УДК 681.3

А.И. КОЧУБИНСКИЙ, А.М. ФАЛЬ

АЛГОРИТМЫ ВЫЧИСЛЕНИЯ СЛЕПОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ НАЦИОНАЛЬНОГО СТАНДАРТА УКРАИНЫ ЦИФРОВОЙ ПОДПИСИ ДСТУ 4145-2002 И РОССИЙСКОГО СТАНДАРТА ЦИФРОВОЙ ПОДПИСИ ГОСТ Р 34.10-2001[1]

Ключевые слова: *слепая цифровая подпись, стандарт, криптографическое преобразование, дискретный логарифм, алгоритмы вычисления и проверки подписи.*

Понятие о слепой цифровой подписи было предложено Д. Хаумом [1]. Такая подпись вычисляется в процессе взаимодействия двух участников — клиента и сервера. В итоге клиент получает подписанное сообщение, при этом сервер не имеет доступа к документу клиента, для которого вычисляется цифровая подпись, и не может аутентифицировать клиента, запросившего услугу относительно вычисления слепой цифровой подписи. В результате вычислений формируется стандартная цифровая подпись. Иными словами, для проверки подписи используется обычный алгоритм проверки цифровой подписи, соответствующий криптографическому преобразованию, выбранному для построения слепой цифровой подписи. Этот алгоритм может применяться в платежных системах, при организации избирательного процесса и любых других областях, где принципиально важно обеспечение анонимности клиента. Д. Хаум использовал в качестве криптографического преобразования алгоритм RSA. Позднее были описаны алгоритмы вычисления слепой цифровой подписи на основе других криптографических алгоритмов. В частности, в работе [2] описан достаточно общий способ построения алгоритмов вычисления слепой цифровой подписи на основе криптографических преобразований, стойкость которых базируется на задаче дискретного логарифмирования. В настоящей статье на основе подхода, описанного в [2], формулируются алгоритмы вычисления слепой цифровой подписи, исходя из криптографических преобразований, определенных в национальном стандарте Украины ДСТУ 4145-2002 [3] и стандарте Российской Федерации ГОСТ Р 34.10-2001 в редакции, представленной в Международном стандарте ISO/IEC 14888-3:2006/Amd1:2010 [4]. В результате появляются функциональные возможности слепой цифровой подписи в рамках существующей в Украине инфраструктуры открытых ключей, в частности пользоваться услугами действующих центров сертификации открытых ключей. В настоящей статье используется терминология и обозначения, принятые в указанных стандартах.

Пусть $E(F_q)$ — эллиптическая кривая над конечным полем F_q, $q = 2^m$, m — степень расширения конечного поля, из числа разрешенных ДСТУ 4145-2002, P — базовая точка эллиптической кривой порядка n. Эллиптическая кривая, конечное поле, базовая точка и ее порядок удовлетворяют требованиям стандарта ДСТУ 4145-2002. Пусть также d — секретный ключ цифровой подписи ДСТУ 4145-2002, а $Q = -dP$ — отвечающий этому секретному ключу открытый ключ цифровой подписи, $H(\cdot)$ — функция хэширования. Цифровая подпись

[1] Работа выполнена при поддержке гранта НАН Украины — РФФД за 2010 г. № 07-07-10 (У).

ДСТУ 4145-2002 вычисляется следующим образом. Сначала генерируется разовый секретный ключ e и определяется точка $R = eP$ эллиптической кривой. Вычисляется хэш-код $H(T)$ сообщения T, который преобразуется в элемент основного поля h. Далее вычисляется элемент основного поля $y = hx_R$, который преобразуется в целое число r и вычисляется целое число $s = (e + dr) \bmod n$. Пара чисел (r, s) образует цифровую подпись согласно ДСТУ 4145-2002. Для проверки цифровой подписи вычисляется точка $\bar{R} = sP + rQ$ $(\bar{R} = (x_{\bar{R}}, y_{\bar{R}}))$ эллиптической кривой, затем вычисляется элемент основного поля $\bar{y} = hx_{\bar{R}}$, который преобразуется в целое число $\bar{r}$. Подпись верна, если $\bar{r} = r$.

Сформулируем алгоритм вычисления слепой цифровой подписи на основе стандарта ДСТУ 4145-2002. Клиент вычисляет слепую цифровую подпись для сообщения T во взаимодействии с сервером следующим образом.

Алгоритм 1

1. По запросу клиента сервер вычисляет случайный разовый секретный ключ e и точку эллиптической кривой $R = eP$. Параметр e сервер сохраняет в секрете, а R передает клиенту.

2. Клиент вычисляет значение функции хэширования $H(T)$ и преобразует это значение в элемент h конечного поля согласно ДСТУ 4145-2002. Клиент формирует два случайных натуральных числа α и β, которые являются маскирующими параметрами слепой цифровой подписи, и вычисляет элемент конечного поля

$$y = h((\alpha P + \beta R)_x), \tag{1}$$

т.е. элемент поля h умножается на координату x точки $\alpha P + \beta R$. Вычисленный элемент конечного поля y преобразуется по правилам ДСТУ 4145-2002 в целое число r, которое является первой составляющей цифровой подписи. Наконец, клиент маскирует вычисленную первую составляющую цифровой подписи

$$\tilde{r} \equiv r\beta^{-1} \bmod n \tag{2}$$

и передает значение $\tilde{r}$ серверу.

3. Сервер вычисляет целое число $\tilde{s} \equiv \tilde{r}d + e \bmod n$. Эта величина, которая представляет собой замаскированное значение второй составляющей цифровой подписи, передается клиенту.

4. Клиент восстанавливает вторую составляющую цифровой подписи

$$s \equiv \tilde{s}\beta + \alpha \bmod n. \tag{3}$$

Пара чисел (r, s) есть цифровая подпись согласно ДСТУ 4145-2002. Действительно, для проверки цифровой подписи ДСТУ 4145-2002 необходимо вычислить выражение

$$sP + rQ = (s - rd)P,$$

$$s - rd = \tilde{s}\beta + \alpha - rd = (\tilde{r}d + e)\beta + \alpha - rd = e\beta + \alpha.$$

Следовательно, $sP + rQ = (e\beta + \alpha)P = \alpha P + \beta R$.

Если сообщение T не искажено, то после вычисления функции хэширования $H(T)$ и преобразования результата в элемент конечного поля получим снова h. Поэтому после умножения координаты x точки $sP + rQ$ на элемент поля h и преобразования результата в целое число $\bar{r}$ получим $\bar{r} = r$, что и является условием проверки цифровой подписи согласно ДСТУ 4145-2002. Стойкость описанного алгоритма вычисления и проверки слепой цифровой подписи определяется стойкостью криптографического преобразования, определенного в ДСТУ 4145-2002.

Из описания алгоритма видно, что сервер в процессе вычисления слепой цифровой подписи не имеет доступа ни к сообщению, ни к составляющим цифровой подписи. Последние становятся известными только после публикации подписанного сообщения.

Маскирующие параметры α и β однозначно по mod n определяются наблюдаемыми параметрами r, s, $\tilde{r}$ и $\tilde{s}$. Действительно, эти маскирующие параметры должны удовлетворять соотношениям (1), (2) и (3). Из соотношения (2) находим β: $\beta \equiv r\tilde{r}^{-1} \bmod n$, из соотношения (3) вычисляем α: $\alpha \equiv (s - \tilde{s}\beta) \bmod n$. Далее используя полученные значения α и β, вычисляем

$$\alpha P + \beta R = (s - \tilde{s}\beta + \beta e)P = (s + \beta(e - \tilde{s}))P =$$

$$= (s + \beta(e - \tilde{r}d - e))P = (s - r\tilde{r}^{-1}\tilde{r}d)P = sP + rQ .$$

Получено в точности проверочное выражение для цифровой подписи согласно ДСТУ 4145-2002. Поэтому вычисленные значения параметров α и β удовлетворяют соотношению (1). Поскольку клиент использует случайные значения маскирующих параметров α и β, то у сервера нет возможности связать подписанный документ с конкретным клиентом.

Обратимся теперь к стандарту Р 34.10-2001. В этом случае общесистемными параметрами являются основное поле $GF(p)$ характеристики p, представляющей простое число, группа точек эллиптической кривой E над полем $GF(p)$, $\# E$ — число точек эллиптической кривой E, G — порождающий элемент подгруппы группы точек эллиптической кривой (точка эллиптической кривой порядка q — простого делителя $\# E$), хэш-функция $H(\cdot)$ (не обязательно соответствующая российскому стандарту Р 34.11–95). Секретным ключом цифровой подписи является случайное число X, $0 < X < q$. Этому секретному ключу отвечает открытый ключ, являющийся точкой эллиптической кривой $Y = [X]G$. Цифровая подпись вычисляется следующим образом. Выбирается случайное K, $0 < K < q$, и вычисляется точка $\Pi = [K]G$. Далее определяется число $W = FE2I(\Pi_x) \bmod q$, где Π_x — координата x точки Π, *FE2I* обозначает преобразование элемента основного поля в целое число. Вычисляется хэш-код $H(T)$, который преобразуется в целое число H. Подписью является пара чисел (W, S), где $S = (WX + KH)(\bmod q)$. Для проверки цифровой подписи вычисляется точка эллиптической кривой $\overline{\Pi} = [-H^{-1}W \bmod q]Y + [H^{-1}S \bmod q]G$, координата x этой точки преобразуется в целое число $\overline{W} = FE2I(\overline{\Pi}_x)$. Подпись верна, если $\overline{W} = W$.

Предлагается следующий алгоритм вычисления слепой цифровой подписи на основе стандарта Р 34.10-2001.

Алгоритм 2

1. Сервер выбирает случайное $\tilde{K} \in Z_q$, вычисляет $\tilde{\Pi} = [\tilde{K}]G$ и отсылает $\tilde{\Pi}$ клиенту.

2. Клиент выбирает случайные $\alpha, \beta \in Z_q$ и вычисляет $\Pi = [\alpha]\tilde{\Pi} + [\beta]G$. Далее вычисляются $\tilde{W} = FE2I(\tilde{\Pi}_x) \bmod q$, $W = FE2I(\Pi_x) \bmod q$ и $\tilde{H} = \alpha H \tilde{W} W^{-1} (\bmod q)$, $\tilde{H}$ отсылается серверу.

3. Сервер вычисляет $\tilde{S} = (\tilde{K}\tilde{H} + \tilde{W}X)(\bmod q)$ и отправляет $\tilde{S}$ клиенту.

4. Клиент вычисляет $S = (\tilde{S}W\tilde{W}^{-1} + \beta H)(\bmod q)$. Подписью является пара чисел (W, S). Эта пара действительно является цифровой подписью Р 34.10-2001, поскольку

$$\overline{\Pi} = [-H^{-1}W \bmod q]Y + [H^{-1}S]G = [-H^{-1}WX + H^{-1}\widetilde{S}W\widetilde{W}^{-1} + \beta]G =$$

$$= [-H^{-1}WX + H^{-1}\widetilde{K}\widetilde{H}W\widetilde{W}^{-1} + H^{-1}WX + \beta]G = [\alpha\widetilde{K} + \beta]G = \Pi .$$

Подпись верна, если $\overline{W} = FE2I(\overline{\Pi}_x) \bmod q$ совпадает с W.

Приведем два протокола вычисления слепой цифровой подписи на основе алгоритма 1 без аутентификации сервера и с аутентификацией сервера. Для алгоритма 2 протоколы строятся аналогично. В процессе вычисления слепой цифровой подписи сервер и клиент обмениваются данными. Для формализации этого обмена будем использовать сообщения вида $\{id, mes, sign\}$, где id — целое число, уникальный идентификатор сессии вычисления слепой цифровой подписи; mes — информационная часть, т.е. набор байтов, содержащий в кодированном виде передаваемые данные; символом *null* обозначается отсутствие данных; $sign$ — цифровая подпись сообщения согласно ДСТУ 4145-2002, этот элемент сообщения может отсутствовать. Заметим, что идентификатор id идентифицирует сессию, а не клиента.

Протокол вычисления слепой цифровой подписи без аутентификации сервера. *Исходные данные сервера*: общие параметры цифровой подписи согласно ДСТУ 4145-2002 (конечное поле F_q, эллиптическая кривая $E(F_q)$ над этим полем, базовая точка P и ее порядок n), секретный ключ цифровой подписи d.

Исходные данные клиента: общие параметры цифровой подписи согласно ДСТУ 4145-2002 (конечное поле F_q, эллиптическая кривая $E(F_q)$ над этим полем, базовая точка P и ее порядок n, функция хэширования $H(\cdot)$), открытый ключ цифровой подписи Q, сообщение T в виде байтовой последовательности.

Вычисление слепой цифровой подписи состоит в следующем.

• Клиент посылает серверу сообщение $M1 = \{0, null\}$.

• Сервер вычисляет уникальный идентификатор id новой сессии вычисления слепой цифровой подписи. Сервер генерирует случайный разовый секретный ключ e и вычисляет точку $R = eP$ эллиптической кривой. Параметр e сервер привязывает к значению id и сохраняет в секрете, клиенту передается сообщение $M2 = \{id, mes1\}$, где $mes1$ — кодированное представление сжатого изображения точки R эллиптической кривой.

• Клиент декодирует принятое сообщение и восстанавливает точку R и далее вычисляет замаскированное значение $\widetilde{r}$ первой составляющей цифровой подписи согласно п. 2 алгоритма 1 и передает серверу сообщение $M3 = \{id, mes2\}$, где $mes2$ — кодированное представление целого числа $\widetilde{r}$.

• Сервер выполняет вычисления согласно п. 3 алгоритма 1 и передает клиенту сообщение $M4 = \{id, mes3\}$, где $mes3$ — кодированное представление целого числа $\widetilde{s}$.

• Клиент восстанавливает целое число s и завершает вычисление слепой цифровой подписи согласно п. 4 алгоритма 1.

• Если в процессе выполнения протокола возникают вычислительные ошибки или ошибки декодирования сообщений, то выполнение протокола прекращается.

Протокол вычисления слепой цифровой подписи с аутентификацией сервера. *Исходные данные сервера*: общие параметры цифровой подписи согласно ДСТУ 4145-2002 (конечное поле F_q, эллиптическая кривая $E(F_q)$ над этим полем, базовая точка P и ее порядок n), секретный ключ цифровой подписи d.

Исходные данные клиента: общие параметры цифровой подписи согласно ДСТУ 4145-2002 (конечное поле F_q, эллиптическая кривая $E(F_q)$ над этим полем,

базовая точка P и ее порядок n, функция хэширования $H(\cdot)$), сертификат C открытого ключа цифровой подписи, выданный одним из действующих центров сертификации открытых ключей Украины, сообщение T в виде байтовой последовательности.

Вычисление слепой цифровой подписи состоит в следующем.

• Клиент посылает серверу сообщение $M1 = \{0, null\}$.

• Сервер вычисляет уникальный идентификатор id новой сессии вычисления слепой цифровой подписи. Сервер генерирует случайный разовый секретный ключ e и вычисляет точку $R = eP$ эллиптической кривой . Параметр e сервер привязывает к значению id и сохраняет в секрете, клиенту передается сообщение $M2 = \{id, mes1, sign1\}$, где $mes1$ — кодированное представление сжатого изображения точки R эллиптической кривой, $sign1$ — цифровая подпись сообщения $M1$, вычисленная с использованием секретного ключа сервера.

• Клиент проверяет цифровую подпись принятого сообщения, используя сертификат C открытого ключа сервера. Если цифровая подпись верна, то клиент декодирует принятое сообщение и восстанавливает точку R. Далее клиент вычисляет замаскированное значение $\tilde{r}$ первой составляющей цифровой подписи согласно п. 2 алгоритма 1 и передает серверу сообщение $M3 = \{id, mes2\}$, где $mes2$ — кодированное представление целого числа $\tilde{r}$.

• Сервер выполняет вычисления согласно п. 3 алгоритма 1 и передает клиенту сообщение $M4 = \{id, mes3, sign2\}$, где $mes3$ — кодированное представление целого числа $\tilde{s}$, $sign2$ — цифровая подпись сообщения $mes3$, вычисленная с использованием секретного ключа сервера.

• Клиент проверяет цифровую подпись принятого сообщения, используя сертификат C открытого ключа сервера. Если цифровая подпись верна, то клиент восстанавливает целое число s и завершает вычисление слепой цифровой подписи согласно п. 4 алгоритма 1.

• Если в процессе выполнения протокола возникают вычислительные ошибки или ошибки декодирования сообщений, то выполнение протокола прекращается. Выполнение протокола сразу прекращается, если проверка цифровой подписи дает отрицательный результат. В процедуру проверки цифровой подписи обязательно входит проверка актуальности и действительности сертификата открытого ключа цифровой подписи сервера.

Пример вычисления слепой цифровой подписи без аутентификации сервера. Общие параметры цифровой подписи: конечное поле $GF(2^{257})$, заданное примитивным многочленом $x^{257} + x^{12} + 1$, эллиптическая кривая

$$y^2 + xy =$$
$$= x^3 + 01cef494720115657e18f938d7a7942394ff9425c1458c57861f9eea6adbe3be10,$$

базовая точка

P=(02a29ef207d0e9b6c55cd260b306c7e007ac491ca1b10c62334a9e8dcd8d20fb7,
010686d41ff744d4449fccf6d8eea03102e6812c93a9d60b978b702cf156d814ef),

порядок базовой точки

$n =$ 800000000000000000000000000000006759213af182e987d3e17714907d470d.

Секретный ключ цифровой подписи

$d =$ 35f4a5899633181992528063bc810ac455f91148f475e63083c41b05a51a4327

и отвечающий ему открытый ключ цифровой подписи

$Q =$ (01f5bbd6715fab4924a80f0112a5aa25612518b745c5d386ccdc9421e698d796d3, 05b3b6ae3493a6454f511a495e01d0ff70b58f035e56cbb0f7514bba26f234250).

Используется функция хэширования ГОСТ 34.311-95. Подписывается сообщение T, состоящее из 1024 нулевых байтов.

Процесс вычисления слепой цифровой подписи:

$$M1 = \{id = 0,\ mes = 0500\},$$

$$M2 = \{id = 4a64e1144d5fa30214472a3f4d5a4e0e,\ mes =$$

$$= 042101197C5869AF1EBE25DF496A51E67C9E92B9443726A69A83434 E446C8B1FF67597\},$$

$$M3 = \{id = 4a64e1144d5fa30214472a3f4d5a4e0e,\ mes =$$

$$= 02201ED01846FDED5C4571ED06F9855C65F2446FD72F95058C96 04DA38C789DC6072\},$$

$$M4 = \{id = 4a64e1144d5fa30214472a3f4d5a4e0e,\ mes =$$

$$= 022031FCE4193837FBD4391F5A3729226A40215ED84133D1FDF067BB2 50BCA4886DD\}.$$

Цифровая подпись:

0440D268ADDF5700378308C39F3B9366A8DEB45C970A9C62B71374DDDF17D4 8A96044AF2572B8AD92E93924C7B2662A1790B084E96BD7C3CC271ED3127878 03A4859.

Эта подпись может быть проверена любым приложением, которое реализует алгоритм проверки цифровой подписи согласно ДСТУ 4145-2002.

СПИСОК ЛИТЕРАТУРЫ

1. Chaum D. Blind signatures for untraceable payments / Advances in Cryptology CRYPTO'82. — P. 199-203.
2. Camenisch J.L., Piveteau J.-M., Stadler M.A. Blind signatures based on the discrete logarithm problem / Advances in Cryptology — EUROCRYPT '94. — 1994. — LNCS, **950**, Springer Verlag, 1995. — P. 428–432.
3. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. — Увед. 28.12.2002. — 37 с.
4. ISO/IEC 14888-3:2006/Amd1:2010 «Information technology — Security techniques — Digital signatures with appendix. Part 3: Discrete logarithm based mechanisms / Amendment 1: Elliptic Curve Russian Digital Signature Algorithm, Schnorr Digital Signature Algorithm, Elliptic Curve Schnorr Digital Signature Algorithm, and Elliptic Curve Full Schnorr Digital Signature Algorithm», 2010. — P. 32.

Поступила 11.01.2011