СПИСОК ЛИТЕРАТУРЫ:

1. *Bernstein D., Birkner P., Joye M., Lange T., Peters C.* Twisted Edwards Curves // AFRICACRYPT 2008. Lecture Notes in Computer Science 5023. Springer-Verlag, New York, 2008. P. 389–405. URL: http://cr.yp.to/newelliptic/twisted-20080313.pdf.
2. *Bernstein D., Lange T.* Faster Addition and Doubling on Elliptic Curves // Advances in Cryptology – ASIACRYPT 2007. Lecture Notes in Computer Science 4833. Springer-Verlag, New York, 2007. P. 29–50.
3. *Imai H., Zheng Y.* Public Key Cryptography // Lecture Notes in Computer Science 1751. Melbourne, 2000. – 504 p.

А. А. Варфоломеев

О КЛАССИФИКАЦИИ СХЕМ ЦИФРОВОЙ ПОДПИСИ ПО ДОВЕРЕННОСТИ

В системах электронного документооборота широко используются различные схемы цифровых подписей, как классические, так и с дополнительными функциональными возможностями. К таким схемам относятся и схемы цифровой подписи по доверенности, для краткости — схемы прокси-подписи (proxy signature).

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. Например, руководитель организации во время своего отсутствия хочет, чтобы его секретарь (заместитель, технический специалист и т. п.) подписывал документы от его имени. При этом позднее любой проверяющий подпись должен быть уверен, что доверенное лицо подписало документ с согласия доверителя.

Для решения этой проблемы М. Мамбо, К. Усадо и Е. Окамото предложили в 1996 г. так называемую цифровую подпись по доверенности (proxy signature schemes) [1]. С момента предложения первой реализации схемы прокси-подписи появилось много публикаций по этой тематике, появились новые разновидности подписи, такие как подписи по доверенности на основе идентификаторов (identity based proxy signature), пороговые цифровые подписи по доверенности (threshold proxy signature), подписи с полностью делегированными правами (fully distributed proxy signature), подписи по доверенности вслепую (proxy blind signature) и др. Это делает необходимым сбор информации по всем таким схемам подписи, их упорядочивание и классификацию для практической реализации.

Как известно, классификация — это процесс группировки объектов исследования в соответствии с их общими признаками. Примером первой классификации является классификация по видам делегирования права подписи: полная делегация, частичная делегация и делегация по доверенности (ордеру) [2]. Предлагаемая в данной работе классификация основана на принципах классификации из работы Ж. Као, которая уточняется и дополняется в виде требований к функциональным возможностям схемы.

A-тип: по требованиям к подписывающей стороне;

B-тип: по требованиям к проверяющей подпись стороне;

C-тип: по требованиям к ясности содержания сообщения;

D-тип: по требованиям к методу производства открытого ключа;

E-тип: по требованиям к последовательности изменения секретного ключа.

На основе многочисленных проанализированных работ по схемам прокси-подписи в классификации Ж. Као предлагается расширение в виде дополнительных параметров F, G, H, I,

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