УДК 681.3

МНОЖЕСТВЕННАЯ ПОДПИСЬ: НОВЫЕ РЕШЕНИЯ НА ОСНОВЕ ПОНЯТИЯ КОЛЛЕКТИВНОГО ОТКРЫТОГО КЛЮЧА

А. И. Галанов,
научный сотрудник
Н. А. Молдовян,
доктор техн. наук, профессор
ФГУП НИИ «Вектор» — специализированный центр программных систем «Спектр»
М. А. Еремеев,
доктор техн. наук, доцент
Военно-космическая академия им. А. Ф. Можайского

Предложены варианты схем построения протоколов множественной электронной цифровой подписи, основанные на понятиях коллективной электронной цифровой подписи и коллективного открытого ключа. Расширена задача построения протоколов множественной подписи на основе применения композиционного открытого ключа композиционной электронной цифровой подписи. В предлагаемых протоколах коллективной электронной цифровой подписи устраняется необходимость использования доверенного посредника.

Введение

В настоящее время наряду с задачами реализации стандартных систем электронной цифровой подписи (ЭЦП) практическую значимость имеют реализации коллективной и групповой подписей. Понятие коллективной подписи созвучно с широко известным понятием групповой подписи, однако по своей сути эти понятия различны и используются для построения криптографических протоколов, решающих различные задачи. В протоколе групповой подписи решается задача обеспечения возможности любому пользователю из некоторой группы сформировать подпись от имени всей группы, в которой есть субъекты, наделенные полномочиями выявления конкретных лиц, сформировавших подпись, тогда как другие субъекты не могут этого сделать.

Коллективная подпись предоставляет возможность достаточно простой реализации протоколов одновременного подписания контракта (электронного документа), поскольку она формируется в результате единого неделимого преобразования и не может быть расчленена на индивидуальные или другие урезанные коллективные подписи; кроме того, ее нельзя расширить, т. е. встроить в нее дополнительную подпись еще одного или нескольких пользователей.

В ряде работ предложены протоколы формирования и проверки коллективной электронной цифровой подписи [1–4]. Данные протоколы построены на основе комбинирования электронных подписей в едином уравнении проверки ЭЦП. В ряде из них не все пользователи вносят свой вклад в коллективную подпись в одинаковых условиях. Это вызывает ограничения, сужающие рамки практического применения.

В данной работе мы предлагаем несколько вариантов схем построения протоколов множественной подписи. Предлагается простое решение, включающее формирование дополнительной интегральной подписи. Вводится понятие композиционного открытого ключа и расширяется задача, решаемая протоколами множественной подписи. Композиционный открытый ключ представляет собой частный вариант коллективного открытого ключа, вычисляемого в зависимости от открытых ключей заданного подмножества пользователей.

Протоколы множественной подписи

Для получения множественной подписи z пользователей сети следует осуществить следующую последовательность действий.

1. Каждым пользователем формируются подписи (R_1, S_1), (R_2, S_2), ..., (R_z, S_z) к хэш-функциям документов $H_1, H_2, ..., H_z$ соответственно.

2. Вычисляются хэш-функции от всех документов $H_\Sigma = F_H(H_1 \| H_2 \| ... \| H_z)$.

3. Формируется подпись (R_Σ, S_Σ) к хэш-функции H_Σ.

Множественная подпись (R_1, S_1), (R_2, S_2), ..., (R_z, S_z), (R_Σ, S_Σ) устраняет недостатки предыдущих схем подписи.

Сформулируем расширенную задачу формирования и проверки множественной подписи. Расширение состоит в том, что в кортеж подписей входят ЭЦП, относящиеся к различным пользователям, т. е. проверяемый в едином уравнении кортеж подписей относится к некоторому множеству пользователей. Каждый пользователь подписывает свой документ. С использованием случайных рандомизирующих значений формируется композиционная подпись $(R_{\text{комп}}, S_{\text{комп}})$. Множественной подписью является кортеж (R_1, S_1), (R_2, S_2), ..., (R_z, S_z), $(R_{\text{комп}}, S_{\text{комп}})$.

Замечания:

а) избыточная подпись (R_Σ, S_Σ) или $(R_{\text{комп}}, S_{\text{комп}})$ незначительно увеличивает сложность процедур формирования и проверки множественной подписи;

б) решается расширенная задача;

в) устраняются проблемы в известных решениях по построению схем множественной подписи.

Алгоритм формирования композиционной подписи.

1. Каждый j-й пользователь генерирует случайное число t_j и вычисляет рандомизирующий элемент ЭЦП R_j: $R_j = \alpha^{t_j} \bmod p$, $j=1, 2, ..., z$.

2. Вычисляется $R_{\text{комп}} = \prod_{j=1}^{z} R_j \bmod p$.

3. Каждый j-й пользователь вычисляет свою долю S_j, вносимую во вторую часть композиционной подписи: $S_j = t_j - k_j R_{\text{комп}} \sum_{i=1}^{\mu_j} H_{ji}$, где $\mu_j \le z$, μ_j — количество документов, подписываемых j-м пользователем, а k_j — секретный ключ j-го пользователя.

4. Формируется композиционная подпись $S_{\text{комп}} = \sum_{j=1}^{m} S_j \bmod q$, где $q|(p-1)$.

Проверка композиционной подписи осуществляется с помощью решения следующего проверочного уравнения: $R_{\text{комп}} = Y_{\text{комп}}^{R_{\text{комп}}} \alpha^{S_{\text{комп}}} \bmod p$, где используется композиционный открытый ключ, определяемый формулой $Y_{\text{комп}} = \prod_{j=1}^{z} y_j^{\sum_{i=1}^{t_j} H_{ji}} \bmod p$.

Особенности введенного расширенного понятия множественной подписи:

• некоторые документы могут быть подписаны несколькими пользователями;

• в рамках композиционной подписи $(R_{\text{комп}}, S_{\text{комп}})$ каждый пользователь подписывает свой личный кортеж документов;

• возможна реализация в различных вариантах;

• в случае $z = 1$ мы имеем обычную множественную подпись, где вместо (R_Σ, S_Σ) в кортеж подписей вносится $(R_{\text{комп}}, S_{\text{комп}})$;

• композиционный открытый ключ $Y_{\text{комп}}$ может быть предварительно вычислен. Именно то, как вычисляется $Y_{\text{комп}}$, и определяет распределение документов H_1, H_2, ..., H_z по пользователям. Это, естественно, должно быть описано как спецификация кортежа, иначе неизвестно, что надо проверять;

• протокол, использующий параметр $H_\Sigma = F_H(H_1 \| H_2 \| ... \| H_z)$, можно построить таким образом, чтобы документы, стоящие на пересечении i-го пользователя и j-го документа (рисунок), подписывались с помощью коллективной ЭЦП.

По аналогии предлагаемым протоколом можно достаточно просто реализовать множественную подпись с использованием математического аппарата эллиптических кривых. В этом случае $R_{\text{комп}}$ является точкой эллиптической кривой, вычисляемой по формуле $R_{\text{комп}} = R_1 + R_2 + ... + R_z$, где $R_j = t_j G$, G — точка эллиптической кривой, значение порядка которой равно достаточно большому числу q. Элемент подписи $e_{\text{комп}}$ вычисляется по формуле $e_{\text{комп}} = x_{R_{\text{комп}}} \bmod q$, где $x_{R_{\text{комп}}}$ — одна из координат точки $R_{\text{комп}}$. Композиционный открытый ключ формируется по формуле $P_{\text{комп}} = h_1 P_1 + h_2 P_2 + ... + h_z P_z$, где P_i — точка эллиптической кривой, являющаяся открытым ключом i-го субъекта, $P_j = k_j G$. Вторая часть подписи S_i определяется по формуле $S_i = t_i - e_{\text{комп}} h_i k_i \bmod q$. При проверке подписи $(e_{\text{комп}}, S_{\text{комп}})$ вычисляется точка эллиптической кривой $R' = e_{\text{комп}} P + S_{\text{комп}} G$, затем значение $e' = x_{R'} \bmod q$, которое сравнивается с $e_{\text{комп}}$.

Рассмотренные выше схемы композиционной подписи представляют интерес также и для построения протоколов формирования и проверки цифровых сертификатов в информационно-вычислительных сетях с динамически изменяющейся конфигурацией, когда получение цифровых сертификатов новыми возникающими узлами сети связа-

i	j									
	1	2	3	4	5	6	7	8	9	10
1	■	■	■	■			■	■	■	
2		■	■			■	■		■	■
3			■	■	■	■	■	■		
4						■	■	■	■	■
Композиционная ЭЦП	1	1 2	1 2 3	1 3	3	2 3 4	1 2 3 4	1 3 4	1 2 4	2 4

■ *Формирование кортежа коллективных подписей: i — i-й пользователь; j — j-й документ; ■ — подписываемый документ*

но с трудностью доступа к центру сертификации. Другим интересным их применением является подписание передаваемых пакетов данных каждым узлом, через который проходит маршрут пакета, в целях обеспечения возможности контроля маршрута передачи данных.

Заключение

Коллективная и композиционная подписи имеют перспективы разнообразных применений в информационных системах. В частности, предложенные схемы коллективной ЭЦП позволяют реализовать известные протоколы множественной подписи, а схемы композиционной ЭЦП обеспечивают существенное расширение функциональности этих протоколов. Для обеспечения стойкости протоколов на основе этих видов подписей следует придерживаться правила разового использования рандомизирующих значений (t_j и R_j в случае алгоритмов на основе мультипликативных групп). Как и в случае обычной ЭЦП, значение t_j следует уничтожить сразу после вычисления рандомизирующего элемента ЭЦП R_j.

Обычную подпись в кортеже можно интерпретировать как частный случай коллективной ЭЦП. Уравнения проверки обычной и коллективной ЭЦП могут быть одинаковыми. Коллективная и композиционная подписи отличаются способом вычисления общего открытого ключа для заданного подмножества пользователей. В отличие от ряда известных схем, в предложенных нами схемах коллективной и композиционной ЭЦП устраняется необходимость использования доверенного посредника.

Литература

1. **Шнайер Б.** Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: ТРИУМФ, 2002. 816 с.
2. **Галанов А. Н., Гортинская Л. В., Гурьянов Д. Ю., Молдовян А. А.** Протокол коллективной электронной цифровой подписи на основе сложности извлечения корней по модулю // Инновационная деятельность в Вооруженных силах Российской Федерации: Тр. всеармейской науч.-практ. конф. / ВАС. СПб., 2007. С. 179–183.
3. **Молдовяну П. А., Молдовян Н. А., Доронин С. Е.** Схемы коллективной подписи на основе задач дискретного логарифмирования // Инновационная деятельность в Вооруженных силах Российской Федерации: Тр. всеармейской науч.-практ. конф. / ВАС. СПб., 2007. С. 243–246.
4. **Дернова Е. С., Еремеев М. А., Молдовяну П. А.** Протоколы композиционной подписи // Инновационная деятельность в Вооруженных силах Российской Федерации: Тр. всеармейской науч.-практ. конф. / ВАС. СПб., 2007. С. 224–229.