A. V. Epishkina, M. Y. Shimkiv

The Systematization of Blind Signature Schemes

Key words: digital signature, blind signature, elliptic curves

The paper presents the systematization of existing schemes of blind signatures. The analysis of different types of digital signatures and blind signatures was done, mathematical background of blind signature schemes was examined. The main result of the work was postulating security of elliptic curves schemes. Further investigation would concern an implementation of blind signatures to the algorithm GOST R 34.10-2012.

А. В. Епишкина, М. Я. Шимкив

О СИСТЕМАТИЗАЦИИ СХЕМ, РЕАЛИЗУЮЩИХ ЭЛЕКТРОННУЮ

ПОДПИСЬ «ВСЛЕПУЮ»

Электронный документооборот с каждым днем получает все большее применение в различных сферах деятельности человека. Почти ни один юридически значимый документ не может существовать без такого атрибута, как электронная подпись (ЭП), что является особенно важным в связи с принятием Федерального закона «об электронной подписи» [1], приравнивающего ЭП к собственноручной подписи.

Всесторонний анализ схем ЭП по различным критериям показал, что в настоящее время одним из развивающихся примитивов является подпись «вслепую» [2, 3], позволяющая подписывающей стороне достоверно не знать содержимое подписываемого документа. Основной областью применения подобных схем являются протоколы электронных платежей. Идея подписи «вслепую» может быть продемонстрирована на примере бумажного аналога — конверта, в который вложен копировальный лист. Когда на конверте ставится собственноручная подпись, она отпечатывается через копировальный лист на вложенном документе.

Электронные платежи основаны на так называемых электронных монетах (electronic coin) — информации, которая, в отличие от бумажных денег, не имеет физического воплощения. В рассматриваемых протоколах субъектом, осуществляющим подпись «вслепую», является банк, подписывающий монету с уникальным номером, известным только ее владельцу. Так как электронная монета является обыкновенными данными, не исключена возможность ее копирования клиентом или банком, следовательно, должен быть реализован контроль уникальности номеров монет при погашении, и банк кроме обычной пары криптографических ключей имеет также последовательность пар ключей, которым ставятся в соответствие номиналы монет. В таблице 1 приведена обобщенная схема подписи «вслепую».

Таблица 1. Обобщенная схема подписи «вслепую»

<table>
<tr><td>Клиент</td><td>Пересылаемые данные</td><td>Банк</td></tr>
<tr><td rowspan="3">Вырабатывает n случайных
номеров mi монеты m,
содержат ее денежный эквивалент, производит маскирование, накладывая на них некоторую маску ai, вычисляя функцию F(m, ai).</td><td>n, m_i, a_i, F(m, a_i)
1 S</td><td rowspan="3">случайным образом выбирает
n — 1 замаскированную монету и просит раскрыть их аргументы.</td></tr>
<tr><td>V
?(m, a.)?
< '</td></tr>
<tr><td></td></tr>
</table>

Открывает значения аргументов (m, a) для каждой из n — 1 выбранных монет.	(m, a) 1 [1] >	Убеждается, что все монеты имеют одинаковое денежное представление.
Проверяет, что замаскированная монета подписана банком верно.	s < 3	Генерирует подпись *S* для оставшейся нераскрытой монеты и отправляет ее клиенту.
Снимает с монеты маску, вычисляя функцию G(s, a.) так, что подпись остается верной и для открытого номера монеты.	Результат: электронная монета (m, s)	

Авторами проведена классификация схем, реализующих ЭП «вслепую» по используемому математическому аппарату, выделены криптографические примитивы, основанные на простых числах, билинейных спариваниях, группах кос и эллиптических кривых, обоснована безопасность рассматриваемых схем ЭП «вслепую», проведены сравнение и обоснование их использования в различных прикладных задачах.

Рассмотрим подробнее схему ЭП «вслепую» Эль Гамаля, основанную на аппарате эллиптических кривых (таблица 2), так как указанные примитивы положены в основу действующего российского алгоритма гост Р 34.10-2012 [4].

Таблица 2. Схема подписи «вслепую», основанная на протоколе Эль Гамаля

Клиент	*Пересылаемые данные*	*Банк*
Проверяет, что точка *R* лежит на эллиптической кривой, выбирает a, вычисляет *R* =aR , коэффициент P и маскированное сообщение *m* .	*R = kQ* < [1] *m* ' >	Выбирает показатель *k* ,0 < *k* < *p'* и вычисляет точку *R = kQ* .
Предъявляет a.	? показатель *a* ? < ' показатель a ' >	Просит клиента открыть содержание маскированного сообщения и удостоверяется, что оно отлично от нуля. Если условие выполнено, то банк вычисляет точку aR, коэффициент P и значение m. В противном случае клиент хочет раскрыть ключ подписи банка, то есть протокол нарушается.

Проверяет выполнение равенства *sQ = h(R)P + mR* , где *h* — используемая хэш-функция (в случае выполнения равенства подпись будет верна), и снимает маску.	s	Убеждается в том, что *m* Ф 0 , и подписывает сообщение. Если *m = 0* , то создание подписи приведет к компрометации ключа и нарушению протокола.
	< 1	

Предполагается продолжить работу по данной тематике в следующих направлениях:

- разработка модификации подписи «вслепую», основанной на алгоритме ГОСт Р 34.10-2012, аппарате эллиптических кривых и проблеме нахождения дискретного логарифма;
- обоснование стойкости предложенной схемы;
- выбор и обоснование средств разработки, необходимых для практической реализации предложенной схемы;
- разработка программного комплекса, реализующего схему ЭП «вслепую», основанную на алгоритме гост Р 34.10-2012.

СПИСОК ЛИТЕРАТУРЫ:

1.Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (редакция от 28.06.2014).

2.Chaum D. Blind signatures for untraceable payments // Advances in Cryptology: Proceedings of Crypto 82. 1983. P. 199—203.

3.Ростовцев А. Г. Подпись «вслепую» на эллиптической кривой для электронных денег // Проблемы информационной безопасности. Компьютерные системы. 2000. № 1. С. 1—8.

4.ГОСт Р 34.10—2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: ИПК «Стандартинформ», 2013.

REFERENCES:

1.Federal’nyj zakon Rossijskoj Federatsii ot 06.04.2011 № 63-FZ “Ob jelektronnoj podpisi” (redaktsia ot 28.06.2014).

2.Chaum D. Blind signatures for untraceable payments // Advances in Cryptology: Proceedings of Crypto 82. 1983. P. 199—203.

3.Rostovtsev A. G. Podpis’ “vslepuju” na jellipticheskoj krivoj dlja jelektronnyh deneg // Problemy informacionnoj bezopasnosti. Komp’juternye sistemy. 2000. № 1. P. 1—8.

4.GOST R 34.10—2012. Informatsionnaja tehnologija. Kriptograficheskaja zashchita informatsii. Processy formirovanija i proverki jelektronnoj tsifrovoj podpisi. M.: IPK “Standartinform”, 2013.