УДК 519.24

ЭФФЕКТИВНЫЕ ПРОТОКОЛЫ ПЕРЕДАЧИ КОМБИНАЦИИ СООБЩЕНИЙ С ЗАБЫВАНИЕМ

А.Б. Фролов

Рассматриваются эффективные интерактивные и неинтерактивные протоколы передачи комбинации m из n сообщений с забыванием, в которых применяется вероятностное шифрование. Использование в последовательных актах вероятностного шифрования различных ключей получателя позволяет применять единственный рандомизатор. При этом возрастает в 2n/(n+1) раз информационная скорость передачи и уменьшается вычислительная сложность на втором раунде интерактивных или на коммуникационной фазе неинтерактивных протоколов. Предложенные решения потенциально применимы во всех протоколах, основанных на передаче с забыванием с использованием вероятностного шифрования, в частности в электронной коммерции

Ключевые слова: передача с забыванием, криптосистема Эль Гамаля, вероятностное шифрование, рандомизатор, информационная скорость передачи данных, сложность вычислений, эллиптическая кривая, полиномиальная схема Беллара – Райвеста

Введение

Понятие передачи с забыванием (OT ― oblivious transfer) было введено М. Рабиным [1] в связи с изучение проблемы обмена секретами, изучавшейся М. Блюмом [2]. В простейшем варианте передачи с забыванием с вероятностью ½ передается одни бит. По соответствующему протоколу (1/2OT-протоколу) отправитель посылает сообщение получателю таким образом, что последний прочитает его с вероятностью ½, при этом отправитель не будет знать, получено ли его сообщение. В работе [3] с использованием вероятностного шифрования по схеме Эль-Гамаля [4] описан протокол передачи одного из двух сообщений с забыванием (1 из 2 OT-протокол). По нему отправитель посылает два сообщения таким образом, что получатель по своему выбору читает только одно из них, при этом отправитель остается в неведении, какое из двух сообщение было получено. Синонимами передачи с забыванием являются «скрытая передача» [5] и «забывающая передача» [6].

Наиболее существенным последующим шагом было создание М. Белларом и Р. Райвестом теории дробной передачи с забыванием и обоснование интерактивных и не интерактивных *m/n* OT-протоколов, по которым отправитель посылает сообщение таким образом, что получатель прочитает его с вероятностью *m/n* [7]. При этом отправитель не узнает, прочитано ли сообщение. *1/n* и *(n–1)/n* OT-протоколы Беллара – Райвеста являются обобщениями ½ OT-протокола, а *m/n* OT-протоколы построены по оригинальной полиномиальной схеме.

В работе [8] указанная схема применена для вычисления ключевой информации протоколов передачи *m* из *n* сообщений с забыванием. По таким протоколам отправитель *A* посылает *n* сообщений, из которых получатель B читает по своему выбору только m, при этом *A* не знает, какая именно комбинация *m* из *n* сообщений получена.

В [9] на основе другой матричной схемы описаны протоколы передачи *m* из *n* с забыванием, многократно использующие протокол цифровой подписи с возвратом сообщения [10].

В работе [11] понятие передачи с забыванием обобщено как понятие обобщенной передачи с забыванием (GOT – generalized oblivious transfer). В GOT-протоколах ограничение доступа описывается в виде монотонно убывающей совокупности подмножеств исходного множества сообщений **U**. По таким протоколам отправитель *A* посылает все сообщения из множества **U** таким образом, что получатель B читает все сообщения одного из доступных ему подмножеств, при этом отправителю не известно, сообщения какого именно подмножества прочитаны.

В [12] описаны GOT-протоколы, в которых многократно используются протоколы передачи комбинации *m* из *n* сообщений.

OT-протоколы, рассматриваемые ниже, включают глобальную установочную фазу, в которой объявляются группа *G* высокого простого порядка *q* с трудными проблемами Диффи ― Хеллмана (ДХП) и дискретного логарифма (ДЛП), образующий элемент *b* этой группы и ее элемент *U* с неизвестным обоим участникам дискретным логарифмом $\log_b U$.

Интерактивные протоколы (OT-протоколы) включают *фазу первого раунда вычисления публичного ключа получателя и верифицируемой его доставки отправителю и фазу второго раунда передачи с забыванием m* из *n* сообщений отправителем получателю.

В не интерактивных протоколах (NIOT-протоколах) вместо фазы первого раунда имеется *фаза вычисления публичного ключа получателя и его сертифицированной доставки в доверенный центр с последующей публикацией*. Функции фазы второго раунда осуществляются *в фазе коммуникации*. Ниже эти фазы обобщенно называются коммуникационной фазой.

В коммуникационной фазе OT- и NIOT-протокола осуществляется *n* актов шифрования по схеме Эль-Гамаля или создания *n* цифровых подписей с возвратом сообщения [9,10]. В каждом акте создается и используется новый рандомизатор. В общем случае вероятностного шифрования повторное использование рандомизатора чревато раскрытием передаваемой информации или даже секретного ключа получателя. Такое случается при многократном использовании публичного ключа получателя. Но в пределах одного исполнения OT-протокола применяются разные ключи получателя и повторное использование рандомизатора оказывается безопасным. Как следствие сокращается время, затрачиваемое отправителем на вычисление рандомизаторов и возведение образующего элемента в соответствующие степени для вычисления сеансовых ключей. Более того, возрастает информационная скорость передачи в фазе коммуникации за счет сокращения передаваемых сеансовых ключей. Тем самым повышается эффективность исполнения протоколов.

Ниже используются следующие обозначения. OT-протокол — это традиционный интерактивный протокол передачи с забыванием, EOT-протокол — это эффективный (вследствие повторных использований рандомизатора) OT-протокол. NIOT- и ENIOT-протоколы — это соответствующие не интерактивные протоколы. SUNIOT- и SUENIOT-протоколы — это NIOT- и ENIOT-протоколы однократного использования.

В настоящей работе дробные *m/n* OT-протоколы [7] преобразованы в *m* из *n* EOT-протоколы. При этом оценивается степень упрощения последних вследствие обоснованного повторного использования рандомизаторов.

Пусть e_{OT} это число элементов группы *G*, передаваемых в коммуникационных фазах при исполнении традиционного OT-протокола, а e_{EOT} — число элементов, передаваемых в этих фазах при исполнении упрощенного (эффективного) EOT-протокола.

Тогда дробь $\rho_{\mathrm{EOT}} = \dfrac{e_{\mathrm{OT}}}{e_{\mathrm{EOT}}}$ выражает возрастание информационной скорости передачи в этих фазах и сокращение сложности вычислений в них, так как числитель и знаменатель характеризуют количества возведений в степень элементов группы *G*. Информационная скорость и вычислительная сложность фазы первого раунда, как и фазы вычисления публичного ключа получателя не изменяются.

Протоколы описываются в терминах мультипликативной группы простого высокого порядка. Мы также полагаем, что предаваемые сообщения представляются как элементы группы *G*. Описания легко трансформируются применительно к использованию операций аддитивной группы с заменой умножений сложениями, а возведений в степень скалярными умножениями. Пример реализации *m* из *n* EOT протокола на несуперсингулярной эллиптической высокого порядка (т. е. в аддитивной группе) приведен в работе [13].

Передача одного из n сообщений

1 из *n* OT- и NIOT-протоколы можно построить на основе ключевой информации дробного *1/n* OT-протокола [7]. Процедура вычисления публичного ключа получателя состоит в следующем: получатель В выбирает случайным образом секретный ключ *(x,i), 0<x<q-1, i∈{0,1,…, n−1},* где *i* есть индекс выбранного им сообщения m_i, вычисляет $\beta_i = b^x$ и $\beta_j=\beta+U^{j-i}$ для $j\neq i$. Публичный ключ получателя есть $(\beta_0, \beta_1,\ldots, \beta_{n-1})$. Получатель ***B*** знает дискретный логарифм $x=x_i$ только элемента β_i и не обладает никакой информацией о дискретных логарифмах $\log_b\beta_j$, $j\neq i$. Проверочная процедура, выполняемая отправителем ***A*** или доверенным центром ***T*** состоит в верификации предикатов $\beta_j = \beta_0 U_j$ для всех $j=0,\ldots, n-1$.

В коммуникационных фазах 1 из *n* OT- или NIOT-протоколов ***A*** выбирает случайно число 0<y<q, вычисляет и посылает к ***B*** элемент $c=b^y$ и набор элементов группы *G*

$(\alpha 0,\alpha 1,\ldots,\alpha n-1)=(m_0\beta_0^{\,y}, m_1\beta_1^{\,y},\ldots, m_{n-1}\beta_{n-1}^{\,y})$..

Эта информации соответствует n криптограммам по схеме Эль-Гамаля

$(b^y, m_j\beta_j{}^y)$, *j=0,…,n− 1.*

B вычисляет

$$\alpha_i c^{-x} = \alpha_i b^{-yx} = m_i \beta_i^y b^{-yx} =$$
$$= m_i \beta_i^y \beta_i^{-y} = m_i.$$

Утверждение 1. Многократное использование рандомизатора *y* в 1 из *n* OT- и NOT-протоколах безопасно. Проблема извлечения получателем второго сообщения эквивалентна проблеме Диффи – Хеллмана.

Доказательство. Заметим, что знание b^y и $b^{x_j} = \beta_j,\ j \neq i$ недостаточно для вычисления $\beta_j{}^y = b^{x_j y}$, так как для этого требуется решить проблему Диффи ─ Хеллмана или проблему дискретного логарифма. Знание m_i, не позволяет вычислить m_j, так как для вычисления β_i и β_j использованы различные секретные ключи x_i x_j криптосистемы Эль-Гамаля. Таким образом, B не в состоянии вычислить m_j и рандомизатор *y* можно использовать многократно в отдельной сессии 1 из *n* OT- и NIOT-протокола: отправитель A может быть уверен, что будет получено лишь одно сообщение. Получатель, сохраняя в секрете *x* и *i*, по-прежнему (как и в случае использования различных рандомизаторов) может полагать, что ***A*** не может различить, каким из n элементов является элемент β_1.

В этой ситуации получателю ***B*** известны элементы x_i, b, $\beta_i = b^{x_i}$, $c = b^y$, $\beta_j = b^{x_j}$, $m_i\beta_i^y = m_i b^{x_i y}$, $m_j\beta_j^y = m_j b^{x_j y}$ и U. Пусть известен алгоритм B1 вычисления m_j в этих условиях. Тогда он позволит решить проблему Диффи ─ Хеллмана: даны b, b^y, b^x, найти b^{xy}. Решение следующее: взять произвольное число *z, 1<z<q*, $b^z \neq b^x$, положить $\beta_0 = b^x$, вычислить $\beta_1 = b^z$, $U = b^z / b^x$, взять произвольные ненулевые элементы d_0 and d_1, $1<d_0, d_1<q$, группы *G*, полагая, что $d_0 = m_0\,\beta_0{}^y = m_0\,b^{x\,y}$, $d_1 = m_1\beta_1{}^y$. Далее, используя b^y и применяя алгоритм B1, можно получить m_1 и далее вычислить $\beta_1{}^y = = b^{xy}$. С другой стороны, если можно вычислить $\beta_j{}^y = b^{xy}$, то можно вычислить и *m*. Таким образом, проблема извлечения второго сообщения и проблема Диффи ─ Хеллмана эквивалентны.

Следствие 1. Имеют место оценки

$\rho_{1\ out\ of\ n\ EOT} = \rho_{1\ out\ of\ n\ ENIOT} = 2n/(n+1)$

и

$\rho_{1\ out\ of\ n\ SUENIOT} = 2$.

Передача n─1 из n сообщений

n ─1 из *n* OT- и NIOT-протоколы можно построить на основе ключевой информации дробного *(n─1)/n* OT-протокола [7]. Процедура вычисления публичного ключа получателя состоит в следующем: получатель B выбирает случайным образом *n* различных чисел $x_1, x_2, \ldots, x_n$ таких, что $0<x_i<q$, $i \in \{1,\ldots,n\}$, $x_1+x_2+\ldots\ \ldots+x_n = q$, и перестановку π на множестве *{1,…, n}* такую, что $\pi(i) = j_i$, $i=1,\ldots,n-1$, где j_i суть индексы выбранных сообщений m_{j_i}, вычисляет

$$\beta_{\pi(i)} = b^{x_i},\ i = 1,\ldots,n-1,\ \beta_{\pi(n)} = Ub^{x_n}.$$

Публичный ключ получателя есть $(\beta_1, \beta_2, \ldots, \beta_n)$. получатель ***B*** знает дискретные логарифмы x_i элементов $\beta_{\pi(i)} = \beta_{j_i}$, $i=1,\ldots,n-1$, и не имеет никакой информации о $log_b\beta_{\pi(n)}$. проверочная процедура, выполняемая отправителем ***A*** или доверенным центром ***T,*** заключается в верификации предиката $\Pi_{i=1}^n \beta_i = U$.

В коммуникационных фазах *n─1* из *n* OT- и NIOT-протоколов ***A*** выбирает случайно число $0<y<q$, вычисляет и посылает к ***B*** элемент $c = b^y$ и набор из *n* элементов группы *G*

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) = (m_1\beta_1{}^y, m_2\beta_2{}^y, \ldots, m_n\beta_n{}^y).$$

Эта информации соответствует n криптограммам по схеме Эль-Гамаля

$$(b^y, m_i\beta_i{}^y),\ i=1,\ldots,n.$$

Для i =1,…, n−1, B вычисляет

$$\alpha_{\pi(i)}c^{-x_i} = \alpha_{\pi(i)}b^{-yx_i} = m_{\pi(i)}\beta_{\pi(i)\,j}^y b^{-yx_i} =$$
$$= m_{\pi(i)}\beta_{\pi(i)}^y\beta_{\pi(i)}^{-y} = m_{\pi(i)} = m_{j_i}.$$

Утверждение 2. Многократное использование рандомизатора y в n−1 из n OT и NOT протоколах безопасно. Проблема извлечения получателем n-го сообщения эквивалентна проблеме Диффи – Хеллмана.

Доказательство. Обратим внимание, что знание b^y и $b^x = \beta_{\pi(n)}$, недостаточно для вычисления $\beta_{\pi(n)}{}^y = b^{xy}$, так как для этого требуется решить проблему Диффи ─ Хеллмана или проблему дискретного логарифма. Дополнительное знание всех сообщений $m_{\pi(i)}$, $i \neq n$ не позволит вычислить $m_{\pi(n)}$, так как для вычисления $\beta_{\pi(i)}$ и $\beta_{\pi(n)}$ были ис-

пользованы различные секретные ключи x_i и х криптосистемы Эль Гамаля. Таким образом, повторное использование рандомизатора в отдельной сессии *n−1* из *n* OT-и NIOT-протоколов безопасно для отправителя: А может быть уверен, что получено только *n−1* сообщений. В то же время получатель, сохраняя в секрете *(x1, x2,…, x_{n-1})* и π, попрежнему (как и в случае использования различных рандомизаторов) может полагать, что А не может различить, каким из *n* элементов является элемент $\beta_{\pi(n)}$.

В этой ситуации, для *i= 1,2,…, n−1* известны элементы x_i, $b, d_{\pi(i)} = m_{\pi(i)}\beta_{\pi(i)}^{y}$, $\beta\pi(i)= b^{x_i}$, $c=b^{y}$, $\beta\pi(n)=b^{x}$, и *U*. Пусть известен алгоритм B2 вычисления $m_{\pi(n)}$ в этих условиях. Тогда он позволит решить проблему Диффи ─ Хеллмана: даны $b, b^{y}, b^{x,}$ найти b^{xy}. Решение следующее: взять произвольные различные числа $x_1, x_2,\ldots,x_{n-1}$ такие, что $0<xi<q$, для *i=1,…, n−1*, вычислить $\beta_i^{y}= (b^{y})^{x_i} = b^{x_i y}$, $U=b^{x}\Pi_{i=1}^{n-1}\beta_i$. Отсюда $\beta_n = b^{x} = Ub^{x_n}$, $x_1+x_2+\ldots+x_n-1+ x_n =q$. Затем выбрать различные элементы $d_1,\ldots,d_{n-1},d_n$, полагая, что для $i=1,\ldots,n$ $1<d_i<q$, $d_i=m_i\beta_i^{y}$. Далее, применив алгоритм B2, с использованием b^{y} можно вычислить m_n и далее $\beta_n^{y} = b^{xy}$. С другой стороны, если получатель может вычислить $\beta_{\pi(n)}{}^{y}=b^{xy}$, то он вычислит и $m_{\pi(n)}$. Таким образом, проблема извлечения *n*-го сообщения и проблема Диффи ─ Хеллмана эквивалентны.

Следствие 2. Имеют место оценки

$\rho_{n-1 \text{ out of } n \text{ EOT}} = =\rho_{n-1 \text{ out of } n \text{ ENIOT}}=2n/(n+1)$, и $\rho_{n-1 \text{ out of } n \text{ SUENIOT}}=2$.

Передача *m* из *n* сообщений

Глобальная установочная фаза этих протоколов пополняется фиксацией $\alpha_0=1\in Z_q$, и *n* различных элементов $\alpha_1,\ldots, \alpha_n$ из множества $Zq\backslash\{\alpha_0\}$. Все эти элементы публикуются.

m из *n* OT- и NIOT-протоколы можно построить на основе ключевой информации дробного *m/n* OT-протокола [7].

Процедура вычисления публичного ключа получателя следующая.

Публичным ключом получателя является вектор $(\beta_1, \beta_2,\ldots, \beta_n, W_0, W_1,\ldots, W_m)\in G^{n+m+1}$.

Для его вычисления получатель ***B*** выбирает случайно *m*-подмножество множества $[n]=\{1,2,\ldots,n\}$, определяя там самым инъективное отображение $\pi:[m]\to[n]$, где $\pi(1),\ldots, \pi(m)$ суть *m* выбранных индексов. Далее он выбирает случайные элементы $x_{\pi\{1\}},\ldots, x_{\pi(m)}\in Z_n$ и вычисляет $\beta_{\pi(i)}=b^{x_{\pi(i)}}\in G$ для $i=1,\ldots,m$. Тем самым определяются *m* элементов из $\beta_1, \beta_2,\ldots\ldots, \beta_n$ таким образом, что получатель ***B*** знает их дискретные логарифмы. Другие *n−m* элементы необходимо задать так, чтобы ***B*** не знал и не мог бы вычислить их дискретные логарифмы. Для этого сначала ***B*** вычисляет элементы $W_0, W_0, W_1,\ldots, W_m$ следующим образом.

Он берет *m+1* на *m+1* матрицу Вандермонда над полем Z_q, $j=0,\ldots,m$, $A = (\alpha_{\pi(j)}^{j})$.

и вычисляет обратную к ней матрицу

$B = A^{-1} = (\beta_{i,j})$, $i=0,\ldots,m$, $j=0,\ldots,m$.

Далее ***B*** вычисляет

$$W_j = U^{\beta_{j,0}}\cdot\Pi_{i=1}^{m}\beta_{\pi(i)}^{\beta_{j,1}},\ j=0,\ldots,m$$

Наконец, ***B*** определяет недостающие элементы открытого ключа: $\beta_i = \Pi_{j=0}^{m}W_j^{\alpha_i^{j}}$ для всех $i\in[m]$ вне области значений отображения π.

Проверочная процедура, выполняемая отправителем или доверенным центром следующая.

Проверить, что публичный ключ состоит из *m+n+1* элементов группы *G*;

Удостоверить предикаты

$$U = \Pi_{j=0}^{m}W_j;\ \beta_i = \Pi_{j=0}^{m}W_j^{\alpha_i^{j}}$$

для всех $i=1,\ldots,n$.

В коммуникационных фазах *m* из *n* OT- и NIOT-протоколов ***A*** выбирает случайно число $0<y<q$, вычисляет и отсылает к ***B*** элемент $c=b^{y}$ и набор из *n* элементов группы *G*

$$(\alpha_1,\alpha_2,\ldots,\alpha_n)=(m_1\beta_1{}^{y}, m_2\beta_2{}^{y},\ldots, m_n\beta_n{}^{y}).$$

Эта информации соответствует n криптограммам по схеме Эль-Гамаля

$(b^{y}, m_i\beta_i{}^{y})$, $i,j=1,\ldots,n$. Для $i=1,\ldots,m$ ***B*** вычисляет

$$\alpha_{\pi(i)}c^{-x_{\pi(i)}} = \alpha_{\pi(i)}b^{-yx_{(i)}} = m_{\pi(i)}\beta_{\pi(i)j}^{y}b^{-yx_{(i)}} =$$

$$= m_{\pi(i)}\beta_{\pi(i)}^{y}\beta_{\pi(i)}^{-y} = m_{\pi(i)} = m_{j_i}.$$

Утверждение 3. Многократное использование рандомизатора *y* в *m* из *n* OT- и NOT-протоколах безопасно.

Доказательство. Заметим, что знание b^y и $b^{x_i} = \beta_i$, где *i* вне области значений π, недостаточно для вычисления $\beta_i{}^y = b^{x_i y}$, так как для этого требуется решить проблему Диффи ─ Хеллмана или проблему дискретного логарифма. Дополнительное знание всех сообщений $m_{\pi(i)}$, не позволит вычислить m_i, так как при вычислении $\beta_{\pi(i)}$ и β_i использованы различные секретные ключи $x_{\pi(i)}$ и x_i криптосистемы Эль-Гамаля. Таким образом, повторное использование рандомизатора в отдельной сессии *m* из *n* OT и NIOT-протоколов безопасно для отправителя: ***A*** может быть уверен, что получены только *m* сообщений. Получатель, сохраняя в секрете $(x_1, x_2, \ldots, x_{m-1}, x_m)$ и π, по-прежнему (как и при использовании различных рандомизаторов) может полагать, что ***A*** не может отличить, какими из *n* элементов являются элементы $\beta_{\pi(l,)}$. $i=1,\ldots,m$.

Следствие 3. Имеют место оценки:
$\rho_{m \text{ out of } n \text{ EOT}} = \rho_{m \text{ out of } n \text{ ENIOT}} = 2n/(n+1)$, и
$\rho_{m \text{ out of } n \text{ SUENIOT}} = 2$.

Заключение

В статье представлены новые эффективные интерактивные и неинтерактивные протоколы передачи комбинации *m* из *n* сообщений с забыванием (OT-протоколы), в которых используется вероятностное шифрование. Ключевая информация этих протоколов формируется как в протоколах дробной передачи с забыванием Беллара ─ Райвеста, а шифрование осуществляется по схеме Эль-Гамаля. Протоколы могут быть реализованы в подгруппе мультипликативной группы конечного поля или (аддитивной) группы точек эллиптической кривой. Порядок такой подгруппы должен быть большим простым числом. Показано, что вследствие использования различных секретных ключей получателя в различных актах шифрования в пределах одного сеанса передачи с забыванием возможно и безопасно использование одного и того же рандомизатора. Данное решение позволяет увеличить в $2n/(n+1)$ раз информационную скорость коммуникационных фаз протоколов и уменьшить в $2n/(n+1)$ раз сложность вычислений отправителя на этих фазах. Эти предложения применимы во всех криптографических протоколах, в которых используется передача комбинаций *m* из *n* сообщений с забыванием с использованием вероятностного шифрования, включая обобщенные протоколы передачи с забыванием. Исследование выполнено при финансовой поддержке РФФИ, проект № 11-01-00792-а.

СПИСОК ЛИТЕРАТУРЫ

1. Rabin, M. How to exchange secrets by oblivious transfer/ M. Rabin, - Technical Report TR-81, Aiken Computation Laboratory, Harvard University, 1981 − 26 с.
2. Blum, M. How to exchange (secret) keys/ M. Blum - Trans. Computer Systems – 1, 1983 − P.175 − 193.
3. Even, S. Randomized Protocol for Signing Contracts/ S. Even, O. Goldreich, A. Lemel - Communications of the ACM, Volume 28, Issue 6, 1985 − P. 637−647.
4. ElGamal, T. A public-key cryptosystem and a signature scheme based on discrete logarithms/ T. ElGamal - IEEE Trans. Inform. Theory, IT-31(4), 1985 − P. 469−472.
5. Коблиц, Н. Курс теории чисел и криптография/ Н. Коблиц − М. : ТВП, 2001 − 260 с.
6. Саломаа, А. Криптография с открытым ключом/ А. Саломаа − М. : Мир, 1996 − 319 с.
7. Bellare, M. Translucent cryptography – An Alternative to Key Escrow, and its Implementation via Fractional Oblivious Transfer/ M.Bellare, R. Rivest - MIT/LCS Technical Report 683, 1990 − 20 с.
8. Мамонтов, А. Об одной схеме передачи комбинации сообщений с забыванием/ А.И. Мамонтов, А.Б. Фролов// Вестник МЭИ. №3, 2005. – С. 113—119.
9. Mu, Y. m out of n Oblivious Transfer/ Yi Mu, Yi Junqi Zhang, Vijay Varandharajan// In Proceedings of ACISP'2002 − P. 395−405.
10. Nyberg, K. A New Signature Scheme Based on the DSA Giving Message Recovery/ K. Nyberg, R. Rueppel - 1st ACM Conference on Computer and Communications Security − Fairfax. Virginia, 1993 − P. 58−61.
11. Ishai, Y. Private simultaneous messages protocols with applications/ Y. Ishai, E. Kushilevitz - Proc. of ISTCS97, IEEE Computer Society, 1997 − P. 174−184.
12. Tassa, T. Generalized oblivious transfer by secret sharing/ Tamir Tassa - Designs, Codes and Cryptography, Volume 58:1, 2011 − P. 11−21.
13. Frolov, A. Effective Oblivious Transfer Using Probabilistic Encryption/ A. Frolov// In Advances in Intelligent and Soft Computing. Springer Verlag, 2012. (Принято к печати).

Профессор кафедры математического моделирования Национального исследовательского университета «Московский энергетический институт» д.т.н., проф. ***Фролов А.Б.*** – *abfrolov@mail.ru*