# ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

УДК 681.3

М. Ю. Ананьев, Л. В. Гортинская, А. А. Костин, Н. А. Молдовян

## РЕАЛИЗАЦИЯ ПРОТОКОЛА КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ СТАНДАРТОВ ЭЦП

Рассматривается обобщенный протокол формирования коллективной электронной цифровой подписи, основанный на выполнении процедур „свертки“ индивидуальных параметров, вырабатываемых отдельными пользователями в зависимости от подписываемого документа и своих секретных ключей. Протокол обеспечивает одновременность формирования подписи и использует стандартную инфраструктуру открытых ключей. Сформулированы основные требования и рассмотрен вопрос создания протоколов коллективной электронной цифровой подписи на основе российских стандартов ЭЦП 1994 и 2001 гг.

***Ключевые слова:*** *цифровая подпись, коллективная подпись, криптографические протоколы.*

**Введение.** В технологиях электронного документооборота широко используются алгоритмы электронной цифровой подписи (ЭЦП), на основе которых в сочетании с нормативно-правовыми механизмами обеспечивается придание юридической силы электронной документации [1, 2]. При разработке разнообразных коллективных проектов важной проблемой является создание протоколов, обеспечивающих реализацию коллективной (или кратной) ЭЦП [3].

Изложенные в работе [3] подходы к решению этой задачи на основе генерации совокупности ЭЦП, принадлежащей отдельным пользователям, имеют следующие недостатки:

— необходимость использования дополнительных процедур проверки целостности коллективной ЭЦП (КЭЦП), которые позволяют проверить ее полноту, т.е. обнаружить попытки формирования КЭЦП, принадлежащей измененному числу пользователей;

— увеличение размера КЭЦП пропорционально числу подписавших документ участников (размер ЭЦП особенно важен при необходимости ее записи в виде штрих-кода на бумажных носителях).

Для устранения указанных недостатков был предложен [4] новый способ формирования и проверки подлинности КЭЦП, использующий понятие общего (коллективного) открытого ключа, формируемого на основе данных, имеющихся в стандартных справочниках открытых ключей.

В настоящей статье рассматриваются вопросы применения предложенной в работе [4] обобщенной схемы формирования КЭЦП с использованием коллективного открытого ключа и вопросы ее реализации на основе процедур генерации и проверки ЭЦП, регламентируемых стандартами ЭЦП — ГОСТ Р 34.10–94 и ГОСТ Р 34.10–2007 [5, 6].

**Концепция коллективной подписи.** Поставлена задача построить протокол формирования и проверки подписи следующим образом: ЭЦП обычного размера должна подтверждать то, что некоторый электронный документ подписан каждым пользователем из некото-

рого заданного множества пользователей. При этом приняты следующие дополнительные требования к разрабатываемому протоколу КЭЦП:

— целостность — из КЭЦП 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 должны быть правильными подписями к каким-либо сообщениям;

— неразрывность — по данной коллективной подписи вычислительно невозможно сформировать другую коллективную подпись

В качестве базовой идеи протокола коллективной подписи была принята концепция использования коллективного открытого ключа, являющегося функцией открытых ключей пользователей. Коллективный открытый ключ некоторой произвольно задаваемой совокупности $m$ пользователей, каждый из которых является владельцем соответствующего открытого ключа из множества $y_1, y_2, \ldots, y_m$, представляет собой некоторое значение $y = f(y_1, y_2, \ldots, y_m)$.

Общая схема формирования КЭЦП была реализована в виде удовлетворяющих перечисленным требованиям конкретных алгоритмов и протоколов с использованием следующих трудных вычислительных задач:

— 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.

Особый интерес представляют алгоритмы, основанные на последней из перечисленных трудных задач, поскольку в этом случае обеспечивается наибольшая производительность процедур генерации и проверки подписи. Достоинство предложенной концепции КЭЦП заключается в использовании стандартной инфраструктуры открытых ключей.

Обратимся, далее, к реализации протоколов КЭЦП, основанной на проверочных уравнениях, предлагаемых стандартами ЭЦП.

**Реализация протоколов на основе стандартов ЭЦП.**

*I. Стандарт ЭЦП — ГОСТ Р 34.10–94 [5]* — 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, при этом 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 $\alpha^q \bmod p = 1$, где $\alpha$ — генератор подгруппы достаточно большого простого порядка $q$. Вычисление ЭЦП осуществляется следующим образом.

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

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

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

4. Вычисляется вторая часть подписи: $S = kH + zR \bmod q$, где $z$ — секретный ключ. Если $S = 0$, процедура генерации подписи повторяется.

Процедура проверки подлинности ЭЦП содержит следующие шаги.

1. Поверяется выполнение условий $r < q$ и $s < q$, если они не выполняются, то подпись недействительна.

2. Вычисляется значение

$$R' = (\alpha^{S/H} y^{R/H} \bmod p) \bmod q, \qquad (1)$$

где $y$ — открытый ключ пользователя, сформировавшего проверяемую подпись.

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

Протокол КЭЦП реализуется следующим образом. Каждый $i$-й пользователь формирует открытый ключ вида $y_i = \alpha^{z_i} \bmod p$, где $z_i$ — личный (секретный) ключ, $i = 1, 2, \ldots, m$. Коллективным открытым ключом является произведение

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

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

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

Затем каждый пользователь по определенному им значению $R_i$ и величине $H$ вычисляет свою часть подписи

$$S_i = k_i H + z_i R \bmod q\ .$$

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 коллективной подписи осуществляется по формуле (1). Если $R = R'$, то КЭЦП совокупности $m$ пользователей 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 на ранее использованные значения, то факт вмешательства в протокол будет сразу же выявлен при проверке подлинности ЭЦП, т. е. будет получено $R' \neq R$. Очевидно, что размер КЭЦП не зависит от $m$.

Покажем корректность предложенного алгоритма КЭЦП. Подставив подпись ($R$, $S$), где $S = \sum_{i=1}^{m} S_i \bmod q$ и $R = \prod_{i=1}^{m} R_i \bmod q$, в проверочное уравнение $R = (\alpha^{S/H} y^{R/H} \bmod p) \bmod q$, убеждаемся, что оно выполняется:

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

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

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

*II. Стандарт ЭЦП — ГОСТ Р 34.10–2001 [6]* — регламентирует использование: простого числа $p$ — модуля эллиптической кривой (ЭК), которая задается в декартовой системе координат уравнением $y^2 = x^3 + ax + b \bmod p$ с коэффициентами $a$ и $b$: $a, b \in GF_p$ ($GF_p$ — поле Галуа порядка $p$); простого числа $q$ — порядка циклической подгруппы точек ЭК; точки $G$ с координатами $(x_G, y_G)$, такой что точка $G$ не совпадает с началом координат, а произведение $qG$ — совпадает. Секретным ключом является достаточно большое целое число $d$, а открытым ключом — точка $Q = dG$. Формирование подписи ($R$, $S$) осуществляется в соответствии со следующим алгоритмом.

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

2. Вычисляются координаты точки ЭК $C = kP$ и определяется значение $R = x_C \bmod q$, где $x_C$ — координата точки $C$.

3. Вычисляется значение $S = \left(Rd + ke\right) \bmod q$ , где $e = H \bmod q$.

Подписью является пара чисел ($R$, $S$).

Проверка подписи заключается в вычислении координат точки ЭК:

$$C = \left(\left(Se^{-1}\right) \bmod q\right) G + \left(\left(q - R\right) e^{-1} \bmod q\right) Q, \qquad (2)$$

а также в 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 $Q = d_i G$ , где $d_i$ — личный (секретный) ключ, $i = 1, 2, \ldots, m$. Коллективным открытым ключом является сумма

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

Коллективная подпись формируется следующим путем. Каждый пользователь выбирает разовый случайный секретный ключ — число $k_i$, затем вычисляет координаты точки $C_i = k_i G$ и предоставляет их для коллективного использования. Далее определяется сумма всех точек $C_i$:

$$C = C_1 + C_2 + C_3 + \ldots + C_m,$$

по которой вычисляется значение $R$. Затем каждый $i$-й пользователь по своему секретному ключу $d_i$, значению $k_i$ и величине $e$ вычисляет свою часть подписи

$$S_i = \left(Rd_i + k_i e\right) \bmod q .$$

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 коллективной подписи осуществляется по проверочной формуле. Если $R' = x_{C'} \bmod q = R$, где координаты точки $C'$ вычисляются по соотношению (2), то КЭЦП совокупности $m$ пользователей 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.

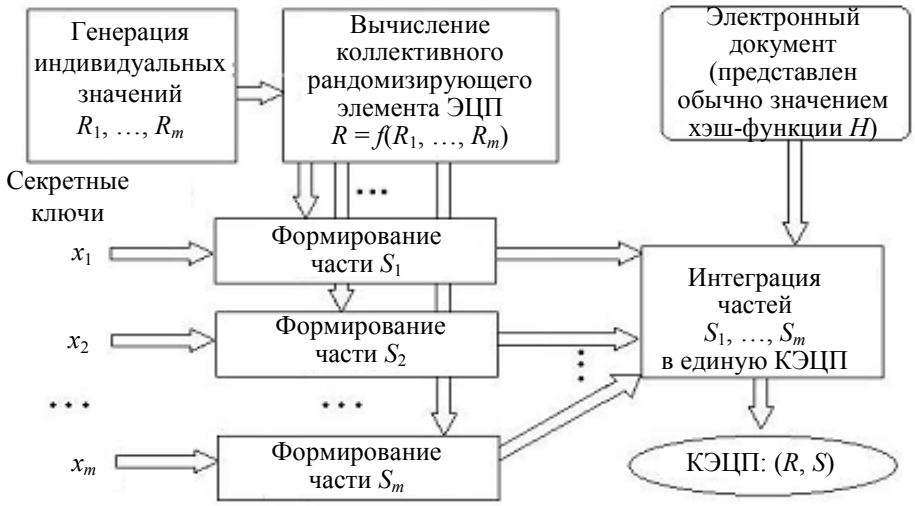


*Рис. 1*

Общая схема формирования коллективной подписи представлена на рис. 1, а процедура проверки подлинности КЭЦП — на рис. 2.

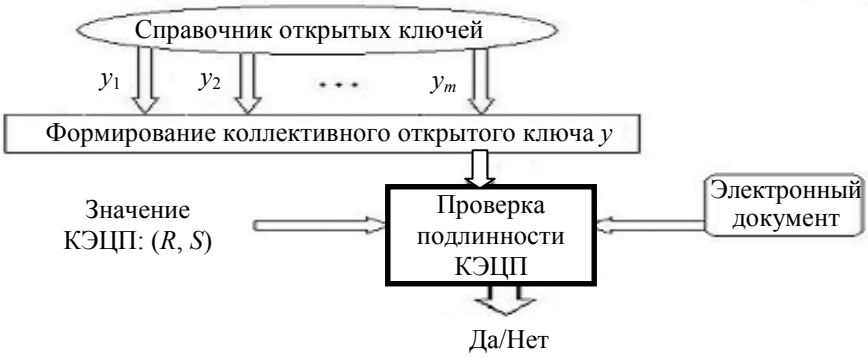


*Рис. 2*

**Заключение.** Применение понятия коллективного открытого ключа позволяет построить протоколы КЭЦП, перспективные для практического применения в технологиях электронного документооборота благодаря обеспечению одновременности формирования подписи и ее целостности. Достоинством таких протоколов является возможность их практической реализации на основе стандартной инфраструктуры открытых ключей и стандартов ЭЦП. Использование КЭЦП является удачным решением известной проблемы одновременного подписания контракта [7]. Представляет интерес использование КЭЦП для построения протоколов „множественной подписи“ [7], что составляет самостоятельную задачу дальнейшего развития протоколов на основе понятия коллективного открытого ключа.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант № 08-07-90100-Мол_а.

## СПИСОК ЛИТЕРАТУРЫ

1. *Венбо Мао.* Современная криптография. Теория и практика. М. — СПб. — Киев: Изд. дом „Вильямс“, 2005. 763 с.
2. *Молдовян Н. А.* Введение в криптосистемы с открытым ключом. СПб.: БХВ-Петербург, 2005. 286 с.
3. *Min-Shiang Hawng, Cheng-Chi Lee.* Research issues and challenges for multiple digital signature // Intern. J. of Network Security. 2005. Vol. 1, N 1. P. 1—7.
4. Способ генерации и проверки подлинности электронной цифровой подписи, заверяющей электронный документ / *А. А. Молдовян, Н. А. Молдовян.* Пат. заявка № 2007130982, РФ. Заявл. 13.08.2007.
5. ГОСТ Р 34.10–94. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Госстандарт Российской Федерации, 1994.
6. ГОСТ Р 34.10–2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Госстандарт России, 2001.
7. *Schneier B.* Applied Cryptography: Protocol, Algorithms, and Source Code. N. Y.: John Wiley & Sons, 1996. 758 p.

***Сведения об авторах***

***Михаил Юрьевич Ананьев*** — аспирант; Санкт-Петербургский государственный университет водных коммуникаций; E-mail: nmold@cobra.ru

***Лидия Вячеславовна Гортинская*** — канд. физ.-мат. наук; Научный филиал ФГУП НИИ „Вектор“ — Специализированный центр программных систем „Спектр“, Санкт-Петербург; E-mail: lydia@cobra.ru

***Андрей Алексеевич Костин*** — канд. техн. наук; Научный филиал ФГУП НИИ „Вектор“ — Специализированный центр программных систем „Спектр“, Санкт-Петербург; E-mail: anya@hotbox.ru

***Николай Андреевич Молдовян*** — д-р техн. наук; Научный филиал ФГУП НИИ „Вектор“ — Специализированный центр программных систем „Спектр“, Санкт-Петербург; E-mail: nmold@cobra.ru

Рекомендована
НИИ „Вектор“

Поступила в редакцию
04.10.07 г.