1. Протоколы открытых сделок

*Протоколы битовых обязательств и их свойства. Протоколы подбрасывания монеты и “игры в покер” по телефону. Забывающая передача информации. Протокол подписания контракта. Протокол сертифицированной электронной почты. Протоколы электронного голосования. Свойства неотслеживаемости и несвязывемости. Протоколы электронных платежей и цифровых денег.*

Представим теперь себе следующую ситуацию. Имеются два абонента А и В сети связи, скажем, компьютерной сети. В – это банк, в котором у А имеется счет и А хочет переслать В по сети в электронной форме платежное поручение перевести, например, 10 фантиков со своего счета на счет другого клиента С. У абонентов А и В нет никакой конфиденциальной информации. Закрытый канал не нужен. В самом деле, клиенты пересылают банку в качестве сообщений платежные поручения, содержание которых стандартно и общеизвестно. Для банка важно убедиться в том, что данное сообщение действительно исходит от Л, а последнему, в свою очередь, необходимо, чтобы никто не мог изменить сумму, указанную в платежном поручении, или просто послать поддельное поручение от его имени. Иными словами, требуется гарантия поступления сообщений из достоверного источника и в неискаженном виде. Такая гарантия называется обеспечением целостности информации и составляет важную задачу криптографических протоколов.

Нетрудно видеть, что при пересылке платежных поручений в электронной форме возникает еще и совершенно иной тип угроз безопасности клиентов: всякий, кто перехватит сообщение от А к В, узнает, что С получил от А 10 фантиков. А что будет, если эта информация попадет в руки мафии? Возможно, кто-то скажет, что здесь как раз и требуется конфиденциальность – закрытый канал. Но закрытый канал не нужен. На самом деле клиентам необходимо нечто, аналогичное свойству анонимности обычных бумажных денег. Хотя каждая бумажная купюра имеет уникальный номер, определить, кто ее использовал и в каких платежах, практически невозможно. Аналог этого свойства в криптографии называется неотслеживаемостью. Обеспечение неотслеживаемости — еще одна задача криптографических протоколов.

Электронная платежная система – аналог традиционной платежной системы, обеспечивающий денежные расчеты между поставщиками и потребителями в электронном виде (без шелеста купюр, рукописных подписей и пр.). Развитие систем электронного бизнеса невозможно без решения следующих задач защиты информации: - аутентификация участников информационного взаимодействия; - обеспечение конфиденциальности и целостности коммерческой информации (документов, удостоверяющих факт сделки, платежных документов, счетов, заказов и пр.) при ее передаче по каналам связи; - обеспечение невозможности отказа от факта получения какого-либо сообщения; - обеспечение юридической значимости пересылаемых электронных документов.

Уже достаточно давно банки и другие коммерческие структуры используют при проведении деловых операций электронный обмен данными EDI (Electronic Data Interchange) и электронный перевод денежных средств EFT (Electronic Funds Transfer). В современных платежных системах весь процесс от начала до конца происходит в электронной (цифровой) форме. При этом для обеспечения безопасности и признания законности (конфиденциальности пересылаемых электронных документов, аутентификации участников информационного обмена) повсеместно используются криптосистемы с открытым ключом для шифрования и формирования электронной подписи. Учитывая, что традиционные денежные купюры есть не что иное, как защищенный от подделки документ, логичным представляется переход к использованию *цифровых денег*. Защиту от подделки при этом может обеспечить электронная подпись банка, которая, очевидно, имеет большую надежность, чем традиционные водяные знаки, металлические полосы и т. п.

Электронные деньги должны обеспечивать приватность и анонимность. Децентрализованные платежи, скрытые от глаз третьего лица – вот что отличает системы электронных денег от традиционной банковской системы Для этого необходима конфиденциальность: подробности сделки между продавцом и покупателем не должны быть известны никому больше. Для обеспечения конфиденциальности требуется, чтобы электронные деньги удовлетворяли двум требованиям:

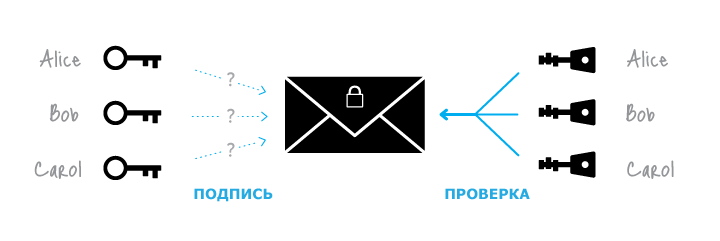
1. Неотслеживаемость. Для каждой входящий транзакции все отправители равновероятны.
2. Несвязанность. Для двух любых исходящих транзакций невозможно доказать, что они отправлены одним и тем же лицом.

Криптографическая схема проведения сделок, обеспечиващая неотслеживаемость и несвязанность – это кольцевая подпись.

Схема групповой подписи, которую впервые представили Д. Чаум и Э. ван Хейст, позволяет пользователю подписать своё послание от имени группы. Но в этом случае существует доверенная третья сторона (так называемый менеджер группы), который может однозначно идентифицировать подписавшего.

В схеме кольцевой подписи нет менеджера группы, схема является автономной. Есть модификации кольцевой подписи, которые позволяют определить, не подписано ли письмо одним и тем же участником дважды. Эта схема обеспечивает именно возможность для пользователя производить только одну действительную подпись своим закрытым ключом. Прослеживаемость ослаблена до двух вариантов: секретный ключ для генерации уникальной анонимной подписи и открытый ключ, который может быть связан с ним в случае попытки двойной траты средств. В этом схеме отправитель генерирует одноразовый открытый ключ на основе адреса получателя и некоторых случайных данных. Во входящей транзакции для получателя используется одноразовый открытый ключ, и только получатель средств может использовать ее с помощью своего закрытого ключа. Получатель может потратить средства с использованием кольцевой подписи, сохраняя анонимность кошелька и свои фактические расходы

Идея одноразовой кольцевой подписи проста – пользователь производит подпись, которая проверяется с помощью набора открытых ключей, а не отдельным уникальным открытым ключом (рис. 7.1). Идентичность подписавшего является неотличимой от других пользователей, чьи открытые ключи находятся в том же наборе.

Рис. 7.1 Проверка одноразовой кольцевой подписи

«Отцом» цифровых денег с полным основанием можно назвать Д. Чаума, основателя и исполнительного директора фирмы DigiCash и одновременно признанного специалиста в области криптографии. DigiCash разработала и запатентовала криптографическую технологию безопасных электронных платежей. Выглядит цифровая купюра приблизительно так, как показано на рис. 7.2. Документ содержит номинал и номер купюры, а также подпись банка-эмитента, которая получена на его секретном ключе. При этом *электронная подпись надежно защищает купюру от подделки, но совершенно не защищает от копирования.* Чтобы избежать превращения цифровой купюры в «неразменный пятак», банк-эмитент должен контролировать каждую сделку.

Рис. 7.2. Цифровая купюра

Клиент А (будущий покупатель), желающий получить определенную сумму цифровых денег, посылает в банк-эмитент, в котором у него имеется счет, «полуфабрикат» цифровой купюры, имеющий вид, аналогичный показанному на рис. 7.2. Только подписан этот документ самим клиентом А. Так как А является клиентом банка, там знают его открытый ключ, а значит, могут проверить подпись. Убедившись, что именно А заказал цифровые деньги, банк удаляет его подпись, ставит свою, вычитает со счета А сумму, равную номиналу купюры, и отсылает последнюю А. Получив электронную купюру, А может потратить ее сам, переслав (или передав) ее в обмен на товар продавцу B1 в магазине, принимающем цифровые деньги, либо переслать (или передать) ее другому человеку B2. Чтобы осуществить процесс передачи цифровой купюры, участники обмена А и В, а также банк-эмитент С должны одновременно находиться на связи. Перед передачей купюры В участник А подписывает ее своим секретным ключом. Получив купюру, В проверяет подпись, а затем, убедившись в ее подлинности, удаляет ее и ставит свою, после чего отправляет в банк-эмитент. Банк проверяет, не получал ли он уже эту банкноту (защита от копирования!), т. е. ищет ее номер в специальном списке купюр, предъявленных к оплате ранее. Если банкнотой никто раньше не пользовался, ее номер заносят в список использованных купюр (второй раз ее к оплате не примут!) и переводят сумму, равную номиналу цифровой купюры, на счет своего клиента В.

Покупатель перечисляет деньги в банк-эмитент либо напрямую, либо через банк – участник системы. Взамен покупатель получает цифровые деньги. Получив их при оплате товара, продавец, проверив их подлинность, отдает товар, перечисляет цифровые деньги банку-эмитенту, а тот переводит обычные денежные средства на счет продавца. Рассмотренная схема не обеспечивает неотслеживаемости электронных платежных средств, так как позволяет проследить за движением денег от А к В. Когда клиент А присылает заявку на цифровую купюру достоинством допустим 100 у.е., банк узнает номер купюры. В результате, когда эту купюру предъявляет к оплате клиент В, банк узнает, что А заплатил В 100 у.е. Таким образом, данная схема не обеспечивает анонимность платежей, банк в состоянии составить полное досье на любого своего клиента: кто, сколько и кому платил, сколько и от кого получал.

Рассмотренная система платежей, требующая участия банка во всех транзакциях, называется *централизованной*. В отличие от нее *автономная система платежей* предполагает, что продавец В сам, без обращения к банку С, проверяет подлинность предъявленной покупателем А электронной наличности. Понятно, что в этом случае банк идет на определенный риск, так как используемые схемы обеспечивают обнаружение злоупотреблений со стороны А постфактум. Основная идея соответствующих протоколов – однозначно идентифицировать нарушителя.

Цифровые деньги (цифровая наличность) – это защищенное от подделки электронное платежное средство. Более того, это единственное платежное средство, обеспечивающее анонимность и неотслеживаемость платежей. Ни одно из множества других электронных платежных средств (платежные карты, электронные чеки и пр.) такими свойствами не обладает. Проблемы информационной безопасности, которые решены в схеме цифровых денег:

– как защититься от кражи купюры (задача защиты прав собственника информации);

– как защититься от повторного использования купюры, учитывая, что электронный документ и ЭЦП можно копировать сколь угодно много раз;

- как защититься от подделки номинала цифровой купюры, учитывая, что ЭЦП банка-эмитента ставится только на номере купюры;

- как обеспечить анонимность и неотслеживаемость платежей, иначе говоря, как получить полный электронный аналог бумажных денег, обладающих такими свойствами.

В некоторых случаях необходимо, чтобы участники, расположенные далеко друг от друга, создали случайную последовательность и при этом не обращались за помощью к третьей стороне. Если участников двое, то действие протокола, решающего поставленную задачу, будет равносильно подбрасыванию монеты по телефону.

Протоколы типа «подбрасывание монеты по телефону» – это вид криптографических протоколов, в которых два участника должны обменяться некоторой информацией. Но участники не доверяют друг другу и каждый из них может оказаться обманщиком. Поэтому, если один из участников по неосторожности «выпустит информацию из рук» преждевременно, то в обмен он может получить совсем не то, о чем договаривались, или вообще не получить ничего.

Из всех криптографических протоколов данного типа, пожалуй, наиболее наглядным, и к тому же достаточно простым, является протокол подбрасывания монеты. Предположим, что двум участникам, Алисе и Бобу, необходимо бросить жребий. В случае, когда они оба физически находятся в одном и том же месте, задачу можно решить с помощью обычной процедуры подбрасывания монеты. Если кто-либо из участников не доверяет монете, можно использовать другие источники случайности. Правда, создание надежных источников случайности – весьма непростая задача, но она уже относится к математической статистике, а не к криптографии.

Если же Алиса и Боб удалены друг от друга и могут общаться лишь по каналу связи, то задача о жребии, на первый взгляд, кажется неразрешимой. В самом деле, если, следуя обычной процедуре подбрасывания монеты, первый ход делает Алиса, которая выбирает один из возможных вариантов – «орел» или «решка», то Боб всегда может объявить тот исход, который ему выгоден.

Легко понять, что задача о жребии решается очень просто, если существует надежный агент – третья сторона, которая пользуется полным доверием и Алисы, и Боба, и которая имеет конфиденциальные (закрытые) каналы связи с обоими участниками. В этом случае Боб и Алиса выбирают случайные биты *b* и *c* соответственно и посылают их в тайне друг от друга агенту. Последний ждет, пока не поступят оба бита, и после этого публикует d = b ⊕ c – исход подбрасывания монеты.

В отсутствие надежного агента срабатывает идея, которую проще всего понять на следующей «физической» реализации. Боб выбирает случайный бит 6, записывает его на листе бумаги, запирает этот лист в ящике, оставляя ключ от замка у себя, и посылает ящик Алисе. Предполагается, что, не имея ключа, Алиса не может добраться до содержимого ящика. Получив ящик, Алиса выбирает случайный бит с и посылает его Бобу. В ответ Боб посылает Алисе ключ от ящика. Исходом подбрасывания монеты будет опять-таки бит d = b ⊕ c.

В этом протоколе для значения*,* в которое упаковывается бит, (аналог ящика в физической реализации) обычно используется термин блоб (blob), для Алисы — получатель, а для Боба — отправитель. Действие по упаковке в ящик обеспечивается протоколом привязки к биту. В этом протоколе требуется такая конструкция блоба, которая обеспечивает одновременное выполнение следующих двух требований:

* после выполнения этапа привязки получатель не может самостоятельно определить, какой бит упакован в блоб;
* на этапе открытия бита отправитель может открыть любой блоб либо только как 0, либо только как 1.

В схеме забывающей передачи основная идея состоит в том, чтобы участник А после передачи некоторого секрета участнику В не знал, передавал ли он секрет или нет, но при этом участник В точно знал, получил он секрет или не получил. Данная задача может быть решена с помощью частичного раскрытия секретов и доверенного арбитра. Однако в ряде случаев возникает ситуация, в которой воспользоваться услугами доверенной стороны не представляется возможным, поэтому особый интерес вызывают протоколы забывающей передачи, не применяющие доверенную сторону.

В настоящее время существуют протоколы, известные как справедливые (честные) обменные протоколы. Эти протоколы – существенная составляющая электронной коммерции, они обеспечивают справедливость – то есть гарантии клиентам и продавцам в том, что никакая сторона не получит преимущества. Справедливая система – это система, которая не предвзято относится к правильно ведущему себя игроку. Пока игрок ведет себя правильно, справедливая система должна гарантировать что другие игроки не получат преимущества перед правильно ведущими себя игроками.

Задача честного обмена цифровыми данными может быть поставлена в двух вариантах. Первый вариант имеет отношение к электронной коммерции и связан с платным распространением по компьютерным сетям цифровых потоков данных (digital content). Такая ситуация реализуется, например, при продаже музыкальных записей, литературных произведений, сводок новостей, курсов акций и т. п. товаров, которые можно преобразовать в цифровую форму, передать по сети и вновь преобразовать для получателей в удобную для восприятия форму (нет необходимости физически доставлять товар потребителю). Покупатель в ответ должен получить чек, подтверждающий факт покупки. Второй вариант возникает, когда необходимо построить систему сертифицированной электронной почты.

Протокол сертифицированной электронной почты (certified e-mail protocol) - криптографический протокол, который предполагает обязательное получение участниками уведомлений о факте отправки и получения сообщения (не зависящих от его содержания), которое в дальнейшем позволит доказать отправителю факт получения сообщения, а получателю – что оно не было отправлено отправителем в случае, если он попытается утверждать обратное.

Этим задачам в настоящее время уделяется очень большое внимание среди общего поля проблем электронной коммерции и электронного документооборота.  
Второй уровень рассмотрения задач электронной коммерции с точки зрения обеспечения безопасности информации - это процессы деловой деятельности. Для решения задач обеспечения безопасности этого уровня применяется концепция транзакций, или дел (deal). Это последовательность шагов, цель которой - осуществить целостный бизнес-процесс, поддерживая взаимосвязь между отдельными его этапами по мере их выполнения. Ход выполнения транзакции записывается всеми участвующими в ней сторонами, причем запись включает получаемую и отправляемую информацию, а также общую информацию о процессе: согласованные атрибуты защиты, идентификаторы участников, логические связи между этапами транзакции и др. Все эти сведения являются основой для обработки исключи-тельных ситуаций и разрешения споров и конфликтов, возникающих между участниками коммерческих отношений.

Примерами процессов деловой деятельности, для которых обеспечение безопасности информации требует целостного их рассмотрения, являются: электронные аукционы, электронные выборы (голосования), электронные биржи, электронные лотереи и т. п. процессы. Для всех них требуются криптографические протоколы честного обмена цифровыми данными. Очень большую роль в обеспечении безопасности бизнес-процессов играют также двусторонние и многосторонние схемы цифровой подписи со специальными свойствами. Примером может являться оформление прав на недвижимое имущество, требующее, как известно, очень большого количества решений и согласований, а также оформление или регистрация каких-либо иных прав или обязанностей субъектов электронного рынка.

Протокол сертифицированной электронной почты основан на схеме равноправного обмена цифровыми подписями без использования третьей доверенной стороны. В общем виде протокол строится следующим образом:

Этап 1. Генерация и публикация ключей.

1.Участники обмена, генерируют закрытый и открытый ключи (sk,pk).

Этап 2. Вычисление подписи и ее проверка.

2.Участники вычисляют подпись.

Подпись содержит доказательство того что подпись связана с некоторым битовым вектором.

Так же на этом этапе вычисляется аргумент доказательства с нулевым разглашением

3.Проверка подписи

Проверяющий получает подпись. Проверяется аргумент доказательства с нулевым разглашением.

Таким образом доказывается знание затемняющего фактора.

Этап 3. Открытие и проверка битов затемнения

4. Генерация бита с секретом

Открытие i-го бита с секретом. Каждый участник отправляет своему оппоненту сообщение бит, с помощью которых составлялся вектор битов с секретом.

5. Проверка бита

Проверка равенства берется из подписи полученной от пописывающего.

В конце этого этапа у каждого участника обмена должны быть все биты составляющие параметр затемнения.

Этап 4. Снятие затемнения с подписи.

6. Каждый участник вычисляет с помощью полученных битов затемнения и снимает затемнение с подписи.