Эссе по курсу "Защита информации", кафедра радиотехники, Московский физикотехнический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec

Идеальные электронные наличные

Студент: *Каменев Владимир Александрович*
Группа: *116 группа*
Курс: *“Защита информации”*

г. Долгопрудный
2005 г.

Содержание

Введение

В данном Эссе описывается без углубления в подробное математическое изложение схема, предложенная японскими криптографами Тацуаки Окамото (Tatsuaki Okamoto) и Казуа Охта (Kazuo Ohta). Ее особенностью является то, что она удовлетворяет шести критериям так называемой идеальной платежной системы и может быть использована в микропроцессорных кредитных карточках. Авторы считают ее первой идеальной системой электронных платежей.

Идеальные электронные наличные

В 1991 году японскими криптографами Тацуаки Окамото (Tatsuaki Okamoto) и Казуа Охта (Kazuo Ohta) были сформулированы шесть критериев, которым должна удовлетворять так называемая идеальная платежная система. Они заключались в следующем:

1. Независимость. Безопасность электронных наличных не зависит от местонахождения. Наличные могут быть переданы по компьютерным сетям.
2. Безопасность. Электронные наличные нельзя повторно использовать.
3. Неотслеживаемость. Тайна личности пользователя защищена, связь между пользователем и его покупками обнаружить невозможно.
4. Автономный платеж. Когда пользователь расплачивается за покупку электронными наличными, протокол между пользователем и продавцом выполняется автономно.
5. Перемещаемость. Наличные могут передаваться другим пользователям.
6. Делимость. Заданная сумма электронных наличных может быть поделена на части меньшей суммы.

Они же показали, что все предложенные до них схемы, не удовлетворяют сразу всем шести требованиям. Например протокол, описанный в [2] (стр. 106-107) удовлетворяет только требованиям с 1 по 4. То есть их нельзя передать другому пользователю, как это имеет место с реальным деньгами, и нельзя тратить эти наличные по частям. Ранее авторами предлагалась схема, удовлетворяющая с 1 по 6 требованиям. Делимость электронных наличных обеспечивалась за счет того, что деньги представлялись в ней в виде совокупности более мелких купюр. Недостатком такой схемы является то, что платеж сопровождается передачей и обработкой значительных объемов данных. Например, если платеж равен 356,27$, а номинал отдельной купюры равен 0,01$, то объем передаваемых данных составит около 200 Мбайт, что приводит к невозможности практического применения схемы. Однако, авторами был найден способ избежать этой трудности. Они предложили протокол, в котором электронные наличные представлялись в виде бинарного дерева. Таким образом, пользователь как бы имеет купюры различного номинала. В такой схеме платеж из предыдущего примера потребовал бы передать всего 20 Кбайт. Всвязи с этим, протокол может быть использован в микропроцессорных кредитных карточках. Авторы считают эту схему первой идеальной системой неотслеживаемых электронных наличных.

Описание схемы

Безопасность и неотслеживаемость электронных наличных

Для того, что бы было проще понять суть схемы, опишем сначала более простой протокол, удовлетворяющий требованиям с 1 по 4 (рис. 1):

1. Клиент сначала отсылает запрос банку по-поводу снятия с своего счета определенной суммы наличных. Банк уменьшает счет клиента на заданную сумму денег и выдает ему электронные наличные в виде некоторого цифрового текста,

причем этот текст включает информацию и о самом клиенте. Но особенность является то, что эти данные банк может извлечь за разумное время, только если клиент попытается смошенничать и попытается использовать наличные дважды.

2. Клиент передает наличные продавцу
3. Продавец предъявляет наличные банку. Если наличные ранее не использовались, банк увеличивает счет продавца на заданную сумму и заносит информацию о наличных в базу данных. Если в базе данных банка уже есть запись об этих наличных, то по двум записям в базе данных банка становится возможным извлечь информацию, идентифицирующую клиента (более подробно о схеме можно узнать в [2])

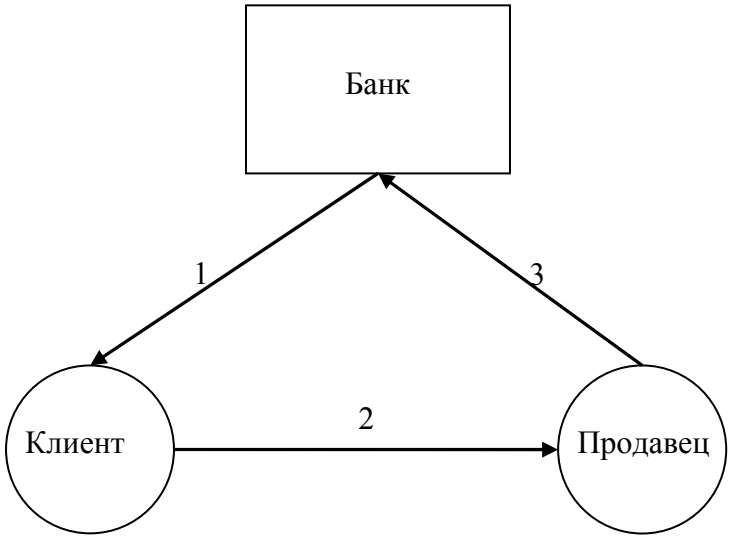

Рис 1

Очевидно, что протокол удовлетворяет требованиям с 1 по 4. Платеж всегда возможен, если имеется доступ в интернет, так как электронные наличные передаются в виде битовых строк. Одни и те же наличные нельзя потратит дважды, так как по двум записям базы данных банка легко устанавливается личность клиента. Если клиент не делает ошибок и не нарушает закон, его личность невозможно установить никакими численными методами за разумное время. Сделка между продавцом и клиентом осуществляется автономно, банк ничего о ней не знает. Однако, клиент А не может непосредственно передать электронные наличные клиенту В, так как после передачи информация, зашифрованная в наличных, все еще будет указывать на клиента А. Если клиент В смошенничает, то посадят клиента А, а не В. Также клиент не может тратить наличные по частям, так как это означает неоднократное использование наличных, а значит личность клиента легко может быть раскрыта. Неотслеживаемость электронных наличных будет нарушена.

Делимость электронных наличных

Для обеспечения делимости электронных наличных, Тацуаки Окамото и Казуа Охта предложили пердставлять электронные наличные в виде бинарного дерева (рис. 2). Каждому узлу дерева соответсвует некоторая сумма наличных. Верхнему узлу дерева соответсвует общая сумма снятых со счета денег. Узлу более нижнего ранга соответствует половина от суммы денег родительского узла. Древовидная структура должна удовлетворять следующим условиям:

1. Никакой узел дерева клиентом не может быть использован дважды (то ест не могут быть потрачены дважды наличные, которые относятся к одному и тому же узлу дерева). Повторное использование одного и того же узла ведет к идентификации клиента.

2. Если некоторый узел дерева уже использован, то его родительские или дочерние узлы использованы уже быть не могут. В противном случае личность клиента устанавливается.

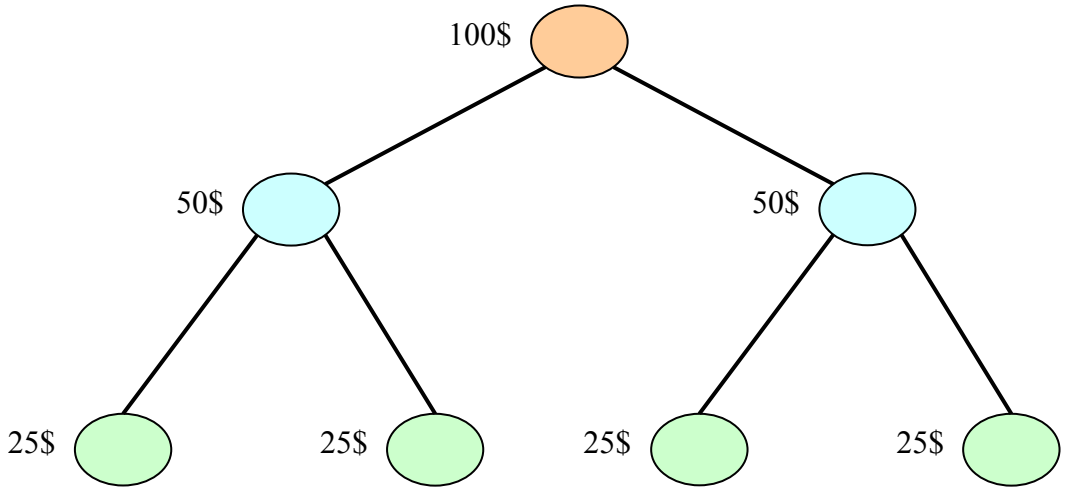

Рис 2

Такое представление электронных наличных полностью аналогично случаю, когда наличные клиента представляются в виде совокупности банкнот различного номинала. Для оплаты услуги, например стоимостью 75$, достаточно задействовать всего два узла дерева, соответствующие 50$ и 25$. Тогда единственный узел, который после проведения оплаты можно будет использовать без риска раскрытия личности клиента, будет соответствовать 25$, то есть остатку.

Технически такая возможность предоставляется посредством проведения как клиентом, так и продавцом довольно сложных математических вычислений. Подробное их написание потребует так же изложения свойств таких математических понятий, как целые числа Уильяма (Williams integer), вычеты и невычеты, символы Лежандра и Якоби, что явно выходит за рамки этого ЭССЕ. С формальной записью протокола можно познакомиться в [1].

Перемещаемость электронных наличных

Пусть клиент А имеет в наличии 100$ и он хочет передать из них 25$ клиенту В. Для осуществления передачи электронных, клиенты должны следовать слеующей схеме:

1. Клиент А вычисляет отправляет клиенту В те же самые битовые строки, как если бы клиент В был продавцом. Кроме того, клиент А посылает клиенту В сертификат Т, означающий передачу электронных наличных. В сертификате в зашифрованном виде хранится информация о электронном “кошельке” клиента А, о том, какой узел дерева используется, и указывается банковский счет клиента В.
2. Клиент В осуществляет те же операции, что и продавец.
3. Если клиент В захочет потратить полученные 25$, то он сначала передает продавцу данные о передачи электронных наличных, которая проверяется затем продавцом. Если все было сделано правильно, продавец и клиент В, следуют обычному протоколу оплаты услуги.
4. Далее, для пополнения своего банковского счета на 25$, продавец предъявляет данные Н о выполнении протокола пункта 3. Банк пополняет банковский счет продавца и заносит данные Н в свою базу данных.

Обзор литературы

1. T. Okamoto and K. Ohta, “Universal Electronic Cash”, Advances in Cryptology CRYPTO ’91 Proceedings, Springer-Verlag, 1992, pp. 324-337.
2. Брюс Шнайер, “Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С”, стр. 103-109.
3. Tatsuo Tanaka, “Possible Economic Consequences of Digital Cash”