J, означающих наличие в схеме того или иного признака, для более точной классификации схем подписи по доверенности.

F-тип: по требованиям к числу раз возможного использования ключевой пары;

G-тип: по требованиям к обоснованию стойкости схемы;

H-тип: по требованиям к необходимости наличия исходного сообщения для проверки подписи;

I-тип: по требованиям к способу передачи прав подписания;

J-тип: по полноте перечня требований безопасности.

Схемы подписи по доверенности нашли многочисленные практические применения также при распределенных вычислениях, в системах электронной коммерции, в системах мобильной связи. Все вышесказанное делает изучение таких схем подписи исключительно актуальным и практически важным.

Термины из работ по схемам подписи по доверенности могли бы пополнить список терминов следующей редакции словаря криптографических терминов [3].

СПИСОК ЛИТЕРАТУРЫ:

1. *Mambo M., Usuda K., Okamoto E.* Proxy signatures: Delegation of the Power to Sign Messages // IEICE Trans. Fundamentals. Sep. 1996. Vol. E79-A. № 9. P. 1338–1353.
2. *Cao Zh.* Classification of Signature-only Signature Models. Department of Mathematics, Shanghai University. China, 2006.
3. Словарь криптографических терминов / Под ред. Б. А. Погорелова и В. Н. Сачкова. М.: МЦНМО, 2006. – 94 с.

А. А. Варфоломеев

РЕАЛИЗАЦИЯ ОДНОЙ СХЕМЫ ЦИФРОВОЙ ПОДПИСИ ПО ДОВЕРЕННОСТИ НА ОСНОВЕ РОССИЙСКИХ СТАНДАРТОВ

Рассматривается возможность применения российских стандартов цифровой подписи в схемах так называемой подписи по доверенности (proxy signature), которая имеет практические применения в системах электронного документооборота, при распределенных вычислениях, в системах электронной коммерции, в системах мобильной связи.

Схема прокси-подписи применяется, например, когда лицо, имеющее право подписи электронного документа, само не может поставить подпись и желает передать это право своему доверенному лицу. При этом позднее любой проверяющий подпись должен быть уверен, что доверенное лицо подписало документ с согласия доверителя.

В работе [1] была предложена первая реализация такой схемы подписи.

В качестве прототипа для использования стандартов ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001 [2] в протоколах с прокси-подписью выбрана схема из работы [3] на основе цифровой подписи Эль-Гамаля [4].

Далее для удобства сравнения рассматривается только ГОСТ Р 34.10-94. Это связано с небольшими различиями в стандартах ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001, основным

из которых является замена мультипликативной группы кольца вычетов целых чисел по модулю простого числа на группу точек эллиптической кривой, где задача дискретного логарифмирования решается сложнее, что позволяет получить более экономичную реализацию.

Для наглядности предлагаемые изменения в протоколе из работы [2] представлены в виде таблицы. В качестве функции хеширования H можно соответственно использовать отечественный стандарт ГОСТ Р 34.11.

№ соотношения в работе [2]	Исходные соотношения	Предлагаемые соотношения
Стадия создания псевдонима		
3	$s_1 = (k_\rho + x_{\rho GC} H(n_\rho, r_1)) \bmod q$	$s_1 = k_\rho H(n_\rho, r_1) + r_1 x_{\rho GC} \pmod q$
4	$r_1 y_2^{H(N\rho,R1)} = g^{S_1} \pmod \rho$	$r_1 = g^{S_1} H^{-1} y_2^{r_1 H^{-1}} \pmod \rho$
Стадия делегации		
5	$s_2 = (k_S + x_S H(t_S, m_w)) \bmod q$	$s_2 = K_S H(t_S, m_w) + t_S x_S \bmod q$
6	$t_S\, y_2^{H(ts,Mw)} = g^{S2} \pmod \rho$	$t_S = g^{S_2 H^{-1}} H^{-1} y_1^{t_s H^{-1}} \bmod \rho$
Проверка подписи		
D.(2)	$v_1 = y^{\,a} a^b \pmod \rho$	$v_1 = g^{bH^{-1}(m, M_w \| id_s \| n_\rho)} \bmod \rho$
D.(3)	$v_2 = g^{H(m, Mw \| IDs \| N\rho)} \bmod \rho$	$v_2 = v_1 y^{aH^{-1}(m, m_w \| id_s \| n_\rho)} \bmod \rho$
D.(4)	$v_1 = v_2$	$a = v_2$

Для полного соответствия стандарту ГОСТ Р 34.10-94 соотношения 4, 6, D.(2) и D.(3) из работы [2] нужно привести по модулю простого числа q.

Встраивание отечественных стандартов цифровой подписи ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001 в схемы подписи по доверенности, основанные на сложности решения задачи дискретного логарифмирования, дает возможность применения схем как в корпоративных системах [5], так и в информационных системах общего пользования.

Достоинствами предложенного протокола являются:

- более высокое быстродействие, связанное с двумя возведениями в степень (вместо трех),
- использование российского стандарта цифровой подписи с подтвержденными характеристиками стойкости против подделки.

СПИСОК ЛИТЕРАТУРЫ:

1. *Mambo M., Usuda K., Okamoto E.* Proxy Signatures: Delegation of the Power to Sign Messages // IEICE Trans. Fundamentals. Sep. 1996. Vol. E79-A. № 9. P. 1338–1353.
2. ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001. Государственный Стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Information technology. Cryptographic data security. Formation and verification processes of [electronic] digital signature.
3. *Han S., Chang E., Wang J., Wanquan L.* A New Proxy Signature Scheme as Secure as ElGamal Signature // Proceedings of World Academy of Science, Engineering and Technology. V. 6 June 2005. P. 5.
4. *Фомичев В. М.* Дискретная математика и криптология. М.: МИФИ, 2003.
5. Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».