A.V. Epishkina, M.Y. Shimkiv

An Analysis of Blind Signature Schemes

Keywords: digital signature, blind signature, El Gamal scheme, homomorphism, elliptic curves.

The purpose of the article was to investigate blind signature schemes, to propose generalized scheme and to obtain its characteristics. The homomorphism of El Gamal scheme was evaluated. Some properties of partial blind signatures and blind signatures based on elliptic curves were estimated. The topic of further work was given.

А.В. Епишкина, М.Я. Шимкив

ОБЗОР И АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СХЕМ, РЕАЛИЗУЮЩИХ ЭЛЕКТРОННУЮ ПОДПИСЬ «ВСЛЕПУЮ»

Введение

Электронный документооборот с каждым днем получает все большее применение в различных сферах деятельности человека. Почти ни один юридически значимый электронный 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. Под ЭП понимается реквизит электронного документа, который был получен в результате криптографического преобразования информации с использованием секретного ключа подписи и позволяет установить отсутствие искажения информации в электронном документе с момента формирования подписи и проверить принадлежность подписи владельцу сертификата ключа подписи. С математической точки зрения ЭП является числом, зависящим от сообщения и от некоторого секретного, известного только подписывающему, ключа. Подпись обязательно должна быть легко проверяемой, а алгоритм проверки, в свою очередь, должен осуществляться без использования секретного ключа. Для реализации ЭП можно применять однонаправленные функции с секретом, т.е. такую функцию $f_t(x): D \to R$, которую легко вычислить для всех $x \in D$, но очень трудно вычислить в обратную сторону для почти всех значений из R.

Всесторонний анализ схем ЭП по различным критериям показал, что в настоящее время одним из развивающихся криптографических примитивов является подпись «вслепую» [2, 3], позволяющая подписывающей стороне достоверно не знать содержимое подписываемого документа. Систематизации указанных схем и посвящена настоящая работа.

Электронная подпись «вслепую» и ее применения

Понятие ЭП «вслепую» ввел Дэвид Чаум (David Chaum) [2]. Основной областью применения подписи «вслепую» являются протоколы электронных платежей, развивающиеся вследствие постоянной автоматизации процессов оплаты товаров и услуг. Инфраструктура электронных платежей может оказывать большое влияние на неприкосновенность личной жизни, а также на «природу» незаконных транзакций, что обуславливает необходимость их защиты. Электронные платежи основаны на так называемых электронных монетах (electroniccoin) – информации, которая в отличие от бумажных

денег, не имеет физического воплощения. В подобных системах субъектом, осуществляющим подпись вслепую, является банк, подписывающий монету с уникальным номером, известным только ее владельцу. Т.е. банк подписывает «сообщение», текст которого известен лишь его автору. Так как электронная монета является обычной информацией, не исключена возможность ее копирования клиентом или банком. Следовательно, необходимо исключить данную возможность, что может быть реализовано контролем уникальности номеров монет при их погашении. Банк кроме обычной пары ключей имеет также последовательность пар ключей, которым ставятся в соответствие номиналы монет.

Опишем процесс снятия клиентом наличности из банка (подпись банка сохраняется):

- клиент и банк выполняют протокол взаимной аутентификации;
- клиент вырабатывает последовательность и маскирует ее, умножая на случайный множитель;
- клиент зашифровывает результат открытым ключом банка и отправляет банку;
- банк расшифровывает результат с использованием своего закрытого ключа, подписывает его с помощью ЭП, соответствующей номиналу монеты;
- банк зашифровывает монету, используя открытый ключ клиента и возвращает ее обратно клиенту, списывая нужную сумму со счета;
- клиент получает монету, расшифровывает ее, используя собственный закрытый ключ, удаляет маскирующий множитель.

Опишем процесс внесения клиентом наличности на счет в банке:

- клиент отправляет банку полученную монету, зашифровав ее открытым ключом банка;
- банк удостоверяется, что полученная монета еще не была использована, заносит ее уникальный номер в список и зачисляет соответствующую сумму на счет клиента.

В табл. 1 приведена обобщенная схема подписи «вслепую».

Таблица 1. Обобщенная схема подписи «вслепую»

Клиент	**Пересылаемые данные**	**Банк**
Вырабатывает n случайных номеров m_i монеты m, которые содержат ее денежный эквивалент, производит маскирование, накладывая на них некоторую маску α_i, вычисляя функцию $F(m,\alpha_i)$.	$n, m_i, \alpha_i, F(m,\alpha_i)$ ⟹ ⟸ $?(m,\alpha_i)?$	Случайным образом выбирает $n-1$ замаскированную монету и просит раскрыть их аргументы.
Открывает значения аргументов (m,α_i) для каждой из $n-1$ выбранных монет.	(m,α_i) ⟹	Убеждается, что все монеты имеют одинаковое денежное представление.
Проверяет, что замаскированная монета подписана банком верно.	s ⟸	Генерирует подпись s для оставшейся нераскрытой монеты и отправляет ее клиенту.
Снимает с монеты маску, вычисляя функцию $G(s,\alpha_i)$ так, что подпись остается верной и для открытого номера монеты.	Результат: электронная монета (m,s)	

Использование подписи «вслепую» не позволяет банку накапливать сведения о клиентах, при этом он может следить за тем, чтобы каждая электронная монета была использована клиентом один раз, и идентифицировать получателя каждого платежа. Клиента нельзя идентифицировать даже в случае сговора продавца с банком, однако при необходимости клиент может идентифицировать себя, чтобы показать факт погашения монеты. Данный подход способен воспрепятствовать несанкционированному использованию электронных монет. Таким образом, подписи «вслепую» образуют новый фундаментальный криптографический примитив, который позволяет создавать автоматизированные платежные системы со следующими свойствами:

- невозможно определить третьим лицам получателя платежа, время и размер платежа, осуществленного пользователем;
- пользователь может предоставить доказательства платежа;
- может быть определена личность получателя платежа в исключительных обстоятельствах;
- платеж возможно остановить.

Математические основы обобщенной схемы подписи «вслепую»

Главным отличием подписи вслепую от обыкновенной ЭП является тот факт, что маска вычисляется и снимается без изменения самой подписи. Также важным условием является то, что маскирование и снятие маски должно выполняться без использования ключа подписи. Функция F должна быть такой, что по некоторому значению F_i очень трудно подобрать пару (m_i, α_i) и вычислить так называемую коллизию, т.е. найти такие пары (m_j, α_j) и (m_k, α_k), что $(F_j = F_k)$. Из вышеизложенных фактов вытекает следующее условие: необходима односторонняя вычислимость функций F и G, т.е. верна формула $G_i SF_i(m) = S(m)$. Данное свойство означает, что существует вычислимый гомоморфизм схемы подписи [4], который не требует знания ключа, иными словами, вычислимое отображение одной пары сообщение-подпись в другую. Подобные гомоморфизмы позволяют создать произвольное число формально правильных пар сообщение–подпись на основании одного подписанного сообщения за счет того, что уравнение (сравнение по модулю порядка группы) формирования подписи остается верным при умножении обеих его частей на некоторое число. Заметим, что выработанные пары не обязательно должны быть осмысленными.

Сообщения являются осмысленными, если лишены избыточности, т.е. нет превышения количества информации, используемой для передачи или хранения сообщения над его энтропией (согласно шенноновскому определению из теории информации). Под свойством вычислимости понимается наличие алгоритма, который за полиномиальное время может по подлинной паре сообщение-подпись (сформированной с использованием секретного ключа) сформировать другую пару сообщение-подпись (не зная секретного ключа), которая при подаче на вход процедуры проверки будет распознана как верная. Из известных протоколов подписи, не использующих хэш-функцию, протоколы Эль-Гамаля [5] и RSA [6] обладают гомоморфизмами. Подпись «вслепую» может использовать подобные гомоморфизмы в интересах обменивающихся информацией.

Для примера рассмотрим протокол Эль-Гамаля, пары сообщение-подпись в которой являются вычислимыми гомоморфизмами. Покажем, что вычислить данные гомоморфизмы довольно просто. Для начала приведем схему обычной ЭП Эль-Гамаля [4].

Пусть x – секретный ключ отправителя, характеристика поля p, образующая a подгруппы простого порядка q. Тогда, чтобы создать подпись для сообщения $m, 0 < m < q$, отправитель выполняет следующие действия:

- вырабатывает случайное $k, 0 < k < q$, причем k взаимно простое с q;
- вычисляет $r = a^k \pmod p$;
- находит s, решая сравнение $m \equiv xr + ks \pmod q$;
- получает подпись для $m : (r, s)$.

Пусть (m, r, s) – правильно подписанное сообщение. Чтобы создать формально правильное сообщение (m', r', s'), которое основано на умножении линейного сравнения создания подписи на некоторое число β. Положим $k' = \alpha k \pmod q$, $r' = a^{k'} \pmod p$. Пусть $r' = \beta r \pmod q$, тогда $m' = \beta m \pmod q$, $s' = \alpha^{-1} \beta s \pmod q$. Отсюда следует, что для создания вычислимого гомоморфизма $(m, r, s) \to (m', r', s')$ необходимо вычислить α, β. Приведем алгоритм вычисления гомоморфизма:

- выберем произвольное α, положим $r' = r^\alpha \pmod p$;
- вычислим $\beta = r' r^{-1} \pmod q$;
- положим $m' = \beta m \pmod q$, $s' = \alpha^{-1} \beta s \pmod q$;
- получим подписанное сообщение (m', r', s').

Для нахождения гомоморфизма было необходимо нарушить порядок вычислений в момент выработки подписи (сначала выбирается α, потом вычисляются β, m'). Безопасность протоколов подписи «вслепую» обеспечивается тем фактом, что в вырабатывании подписи участвуют обе стороны протокола. Причем ни одна из сторон не обязана доверять второй. Таким образом клиент банка может отсылать на подпись такие сообщения, которые позволяют несанкционированно получить ключ, например путем атаки на основе подобранных сообщений, а банк – раскрыть содержание зашифрованного сообщения клиента.

Классификация схем, реализующих подпись «вслепую»

Криптографические схемы, реализующие ЭП «вслепую», могут быть классифицированы по различными критериям, рассмотрим некоторые из них.

- По области применения:
  - а) электронные платежи;
  - б) банковские системы;
  - в) тайное голосование.
- По используемому математическому аппарату, рис. 1.

Заметим, что на билинейных спариваниях возможно реализовать не только ЭП «вслепую», но и частичную подпись «вслепую».

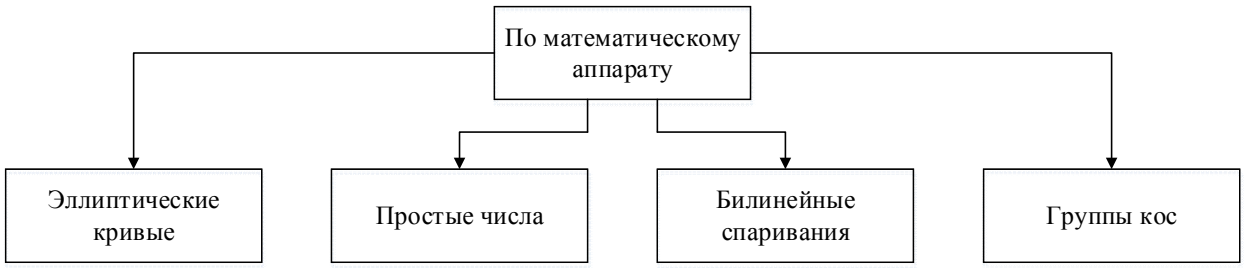

Рис. 1. Классификация схем, реализующих ЭП «вслепую», по используемому математическому аппарату

Частичная подпись «вслепую»

У обычных подписей «вслепую» присутствуют два основных недостатка:

- чтобы банк мог не допустить повторное погашение монет, ему необходимо вести учет каждой использованной монеты, т.е. иметь базу данных. При этом необходимо, чтобы база данных могла постоянно увеличиваться и обновляться, ведь количество погашенных монет стремится к бесконечности, следовательно объем базы данных также должен стремиться к бесконечности;

- банк не в состоянии определить, что клиент предоставляет для подписи, клиент может подменить номинал. Чтобы решить эту проблему, существует специальный метод. Банк использует разные открытые ключи для монет разного наминала, а клиент в свою очередь должен иметь у себя полный список этих ключей.

Впервые понятие частичной подписи «вслепую» ввели Абе (Abe) и Фуджисаки (Fujisaki) [7]. Основным отличием такой разновидности подписи от обычной подписи «вслепую» является то, что она позволяет включить некоторую дополнительную информацию в подпись «вслепую». Такой подход позволяет предотвратить увеличение базы данных потраченных монет банка путем включения в подпись информации о сроке действия монеты, т.е. все монеты с окончившимся сроком действия могут быть удалены из базы. Еще одним интересным способом встраивания дополнительной информации в подпись «вслепую» является встраивание номинала монеты. Во время генерации частичной подписи «вслепую» банк и клиент договариваются о некоторой информации, известной обеим сторонам. В одном случае содержание общей информации выбирает банк, соответственно в другом – клиент. Чтобы схема частичной подписи «вслепую» была безопасной, необходимо изолировать процесс согласования содержания общей информации из протокола подписи.

Подпись «вслепую» на основе алгоритма Эль-Гамаля

Рассмотрим подробнее схему ЭП «вслепую» Эль-Гамаля, основанную на аппарате эллиптических кривых (табл. 2), т.к. указанные примитивы положены в основу действующего российского алгоритма ГОСТ Р 34.10-2012 [8].

Проанализируем безопасность данного протокола. Существует несколько типов атак на протокол Эль-Гамаля:

- раскрытие ключа подписи;
- подделка подписи без компрометации ключа;
- раскрытие содержания сообщения банком.

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

Клиент	**Пересылаемые данные**	**Банк**
Проверяет, что точка $\bar{R}$ лежит на эллиптической кривой, выбирает α, вычисляет $R = \alpha\bar{R}$, коэффициент β и маскированное сообщение $\bar{m}$.	$\bar{R} = \bar{k}Q$ ⟸ $\bar{m}$ ⟹	Выбирает показатель $\bar{k}, 0 < \bar{k} < p'$ и вычисляет точку $\bar{R} = \bar{k}Q$.
Предъявляет α.	?показатель α ? ⟸ показатель α ⟹	Просит клиента открыть содержание маскированного сообщения и удостоверяется, что оно отлично от нуля. Если условие выполнено, то банк вычисляет точку $\alpha\bar{R}$, коэффициент β и значение m. В противном случае клиент хочет раскрыть ключ подписи банка, т.е. протокол нарушается.
Проверяет выполнение равенства $\bar{s}Q = h(\bar{R})P + \bar{m}\bar{R}$, где h – используемая хэш-функция (в случае выполнения равенства подпись будет верна) и снимает маску.	$\bar{s}$ ⟸	Убеждается в том $\bar{m} \neq 0$ и подписывает сообщение. Если $\bar{m} = 0$, то создание подписи приведет к компрометации ключа и к нарушению протокола.

Так как в основе протокола Эль-Гамаля лежит проблема логарифмирования в группе точек эллиптической кривой, то для компрометации ключа подписи банка достаточно вычислить логарифм l. Несмотря на это, существуют и другие атаки, такие как использование банком два раза показателя $\bar{k}$, использование предсказуемого показателя $\bar{k}$. Оба эти метода позволяют скомпрометировать ключ подписи банка путем решения линейных сравнений. Именно поэтому введение в состав k неповторяющегося номера, отвечающего за порядок, приводит к уменьшению числа подписей на одном ключе. Отсюда следуют жесткие требования к генератору случайного числа k, аналогичные требованиям к генератору ключей. Необходимо отдельно отметить тот факт, что если $h(\bar{R}) = 0$, то подпись не зависит от ключа l. В таком случае клиент может найти точку, которая даст значение хэш-функции, равное 0. Подделка подписи без знания ключа является не менее сложной задачей, чем логарифмирование в группе точек, если учесть верный выбор ключа. Если же ключ выбран неверно, то это будет легко выявлено с помощью тестов проверки на простоту. Существуют атаки, связанные с тем, что точка $\bar{R}$ не принадлежит эллиптической кривой, например, если точка не лежит в группе $<Q>$. Существует неустранимый недостаток подписи «вслепую» на основе протокола Эль-Гамаля, связанный с наличием гомоморфизма подписи. Заключается он в том, что пользователь может изменить подписанное замаскированное сообщение, воспользовавшись как раз гомоморфизмом подписи. Именно на этом и основана подпись «вслепую» – банк, в свою очередь, может быть уверен в честности пользователя лишь с некоторой долей вероятности. Единственным способом борьбы с данным недо-

статком является добавление избыточности в сообщение, т.е. чтобы электронная монета имела некоторый вид, и об этом виде было заведомо известно банку и клиенту. Допустим, что сложность подмены сообщения равна сложности компрометации ключа. В таком случае длина избыточного отрезка должна быть равна $\frac{\log_2 p'}{2}$. Чтобы обеспечить необходимую избыточность, можно заменить сообщение m на объединение строк $m \| g(m)$ с последующим сокращением длины m для некоторой хэш-функции g, стойкой к коллизиям. Можно использовать следующий способ: положить k битов каждой монеты нулями. С помощью избыточности может быть сужено множество двоичных строк, которые могли бы быть электронными монетами, что значительно усложняет процесс подделки для нарушителя.

Заключение

В процессе выполнения настоящей работы получены следующие основные результаты:

- проведен анализ и предложена классификация существующих разновидностей схем подписи «вслепую»;
- обозначены области применения подписи «вслепую» и приведены примеры;
- сформулированы вычислительные проблемы, лежащие в основе протоколов подписи «вслепую».

Дальнейшую работу по данной тематике предполагается проводить 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 Российской Федерации от 10.01.2002 № 1-ФЗ (ред. от 08.11.2007) «Об электронной цифровой подписи».
2. Chaum D. Blind signatures for untraceable payments // Advances in Cryptology: Proceedings of Crypto 82, 1983. Pp. 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. Ростовцев А.Г., Маховенко Е.Б. Введение в криптографию с открытым ключом. – СПб.: Мир и Семья, 2001.
5. Pointcheval D., Stern J. Security Arguments for Digital Signatures and Blind Signatures // Journal of Cryptology, No 13(3), 2000. P. 361-396.
6. Bellare M., Namprempre C., Pointcheval D., Semanko M. The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme // Journal of Cryptology, No 16(3), 2003. P. 185-215.
7. Abe M., Fujisaki E. How to date blind signatures // Advances in Cryptology – AisaCrypt' 96, Springer-Verlag, 1996, LNCS 1163. P. 244-251.
8. 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 Federacii ot 06 aprelia 2011 goda № 63-FZ «Ob jelektronnoj podpisi» (redakcia ot 28.06.2014).
2. Chaum D. Blind signatures for untraceable payments // Advances in Cryptology: Proceedings of Crypto 82, 1983. P. 199-203.
3. Rostovcev A.G. Podpis' «vslepuju» na jellipticheskoj krivoj dlja jelektronnyh deneg // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy, 2000. № 1. P. 1-8.
4. Rostovcev A.G., Mahovenko E.B. Vvedenie v kriptografiu s otkritim kluchom. – SPb.: Mir i sem'a, 2001.
5. Pointcheval D., Stern J. Security Arguments for Digital Signatures and Blind Signatures // Journal of Cryptology, No 13(3), 2000. P. 361-396.
6. Bellare M., Namprempre C., Pointcheval D., Semanko M. The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme // Journal of Cryptology, No 16(3), 2003. P. 185-215.
7. Abe M., Fujisaki E. How to date blind signatures // Advances in Cryptology – AisaCrypt' 96, Springer-Verlag, 1996, LNCS 1163. P. 244-251.
8. GOST R 34.10–2012. Informacionnaja tehnologija. Kriptograficheskaja zashhita informacii. Processy formirovanija i proverki jelektronnoj cifrovoj podpisi. M.: IPK «Standartinform», 2013.