УДК 519.719.325 DOI 10.17223/20710410/57/3

РАНДОМИЗИРОВАННЫЙ АНАЛОГ НЕОСПОРИМОЙ ПОДПИСИ ЧАУМА — ВАН-АНТВЕРПЕНА

П. А. Полищук*, А. В. Черемушкин**

*Белорусский государственный университет, г. Минск, Беларусь
**Академия криптографии РФ, г. Москва, Россия

E-mail: poulpvp101@gmail.com, avc238@mail.ru

Предлагается модификация неоспоримой подписи Д. Чаума и Х. ван Антверпена, основанная на группе точек эллиптической кривой. Алгоритм формирования подписи дополнен предварительным этапом рандомизации. Для протоколов проверки подписи и отказа от неё предложено два варианта выполнения. Доказаны теоремы, показывающие, что эти протоколы отвечают своему назначению. Описан способ преобразования неоспоримой подписи в обычную цифровую подпись, проиллюстрированный на примере схемы цифровой подписи Шнорра.

Ключевые слова: *цифровая подпись, неоспоримая подпись, группа точек эллиптической кривой.*

A RANDOMIZED ANALOG OF CHAUM — VAN ANTWERPEN UNDENIABLE SIGNATURE

P. A. Polyschuk*, A. V. Cheremushkin**

*Belarusian State University, Minsk, Belarus,
**Academy of Cryptography of the Russian Federation, Moscow, Russia

We suggest an elliptic curve modification of the undeniable signature introduced by D. Chaum and H. van-Antwerpen. The signature generation algorithm is supplemented with a preliminary stage of randomization. For signature verification and disavowal protocols, two options are offered. Theorems showing that these protocols meet their purpose have been proven. A method for converting an undeniable signature into a regular digital signature is described, illustrated by the Schnorr electronic signature scheme as an example.

Keywords: *digital signature, undeniable signature, elliptic curve.*

Введение

Неоспоримая цифровая подпись, иначе называемая конфиденциальной, в отличие от обычной электронной подписи не может быть проверена без участия сформировавшего её лица. Поэтому она обеспечивает конфиденциальность и частичную анонимность подписавшей стороны. Название «неоспоримая подпись» объясняется тем, что если подписавшая сторона будет обязана участвовать в процедуре проверки подписи, то она не сможет отказаться от факта подписания документа, если подпись является настоящей, но сможет доказать, что это не её подпись, если она не подписывала документ.

Как отмечают авторы схемы, данный вид подписи удобен для компаний, занимающихся удалённым распространением своей продукции. Предположим, некоторая компания желает осуществить удалённую продажу произведённого ею программного продукта. В этом случае в роли текста выступает код программного продукта. Приобретя программные продукты, снабжённые лицензией с неоспоримыми подписями, покупатель после оплаты может получить доказательство её корректности, гарантирующее оригинальность продукта. Если же он не произвёл оплату, то никакими способами не сможет убедиться в достоверности подписи и лицензионности самого программного продукта, возможно, содержащего вредоносный код. С другой стороны, если вредоносный код будет обнаружен, то продавец может доказать, что выданную от его имени лицензию с неоспоримой подписью он никогда не создавал.

Для того чтобы у покупателя осталось подтверждение положительного результата проведённой проверки корректности неоспоримой подписи, она может быть конвертирована в обычную цифровую подпись, которая может быть привязана к имеющейся неоспоримой подписи, а также к идентификационным данным покупателя для того, чтобы независимый арбитр всегда мог убедиться в легитимности подписи и лицензионности продукта.

Исследованию неоспоримых подписей посвящено значительное количество публикаций. Их авторы сосредоточены в основном на распространении схем неоспоримой подписи на различные практические ситуации: (t, n)-пороговые схемы [1, 2], стойкие схемы неоспоримых подписей [3, 4], схема с возможностью конвертирования в обычную цифровую подпись [5, 6], схемы, позволяющие построить протокол честного обмена секретами [7], схемы с открытыми ключами на основе идентификационной информации [8], применение неоспоримых сертификатов для проверки подписей [9], схемы с делегированием права проверки подписи, позволяющие подписывающему лицу заранее назначить верификатора, способного проверить или отвергнуть подпись без участия подписавшего [10, 11], схемы подписи, не требующие сертификатов [12], содержащих указание на автора подписи, групповые неоспоримые подписи и др.

В исходных работах [13, 14] для построения схемы неоспоримой подписи Д. Чаум и Х. ван Антверпен использовали мультипликативную группу конечного поля. В дальнейшем было исследовано множество других вариантов построения схем неоспоримых цифровых подписей на основе различных математических конструкций: на основе RSA [5, 6], схемы с трудоёмким возведением в чётную степень по составному модулю [15], на основе логарифмирования в полной линейной группе над групповым кольцом [16], на основе группы кос [17], на основе операции билинейного спаривания [7, 8], на основе неабелевых групп [18], на основе изогений эллиптических кривых [19], на решётках [20] и др.

В связи с появлением субэкспоненциальных алгоритмов дискретного логарифмирования в целях повышения стойкости большинство вариантов схем цифровых подписей было адаптировано для циклических подгрупп группы точек эллиптической кривой путём замены операции умножения в конечном поле на операцию сложения в группе точек эллиптической кривой. Так, в США, России, Беларуси и др. государствах были приняты новые национальные стандарты цифровых подписей (ECDSA, ГОСТ Р 34.11-2012, СТБ 34.101.45-2013).

Для эллиптических кривых предложено много способов построения различных вариантов неоспоримых подписей. Вместе с тем эллиптические кривые с операцией спаривания составляют относительно небольшой класс эллиптических кривых, к тому же обладающий потенциальной уязвимостью к сведению двумерного представления

к одномерному. Поэтому представляет интерес нахождение способов построения таких подписей на основе групп точек эллиптических кривых без использования операции спаривания. Этой задаче в литературе уделено меньше внимания. Авторам удалось найти только одну публикацию [21], в которой схема Чаума — ван-Антверпена из [14] дословно перенесена с мультипликативной группы конечного поля на случай группы точек эллиптической кривой. Следует заметить, что предложенная в [21] схема обладает тем недостатком, что для неё необходим алгоритм вложения значения произвольной хеш-свёртки открытого текста в циклическую подгруппу группы точек эллиптической кривой, что представляет неудобство с практической точки зрения, ограничивая область применения.

В настоящей работе предложен способ модификации схемы неоспоримой цифровой подписи Чаума — ван Антверпена применительно к циклической подгруппе группы точек эллиптической кривой, не обладающий подобным недостатком. Для решения проблемы соответствия между числовыми значениями и точками этой подгруппы применён приём, решающий эту проблему за счёт введения в алгоритм формирования цифровой подписи предварительного этапа рандомизации алгоритма по аналогии со схемами цифровых подписей семейства Эль-Гамаля и подписи Шнорра, используемыми в национальных стандартах. Предложено два аналогичных варианта протоколов, а также алгоритм преобразования неоспоримой подписи в обычную цифровую подпись, сформированную аналогично схеме подписи Шнорра.

1. Протоколы неоспоримой подписи

Приведём необходимые для дальнейшего изложения сведения. Пусть p — простое, $p > 3$ и $\mathrm{GF}(p)$ — конечное поле из p элементов. Каждому элементу a поля $\mathrm{GF}(p)$ поставим в соответствие его представление в двоичном алфавите вектором длины $\lceil \log_2 p \rceil$, которое будем обозначать $\bar{a}$.

Для модификации схемы подписи Д. Шаума и Х. ван-Антверпена будем использовать такой же класс эллиптических кривых, как и в ГОСТ Р 34.10-2012 [22]. Уравнение эллиптической кривой $E_{a,b}(\mathrm{GF}(p))$ имеет вид

$$y^2 = x^3 + ax + b \pmod p,$$

где $a, b \in \mathrm{GF}(p)$. Точки кривой — это пары (x, y), удовлетворяющие этому уравнению, а также специальная бесконечно удалённая точка $\mathcal{O}$. Для обеспечения условия гладкости, которое позволяет ввести на множестве точек кривой групповую операцию, должно выполняться условие на дискриминант $4a^3 + 27b^2 \neq 0$.

Пусть $m = |E_{a,b}(\mathrm{GF}(p))|$ и $P = (x_P, y_P) \neq \mathcal{O}$ — точка эллиптической кривой, порождающая циклическую подгруппу $\langle P \rangle$ порядка q, где q — большое простое число, делящее порядок группы точек эллиптической кривой $m = qd$. Эллиптическая кривая и точка P должны быть выбраны таким образом, чтобы задача дискретного логарифмирования для элементов циклической группы $\langle P \rangle$ была труднорешаемой. Поэтому далее будем полагать, что эллиптическая кривая и точка P выбраны в соответствии с требованиями ГОСТ Р 34.10-2012. Кроме того, не ограничивая общности, будем полагать, что q^2 не делит m. Это условие не является исключительным, поскольку выполняется автоматически при выборе эллиптической кривой и циклической подгруппы с высокой эффективностью реализации: $q \approx m$ и соответственно $m \ll q^2$. Данные предположения делают невозможным успешное проведение MOV-атаки в задаче дискретного логарифмирования для циклической группы $\langle P \rangle$ большого простого

порядка q, относительного которого кривая обладает достаточно большой степенью вложения (в соответствии с ГОСТ Р 34.10-2012).

Обозначим $V_\infty = \bigcup\limits_{m \geqslant 1} V_m$, где V_m — множество двоичных последовательностей длины m. Пусть также $h : V_\infty \to V_{\lceil \log_2 p \rceil}$ — хеш-функция, удовлетворяющая условию однонаправленности, а также устойчивости к подбору коллизий и второго прообраза.

Ключом подписи является целое число k, $1 < k < q$, а ключом проверки подписи — точка $Q = [k]P = \underbrace{P + \ldots + P}_{k}$, точнее, строка $\bar{x}_Q || \bar{y}_Q$ — конкатенация двоичных векторов $\bar{x}_Q, \bar{y}_Q \in V_{\lceil \log_2 p \rceil}$, соответствующих координатам (x_Q, y_Q) точки Q.

Схема неоспоримой цифровой подписи включает три протокола:

— алгоритм формирования подписи;
— протокол её проверки при участии подписавшего;
— протокол отказа от подписи, т. е. доказательства того факта, что автором подписи данное лицо не является.

Предлагаемые ниже варианты схем неоспоримой подписи являются рандомизированными модификациями неоспориомой подписи Чаума — ван-Антверпена, адаптированными для случая группы точек эллиптической кривой.

1.1. Первый вариант

Пусть A и B обозначают соответственно доказывающую и проверяющую стороны.

1. *Алгоритм формирования подписи*

(1) вычислить хеш-код $h(T)$ сообщения $T \in V_\infty$;
(2) вычислить целое число t, двоичным представлением которого является вектор $h(T)$, и определить $l = t \bmod q$. Если $l = 0$, то определить $l = 1$;
(3) сгенерировать случайное (псевдослучайное) целое число r, $1 < r < q$, $r \neq l$;
(4) вычислить точку $R = [r]P = (x_R, y_R)$ эллиптической кривой $E_{a,b}(\mathrm{GF}(p))$;
(5) вычислить целое число $s = k(l - r) \bmod q$;
(6) вычислить двоичные векторы $\bar{x}_R, \bar{y}_R \in V_{\lceil \log_2 p \rceil}$ и $\bar{s} \in V_{\lceil \log_2 p \rceil}$, соответствующие координатам точки $R = (x_R, y_R)$ и числу s, определить цифровую подпись

$$sig(T) = \bar{x}_R || \bar{y}_R || \bar{s}.$$

Для краткости рассуждений будем полагать, что подписью является пара (R, s), не акцентируя внимание на том, что её в дальнейшем надо преобразовать в двоичную строку.

2. *Протокол проверки подписи*

(0) B: если $R \notin \langle P \rangle$ или $s = 0$, то подпись некорректна;
(1) B: генерирует $e_1, e_2 : 0 \leqslant e_1, e_2 \leqslant q - 1$;
вычисляет $C = [e_1]P + [e_2]R$;
(2) B: если $C = \mathcal{O}$, перейти к (1);
(3) $A \leftarrow B$: C;
(4) A: если $C \notin \langle P \rangle$, завершить выполнение;
(5) $A \to B$: $D = [k]C$;
(6) B: проверяет равенство: $D \stackrel{?}{=} [e_1]Q + [e_2]([l]Q - [s]P)$.

На шаге (0) выполняется проверка включения $R \in \langle P \rangle$, необходимого для корректности формирования подписи, а также для того, чтобы точки C и D принадлежали

циклической группе $\langle P\rangle$. Для этого надо сначала убедиться, что $R \in E_{a,b}(\mathrm{GF}(p))$, а затем — что её порядок равен q, путём проверки равенства $[m/q-1]R = -R$. Случай $s = 0$ недопустим при формировании подписи, так как в этом случае $r = l$, пара $(R, 0)$ не зависит от ключа подписи k и поэтому при любом ключе удовлетворяет протоколу проверки подписи.

Проверка условия $C = \mathcal{O}$ на шаге (2) проводится сравнением точек $[e_1]P \stackrel{?}{=} -[e_2]R$. Заметим, что нахождение такой пары e_1, e_2 приводит к раскрытию ключа k. Из сравнения $e_1 = -e_2 r \bmod q$ можно вычислить r, а затем $k = s(l-r)^{-1} \bmod q$. Вероятность такого события равна $1/q$.

Корректность протокола вытекает из равенств

$$\begin{aligned} D = kC &= [k]([e_1]P + [e_2]R) = [e_1]([k]P) + [e_2]([k]R) = \\ &= [e_1]Q + [e_2]([kl]P - [kl]P + [rk]P) = \\ &= [e_1]Q + [e_2]([lk]P - [(l-r)k]P) = \\ &= [e_1]Q + [e_2]([l]Q - [s]P). \end{aligned}$$

Данный протокол обеспечивает нулевое разглашение информации о ключе подписи, так как проверяющая сторона может для любого ключа проверки подписи Q самостоятельно получить любое число корректных стенограмм (e_1, e_2, C, D) выполнения протокола, задавая произвольные числа e_1, e_2, $0 \leqslant e_1, e_2 < q-1$, и вычисляя точки C и D по формулам

$$C = [e_1]P + [e_2]R, \quad D = [e_1]Q + [e_2]([l]Q - [s]P). \tag{1}$$

При этом ключ подписи k никак не задействован.

С другой стороны, в ходе реализации протокола будут возникать только точки R, C и D из циклической подгруппы $\langle P\rangle$ большого простого порядка q группы точек эллиптической кривой. Вычисленные по формулам (1) пары (C, D) ничего не дают для определения ключа подписи k подписавшей стороны, поскольку нахождение k равносильно решению задачи дискретного логарифмирования $D = [k]C$, или, что равносильно, решению уравнений $[l]Q - [s]P = [k]R$ или $Q = [k]P$. В силу выбора параметров кривой m и q MOV-атака для задачи дискретного логарифмирования в этой группе оказывается неэффективной, а шаг 4 защищает от возможности применения атаки на ключ k типа «малая подгруппа» со стороны B, когда B может отправлять стороне A специально подобранные элементы малых порядков из группы точек эллиптической кривой. Невыполнение проверяемого на шаге (4) равенства доказывает стороне A, что полученная от B точка C имеет порядок q.

Поэтому данный протокол обеспечивает конфиденциальность подписавшей стороны, а также защищает от возможности подделки подписи путём раскрытия ключа подписи.

Замечание 1. В протоколах, относящихся к семейству Эль-Гамаля, и в протоколе Шнорра повторение числа r, которое применяется для рандомизации протокола формирования подписи, приводит к возможности раскрытия ключа. В данном случае это также имеет место. Пусть имеются два сообщения T_1 и T_2, подписанные стороной A, подписи для которых (R, s_1) и (R, s_2) получены при одинаковых значениях r. В этом случае значения k и r можно найти из системы уравнений

$$\begin{cases} s_1 = k(l_1 - r), \\ s_2 = k(l_2 - r). \end{cases}$$

Это событие маловероятно, так как при равномерном распределении значений r его вероятность оценивается как $1/q$.

Можно предложить модификацию алгоритма формирования подписи, где значение $R = f(r, l)P$ зависит от r и l. Однако такое решение не устраняет проблему, так как если у подписей для сообщений T_1 и T_2 совпадут значения $f(r_1, l_1) = f(r_2, l_2)$, то получается аналогичная система:

$$\begin{cases} s_1 = k(l_1 - f(r_1, l_1)), \\ s_2 = k(l_2 - f(r_2, l_2)), \end{cases}$$

при этом вероятность данного события оценивается как $1/q$, точно так же, как и в случае повторения числа r в исходном варианте алгоритма.

3. *Протокол отказа от подписи* состоит в двукратном повторении протокола проверки подписи с последующей проверкой равенства на шаге (9), позволяющего обнаружить нечестное поведение подписывающей стороны:

(0) B: если $R \notin \langle P \rangle$ или $s = 0$, то подпись некорректна;
(1) B: генерирует $e_1, e_2 : 0 \leqslant e_1, e_2 \leqslant q - 1$;
вычисляет $C_1 = [e_1]P + [e_2]R$;
(2) B: если $C_1 = \mathcal{O}$, перейти к (1);
(3) $A \leftarrow B$: C_1;
(4) A: если $C_1 \notin \langle P \rangle$, завершить выполнение;
(5) $A \to B$: $D_1 = [k]C_1$;
(6) B: проверяет равенство: $D_1 \stackrel{?}{=} [e_1]Q + [e_2]([l]Q - [s]P)$;
(7) B: генерирует $f_1, f_2 : 0 \leqslant f_1, f_2 \leqslant q - 1$;
вычисляет $C_2 = [f_1]P + [f_2]R$;
(8) B: если $C_2 = \mathcal{O}$, перейти к (1);
(9) $A \leftarrow B$: C_2;
(10) A: если $C_2 \notin \langle P \rangle$, завершить выполнение;
(11) $A \to B$: $D_2 = [k]C_2$;
(12) B: проверяет равенство: $D_2 \stackrel{?}{=} [f_1]Q + [f_2]([l]Q - [s]P)$;
(13) B: проверяет равенство: $[f_2](D_1 - [e_1]Q) \stackrel{?}{=} [e_2](D_2 - [f_1]Q)$.

Протокол выполняется за 13 шагов: шаги 1–6 и 7–12 повторяют предыдущий протокол, а шаг 13 — это проверка, что A честно выполнял предыдущие действия. Если A не ставил свою подпись и правильно выполнял протокол, то шаги 6 и 12 протокола будут свидетельствовать о нарушении условия проверки подписи, а на шаге 13 будет подтверждено, что участник A корректно выполнял протокол. Тем самым будет с большой вероятностью доказано, что эту подпись поставил не он (см. теорему 2). Если же он обманывает, то для отказа от подписи участник A должен дважды отправить неправильные значения D_1 на шаге 5 и D_2 на шаге 11. Отправка неправильных значений на шагах 5 и 11 протокола со стороны A будет обнаружена проверяющей стороной B при нарушении последнего равенства на шаге 13 (см. теорему 3).

Теоретическое обоснование надежности схемы проводится аналогично рассуждениям в [14].

Теорема 1. Пусть сторона A, обладающая ключом подписи k, $Q = [k]P$, участвует в протоколе проверки подписи (R, s) для сообщения с хеш-свёрткой l, где $R = [r]P$, $r \neq l$, которую она не создавала. Если $s \neq k(l - r) \bmod q$, то вероятность того, что проверяющая сторона B признает корректность подписи, равна $1/q$.

Доказательство. Рассмотрим стенограмму (C, D) выполнения протокола проверки подписи

$$\begin{cases} C = [e_1]P + [e_2]R, \\ D = [k]C \end{cases}$$

относительно неизвестных упорядоченных пар (e_1, e_2).

Проверяющая сторона B признает корректность подписи только в случае, когда выполнено равенство

$$D = [e_1]Q + [e_2]([l]Q - [s]P). \tag{2}$$

Если бы подпись (R, s) была сформирована участником A, то вторая компонента подписи равнялась бы $s_0 = k(l - r)$, откуда

$$[k]C = [k]([e_1]P + [e_2]R) = [e_1]Q + [e_2]([l]Q - [s_0]P).$$

Поэтому равенство (2) можно переписать в виде

$$[e_1]Q + [e_2]([l]Q - [s_0]P) = [e_1]Q + [e_2]([l]Q - [s]P).$$

Оно будет выполнено только в случае

$$[e_2(s - s_0)]P = 0,$$

где $s - s_0 \neq 0$, а значит, $e_2 = 0$. Следовательно, для запроса $C = [e_1]P + [e_2]R$ ответ D на него может быть признан корректным, только если $(e_1, e_2) = (e_1, 0)$. Таким образом, среди q^2 пар (e_1, e_2) число пар, для которых ответ будет признан корректным, равно q. ■

Теорема 2. Пусть сторона A, обладающая ключом подписи k, $Q = [k]P$, участвует в протоколе отказа от подписи (R, s) для сообщения с хеш-сверткой l, где $R = [r]P$, $r \neq l$, которую она не создавала. Если $s \neq k(l - r) \bmod q$, но A и B корректно выполняют протокол отказа от подписи, то равенство

$$[f_2](D_1 - [e_1]Q) = [e_2](D_2 - [f_1]Q) \tag{3}$$

выполнено.

Доказательство. Доказательство основывается на том, что левая и правая части равенства (3) могут быть представлены следующим образом:

$$\begin{cases} [f_2](D_1 - [e_1]Q) & = [f_2]([k]([e_1]P + [e_2]R) - [e_1]Q) = \\ & = [f_2]([e_1k]P + [e_2k]R - [e_1]Q) = [f_2e_2k]R, \\ [e_2](D_2 - [f_1]Q) & = [e_2](([k][f_1]P + [f_2]R) - [f_1]Q) = \\ & = [e_2]([f_1k]P + [f_2k]R - [f_1]Q) = [e_2f_2k]R. \end{cases}$$

Теорема 2 доказана. ■

Теорема 3. Пусть сторона A, обладающая ключом подписи k, $Q = [k]P$, участвует в протоколе отказа от подписи (R, s) для сообщения с хеш-сверткой l, где $R = [r]P$, $r \neq l$, которую она создала, но не хочет в этом сознаваться. Пусть $s = k(l - r)$ и проверяющая сторона B корректно выполняет протокол. Если сторона A на шагах 4 и 10 протокола отправляет сообщения

$$D_1 \neq [e_1]Q + [e_2]([l]Q - [s]P), \quad D_2 \neq [f_1]Q + [f_2]([l]Q - [s]P),$$

то вероятность того, что равенство (3) будет нарушено, равна $1 - 1/q$.

Доказательство. Предположим, что равенство (3) выполнено. Преобразуем его:

$$[e_2]D_2 = [e_2 f_1]Q + [f_2](D_1 - [e_1]Q).$$

Если $e_2 = 0$, то оно имеет вид $[f_2](D_1 - [e_1]Q) = \mathcal{O}$, и поскольку по условию $D_1 \neq [e_1]Q$, то должно быть $f_2 = 0$. Поэтому вероятность того, что последнее равенство выполнено, равна $1/q$.

Если $e_2 \neq 0$, то равенство (3) можно привести к виду

$$D_2 = [f_1]Q + [f_2]D_0, \tag{4}$$

где $D_0 = [e_2^{-1}](D_1 - [e_1]Q)$ определяется действиями участников A и B на шагах 4 и 10 протокола отказа от подписи. Поскольку шаг 5 протокола отказа от подписи подтверждает, что $D_1 \in \langle P\rangle$, то D_0 также принадлежит циклической группе $\langle P\rangle$. Значит, найдётся элемент $l_0 \in \mathrm{GF}(p)$, для которого $D_0 = [l_0]Q - [s]P$. По условию теоремы $D_0 \neq [l]Q - [s]P$, и значит, $l_0 \neq l$. Согласно протоколу проверки подписи, выполнение равенства (4) доказывает, что подпись (R, s) соответствует сообщению со значением хеш-свертки $l_0 \neq l$, для которого выполняется неравенство $s \neq k(l_0 - r)$, причём в силу теоремы 1 вероятность того, что проверяющая сторона B признает корректность подписи (R, s) для сообщения с хеш-свёрткой l, равна $1/q$.

Поэтому вероятность того, что равенство (3) будет выполнено, равна $1/q$. ■

1.2. Второй вариант

1. ***Алгоритм формирования подписи*** полностью повторяет алгоритм первого варианта.

2. ***Протокол проверки подписи***:

(0)	B :	если $R \notin \langle P\rangle$ или $s = 0$, то подпись некорректна;
(1)	B :	генерирует $e_1, e_2 : 0 < e_1, e_2 < q - 1$;
		вычисляет $C = [e_1]([l]Q - [s]P)[+e_2]Q$;
(2)	B :	если $C = \mathcal{O}$, перейти к (1);
(3)	$A \leftarrow B$:	C;
(4)	A :	если $C \notin \langle P\rangle$, завершить выполнение;
(5)	$A \rightarrow B$:	$D = [k^{-1}]C$;
(6)	B :	проверяет равенство: $D \stackrel{?}{=} [e_1]R + [e_2]P$.

Корректность протокола вытекает из равенств

$$\begin{aligned} C &= [e_1]([l]Q - [s]P) + [e_2]Q = \\ &= [e_1]([l]Q - [(l-r)k]P) + [e_2 k]P = \\ &= [e_1]([l]Q - [l]Q + [rk]P) + [e_2 k]P = \\ &= [k]([e_1]R + [e_2]P) = [k]D. \end{aligned}$$

То, что данный протокол также обеспечивает нулевое разглашение информации о ключе подписи и конфиденциальность подписавшей стороны, показывается полностью аналогично.

3. *Протокол отказа от подписи*:

(0) B: если $R \notin \langle P \rangle$ или $s = 0$, то подпись некорректна;
(1) B: генерирует $e_1, e_2 : 0 < e_1, e_2 < q - 1$;
вычисляет $C_1 = [e_1]([l]Q - [s]P)[+e_2]Q$;
(2) B: если $C_1 = \mathcal{O}$, перейти к (1);
(3) $A \leftarrow B$: C_1;
(4) A: если $C_1 \notin \langle P \rangle$, завершить выполнение;
(5) $A \rightarrow B$: $D_1 = k^{-1}C_1$;
(6) B: проверяет равенство: $D_1 \stackrel{?}{=} [e_1]R + [e_2]P$;
(7) B: генерирует $f_1, f_2 : 0 < f_1, f_2 < q - 1$;
вычисляет $C_2 = [f_1]([l]Q - [s]P)[+f_2]Q$;
(8) B: если $C_2 = \mathcal{O}$, перейти к (1);
(9) $A \leftarrow B$: C_2;
(10) A: если $C_2 \notin \langle P \rangle$, завершить выполнение;
(11) $A \rightarrow B$: $D_1 = [k^{-1}]C_1$;
(12) B: проверяет равенство: $D_2 \stackrel{?}{=} [f_1]R + [f_2]P$;
(13) B: $M_1 = D_1 - ([e_1]R + [e_2]P)$,
(14) B: $M_2 = D_2 - ([f_1]R + [f_2]P)$,
(15) B: проверяет равенство: $[f_1]M_1 = [e_1]M_2$.

Теоретическое обоснование надёжности схемы повторяет рассуждения для первого варианта.

2. Преобразования в обычную цифровую подпись

Пусть имеется уже сформированная неоспоримая подпись (R, s) для сообщения T, полученная для ключевой пары (k, Q). Предлагаемый способ является по сути не конвертацией, а заменой неоспоримой подписи на обычную цифровую подпись, полученную при том же ключе подписи k с учётом зависимости от ранее сформированной неоспоримой подписи. Рассмотрим вариант преобразования, использующий схему цифровой подписи, аналогичную схеме подписи Шнорра [23].

Для преобразования неоспоримой подписи (R, s) в обычную владелец ключа подписи вычисляет пару (x, s') в соответствии со следующим алгоритмом:

***Алгоритм формирования цифровой подписи*:**

(1) выбрать случайный элемент r', $1 < r' < q$;
(2) вычислить точку эллиптической кривой $R' = [r']P = (x_{R'}, y_{R'})$;
(3) вычислить точку $Q' = [l]Q - [s]P = (x_{Q'}, y_{Q'})$;
(4) вычислить целое число t', двоичным представлением которого является вектор $h(T||\bar{x}_{Q'}||\bar{y}_{Q'}||\bar{x}_{R'}||\bar{y}_{R'})$, и определить $l' = t' \bmod q$. Если $l' = 0$, то определить $l' = 1$;
(5) вычислить $s' = kl' - r' \bmod q$.

Покажем, что $\bar{l}'||\bar{s}'$ является обычной цифровой подписью для сообщения T (для удобства будем, как и выше, использовать запись (l', s')).

Имея неоспоримую подпись (R, s), цифровую подпись (l', s') и открытый ключ Q, любой проверяющий B может осуществить проверку подписи в соответствии со следующим алгоритмом:

Алгоритм проверки цифровой подписи:

(1) вычислить $Y = lQ - sP = (x_Y, y_Y)$;
(2) вычислить $Z = l'Q - s'P = (x_Z, y_Z)$;
(3) вычислить целое число w, двоичным представлением которого является вектор $h(T||\bar{x}_Y||\bar{y}_Y||\bar{x}_Z||\bar{y}_Z)$, и определить $w' = w \bmod q$. Если $w' = 0$, то определить $w' = 1$;
(4) проверить соответствие $l' \stackrel{?}{\leftrightarrow} w$; если оно выполнено, то подпись (l', s') принимается и признается корректной; в противном случае отвергается.

Корректность алгоритма.
Из равенств $s = k(l - r)$ и $s' = kl' - r'$ следует

$$[s]P = [k(l-r)]P = [l]Q - [r]Q,$$
$$[s']P = [kl']P - [r']P = [l']Q - R',$$

а значит, должны выполняться равенства

$$Y = [l]Q - [s]P = Q',$$
$$Z = [l']Q - [s']P = R'.$$

Таким образом, $w' = l'$.

В случае, когда автор неоспоримой подписи, занимающийся удалённым распространением своей продукции, после проведённой проверки неоспоримой подписи пожелает осуществить привязку сформированной цифровой подписи к идентификационным данным ID покупателя, он может внести эти данные в хеш-функцию

$$h(T||x_{rQ}||y_{rQ}||x_{R'}||y_{R'}||ID),$$

тем самым подтверждая положительный результат проверки неоспоримой подписи и лицензионность приобретённого покупателем программного продукта.

Авторы выражают благодарность С. В. Агиевичу за многочисленные полезные замечания и исправления.

ЛИТЕРАТУРА

1. *Harn L. and Yang S.* Group-oriented undeniable signature schemes without the assistance of a mutually trusted party // LNCS. 1993. V. 718. P. 133–142.
2. *Wang G. and Qing S.* A threshold undeniable signature scheme without a trusted party // J. Software. 2002. V. 13. No. 9. P. 1757–1764.
3. *Chaum D., van Heijst E., and Pfitzmann B.* Cryptographically strong undeniable signatures, unconditionally secure for the signer // LNCS. 1992. V. 576. P. 470–484.
4. *Zhu H.* Universal Undeniable Signatures. ePrint Archive. `eprint.iacr.org/2004/005`.
5. *Boyar J., Chaum D., Damgard I., and Pedersen T.* Convertible undeniable signatures // LNCS. 1991. V. 537. P. 189–205.
6. *Gennaro R., Krawczyk H., and Rabin T.* RSA-based undeniable signature // LNCS. 1997. V. 1294. P. 132–148.
7. *Horng S.-J., Tzeng S.-F., Fan P., et al.* Secure convertible undeniable signature scheme using extended Euclidean algorithm without random oracles // KSII Trans. Internet Inform. Systems. 2013. V. 7. No. 6. `http://dx.doi.org/10.3837/tiis.2013.06.010`.
8. *Libert Q. and Quisquater J.-J.* Identity Based Undeniable Signatures. ePrint Archive. `eprint.iacr.org/2003/206`.

9. *Gennaro R., Krawczyk Y. M., and Rabin T. D.* Udeniable Certificates for Digital Signature Verification. United States Patent No. US 6292897 B1, Sep. 18, 2001.
10. *Chaum D.* Designated confirmer signatures // LNCS. 1994. V. 950. P. 86–91.
11. *Okamoto T.* Designated confirmer signatures and public-key encryption are equivalent // LNCS. 1994. V. 839. P. 61–74.
12. *Duan S.* Certificateless undeniable signature scheme // Inform. Sci. 2008. V. 178. Iss. 3. P. 742–755.
13. *Chaum D.* Zero-knowledge undeniable signatures // LNCS. 1991. V. 473. P. 458–464.
14. *Chaum D. and Van-Antwerpen H.* Undeniable signature // LNCS. 1990. V. 435. P. 212–216.
15. *Mao W.* New Zero-knowledge Undeniable Signatures — Forgery of Signature Equivalent to Factorisation. ePrint Archive. `eprint.iacr.org/2001-011`.
16. *Pandey A. and Gupta I.* A new undeniable signature scheme on general linear group over group ring // J. Discrete Math. Sci. Cryptography. 2020. P. 1–13. `https://doi.org/10.1080/09720529.2020.1744814`.
17. *Thomas T. and Lal A. K.* Undeniable Signature Schemes Using Braid Groups. `https://arxiv.org/abs/cs/0601049`.
18. *Thomas T. and Lal A. K.* A zero-knowledge undeniable signature scheme in non-Abelian group setting // Intern. J. Network Security. 2008. V. 6. No. 3. P. 265–269.
19. *Jao J. and Soukharev V.* Isogeny-based quantum-resistant undeniable signatures // LNSC. 2014. V. 8772. P. 160–179.
20. *Tian M. and Huang L.* Efficient Identity-Based Signature from Lattices. `https://hal.inria.fr/hal-01370379`. 2016.
21. *Александрова Е. Б., Шкоркина Е. Н.* Применение неоспоримой подписи на эллиптических кривых для верификации сервера при аутсорс-вычислениях // Проблемы информационной безопасности. Компьютерные системы. СПб.: Изд-во СПбТУ, 2018. С. 97–101.
22. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. `https://docs.cntd.ru/document/1200095034`.
23. *Schnorr C. P.* Efficient identification and signature for smart cards // LNCS. 1990. V. 435. P. 235–251.

REFERENCES

1. *Harn L. and Yang S.* Group-oriented undeniable signature schemes without the assistance of a mutually trusted party. LNCS, 1993, vol. 718, pp. 133–142.
2. *Wang G. and Qing S.* A threshold undeniable signature scheme without a trusted party. J. Software, 2002, vol. 13, no. 9, pp. 1757–1764.
3. *Chaum D., van Heijst E., and Pfitzmann B.* Cryptographically strong undeniable signatures, unconditionally secure for the signer. LNCS, 1992, vol. 576, pp. 470–484.
4. *Zhu H.* Universal Undeniable Signatures. ePrint Archive, `eprint.iacr.org/2004/005`.
5. *Boyar J., Chaum D., Damgard I., and Pedersen T.* Convertible undeniable signatures. LNCS, 1991, vol. 537, pp. 189–205.
6. *Gennaro R., Krawczyk H., and Rabin T.* RSA-based undeniable signature. LNCS, 1997, vol. 1294, pp. 132–148.
7. *Horng S.-J., Tzeng S.-F., Fan P., et al.* Secure convertible undeniable signature scheme using extended Euclidean algorithm without random oracles. KSII Trans. Internet Inform. Systems, 2013, vol. 7, no. 6, `http://dx.doi.org/10.3837/tiis.2013.06.010`.
8. *Libert Q. and Quisquater J.-J.* Identity Based Undeniable Signatures. ePrint Archive. `eprint.iacr.org/2003/206`.

9. *Gennaro R., Krawczyk Y. M., and Rabin T. D.* Udeniable Certificates for Digital Signature Verification. United States Patent No. US 6292897 B1, Sep. 18, 2001.
10. *Chaum D.* Designated confirmer signatures. LNCS, 1994, vol. 950, pp. 86–91.
11. *Okamoto T.* Designated confirmer signatures and public-key encryption are equivalent. LNCS, 1994, vol. 839, pp. 61–74.
12. *Duan S.* Certificateless undeniable signature scheme. Inform. Sci., 2008, vol. 178, iss. 3, pp. 742–755.
13. *Chaum D.* Zero-knowledge undeniable signatures. LNCS, 1991, vol. 473, pp. 458–464.
14. *Chaum D. and Van-Antwerpen H.* Undeniable signature. LNCS, 1990, vol. 435, pp. 212–216.
15. *Mao W.* New Zero-knowledge Undeniable Signatures — Forgery of Signature Equivalent to Factorisation. ePrint Archive. `eprint.iacr.org/2001-011`.
16. *Pandey A. and Gupta I.* A new undeniable signature scheme on general linear group over group ring. J. Discrete Math. Sci. Cryptography, 2020, pp. 1–13, `https://doi.org/10.1080/09720529.2020.1744814`.
17. *Thomas T. and Lal A. K.* Undeniable Signature Schemes Using Braid Groups. `https://arxiv.org/abs/cs/0601049`.
18. *Thomas T. and Lal A. K.* A zero-knowledge undeniable signature scheme in non-Abelian group setting. Intern. J. Network Security, 2008, vol. 6, no. 3, pp. 265–269.
19. *Jao J. and Soukharev V.* Isogeny-based quantum-resistant undeniable signatures. LNSC, 2014, vol. 8772, pp. 160–179.
20. *Tian M. and Huang L.* Efficient Identity-Based Signature from Lattices. `https://hal.inria.fr/hal-01370379`. 2016.
21. *Aleksandrova E. B. and Shkorkina E. N.* Primenenie neosporimoy podpisi na ellipticheskikh krivykh dlya verifikatsii servera pri autsors-vychisleniyakh [Elliptic curve undeniable signature for server verification in outsource computations]. Problemy Informatsionnoy Bezopasnosti. Komp'yuternye Sistemy. SPbTU Publ., 2018, pp. 97–101. (in Russian)
22. GOST R 34.10-2012. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Protsessy formirovaniya i proverki elektronnoy tsifrovoy podpisi [Informatiom technology. Cryptographic protection information. Electronic digital signature process]. `https://docs.cntd.ru/document/1200095034`. (in Russian)
23. *Schnorr C. P.* Efficient identification and signature for smart cards. LNCS, 1990, vol. 435, pp. 235–251.