УДК 621.391.7; 336.71 (075.8)

В.К. Задирака, А.С. Олексюк

Неотслеживаемые электронные платежные средства

На основе использования «слепой» электронной подписи предложены криптографические протоколы неотслеживаемости электронных денег и платежей.

The cryptographic protocols of untraceability of electronic money and payments based on the use of a «blind» *e*-signature are suggested.

На основі використання «сліпого» електронного підпису запропоновано криптографічні протоколи невідслідковуваності електронних грошей і платежів.

Введение. Сегодняшнее общество вполне обоснованно называют информационным. По характеру организационной структуры – сетевое, что дает основание назвать формацию информационно-сетевым обществом. Развитие информационно-коммуникационных технологий тесно связано с таким феноменом, как деньги, электронные деньги (нано-деньги). В слове «нано-деньги» приставка нано- обозначает одну миллиардную (10^{-9}) долю единицы измерения. Важный вопрос – решение проблемы безопасности функционирования электронных денег (ЭД).

Сегодня выделяют два основных вида электронных денег: на основе карточек (*card-based e-money*) и электронные деньги серверных схем (*server-based e-money*). Карточка полностью идентифицирует своего владельца, что дает возможность собирать информацию о том, какие товары и где он покупает, какими услугами пользуется и т.д. Компьютерный доступ к хранилищам информации создает предпосылки для ведения досье и организации тотальной слежки. Поэтому необходимо реализовать такую систему доступа к ресурсам и услугам, в которой одновременно с решением задач идентификации, аутентификации и авторизации клиента была бы решена задача обеспечения анонимности последнего. Проблема состоит в том, чтобы сделать электронные платежи в такой же степени анонимными, как и расчет с помощью обычных денег. Иными словами, возникает задача обеспечения неотслеживаемости электронных документов, и в частности электронных (цифровых) денег.

Одно из распространенных определений «электронные деньги» приведено в Глоссарии терминов, которые используются в платежных системах [1]: электронные деньги – это «стоимость, которая сохраняется в электронном виде на таких устройствах, как чиповая карточка или накопитель на жестком диске персонального компьютера».

По мнению авторов «электронные деньги» – это нано-информационно-измерительная институция стоимости в социально-экономических отношениях, представленная на электронном носителе.

Развитие концепции электронных денег повлекло создание виртуальных банков, не имеющих обычных атрибутов банковского учреждения. Они существуют в глобальной компьютерной сети *Internet* в форме электронных страничек, представляя собой набор интеллектуальных компьютерных программ по обслуживанию безналичных денежных средств клиента и успешно выполняя большинство традиционных функций банковских учреждений на финансовых рынках мира. Виртуальные банки и банковские системы начали свой жизненный цикл с американской денежной системы. Начался процесс создания виртуальных банков также в странах Европейского содружества.

Возможность перемещать электронные деньги скрытно и быстро недоступными для традиционной банковской системы способами, подогревает интерес к преступной деятельности. Один из элементов защиты электронных денег – установление ограничений на их сумму, которая может сохраняться на электронных устройствах покупателей и продавцов и на величину транзакции. Данные Европейского центрального банка свидетельствуют о том, что на практике в Европе максимальная сумма электронных денег часто устанавливается самими системами и изменяется в пределах нескольких сотен евро. Например, для системы *Geldkarte* (Германия) эта сумма составляет 200 евро, для систем *Quik* (Австрия) и *Avant* (Финляндия) – 400 евро, для системы *Chipknip* (Нидерланды) – 450 евро [2].

Понимание важности вопросов защиты в системах электронных денег привело к проведению Банком международных расчетов отдельного исследования [3], результатом которого стало обнародование в августе 1996 года документа «Защита электронных денег», содержащего главные особенности построения систем электронных денег, а также связанные с ними риски.

В 2003 году Европейский центральный банк обнародовал «Требования к защите электронных денег», в которых проведен анализ рисков и атак в системах электронных денег и приведен перечень необходимых мероприятий по их защите с целью уменьшения этих рисков [4].

Хеш-функция и слепая цифровая подпись

Хеш-функцией называется преобразование $h(x)$, превращающее информационную последовательность M произвольной длины в информационную последовательность (хеш-образ) фиксированной длины $h(M)$. Хеш-функция должна удовлетворять некоторым требованиям:

1. Результат работы хеш-функции должен зависеть от всех двоичных символов исходного сообщения, а также от их взаимного расположения, т.е. $h(x)$ должна быть чувствительна к любым изменениям входной информационной последовательности.

2. Хеш-функция должна быть стойкой в смысле обращения.

3. Хеш-функция должна быть стойкой в смысле существования коллизий.

Области использования хеш-функций:

- защита паролей при их передаче и хранении;
- получение хеш-образа перед формированием электронной подписи.

Наиболее используемые алгоритмы получения хеш-образов сообщений:

- семейство алгоритмов вычисления хеш-функций (*Message Digest Algorithm*) – разработаны Р.Л. Ривестом. Хеш-функции в этих алгоритмах преобразуют входные сообщения произвольной длины в сжатый 128 или 160-битный образ;
- *TIGER* – разработан Р. Андерсоном и Э. Бихэмом; предназначен для реализации на 64-разрядных компьютерах; преобразует информационную последовательность произвольной длины в хеш-образ разрядностью 192 бита;
- хеш-функция на основании теоретико-числового преобразования (быстрого преобразования Фурье), предложенная К. Шнорром, ставит в соответствие сообщению произвольной длины 128-битный образ.

Источником атак на хеш-функцию есть неполное выполнение требований 1 – 3. В настоящее время, с целью повышения качества хеш-функций, объявлен международный конкурс на новый стандарт на хеш-функцию.

Хеш-функция – неотъемлемая часть схем электронной цифровой подписи (ЭЦП). Применение медленных (в сравнении с симметричными) несимметричных криптоалгоритмов для преобразования всего исходного сообщения нерационально, поэтому для повышения быстродействия схемы ЭЦП перед процедурой формирования подписи используется функция необратимого сжатия информации.

Схемы ЭЦП – основные криптографические средства обеспечения аутентичности информации:

- с их помощью получатель документа может доказать, что документ принадлежит отправи-

телю, при этом автор подписи не сможет оспорить факт отправки подписанного документа;

• ЭЦП невозможно подделать, только абонент, чья подпись стоит на документе, мог подписать данный документ;

• ЭЦП – неотъемлемая часть документа, перенести ее на другой документ нельзя;

• ни противник, ни получатель не могут изменить документ, оставив данный факт незамеченным;

• любой пользователь, имеющий образец подписи, может удостовериться в подлинности документа.

В некоторых случаях могут потребоваться схемы электронной подписи, отличные от классической. Известны следующие *специальные схемы ЭЦП*:

• слепой подписи (как раз для решения проблемы неотслеживаемости электронных денег), когда абонент A подписывает документ, не зная его содержимого;

• групповой подписи, позволяющая верификатору убедиться в принадлежности полученного сообщения некоторой группе претендентов, но кто именно из членов группы подписал документ, верификатор определить не в состоянии;

• разделяемой подписи, которая формируется только при участии определенного количества участников протокола, иначе говоря, данная схема является объединением классической схемы подписи и схемы разделения секрета;

• конфиденциальной (неотвергаемой) подписи, которая не может быть проверена без участия сформировавшего ее участника протокола;

• неоспоримой подписи, в которой подделка подписи может быть доказана.

Рассмотрим схему слепой электронной цифровой подписи (ЭЦП), когда подписывающий (абонент B) не знает, какую информацию он подписывает. Практическое применение этой схемы рассмотрено далее.

Пусть $E(x) = x^e \bmod N$ – открытая функция зашифрования*, а $D(x) = x^d \bmod N$ – секретная функция расшифрования, где $(e, N) – PK_B$ – открытый ключ абонента B, $d – SK_B$ – секретный ключ абонента B.

Пошаговое описание схемы слепой ЭЦП следующее:

Ш а г 1. Абонент A вычисляет хеш-образ $h(M)$ последовательности M;

Ш а г 2. Абонент A формирует случайное число R $(1 \le R \le N-1)$ – «ослепляющий» параметр;

Ш а г 3. Абонент A шифрует R на секретном ключе PK_B и формирует сообщение

$$y_A = h(M) \cdot R^e \bmod N,$$

которое отправляет абоненту B.

Ш а г 4. Абонент B зашифровывает сообщение y_A своим секретным ключем

$$y_B = SK_B(y_A) = (y_A)^d \bmod N =$$
$$= h^d(M) \cdot R^{ed} \bmod N = h^d(M) \cdot R \cdot \bmod N$$

и отправляет результат абоненту A.

Ш а г 5. Абонент A снимает действие «ослепляющего» параметра

$$y_B/R = h^d(M) \bmod N$$

и получает ЭЦП абонента B на документе M, при этом B не получил никакой информации о подписанном документе.

Определение $h(M)$ из $h(M) \cdot R^e$ невозможно из теоретико-информационных соображений, поскольку для произвольного $h(M)$ существуют такое R, что вычисление $h(M) \cdot R^e$ не дает возможности получить подпись $h(M)$.

Криптографические протоколы электронных платежей

Итак, изложены те основные понятия, которые неоднократно используются в криптографических протоколах неотслеживаемости электронных денег и платежей.

Теперь выделим свойства, которыми должна обладать система ЭД:

• трудоемкость подделки ЭД;

• предотвращение возможности дублирования;

• обеспечение анонимности покупателя.

Для работы с ЭД разрабатываются специальные криптографические протоколы, называемые протоколами электронных платежей. В таком протоколе задействованы три участника:

* Имеется в виду использование алгоритма *RSA*

банк, покупатель и продавец. Покупатель и продавец имеют счета в банке, и покупатель желает заплатить продавцу за товар или услугу.

В платежной системе используются три основные транзакции [5] – [7]:

– снятие со счета;

– платеж;

– депозит.

Протокол снятия со счета. Его пошаговое описание:

Ш а г 1. Пользователь сообщает банку, что он желает снять со своего счета некоторую сумму, например $100;

Ш а г 2. Банк в ответ на запрос отправляет цифровую купюру, имеющую следующий формат:

{Номинал купюры: $100;
номер купюры: 260577} SK_B,

где SK_B – секретный ключ банка;

Ш а г 3. Пользователь проверяет подпись банка, и если она верна, принимает купюру.

Платежный протокол. Его пошаговое описание:

Ш а г 1. Пользователь оплачивает товар, предъявляя купюру;

Ш а г 2. Продавец проверяет подпись банка и, если она верна, принимает купюру в качестве платы.

Депозитный протокол. Его пошаговое описание:

Ш а г 1. Продавец посылает купюру банку;

Ш а г 2. Банк проверяет свою подпись и, если она верна, начисляет на счет продавца сумму, равную номиналу купюры.

Недостатки приведенных протоколов:

• банк может связать имя пользователя с серийным номером купюры при ее выдаче и отслеживать все его действия;

• полученные от банка купюры можно дублировать и многократно использовать.

Анонимность покупателя обеспечивает применение слепой подписи в протоколе снятия со счета. Для предотвращения повторной траты банк должен поддерживать список номеров ранее потраченных купюр.

Заключение. Можно выделить следующие группы последствий широкого принятия цифровой наличности в качестве платежного инструмента:

• увеличение скорости обращения денежной массы;

• низкая стоимость денежного обращения;

• приватный статус, т.е. электронные деньги не являются законным платежным средством (*legal tender*), так как законодательство не обязывает принимать ЭД как средство платежа;

• увеличение скорости исполнения принятых экономическими агентами решений о перемещении средств;

• изменение роли банков в национальных и мировой финансовых системах.

1. *A Glossary* of Terms Used in Payments and Settlement System, BIS, 2003. – P. 51.
2. *Survey* of Developments in Electronic Money and Internet and Mobile Payments, BIS, CPSS, 2004. – http://www.bis.org/publ/cpss62.pdf
3. *Security* of electronic money, BIS, CPSS, 1996. – http://www.bis.org/publ/cpss18.pdf
4. *Electronic* Money System Security Objectives Report, ECB, 2003.
5. *Деднев М.А.*, *Дыльнов Д.В.*, *Иванов М.А.* Защита информации в банковском деле и электронном бизнесе. – М.: КУДИЦ-ОБРАЗ, 2004. – 512 с.
6. *Введение* в криптографию / Под ред. В.В. Ященко. – М.: МЦНМО: «ЧеРо», 1999. – 272 с.
7. *Комп'ютерна* криптологія: Підручник / В.К. Задірака, О.С. Олексюк. – К.: 2002. – 504 с.

Поступила 01.03.2011

Тел. для справок: (044) 526-0288 (Киев)
E-mail: *zvk*140*@ukr.net*