующая два указанных типа маскирующих операций.

1. Выбрать случайный необратимый вектор $\mathbf{G}$, локальный порядок которого равен простому числу q.

2. Генерируя случайные пары значений (d, h) и используя формулу (9), вычислить две локальные правые единицы $\mathbf{R}_1$ и $\mathbf{R}_2$, являющиеся обратимыми элементами рассматриваемой КНАА.

3. Генерируя случайные пары значений (d, h) и используя формулу (8), вычислить случайную локальную левую единицу $\mathbf{L}$, являющуюся обратимым элементом алгебры.

4. Вычислить четырехмерный вектор $\mathbf{A}$ из уравнения $\mathbf{A} \circ \mathbf{R}_2 = \mathbf{L}$.

5. Сгенерировать случайное натуральное число $x < q$ и вычислить открытый ключ в виде пары четырехмерных векторов $\mathbf{Y}$ и $\mathbf{Z}$:

$$\mathbf{Y} = \mathbf{R}_1 \circ \mathbf{G}^x; \mathbf{Z} = \mathbf{R}_2 \circ \mathbf{G} \circ \mathbf{A}.$$

Личным секретным ключом подписанта является четверка значений x, $\mathbf{G}$, $\mathbf{R}_1$ и $\mathbf{A}$. Процедура вычисления ЭЦП к электронному документу M включает следующие шаги.

1. Сгенерировать случайное натуральное число $k < q$.

2. Вычислить фиксатор в виде четырехмерного вектора $\mathbf{W} = \mathbf{R}_1 \circ \mathbf{G}^k \circ \mathbf{A}$.

3. Вычислить первый элемент ЭЦП как значение хэш-функции $e = F_h(M, \mathbf{W})$, где F_h — некоторая хэш-функция, являющаяся частью протокола ЭЦП.

4. Вычислить второй элемент ЭЦП в виде двоичного числа s:

$$s = k + ex \bmod q.$$

Проверка подлинности ЭЦП (e, s) к документу M выполняется с использованием открытого ключа $(\mathbf{Y}, \mathbf{Z})$ по следующему алгоритму.

1. Вычислить значение вектора $\tilde{\mathbf{W}} = \mathbf{Y}^{-e} \circ \mathbf{Z}^s$.

2. Присоединив к документу вектор $\tilde{\mathbf{W}}$, вычислить значение хэш-функции $\tilde{e} = F_h\left(M, \tilde{\mathbf{W}}\right)$.

3. Сравнить значения $\tilde{e}$ и e. Если $\tilde{e} = e$, то подпись (e, s) принимается как подлинная ЭЦП. Если $\tilde{e} \neq e$, то подпись (e, s) отклоняется как ложная ЭЦП.

Протоколы слепой ЭЦП

В некоторых специальных информационных технологиях, например в системах электронных денег [21], одним из важных требований является обеспечение неотслеживаемости (анонимности) пользователей. Для решения этой задачи в работе [22] впервые был предложен механизм формирования ЭЦП «вслепую», реализуемый с помощью протоколов слепой подписи. В протоколах данного типа участвуют два субъекта: 1) клиент, формирующий электронный документ и желающий получить подлинную подпись другого лица к этому документу, и 2) подписант, вычисляющий некоторые параметры (элементы слепой подписи) и передающий их значения клиенту, из которых последний вычисляет подлинную ЭЦП. Проверка подлинности подписи, полученной клиентом, осуществляется по тому же алгоритму, как и проверка обычной подписи.

При этом по данным, использованным в ходе протокола слепой подписи, клиент не может получить информацию о личном секретном ключе подписанта, а подписант не может однозначно установить связь некоторого выполненного протокола слепой подписи с некоторым электронным документом и приложенной к нему подлинной ЭЦП (предполагается, что подписант многократно выполнял подписывание документов «вслепую»). Последний момент называется требованием обеспечения неотслеживаемости пользователей, которое предъявляется к протоколам слепой подписи.

Первый протокол слепой ЭЦП был реализован на основе схемы подписи RSA [23], основанной на вычислительной сложности задачи факторизации. В дальнейшем были разработаны протоколы слепой ЭЦП, основанные на вычислительной сложности ЗДЛ [14]. В обоих случаях анонимность клиента обеспечивается механизмом внесения в слепую подпись одного или двух случайных ослепляющих множителей. После получения слепой подписи от подписанта клиент удаляет ослепляющие множители, в результате чего получает подлинную подпись. Протоколы слепой подписи могут быть реализованы на основе ряда известных схем ЭЦП, например, на основе RSA [23], схемы Шнорра [20], ГОСТ Р 34.10–94 и ГОСТ Р 34.10–2001 [24, 25].

Протоколы слепой ЭЦП, основанные на вычислительной сложности СЗДЛ

Использование КНАА с множеством глобальных левых единиц

Протокол слепой ЭЦП, основанный на схеме ЭЦП из статьи [19], описывается следующим образом.

1. Подписант генерирует случайное число $k < q$ и вычисляет вектор-фиксатор. Затем он направляет вектор-фиксатор $\bar{\mathbf{V}}$ клиенту, имеющему намерение сформировать подлинную ЭЦП подписанта к некоторому документу M.

2. Клиент выбирает два случайных равновероятных натуральных числа $\tau < q$ и $\varepsilon < q$, используя которые вычисляет левый $\mathbf{Y}^{\tau}$ и правый $\mathbf{Z}^{\varepsilon}$ ослепляющие множители. Затем он модифицирует вектор-фиксатор $\bar{\mathbf{V}}$ по формуле $\mathbf{V} = \mathbf{Y}^{\tau} \circ \bar{\mathbf{V}} \circ \mathbf{Z}^{\varepsilon}$ и вычисляет первый элемент подписи $v = F_h(M, \mathbf{V})$.

3. По значению v клиент формирует первый элемент слепой подписи в виде натурального числа $\bar{v} = v + \tau \bmod q$ и передает его подписанту.

4. Подписант вычисляет второй элемент $\bar{s}$ слепой подписи по формуле $\bar{s} = k + \bar{v}x \bmod q$, где x — значение личного секретного ключа подписанта. Затем значение $\bar{s}$ передается клиенту.

5. Получив второй элемент слепой подписи, клиент вычисляет значение $s = \bar{s} + \varepsilon \bmod q$, которое является вторым элементом s подлинной подписи.

На выходе этого протокола клиент получает подлинную подпись (v, s) к документу, который был недоступен подписанту в ходе протокола. Доказательство корректности работы протокола состоит в том, чтобы доказать, что полученная клиентом ЭЦП проходит процедуру проверки подлинности подписи, как правильная подлинная подпись. Действительно, подавая на вход проверочной процедуры подпись (v, s), получим следующее доказательство:

$$\mathbf{V}' = \mathbf{Y}^{-v} \circ \mathbf{T} \circ \mathbf{Z}^{s} = \mathbf{Y}^{-(\bar{v}-\tau)} \circ \mathbf{T} \circ \mathbf{Z}^{\bar{s}+\varepsilon} =$$
$$= \mathbf{Y}^{\tau} \circ \mathbf{Y}^{-\bar{v}} \circ \mathbf{T} \circ \mathbf{Z}^{\bar{s}} \circ \mathbf{Z}^{\varepsilon} = \mathbf{Y}^{\tau} \circ \bar{\mathbf{V}} \circ \mathbf{Z}^{\varepsilon} \Rightarrow$$
$$\Rightarrow v' = F_h\left(M, \mathbf{V}'\right) = F_h\left(M, \mathbf{V}\right) = v.$$

Поскольку выполняется условие $v' = v$, то подпись (v, s) принимается как подлинная ЭЦП к документу M.

Аналогичным способом другие известные схемы ЭЦП, основанные на вычислительной трудности СЗДЛ и использующие в качестве алгебраического носителя КНАА с большим множеством односторонних единиц, также могут применяться для разработки протоколов слепой ЭЦП.

Использование КНАА с глобальной двухсторонней единицей

В протоколе слепой ЭЦП, основанном на схеме ЭЦП из статьи [13], выполняются следующие шаги.

1. Сформировав случайное равновероятное натуральное число $k < q$, подписант вычисляет вектор-фиксатор $\bar{\mathbf{W}} = \mathbf{R}_1 \circ \mathbf{G}^{k} \circ \mathbf{A}$. Затем он передает вектор-фиксатор $\bar{\mathbf{W}}$ клиенту, имеющему намерение получить подлинную ЭЦП подписанта к документу M.

2. Клиент выбирает два случайных равновероятных натуральных числа $0 < \tau < q$ и $0 < \varepsilon < q$, используя которые вычисляет левый $\mathbf{Y}^{\tau}$ и правый $\mathbf{Z}^{\varepsilon}$ ослепляющие множители. Затем он модифицирует вектор-фиксатор по формуле $\mathbf{W} = \mathbf{Y}^{\tau} \circ \bar{\mathbf{W}} \circ \mathbf{Z}^{\varepsilon}$ и вычисляет первый элемент e ЭЦП в виде значения хэш-функции $e = F_h(M, \mathbf{W})$.

3. Первый элемент слепой ЭЦП $\bar{e}$ вычисляется клиентом по формуле $\bar{e} = e + \tau \bmod q$ и направляется подписанту.

4. Подписант находит значение второго элемента $\bar{s}$ слепой подписи по формуле $\bar{s} = k + \bar{e}x \bmod q$, где x — личный секретный ключ подписанта. Значение $\bar{s}$ передается клиенту.

5. Используя второй элемент $\bar{s}$ слепой подписи, клиент вычисляет значение $s = \bar{s} + \varepsilon \bmod q$, которое является вторым элементом подлинной подписи.

Полученная клиентом подпись (e, s) к документу M проходит процедуру проверки подписи как подлинная ЭЦП. Действительно, при использовании открытого ключа $(\mathbf{Y}, \mathbf{Z})$ в ходе осуществления процедуры проверки подлинности ЭЦП имеем следующее доказательство:

$$\tilde{\mathbf{W}} = \mathbf{Y}^{-e} \circ \mathbf{Z}^{s} = \mathbf{Y}^{-\bar{e}+\tau} \circ \mathbf{Z}^{\bar{s}+\varepsilon} =$$
$$= \mathbf{Y}^{\tau} \circ \mathbf{Y}^{-\bar{e}} \circ \mathbf{Z}^{\bar{s}} \circ \mathbf{Z}^{\varepsilon} = \mathbf{Y}^{\tau} \circ \bar{\mathbf{V}} \circ \mathbf{Z}^{\varepsilon} \Rightarrow$$
$$\Rightarrow \tilde{e} = F_h\left(M, \tilde{\mathbf{W}}\right) = F_h\left(M, \mathbf{W}\right) = e.$$

В соответствии с проверочной процедурой при выполнении условия $\tilde{e} = e$ подпись (e, s) принимается как подлинная, т. е. описанный протокол слепой подписи является корректным.

Заключение

Предложены реализации двух протоколов слепой подписи, основанных на вычислительной трудности СЗДЛ. В качестве базовых схем ЭЦП использованы схемы ЭЦП, алгебраическими носителями которых являются четырехмерные КНАА двух разных типов. Предложенные протоколы представляют интерес как кандидаты на постквантовые протоколы слепой ЭЦП. Особенностью построения протоколов слепой подписи, основанных на вычислительной трудности СЗДЛ, является то, что один из вносимых ослепляющих множителей должен играть роль правого операнда, а второй — роль левого операнда. Данная специфика связана с тем, что алгебраическими носителями таких протоколов являются некоммутативные алгебры.

Финансовая поддержка

Работа выполнена при частичной финансовой поддержке РФФИ (грант № 18-07-00932-а).

Литература

1. **Shor P. W.** Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. *SIAM Journal of Computing*, 1997, vol. 26, pp. 1484–1509.
2. **Smolin J. A., Smith G., Vargo A.** Oversimplifying quantum factoring. *Nature*, 2013, vol. 499, no. 7457, pp. 163–165.
3. **Yan S. Y.** *Quantum Computational Number Theory*. Springer, 2015. 252 p.
4. **Yan S. Y.** *Quantum Attacks on Public-Key Cryptosystems*. Springer, 2014. 207 p.
5. Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (дата обращения: 13.11.2019).
6. *Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018*, Fort Lauderdale, FL, USA, April 9–11, 2018, Proceedings. *Lecture Notes in Computer Science(LNCS)*, Springer, 2018, vol. 10786. 529 p. doi:10.1007/978-3-319-79063-3
7. *Post-Quantum Cryptography. 10th International Conference, PQCrypto 2019*, Chongqing, China, May 8–10, 2019. *Lecture Notes in Computer Science (LNCS)*, Springer, 2019, vol. 11505. doi:10.1007/978-3-030-25510-7
8. **Moldovyan N. A., Moldovyan A. A.** Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem. *Вестник ЮУрГУ. Серия: Математическое моделирование и программирование*, 2019, т. 12, № 1, с. 66–81.
9. **Moldovyan D. N.** Non-commutative finite groups as primitive of public-key cryptoschemes. *Quasigroups and Related Systems*, 2010, vol. 18, pp. 165–176.
10. **Moldovyan N. A.** Unified method for defining finite associative algebras of arbitrary even dimensions. *Quasigroupsand Related Systems*, 2018, vol. 26, no. 2, pp. 263–270.
11. **Молдовян Н. А., Абросимов И. К.** Схема постквантовой электронной цифровой подписи на основе усиленной формы скрытой задачи дискретного логарифмирования. *Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления*, 2019, т. 15, вып. 2, с. 212–220. https://doi.org/10.21638/11702/spbu10.2019.205
12. **Moldovyan N. A.** Finite non-commutative associative algebras for setting the hidden discrete logarithm problem and post-quantum cryptoschemes on its base. *Buletinul Academiei de Stiinte a Republicii Moldova. Matematica*, 2019, no. 1 (89), pp. 71–78.
13. **Молдовян А. А., Молдовян Д. Н.** Постквантовая схема ЭЦП на основе скрытой задачи дискретного логарифмирования в четырехмерной конечной алгебре. *Вопросы защиты информации*, 2019, № 2, с. 18–22.
14. **Camenisch J. L., Piveteau J.-M., Stadler M. A.** Blind signatures based on the discrete logarithm problem. *Advances in Cryptology — EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques*, Perugia, Italy, May 9–12, 1994. Proceedings. Springer, 1995, vol. 950. *Lecture Notes in Computer Science (LNCS)*, pp. 428–432.
15. **Pointcheval D., Stern J.** Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 2000, vol. 13, no. 3, pp. 361–396.
16. **Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.** Cryptographic algorithms on groups and algebras. *Journal of Mathematical Sciences*, 2017, vol. 223, no. 5, pp. 629–641.
17. **Кузьмин А. С., Марков В. Т., Михалев А. А., Михалев А. В., Нечаев А. А.** Криптографические алгоритмы на группах и алгебрах. *Фундаментальная и прикладная математика*, 2015, т. 20, № 1, с. 205–222.
18. **Глухов М. М.** К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах. *Математические вопросы криптографии*, 2010, т. 1, № 4, с. 5–22.
19. **Moldovyan D. N., Moldovyan A. A., Sklavos N.** Post-quantum signature schemes for efficient hardware implementation. *Proceedings of 10th IFIP International Conference on New Technologies, Mobility & Security (NTMS'19)*, Canary Islands, Spain, June 24–26, 2019, pp. 1–5.
20. **Schnorr C. P.** Efficient signature generation by smart cards. *Journal of Cryptology*, 1991, vol. 4, pp. 161–174.
21. **Chaum D.** Blind signatures for untraceable payments. *Advances in Cryptology: Proc. of CRYPTO'82*, Plenum Press, 1983, pp. 199–203.
22. **Chaum D.** Security without identification: Transaction systems to make big brother obsolete. *Communication of the ACM*, Oct. 1985, vol. 28, no. 10, pp. 1030–1044.
23. **Rivest R. L., Shamir A., Adleman L. M.** A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 1978, vol. 21, pp. 120–126.
24. **Молдовян Н. А.** Протоколы слепой коллективной подписи на основе стандартов цифровой подписи. *Вопросы защиты информации*, 2010, № 1, с. 2–6.
25. **Moldovyan N. A.** Blind signature protocols from digital signature standards. *Int. Journal of Network Security*, 2011, vol. 13, no. 1, pp. 22–30.

UDC 003.26
doi:10.31799/1684-8853-2020-3-71-78

Blind signature protocols based on hidden discrete logarithm problem

D. N. Moldovyan[a], PhD, Tech., Research Fellow, orcid.org/0000-0001-5039-7198, mdn.spectr@mail.ru
A. A. Moldovyan[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-5480-6016
D. Yu. Gurianov[b], PhD, Tech., Associate Professor, orcid.org/0000-0002-2923-4965
[a]Saint-Petersburg Institute for Informatics and Automation of the RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation
[b]Admiral Makarov State University of Maritime and Inland Shipping, 5/7, Dvinskaya St., 198035, Saint-Petersburg, Russian Federation

Introduction: The progress in the development of quantum computing has raised the problem of constructing post-quantum public-key cryptographic algorithms and protocols, i. e. cryptoschemes resistant to quantum attacks. Based on the hidden discrete logarithm problem, some practical post-quantum digital signature schemes have been developed. The next step could be the development of post-quantum blind signature protocols. **Purpose:** To develop blind signature protocols based on the computational difficulty of the hidden discrete logarithm problem. **Method:** The use of blinding factors introduced by the client during the blind signature protocol when the parameters necessary for the blind signature formation are passed to the signer. **Results:** It has been proposed to use blinding multipliers of two different types: left-sided and right-sided ones. With them, you can develop blind signature protocols on the base of schemes with a verification equation defined in non-commutative algebraic structures. New blind signature protocols have been developed, based on the computational difficulty of the hidden discrete logarithm problem. As the algebraic carrier for the developed protocols, finite non-commutative associative algebras of two types are used: 1) those with a global two-sided unit, and 2) those with a large set of global left units. **Practical relevance:** The proposed protocols have a high performance and can be successfully implemented either in software or in hardware.

Keywords — post-quantum crypto schemes, computer security, information protection, digital signature, blind signature, discrete logarithm problem, non-commutative associative algebras, computationally difficult problem.

For citation: Moldovyan D. N., Moldovyan A. A., Gurianov D. Yu. Blind signature protocols based on hidden discrete logarithm problem. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 3, pp. 71–78 (In Russian). doi:10.31799/1684-8853-2020-3-71-78

References

1. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. *SIAM Journal of Computing*, 1997, vol. 26, pp. 1484–1509.
2. Smolin J. A., Smith G., Vargo A. Oversimplifying quantum factoring. *Nature*, 2013, vol. 499, no. 7457, pp. 163–165.
3. Yan S. Y. *Quantum Computational Number Theory*. Springer, 2015. 252 p.
4. Yan S. Y. *Quantum Attacks on Public-Key Cryptosystems*. Springer, 2014. 207 p.
5. *Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms.* Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (accessed 13 November 2019).
6. *Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018*, Fort Lauderdale, FL, USA, April 9–11, 2018, Proceedings. *Lecture Notes in Computer Science (LNCS)*, Springer, 2018, vol. 10786. 529 p. doi:10.1007/978-3-319-79063-3
7. *Post-Quantum Cryptography. 10th International Conference, PQCrypto 2019*, Chongqing, China, May 8–10, 2019. *Lecture Notes in Computer Science (LNCS)*, Springer, 2019, vol. 11505. doi:10.1007/978-3-030-25510-7
8. 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. Series "Mathematical Modelling, Programming & Computer Software"*, 2019, vol. 12, no. 1, pp. 66–81.
9. Moldovyan D. N. Non-commutative finite groups as primitive of public-key cryptoschemes. *Quasigroups and Related Systems*, 2010, vol. 18, pp. 165–176.
10. 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.
11. Moldovyan N. A., Abrosimov I. K. Post-quantum electronic digital signature scheme based on the enhanced form of the hidden discrete logarithm problem. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2019, vol. 15, iss. 2, pp. 212–220 (In Russian). https://doi.org/10.21638/11702/spbu10.2019.205
12. Moldovyan N. A. Finite non-commutative associative algebras for setting the hidden discrete logarithm problem and post-quantum cryptoschemes on its base. *Buletinul Academiei de Stiinte a Republicii Moldova. Matematica*, 2019, no. 1 (89), pp. 71–78.
13. Moldovyan A. A., Moldovyan D. N. Post-quantum signature algorithms based on the hidden discrete logarithm problem in four-dimensional finite algebra. *Voprosy zashchity informatsii*, 2019, no. 2, pp. 18–22 (In Russian).
14. Camenisch J. L., Piveteau J.-M., Stadler M. A. Blind signatures based on the discrete logarithm problem. *Advances in Cryptology — EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques*, Perugia, Italy, May 9–12, 1994. Proceedings. Springer, 1995, vol. 950. *Lecture Notes in Computer Science (LNCS)*, pp. 428–432.
15. Pointcheval D., Stern J. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 2000, vol. 13, no. 3, pp. 361–396.
16. Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A. Cryptographic algorithms on groups and algebras. *Journal of Mathematical Sciences*, 2017, vol. 223, no. 5, pp. 629–641.
17. Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A. Cryptographic algorithms on groups and algebras. *Fundumental and Applied Mathematics*, 2015, vol. 20, no. 1, pp. 205–222 (In Russian).
18. Glukhov M. M. On analysis of some public key distribution systems based on non-abelian groups. *Mathematical Aspects of Cryptography*, 2010, vol. 1, no. 4, pp. 5–22 (In Russain).
19. Moldovyan D. N., Moldovyan A. A., Sklavos N. Post-quantum signature schemes for efficient hardware implementation. *Proceedings of 10th IFIP International Conference on New Technologies, Mobility & Security (NTMS'19)*, Canary Islands, Spain, June 24–26, 2019, pp. 1–5.
20. Schnorr C. P. Efficient signature generation by smart cards. *Journal of Cryptology*, 1991, vol. 4, pp. 161–174.
21. Chaum D. Blind Signatures for Untraceable Payments. *Advances in Cryptology: Proc. of CRYPTO'82*, PlenumPress, 1983, pp. 199–203.
22. Chaum D. Security without identification: Transaction systems to make big brother obsolete. *Communication of the ACM*, Oct. 1985, vol. 28, no. 10, pp. 1030–1044.
23. Rivest R. L., Shamir A., Adleman L. M. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 1978, vol. 21, pp. 120–126.
24. Moldovyan N. A. Blind collective signature protocols based on digital signature standards. *Voprosy zashchity informatsii*, 2010, vol. 1, pp. 2–6 (In Russian).
25. Moldovyan N. A., Moldovyan D. N. Blind signature protocols from digital signature standards. *Int. Journal of Network Security*, 2011, vol. 13, no. 1, pp. 22–30.