Министерство образования и науки РФ

Федеральное государственное автономное образовательное учреждение высшего профессионального образования <<Казанский (Приволжский) федеральный университет>>

ИНСТИТУТ МАТЕМАТИКИ И МЕХАНИКИ

КАФЕДРА АЛГЕБРЫ И МАТЕМАТИЧЕСКОЙ ЛОГИКИ
Направление: 010301 – математика

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(бакалаврская работа)

О некоторых затемненных цифровых подписях, основанных на сложности проблемы дискретного логарифмирования

Работа завершена:
“___”_____ 2015 г. _____ (П.С.Павлов)

Работа допущена к защите:
Научный руководитель
Доктор физ.-мат. наук,
профессор кафедры алгебры
и математической логики КФУ

“___”_____ 2015 г. _____ (С.Н.Тронин)

Заведующий кафедрой алгебры
и математической логики КФУ
Доктор физ.-мат. наук, профессор
“___”_____ 2015 г. _____ (М.М. Арсланов)

Казань-2015

ОГЛАВЛЕНИЕ

Введение

Финансовая криптография (в ее математической части) решает целый ряд проблем, одной из которых является построение электронных платежных систем. Важнейшей частью каждой электронной платежной системы является та или иная затемненная («слепая») цифровая подпись. С помощью такой подписи формируются банкноты (e-cash), которые затем используются в коммерческих расчетах между удаленными пользователями. Чаще всего при этом присутствует посредник (центр доверия), в роли которого, например, может выступить банк. Подписывает банкноты именно этот посредник.

Известно довольно много различных видов затемненных подписей, но большая часть из них не годится для непосредственного использования в платежных системах. В частности, в большинстве затемненных подписей отсутствует возможность встраивания в электронную банкноту, формируемую с помощью такой подписи, сведений о той сумме, которая соответствует этой банкноте, и которая была снята со счета пользователем, сформировавшим эту банкноту (при помощи банка). Эти сведения могут выглядеть как параметр, передаваемый пользователем банку во время осуществления протокола (транзакции) снятия суммы со счета и формирования электронной банкноты на эту сумму. В дальнейшем этот параметр (сумма) становиться открытой частью электронной банкноты, и должен участвовать в проверке подписи, осуществляемой посредником-банком, при этом не должна страдать неотслеживаемость электронной банкноты.

Целью нашей работы является изменение некоторых известных затемненных подписей в соответствии с изложенной выше идеей. В подпись встраивается параметр (сумма), который становиться частью электронной банкноты, и участвует в проверке подписи. В известной нам литературе (в частности в литературе на русском языке) такая постановка задачи не встречается.

Прежде чем перейти к обзору содержания работы, упомянем некоторые книги по финансовой криптографии. Самый известный учебник на русском языке – книга [1], где о слепых подписях и электронных деньгах пишется в §3 гл.3. Необходимо также упомянуть книгу [7] и самый известный англоязычный учебник [4]. Отметим еще книгу [5], посвященную платежным системам.

Теперь опишем содержание работы. В главе 1 напоминаются основные идеи и протоколы из криптографии с открытым ключом. В частности, односторонние функции, хэш-функции, некоторые системы шифрования (RSA, схема Эль-Гамаля), некоторые известные цифровые подписи (RSA, Эль-Гамаля, Шнора), а также протокол обмена платежами Диффи-Хелмана. Кроме того, в главе 1 также изложены известные затемненные подписи на основе подписей RSA и Шнора. В главе 2 излагается известная [7] [4] система электронных платежей Бранса, основанная на затемненной подписи Шнора. В главе 3 излагается основой результат работы. Сначала напоминается обычная цифровая подпись Ньюберг-Руппеля. Затем следуя работе [8], излагается затемненная версия этой подписи.

Наконец в §3, мы описываем осуществленную нами переделку затемненной подписи Ньюберг-Руппеля. В эту подпись вводиться параметр таким образом, что она становиться пригодной для использования в электронных платежных системах, для формирования электронных банкнот.

Глава 1. Введение в криптографию с открытым ключом.

§1. Криптография с открытым ключом. Односторонние функции. Хэш-функции.

В основе преобразований с открытым ключом лежит теоретико-числовой подход к определению стойкости криптоанализа, т.е. проблема обоснования стойкости криптографической схемы свелась к доказательству отсутствия полиномиального алгоритма, который решает задачу, стоящую перед злоумышленником. Основной идеей шифрования с открытым ключом является возможность шифрования секретного сообщения одним ключом, а дешифрования другим ключом, отличным от первого.

Предпосылкой появления алгоритмов шифрования с открытым ключом послужила потребность использования разных ключей для шифрования и дешифрования. То есть злоумышленник получивший ключ, с помощью которого шифровали сообщение не имеет возможности расшифровать его.

Ключ, который используют для шифрования, называют открытым ключом, его можно распространить на всех пользователей системы, не боясь при этом злоумышленников. Процесс дешифрования с помощью этого ключа не представляется возможным. Второй ключ, участвующий в расшифровке секретного сообщения, называем секретным ключом, который знает только получатель секретного зашифрованного сообщения. Широкое распространение в криптографии с открытым ключом получили односторонние или необратимые функции.

Определение 1.1. Односторонней функцией называется функция, с помощью которой легко вычислить значение функции при заданном значении аргумента x, но, если изначально задано значение функции y = f(x), то нет простого пути для определения значения аргумента x.

Пример 1.1. Например, функция $\sin(x)$. Зная значение аргумента x, не составит труда найти значение функции $\sin(x)$ (например при $x = \pi$ $\sin(\pi) = 0$). Но, если $\sin(x) = 0$, однозначно определить x невозможно, т.к. x может быть любым числом, определяемым по формуле $k * \pi$, где k – целое число.

Но не любая необратимая функция пригодна для использования в реальных криптосистемах. В их числе и функция $sin(x)$. Необходимо отметить, что в самом определении необратимости функции присутствует неопределённость. Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.

Определение 1.2. Криптографическая хэш-функция h — это функция, определённая на битовых строках произвольной длины со значениями в строках битов фиксированной длины.

Значение хэш-функции называют хэш-кодом. В других областях науки также используются хэш-функции, но главным отличительным свойством криптографических хэш-функций является односторонность

функции. То есть имея y из множества значений хэш-функции невозможно найти x из области определения, для которого выполняется $h(x) = y$.

Необходимо подчеркнуть, что на данный момент еще не доказано существование необратимых хэш-функций, для которых определение какого-либо прообраза заданного значения хеш-функции теоретически невозможно. Чаще всего нахождение обратного значения лишь вычислительно сложная задача.

Хэш-функция K, используемая для аутентификации сообщений, должная создавать хэш-код для любого сообщения, не должна позволить восстановить сообщение по заданному хэш-коду, должна обеспечить невозможность нахождения другого сообщения, значение которого совпадает со значением хэш-функции.

§ 2. Сравнения, кольца вычетов и конечные поля

Для современных методов криптографии характерно применение алгебраической теории чисел.

Определение 2.1. Два целых числа n и k называют сравнимыми по модулю m, если разность $n-k$ делится на m. Это записывают следующим образом: $n \equiv k \pmod m$. Число mназывают модулем сравнения.

Замечание 2.1. Для любого простого числаа p числаа a^p и a сравнимы по модулю p

Определение 2.2. Для данного модуля m все целые числа, сравнимые по $\pmod m$, называют классом вычетов по модулю m.

Определение 2.3. Множество классов вычетов по модулю m с выведенными операциями сложения и умножения называют кольцом классов вычетов $\pmod m$ и обозначают Z_m.

Определение 2.4. Общим делителем двух целых чисел m и n называют целое число d, на которое m и n делятся без остатка, а наибольшим общим делителем наибольшее из таких чисел, и обозначают его НОД(m,n) или просто (m,n).

Теорема 2.1. *Наибольший общий делитель чисел a и b равен последнему ненулевому остатку от деления $(a,b) = r_n$.*

Доказательство. Согласно равенству $(a,b) = (b,r)$ имеем: $(a,b) = (b,r) = (r,r_1) = (r_1,r_2) = \ldots = (r_n-2, r_n-1) = (r_n-1, r_n) = (r_n,0) = r_n$. ■

Для теоретико-числовых приложений особый интерес имеет множество обратимых элементов кольца классов вычетов Z_m, которое обозначают Z_m^* или U_m и называют группой обратимых элементов кольца вычетов.

Определение 2.5. Для натурального числа m функцией Эйлера $\varphi(m)$ называют число натуральных чисел, меньших m и взаимно простых с m.

Теорема 2.2. *Для простого числа p и натурального n $\varphi(p^n) = p^{n-1}(p-1)$.*

Доказательство.

Достаточно посчитать количество натуральных чисел, не превосходящих p^n и делящихся на p, т.е. чисел вида ap, $1 \leqslant a \leqslant p^{n-1}$. Поскольку a принимает p^{n-1} значений, то количество натуральных чисел, взаимно простых с p и меньших p^n, будет равно $p^n - p^{n-1}$, что доказывает формулу. ■

Пример 2.1. Пусть $m = 5$. Тогда $\varphi(5) = 4$, т.к. число 5 - простое. Заметим, что $24 = 16 \equiv 1 \pmod 5$, $34 = 81 \equiv 1 \pmod 5$, $44 = 256 \equiv 1 \pmod 5$. Оказывается, что и в общем случае для любого целого числа $a \neq 0$ выполняется сравнение $a^{p-1} \equiv 1 \pmod p$ для любого простого числа p (так называемая малая теорема Ферма).

Определение 2.6. Порядком элемента $a \in U_n$ называют наименьшее натуральное число r , для которого $a^r \equiv 1 \pmod{n}$.

Теорема 2.3. (Лагранжа) *Порядок элемента конечной группы является делителем порядка группы.*

Доказательство.

Пусть r является порядком элемента a группы U_n порядка m. Разделим m на r с остатком $m = rq + t, 0 \leqslant t < r$. Тогдаа $a^m = 1 = a^{rq+t} = (a^r)^q * a^t = a^t$, так что $a^t = 1$. Но $t < r$, поэтому $t = 0$, что и требовалось доказать. ■

Следствие 2.1. *Таким образом, для* $x \in (Z/NZ)*$ *выполнено равенство* $x^{\varphi(N)} = 1 \pmod{N}$, *поскольку* $(Z/NZ)* = \varphi(N)$.

Это следствие теоремы Лагранжа подводит нас к малой теореме Ферма.

Теорема 2.4. (Малая теорема Ферма) *Для любого целого числа* a, *не делящегося на простое число* p, *выполняется сравнение* $a^{p-1} \equiv 1 \pmod{p}$

Доказательство.

Докажем, что для любого простого p и целого неотрицательного a, $a^p - a$ делится на p. Доказываем индукцией по a. База. Для $a = 0$, $a^p - a = 0$ и делится на p. Переход. Пускай утверждение верно для $a = k$. Докажем его для $a = k + 1$.

$$a^p - a = (k+1)^p - (k+1) = k^p + 1 + \sum_{l=1}^{p-1} \binom{p}{l} k^l - k - 1 == k^p - k + \sum_{l=1}^{p-1} k^l \binom{p}{l}$$

Но $k^p - k$ делится на p по предположению индукции. Что же касается остальных слагаемых, то $\binom{p}{l} = \frac{p!}{l!(p-l)!}.1 \leq l \leq p-1$, числитель этой дроби делится на p, а знаменатель — не делится, следовательно, $\binom{p}{l}$ делится на p. Таким образом, вся сумма $k^p - k + \sum_{l=1}^{p-1} \binom{p}{l}$ делится на p. Для отрицательных a и нечётных p теорему легко доказать подстановкой $b = -a$. Для отрицательных a и $p = 2$, истинность теоремы следует из $a^2 - a = a(a-1)$ ■

§ 3. Протокол Диффи-Хеллмана

Рассматривается решение следующей задачи: передача Дашей Мише по открытому (незащищенному)каналу связи информации, благодаря которой они смогут получить общий секретный ключ для дальнейшего обмена зашифрованными сообщениями.

В рамках задачи даны: p — достаточно большое простое число, g — порождающий элемент циклической группы $\mathbb{F}_p^*$.

Протокол 3.1.

1) Даша генерирует случайное натуральное число a, $1 < a < p-1$, вычисляет $A = g^a \pmod p$, и посылает A Мише.

2) В это время, независимо от Даши, Миша генерирует случайное натуральное число b, $1 < b < p-1$, и вычисляет $B = g^b \pmod p$, далее посылает B Даше.

3) Даша вычисляет $K_A = B^a \pmod p$.

4) Далее Миша вычисляет $K_B = A^b \pmod p$.

Так как $K_A = K_B$, то задача решена.

Сгенерированный ключ можно использовать в качестве общего секретного ключа (ключа шифрования ключей или сеансового ключа) в симметричной криптосистеме.

Злоумышленник перехватив значения N, q, y_A и y_B, может попытаться определить значение сгенерированного ключа. При этом он сможет - вычислять такое значение K_A по известным N, q, y_A и y_B, что

$q^{KA} \pmod N = y_A$. Однако нахождение K_A по N, q и y_A - это задача нахождения дискретного логарифма в конечном поле, которая считается неразрешимой при достаточно большом $N(> 512)$. Кроме того число $(N-1)/2$ также должно быть простым числом.

Протокол открытого распределения ключей Диффи-Хеллмана позволяет обойтись без защищенного канала связи для передачи ключей. Однако, работая с этим алгоритмом, необходима гарантия того, что Даша получала открытый ключ именно от Миши, и наоборот. Решением данной проблемы является использование электронной цифровой подписи, которой подписываются сообщения с открытом ключом.

В алгоритм Диффи — Хеллмана можно встроить неограниченное количество пользователей. Рассмотрим ситуацию, когда Даша, Миша и Рома вместе сгенерировали исходный ключ. В таком случае последовательность действий будет следующая:

- Изначально стороны договариваются о параметрах p и g.
- Даша, Миша и Рома генерируют свои ключи — a, b и c.
- Даша вычисляет $A = g^a$ и отправляет его Мише.
- Миша вычисляет $A = (g^a)^b = g^{ab}$ и $A = g^b$ отправляет его Роме.
- Рома вычисляет $A = (g^b)^c = g^{bc}$ и отправляет его Даше.
- Даша вычисляет $A = (g^{bc})^a = g^{bca} = g^{abc}$ и использует его в качестве своего секретного ключа.
- Рома вычисляет $A = g^c$ и отправляет его Даше.

- Даша вычисляет $A = (g^c)^a = g^{ca}$ и отправляет его Мише.
- Миша вычисляет $A = (g^{ca})^b = g^{cab} = g^{abc}$ и использует его в качестве своего секретного ключа.

В данной ситуации любой участник алгоритма имеет доступ к $A = g^a$, $A = g^b$, $A = g^c$, $A = g^{ab}$, $A = g^{ac}$, $A = g^{bc}$, но при этом не может вычислить любую комбинацию $A = g^{abc}$.

Для того чтобы данный алгоритм возможно было применять повсеместно, необходимо:

- изначально передавать "пустой"ключ g, основная задача алгоритма состоит в повышении текущего значения показателя каждого участника один раз;
- любое промежуточное значение может быть раскрыто публично, но окончательное значение представляет из себя секретный ключ, который никогда не должен быть публично раскрыт, таким образом, каждый пользователь получает свою копию секретного ключа и переедает его последующему.

Протокол Диффи-Хеллмана позволяет шифровать данные при каждом сеансе связи с использованием новых секретных ключей. Основным преимуществом протокола Диффи-Хеллмана в сравнению с методом RSA заключается в том, что формирование общего секретного ключа происходит в тысячи раз быстрее. В системе RSA создание новых секретных и открытых ключей основано на генерации новых простых чисел, что занимает много времени.

§ 4. Криптосистема и подпись RSA

Определение 3.1. RSA – криптографическая система с открытым ключом, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись (аутентификация – установление подлинности).

Криптосистема RSA основана на теореме Эйлера, согласно которой для любых взаимно простых целых чисел и n, где $< n$, выполняется соотношение $M^{\varphi(n)} \equiv 1 \pmod{n}$.

Секретное сообщение в RSA представляется в виде числа , которое далее будет подписываться или шифроваться.

Пусть и n взаимопросты. Далее берем два различных больших простых числа p, q, их произведение представим в виде $N = pq$. Возьмем число E такое, что $1 < E < \varphi(N)$ удовлетворяющее следующему условию НОД$(E, \varphi(N)) = 1$. Подберем число d такое, что $Ed = 1 + \varphi(N)t$.

Битовую строку, которую мы решили зашифровать, можно представить в виде двоичной записи натурального числа m. Но с одним условием $0 \leq m \leq N - 1$.

Секретным ключом данной криптосистемы является тройка (p, q, d). Даша, отправитель секретного сообщения m, знает значения N и E. Получатель секретного сообщения C (Миша) знает N и E и секретный ключ (ему даже достаточно знать d).

Отсутствие на данный момент действенных методов разложения на сомножители гарантирует невозможность получения частного ключа d.

Исходя из этого надежность криптосистемы RSA основана на трудноразрешимой (практически неразрешимой в данное время) задаче разложения N на сомножители.

Протокол 3.2.

1) Процесс шифрования $C = m^E \pmod N$.

2) Процесс дешифрования $m = C^d \pmod N$.

Пример 3.1. Пусть заданы простые числа $p = 13$ и $q = 11$. Тогда их произведение $N = 143$, а $(p-1)(q-1) = 12 * 10 = 120$. В качестве открытой шифрующей переменной возьмем число $E = 113$, поскольку $(113, 120) = 1$.Применяя расширенный алгоритм Евклида, найдем $d = 17$, т.к

$$113 * 17 = 1921 = 1 \pmod{120}.$$

Предположим, нужно зашифровать сообщение, численно равное $m = 123$. Тогда мы найдем

$$C = m^E(modN) = 123^{113} \pmod{143} = 41.$$

Процесс дешифровывания происходит аналогично:

$$m = C^d(modN) = 41^{17} \pmod{143} = 123.$$

Теорема 3.1. (Теорема Эйлера) *Если a и m взаимно просты, то $a^{\varphi(m)} \equiv 1 \pmod m$, где $\varphi(m)$ – функция Эйлера.*

Доказательство.

Пусть $x_1, \ldots, x_{\varphi(m)}$ — все различные натуральные числа, меньшие m и взаимно простые с ним. Рассмотрим всевозможные произведения $x_i a$ для всех i от 1 до $\varphi(m)$. Поскольку a взаимно просто с m и x_i взаимно просто с m, то и $x_i a$ также взаимно просто с m, то есть $x_i a \equiv x_j \pmod{m}$ для некоторого j. Отметим, что все остатки $x_i a$ при делении на m различны. Действительно, пусть это не так, то существуют такие $i_1 \neq i_2$, что

$$x_{i_1} a \equiv x_{i_2} a \pmod{m}$$

или

$$(x_{i_1} - x_{i_2}) a \equiv 0 \pmod{m}.$$

Так как a взаимно просто с m, то последнее равенство равносильно тому, что

$$x_{i_1} - x_{i_2} \equiv 0 \pmod{m}$$

или

$$x_{i_1} \equiv x_{i_2} \pmod{m}.$$

Это противоречит тому, что числа $x_1, \ldots, x_{\varphi(m)}$ попарно различны по модулю m. Перемножим все сравнения вида $x_i a \equiv x_j \pmod{m}$. Получим:

$$x_1 \cdots x_{\varphi(m)} a^{\varphi(m)} \equiv x_1 \cdots x_{\varphi(m)} \pmod{m}$$

или

$$x_1 \cdots x_{\varphi(m)} (a^{\varphi(m)} - 1) \equiv 0 \pmod{m}.$$

Так как число $x_1 \cdots x_{\varphi(m)}$ взаимно просто с m, то последнее сравнение равносильно тому, что

$$a^{\varphi(m)} - 1 \equiv 0 \pmod{m}$$

или

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

■

Протокол 3.3. (Цифровая подпись RSA.) Предположим что Даша хочет послать Мише засекреченное сообщение M, причем таким образом, чтобы Миша был уверен, что сообщение не было взломано и что автором сообщения действительно является Даша. Для этого Даша создает цифровую подпись S возводя M в степень d и умножая на модуль n: Секретный ключ знает только Даша.

1) Подписание $S = m^d \pmod{N}$, где d и N - частный ключ Даши.

2) Даша отправляет Мише сообщение m и подпись S.

3) Проверка подписи $m \equiv S^E \pmod{N}$, где E и N - открытый ключ Даши.

Для того чтобы установить подлинность автора, не надо передавать секретные ключи, так как оба персонажа пользуются исключительно открытым ключом своего собеседника либо собственным секретным ключом. Поделиться зашифрованным сообщением и проверить подписанное сообщение может любой из персонажей, но расшифровать или подписать сообщение может только владелец соответствующего секретного ключа.

Использование в алгоритме криптографических хэш-функций создает возможность формирования схемы подписи RSA без восстановления сообщения. Далее рассмотрим схему электронной цифровой подписи RSA.

$$S = h(M)^d \pmod{N}; \qquad h(M) \equiv S^E \pmod{N}.$$

В соответствии с RSA формируются два ключа, секретный и открытый.

Открытый ключ подписи (E, N), отправитель отправляет всевозможным адресатам своих сообщений. Именно эта пара позволит определить подлинность и принадлежность отправителю полученных от него сообщений. Значение d хранится отправителем в секрете. Оно в паре с модулем N является секретным ключом, который будет использоваться при подписывании.

1. Отправитель преобразует сообщение M при помощи криптографической хеш-функции h в целое число $m = h(M)$.

2. Отправитель вычисляет значение цифровой подписи S для сообщения M на основе ранее полученного значения хеш-образа m и значения своего закрытого (секретного) ключа подписи d. Для этого используется преобразование, аналогичное преобразованию, выполняемому при шифровании по алгоритму RSA:

$$S = m^d \pmod{N}$$

Пара (M, S), представляющая собой подписанное отправителем сообщение, передаётся получателю. Сформировать подпись S мог только обла-

датель закрытого ключа d. Процедура проверки получателем подлинности сообщения и принадлежности его отправителю состоит из следующих шагов.

Получатель сжимает полученное сообщение M' при помощи криптографической хеш-функции h, идентичной той, которая была использована отправителем, в целое число m'.

Получатель выполняет расшифрование открытым ключом E отправителя дайджеста m оригинального сообщения, преобразуя значение подписи S по алгоритму RSA:

$$m = S^E \pmod{N}$$

3. Получатель сравнивает полученные значения m' и m. Если данные значения совпадают, т. е.

$$S^E \pmod{N} = h(M)$$

то получатель признает полученное сообщение подлинным и принадлежащим отправителю.

Фальсификация сообщения при его передаче по каналу связи возможна только при получении злоумышленником секретного ключа d либо за счет проведения успешной атаки против использованной хеш-функции. При использовании достаточно больших значений p и q определение секретного значения d по открытому ключу (E, N) является чрезвычайно трудной задачей, соответствующей по сложности разложению модуля N на множители. Используемые в реальных приложениях хеш-функции

обладают характеристиками, делающими атаку против цифровой подписи практически неосуществимой. Поскольку подписываемые документы - переменного (и как правило достаточно большого) объёма, в схемах электронных платежей зачастую подпись ставится не на сам документ, а на его хэш. Для вычисления хэша используются криптографические хеш-функции, что гарантирует выявление изменений документа при проверке подписи. Хеш-функции не являются частью алгоритма электронной подписи, поэтому в схеме может быть использована любая надёжная хеш-функция.

§ 5. Слепая подпись RSA.

Определение 5.1. Слепая подпись (Blind Signature) представляет собой разновидность электронной цифровой подписи, главной особенностью которой является то, что подписывающий не может точно знать содержание подписываемого документа.

Слепая подпись используется в протоколах электронных платежей, основанных на использовании электронной монеты (electronic coin) — информации, не имеющей трудно подделываемого физического воплощения в отличии от обычных денег. Слепая подпись выполнится банком для уникального номера монеты, известного только его владельцу. Таким образом, протокол слепой подписи должен обеспечивать возможность подписи для сообщения, текст которого не известен подписывающему. Отличие слепой подписи от обычной цифровой подписи состоит в возможности вычисления маски и ее последующего снятия так, что подпись остается верной. Кроме того, наложение и снятие маски должно выполнятся без знания ключа подписи. Снятие маски должно исключать возможность подделывания сообщения.

Для реализации возможности использования электронных денежных средств, создаются специализированные криптографические схемы электронных платежей. В этих схемах в роли основных действующих лиц выступают банк, покупатель и продавец. Согласно легенде продавец и покупатель имеют счета в банке, и при этом покупатель хочет заплатить продавцу за товар или услугу.

В платёжной системе используются три основные транзакции: снятие со счета, платежа, депозита.

В транзакции снятия со счета покупатель получает подписанную банком электронную банкноту на затребованную сумму. При этом банковский счет покупателя автоматически уменьшается на эту же сумму. В транзакции платежа покупатель отправляет банкноту продавцу и указывает сумму платежа. Продавец в свою очередь, отправляет эту информацию банку, который проверяет подлинность банкноты. Если банкнота подлинная, то банк проверяет, не была ли она потрачена ранее. Если нет, то банк заносит ее в специальный регистр, зачисляет требуемую сумму на счета продавца, уведомляет продавца об этом, и, если достоинство банкноты выше, чем сумма платежа, возвращает покупателю «сдачу» через продавца. С помощью транзакции депозита, покупатель может положить «сдачу» на свои счет в банке.

Гарантией безопасности банка является невозможность подделать его подпись для создания фальшивой банкноты, или, более общим словами невозможность, получив набор подлинных электронных банкнот, подделать подпись ещё хотя бы одной банкноты. Для достижения неотслеживаемости покупателя необходимо чтобы банк, получив банкноту в транзакции платежа, не смог установить, кому она была выдана. Такая же ситуация и со «сдачей». Неотслеживаемость гарантируется тем, что банк просто не знает, что именно он подписал.

Далее приведем пример самой простой платежной системы с использованием слепой подписи RSA. Банк, в данном случае являющийся под-

писывающим персонажем, выбирает два очень больших секретных простых числа p и q, и публикует их произведение $N = pq$. Пусть e и d, где $ed = 1 \pmod{\varphi(N)}$,- открытый и секретный ключи RSA. Сформируем подпись, для этого применим к сообщению m функцию дешифрования RSA $s = m^d \pmod{N}$. Применив функцию шифрования мы сможем провести проверку подписи. Если $s^e = m \pmod{N}$, то s - корректная подпись для сообщения m.

Банк выбирает и публикует числа N и e, а так же некоторую одностороннюю функцию $f : Z_N \to Z_N$, назначение которой станет ясно из дальнейшего. Пара ключей (e, d) используется банком исключительно для создания электронных банкнот, т.е. устанавливается соглашение о том, что электронной подписи, сгенерированной на ключе d, соответствует электронная банкнота достоинством, скажем, в один юань.

Для того чтобы снять со счета средства покупателю необходимо выбрать случайное число $n \epsilon Z_N$ и вычисляет $f(n)$. Далее он должен получить подпись банка на этой банкноте, т.е. значение $f(n)^d$. Далее покупатель выбирает случайное число $r \epsilon Z_N$, $r \neq 0$, вычисляет $f(n)r^e \pmod{N}$ и отправляет его банку. r^e называют затемняющим множителем. Банк вычисляет $f(n)^d \cdot r \pmod{N}$ и отправляет обратно покупателю. Теперь покупатель в состоянии легко “снять” затемняющий множитель и получить подписанную банкноту $(n, f(n)^d \pmod{N})$.

Для оплаты товаров или услуг покупателю необходимо отправить продавцу банкноту $(n, f(n)^d \pmod{N}))$. Неотслеживаемость покупателя в данной системе не обсуждается. Значение $f(n)^d \cdot r \pmod{N}$, кото-

рое благодаря затемняющему множителю r является неким случайным числом из Z_N. Поэтому банк не знает какую банкноту он выдал покупателю.

§ 6. Криптосистема Эль-Гамаля

Криптосистема Тахира Эль-Гамаля является криптосистемой, альтернативной системе RSA, и обеспечивает тот же уровень криптостойкости. За основу криптосистеме взяты числа p и a, где p – большое простое число, a–первообразный корень в циклической группе $(\mathbb{Z}/p\mathbb{Z}^*, \cdot)$. Числа p и a не нуждаются в скрытии и доступны всем пользователям.

Для начала разберемся с формированием ключей в системе Эль-Гамаля. Для этого выберем случайное простое число p длины n битов. Возьмем случайный примитивный элемент g поля $\mathbb{Z}_p$. Далее выберем случайное целое число x, которое $1 < x < p-1$. Вычислим $y = g^x \pmod p$. В данном случае открытый ключ это тройка (p, g, y), закрытый - x.

Процесс шифровки сообщение M начинается с выбора сессионного ключа, которым является случайно выбранное целое число k такое, что $1 < k < p-1$. Далее необходимо вычислить $a = g^k \pmod p$ и$b = y^k M \pmod p$. Тогда пара чисел (a, b) будет зашифрованным текстом.

Возможно восстановить зашифрованное сообщение, но для этого надо знать секретный ключ x и воспользоваться формулой $M = b(a^x)^{-1} \pmod p$ Можно заметить, что $(a^x)^{-1} \equiv g^{-kx} \pmod p$ и поэтому $b(a^x)^{-1} \equiv (y^k M)g^{-xk} \equiv (g^{xk}M)g^{-xk} \equiv M \pmod p$ Чаще всего в практике используют следующую формулу $M = b(a^x)^{-1} \pmod p p = b \cdot a^{(p-1-x)} \pmod p$

Даша подписывает сообщение m следующим образом.

1) Выбирается случайным образом число k, $0 < k < p - 1$. Необходимо чтобы НОД$(k, p-1) = 1$.

2) Вычисляется $s_1 = g^k \pmod{p}$, а s_2 корень следующего уравнения $h(m) \equiv xs_1 + ks_2 \pmod{(p-1)}$.

4) Тогда подписью сообщения m является пара чисел s_1, s_2. Таким образом, Даша отправляет Мише три числа: m, s_1, s_2.

Миша не знает ни x, ни k, но при этом знает p, g, y, h. Для проверки подписи Мише надо проверить, что $g^{h(m)} \equiv y^{s_1} s_1^{s_2} \pmod{p}$. Если сравнение выполняется, то подпись принимается, если нет, то отвергается.

Криптостойкость основана на трудности решения задачи о дискретном логарифме: ПО известным p, g, y, если число p достаточно велико, вычислительно очень трудно найти решение сравнения: $y \equiv g^x \pmod{p}$.

§ 7. Подпись Шнора. Слепая подпись Шнора

Теперь рассмотрим цифровую подпись Шнора. Стойкость данной подписи основана на трудности вычисления дискретных логарифмов. У нас есть два персонажа Даша и Миша. Даша хочет передать сообщение Мише. Для создания ключей выберем большие простые числа p и p' такие, что $p'|p-1$. $Q \in Z_p = 0, 1, ..., p-1$ - элемент порядка p' , т.е $Q^{p'} \equiv 1 \pmod{p'}$ $P = Q^x \pmod{p}$. $0 < l < p'$ - секретный ключ Даши, которая подписывает сообщение M, $0 < M < p$. p, p',Q,R все числа находиться в свободном доступе. Подпись сообщения осуществляется применением хэш-функции h.

Даша выбирает случайное число $0 < r < p'$ ("эфемерный ключ"), и вычисляет $R = Q^r \pmod{p}$. Для того, чтобы подписать сообщение M Даше необходимо выполнить следующие действия:

(1) вычислить $E = h(M||R) \pmod{p'}$, где $||$ - сцепление, r строке бит M ,

(2) вычислить $S = (r + lE) \pmod{p'}$. Подписью являются значения l и E, их нужно выслать Мише.

Для проверки подлинности Миша вычисляет $R' = Q^S * P^{-E}$ и $E = h(M||R')$. Если $E = E'$, то подпись верна.

Рассмотрим слепую подпись Шнора. Возьмём также персонажей Дашу и Мишу. Пусть Даша хочет получить подпись к сообщению M такую, чтобы подписывающий прочитать сообщение в ходе его формирования, при получении сообщения не смог опознать пользователя, который запустил генерацию данной слепой подписи.

Миша, который будет подписывающим персонажем, владеет секретным ключом l. Тогда при обращении Даши к Мише, ему приходится отправить Даше $R = q^k \pmod{p}$, где k - выбирается Мишей, $0 < k < p')$. В ответ на это Даша выбирает числа ϵ и τ, такие что $0 < \epsilon, \tau < p'$ и вычисляет $R' = RQ^{\epsilon}y^{\tau} \pmod{p}$, $E' = h(M||R') \pmod{p'}$, $E = (E' + \tau) \pmod{p'}$ и делиться со значением E с Мишей. После получения E Миша вычисляет $S = k + lE \pmod{p'}$ и отправляет S Даше. Даша вычисляет подпись M которая равная паре (E', S'), где $E' = (E - \tau) \pmod{p'}$ и $S' = (S - \epsilon) \pmod{p'}$

Для проверки сообщения надо вычислить $R' = Q^{S'}y^{E'} \pmod{p}$ и проверить, будет ли $E' = h(M||R')$.

Глава 2. Система электронных платежей

§1. Системы электронных платежей и перспективы их развития

Системы электронных платежей (далее СЭП) это комплекс специализированных программных средств, который обеспечивает транзакции (переводы) денежных средств от потребителя к поставщику товаров или услуг.

На данный момент в мире функционирует множество видов СЭП, т.к. PayPal, Qiwi Wallet, Яндекс.Деньги и т.д. Наиболее распространенными являются Visa и MasterCard, системы, с которыми сотрудничает львиная доля мировых банковских структур.

В СЭП применяются электронные деньги. Электронные деньги, как и свои бумажные аналоги, обладают ликвидностью, универсальностью, делимостью, но возникают и относительно новые свойства, такие как безопасность, анонимность и долговечность. Доступ к СЭП пользователи получают посредствам использования платежных карт, электронных чеков и дистанционного банкинга.

Главными отличительными свойствами электронных денег являются: удобство оплаты товаров или услуг, скорость платежа, отсутствие очередей.

С развитием новых информационных технологий и возникновения интернет торговли перед человечеством возникает проблема обеспечения безопасности личных данных и сохранности средств на электронных счетах при осуществлении денежных переводов, оплаты услуг и т.д. В

связи с этим дополнительную актуальность приобретает вопрос разработки, тестирования и внедрения новых СЭП, которые смогут защитить интересы конечных потребителей.

Внешнеполитическая ситуация в стране, а так же санкции со стороны запада создают благоприятную среду для создания внутрироссийской СЭП, которая в свою очередь сможет вытеснить с рынка таких гигантов отросли как Visa и MasterCard.

Далее в моей работе будет рассмотрена СЭП Брандса на базе затемнено подписи Шнора.

§ 2. Система электронных платежей Брандса

СЭП Брандса является анонимной автономной системой электронных платежей. Она достаточно эффективна, но ей свойства не сформулированы в терминах модели доказательной безопасности, и в этом ей слабость. Основой данной СЭП является затемненная подпись Шнора, основанная на задаче дискретного логарифмирования. Ей можно рассматривать как расширение схемы цифровой подписи Шнора.

В схеме подписи Шнора выбирают два больших простых числа p, q, таких, что $q|p-1$, $g \in G_q$ - образующий элемент подгруппы $\mathbf{Z}_p^*$ порядка q. Случайное число $ \in Z_q$ будет секретным ключом для данной подписи. Набор чисел (p, q, g, h) будет составлять открытый ключ, где $h = g_x$; m - подписываемое сообщение. Подписывающий выбирает $w \in Z_q$, находит $c = (m, a) \in Z_q$, $r = w + cx$ и отправляет $[m, c, r]$ проверяющему. Последний должен проверить: $g^r = ah^c \mod p$. Если проверка прошла, тогда проверяющий принимает подпись, в обратном случае отвергает ее.

Полученную схему возможно использовать для анонимных платежей онлайн по аналогии со схемой слепой подписи RSA. Для реализации данной возможности необходимо расширить функционал СЭП путем добавления механизма идентификации повторной траты монеты, а именно необходимо закодировать идентификаторы владельцев монет в самих монетах и разработать механизм запросов и ответов для платежей. Так как банк может только проверять факт присутствия корректного идентификатора в монете, которую он подписывает (в то время как в самом платеже будет использовано m'), закодированный идентификатор вла-

дельца должен каким-то образом «пережить» этот процесс затемнения. Это свойство будем называть удержанием идентичности.

Основной идеей метода является: представление m в форме $m = g_1^{id} \cdot g_2$, где g_1, g_2 - образующие элементы, отличные от g, использовавшегося ранее, т.е. $g_1 = g_2 = g \in G_q$, но при этом пользователь - плательщик должен знать id. Тогда в случае корректности затемненной подписи, результат будет следующим: $m = m^s g^t = g_1^{id \cdot s} \cdot g_2^s g^t$. Протокол платежа будет вынуждать плательщика демонстрировать знание экспонент x_1, x_2, таких, что $m' = g_1^{x_1} \cdot g_2^{x_2}$. Кроме того, можно показать, что тройное экспоненцирование, т.е. функция $(x_1, x_2, x_3) \to g_1^{x_1} g_2^{x_2} g^{x_3}$, не имеет коллизий. Тогда, два представления m', используя тройки $(id \cdot s, s, t)$ и $(x_1, x_2, 0)$, должно совпадать. В таком случае, для затемнения плательщик должен выбрать $t = 0$. Тогда получается следующее: $(x_1, x_2) = (id \cdot s, s)$. Очевидно, что идентификатор id вычисляется следующим образом: $id = x_1/x_2$. Теперь в случае повторной траты будут разглашается все секретные параметры, x_1, x_2, и следовательно id.

Полностью СЭП Брандса возможно описать следующими протоколами:

Инициализация системы. Протокол инициализации выполняется однократно при вводе СЭП в эксплуатацию. Банк выбирает тройку порождающих (g, g_1, g_2) группы G_q простого порядка и число $x \in_R \mathbb{Z}_q^*$. Также банком выбираются две хэш-функции H и H_0. Хэш-функция H отображает пятерик элементов группы G_q в $\mathbb{Z}_q^*$, а H_0 - пары элементов G_q - в $\mathbb{Z}_q$. H_0 находится в зависимости от некоторого параметра id,

идентифицирующего продавца (далее $Seller$), а также - от временного параметра t, который представляет собой дату и время выполнения транзакции. Банк оглашает описание группы G_q (простые числа p и q, если $G_q \subset \mathbb{Z}_p^*$), тройку (g, g_1, g_2) и функции H, H_0 в качестве своего открытого ключа. Секретным ключом банка является x. Также часть открытого ключа является параметр $h = g^x$.

Подписью банка $sign(A, B)$ для пары (A, B), $A, B \in G_q$ является четверка (z, a, b, r), где $z, a, b \in G_q$, $r \in \mathbb{Z}_q$, определенная следующим образом $g^r = h^{H(A,B,z,a,b)}a, A^r = z^{H(A,B,z,a,b)}b$

Открытие счета. Протокол открытия счета выполняется единожды при вводе нового пользователя в СЭП. Протокол состоит из следующих шагов. Пользователь (далее $User$) выбирает число $u_1 \in_R \mathbb{Z}_q$ и находит $I = g_1^{u_1}$. Если $Ig_2 \neq 1$, то $User$ отправляет значение I банку, а u_1 хранит в секрете. Для банка критичным является различие значения I для разных клиентов. Банк определяет $z = (Ig_2)^x$ и отправляет его $User$.

Снятие со счета. Перед тем как произвести снятие средств со счета, $User$ необходимо пройти аутентификацию, т.е. доказать банку, что он владелец данного счета. Затем выполняется следующее:

1. Банк выбирает число $w \in_R \mathbb{Z}_q$ и отправляет $a = g^w$ и $b = (Ig_2)^w$ пользователю $User$.

2. $User$ выбирает три числа $s \in_R \mathbb{Z}_q^*$, $x_1, x_2 \in_R \mathbb{Z}_q$ и находит $A = (Ig_2)^s$, $B = g_1^{x_1}g_2^{x_2}$ и $z' = z^s$. Также, $User$ выбирает числа $u, v \in_R$

$\mathbb{Z}_q$ и вычисляет $a' = a^u g^v$ и $b' = b^{su} A^v$. Далее он вычисляет $c' = H(A, B, z', a', b')$ и отправляет запрос $c = c'/u \bmod q$ банку.

3. Банк присылает ответ $r = (cx + w) \bmod q$ и снимает со счета $User$ необходимую сумму средств. $User$ принимает ответ тогда и только тогда, когда $g^r = h^c a$ и $(Ig_2)^r = z^c b$. Еслы все вычислено $User$ находит $r' = (ru + v) \bmod q$. Пара (A, B) и подпись банка (z', a', b', r') являются электронной банкнотой.

Платеж. В транзакции платежа $User$ и $Seller$ выполняется следующий протокол.

1. $User$ отправляет $Seller$ электронную монету: A, B, $sign(A, B)$.

2. Если $A \neq 1$, то $Seller$ вычисляет запрос $d = H_0(A, B, id, t)$, где id - идентификатор $Seller$, а t – дата и время транзакции. $Seller$ посылает $User$ значение d.

3. $User$ вычисляет значение $r_1 = (d(u_1 s) + x_1) \bmod q$ и $r_2 = (ds + x_2) \bmod q$ и посылает их $Seller$. $Seller$ принимает монету тогда и только тогда, когда $sign(A, B)$ является подписью для (A, B) и $g_1^{r_1} g_2^{r_2} = A^d B$.

Депозит. $Seller$ посылает банку $A, B, sign(A, B), (r_1, r_2)$, а также дату и время транзакции платежа t. Если $A = 1$, то банк не принимает монету. В противном случае он вычисляет d, используя полученные данные и идентификатор id продавца $Seller$. Затем банк проверяет, что $g_1^{r_1} g_2^{r_2} = A^d B$ и что $sign(A, B)$ является подписью для (A, B). Если все

корректно, то банк проверяет, не была ли монета потрачена ранее. Если нет, то банк запоминает (A, t, r_1, r_2) и кладет монету на счет $Seller$.

Если данная электронная монета уже была потрачена ранее, то банк имеет в своем распоряжении две несовпадающие тройки (d, r_1, r_2) и (d', r_1', r_2') и может вычислить тдентификатор нарушителя $g_1^{(r_1-r_1')/(r_2-r_2')}$.

Глава 3. Произвольные суммы в платежных системах

§1. Подпись Ньюберг-Руппеля

Подпись Ньюберг-Руппеля является схемой электронной подписи с открытым ключом, основанной на задаче дискретного логарифмирования в конечном поле. Имеются два пользователя Даша, Миша и незащищенный канал связи между ними. Пользователь Даша подписывает открытое сообщение секретным ключом, а полученную подпись пересылает пользователю Мише, который в свою очередь с помощью открытого ключа проверяет подлинность подписи и восстанавливает сообщение. При положительном результате проверки, Миша убеждается в целостности сообщения, в его оригинальности (то есть в том, что сообщение было послано именно пользователем Дашей), а также лишается возможности утверждать, что Даша не посылала это сообщение. Важно, что только Даша способна подписать свое сообщение, потому что только она знает свой секретный ключ, и то, что её подпись может быть проверена любым пользователем, так как для этого нужен лишь открытый ключ.

Введем необходимые параметры p-большое простое число, простое $q|p-1$, и $g \in \mathbf{Z}_q^*$. Секретным ключом в данной схеме является случайное число $x \in \mathbf{Z_q}$, а открытым ключом является $y \equiv g^x \pmod{p}$. Для подписи сообщения $m \in \mathbf{Z_p}$, подписывающий выбирает случайное значение $k \in \mathbf{Z_q}$ и вычисляет r и s:

$$r \equiv mg^k \pmod{p}$$

$$s \equiv xr + k \pmod{q}$$

Пара (r, s) и является подписью сообщения m. Для проверки подписи достаточно вычислить

$$m \equiv q^{-s} y^r r \pmod{p}.$$

Так как данная подпись позволяет восстанавливать сообщение, подпись не должна содержать его.

§2. Слепая подпись Ньюберг-Руппеля

Данная слепая подпись основана на схеме подписи Ньюберг-Руппеля, рассмотренной в предыдущем параграфе.

1. Банк выбирает $k \in \mathbf{Z}_q$, вычисляет $\tilde{r} \equiv g^k \pmod{p}$ и отправляет $\tilde{r}$ клиенту.

2. Клиент выбирает случайные $\alpha \in \mathbf{Z}_q$ и $\beta \in \mathbf{Z}_q^*$, вычисляет $r \equiv mg^{\alpha}\tilde{r}^{\beta} \pmod{p}$ и $\tilde{m} \equiv r\beta^{-1} \pmod{q}$. Если $\tilde{m} \in \mathbf{Z}_q^*$ тогда клиент отправляет $\tilde{m}$ Банку, если $\tilde{m} \notin \mathbf{Z}_q^*$ тогда клиент выбирает новые α и β.

3. Банк вычисляет $\tilde{s} \equiv \tilde{m}x + k \pmod{q}$ и отправляет $\tilde{s}$ клиенту.

4. Банк вычисляет $s \equiv \tilde{s}\beta + \alpha \pmod{q}$.

Пара (r, s) составляет слепую подпись.

Действительность слепой подписи (r, s) устанавливается из следующего соотношения

$$g^{-s}y^r r \equiv mg^{-\tilde{s}\beta-\alpha+xr+k\beta+\alpha} \equiv mg^{-\tilde{m}\beta x+xr-k\beta+k\beta} \equiv m \pmod{p}$$

Выбранная клиентом уникальная пара $\alpha \in \mathbf{Z}_q$ и $\beta \in \mathbf{Z}_q^*$ гарантирует затемненность подписи (r, s). Подпись (r, s) формируется на основе k, $\tilde{r} \equiv g^k \pmod{p}$, $\tilde{m}$ и $\tilde{s} \equiv \tilde{m}x + k \pmod{q}$, и

$$r \equiv mg^{\alpha}\tilde{r}^{\beta} \pmod{p}$$

$$\tilde{m} \equiv r\beta^{-1} \pmod{q}$$

$$s \equiv \tilde{s}\beta + \alpha \pmod{q}$$

В таком случае, так как $\tilde{m} \in \mathbf{Z}_q^*$, α и β можно вычислить по следующим формулам

$$\beta \equiv r\tilde{m}^{-1} \pmod{q}$$

$$\alpha \equiv s - \tilde{s}\beta \pmod{q}$$

В качестве проверки необходимо проверить следующее соотношение (используем $(g^{-s}y^r r) \equiv m \pmod{p}$):

$$mg^{\alpha}\tilde{r}^{\beta} \equiv g^{-s+rx+\alpha+k\beta}r \equiv g^{-\tilde{s}\beta+rx+k\beta}r \equiv g^{-\tilde{m}x\beta+rx}r \equiv r \pmod{p}$$

§3. Произвольные суммы в подписи Ньюберг-Руппеля

Основной задачей, которуя я пытался решить в рамках данной дипломной работы, является проблема снятия и получения подписи для произвольной суммы. Для решения данной задачи необходимо введения нового параметра t в структуру имеющейся подписи, то есть в данном случае электронная банкнота - это (m, r, s, t).

Новый параметр t в некотором виде должен присутствовать в вычесляемом банком $\tilde{s}$. Но при этом должны выполняться следующие требования:

1. должна быть обеспечена неподделываемость подписи и сообщения m;

2. банк не может быть злоумышленником;

3. параметр t должен появляться в подписи только при вычислениях банка так как, покупатель может быть злоумышленником.

Введем параметр t в иследуемую подпись $\tilde{s} \equiv \tilde{m}xt + k \pmod{q}$. В таком случае пункты 1 и 2 слепой подписи Ньюберг-Руппеля не изменятся. Далее подпись будет выглядеть следующим образом:

3' Банк вычисляет $\tilde{s} \equiv \tilde{m}tx + k \pmod{q}$ и отправляет $\tilde{s}$ клиенту.

4' Банк вычисляет $s \equiv \tilde{s}\beta + \alpha \equiv rxt + k\beta + \alpha \pmod{q}$.

Далее также изменяем алгоритмы проверки, так как слепую подпись будут уже составлять (t, r, s).

Действительность слепой подписи (t, r, s) устанавливается из следующего соотношения

$$g^{-s}y^{tr}r \equiv g^{-s}g^{xtr}r \equiv mg^{-\tilde{s}\beta-\alpha+xr+k\beta+\alpha} \equiv mg^{-\tilde{m}\beta x+xr-k\beta+k\beta} \equiv m \pmod{p}$$

Выбранная клиентом уникальная пара $\alpha \in \mathbf{Z}_q$ и $\beta \in \mathbf{Z}_q^*$ обеспечивает затемненность подписи (t, r, s), то есть невозможность ее подделки. Слепая подпись формируется на основе параметров k, $\tilde{r} \equiv g^k \pmod{p}$, $\tilde{m}$ и $\tilde{s} \equiv \tilde{m}tx + k \pmod{q}$, и

$$r \equiv mg^{\alpha}\tilde{r}^{\beta} \pmod{p}$$

$$\tilde{m} \equiv r\beta^{-1} \pmod{q}$$

$$s \equiv \tilde{s}\beta + \alpha \pmod{q}$$

В таком случае, так как $\tilde{m} \in \mathbf{Z}_q^*$, α и β можно вычислить по следующим формулам

$$\beta \equiv r\tilde{m}^{-1} \pmod{q}$$

$$\alpha \equiv s - \tilde{s}\beta \pmod{q}$$

В качестве проверки необходимо проверить следующее соотношение (используем $g^{-s}y^{tr}r \equiv m \pmod{p}$):

$$mg^{\alpha}\tilde{r}^{\beta} \equiv g^{-s+rx+\alpha+k\beta}r \equiv g^{-\tilde{s}\beta+rx+k\beta}r \equiv g^{-\tilde{m}x\beta+rx}r \equiv r \pmod{p}$$

Итак, проверка прошла успешно. Возможность использования произвольных сумм установлена.

Список литературы

[1] Введение в криптографию/ Под общ. ред. В.В. Ященко.— 3-е изд., доп. — М.: МЦНМО: “ЧеРо”, 2000. — 288 с.

[2] Молдовян Н.А., Практикум по криптосистемам с открытым ключом. — СПб.: БХВ-Петербург, 2007. — 304 с.

[3] Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов.— М.: Горячая линия-Телеком, 2005. — 229 с.

[4] Burton Rosenberg. Handbook of financial criptography and security. Taylor and Francis Group, LLC. Chapman and Hall/CRC is an imprint of Taylor and Francis Group, an Informa business, —-2011. —-584 c.

[5] Donal O’Mahony, Michael Peirce, Hitesh Tewari. Electronic Payment Systems for E-Commerce Second Edition. ARTECH HOUSE,INC. 685 Canton Street Notwod, MA 02062. —- 2001.-— 345 c.

[6] Смарт Н. Криптография.— М.: Техносфера, 2005.—528 с.

[7] С.В. Запечников Криптографические протоколы и их применение в финансовой и коммерческой деятельности.— М.: Горячая линия-Телеком, 2007.—320 с.

[8] Jan L. Camenisch, Jean-Marc Piveteau, Markus A.Stadler Blind signatures based on the discrete logarithm problem.—Institute for Theoretical Computer Science ETH Zurich