A. V. Beresneva, A. V. Epishkina

Review and Analysis of Cryptographic Schemes Implementing Threshold Signature

Key words: digital signature, threshold signature, elliptic curves

This work is devoted to the study of threshold signature schemes. The systematization of the threshold signature schemes was done, cryptographic constructions based on interpolation Lagrange polynomial, ellipt ic curves and bilinear pairings were investigated. Different methods of generation and verification of threshold signatures were explored, e.g. used in a mobile agents, Internet banking and e-currency. The significance of the work is determined by the reduction of the level of counterfeit electronic documents, signed by certain group of users.

А. В. Береснева, А. В. Епишкина

О СИСТЕМАТИЗАЦИИ КРИПТОГРАФИЧЕСКИХ СХЕМ,
РЕАЛИЗУЮЩИХ ПОРОГОВУЮ ПОДПИСЬ

Вопрос о применении электронной подписи является крайне актуальным. Растет число ситуаций, когда необходимо, чтобы сообщение было подписано группой пользователей и все они обладали равными правами по отношению к подписи. Кроме того, зачастую возникает задача распределения криптографических ключей между различными устройствами, принадлежащими одному пользователю. В таких случаях необходимо применять пороговое разделение секрета, а именно пороговую подпись.

Пороговая подпись — схема электронной подписи, в которой любые *t* или более участников группы, состоящей из *n* абонентов (t < n), могут формировать подпись от имени группы. Секретная информация распределена среди всех *n* пользователей. Любое подмножество из более чем *t* пользователей может восстановить секрет.

Схема пороговой подписи (t, n) состоит из трех протоколов:

- протокол генерации ключа;
- протокол генерации подписи, заключающийся в генерации частичных подписей, возможной проверке частичных подписей и их объединении;
- протокол проверки подписи.

Перечислим основные математические аппараты, применимые для формирования пороговой подписи:

- интерполяционный многочлен Лагранжа;
- эллиптические кривые;
- билинейные спаривания.

Протокол работы пороговой схемы может быть нарушен в следующих случаях:

- владелец одной из долей может помешать восстановлению общего секрета, отдав в нужный момент неверную (случайную) долю;

- злоумышленник, не имея доли, может присутствовать при восстановлении секрета.

Поскольку действующий российский стандарт на алгоритм электронной подписи ГОСт Р 34.10-2012 основан на алгоритме Эль Гамаля, приведем для него схему пороговой подписи [2, 3], состоящую из трех этапов: генерации ключей, генерации подписи и проверки подписи.

Схема генерации ключа. Сервер формирует и публикует системные параметры — открытый ключ, устойчивую к коллизиям хэш-функцию H, модуль *p,* эллиптическую кривую 8_p. (*t*, п)- пороговая функция *f(x)* имеет следующий вид: *f* (x) = $a_{t_1}\, x^{t-1}$ +... + a_1 x + a_0 (mod *n)*,

где *a.* — случайное число от 1 до *n* — 1, *i* = 0, 1,..., *t* — 1, f(0) = a_Q — групповой секретный ключ, *f*(x_i) — индивидуальный секретный ключ участника *U.*

Схема генерации подписи. Группа участников, которая должна подписать сообщение, состоит из участников $^{U}V\,^{U}2$ — клиента и сервера. Для генерации результирующей пороговой подписи сообщения *m* требуются формирование отдельных электронных подписей, проверка отдельных подписей и генерация (t, п)-пороговой подписи.

Шаг 1. Сервер посылает каждому участнику *U* секретный ключ *f*(x_i). Пользователь использует выбранную им точку на эллиптической кривой *R,,* случайное целое число k_t *,1* < k_t < *n* _ 1, вычисляет свою долю подписи *(r,* s_i) для сообщения *m* и высылает ее серверу.

Шаг 2. После получения долей электронной подписи всех участников группы *(r,* s_i) сервер проверяет достоверность всех частичных подписей.

Шаг 3. Сервер вычисляет и публикует групповую подпись (r, s) сообщения m.

Схема проверки подписи. Любой пользователь может проверить подлинность пороговой подписи (r, s) сообщения m. Для этого необходимо вычислить следующее значение:*t*

S = **^** $r_i s_i$ **(mod n)** и сравнить его со значением s, в случае выполнения равенства *S = S* подпись является подлинной, иначе подпись не верна.

Укажем особенности данной схемы:
- подпись не является анонимной, то есть активное подмножество участников схемы подписи должно быть известно проверяющему;
- частичные подписи могут быть проверены посредником, то есть данная схема позволяет обнаруживать и корректировать неисправные частичные подписи.

Следует отметить, что схемы пороговой подписи в настоящее время применяются в различных областях, таких как:
- электронные платежные системы;
- системы хранения данных;
- системы электронных денежных переводов.

таким образом, пороговые подписи являются развивающимся криптографическим примитивом, применимым во многих сферах деятельности человека. Однако все существующие схемы основаны на зарубежных алгоритмах электронной подписи, поэтому весьма актуальна разработка пороговой схемы подписи для алгоритма ГОСт Р 34.10-2012.

Основными результатами проделанной работы являются следующие:
- систематизированы различные способы формирования и проверки пороговой подписи;
- проанализированы различные виды электронной подписи, приведены иллюстрирующие примеры;
- исследован математический аппарат, положенный в основу различных типов пороговой подписи;
- приведены примеры практического применения схем пороговой подписи.

В рамках дальнейшего исследования по данной тематике предполагается создать схему пороговой подписи, основанную на российском стандарте гост Р 34.10-2012, и разработать программный комплекс, реализующий указанный алгоритм пороговой подписи.

СПИСОК ЛИТЕРАТУРЫ:

1. Desmedt Y., Frankel Y. Threshold cryptosystems // Advances in Cryptology — Crypto'89. 1989. P. 307—315.

2.Chen T. S. A specifiable verifier group-oriented threshold signature scheme based on the elliptic curve cryptosystem // Computer Standard & Interfaces. 2004. Vol. 27. № 1. P. 33—38.

3.Pederson T. P. Non-interactive and information-theoretic secure verifiable secret sharing // Advances in Cryptology. 1992. P. 129—140.

REFERENCES:

1.Desmedt Y., Frankel Y. Threshold cryptosystems // Advances in Cryptology — Crypto'89. 1989. P. 307—315.

2.Chen T. S. A specifiable verifier group-oriented threshold signature scheme based on the elliptic curve cryptosystem // Computer Standard & Interfaces. 2004. Vol. 27. № 1. P. 33—38.

3.Pederson T. P. Non-interactive and information-theoretic secure verifiable secret sharing // Advances in Cryptology. 1992. P. 129—140.