3. Положение о защите информации в информационных системах и ресурсах органов исполнительной власти города Москвы. Утверждено Мэром Москвы Ю. М. Лужковым 29 ноября 2006 года.
4. Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ от 31.07.2006, № 31 (Ч. 1). С. 34–48.
5. Информационная безопасность информационных систем и ресурсов органов исполнительной власти города Москвы. Классификатор конфиденциальной информации, содержащейся в информационных системах и ресурсах органов исполнительной власти города Москвы. Утвержден Мэром Москвы Ю. М. Лужковым 29 ноября 2006 года.
6. Положение о Реестре конфиденциальной информации, содержащейся в информационных системах и ресурсах органов исполнительной власти города Москвы. Утверждено Мэром Москвы Ю. М. Лужковым 29 ноября 2006 года.
7. Постановление Правительства Москвы от 07.12.2004 № 848-ПП «Об определении Уполномоченных удостоверяющих центров» // Вестник Мэра и Правительства Москвы. № 71. 22.12.2004;
8. Постановление Правительства Москвы от 26.07.2005 № 544-ПП «Об утверждении Положения о системе уполномоченных удостоверяющих центров органов исполнительной власти города Москвы» // Вестник Мэра и Правительства Москвы. № 46. 17.08.2005.
9. Постановление Правительства Москвы от 14.06.2005 № 439-ПП «О дальнейшем проведении работ по созданию Московского городского портала» // Вестник Мэра и Правительства Москвы. № 40. 18.07.2005.
10. Основные направления Политики информационной безопасности Правительства Москвы до 2010 года. Утверждены Мэром Москвы Ю. М. Лужковым 29 ноября 2006 года.
11. Единые требования к оформлению, структуре и содержательной части технических заданий. Утверждены Приказом Управления информатизации города Москвы от 16.03.2007 №64-06-13/07.

Е. С. Дернова, Н. А. Молдовян (д. т. н.)
ФГУП НИИ «Вектор» – СЦПС «Спектр», Санкт-Петербург

ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЦИФРОВОЙ ПОДПИСИ, ОСНОВАННЫЕ НА СЛОЖНОСТИ РЕШЕНИЯ ДВУХ ТРУДНЫХ ЗАДАЧ[1]

Рассматриваются новые криптографические протоколы коллективной электронной цифровой подписи (КЭЦП). С целью снижения вероятности компрометации подписи предлагаются реализации схем КЭЦП, взлом которых требует одновременного решения двух сложных задач – дискретного логарифмирования на эллиптической кривой и в конечной числовой группе большого порядка.

Введение

Одной из актуальных задач криптографии является разработка протоколов, обеспечивающих одновременное подписание документа или пакета документов (контрактов) несколькими лицами. Другая важная задача возникает при разработке коллективных проектов и юридически значимых электронных документов и сообщений, которые должны быть подписаны совокупностью субъектов. Она состоит в том, чтобы уменьшить объем дополнительной информации, необходимой для аутентификации электронных документов, т. е. требуется сформировать коллективную электронную цифровую подпись (КЭЦП) сравнительно малого размера, эквивалентную полной совокупности электронных цифровых подписей (ЭЦП), принадлежащих отдельным субъектам. Алгоритмы формирования компактной КЭЦП устраняют следующие недостатки. Не требуется выполнять многократные процедуры проверки подлинности коллективной ЭЦП и дополнительные процедуры, необходимые для проверки полноты и целостности КЭЦП, например, с целью обнаружения атак, связанных с формированием КЭЦП,

[1] Работа поддержана грантом РФФИ – 08-07-00096-а.

принадлежащей меньшему числу пользователей. Размер подписи не увеличивается пропорционально числу подписавших. Интересен недавно предложенный вариант построения КЭЦП [1], основанный на понятии коллективного (общего) открытого ключа, формируемого на основе данных, имеющихся в стандартных справочниках открытых ключей. Существуют реализации протокола КЭЦП на основе алгоритмов ЭЦП, безопасность которых основывается на сложности решения задачи дискретного логарифмирования [2], новой сложной задачи — извлечения корней большой простой степени по большому простому модулю специального вида, предложенной в работе [1]. Представляет интерес разработка схем КЭЦП, которые обладают повышенной стойкостью в смысле уменьшения вероятности их взлома при решении сложной задачи, положенной в их основу. В данной работе этот вопрос решается путем создания схем, в основе которых лежат две сложные задачи, причем взлом алгоритма КЭЦП требует одновременного решения этих задач, благодаря чему достигается отмеченная цель.

1. Описание протокола коллективной цифровой подписи

Протокол коллективной подписи изящно решает задачу одновременного дистанционного подписания электронного документа произвольным числом лиц, поскольку КЭЦП формируется одновременно всеми лицами, которые являются участниками единой процедуры генерации подписи. При этом КЭЦП имеет размер обычной индивидуальной подписи, который не зависит от количества участников протокола, подписывающих документ, и в протокол не вовлекается какая-либо доверенная сторона, которой подписывающие передают свои секретные ключи. Более того, протокол обеспечивает доказуемость того, что каждый пользователь подписал сообщение, и невозможность вычислить урезанную или расширенную КЭЦП [3]. В протоколе КЭЦП используется понятие *коллективного ключа* некоторой произвольно задаваемой совокупности m пользователей, который представляет собой функцию их открытых ключей $r_1, r_2,..., r_m : r = f(r_1, r_2,..., r_m)$. Общая схема формирования КЭЦП представлена на рис 1.

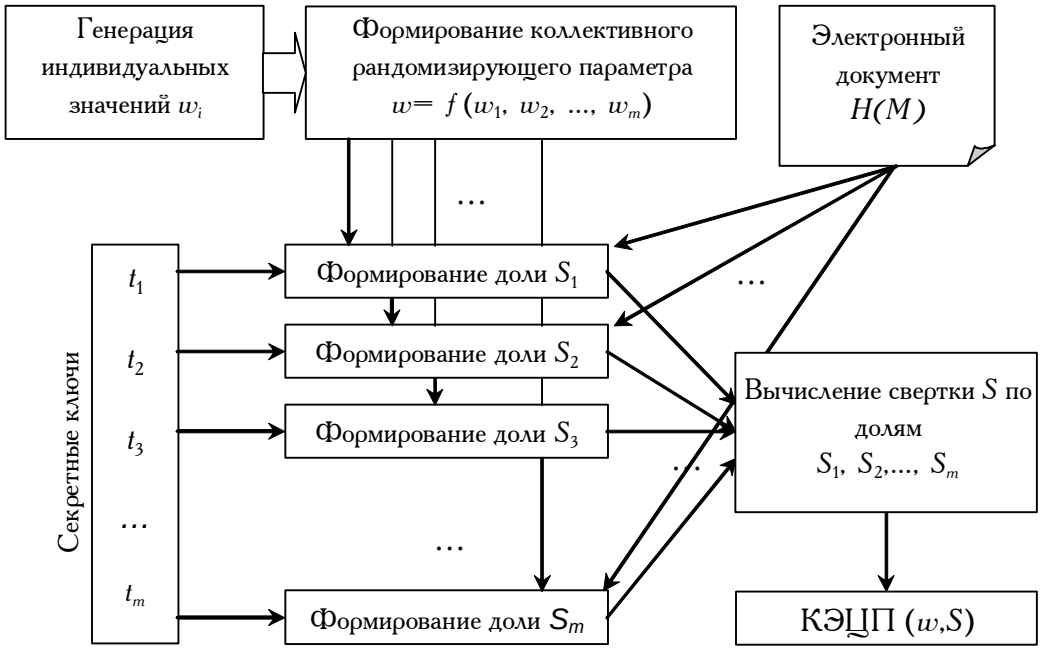

Рис. 1. Схема формирования коллективной подписи

В соответствии с протоколом КЭЦ каждый i-й пользователь генерирует разовый секретный ключ u_i, используя который он формирует открытый параметр рандомизизации w_i, играющий роль его разового индивидуального открытого ключа. Сформированные параметры объединяются в коллективный разовый открытый ключ w, являющийся общим параметром рандомизации (w — это свертка всех значений w_i, $i = 1, 2,..., m$) и используемый при формировании коллективной подписи к электронному

документу M, которому соответствует значение хэш-кода $H = F_H(M)$, где F_H — функция хэширования. Значение R является первым элементом коллективной подписи. Вторым элементом коллективной подписи является число S, представляющее собой свертку долей S_i, $i = 1, 2, \ldots, m$, генерируемых подписывающими в зависимости от предварительно вычисленного параметра w, секретного ключа x_i и значения H. Доли S_i являются общедоступными и любой из пользователей может вычислить свертку S. При этом в протоколе можно предусмотреть процедуры аутентификации индивидуальных значений w_i и S_i, однако этот момент не является критичным, поскольку любое нарушение протокола приведет к неправильному значению КЭЦП, которое не будет удовлетворять проверочному уравнению. При этом полученное значение КЭЦП не будет иметь никакой связи с каким-либо пользователем или группой пользователей как цифровая подпись, т. е. будет получено случайное «постороннее» значение. При этом компрометации секретных ключей не происходит, а пользователя, который осуществил неправильные действия, легко установить по его индивидуальным значениям w_i и S_i. Общая схема процедуры проверки КЭЦП представлена на рис. 2.

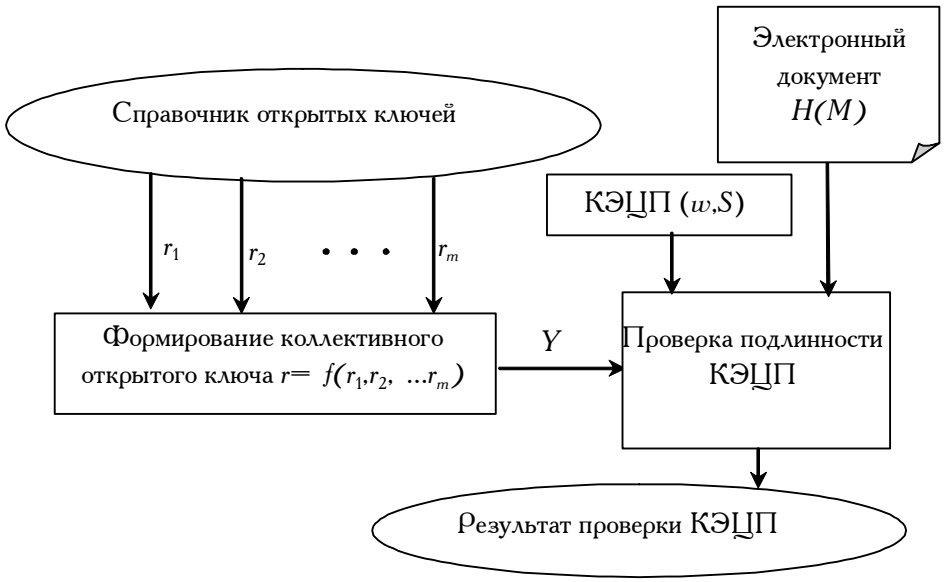

Рис. 2. Схема проверки подлинности коллективной подписи

В процедуре проверки используется стандартный справочник открытых ключей или совокупность стандартных сертификатов всех подписывающих, из которых извлекаются их индивидуальные открытые ключи. Коллективный открытый ключ вычисляется как свертка всех индивидуальных открытых ключей подписывающих, например, в некоторых алгоритмах КЭЦП свертка вычисляется как произведение индивидуальных открытых ключей по модулю большого простого числа, а в других алгоритмах — как сумма точек эллиптической кривой. Далее коллективный открытый ключ и КЭЦП подставляются в обычное уравнение проверки подписи, которое при $m = 1$ совпадает с уравнением проверки индивидуальной ЭЦП.

Наиболее разнообразные варианты построения схем КЭЦП, в безопасность которых вносят вклад две различные вычислительно сложные задачи, могут быть получены путем комбинирования двух схем ЭЦП с использованием общего параметра рандомизации. Данный способ построения алгоритмов ЭЦП на основе двух сложных задач хорошо апробирован для случая обычных индивидуальных ЭЦП [4]. Особенностью этого способа является то, что параметр рандомизации является одним элементом ЭЦП, который определяет два других элемента ЭЦП, вычисляемых в зависимости от него и от секретного ключа. При этом секретный ключ состоит из двух элементов, относящихся к разным сложным задачам. Такой механизм позволяет объединять сложные задачи, относящиеся к различным алгебраическим структурам, и формировать подпись сравнительно небольшого размера (400—480

бит). Детали построения таких алгоритмов ЭЦП достаточно подробно представлены в работе [4]. Применение подобного подхода к повышению безопасности к алгоритмам коллективной подписи до настоящей работы не рассматривался. Мы впервые показываем, что он может быть применен и при построении протоколов КЭЦП.

2. Схемы КЭЦП, взлом которых требует решения двух сложных задач одновременно

В качестве базовой схемы ЭЦП выберем схему, сложность которой основывается на одновременном решении задач дискретного логарифмирования в конечном поле и на эллиптических кривых. Выберем некоторый простой модуль n и параметр α — число, относящееся к показателю γ по модулю n. Первый элемент открытого ключа r зададим в соответствии с выражением $r = \alpha^t \bmod n$, где t — первый элемент секретного ключа, выбираемый случайным образом [5]. Пусть также задана некоторая криптографически стойкая эллиптическая кривая (ЭК) над полем с характеристикой ρ [6], на которой имеется подгруппа точек достаточно большого порядка q, а генератором этой подгруппы является точка G, принадлежащая ЭК. Тогда вторым элементом открытого ключа будет точка $R = s*G$, где s — это второй элемент секретного ключа, а «*» — это операция умножения точки G на число s. Обозначим, через $\Psi[R]$ функцию от точки $R(x_R, y_R)$, которая возвращает x_R — координату точки R. Тогда схема ЭЦП задается следующим уравнением проверки:

$$k = \{y^k \alpha^{gH} \bmod n + \Psi[kg * R + vgH * G]\} \bmod \delta, \quad (1)$$

где (k, g, v) — подпись к сообщению, хэш-функция от которого имеет значение H, (r, R) — открытый ключ, δ — сжимающий параметр, который в общем случае не связан со значениями n и ρ и обычно имеет длину 160 бит.

Алгоритм формирования цифровой подписи имеет следующий вид.

1. Вычисляется хэш-функция H от сообщения M: $H = F_H(M)$.

2. Генерируются случайные u' и u''.

3. Вычисляются значения k, g и v в следующем порядке:

3.1. $k=(\alpha^{u'} \bmod n + \Psi[u'' * G]) \bmod \delta$.

3.2. $g = \dfrac{u' - kt}{} \bmod \gamma$.

3.3. $v = \dfrac{u'' - Hkgs}{gH} \bmod q$.

4. Тройка чисел (k, g, v) является подписью к документу M.

На основе описанной выше схемы ЭЦП предлагается следующий протокол коллективной подписи, т. е. цифровой подписи, принадлежащей некоторой совокупности из m пользователей. Пусть некоторая система ЭЦП имеет своими абонентами z пользователей, которые являются владельцами открытых ключей (r_1, R_1), (r_2, r_2), …, (r_z, R_z), которым соответствуют секретные ключи (t_1, s_1), (t_2, s_2), …, (t_z, s_z). Предположим, что некоторые m пользователей желают подписать документ M, не раскрывая кому-либо своих личных секретных ключей. Все их подписи могут быть объединены в одну подпись, размер которой не зависит от числа подписывающих m и равен длине подписи одного пользователя. Это может быть осуществлено в соответствии со следующим протоколом.

1. Вычисляется хэш-функция H от сообщения M: $H = F_H(M)$.

2. Каждый i-й пользователь генерирует пару случайных чисел u_i' и u_i'', вычисляет значения числа $w_i = \alpha^{u_i'} \bmod n$ и точки ЭК $Z_i = u_i'' * G$ и рассылает их другим пользователям.

3. Получив все значения w_i и точки ЭК Z_i, $i = 1, 2, \ldots, m$, пользователи (все или некоторые из них) вычисляют:

3.1. $w = w_i = \prod_{i=1}^{i=m} \alpha^{u_i'} \bmod n$.

3.2. $Z = \sum_{i=1}^{m} Z_i = \sum_{i=1}^{m} (u_i'' * G)$.

3.3. $k=(w + \Psi[Z]) \bmod \delta$.

4. Каждый i-й пользователь вычисляет значение $g_i = \frac{u_i' - kt_i}{H} \bmod \gamma$, рассылает вычисленное значение g_i всем другим участникам протокола.

5. Получив все значения g_i, пользователи вычисляют второй элемент коллективной подписи: $g = \sum_{i=1}^{i=m} g_i \bmod \gamma$.

6. Каждый i-й пользователь вычисляет свою долю в третьем элементе коллективной подписи $v_i = \frac{u_i'' - kgs_i}{gH} \bmod q$, рассылает вычисленное значение υ_i.

7. Получив все значения υ_i, каждый пользователь (или некоторые из них) вычисляют третий элемент КЭЦП $v = \sum_{i=1}^{m} v_i \bmod q$.

Полученная тройка чисел (k, g, υ) является коллективной цифровой подписью к сообщению M, представленному хэш-кодом H.

Проверка КЭЦП выполняется по уравнению (1), а коллективный открытый ключ (y, R), используемый в этом соотношении, формируется следующим образом.

1. Вычисляется коллективное значение $r = \prod_{i=1}^{m} r_i \bmod n$, представляющее собой первый элемент коллективного открытого ключа.

2. Вычисляется общая точка на ЭК $R = \sum_{i=1}^{m} R_i$ (сумма открытых ключей подписывающих), представляющая собой второй элемент коллективного открытого ключа.

Подставляя значение коллективного открытого ключа и КЭЦП в правую часть проверочного уравнения, легко показать корректность рассматриваемого алгоритма. Действительно, мы имеем:

$$
\begin{aligned}
&\{r^k \alpha^{gH} \bmod n + \Psi[kg * R + vgH * G]\} \bmod \delta = \\
&= \left\{\left(\prod_{i=1}^{m} r_i\right)^k \alpha^{gH} \bmod n + \Psi\left[kg * \left(\sum_{i=1}^{m} R_i\right) + vgH * G\right]\right\} \bmod \delta = \\
&= \left\{\left(\prod_{i=1}^{m} r_i^k\right) \alpha^{\sum_{i=1}^{m} g_i H \bmod \gamma} \bmod n + \Psi\left[kg * \left(\sum_{i=1}^{m} R_i\right) + \left(gH \sum_{i=1}^{m} v_i\right) * G\right]\right\} \bmod \delta = \\
&= \left\{\left(\prod_{i=1}^{m} \alpha^{t_i k}\right)\left(\prod_{i=1}^{m} \alpha^{g_i H}\right) \bmod n + \Psi\left[\left(\sum_{i=1}^{m} kgs_i\right) * G + \left(\sum_{i=1}^{m} gHv_i\right) * G\right]\right\} \bmod \delta = \\
&= \left\{\prod_{i=1}^{m} \left(\alpha^{t_i k + g_i H}\right) \bmod n + \Psi\left[\left(\sum_{i=1}^{m} \left(kgs_i + gHv_i\right) \bmod q\right) * G\right]\right\} \bmod \delta = \\
&= \left\{\prod_{i=1}^{m} \alpha^{u_i'} \bmod n + \Psi\left[\left(\sum_{i=1}^{m} u_i'' \bmod q\right) * G\right]\right\} \bmod \delta = \left(w + \Psi[Z]\right) \bmod \delta = k.
\end{aligned}
$$

Таким образом, при использовании значения коллективного открытого ключа, соответствующего заданной совокупности пользователей, и подстановке значения подписи в правую часть проверочного уравнения (1) получаем значение, равное левой части (1), т. е. подлинная подпись удовлетворяет проверочному уравнению.

В качестве другого варианта реализации протокола коллективной подписи на двух сложных задачах рассмотрим вариант, стойкость которого основывается на решении дискретного логарифмирования на эллиптических кривых разного типа. Пусть заданы две эллиптические кривые ЭК1 и ЭК2, определенные над полями с характеристиками ρ' и ρ'', точка G' – генератор подгруппы точек порядка q' на эллиптической кривой ЭК1, точка G'' – генератор группы точек порядка q'' на ЭК2. Исходная схема ЭЦП задается следующим уравнением проверки:

$$k = \{\Psi[k * R' + gH * G'] + \Psi[kg * R'' + \upsilon gH * G'']\} \bmod \delta, \qquad (2)$$

где тройка чисел (k, g, υ) является подписью к сообщению H. Открытым ключом является пара точек (R', R''), которые вычисляется как $R' = s' * G'$ и $R'' = s'' * G''$, s_i', s_i'' — секретные ключи соответственно. Параметр δ – сжимающий параметр, который обычно имеет длину 160 бит.

Алгоритм формирование индивидуальной ЭЦП имеет следующий вид.

1.Вычисляется хэш-функция H от сообщения M: $H = F_H(M)$.

2. Пользователь генерирует пару случайных чисел u' и u'', вычисляет точки ЭК $W = u' * G'$ и $Z = u'' * G''$.

3. Пользователь выполняет последовательно следующие вычисления:

3.1. $k = (\Psi[W] + \Psi[Z]) \bmod \delta$.

3.2. $g = \dfrac{u' - ks'}{} \bmod q'$.

3.3. $v = \dfrac{u'' - Hkgs''}{gH} \bmod q''$.

Подписью к документу M является тройка чисел (k, g, υ). На основе этой схемы ЭЦП предлагается следующий протокол коллективной подписи. Пусть s пользователей являются владельцами открытых ключей (R'_1, R''_1), (R'_2, R''_2) … (R'_z, R''_z), которым соответствуют секретные ключи (s'_1, s''_1), (s'_2, s''_2) … (s'_z, s''_z), и m из них необходимо подписать документ M. Все их подписи могут быть объединены в одну подпись, размер которой не зависит от m и равен длине подписи одного пользователя. Это может быть осуществлено в соответствии со следующим протоколом.

1. Вычисляется хэш-функция H от сообщения M: $H = F_H(M)$.

2. Каждый i-й пользователь генерирует пару случайных чисел u_i' и u_i'', вычисляет точки ЭК $W_i = u_i' * G'$ и $Z_i = u'' * G''$, которые рассылает остальным участникам протокола.

3. Все участники протокола (или хотя бы один из них) вычисляют:

3.1 $W = \sum_{i=1}^{m} W_i = \sum_{i=1}^{m} (u_i' * G')$.

3.2 $Z = \sum_{i=1}^{m} Z_i = \sum_{i=1}^{m} (u_i'' * G'')$.

3.3 $k = (\Psi[W] + \Psi[Z]) \bmod \delta$.

4. Каждый i-й пользователь вычисляет значение $g_i = \dfrac{u_i' - ks_i'}{H} \bmod q'$ и рассылает вычисленное значение g_i другим участникам протокола.

5. Получив все значения g_i, участники протокола вычисляют величину $g = \sum_{i=1}^{m} g_i \bmod q'$ (это может сделать один из пользователей, а потом разослать остальным полученное значение g).

6. Каждый i-й пользователь вычисляет значение $v_i = \dfrac{u_i'' - kgs_i''}{gH} \bmod q''$ и рассылает вычисленное значение υ_i другим участникам протокола.

7. Получив все значения υ_i, участники протокола вычисляют величину $v = \sum_{i=1}^{m} v_i \bmod q''$ (это может сделать один из пользователей, а потом разослать остальным полученное значение υ).

Полученная тройка чисел (k, g, υ) является коллективной подписью к сообщению M, соответствующему значению хэш-кода H. Проверка КЭЦП выполняется по уравнению (2) при использовании открытого ключа (R', R''), элементы которого представляют собой точки ЭК, вычисляемые следующим образом.

1.Вычисляется общая точка на первой ЭК $R' = \sum_{i=1}^{m} R_i'$.

2. Вычисляется общая точка на второй ЭК $R'' = \sum_{i=1}^{m} R_i''$.

Покажем, что уравнение проверки действительно выполняется. Действительно, подставляя значение КЭЦП в правую часть проверочного уравнения, получаем:

$$\left\{\Psi\left[k*R'+gH*G'\right]+\Psi\left[kgR''+vgH*G''\right]\right\}\bmod\delta=$$

$$=\left\{\Psi\left[\left(k\sum_{i=1}^{m}s_i'\right)*G'+\left(H\sum_{i=1}^{m}g_i\right)*G'\right]+\Psi\left[\left(kg\sum_{i=1}^{m}s_i''\right)*G''+\left(gH\sum_{i=1}^{m}v_i\right)*G''\right]\right\}\bmod\delta=$$

$$=\left\{\Psi\left[\left(\sum_{i=1}^{m}\left(ks_i'+Hg_i\right)\right)*G'\right]+\Psi\left[\left(\sum_{i=1}^{m}\left(kgs_i''+gHv_i\right)\right)*G''\right]\right\}\bmod\delta=$$

$$=\left\{\Psi\left[\sum_{i=1}^{m}w_i*G'\right]+\Psi\left[\sum_{i=1}^{m}z_i*G''\right]\right\}\bmod\delta=\left\{\Psi\left[\sum_{i=1}^{m}W_i\right]+\Psi\left[\sum_{i=1}^{m}Z_i\right]\right\}\bmod\delta=$$

$$=\left\{\Psi\left[W\right]+\Psi\left[Z\right]\right\}\bmod\delta=k.$$

Заключение

В статье предложены две реализации протокола коллективной подписи, в основе которых лежат две сложные задачи, связанные с дискретным логарифмированием на эллиптических кривых и в конечном числовом поле. Отметим, что оба предложенных варианта протокола коллективной подписи обладают следующими свойствами:

· Длина коллективной подписи не зависит от числа лиц, которые подписали электронный документ.

· Из отдельных долей подписи вычислительно сложно сформировать подпись, соответствующую сокращенному коллективу подписавших. Это свойство является важным для обеспечения неотказуемости от коллективной подписи со стороны любого субъекта, участвовавшего в формировании коллективной подписи.

· Схемы обладают повышенной безопасностью, достигнутой благодаря комбинированию двух сложных задач.

· Идея использования общего значения рандомизации позволяет получить подпись небольшого размера (400—480 бит при обеспечении уровня безопасности, соответствующего 1024-битовому варианту алгоритма RSA).

Эти свойства, особенно резкое уменьшение вероятности взлома за счет прогресса в решении вычислительно сложных задач, делают предложенные схемы ЭЦП привлекательными для их практического применения.

Представляет интерес разработка алгоритмов КЭЦП, основанных на комбинировании задач дискретного логарифмирования для следующих случаев: 1) в конечном числовом поле и в конечной группе матриц, 2) в группе точек ЭК и в конечной группе матриц и 3) в конечных группах матриц различной размерности. Такие алгоритмы могут быть построены по аналогии со схемами КЭЦП, предложенными в данной статье, однако требуется выполнить предварительный этап исследований, включающий вопрос обоснования выбора и применения конечных групп матриц в качестве криптографического примитива.

СПИСОК ЛИТЕРАТУРЫ

1. *Молдовян А. А., Молдовян Н. А.* Коллективная ЭЦП — специальный криптографический протокол на основе новой трудной задачи // Вопросы защиты информации. 2008 (в печати).

2. *Молдовян А. А., Молдовян Н. А.* Новые алгоритмы и протоколы для аутентификации информации в АСУ // Автоматика и телемеханика. 2008 (в печати).

3. *Молдовян Н. А., Молдовян П. А.* Новые протоколы слепой подписи // Безопасность информационных технологий. 2007. № 3.

4. *Молдовян Д. Н., Молдовян Н. А.* Двухключевые криптосистемы с новым механизмом формирования цифровой подписи // Управление защитой информации. 2006. Т. 10. № 3. С. 307—312.

5. *Венбо Мао.* Современная криптография. Теория и практика. М.; СПб.; Киев: Издательский дом «Вильямс», 2005.

6. *Koblitz N.* A Course in Number Theory and Cryptography. Berlin, Heidelberg, New York: Springer, 1994.