Н. А. Мацук

ПРОТОКОЛ ЭЛЕКТРОННОЙ ТОРГОВЛИ БЕЗ АРБИТРА

В настоящее время бурного развития электронной коммерции широкое применение находят криптографические протоколы, обеспечивающие защиту интересов покупателей и продавцов при торговле информацией. Основная часть таких протоколов требует участия третьей стороны (например, банка), пользующейся доверием обеих сторон и выступающей в качестве гаранта справедливости сделки. Известен алгоритм, позволяющий покупателю и продавцу безопасно обмениваться секретами без посредника, но для этого стороны должны друг другу доверять, так как в процессе обмена каждому из участников предоставляется возможность для обмана [1]. В конце протокола оба должны раскрыть свои закрытые ключи и доказать свою честность.

Наиболее разработанной областью применения криптографии в сфере электронной коммерции на сегодняшний день является организация микроплатежей. Данной проблематике посвящены десятки работ, в которых решается задача минимизации накладных расходов банка по обслуживанию микроплатежей и повышения рентабельности электронной торговли. В большей части работ предлагается собственный вариант электронной платежной системы, реализующий либо механизм отложенных платежей [2], либо агрегацию платежных поручений многих клиентов [3, 4]. При этом предполагается, что покупатель и продавец пользуются взаимным доверием, а банк является непременным гарантом их платежеспособности.

Между тем возможно построение протокола электронной торговли, предназначенного для ситуации, когда покупатель и продавец хотели бы совершить сделку, но опасаются мошенничества, а привлечь общего надежного арбитра не представляется возможным. Такой протокол должен решать две главные проблемы, возникающие при торговле без посредника: проблему одновременности обмена и так называемую проблему «кота в мешке».

Суть проблемы одновременности обмена заключается в следующем: если в какой-либо момент времени покупатель получает товар до перечисления денег, то он может выйти из протокола, присвоив и то, и другое. Аналогично ведет себя продавец, получив предоплату до отправки товара. Проблема усугубляется введением дополнительного условия анонимности сторон. Когда покупатель и продавец взаимодействуют конфиденциально, не раскрывая своих истинных личностей, неизвестно, кому предъявлять претензии и на кого подавать в суд. Следовательно, необходимо добиться, чтобы на всех стадиях исполнения протокола как покупатель, так и продавец находились в равном положении относительно приобретенной выгоды, или, по крайней мере, несли одинаковые риски.

Обычно возможность изучить товар и выявить его потребительские качества покупатель получает только после свершения сделки. До и во время торгов он вынужден довольствоваться тем описанием товара, которое ему дает продавец. В связи с этим может возникнуть ситуация, когда покупатель платит деньги вовсе не за то, что предполагал. Трудности подобного рода принято считать проблемой «кота в мешке». Эта проблема очень сложна и в общем случае не имеет решения даже в обычной повседневной жизни, однако существуют методы, позволяющие свести риск покупателя к минимуму.

В этом смысле наиболее многообещающими выглядят вероятностные методы в протоколах электронной коммерции. Например, Р. Липтон и Р. Островский описали протокол, в котором покупатель за одну транзакцию одновременно оплачивает значительную порцию товаров или услуг, а момент оплаты определяется подбрасыванием несимметричной монеты [5]. Еще более оригинальный подход выдвинут Р. Ривестом [6]. Он предложил использовать в качестве платежного средства лотерейные билеты, которые выпускались бы покупателем на имя продавца при покупке товара.

За товар стоимостью 1 у.е. покупатель дает купон номиналом 100 у.е. с вероятностью выигрыша $\frac{1}{100}$. Банк в качестве платежных поручений принимал бы только «выигрышные» билеты, переводя деньги со счета покупателя на счет продавца. Таким образом, продавец смог бы обналичить только небольшую часть всех принятых к оплате купонов. Для обоснования справедливости своего протокола Ривест апеллировал к закону больших чисел, которому подчинялись бы математическое ожидание и дисперсия суммарной прибыли продавца.

Следует особо отметить, что все вышеупомянутые криптографические протоколы микроплатежей были разработаны с целью удешевления электронной коммерции и снижения нагрузки на банковскую инфраструктуру. Ни один из них не обеспечивает анонимности участников торговых отношений, и каждый требует обязательного присутствия доверенного брокера по обслуживанию платежных средств. Несмотря на это, некоторые из рассмотренных подходов могут быть использованы для эффективного решения проблем одновременности обмена и «кота в мешке».

Рассмотрим правдоподобный гипотетический пример. Покупатель **П** желает купить виртуальный товар D у торговца **Т**, но при этом опасается платить деньги первым. В качестве подтверждения своих намерений **Т** зашифровывает D на случайном ключе k по какому-либо симметричному алгоритму и высылает результат **П**.

$T: \quad E_k(D) = D \rightarrow П.$

В дальнейшем покупка D сводится к выкупу ключа шифрования k. Это удобно, так как секрет D может быть достаточно большого размера и проводить с ним какие-либо манипуляции неэффективно.

Покупатель и продавец договариваются о принципе безопасной торговли без посредника. Всю сумму, предназначенную для оплаты D, **П** разбивает на N равных частей. Например, он может подготовить N цифровых купюр номиналом M так, чтобы стоимость D составляла $\frac{N \cdot M}{2}$. Затем **Т** и **П** начинают последовательный обмен сообщениями. **П** отсылает **Т** одну купюру, а **Т** в ответ передает ключ шифрования с вероятностью $\frac{1}{N}$. Если **П** повезло и получен ключ, то D расшифровывается и протокол на этом завершается. В противном случае **П** должен иметь возможность проверить, что **Т** поступает честно и не высылает просто случайные числа. На следующем шаге **П** снова платит одну купюру, а **Т** отсылает секрет с вероятностью $\frac{1}{N-1}$ и так далее, пока **П** не получит желаемое.

Для данного протокола можно привести более наглядную бытовую аналогию. Пусть у продавца есть бумажный документ, который хочет купить покупатель. Тогда **Т** помещает свой документ в непрозрачный конверт и запечатывает его специальной печатью. Печать разработана так, что наложить и снять ее может только ее владелец. Запечатанный конверт передается **П**.

Затем **Т** изготавливает $N - 1$ произвольных документов, помещает их в одинаковые конверты, которые также запечатывает своей печатью, и пересылает все $N - 1$ конвертов **П**. Содержание документов предварительно согласовано с **П** и известно ему. **П** запечатывает своей печатью все конверты, полученные от **Т**. В результате получаются N одинаковых, ничем не различающихся конвертов, которые перемешиваются между собой и отправляются **Т**.

Получив N пакетов, **Т** проверяет их целостность и снимает с них свою печать. Так как на всех конвертах стоит печать **Т**, он может быть уверен, что в одном из этих конвертов спрятан его документ, хотя и не известно, в каком именно. В дальнейшем **Т** продает конверты **П** в случайном порядке по рублю за штуку до того момента, когда будет выкуплен конверт, содержащий секретный документ.

После покупки каждого пакета **П** снимает с него свою печать и изучает содержимое. В любом полученном конверте может лежать либо секретный документ **Т**, либо одно из $N - 1$ сообщений, подготовленных им самим. Если в пакете находится что-то другое или если **П** получает

одно из своих контрольных сообщений повторно, то это означает, что **Т** захотел смошенничать и подменил конверты. Обнаружив подделку, покупатель немедленно прекращает торговлю.

Протокол будет работать только в том случае, если **Т** будет беспристрастен. Его цель должна состоять в получении максимальной материальной выгоды, а не в том, чтобы просто навредить **П**. По большому счету, **Т** все равно, получит ли **П** свой товар или нет. Главное — максимизация собственной прибыли от продажи. **П** скупает конверты по одному до тех пор, пока не получит требуемый документ или не уличит **Т** в обмане. Следовательно, **Т** невыгодно подменять запечатанные конверты и нарушать правила «игры», так как при этом «игра» закончится раньше и будет заработано меньше денег. Он хотел бы выкинуть из пачки свой конверт с секретом и положить на его место пакет с безопасным сообщением, чтобы растянуть куплю-продажу подольше, но это невозможно, ведь все конверты одинаковы, а вероятность угадать слишком мала. Даже если **Т** поступит нелогично и прервет протокол на середине, присвоив себе часть денежных средств, **П** может утешиться мыслью, что, отдав сразу всю сумму, он потерял бы больше.

К сожалению, для перенесения описанного «материального» протокола в электронно-цифровую форму требуется прибегнуть к дополнительным ухищрениям. Дело в том, что если пакеты будут заменены на последовательности байт, то ничто не помешает **П**, получив «конверт» **Т**, скопировать его $N - 1$ раз и выдать копии вместе с оригиналом за N различных сообщений, предварительно по-разному их затемнив. Предлагаемая реализация протокола преодолевает эту трудность. В протоколе торговли между покупателем и продавцом условно выделены две фазы.

Фаза 1

Первая фаза — подготовительная. Обе стороны производят предварительные вычисления и устанавливают необходимое исходное состояние для проведения торгов. Цель продавца в фазе 1 — выработать множество сообщений, содержание которых было бы ему известно. Задача покупателя — сделать так, чтобы продавец не знал местоположение конкретных сообщений в массиве. Другими словами, в конце фазы 1 **Т** должен знать, из каких элементов состоит массив, но при этом не иметь ни малейшего представления, в каком порядке они расположены.

Далее приводится развернутое описание протокола.

1. **Т** вырабатывает пару ключей RSA $(e,\ d)$, соответствующих модулю n. Открытый ключ $(e,\ n)$ публикуется, а закрытый ключ d сохраняется в тайне.

2. **Т** зашифровывает ключ k по алгоритму RSA и передает его **П**.

$$T: \quad k^e \bmod n \rightarrow П.$$

3. **П** формирует a сообщений $m_1, \ldots, m_a$, удовлетворяющих двум условиям:

a. сообщения произвольны (вероятность их угадывания пренебрежимо мала);

b. сообщения осмысленны (маловероятно, что они не получены в результате некоторых математических преобразований).

4. **П** затемняет зашифрованный ключ k и полученные сообщения при помощи случайного множителя r_n, объединяет их в массив, перемешивает и отсылает **Т**. При желании, k может быть предварительно затемнено множителем r.

$$П: \begin{pmatrix} m_1^e r_n^e \bmod n \\ \cdots \\ m_a^e r_n^e \bmod n \\ k^e r^e r_n^e \bmod n \end{pmatrix} \rightarrow T.$$

5. **Т** расшифровывает каждое из полученных сообщений, тем самым подписывая их «вслепую». Поскольку **Т** не знает порядка расположения сообщений в массиве, он не может определить, в каком из них скрыт ключ k.

$$T: \begin{pmatrix} \cdots \\ m_i r_n \bmod n \\ \cdots \\ krr_n \bmod n \\ \cdots \end{pmatrix}, \quad i \in [1, a\ ].$$

6. **Т** зашифровывает каждое сообщение по схеме Полига—Хеллмана. Для этого **Т** берет большое простое число $\rho > n$ и выбирает произвольное q, взаимно простое с $\rho - 1$. **Т** сообщает ρ своему клиенту.

$$T: \begin{pmatrix} \cdots \\ (m_i r_n \bmod n)^q \bmod p \\ \cdots \\ (krr_n \bmod n)^q \bmod p \\ \cdots \end{pmatrix}, \quad i \in [1, a\ ].$$

7. **Т** производит случайное число $r_m < p$ и затемняет им каждое сообщение. Затем к массиву добавляется r_m, все $a + 2$ сообщения перемешиваются и передаются **П**.

$$T: \begin{pmatrix} \cdots \\ (m_i r_n \bmod n)^q r_m^q \bmod p \\ \cdots \\ (krr_n \bmod n)^q r_m^q \bmod p \\ \cdots \\ r_m \\ \cdots \end{pmatrix} \to П, \quad i \in [1, a\ ].$$

8. **П** находит произвольное s, взаимно простое с $\rho - 1$, и зашифровывает каждое принятое сообщение по схеме Полига—Хеллмана. **П** не в состоянии определить, какое из присланных сообщений — просто случайное число, а потому вынужден их обрабатывать одинаково. Результаты перемешиваются и вместе с r_n отсылаются **Т**.

$$П: \begin{pmatrix} \cdots \\ (m_i r_n \bmod n)^{sq} r_m^{sq} \bmod p \\ \cdots \\ (krr_n \bmod n)^{sq} r_m^{sq} \bmod p \\ \cdots \\ r_m^s \bmod p \\ \cdots \end{pmatrix} \to T, \quad i \in [1, a]; \quad r_n \to T.$$

9. **Т** снимает затемнение со значений, полученных им на шаге 5, и проверяет соответствие $m_1, \ldots, m_a$ указанным ранее требованиям. В частности, **Т** удостоверяется, что эти сообщения с высокой вероятностью не могут быть затемненным ключом:

$\forall\ i \in [1, a]$: *пренебрежимо мала вероятность подобрать такой* x, *что при* $m_i^e \equiv k^e x^e\ (\bmod n)\ m_i$ *осмысленно*

Таким образом, **Т** пресекает мошенничество со стороны **П**, если тот высылает ему фактически одинаковые сообщения $a + 1$ раз. В случае возникновения у **Т** подозрений он может потребовать заменить $m_1, \ldots, m_a$ и начать протокол заново.

10. **Т** просит **П** раскрыть расположение сообщения $r_m^s \bmod p$ в полученном множестве. Если на шаге 7 в отсылаемом массиве сообщение r_m находилось на позиции i, то **Т** просит передать ему номер строки j, на которую переместилась i-я строка в результате перемешивания на шаге 8. Если **П** заинтересован в корректном исполнении протокола, он в точности выполняет просьбу **Т**.

11. Узнав местоположение $r_m^s \bmod p$, **Т** возводит его в степень $-q$ и умножает каждое оставшееся зашифрованное сообщение на $r_m^{-sq} \bmod p$.

$$T: \begin{pmatrix} \cdots \\ (m_i r_n \bmod n)^{sq} r_m^{sq} \bmod p \\ \cdots \\ (krr_n \bmod n)^{sq} r_m^{sq} \bmod p \\ \cdots \end{pmatrix} \cdot r_m^{-sq} \bmod p = \begin{pmatrix} \cdots \\ (m_i r_n \bmod n)^{sq} \bmod p \\ \cdots \\ (krr_n \bmod n)^{sq} \bmod p \\ \cdots \end{pmatrix}, \quad i \in [1, a].$$

12. **Т** находит ключ $q^{-1} \bmod p$ и расшифровывает на этом ключе каждое сообщение. В итоге **Т** получает массив сообщений $\{x\}$, выступающих в качестве товара в фазе 2. **Т** никаким образом не способен определить, в каком именно из x_i скрыт ключ k, однако в том, что в одном из них ключ скрыт, он уверен благодаря шагу 9.

$$T: \begin{pmatrix} \cdots \\ (m_i r_n \bmod n)^s \bmod p \\ \cdots \\ (krr_n \bmod n)^s \bmod p \\ \cdots \end{pmatrix} = \begin{pmatrix} x_1 \\ \cdots \\ x_{a+1} \end{pmatrix}, \quad i \in [1, a].$$

Идея протокола, в общем, прозрачна, так как она уже была пояснена на аналогичном «материальном» примере. Отдельных комментариев заслуживают лишь шаги 7, 10 и 11. Необходимость множителя r_m объясняется тем, что на восьмом шаге **П** мог бы перемножить все полученные сообщения между собой, продублировать произведение $a + 1$ раз и возвести каждую копию в свою степень s_i, выдавая результат за зашифрованные оригинальные сообщения.

$$П: \begin{pmatrix} \left(\prod_{i=1}^{a} (m_i) \cdot krr_n^{a+1} \bmod n\right)^{s_1 q} \bmod p \\ \cdots \\ \left(\prod_{i=1}^{a} (m_i) \cdot krr_n^{a+1} \bmod n\right)^{s_{a+1} q} \bmod p \end{pmatrix} \to T.$$

Т никак не сможет выявить подлог и вернет этот массив **П**, предварительно сняв со всех его элементов степень q. Поскольку **П** знает $m_1, \ldots, m_a, r, r_n, n, \rho$ и a, он сможет извлечь k из любого сообщения, просто перебрав все возможные $s_1, \ldots, s_{a+1}$. Торговля закончится на первом же сообщении.

Компрометация протокола вытекает из свойства мультипликативного гомоморфизма схемы Полига—Хеллмана и направлена против **Т**, а потому он вынужден прибегнуть к дополнительным мерам для обеспечения своей безопасности. Введение вспомогательного множителя при шифровании нарушает гомоморфизм. Пусть **П** подменяет сообщения на зашифрованное произведение всех сообщений, как и раньше.

$$П: \begin{pmatrix} \cdots \\ \left(\prod_{i=1}^{a} (m_i) \cdot krr_n^{a+1} \bmod n\right)^{s_j q} r_m^{(a+1) s_j q} \bmod p \\ \cdots \end{pmatrix} \to T, \quad j \in [1, a+1].$$

Когда на десятом шаге **Т** потребует раскрыть местоположение зашифрованного множителя r_m, **П** не останется ничего другого, кроме как, не вызывая подозрений **Т**, указать на одно из сообщений. Пусть это будет сообщение υ. **Т** выполняет шаги 11 и 12.

$$T: \quad \begin{pmatrix} \cdots \\ \left(\prod_{i=1}^{a}(m_i)\cdot krr_n^{a+1} \bmod n\right)^{s_j - s_\upsilon q} r_m^{(a+1)\left(s_j - s_\upsilon q\right)} \bmod p \\ \cdots \end{pmatrix}, \; j \in [1, a+1].$$

Очевидно, что, с точки зрения **П**, не знающего ни q, ни r_m, любое из этих сообщений — бесполезное псевдослучайное число. Получить из них k — вычислительно трудная задача, требующая дискретного логарифмирования. **П** следует выходить из протокола, потому что покупать такие сообщения бессмысленно. Успешное мошенничество **П** возможно только в том случае, если он сумеет угадать местоположение r_m на шаге 8, но вероятность этого составляет лишь $\frac{1}{a+2}$.

Стоит заметить, что во время всей фазы 1 никаких денег не выплачивается, а потому любая из сторон имеет возможность выйти из протокола без последствий для другой стороны. Если у **Т** (или **П**) возникнут хотя бы малейшие сомнения в честном соблюдении протокола оппонентом, он имеет право отказаться переходить к фазе 2 без объяснения причины и потребовать повторения фазы 1.

Фаза 2

Вторая фаза протокола электронной торговли без посредника итерационна и включает многократно повторяющуюся операцию купли-продажи. **Т** последовательно продает **П** сообщения x, полученные в фазе 1, одно за другим. Обмен сообщениями завершается после того, как **П** завладеет секретным ключом k, с помощью которого сумеет расшифровать ранее принятые данные D.

При каждой итерации **П** расшифровывает очередное принятое сообщение на ключе s^{-1}, после чего снимает свое затемнение множителем r_n. В результате данных преобразований у **П** должно получиться либо m_i для некоторого i, либо $kr \bmod n$. Если же полученный результат не является ни контрольным сообщением, ни секретным ключом, то **П** делает вывод, что имело место нарушение протокола в фазе 1, и реагирует на это соответствующим образом.

В конечном итоге, каждый из участников протокола получает определенную гарантию соблюдения условий сделки другой стороной. За счет трехкратного случайного перемешивания сообщений угадать их взаимный порядок становится практически невозможно, а следовательно, невозможно с достаточной достоверностью угадать, на какой итерации протокол будет завершен. Риск идущего на обман не окупается, и он, в конечном итоге, теряет больше, чем приобретает.

Идея, лежащая в основе первого базового варианта протокола электронной торговли без доверенного лица, проста, но, к сожалению, не способна решить все возникающие проблемы. В частности, нерешенной остается проблема «кота в мешке». Действительно, на втором шаге фазы 1 **Т** способен подменить ключ k любым случайным числом, и **П** ни о чем бы не догадался до самого конца протокола. В связи с этим данный вариант протокола может безопасно использоваться только в том случае, если **П** уверен, что на шаге 4 он имеет дело именно с ключом шифрования, а не с подделкой.

Рассмотрим второй вариант протокола. Модифицируем первый вариант, чтобы позволить покупателю заблаговременно выявлять подлог со стороны продавца. Заметим, что изначально **П** находится в более уязвимом положении, чем **Т**. Продавец может прекратить торговлю в любой момент, присвоив часть денег и нанеся покупателю невосполнимый урон. Это обусловлено тем, что в процессе купли-продажи сообщений **П** передает **Т** реальные ценности (деньги), а в ответ получает лишь шанс приобретения всего товара сразу. На промежуточных стадиях протокола возникает ситуация, когда траты **П** ничем не компенсированы. Для устранения сложившейся несправедливости необходимо ввести дополнительное условие, касающееся электронного товара D:

Пусть $\exists\ n > 1:\quad D = D_1 \cup D_2 \cup \ldots \cup D_n,\quad$ *где* $\forall\ i \in [1, n]$*:*
D_i *имеет самостоятельную ценность и служит показателем целостности* D*.*

Проще всего пояснить данное условие на примере. Пусть электронный товар D — это видеофайл. Любой видеофайл всегда может быть разбит на n фрагментов (где n не больше числа опорных кадров), причем каждый фрагмент будет являться самостоятельной функционирующей видеозаписью. Просмотрев любой фрагмент, можно получить некоторое представление о фильме в целом или, по крайней мере, убедиться в том, что это действительно часть какого-то фильма. Каждый фрагмент следует снабдить указанием его порядкового номера в целях облегчения последующей сборки цельного файла с фильмом по частям.

Суть взаимодействия продавца и покупателя остается такой же, как и в предыдущем варианте. Различие заключается в том, что в начале протокола **Т** разбивает свой товар (фильм F) на b частей, зашифровывает каждую часть на собственном случайном ключе k_i и передает все b криптограмм **П**:

$$T: \begin{pmatrix} E_{k_1}(F_1) \\ \cdots \\ E_{k_b}(F_b) \end{pmatrix} \to П.$$

Теперь в фазе 1 на шаге 2 **Т** отсылает **П** не один, а сразу все зашифрованные ключи:

$$T: \begin{pmatrix} k_1^e \bmod n \\ \cdots \\ k_b^e \bmod n \end{pmatrix} \to П.$$

В дальнейшем протокол не претерпевает никаких изменений вплоть до начала фазы 2, когда на руках у **Т** окажутся $a + b$ затемненных сообщений, причем он не будет знать, какое из них содержит один из ключей, а какое — контрольную строку. Несмотря на это, как и раньше, **Т** будет убежден, что в итоговом массиве присутствуют все его секретные ключи шифрования и a произвольно выбранных контрольных сообщений.

Вторая фаза в новом варианте протокола, хотя внешне и не меняется, имеет ряд существенных качественных отличий. Если раньше в планы **П** входил выкуп единственного нужного ему пакета, содержащего ключ k, то теперь его целью становится приобретение b секретных ключей из всего множества сообщений. Ни **П**, ни **Т** не знают, в каком порядке расположены все $a + b$ элементов массива, а потому **П** будет принимать ключи в случайной последовательности. При этом, как и в предыдущем варианте, полезные для **П** пакеты будут перемежаться с контрольными сообщениями m_i, гарантирующими честность **Т**.

При первой же итерации вероятность покупки одного из секретных ключей составит $\frac{b}{a+b}$, что больше вероятности выкупа ключа в том случае, если бы он был единственным. Следовательно, в целом, в данном варианте протокола **П** получит хотя бы один ключ быстрее (за меньшее число итераций), чем единственный ключ в предыдущем варианте. Это значит, что если **Т** попытается сжульничать и вместо какого-либо из зашифрованных фрагментов F подсунет мусор или выдаст неверные ключи, то этот обман раскроется намного раньше. Поскольку **П** прекращает торговлю сразу же после обнаружения мошенничества, его риск потратить деньги впустую уменьшается, как и прибыль недобросовестного торговца.

У этого особого свойства данного протокола есть и положительный аспект, которому можно найти практическое применение. Суть здесь в том, что еще до начала торгов продавцу предоставляется возможность доказать подлинность своего товара, не жертвуя при этом частью прибыли. После получения b зашифрованных фрагментов фильма **П** следует произвольно выбрать

из них несколько и попросить выдать ему ключи шифрования для этих фрагментов. Продавец не способен заранее предугадать, какие именно фрагменты захочет проверить покупатель, а потому будет вынужден подготовить все части фильма в полном соответствии с протоколом и честно раскрыть требуемые ключи. Расшифровав выбранные части и ознакомившись с их содержимым, покупатель сможет точно убедиться в добропорядочности **Т** и окончательно утвердиться в намерении с ним торговать.

Казалось бы, подобное дополнительное нововведение совершается полностью в интересах **П**, снимая проблему «кота в мешке» за счет бескорыстной жертвы со стороны **Т**. На самом деле, это не так. За все фрагменты, полученные безвозмездно перед началом протокола, покупатель все равно будет вынужден заплатить с большой вероятностью, поскольку он не решает, в каком порядке какие части покупать. Во второй фазе будут фигурировать все затемненные и перемешанные между собой фрагменты вне зависимости от того, были ли они уже раскрыты или нет.

Единственный существенный фактор риска, на который **Т** следует обратить внимание, — это соблюдение оптимального соотношения между раскрываемыми и скрытыми фрагментами. Если для **П** будет раскрыто слишком много, то он может и вовсе отказаться торговать, довольствуясь бесплатно принятыми данными. В такой ситуации вместо удачной рекламы своего товара **Т** получит одни убытки.

В первом варианте протокола, очевидно, всю полезную секретную информацию составляет единственный пакет с ключом шифрования, и для окончания торгов достаточно выкупить именно одно это сообщение. Во втором варианте все несколько сложнее. Предварительно рассмотрим наиболее простой случай, когда **П** обязательно требуются все части секрета D. Покупатель продолжает покупать зашифрованные сообщения, пока некупленым остается хотя бы один фрагмент.

Пусть имеется конечная совокупность, состоящая из $a + b$ элементов, причем b из них обладают некоторым особым свойством. Оставшиеся a элементов таким свойством не обладают. Случайным образом из общей совокупности выбирается группа из n элементов. Требуется найти вероятность того, что из всех выбранных элементов только k будут обладать особым свойством.

Эта задача соответствует проблеме нахождения прибыли **Т** и была известна математикам уже достаточно давно. Вероятность присутствия k особых элементов в выборке из n элементов определяется по формуле

$$P(k) = f(k;\, a+b,\, b,\, n) = \frac{C_b^k \cdot C_a^{n-k}}{C_{a+b}^n},$$

которая носит название *гипергеометрического распределения* вероятностей. На рис. 1 приведены два графика, отражающих вероятную длительность второй фазы для двух описанных вариантов протокола электронной торговли. Для первого варианта протокола все множество сообщений, участвующих в торгах, состоит из одного секретного ключа и 999 контрольных пакетов ($a = 999$). Во втором варианте фигурируют 900 контрольных сообщений ($a = 900$) и 100 индивидуальных ключей шифрования ($b = 100$) от фрагментов секрета D. Очевидно, что первый вариант протокола является частным случаем второго при $b = 1$, а потому графики функций распределения для обоих вариантов могут быть получены одинаковыми методами, изображены на общей координатной сетке и сопоставлены друг с другом.

На графике представлен тот случай, когда для выхода из протокола покупателю требуется выкупить все 100 фрагментов товара. В соответствии с графиком функции гипергеометрического распределения при любом практически осуществимом числе повторений протокола количество проданных сообщений будет лежать в пределах от 950 до 1000. Менее 950 сообщений будет продано меньше, чем в 1 % случаев. Таким образом, во втором варианте протокола по сравнению с первым средняя выручка продавца в несколько раз выше, а риск — в несколько раз меньше.

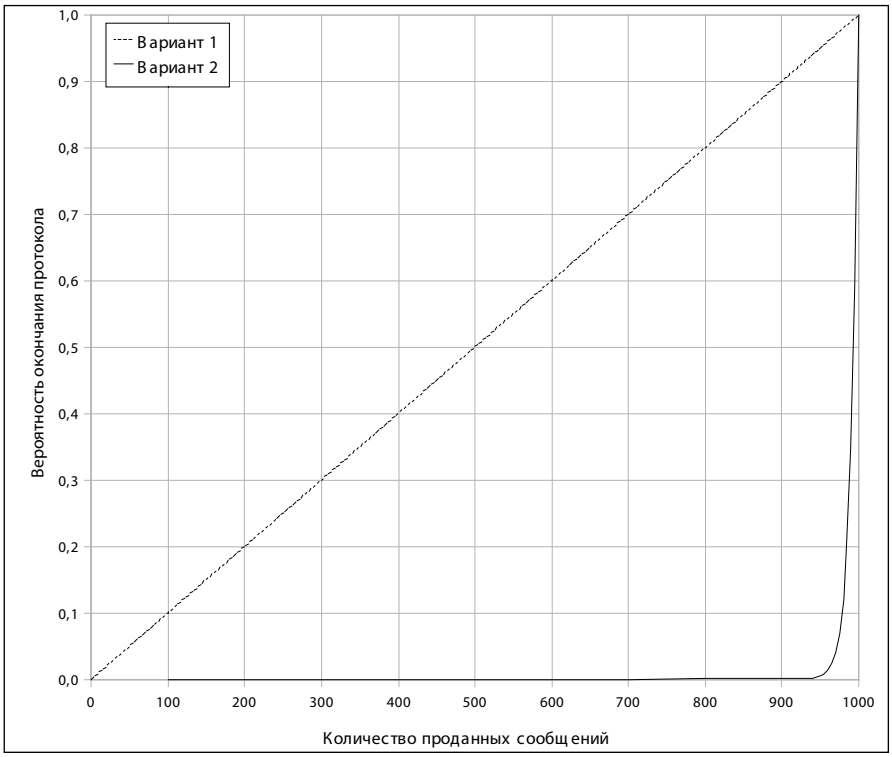

Рис. 1. Графики функции распределения вероятности продолжительности протокола

Остается рассмотреть ситуацию, при которой **П** может остановить вторую фазу протокола до того, как получит все фрагменты D. Допустим, на некоторой итерации покупатель посчитает, что тех частей секрета, которые он уже успел получить, вполне достаточно и оставшиеся части не представляют особого интереса. К сожалению, в общем случае очень трудно заранее предусмотреть, какую долю принятых фрагментов **П** посчитает достаточной. Это слишком сильно зависит от вида товара и удачи покупателя. Например, при торговле видеофайлами следует учитывать, что около 5 % продолжительности среднего фильма занимают завершающие титры, которыми зритель может пренебречь. Следовательно, если покупателю повезет и после выкупа 95 % фрагментов окажется, что зашифрованными остаются только титры, то можно ожидать, что он выйдет из протокола.

С таким же успехом можно учесть, что в любом фильме есть фрагменты, более или менее интересные с точки зрения разных покупателей, и тогда точное предсказание достаточного числа проданных сообщений и вовсе становится невозможным. Предположим, что в большинстве случаев для завершения протокола покупателю будет достаточно расшифровать 90 % произвольно расположенных частей товара. Это условие гораздо мягче требования покупки всех 100 % фрагментов и, безусловно, сильно влияет на вид графика функции распределения.

Согласно графику, представленному на рис. 2, в подавляющем большинстве прогонов протокола продавец продаст от 800 до 950 сообщений. Несмотря на то что с учетом достаточности 90 % фрагментов результат ухудшается, он все равно намного лучше, чем достигаемый в первом варианте протокола.

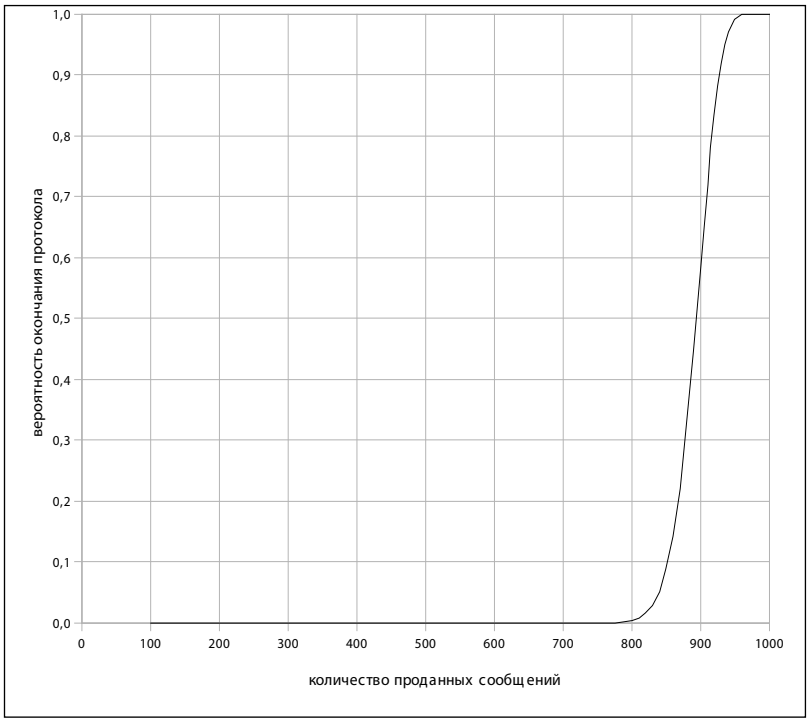

Рис. 2. График распределения вероятности продолжительности второй фазы во втором варианте протокола при достаточности раскрытия 90 % фрагментов

Заключение

Рассмотрены два варианта криптографического протокола, различающиеся по сложности, но объединенные общим оригинальным подходом к решению актуальных проблем товарно-денежного обмена. Отличительной чертой предлагаемых решений является применение стохастических методов защиты интересов как продавца, так и покупателя. При этом прибыль и риски обоих участников носят недетерминированный характер. Представленная математическая реализация выдвинутых идей обеспечивает криптографическую стойкость и позволяет управлять вероятностными параметрами протокола.

СПИСОК ЛИТЕРАТУРЫ:

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Издательство ТРИУМФ, 2002.
2. *Chi E.* Evaluation of Micropayment Schemes // HP Laboratories Technical Report. № 97-14. 1997. P. 1–29.
3. *Pedersen T. P.* Electronic Payments of Small Amounts // Security Protocols Workshop / Ed. by T. M. Lomas. Vol. 1189 of LNCS. Springer, 1996. P. 59–68.
4. *Rivest R. L., Shamir A.* PayWord and MicroMint: two simple micropayment schemes // CryptoBytes. 1996. P. 69–87.
5. *Lipton R. J., Ostrovsky R.* Micro-Payments via Efficient Coin-Flipping (Extended Abstract). 1996.
6. *Rivest R. L.* Electronic lottery tickets as micropayments // Financial Cryptography. Springer Verlag, 1997. P. 307–314.