УДК 681.3

А. И. Кочубинский, Н. А. Молдовян, А. М. Фаль

Слепые мультиподписи на основе стандартов ДСТУ 4145-2002 и ГОСТ Р 34.10-2001

(Представлено академиком НАН Украины И. Н. Коваленко)

Приведены алгоритмы слепых мультиподписей, использующих обычные цифровые подписи, отвечающие стандартам ДСТУ 4145-2002 и ГОСТ Р 34.10-2001. Эти алгоритмы можно использовать в системах электронного документооборота и, в частности, в системах электронных платежей. Они согласованы с системами электронной цифровой подписи, внедренными в Украине и России.

Широкое внедрение цифровых подписей в системы электронного документооборота способствует разработке и реализации их разнообразных видов, приспособленных к решению вновь возникающих задач современного цифрового мира.

Одной из таких разновидностей цифровой подписи являются слепые цифровые подписи. Они изобретены в 80-х годах прошлого столетия Девидом Шаумом [1]. Слепая цифровая подпись вычисляется в процессе взаимодействия двух участников, клиента и сервера. Таким образом, 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 вычисления слепой цифровой подписи. Это свойство слепой цифровой подписи называется неотслеживаемостью. В результате вычислений формируется стандартная цифровая подпись, т. е. для проверки подписи используется обычный алгоритм проверки цифровой подписи, отвечающий выбранному для построения слепой цифровой подписи криптографическому преобразованию. Слепые цифровые подписи нашли активное применение в системах, использующих электронную наличность. Это связано как раз с тем, что слепые цифровые подписи обеспечивают свойство неотслеживаемости покупок, осуществленных владельцем электронной наличности. Второе, не менее активное, использование слепых цифровых подписей происходит в системах электронного голосования, благодаря все тому же свойству неотслеживаемости.

Как и в обычных бумажных документах, часто возникает необходимость применения нескольких подписей в электронных документах. Самым простым способом является поочередное формирование цифровых подписей различных субъектов, причастных к созданию электронного документа. В этом случае суммарная длина таких подписей растет пропорционально числу субъектов и, соответственно, увеличивается время проверки таких подписей. В тех же 80-х годах была предложена схема мультиподписи, создаваемой несколькими субъектами, но имеющей длину, равную длине одиночной подписи [2]. Такие схемы особенно удобно применять в XML-документах, в которых представители различных подразделений организации подписывают лишь ту часть документа, которая относится к их компетенции. Результирующая же мультиподпись касается всего документа и проверяется, как и обычная подпись, с помощью одного общего открытого ключа.

Ниже предлагаются алгоритмы вычисления слепой цифровой мультиподписи на основе криптографических преобразований, определенных в национальном стандарте Украины ДСТУ 4145-2002 [3, 4] и стандарте Российской Федерации Р 34.10-2001 в редакции, представленной в международном стандарте ISO/IEC 14888-3 : 2006/Amd1 : 2010 [5]. Это позволит использовать функциональные возможности слепой цифровой мультиподписи в рамках существующей на Украине инфраструктуры открытых ключей, в частности, пользоваться услугами действующих центров сертификации открытых ключей. В работе введены обозначения и терминология, принятые в указанных стандартах.

Цифровая подпись, согласно ДСТУ 4145-2002, вычисляется следующим образом. 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 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 ДСТУ 4145-2002 вычисляется так. Сначала генерируется разовый секретный ключ e и вычисляется точка эллиптической кривой $R = eP$. Вычисляется хэш-код $H(T)$ сообщения T и преобразуется в элемент основного поля h. Далее вычисляется элемент основного поля $y = h(R)_x$, $(\bullet)_x$ обозначает x — координату точки эллиптической кривой в скобках. Этот элемент основного поля преобразуется в целое число r и вычисляется целое число $s = (e + dr) \bmod n$. Пара чисел (r, s) образует цифровую подпись ДСТУ 4145-2002. Для проверки цифровой подписи вычисляется точка эллиптической кривой $\overline{R} = sP + rQ$, затем вычисляется элемент основного поля $\overline{y} = h(\overline{R})_x$. Этот элемент основного поля преобразуется в целое число $\overline{r}$. Подпись верна, если $\overline{r} = r$.

Сформулируем алгоритм вычисления слепой цифровой мультиподписи на основе стандарта ДСТУ 4145-2002. В вычислении слепой мультиподписи принимает участие группа из L субъектов, которые находятся в пределах одной локальной вычислительной сети. Все члены группы используют общую эллиптическую кривую $E(F_q)$ и одну и ту же функцию хэширования $H(\cdot)$. Каждый член группы обладает личным ключом цифровой подписи d_i и отвечающим ему открытым ключом $Q_i = -d_i P$. При работе в инфраструктуре открытых ключей все эти открытые ключи сертифицируются, это дает возможность аутентифицировать субъектов в процессе вычисления слепой мультиподписи и в случае необходимости задавать определенный порядок вычисления слепой мультиподписи. В состав локальной сети входит координатор группы, который обеспечивает взаимодействие членов группы и выполняет некоторые вычисления, в которых не используются секретные параметры, в частности, он вычисляет общий открытый ключ группы $Q = \sum_{i=1}^{L} Q_i$, который в дальнейшем используется для проверки вычисленной слепой мультиподписи. Координатор группы не имеет своих ключей. Клиент вычисления слепой мультиподписи находится вне указанной локальной вычислительной сети и взаимодействует с группой как с целым, он не имеет своей пары ключей цифровой подписи. Взаимодействие происходит через специальный шлюз, который не выполняет никаких криптографических операций. Координатор регистрирует активных членов группы, вычисление слепой мультиподписи не может начаться, пока не будут зарегистрированы все L членов группы.

Клиент вычисления слепой мультиподписи вычисляет слепую цифровую подпись для сообщения T во взаимодействии с группой следующим образом.

Клиент вычисления слепой мультиподписи вычисляет хэш-код сообщения $H(T)$ и передает вычисленный хэш-код группе через шлюз. Получение хэш-кода от клиента является для группы сигналом начала вычисления слепой мультиподписи.

Координатор инициирует вычисление слепой мультиподписи, по его сигналу каждый член группы вычисляет свой частичный разовый открытый ключ $R_i = e_i P$, где e_i — индивидуальный разовый секретный параметр.

Координатор собирает все частичные разовые открытые ключи членов группы и вычисляет общий разовый открытый ключ $R = \sum\limits_{i=1}^{L} R_i$. Координатор передает через шлюз полученный общий разовый открытый ключ клиенту вычисления слепой мультиподписи.

Клиент вычисления слепой мультиподписи преобразует хэш-код сообщения $H(T)$ в элемент основного поля h по правилам ДСТУ 4145 и вычисляет элемент основного поля

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

α и β — маскирующие параметры, затем клиент преобразует элемент основного поля y в целое число r по правилам ДСТУ 4145 и вычисляет целое число

$$\widetilde{r} = r\beta^{-1} \bmod n. \tag{2}$$

Это число клиент передает через шлюз координатору группы.

Координатор группы передает полученное целое число всем членам группы. Каждый член группы вычисляет свою частичную замаскированную цифровую подпись $(\widetilde{r}, s_i)$, где $(s_i = e_i + \widetilde{r}d_i) \bmod n$, и проверочный параметр r_i, который вычисляется путем преобразования в целое число по правилам ДСТУ 4145 элемента основного поля $y_i = h(R_i)_x$. Эти данные все члены группы передают координатору группы.

Координатор проверяет правильность каждой частичной цифровой подписи. Для этого он вычисляет точку эллиптической кривой $s_i P + \widetilde{r}Q_i$, умножает x — координату этой точки на h и преобразует полученный элемент основного поля в целое число $\widetilde{r}_i$ по правилам ДСТУ 4145. Если $\widetilde{r}_i = r_i$, то i-я частичная цифровая подпись верна. Действительно, $s_i P + \tilde{r}Q_i = e_i P$, поэтому после умножения x — координаты этой точки на h и преобразования в целое число получим в точности проверочный параметр при условии, что в процессе вычислений и передачи данных не произошло их искажения или подмены.

Если все частичные цифровые подписи верны, то координатор вычисляет вторую замаскированную составляющую цифровой подписи $\tilde{s} = \sum\limits_{i=1}^{L} s_i$ и передает ее клиенту.

Клиент вычисления слепой мультиподписи вычисляет вторую составляющую цифровой подписи по формуле

$$s = (\widetilde{s}\beta + \alpha) \mod n. \tag{3}$$

Пара чисел $(r,\ s)$ есть цифровая подпись ДСТУ 4145 и может быть проверена обычным образом.

Действительно, для проверки цифровой подписи ДСТУ 4145-2002 небходимо вычислить выражение

$$sP + rQ = \left(s - r\sum_{i=1}^{L} d_i\right)P,$$

$$s - r\sum_{i=1}^{L} d_i = \sum_{i=1}^{L} s_i\beta + \alpha - r\sum_{i=1}^{L} d_i = \alpha + \beta\sum_{i=1}^{L}(e_i + r\beta^{-1}d_i) - r\sum_{i=1}^{L} d_i = \alpha + \beta\sum_{i=1}^{L} e_i.$$

Следовательно,

$$sP + rQ = \left(\beta\sum_{i=1}^{L} e_i + \alpha\right)P = \alpha P + \beta R.$$

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 x-координаты 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 $\bmod n$ 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:

$$\beta \equiv r\widetilde{r}^{-1} \mod n,$$

Из соотношения (3) вычисляем α:

$$\alpha \equiv (s - \widetilde{s}\beta) \mod n.$$

Далее, используя полученные значения α и β, вычислим

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

Получили в точности проверочное выражение для цифровой подписи 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.

Для работы в инфраструктуре открытых ключей общий открытый ключ должен быть сертифицирован одним из центров сертификации открытых ключей. Одним из этапов такой сертификации является вычисление подписанной группой заявки на сертификат открытого ключа. Это вычисление группа может выполнить, обратившись к самой себе в качестве клиента слепой мультиподписи.

Цифровая подпись, согласно ISO/IEC 14888-3 : 2006, Amendment 1, вычисляется следующим образом.

Генерирование общесистемных параметров:

p — простое число, E — группа точек эллиптической кривой над полем $GF(p)$, $\#E$ — количество точек на E, q — простой делитель $\#E$, G — точка эллиптической кривой порядка q, выбранная хэш-функция (не обязательно соответствующая российскому стандарту ГОСТ Р 34.11 — 95).

Генерирование секретного и открытого ключей.

Секретным ключом является случайно сгенерированное число X, $0 < X < q$. Соответствующим открытым ключом является точка $Y = [X]G$.

Процесс формирования подписи.

Подписывающий выбирает случайное K, $0 < K < q$ и вычисляет $\Pi = [K]G$.

Далее вычисляется число $R = FE2I(\Pi_x) \bmod q$, где Π_x — x-координата точки Π ($FE2I$ — преобразование элемента поля в целое число).

Вычисляется $H(T)$ и хэш-код преобразуют в целое число H. Подписью является пара чисел (R, S), где S вычисляется по формуле $S = (RX + KH) \pmod q$.

Процесс проверки подписи.

Вычисляют $\overline{\Pi} = [-H^{-1}R \bmod q]Y + [H^{-1}S \bmod q]G$, $\bar{R} = FE2I(\overline{\Pi}_x)$. Подпись верна, если $\bar{R} = R$.

Протокол создания слепой цифровой мультиподписи на основе ISO/IEC 14 888–3 : 2006, Amendment 1.

Все члены группы используют общую эллиптическую кривую над полем $GF(p)$ и одну и ту же функцию $H(\cdot)$. Каждый член группы генерирует личный ключ X_i, $0 < X_i < q$ и вычисляет соответствующий ему открытый ключ $Y_i = [X_i]G$. Координатор группы вычисляет общий открытый ключ $Y = \sum\limits_{i=1}^{L} Y_i$.

По сигналу координатора группы каждый член группы вычисляет свой разовый открытый ключ $\tilde{\Pi}_i = [\tilde{K}_i]G$, где $0 < \tilde{K}_i < q$ является индивидуальным разовым секретным параметром. Координатор собирает все $\tilde{\Pi}_i$ и вычисляет общий разовый открытый ключ $\tilde{\Pi} = \sum\limits_{i=1}^{L} \tilde{\Pi}_i$ и передает его клиенту вычисления слепой мультиподписи.

Клиент выбирает случайные маскирующие параметры $\alpha, \beta \in Z_q$ и вычисляет $\Pi = [\alpha]\tilde{\Pi} + [\beta]G$. Далее вычисляет $\tilde{R}$ и R, полученные в результате преобразования элементов основного поля $\tilde{\Pi}_x$ и Π_x в целые числа по модулю q. Затем вычисляет $\tilde{H} = \alpha H \tilde{R} R^{-1} \pmod q$, где $H = H(T)$ — значение хэш-функции, примененной к сообщению T. Это число клиент передает координатору группы.

Координатор передает числа $\tilde{H}$ и $\tilde{R}$ всем членам группы. Каждый член группы вычисляет свою частичную замаскированную цифровую подпись $(\tilde{R}, \tilde{S}_i)$, где $\tilde{S}_i = (\tilde{K}_i \tilde{H} + \tilde{R} X_i) \pmod q$. Эти данные все члены группы передают координатору группы.

Координатор проверяет правильность каждой частичной цифровой подписи. Для этого он вычисляет

$$\overline{\Pi}_i = [-\widetilde{H}^{-1}\widetilde{R} \bmod q]Y_i + [\widetilde{H}^{-1}\widetilde{S}_i \bmod q]G,$$

$\bar{R}_i$ — число, полученное в результате преобразования $(\bar{\Pi}_i)_x$ в целое число по модулю q. Если $\bar{R}_i = \tilde{R}_i$ ($\tilde{R}_i$ — результат преобразования x-координаты точки $\tilde{\Pi}_i$ в целое число), то подпись верна. Это следует из того, что $\bar{\Pi}_i$ равняется $[\tilde{K}_i]G = \tilde{\Pi}_i$.

Если все частичные цифровые подписи верны, то координатор вычисляет вторую замаскированную составляющую цифровой подписи $\tilde{S} = \sum\limits_{i=1}^{L} \tilde{S}_i (\bmod n)$ и передает ее клиенту.

Клиент вычисляет $S = (\tilde{S}R\tilde{R}^{-1} + \beta H) \pmod q$. Конечной подписью является пара чисел (R, S).

Процесс проверки этой цифровой подписи состоит в следующем. Вычисляем $\bar{\Pi} = [-H^{-1}R \bmod q]Y + [H^{-1}S]G$. $\bar{\Pi}$ — результат преобразования $(\bar{\Pi})_x$ в целое число. Если $\bar{R} = R$, то подпись верна.

Действительно,

$$\begin{aligned}\overline{\Pi} &= [-H^{-1}R \bmod q]Y + [H^{-1}S \bmod q]G = \\ &= \sum_{i=1}^{L}[-H^{-1}RX_i]G + \sum_{i=1}^{L}[H^{-1}R\widetilde{R}^{-1}\widetilde{S}_i \bmod q]G + [\beta H^{-1}H]G = \\ &= \sum_{i=1}^{L}[-H^{-1}RX_i \bmod q]G + \sum_{i=1}^{L}[H^{-1}R\widetilde{R}^{-1}\widetilde{K}_i\widetilde{H}]G + \sum_{i=1}^{L}[H^{-1}RX_i \bmod q]G + [\beta]G = \\ &= [\alpha]\widetilde{\Pi} + [\beta]G = \Pi.\end{aligned}$$

Исследования А. И. Кочубинского и А. М. Фаля поддержаны Национальной академией наук Украины, грант НАН Украины — РФФИ за 2010 г. No 07-07-10, исследование Н. А. Молдовяна — Российским фондом фундаментальных исследований, грант No 10-07-90403-Укр_ а.

1. *Chaum D.* Blind signatures for untraceable payments // Advances in Cryptology. – CRYPTO'82. – P. 199–203.
2. *Itakura K., Nakamura K.* A public key cryptosystem suitable for digital multisignatures // NEC Research & Development. – 1983. – **71**. – P. 1–8.
3. *ДСТУ* 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння. – Увед. 28.12.2002. – 37 с.
4. *Коваленко И. Н., Кочубинский А. И.* Асимметричные криптографические алгоритмы // Кибернетика и систем. анализ. – 2003. – № 4. – С. 95–102.
5. *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". – P. 32.

Институт кибернетики им. В. М. Глушкова НАН Украины, Киев

Поступило в редакцию 18.08.2011

А. І. Кочубинський, Н. А. Молдовян, О. М. Фаль

Сліпі мультипідписи на основі стандартів ДСТУ 4145-2002 та ГОСТ Р 34.10-2001

Наведено алгоритми сліпих мультипідписів, що використовують звичайні цифрові підписи, які відповідають стандартам ДСТУ 4145-2002 та ГОСТ Р 34.10-2001. Ці алгоритми можна використовувати в системах електронного документообігу і, зокрема, в системах електронних платежів. Вони узгоджені з системами електронного цифрового підпису, запровадженими в Україні та Росії.

A. I. Kochubinsky, N. A. Moldovyan, A. M. Fal'

Blind multisignatures based on the standards DSTU 4145-2002 and GOST R 34.10-2001

Blind multisignature algorithms using ordinary digital signatures according to the standards DSTU 4145-2002 and GOST R 34.10-2001 are provided. These algorithms may be used in the systems of electronic document exchange and, in particular, in electronic payment systems. They are compliant with electronic digital signature systems implemented in Ukraine and Russia.