Развернутый отчет по проекту РФФИ № 12-07-31164

Методы повышения безопасности криптографических механизмов аутентификации и алгоритмов цифровой подписи в технологиях электронного документооборота

Код и название конкурса: мол_а Конкурс научных проектов, выполняемых молодыми учеными (Мой первый грант)

Год представления отчета: 2013

Вид отчета: итоговый

Полное название организации:

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина)"

Руководитель:

Новикова Евгения Сергеевна, к.т.н.

Исполнители:

Гурьянов Денис Юрьевич, к.т.н.

Демьянчук Анна Алексеевна

Молдовян Дмитрий Николаевич

Мондикова Яна Александровна

Аннотация

Важным моментом для практического применения криптографических алгоритмов является их безопасность, которая во многом определяется некоторой вычислительно трудной задачей, лежащей в основе криптографического алгоритма. В настоящем отчете представлен и обоснован подход к построению криптосхем на основе трудности задачи дискретного логарифмирования по трудно разложимому модулю. В работе показано, что в рамках предложенного подхода повышается безопасность криптосхем по сравнению со схемами, использующих ЗФ или ЗДЛ по простому модулю. По сравнению с ранее известными подходами к синтезу криптосхем, основанных на трудности одновременного решения ЗФ и ЗДЛ по простому модулю предложенный подход обеспечивает существенное сокращение размера цифровой подписи и высокую вычислительную эффективность. Был также разработан механизм расщепления сообщения, обеспечивающий возможность применения предложенного подхода для проектирования алгоритмов коммутативного шифрования и расшифрования.

В рамках данного подхода были разработан ряд криптографических протоколов:

1. протокол электронной цифровой подписи, взлом которых требует решения двух вычислительно трудных задач, обеспечивающих малую длину генерируемой подписи;

2. новый протокол открытого распределения ключей.

3. новые протоколы групповой и слепой электронной цифровой подписи.

4. новый протокол слепой коллективной подписи.

5. новый алгоритм коммутативного шифрования.

Сформулированы требования к выбору системных параметров, обеспечивающих заданный уровень сложности, доказана их вычислительная эффективность.

3.4. Объявленные ранее цели проекта на 2013

В проекте была заявлена следующая цель: расширение набора криптографических средств аутентификации электронной информации, обеспечивающий высокий уровень безопасности. Для этого должны быть получены следующие частные результаты:
1) разработка протоколов слепой коллективной цифровой подписи, основанных на трудности одновременного решения задачи факторизации и дискретного логарифмирования по простому модулю;
2) разработка протоколов аутентификации удаленных абонентов телекоммуникационной системы с нулевым разглашением секрета, основанных на трудности одновременного решения задачи факторизации и дискретного логарифмирования по простому модулю;
3) разработка алгоритма коммутативного шифрования на основе двух трудных задач -- факторизации и дискретного логарифмирования;
4) разработка протокола открытого шифрования на основе двух трудных задач -- факторизации и дискретного логарифмирования.

3.5. Степень достижения поставленных в проекте целей

Заявленные цели достигнуты в полной мере, результатом чего явилось получение следующих результатов:

1. Разработан новый подход к синтезу криптосхем, основанных на трудности одновременного решения двух вычислительно трудных задач – задачи факторизации и задачи дискретного логарифмирования по простому модулю и обеспечивающих малую длину генерируемой подписи.

2. Сформулированы требования к выбору параметров криптосхем, основанных на трудности одновременного решения задачи факторизации и задачи дискретного логарифмирования.

3. Разработан новый протокол открытого распределения ключей.

4. Разработаны новые протоколы групповой и слепой электронной цифровой подписи.

5. Разработан новый протокол слепой коллективной подписи.

6. Разработан новый алгоритм коммутативного шифрования.

3.6. Полученные в 2013 важнейшие результаты

Основным результатом за 2013 является разработка криптографических протоколов, *обеспечивающих функциональность* телекоммуникационной системы и *основанных на подходе*, разработанного в рамках данного проекта:

1. *протокол аутентификации удаленных абонентов телекоммуникационной системы с нулевым разглашением секрета на основе двух вычислительно трудных задач;*
2. *алгоритм коммутативного шифрования на основе двух вычислительно трудных задач;*
3. *протокол открытого шифрования на основе двух вычислительно трудных задач;*
4. *протокол слепой коллективной цифровой подписи, в основе которого лежат две вычислительно трудные задачи.*

В основе разработанных протоколов лежит задача дискретного логарифмирования по трудно разложимому модулю n, которая при соответствующем выборе простых делителей модуля для своего решения требует решения независимых задач факторизации и дискретного логарифмирования по простому модулю. Благодаря использованию составного модуля специальной структуры в качестве системного параметра криптопротоколов достигается снижение

размера формируемой ЭЦП, передаваемого объема данных при аутентификации пользователей и повышается безопасность применения ,т.к. вскрытие секретных параметров участников протокола требует одновременного умения решать две качественно разные вычислительно трудные задачи. Кроме того, были сформулированы основные требования к выбору системных параметров протоколов и способ их формирования. Например, для протоколов коллективной подписи, открытого распределения ключей, коллективной слепой ЭЦП составной модуль *n* должен быть сформирован удостоверяющим центром, а для протоколов обычной и слепой подписи, открытого шифрования и протокола с нулевым разглашением предпочтительным вариантом использования на практике является генерация трудно разложимого модуля самим пользователем, поскольку в этом случае устраняются атаки с участием недобросовестного доверительного центра. Однако при этом этот параметр, являясь уникальным для каждого пользователя, должен быть включен в состав открытого ключа пользователя, и в результате длина открытого ключа увеличивается.

1. Протокол аутентификации удаленных пользователей с нулевым разглашением секрета.

Протоколы с нулевым разглашением используются в процедурах строгой аутентификации удаленных абонентов телекоммуникационных систем. Термин "нулевое разглашение секрета" подчеркивает, что при обмене информацией между доказывающим - пользователем, который доказывает свою подлинность - и проверяющим не происходит какой-либо утечки информации о личном секретном ключа доказывающего.

Основным отличием разработанного протокола с нулевым разглашением является использование трудно разложимого составного модуля *n*. Открытый ключ (ОК) пользователя в этом случае вычисляется по формуле y = α^x mod n. Доказывающий в ходе протокола показывает, что он знает секретный ключ x, соответствующий его ОК, многократно повторяя процедуру "заявка-запрос-ответ".

Один раунд протокола имеет следующий вид. Доказывающий выбирает текущий разовый секрет *k*, вычисляет значение $R = \alpha^k \bmod n$, которое играет роль разового ОК, и передает его проверяющему.

Проверяющий случайным образом выбирает значение бита e и направляет его доказывающему (случайный запрос проверяющего).

Доказывающий направляет проверяющему ответ w в виде числа, вычисляемого по формуле $w = x + k \bmod \gamma$, и направляет его проверяющему.

Проверяющий проверяет выполнимость соотношения $\alpha^w \equiv y^e R \bmod n$. При положительной проверке делается заключение, что доказывающий знает значение x.

С целью уменьшения большого числа интерактивных шагов было предложено использовать *трехпроходный* протокол с нулевым разглашением, в котором ОК доказывающего является набор из *h* значений y_i, $i = 0, 1, 2, \ldots, h-1$, вычисленных по формуле $y_i = \alpha^{x_i} \bmod n.$, где x_i, $i = 0, 1, 2, \ldots, h-1$, составляют личный секретный ключ доказывающего..

Трехшаговый протокол включает следующие шаги.

1. Доказывающий выбирает случайное число *k* такое, что $1 < k < \gamma$, вычисляет значение $R = \alpha^k \bmod n$ и посылает его проверяющему (значение *R* называется фиксатором).

2. Проверяющий отправляет доказывающему запрос в виде случайной равновероятной h-битовой строки $E = (e_0, e_1, \ldots, e_{h-1})$, в которой каждый бит e_i с вероятностью 0,5 равен 1.

3. Доказывающий вычисляет ответ *W* на запрос E по формуле $W = k + \sum_{i=0}^{h-1} x_i e_i \bmod \gamma$ и направляет его проверяющему.

Проверяющий считает ответ положительным, если выполняется соотношение

$$\alpha^W = R \prod_{i=0}^{h-1} y_i^{e_i} \bmod n.$$

Легко показать, что вероятность обмана проверяющего в этом протоколе составляет 2^{-h}.

2. Алгоритм коммутативного шифрования на основе двух вычислительно трудных задач

Алгоритмы коммутативного шифрования используются для решения ряда специфических задач информационных технологий, таких как построение протоколов бесключевого шифрования и игры в покер по телефону. Разработанный в рамках проекта протокол *отличается* от существующих тем, что для его взлома необходимо одновременно решить две вычислительно трудные задачи - задачу факторизации (ЗФ) и задачу дискретного логарифмирования (ЗДЛ).

При проектировании данного протокола в рамках предложенного подхода основной задачей являлось определение системных параметров протокола и индивидуальных ключей пользователей. Это связано с тем, что значение модуля вычислений не может использоваться в качестве секретного ключа или его части, поскольку вычисление по различным модулям не обладает свойством коммутативности. Его значение должно быть общим системным параметром алгоритма, известным всем пользователям. Поскольку предполагается, что стойкость алгоритма основывается на трудности ЗФ, то значение n должно вырабатываться некоторым доверительным центром, который уничтожит случайно сгенерированные им сильные простые числа q и r после вычисления числа $n = qr$. Поскольку значения q и r являются для пользователей недоступными, то для них является вычислительно невозможным вычисление функции Эйлера $\varphi(n) = (q - 1)(r - 1)$ от числа n, что позволило бы вычислить пару значений e и d, таких, что $ed = 1 \bmod \varphi(n)$, которые могли бы быть использованы в качестве ключей шифрования/расшифрования пользователя. Для нахождения пары значений, которая позволила бы выполнять коммутативное шифрование, было предложено использовать механизм формирования числа α, порядок которого по модулю n равен достаточно большому простому числу γ (размером не менее 160 бит), удовлетворяющему следующим условиям делимости: $\gamma | q - 1$ и $\gamma | r - 1$. Эти условия сохраняют высокую трудность ЗФ модуля n при известных значениях α и γ. Тогда каждый пользователь генерирует случайное значение $e < \gamma$ и вычисляет значение $d = e^{-1} \bmod \gamma$. Пара значений e и d составляет ключ шифрования и расшифрования, соответственно.

Однако в этом случае механизм коммутативного шифрования работает корректно только для сообщений, которые могут быть описаны следующим образом: $\alpha^i \bmod n$, где $i = 1, 2, \ldots, \gamma$. Для устранения этого недостатка был адаптирован механизм *расщепления* сообщения. Сообщение M можно представить в виде пары чисел (C, K), причем C – число произвольного вида, а $K \in \{\alpha^1 \bmod n, \alpha^2 \bmod n., \ldots, \alpha^\gamma \bmod n\}$. Для вычисления пары (C, K) пользователь должен выбрать случайное число $k < \gamma$ и вычислить значение $K = \alpha^k \bmod n$; параметр C вычисляется по формуле $C = M + K \bmod n$.

Имеются два варианта алгоритма коммутативного шифрования, разработанных в рамках проекта. В первом случае операции шифрования/расшифрования производятся только над элементом K, который возводится в соответствующую степень по модулю n. Данная схема коммутативного шифрования становится основанной на трудности **одновременного решения двух независимых трудных задач --** ЗФ и ЗДЛ по простому модулю, если выбрать значения размера делителей числа n такими, что их отношение равно 1:2 при размере меньшего делителя, равном 512 бит и более, т.е. если применить подход разрабатываемый в настоящем проекте.

Алгоритм шифрования в этом случае имеет следующий вид.

1. Первичное шифрование сообщения M выполняется как расщепление M: $M = (C, K)$ и шифрование значения K: $S = K^e \bmod n$. На выходе первичной процедуры шифрования имеем пару значений (C, S).

2. Последующие шаги зашифрования/расшифрования выполняются как шифрование значения S.

3. Завершающий шаг расшифрования выполняется как расшифрование значения S, приводящее к восстановлению значения K, выбранного на шаге первичного шифрования сообщения, и вычисление значения M по формуле $M = C - K \bmod n$.

Второй вариант алгоритма коммутативного шифрования предполагает использование двух вычислительно трудных задач в явном виде. Для этого каждый пользователь выбирает две пары ключей (e_1, d_1) и (e_2, d_2), удовлетворяющих условиям $e_1 d_1 = 1 \bmod \gamma$ и $e_2 d_2 = 1 \bmod p - 1$.

Шифрование первого значения *C* в паре расщепления выполняется по первой паре подключей как возведение в степень e_1 (зашифрование) или d_1 (расшифрование) по модулю *p*. Шифрование второго значения K в паре расщепления выполняется по второй паре подключей как возведение в степень e_2 (зашифрование) или d_2 (расшифрование) по модулю *n*. Нетрудно видеть, что взлом данного алгоритма коммутативного шифрования требует одновременного решения ЗФ и ЗДЛ в конечном простом поле. Шифрование второго элемента пары расщепления осуществляется как возведение в степень по модулю *n*, поэтому можно говорить не о ЗФ, а о ЗДЛ по трудно разложимому модулю *n*. Однако эта задача принципиально отличается от ЗДЛ по простому модулю, причем алгоритм решения ЗДЛ модулю *n* может быть использован для факторизации значения модулю *n*.

Алгоритм шифрования в этом случае имеет следующий вид.

1. Первичное зашифрование сообщения *M* выполняется как расщепление *M*: *M* = (*C*, *K*) и зашифрование значения *K* по формуле $S = K^{e_2} \bmod n$ и значения *C* по формуле *C** = $C^{e_1} \bmod p$. На выходе первичной процедуры шифрования имеем пару значений (*C**, *S*).

2. Последующие шаги зашифрования/расшифрования выполняются как шифрование значения *S* путем выполнения операции возведения в степень по модулю *n* и шифрование значения C^* путем выполнения операции возведения в степень по модулю *p*.

3. Завершающий шаг расшифрования выполняется как расшифрование значения *S*, приводящее к восстановлению значения *K*, расшифрование значения *C**, приводящее к восстановлению значения *C*, и вычисление значения *M* по формуле $M = C - K \bmod n$.

Протокол открытого шифрования

Используя ОК некоторого пользователя, можно послать секретное сообщение этому пользователю по открытым каналам связи. Для этого сообщение следует зашифровать по ОК, применяя алгоритм, построенный по аналогии с алгоритмом открытого шифрования Эль-Гамаля и ***отличающийся*** от него использованием трудно разложимого модуля.

1. Сгенерировать случайное число *k*.
2. Вычислить число $R = \alpha^k \bmod n$.
3. Используя ОК получателя *y*, вычислить значение $Q = y^k \bmod n$.
4. Зашифровать сообщение *M* путем умножения сообщения на значение *Q*, играющее роль разового ключа шифрования: $C = QM \bmod n$.
5. Отправить получателю криптограмму в виде пары чисел (*R*, *C*).

Получатель криптограммы (*R*, *C*), используя свой личный секретный ключ *x*, выполняет процедуру дешифрования сообщения *M*, которая описывается следующими шагами.

1. Вычислить разовый общий секретный ключ $Q' = R^x \bmod n$.
2. Используя расширенный алгоритм Евклида, вычислить значение Q'^{-1}, обратное значению *Q'* по модулю *n*. (Легко показать, что число *Q'* является взаимно простым с модулем *n*, поэтому обратное значение Q'^{-1} существует и легко вычисляется с помощью расширенного алгоритма Евклида.)
3. Расшифровать сообщение *M* путем умножения значения *C* на целое число Q'^{-1}: $M = CQ'^{-1} \bmod n$.

Прокол слепой коллективной подписи

Для построения протокола слепой коллективной подписи, основанной на рудности одновременного решения задачи дискретного логарифмирования по простому модулю и задачи факторизации в качестве базовой криптосхемы был использован протокол коллективной ЭЦП, разработанный в ходе решения исследовательских задач по плану 2012

Протокол слепой коллективной ЭЦП необходим в случаях, когда в технологии тайного электронного голосования электронный бюллетень предоставляется голосующим сразу в несколько независимых коллекторных пунктов, действующих от имени избирательного комитета. В протоколе коллективной подписи системные параметры (*n*, α, γ) протокола генерируются

доверительным центром, а открытые ключи y_i соответствующие им личные секретные ключи (ЛСК) x_i m пользователей, где (i = 1, 2,…, m), выбираются согласно следующим требованиям.

Выбор параметров протокола. В разработанном протоколе используется ОК, представляемый в виде тройки чисел {n, α, y}, где y вычисляется по следующей формуле

$$y = \alpha^x \bmod n.$$

Личным секретным ключом (ЛСК) пользователя является тройка чисел (r, q, x), где $n = rq$, q – простое 1024-битовое число, r – простое 512-битовое число, x – случайное число, меньшее, чем порядок числа α по модулю n, который обозначим как число γ. При этом удовлетворяются следующие два требования.

1. Простые числа r и q имеют следующую структуру: $r = N_r\gamma + 1$ и $q = N_q\gamma + 1$, где N_r и N_q – два больших четных числа, содержащих большой простой делитель. Параметр γ имеет размер не менее 160 бит и не является секретным.

2. Простые числа r и q представляются в виде $r = N_r\gamma' + 1$ и $q = N_q\gamma'' + 1$, где N_r и N_q –два больших четных числа, содержащих большой простой делитель. Значение порядка числа α равно $\gamma = \gamma'\gamma''$. Каждое из чисел γ' и γ'' имеет размер не менее 80 бит, а параметр γ является дополнительным элементом секретного ключа.

Базовый протокол коллективной ЭЦП.

1. Участники протокола вычисляют коллективный ОК $Y = Y_1Y_2...Y_m \bmod n$

1. Каждый i-ый пользователь формирует случайное число $k_i < \gamma$ и вычисляет значение $R_i = \alpha^{k_i} \bmod n$ и рассылает его остальным пользователям.

2. Пользователи вычисляют общий рандомизирующий параметр $R = R_1R_2...R_m \bmod n$ и первый элемент коллективной подписи $E = F_H(M, R, Y)$.

3. Каждый i-ый пользователь вычисляет свою долю во втором элементе коллективной подписи: $S_i = k_i + x_iE \bmod \gamma$ и рассылает ее остальным пользователям.

4. После этого пользователи вычисляют второй элемент коллективной подписи (E, S) по формуле $S = S_1 + S_2 + ... + S_m \bmod \gamma$.

Проверка подлинности коллективной подписи (E, S) к сообщению M выполняется следующим образом.

1. Вычислить коллективный ОК $Y = Y_1Y_2...Y_m \bmod n$ и значение $\tilde{R} = y^{-E}\alpha^S \bmod n.$

2. Вычислить значение $\tilde{E} = F_H(M, \tilde{R}, Y)$. Если $\tilde{E} = E,$ то подпись признается подлинной.

Разработанный протокол слепой коллективной ЭЦП описывается следующим образом.

1. Некоторый пользователь инициирует взаимодействие с подписантами (лица которые должны подписать некоторое сообщение M вслепую).
2. Каждый i-ый подписант формирует случайное число $k_i < \gamma$ и вычисляет значение $R_i = \alpha^{k_i} \bmod n$ и рассылает его остальным подписантам.
3. Участники протокола вычисляют общий рандомизирующий параметр $\overline{R} = R_1R_2...R_m \bmod n$ и отправляют его пользователю.
4. Пользователь генерирует случайные числа τ и ε (ослепляющие параметры, не превосходящие γ) и вычисляет значения $R = \overline{R}y^\tau\alpha^\varepsilon \bmod n$, $E = F_H(M, R)$ и $\overline{E} = E + \tau \bmod \gamma$, после чего отправляет подписантам значение $\overline{E}$, которое является первым элементом слепой коллективной подписи. Значение E является первым элементом коллективной подписи к сообщению M и остается неизвестным для подписантов.

5. Каждый *i*-ый участник протокола вычисляет значение $\overline{S}_i$, такое что $R_i = y^{-\overline{E}}\alpha^{\overline{S}_i} \bmod n$: $\overline{S}_i = k_i + x_i\overline{E} \bmod \gamma$), и рассылает значение $\overline{S}_i$ остальным подписантам.
6. После этого подписывающие вычисляют второй элемент слепой коллективной подписи ($\overline{E}.$, $\overline{S}$) по формуле $\overline{S} = \overline{S}_1 + \overline{S}_2 + ... + \overline{S}_m \bmod \gamma$ и отправляют значение $\overline{S}$ пользователю.
7. Пользователь вычисляет второй элемент подписи (*E, S*) к сообщению *M* по формуле $S = \overline{S} + \varepsilon \bmod \gamma$.

Проверка подлинности коллективной подписи (*E*, *S*) к сообщению *M* выполняется следующим образом.

1. Вычислить коллективный ОК $Y = Y_1Y_2...Y_m \bmod n$ и значение $\widetilde{R} = y^{-E}\alpha^{S} \bmod n.$

2. Вычислить значение $\widetilde{E} = F_H\left(M, \widetilde{R}, Y\right)$. Если $\widetilde{E} = E,$ то подпись признается подлинной.

Корректность разработанного прокола слепой коллективной подписи доказывается путем подстановки значения (*E, S*) на вход процедуры проверки подлинности ЭЦП:

$$\widetilde{R} \equiv y^{-E}\alpha^{S} \equiv y^{-\overline{E}+\tau}\alpha^{\overline{S}+\varepsilon} \equiv y^{-\overline{E}}y^{\tau}\alpha^{\overline{S}}\alpha^{\varepsilon} \equiv \left(y^{-\overline{E}}\alpha^{\overline{S}}\right)y^{\tau}\alpha^{\varepsilon} \equiv \overline{R}y^{\tau}\alpha^{\varepsilon} \bmod n \Rightarrow$$

$$\Rightarrow \widetilde{R} = R \Rightarrow \widetilde{E} = E.$$

Предложенным протоколом анонимность пользователей обеспечивается тем, что произвольная коллективная подпись (*E*, *S*), сформированная подписантами, может быть сопоставлена с любой слепой подписью $\left(\overline{E}, \overline{S}\right)$. Действительно, если выполняются следующие равенства $R = y^{-E}\alpha^{S} \bmod n$ и $\overline{R} = y^{-\overline{E}}\alpha^{\overline{S}} \bmod n$, то верны и следующие сравнения $R/\overline{R} \equiv y^{\overline{E}-E}\alpha^{S-\overline{S}} \equiv y^{\tau}\alpha^{\varepsilon} \bmod n$, т. е. при равновероятном случайном выборе «ослепляющих» параметров τ и ε подпись (*E*, *S*) с равной вероятностью могла быть порождена из любой слепой коллективной подписи, формировавшейся когда-либо подписантами.

3.7. Степень новизны полученных результатов

Полученные результаты имеют мировую новизну: предложен новый подход к синтезу криптосхем, основанных на вычислительной трудности одновременного решения задачи факторизации и задачи дискретного логарифмирования.

Полученные результаты были представлены на российских и международных конференциях:

1. VIII Межрегиональная конференция "Информационная безопасность регионов России (ИБРР-2013)»,Санкт-Петербург, 23-25 октября 2013.
2. Международная конференция "Mathematical Methods, Models and Architectures for Computer Network Security 2012" (MMM-ACNS-2012)". Санкт-Петербург, 17–20 октября 2012 г
3. Всеармейская научно-практическая конференция «Инновационная деятельность в Вооруженных силах Российской Федерации». Санкт-Петербург, 29-30 ноября 2012
4. Санкт-Петербургская международная конференция "Региональная информатика -2012»,Санкт-Петербург, XX октября 2012

3.8. Сопоставление полученных результатов с мировым уровнем

Полученные результаты являются новыми и оригинальными, они основываются как на результатах, полученные непосредственно исполнителями ранее, так и на современных достижениях двухключевой криптографии. В сравнением с известными способами синтеза схем электронной цифровой подписи, основанных на трудности одновременного решения вычислительно трудных задач факторизации и дискретного логарифмирования по простому модулю, разработанный подход является новым и снимает ряд ограничений, что позволило *разработать криптографические протоколы других типов* на основе указанных двух задач и

существенно сократить размер цифровой подписи. Впервые разработаны следующие криптографические алгоритмы и протоколы, основанные на трудности одновременного решения двух вычислительно трудных задач – задачи факторизации и задачи дискретного логарифмирования по простому модулю: протокол открытого распределения ключей, протокол коллективной подписи, протокол слепой коллективной подписи, алгоритм коммутативного шифрования. Разработанные криптосхемы отличаются от существующих криптосхем, основанных на сложности решения двух вычислительно трудных задачах, более высоким уровнем быстродействия (в 2,5 и более раз, в зависимости от выбираемой для сравнения известной схемы ЭЦП) и сокращенной длиной подписи (от 5 до 17 раз, в зависимости от выбираемой для сравнения известной схемы ЭЦП).

3.9. Методы и подходы, использованные в ходе выполнения проекта (указать новизну и оригинальность)

Для достижения поставленной в проекте цели были использованы следующие два подхода:

1) использование задачи дискретного логарифмирования (ЗДЛ), заданной над конечным кольцом вычетов по составному модулю $n = rq$, где размер числа r равен 1024 бит, а размер числа q – 512 бит для построения криптографического протокола;

2) механизм "расщепления" сообщения, использующийся в алгоритме коммутативного шифрования.

Переход от простого модуля к составному означает, что в модифицированных криптосхемах используется трудность ЗДЛ по составному модулю, которая принципиально отличается от ЗДЛ по простому модулю. Для решения ЗДЛ по составному модулю можно использовать общие методы дискретного логарифмирования (метод больших и малых шагов, переборный метод, метод Полларда), имеющие экспоненциальную сложность, или метод сведения к ЗДЛ по простому модулю (имеющий субэкспоненциальную сложность) путем факторизации составного модуля и использования китайской теоремы об остатках. Можно также показать, что алгоритм вычисления дискретного логарифма по составному модулю n может быть использован для факторизации числа n. Это подтверждает принципиальное различие ЗДЛ по простому и составному модулям.

Если будут найдены прорывные решения задачи факторизации (ЗФ), то ЗДЛ по составному модулю n потребует решения ЗДЛ по простым модулям q и r. Так как размер числа r в два раза больше размера q, то основной вклад в трудоемкость дискретного логарифмирования в рассматриваемом случае будет вносить ЗДЛ по простому модулю r. При 1024-битовом размере числа r трудоемкость ЗДЛ о модулю r равна 2^{80} операций модульного умножения. Это обеспечит 80-битовую стойкость криптосхем, основанных на трудности ЗДЛ по модулю n даже в случае появления прорывных алгоритмов факторизации. Если будут найдены прорывные решения ЗДЛ по простому модулю, то эти методы смогут быть применены для взлома предлагаемых криптосхем только после решения ЗФ модуля n. Таким образом для взлома предлагаемых криптосхем потребуется решить как ЗФ, так и ЗДЛ по большому простому модулю r.

Использование предложенного подхода позволяет *значительно снизить* сложность вычислительных процедур проверки подписи и *сократить* длину цифровой подписи *по сравнению* с существующими криптопротоколами, основанными на сложности решения задачи факторизации и задачи дискретного логарифмирования одновременно.

Механизм "расщепления" сообщений был разработан для создания алгоритмов коммутативного шифрования и дешифрования. Использование составного модуля n в качестве системного параметра накладывает определенные ограничения на вид шифруемого сообщения, в частности, оно должно быть представимо в виде : $\alpha^i \bmod n$, где α является генератором группы простого порядка γ, являющегося делителем $\varphi(n)$, а $i = 1, 2, \ldots, \gamma$. Идея механизма

расщепления заключается в представлении произвольного сообщения в виде пары числе (C, K), где C - число произвольного вида, а K имеет вид $\alpha^i \bmod n$. Операции шифрования/дешифрования осуществляются над параметром K.

3.10.1.1 Количество научных работ, опубликованных в ходе выполнения Проекта (для Отчетов по продолжающимся Проектам – за 2013 год, для итоговых Отчетов – за весь период выполнения Проекта, цифрами)

10

3.10.1.2 Из них включенных в перечень ВАК

1

3.10.1.3. Из них включенных в системы цитирования *(Web of Science, Scopus, Web of Knowledge, Astrophysics, PubMed, Mathematics, Chemical Abstracts, Springer, Agris, GeoRef)*

1

3.10.2. Количество научных работ, подготовленных в ходе выполнения Проекта и принятых к печати в 2013 году (цифрами)

3.11. Участие в научных мероприятиях по тематике Проекта, которые проводились при финансовой поддержке Фонда *(указать только количество мероприятий – цифрами)*

0

3.12. Участие в экспедициях по тематике Проекта, которые проводились при финансовой поддержке Фонда *(указать только количество экспедиций – цифрами)*

0

3.13. Финансовые средства, полученные от РФФИ *(указать общий объем, в руб.)*

300 тыс. руб (за 2013 год)

3.14. Адреса *(полностью*) **ресурсов в Интернете, подготовленных авторами по данному проекту, например, http://www.somewhere.ru/mypub.html** *(если адресов несколько – для них последовательно заполняются подпункты 3.14.1; 3.14.2 и т.д.)*

http://www.comsec.spb.ru/en/staff/novikova

3.15. Библиографический список всех публикаций по проекту за весь период выполнения проекта, в порядке значимости: монографии, статьи в научных изданиях, тезисы докладов и материалы съездов, конференций и т.д. *(к отчету за второй год выполнения проекта – список публикаций за два*

1. Moldovyan A., Moldovyan N. and Novikova E. Blind 384-bit Digital Signature Scheme // Springer LNCS.vol. 7531.2012. PP 77-83/ 6th Int. Conference MMM-ACNS'12. St.Petersburg, Russia October 17-20.

2. Демьянчук А.А., Молдовян Д.Н., Новикова Е.С., Гурьянов Д.Ю. Подход к построению криптосхем на основе нескольких вычислительно трудных задач // Информационно-управляющие системы. Санкт-Петербург. № 2. 2013 С. 60-66.

3. А.А. Демьянчук, Березин А.Н. Молдовян Д.Н., Рыжков А.В. Протоколы аутентификации с нулевым разглашением секрета: приложения, повышение безопасности и новые реализации. // Труды XIII Санкт-Петербургской международной конференции "Региональная информатика "РИ-2012". 24-26 октября 2012, г. Санкт-Петербург / СПб.: СПОИСУ, 2013. С. 125-130.

4. Демьянчук А.А., Молдовян Д.Н., Новикова Е.С. Протоколы с нулевым разглашением типа «запрос – ответ»// Инновационная деятельность в Вооруженных силах Российской Федерации:

Труды юбилейной всеармейской научно-практической конференции. 29-30 ноября 2012, г. Санкт-Петербург / СПб.: ВАС, 2012. С. 144-148.

5. Гурьянов Д.Ю., Костина А.А., Краснова А.И., Молдовян Д.Н. Протокол цифровой подписи на основе операций многоуровневого возведения в степень // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 29-30 ноября 2012, г. Санкт-Петербург / СПб.: ВАС, 2012. С. 114-119.

6. Гурьянов Д.Ю., Демьянчук А.А., Мондикова Я.А. Протокол строгой аутентификации на основе процедуры последовательного возведения в квадрат // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 29-30 ноября 2012, г. Санкт-Петербург / СПб.: ВАС, 2012. С. 111-113.

7. Демьянчук А.А. Приложения протоколов с нулевым разглашением // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 29-30 ноября 2012, г. Санкт-Петербург / СПб.: ВАС, 2011. С. 140-143.

8. Новикова Е.С., Мондикова Я. А. Об особенностях разработки практических работ по теме "Слепая цифровая подпись" для дисциплины "Криптографические протоколы"// XIX Международная научно-методическая конференция «Современное образование: содержание, технологии, качество», 24 апреля 2013г. Материалы конференции. Том 1. СПб. ООО "Технолит", 2013. С. 135-136.

9. Березин А.Н., Демьянчук А.А. Расширенное изложение протоколов с нулевым разглашением секрета в дисциплине "Криптографические протоколы"// XIX Международная научно-методическая конференция «Современное образование: содержание, технологии, качество», 24 апреля 2013г. Материалы конференции. Том 1. СПб. ООО "Технолит", 2013. С. 138-140.

10. Демьянчук А.А., Новикова Е.С., Молдовян Д.Н. Способ повышения уровня безопасности протоколов аутентификации с нулевым разглашением секрета// Материалы VIII СПб межрегион. конф.«Информационная безопасность регионов России (ИБРР-2013)»,СПб, 23-25 окт.2013.-51-52.