УДК 681.3

ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ СВЕРТКИ ИНДИВИДУАЛЬНЫХ ПАРАМЕТРОВ

М. Ю. Ананьев,
аспирант
Л. В. Гортинская,
научный сотрудник
Н. А. Молдовян,
доктор техн. наук, профессор
НФ ФГУП НИИ «Вектор» — специализированный центр программных систем «Спектр»

Предлагается новый протокол коллективной подписи, устраняющий недостаток ранее известных протоколов такого типа, заключающийся в участии в протоколе доверенной стороны, которой передаются личные секретные ключи пользователей, подписывающих электронный документ.

Введение

В основе процедур аутентификации электронной информации лежат алгоритмы электронной цифровой подписи (ЭЦП), при разработке которых обычно используются три вычислительно сложные задачи:

1) факторизация составных чисел вида $n = qr$, где q и r — два больших простых числа, удовлетворяющих специальным требованиям [1];

2) нахождение дискретного логарифма по простому модулю p [2];

3) нахождение дискретного логарифма на эллиптической кривой (ЭК) специального вида [3].

Предложенная недавно [4] в качестве нового криптографического примитива трудная вычислительная задача извлечения корней большой простой степени по большому простому модулю специального вида дала возможность построить алгоритмы ЭЦП, позволяющие осуществить свертку индивидуальных параметров, генерируемых при вычислении подписи, в некоторые коллективные значения, по которым формируется коллективная ЭЦП (КЭЦП) малого размера. В отличие от известных протоколов аналогичного типа [5, 6] протокол на основе свертки индивидуальных параметров устраняет необходимость передачи индивидуальных секретных ключей некоторой доверенной стороне, что делает его весьма перспективным для практического применения.

В настоящей работе рассматривается механизм формирования КЭЦП на основе процедур свертки индивидуальных параметров, показывается возможность его переноса на схемы ЭЦП, основанные на трудности дискретного логарифмирования, предлагаются протоколы КЭЦП, использующие алгоритмы генерации ЭЦП, специфицируемые ГОСТ Р 34.10–94 и ГОСТ Р 34.10–2001, и формально доказывается стойкость предложенных протоколов КЭЦП.

Коллективная подпись для двух пользователей

Рассмотрим схему КЭЦП, использующую трудность извлечения корней большой простой степени k по простому модулю вида $p = Nk^s + 1$, где N — четное число, $s \geq 2$ и k — простое число достаточно большого размера. Открытый ключ y вычисляется по формуле $y = x^k \bmod p$. Подписью является пара чисел S и R. Формирование подписи к сообщению M выполняется следующим образом.

1. Выбрать случайное значение $t < p - 1$ и вычислить $R = t^k \bmod p$.

2. Используя некоторую специфицированную хэш-функцию F_H, вычислить $H = F_H(M)$ и значение некоторой сжимающей функции $f(R, M)$, в качестве которой можно использовать $f(R, M) = RH \bmod \delta$, где δ — большое простое число, например δ, имеющее длину 160 бит.

3. Вычислить второй элемент ЭЦП: $S = x^{f(R,M)} \times t \bmod p$.

Соотношением проверки подписи является уравнение $S^k = y^{f(R,M)} R \bmod p$.

Реализация единой подписи, принадлежащей одновременно двум пользователям A и B, обладающим открытыми ключами $y_A = {x_A}^k \bmod p$ и $y_B = {x_B}^k \bmod p$ соответственно, выполняется следующим образом.

1. Пользователь A генерирует $R_A = r_A^k \bmod p$, где r_A — случайное число.

2. Пользователь B генерирует $R_B = r_B^k \bmod p$, где r_B — случайное число.

3. Вычисляют $R = R_A R_B \bmod p$.

4. A вычисляет $S_A = x_A^{f(R)} r_A^H \bmod p$.

5. B вычисляет $S_B = x_B^{f(R)} r_B^H \bmod p$.

6. Вычисляют общую подпись (R, S):

$$S = S_A S_B \bmod p.$$

Проверка такой коллективной подписи осуществляется по уравнению $S^k = (y_A\, y_B)^{f(R)} R^H \bmod p$, в котором произведение $y_A\, y_B$ может быть заменено сверткой индивидуальных открытых ключей пользователей: $y_{AB} = y_A\, y_B \bmod p$. Из приведенной процедуры генерации КЭЦП, принадлежащей двум пользователям, вытекают следующие свойства подписи:

1) общая подпись имеет размер обычной подписи;

2) подписи (R_A, S_A) и (R_B, S_B) недействительны к H;

3) можно сформировать коллективную подпись для произвольного числа пользователей m ($m = 2, 3, 4...$).

Обобщенная схема формирования КЭЦП для m пользователей

При реализации протокола КЭЦП на основе свертки индивидуальных параметров, генерируемых подписывающими сторонами в процессе формирования подписи, обеспечиваются следующие важные для практики свойства.

• Целостность — из КЭЦП, принадлежащей заданному подмножеству пользователей, нельзя вычислить правильную подпись, соответствующую другому подмножеству пользователей.

• Независимость от пользователей — КЭЦП может сформировать любая группа пользователей, независимо от их числа и состава.

• Одновременность генерации КЭЦП — все значения, возникающие на промежуточных этапах процедуры генерации КЭЦП, не являются правильными подписями к каким-либо сообщениям, и из них не могут быть вычислены индивидуальные секретные ключи или значения.

• Возможность обнаружить нарушителя — умышленные или неумышленные отклонения от процедур, специфицируемых протоколом, обнаруживаются по проверочному уравнению, причем анализ индивидуальных параметров позволяет установить, кто из пользователей осуществил неправильные действия.

• Использование стандартной инфраструктуры открытых ключей — никакие дополнительные изменения в используемые на практике процедуры распределения открытых ключей не требуются.

В качестве базовой для протокола коллективной подписи была принята идея использования коллективного открытого ключа, являющегося функцией открытых ключей подписывающих. Коллективный открытый ключ некоторой произвольно задаваемой совокупности m пользователей, каждый из которых является владельцем соответствующего открытого ключа из множества Y_1, Y_2, ..., Y_m, представляет собой некоторое значение $Y = f(Y_1, Y_2, ..., Y_m)$. Общая схема формирования коллективной подписи представлена на рис. 1, а процедура проверки подлинности КЭЦП — на рис. 2.

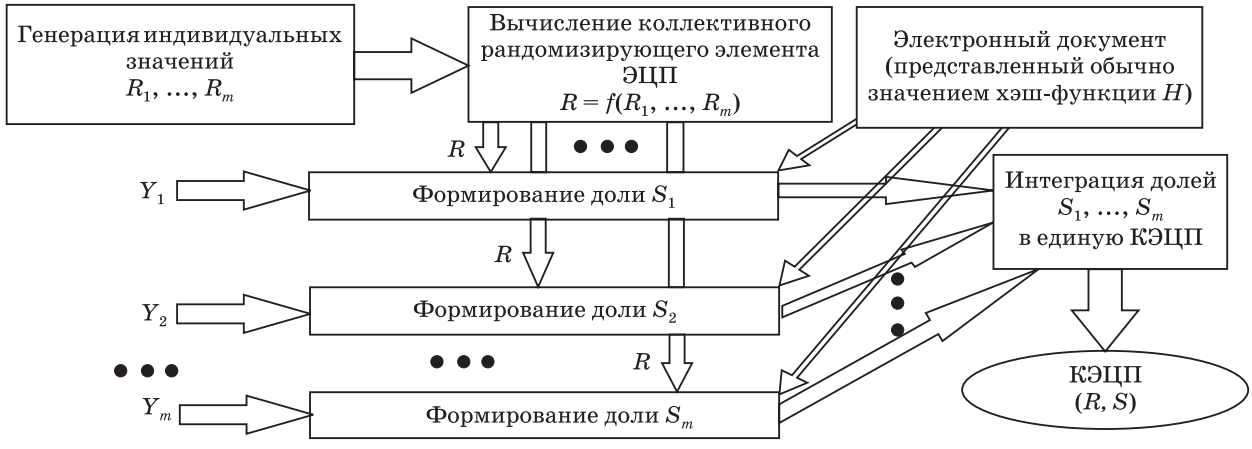
Представленная выше общая схема формирования КЭЦП была реализована в виде конкретных алгоритмов и протоколов, удовлетворяющих перечисленным требованиям. Использовались следующие трудные вычислительные задачи:

• извлечение корней большой простой степени по большому простому модулю;

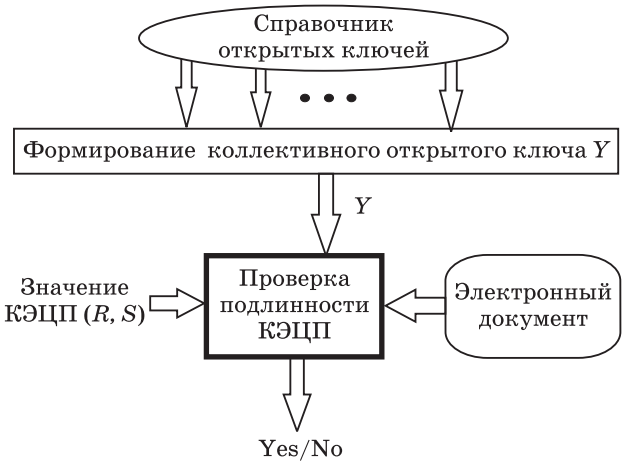
• дискретное логарифмирование в мультипликативной группе большого простого порядка;

• дискретное логарифмирование в группе точек эллиптической кривой специального вида.

Наибольший интерес представляют алгоритмы, основанные на последней задаче, поскольку в этом случае обеспечивается наибольшая производитель-



■ ***Рис. 1.*** *Общая схема формирования коллективной подписи*



■ ***Рис. 2.*** *Процедура проверки подлинности КЭЦП*

ность процедур генерации и проверки подписи. Достоинство предложенной идеологии КЭЦП состоит в использовании стандартной инфраструктуры открытых ключей и возможности реализации с применением процедур генерации и проверки, регламентируемых российскими стандартами ЭЦП.

Рассмотрим реализацию описанной идеологии построения протоколов КЭЦП на основе трудности задачи дискретного логарифмирования в конечной мультипликативной группе (на примере использования ЭЦП Шнорра и ГОСТ Р 34.10–94 в качестве базовой схемы) и трудности логарифмирования на ЭК (на примере использования ГОСТ Р 34.10–2001).

Реализация на основе алгоритма Шнорра

Как указано выше, схема Шнорра основывается на сложности задачи дискретного логарифмирования. Общими параметрами являются: p и q — большие простые числа такие, что q делит $p-1$; α — число, относящееся к показателю q по модулю p, т. е. $\alpha^q \bmod p = 1$. Секретный ключ представляет собой случайно генерируемое число k, $1 < k < q$. Формирование открытого ключа осуществляется путем возведения числа α в степень k по модулю p: $y = \alpha^k \bmod p$.

Вычисление подписи к сообщению M включает следующие шаги.

1. Генерируется случайное число t, $1 < t < q$, играющее роль разового секретного ключа.

2. Вычисляется значение $R = \alpha^t \bmod p$.

3. К сообщению M присоединяется число R, и вычисляется хэш-функция H от значения $M\|R$: $E = F_H(M\|R)$. Значение E является первой частью подписи.

4. Вычисляется вторая часть подписи: $S = t + kE \bmod q$, где k — секретный ключ.

Процедура проверки подлинности ЭЦП.

1. Вычисляется значение R': $R' = \alpha^S y^{-E} \bmod p$.

2. К сообщению M присоединяется число R', и вычисляется хэш-функция H от значения $M\|R'$: $E' = F_H(M\|R')$.

3. Сравниваются значения E и E'. Если $E = E'$, то подпись признается верной.

Протокол коллективной подписи на основе схемы Шнорра реализуется следующим образом. Каждый i-й пользователь формирует открытый ключ вида $y_i = \alpha_i^k \bmod p$, k_i — личный (секретный) ключ, $i = 1, 2, \ldots, m$.

1. Каждый подписывающий генерирует разовый случайный секретный ключ — число t_i, затем вычисляет $R_i = \alpha_i^t \bmod p$ и предоставляет это значение для коллективного использования.

2. Вычисляется произведение

$$R = R_1 R_2 R_3 \ldots R_m \bmod p.$$

3. Вычисляется $E = F_H(M\|R)$.

4. Каждый i-й пользователь вычисляет свою долю второй части подписи: $S_i = t_i + k_i E \bmod q$.

Коллективной подписью является пара чисел (R, S), где S вычисляется по формуле

$$S = S_1 + S_2 + S_3 + \ldots + S_m \bmod q.$$

Проверка подписи осуществляется по алгоритму, описанному выше. Покажем корректность алгоритма:

$$R = y^{-E}\alpha^S \bmod p = y^{-E}\alpha^{\sum_{i=1}^{m} S_i} \bmod p =$$

$$= y^{-E}\alpha^{\sum_{i=1}^{m}(t_i + k_i E)} \bmod p =$$

$$= y^{-E}\alpha^{\sum_{i=1}^{m} t_i}\, \alpha^{E\sum_{i=1}^{m} k_i} \bmod p = y^{-E}\alpha^{\sum_{i=1}^{m} t_i}\, y^E \bmod p =$$

$$= \alpha^{\sum_{i=1}^{m} t_i} \bmod p = \prod_{i=1}^{m} R_i \bmod p.$$

Реализация на основе ГОСТ Р 34.10–94

Стандарт ЭЦП ГОСТ Р 34.10–94 регламентирует использование простого числа p такого, что $510 \le |p| \le 512$ бит либо $1022 \le |p| \le 1024$ бит, где $|p|$ — разрядность p в двоичном представлении, причем число $p-1$ содержит большой простой делитель $2^{255} \le q \le 2^{256}$ либо $2^{511} \le q \le 2^{512}$ соответственно. Специфицируемые алгоритмы генерации и проверки ЭЦП используют число $\alpha \ne 1$ такое, что $\alpha^q \bmod p = 1$. Вычисление ЭЦП осуществляется следующим образом.

1. Генерируется случайное число t, $1 < t < q$.

2. Вычисляется значение $R = (\alpha^t \bmod p) \bmod q$, являющееся первой частью подписи.

3. По ГОСТ Р 34.11–94 вычисляется хэш-функция H от подписываемого сообщения.

4. Вычисляется вторая часть подписи: $S = tH + kR \bmod q$.

Если $S = 0$, процедура генерации подписи повторяется.

Процедура проверки подлинности ЭЦП.

1. Проверяется выполнение условий $R < q$ и $S < q$. Если они не выполняются, то подпись недействительна.

2. Вычисляется значение

$$R' = (\alpha^{S/H} y^{-R/H} \bmod p) \bmod q.$$

3. Сравниваются значения R и R'. Если $R = R'$, то подпись признается действительной.

Рассмотрим реализацию КЭЦП на основе этого стандарта. Каждый i-й пользователь формирует открытый ключ вида $y_i = \alpha_i^k \bmod p$, где α — генератор подгруппы достаточно большого простого порядка q (т. е. $\alpha^q \bmod p = 1$). Коллективным открытым ключом является произведение

$$y = y_1 y_2 y_3 ... y_m \bmod p.$$

Коллективная подпись формируется следующим путем. Каждый подписывающий выбирает разовый случайный секретный ключ — число t_i, затем вычисляет $R_i = (\alpha_i^t \bmod p) \bmod q$ и предоставляет это значение для коллективного использования. Далее вычисляется произведение

$$R = R_1 R_2 R_3 ... R_m \bmod q.$$

Затем каждый пользователь по своему значению R_i и величине H вычисляет свою долю подписи $S_i = t_i H + k_i R \bmod q$.

Коллективной подписью является пара чисел (R, S), где S вычисляется по формуле

$$S = S_1 + S_2 + S_3 + ... + S_m \bmod q.$$

Проверка коллективной подписи осуществляется по проверочной формуле

$$R' = (\alpha^{S/H} y^{-R/H} \bmod p) \bmod q.$$

Если $R = R'$, то КЭЦП совокупности пользователей 1, 2, ..., m является подлинной, так как она могла быть сформирована только при участии каждого пользователя из этой группы, поскольку для ее формирования требуется использование секретного ключа каждого из них. Отметим, что аутентификация значений R_i осуществляется автоматически при проверке подлинности коллективной ЭЦП. Если нарушитель попытается подменить какое-либо из этих значений или заменить ранее использованными значениями, то факт вмешательства в протокол будет сразу же выявлен при проверке подлинности ЭЦП, т. е. будет получено $R' \neq R$. Легко видеть, что размер КЭЦП не зависит от m.

Покажем корректность предложенного алгоритма КЭЦП. Подставив подпись (R, S) в проверочное уравнение

$$R = (\alpha^{S/H} y^{-R/H} \bmod p) \bmod q,$$

где

$$S = \sum_{i=1}^{m} S_i \bmod q \quad \text{и} \quad R = \prod_{i=1}^{m} R_i \bmod q,$$

убеждаемся, что оно выполняется:

$$R = \left(\alpha^{\sum_{i=1}^{m} S_i / H} \left(\prod_{i=1}^{m} y_i \right)^{-R/H} \bmod p \right) \bmod q =$$

$$= \left(\prod_{i=1}^{m} \alpha^{S_i/H} \prod_{i=1}^{m} y_i^{-R/H} \bmod p \right) \bmod q =$$

$$= \left(\prod_{i=1}^{m} \left(\alpha^{S_i/H} \alpha^{-k_i R/H} \bmod p \right) \right) \bmod q =$$

$$= \left(\prod_{i=1}^{m} \left(\alpha^{(t_i H + k_i R)/H} \alpha^{-k_i R/H} \bmod p \right) \right) \bmod q =$$

$$= \left(\prod_{i=1}^{m} \alpha^{t_i} \bmod p \right) \bmod q =$$

$$= \left(\prod_{i=1}^{m} \left(\alpha^{t_i} \bmod p \right) \bmod q \right) \bmod q = \left(\prod_{i=1}^{m} R_i \right) \bmod q.$$

Реализация на основе ГОСТ Р 34.10–2001

Стандарт ЭЦП ГОСТ Р 34.10–2001 регламентирует использование простого числа p — модуля ЭК, которая задается в декартовой системе координат уравнением $y^2 = x^2 + ax + b \bmod p$ с коэффициентами a и b: $a, b \in GF_p$; простого числа q — порядка циклической подгруппы точек ЭК; точки G с координатами (x_G, y_G), такой, что $G \neq O$, $qG = O$. Секретным ключом является достаточно большое целое число k, а открытым ключом — точка $Q = kG$. Формирование подписи (R, S) осуществляется в соответствии со следующим алгоритмом.

1. Генерируется случайное целое число t, $0 < t < q$.

2. Вычисляется точка ЭК $C = tG$ и определяется значение $R = x_C \bmod q$, где x_C — координата точки C.

3. Вычисляется значение $S = (Rk + te) \bmod q$, где $e = H \bmod q$, H — значение хэш-функции от подписываемого сообщения.

Подписью является пара чисел R и S.

Проверка подписи заключается в вычислении координат точки ЭК:

$$C = ((Se^{-1}) \bmod q)G + ((q - R)e^{-1} \bmod q)Q, \quad (1)$$

определении значения $R' = x_C \bmod q$ и проверке выполнения равенства $R' = R$.

Протокол КЭЦП реализуется следующим образом. Каждый i-й пользователь формирует открытый ключ вида $Q_i = Gk_i$. Коллективным открытым ключом является сумма

$$Q = Q_1 + Q_2 + Q_3 + ... + Q_m.$$

Коллективная подпись формируется следующим путем. Каждый подписывающий выбирает разовый случайный секретный ключ — число t_i, затем вычисляет $C_i = t_i G$ и предоставляет это зна-

чение для коллективного использования. Далее вычисляется сумма всех точек C_i

$$C = C_1 + C_2 + C_3 + ... + C_m,$$

по которой вычисляется значение $R = x_C \bmod q$. После этого каждый i-й пользователь по своему секретному ключу, значению t_i и величине e вычисляет свою долю подписи $S_i = (Rk_i + t_i e) \bmod q$.

Коллективной подписью является пара чисел R и S, где S вычисляется по формуле

$$S = S_1 + S_2 + S_3 + ... + S_m \bmod q.$$

Проверка коллективной подписи осуществляется по проверочной формуле. Если

$$R' = x_{C'} \bmod q = R,$$

где точка C' вычисляется по проверочному соотношению (1), то КЭЦП совокупности пользователей 1, 2, ..., m является подлинной, так как она могла быть сформирована только при участии каждого пользователя из этой группы, поскольку для ее формирования требуется использование секретного ключа каждого из них.

Сведение стойкости протокола КЭЦП к стойкости базового алгоритма ЭЦП

При разработке криптографических протоколов важным вопросом является доказательство их стойкости. В предлагаемых протоколах КЭЦП это может быть сделано путем формального доказательства того факта, что если протокол КЭЦП не является стойким, то тогда может быть взломан базовый алгоритм ЭЦП. Из этого доказательства вытекает безопасность протокола при использовании стойкой базовой схемы ЭЦП. Если в протоколе использовать стойкие апробированные алгоритмы ЭЦП, например стандарты ЭЦП, то и сам протокол будет стойким.

Рассмотрим формальное доказательство стойкости протокола КЭЦП при использовании проверочного уравнение $R = (\alpha^{S/H}\alpha^{-R/H} \bmod p) \bmod q$, регламентируемого стандартом ЭЦП ГОСТ Р 34.10–94. При доказательстве следует рассмотреть две возможности: подделки КЭЦП и вычисления секретного ключа одного из пользователей, являющегося совладельцем коллективной подписи, объединенными усилиями остальных совладельцев КЭЦП. Рассмотрим первый вариант.

Очевидно, что для посторонних нарушителей, не являющихся абонентами рассматриваемой системы ЭЦП, подделка КЭЦП так же сложна, как и подделка индивидуальной подписи некоторого отдельного пользователя. Новые возможности возникают у пользователей, объединяющих свои усилия, чтобы сформировать КЭЦП, относящуюся к коллективу, в который кроме них входит еще один или несколько других пользователей, которые об этом не оповещаются (доказательство для обоих случаев аналогично). Пусть $m - 1$ пользователей хотят сформировать КЭЦП, проверяемую по коллективному открытому ключу $y = y' y_m \bmod p$,

где $y' = \prod_{i=1}^{m} y_i \bmod p$, т. е. $m - 1$ пользователей объединяют свои усилия, чтобы сформировать пару чисел (R, S) такую, что $R = (\alpha^{S/H}(y' y_m)^{-R/H} \bmod p) \bmod q$. Это означает, что они могут подделать подпись «под» открытый ключ $y^* = y' y_m \bmod p$, т. е. вычислить значения R и S, которые удовлетворяют уравнению $R = (\alpha^{S/H}(y^*)^{-R/H} \bmod p) \bmod q$. Из интуитивных соображений ясно, что последнее означает возможность подделать цифровую подпись в базовой схеме ЭЦП, поскольку открытый ключ y^* имеет случайное значение, так же как и открытый ключ, принадлежащий какому-то отдельному пользователю. Рассмотрим формальное доказательство этого факта. Используя предполагаемую возможность, коллективный нарушитель формирует КЭЦП (R^*, S^*), соответствующую коллективному открытому ключу $y = y' y'_m \bmod p$, где в качестве y'_m взято значение $y'_m = y_m / y' \bmod p$. Коллективная подпись удовлетворяет соотношению

$$R^* = (\alpha^{S^*/H} y^{-R^*/H} \bmod p) \bmod q =$$
$$= \left(\alpha^{S^*/H} (y' y'_m)^{-R^*/H} \bmod p\right) \bmod q \Rightarrow$$
$$\Rightarrow R^* = \left(\alpha^{S^*/H} y_m^{-R^*/H} \bmod p\right) \bmod q.$$

Последнее выражение показывает, что (R^*, S^*) является подлинной индивидуальной ЭЦП m-го пользователя. Таким образом, мы формально показали, как возможность подделать коллективную подпись может быть легко использована для подделки подписи в базовой схеме ЭЦП.

Рассмотрим атаку, осуществляемую объединенными усилиями подмножества совладельцев коллективной подписи и направленную на вычисление секретного ключа другого совладельца КЭЦП. Рассмотрим случай, связанный с наибольшими возможностями у атакующих. Покажем, что если $m - 1$ совладельцев КЭЦП могут вычислить секретный ключ m-го совладельца, против которого направлена атака, то тогда они могут вычислить секретный ключ по индивидуальной ЭЦП, сформированной по базовому алгоритму ЭЦП. Пусть (R^*, S^*) — это ЭЦП, сформированная m-м пользователем к документу, соответствующему хэш-функции H. Тогда выполняется

$$R^* = (\alpha^{S/H}(y_m)^{-R^*/H} \bmod p) \bmod q. \qquad (2)$$

Атакующие генерируют случайные значения t_i и вычисляют $R_i = (\alpha_i^t \bmod p) \bmod q$ для $i = 1, 2, ..., m - 1$. После этого они вычисляют параметры $R = \left(R^* \prod_{i=1}^{m-1} y_i \bmod p\right) \bmod q$ и S_i, удовлетворяющие уравнениям

$$R_i = \left(\alpha^{S_i/H} y_i^{-R/H} \bmod p\right) \bmod q, \qquad (3)$$

где $i = 1, 2, \ldots, m-1$. Вводя обозначение

$$y^* = y^{R^*/R} \bmod p, \qquad (4)$$

из (3) и (4) получаем

$$R = (\alpha^{S/H}(Y)^{-R/H} \bmod p) \bmod q,$$

где $S = \left(S^* + \sum_{i=1}^{m-1} S_i\right) \bmod q$ и $Y = \left(y^* \prod_{i=1}^{m-1} y_i\right) \bmod p$. Это означает, что атакующие получили правильное значение коллективной подписи (R, S), в которой участвуют они и еще один пользователь, обладающий открытым ключом $y^* = \alpha^{k^*} \bmod p$. Согласно допущению, из полученной коллективной подписи атакующие могут вычислить секретный ключ k^*. Из (4) легко получить

$$k = Rk^*/R^* \bmod q.$$

Таким образом, атакующие вычислили секретный ключ m-го пользователя по его индивидуальной ЭЦП, сформированной в рамках базового алгоритма ЭЦП. То есть было формально доказано, что если протокол КЭЦП допускает вычисление секретного ключа одного из пользователей, то по индивидуальной ЭЦП, сформированной по базовому алгоритму ЭЦП, также можно вычислить секретный ключ. Это означает, что предложенный протокол КЭЦП не снижает стойкости базового алгоритма ЭЦП. (С интуитивной точки зрения, доказанное утверждение изначально очевидно. Однако ценность данного доказательства состоит в том, что оно является формальным.)

Заключение

В данной работе показана возможность применения подхода к построению протокола КЭЦП на основе процедур свертки индивидуальных параметров отдельных пользователей в коллективные значения с использованием алгоритмов на основе сложности задачи дискретного логарифмирования в конечной мультипликативной группе и в группе точек ЭК, включая использование стандартов ЭЦП, действующих в России. Показана сводимость безопасности предложенных протоколов КЭЦП к безопасности алгоритмов ЭЦП, на основе которых строятся данные протоколы.

Работа выполнена при поддержке гранта РФФИ 08-07-00096-а.

Литература

1. **Молдовян Н. А.** Практикум по криптосистемам с открытым ключом. СПб.: БХВ-Петербург, 2007. 298 с.
2. **Pieprzyk J., Hardjono Th., Seberry J.** Fundamentals of Computer Security. Berlin: Springer-Verlag, 2003. 677 p.
3. **Венбо Мао.** Современная криптография. Теория и практика. М.; СПб.; Киев: Издательский дом «Вильямс», 2005. 763 с.
4. **Koblitz N.** A Course in Number Theory and Cryptography. Berlin: Heidelberg; N. Y.: Springer, 1994. 235 p.
5. **Молдовян Н. А., Молдовяну П. А.** Новые протоколы слепой подписи // Безопасность информационных технологий. 2007. № 3.
6. **Boldyreva A.** Efficient Threshold Signature, Multisignature and Blind Signature Shemes Based on the Gap-Diffi-Hellman-Group Signature Sheme // LNCS. 2003. Vol. 2139. P. 31–46.