УДК 681.3

ПОДХОД К ПОСТРОЕНИЮ КРИПТОСХЕМ НА ОСНОВЕ НЕСКОЛЬКИХ ВЫЧИСЛИТЕЛЬНО ТРУДНЫХ ЗАДАЧ

А. А. Демьянчук,
младший научный сотрудник
Д. Н. Молдовян,
младший научный сотрудник
Санкт-Петербургский институт информатики и автоматизации РАН
Е. С. Новикова,
канд. техн. наук, ассистент
Д. Ю. Гурьянов,
канд. техн. наук, ассистент
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Предлагается подход к построению криптосхем, основанных на двух вычислительно трудных задачах, который обеспечивает формирование подписи небольшой длины. Определены требования к выбору системных параметров криптосхем и личных ключей пользователя. Разработанный способ построения криптосхем обладает свойством универсальности и может быть применим для построения протоколов различного типа, таких как протокол открытого распределения ключей, протокол аутентификации с нулевым разглашением секрета.

Ключевые слова *— электронная цифровая подпись, протокол открытого шифрования, протокол обмена ключами, задача дискретного логарифмирования, задача факторизации.*

Введение

В основе криптосистем с открытым ключом (ОК), например протоколов электронной цифровой подписи (ЭЦП), лежит некоторая трудная математическая задача, которая определяет верхнюю границу безопасности соответствующей схемы. Криптосистемы такого типа используются для защиты и аутентификации информации в информационно-телекоммуникационных системах при условии, что неизвестны алгоритмы взлома криптосхемы и вероятность появления в обозримом будущем практически реализуемых прорывных решений используемой трудной задачи является достаточно малой. В настоящее время на практике наиболее широко используются две трудные задачи: 1) задача факторизации (ЗФ) целых чисел специального вида и 2) задача дискретного логарифмирования (ЗДЛ) по простому модулю (т. е. в простом конечном поле). Данные задачи независимы, и вероятность появления прорывного решения каждой из них в обозримом будущем имеет достаточно низкое значение. Для повышения безопасности алгоритмов ЭЦП, достигаемого за счет снижения вероятности взлома путем применения качественно новых прорывных решений используемых трудных задач, в работах [1–3] предложены схемы ЭЦП, взлом которых требует одновременного решения ЗФ и ЗДЛ. В этих криптосхемах используется ЗДЛ по простому модулю p, имеющему специальную структуру: $p - 1 = erq$, где r и q — 512-битовые простые числа и e — четное число небольшого размера, а в качестве основания дискретных логарифмов выбирается число, имеющее порядок $n = rq$. Параметры r и q являются элементами секретного ключа, а значения p, α и y, где $y = \alpha^x \bmod p$ (x — элемент секретного ключа), составляют ОК. Один из элементов подписи вычисляется по модулю n, поэтому суммарный размер ЭЦП превышает 1024 бит. Данный подход применяется для построения протоколов слепой ЭЦП [3–5], открытого шифрования и открытого согласования ключей [6]. Однако предложенные в работах схемы характеризуются сложностью построения и большой длиной вырабатываемой подписи.

В настоящей работе предлагается подход к построению криптосхем различного типа, основанных на трудности одновременного решения ЗФ и ЗДЛ по простому модулю. Использование

данного подхода обеспечивает снижение размера подписи в схемах ЭЦП и устраняет громоздкость построения криптографических протоколов других видов.

Подход к построению криптосхем

Для построения криптографических протоколов предлагается использовать ЗДЛ по трудно разложимому модулю n, для решения которой необходимо выполнить факторизацию составного модуля и решить ЗДЛ по простым модулям, являющимся делителями числа n, или применить один из общих методов дискретного логарифмирования (метод больших и малых шагов, переборный метод, метод Полларда [7]), используемых для решения ЗДЛ в любых конечных группах. Следует отметить, что общие методы становятся вычислительно нереализуемыми при сравнительно малых порядках конечной группы, равных примерно значению 2^{256}. Однако существование специальных методов решения ЗДЛ по простому модулю p, таких как метод вычисления индексов [7], обладающих субэкспоненциальной сложностью, требует использования в криптосхемах чисел p, имеющих достаточно большой размер, не менее 1024 бит. Появление прорывных специализированных методов решения ЗДЛ и ЗФ в обозримом будущем оценивается достаточно малыми значениями вероятности, тем не менее снижение вероятности взлома криптосхем в результате применения прорывных решений является важным моментом для криптосхем, применяемых на практике. Если криптосхема устроена таким образом, что для ее взлома требуется решить обе указанные задачи, то вероятность ее взлома существенно снижается, так как в этом случае необходима одновременная реализация двух маловероятных событий. Получение точных оценок рассматриваемых вероятностей проблематично, однако существенность указанного снижения вероятности взлома, основанного на прорывных решениях трудных задач, достаточно очевидна.

Следует отметить, что необходимость решать две трудные задачи практически не приводит к повышению стойкости криптосхем, поскольку при взломе криптосхемы задачи решаются независимо друг от друга. Однако если сложности решения ЗФ и ЗДЛ по простому модулю примерно равны, то появление прорывного решения одной из этих задач не приводит к снижению стойкости заданной криптосхемы. Известно, что ЗФ составного модуля n и ЗДЛ по простому модулю p имеют субэкспоненциальную сложность, причем сложности решения этих задач примерно одинаковы, если размеры чисел n и p равны и делители числа n имеют примерно одинаковый размер. Если делители числа n имеют различный размер, то сложность ЗФ определяется делителем меньшего размера [8]. Идея предлагаемого подхода состоит в построении криптосхем с использованием трудности ЗДЛ по трудно разложимому модулю n, для которого выполняется следующее условие: размер минимального делителя r модуля в 2 раза меньше разрядности второго делителя q. В этом случае сложность решения ЗФ примерно равна сложности ЗДЛ по простому модулю q. Построение криптосхем выполняется по аналогии с известными криптосхемами, основанными на трудности ЗДЛ по простому модулю, с учетом того, что значения оснований дискретных логарифмов следует выбирать таким образом, чтобы их нельзя было бы использовать для выполнения вычислительно осуществимых алгоритмов факторизации модуля n.

Выбор параметров криптосхем

В криптосхемах, создаваемых в рамках предложенного подхода, используется ОК, представляемый тройкой чисел $\{n, \alpha, y\}$, где y вычисляется по 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. Требования к генерации элементов секретного ключа рассмотрены в работе [9], где показано, что число α с достаточно малым значением порядка (требование малого порядка генератора группы α необходимо для построения схем ЭЦП с малым размером подписи) может быть использовано для факторизации числа n, если числа r, q и α не удовлетворяют одному из следующих двух требований.

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.

Генерация ОК и ЛСК в соответствии с одним из этих требований может быть легко выполнена [9], поэтому указанные требования не препятствуют практическому применению криптосхем на основе ЗДЛ по модулю n специальной структуры.

Криптографические протоколы, основанные на сложности ЗДЛ по трудно разложимому модулю

В этом разделе описаны протоколы ЭЦП, слепой подписи, коллективной подписи, а также протоколы открытого шифрования, открытого распределения ключей. Системные параметры и ключи пользователя, открытый и закрытый, формируются согласно требованиям, определенным в предыдущем разделе.

Протокол ЭЦП

Генерация подписи к сообщению M выполняется следующим образом.

1. Сформировать случайное число $k < \gamma$ и вычислить параметр $R = \alpha^k \bmod n$.

2. Используя некоторую специфицированную хэш-функцию F_H, вычислить ее значение от сообщения с присоединенным к нему числом R: $E = F_H(M, R)$. Параметр E является первым элементом подписи.

3. Вычислить второй элемент подписи: $S = k + xE \bmod \gamma$.

Проверка подлинности подписи (E, S) к сообщению M выполняется по ОК владельца подписи следующим образом.

1. Вычислить значение $\tilde{R} = y^{-E}\alpha^S \bmod n$.

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

Протокол слепой подписи

Протокол слепой подписи используется в тех случаях, когда пользователь желает получить подпись к сообщению M таким образом, чтобы подписывающий не мог впоследствии при получении M и соответствующей подписи идентифицировать этого пользователя. Протокол слепой подписи построен на основе алгоритма ЭЦП, описанного в предыдущем подразделе, и реализуется по аналогии со способом, впервые предложенным в работе [10], следующим образом.

1. Пользователь инициирует взаимодействие с подписывающим лицом.

2. Подписывающий генерирует случайное число k и вычисляет значение параметра $\bar{R} = \alpha^k \bmod n$, которое затем отправляет пользователю.

3. Пользователь генерирует случайные числа τ и ε (ослепляющие параметры, не превосходящие γ) и вычисляет значения $R = \bar{R}y^{\tau}\alpha^{\varepsilon} \bmod n$, $E = F_H(M, R)$ и $\bar{E} = E + \tau \bmod \gamma$, после чего отправляет подписывающему значение $\bar{E}$.

4. Подписывающий вычисляет значение $\bar{S}$ такое, что $\bar{R} = y^{-\bar{E}}\alpha^{\bar{S}} \bmod n$ (т. е. $\bar{S} = k + x\bar{E} \bmod \gamma$), и направляет $\bar{S}$ пользователю.

5. Пользователь вычисляет второй элемент подписи (E, S) к сообщению M по формуле $S = \bar{S} + \varepsilon \bmod \gamma$.

Процедура проверки подписи выполняется так же, как и в схеме ЭЦП. Подлинность подписи доказывается путем подстановки значения (E, S) на вход процедуры проверки подлинности:

$$\tilde{R} \equiv y^{-E}\alpha^S \equiv y^{-\bar{E}+\tau}\alpha^{\bar{S}+\varepsilon} \equiv$$

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

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

При этом проблема анонимности решена, поскольку произвольная подпись (E, S), сформированная подписывающим, может быть сопоставлена с любой слепой подписью $\left(\bar{E}, \bar{S}\right)$. Действительно, если выполняются равенства $R = y^{-E}\alpha^S \bmod n$ и $\bar{R} = y^{-\bar{E}}\alpha^{\bar{S}} \bmod n$, то верны и следующие сравнения: $R/\bar{R} \equiv y^{\bar{E}-E}\alpha^{S-\bar{S}} \equiv y^{\tau}\alpha^{\varepsilon} \bmod n$, т. е. при равновероятном случайном выборе «ослепляющих» параметров τ и ε подпись (E, S) с равной вероятностью могла быть порождена из любой слепой подписи, формировавшейся когда-либо подписывающим.

Следует отметить, что в данном протоколе приемлемы два варианта построения модуля n. В первом варианте параметр γ не является составным и входит в состав ОК пользователя, поскольку его раскрытие не может быть использовано для разложения модуля. Во втором варианте параметр γ является составным и является частью ЛСК пользователя. В этом случае вместо формул $\bar{E} = E + \tau \bmod \gamma$ и $S = \bar{S} + \varepsilon \bmod \gamma$ можно использовать формулы $\bar{E} = E + \tau \bmod 2^g$ и $S = \bar{S} + \varepsilon \bmod 2^g$ соответственно. В остальном описание протокола не меняется. В последних двух формулах значение g является специфицируемым параметром протокола и превосходит на единицу значение разрядности параметра γ.

Протокол коллективной ЭЦП

Протокол коллективной ЭЦП необходим в случаях, когда несколько пользователей должны одновременно сформировать подпись к документу. В настоящей работе предлагается протокол коллективной ЭЦП, аналогичный протоколам с формированием общего параметра рандомизации [11, 12], однако системные параметры (n, α, γ) протокола, генерируемые доверительным центром, и ОК y_i и ЛСК x_i m пользователей, где $i = 1, 2, ..., m$, вычисляются с учетом требований, определенных в предыдущем разделе. Протокол коллективной ЭЦП включает следующие шаги.

1. Участники протокола вычисляют коллективный ОК $Y = y_1 y_2 ... y_m \bmod n$.

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

3. Пользователи вычисляют общий рандомизирующий параметр $R = R_1 R_2 ... R_m \bmod n$ и первый элемент коллективной подписи $E = F_H(M, R, Y)$.

4. Каждый i-й пользователь вычисляет свою долю во втором элементе коллективной подписи: $S_i = k_i + x_i E \bmod \gamma$, и рассылает ее остальным пользователям.

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

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

1. Вычислить коллективный ОК $Y = y_1 y_2 \ldots y_m \bmod n$ и значение $\tilde{R} = Y^{-E} \alpha^S \bmod n$.

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

Используя в качестве прототипа протоколы, описанные в работах [13–15], легко разработать протокол коллективной слепой подписи, в котором общая тройка значений n, α и γ генерируется доверительным центром.

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 следующий алгоритм, построенный по аналогии с алгоритмом открытого шифрования Эль-Гамаля [16].

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 ЛСК 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}: $M = CQ'^{-1} \bmod n$.

Корректность описанной схемы шифрования легко доказать самостоятельно.

Протокол открытого распределения ключей

Для реализации протокола открытого распределения необходимо участие доверительного центра, который генерирует системные параметры протокола, отвечающие требованиям, определенным в предыдущем разделе. Пользователи генерируют случайный ЛСК в виде числа x и вычисляют свой ОК по формуле $y = \alpha^x \bmod n$. Протокол включает стандартные шаги схемы Диффи — Хеллмана.

1. Пользователь А вычисляет общий секретный ключ с удаленным пользователем В по ОК последнего y_B и своему ЛСК x_A по формуле $Z_{AB} = y_B^{x_A} \bmod n$.

2. Пользователь В вычисляет общий секретный ключ с пользователем А по ОК последнего y_A и своему ЛСК x_B по формуле $Z_{AB} = y_A^{x_B} \bmod n$.

В результате этих шагов оба пользователя получают одно и то же значение, которое известно только им, и для этого не потребовалось использовать защищенный канал связи.

Если атаку на протокол проводить с участием доверительного центра, то она окажется эффективной в случае появления прорывного решения ЗДЛ по простому модулю. Таким образом, стойкость протокола к таким атакам примерно равна его стойкости к атакам без участия доверительного центра, однако его безопасность существенно выше, если учесть вероятность взлома в результате появления прорывных решений трудных задач.

Протокол аутентификации с нулевым разглашением секрета

Протоколы с нулевым разглашением используются в процедурах строгой аутентификации удаленных абонентов телекоммуникационных систем. Пользователь, подлинность которого устанавливается, называется *доказывающим*. Пользователь, который проверяет подлинность доказывающего, называется *проверяющим*. Термин «*нулевое разглашение секрета*» подчеркивает, что при обмене информацией между доказывающим и проверяющим не происходит какой-либо утечки информации о ЛСК доказывающего.

Рассмотрим протокол с нулевым разглашением на основе сложности ЗДЛ по составному модулю n, в котором ОК вычисляется по формуле $y = \alpha^x \bmod n$. Доказывающий в ходе протокола показывает, что он знает ЛСК x, соответствующий его ОК. Протокол состоит из многократного выполнения следующего раунда.

1. Доказывающий выбирает текущий разовый секрет k, вычисляет значение $R = \alpha^k \bmod n$, которое играет роль разового ОК, и передает его проверяющему.

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

3. Доказывающий направляет проверяющему ответ w в виде числа, вычисляемого по формуле $w = ex + k \bmod \gamma$, 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. Нарушитель может дать правильный ответ с вероятностью 0,5, поэтому протокол включает в себя многократное выполнение описанного раунда, при котором достигается приемлемо малая вероятность обмана 2^{-h}, где h — число повторенных раундов.

С целью уменьшить большое число интерактивных шагов можно использовать трехшаговый протокол с нулевым разглашением, в котором ОК доказывающего является набор из h значений y_i, $i = 0, 1, 2, ..., h - 1$, вычисленных по формуле $y_i = \alpha^{x_i} \bmod n$. Набор чисел x_i, $i = 0, 1, 2, ..., h - 1$, составляет ЛСК доказывающего. Протокол включает три следующих шага.

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 $E = (e_0, e_1, ..., e_{h-1})$, 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}.

Описанный трехпроходный протокол с нулевым разглашением может быть преобразован в схему ЭЦП, пригодную для практического использования, по аналогии с построениями, выполненными в работе [17]. В таком преобразовании рассматривается следующий сценарий формирования цифровой подписи. Подписывающее лицо генерирует конкретное значение фиксатора R. Затем в зависимости от фиксатора и подписываемого документа M он вычисляет значение запроса E, после чего формирует ответ S на запрос. Пара чисел (E, S), включающая запрос и ответ, является цифровой подписью к документу. Для того чтобы подделка подписи была практически невозможной, схема ЭЦП строится таким образом, чтобы после вычисления значения запроса изменить значение фиксатора без изменения запроса было вычислительно трудно. Это требование может быть достигнуто путем задания запроса как значения стойкой хэш-функции, вычисляемой от значения фиксатора с присоединенным к нему сообщением. В этом значение запроса зависит от каждого бита фиксатора и каждого бита подписываемого документа, и без знания ЛСК формирование подписи становится вычислительно невыполнимым. Согласно описанному способу преобразования трехпроходного протокола с нулевым разглашением в протокол ЭЦП, алгоритм генерации ЭЦП включает следующие шаги.

1. Подписывающий выбирает случайное число k $(1 < k < \gamma)$, вычисляет значение фикатора $R = \alpha^k \bmod n$.

2. Затем, используя специфицированную хэш-функцию F_H, он вычисляет значение $E = F_H(M, R) = (e_0, e_1, ..., e_{h-1})$, которое может быть рассмотрено как случайный запрос со стороны документа.

3. Подписывающий вычисляет ответ S на запрос E по формуле $S = k + \sum_{i=0}^{h-1} x_i e_i \bmod \gamma$, который является вторым элементом цифровой подписи к документу M.

Проверка подлинности ЭЦП (E, S) состоит в проверке выполнимости соотношения $\alpha^S = R \prod_{i=0}^{h-1} y_i^{e_i} \bmod n$, которое является проверочным соотношением в исходном протоколе с нулевым разглашением. Процедура проверки подписи включает следующие шаги.

1. Вычисляется значение фиксатора

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

2. Вычисляется значение хэш-функции

$$\tilde{E} = F_H\left(M, \tilde{R}\right).$$

3. Сравниваются значения $\tilde{E}$ и E. Если $\tilde{E} = E$, то подпись (E, S) считается подлинной. В противном случае подпись отклоняется как ложная.

Нарушитель, который пытается подделать подпись, не может вычислить правильный ответ на запрос, формируемый по значению документа, поскольку ему неизвестен ЛСК. Однако он может попытаться сгенерировать случайные значения запроса $E' = \left(e'_0, e'_1, \ldots, e'_{h-1}\right)$ и ответа S' и вычислить по формуле $R' = \alpha^{S'} \prod_{i=0}^{h-1} y_i^{-e'_i} \bmod n$ значение фиксатора R', которое вместе со значениями E' и S' будет удовлетворять проверочному соотношению. С вероятностью 2^{-h} будет выполняться соотношение $E' = F_H(M, R')$, и подпись (E', S') пройдет процедуру проверки как подлинная подпись. Однако чтобы такая атака с вероятностью 50 % привела к удачной подделке подписи, потребуется сформировать примерно 2^{h-1} вариантов подписи (E', S'), поэтому при $h \geq 80$ атака вычислительно невыполнима в настоящее время.

Недостатком данной схемы ЭЦП является большой размер ОК, который составляет не менее $1536h = 122\,880$ бит. Сокращение размера ОК

можно достигнуть приемом, который состоит в том, что генерируется ЛСК в виде случайного числа x, по которому вычисляется значение $y_0 = \alpha^x \bmod n$, а значения y_i, $i = 1,..., h - 1$, определяются формулой $y_i = y_0^{2^i} = \alpha^{2^i x} = \alpha^{x_i} \bmod n$. Тогда в описанной схеме ЭЦП $x_i = 2^i x \bmod \gamma$ и выражение $S = k + \sum_{i=0}^{h-1} x_i e_i \bmod \gamma$ принимает вид $S = k + xE \bmod \gamma$, а выражение $\alpha^S = R\prod_{i=0}^{h-1} y_i^{e_i} \bmod n$ приводится к виду

$$\alpha^S = R\prod_{i=0}^{h-1} y_i^{e_i} = R\prod_{i=0}^{h-1} y_0^{2^i e_i} = Ry_0^{\sum_{i=0}^{h-1} 2^i e_i} = Ry_0^E \bmod n,$$

где битовая строка запроса E рассматривается как двоичное число. Заменяя обозначение y_0 на y, можно перейти к схеме ЭЦП, описываемой следующими шагами.

1. Подписывающий выбирает случайное число k ($1 < k < \gamma$), вычисляет значение фиксатора $R = \alpha^k \bmod n$.

2. Затем он, используя специфицированную хэш-функцию F_H, вычисляет первый элемент подписи в виде значения $E = F_H(M, R) = (e_0, e_1, ..., e_{h-1})$, которое рассматривается как двоичное число $E = \sum_{i=0}^{h-1} 2^i e_i$.

3. Подписывающий вычисляет ответ S на запрос E по формуле $S = k + xE \bmod \gamma$, который является вторым элементом цифровой подписи к документу M.

Процедура проверки подписи (E, S) включает следующие шаги.

1. Вычисляется значение фиксатора

$$\tilde{R} = y^{-E}\alpha^S \bmod n.$$

2. Вычисляется значение хэш-функции

$$\tilde{E} = F_H\left(M, \tilde{R}\right).$$

3. Сравниваются значения $\tilde{E}$ и E. Если $\tilde{E} = E$, то подпись (E, S) считается подлинной. В противном случае подпись отклоняется как ложная.

То есть получен протокол ЭЦП, описанный в первом подразделе. Его «вывод» из протокола с нулевым разглашением может быть использован как формальное доказательство его стойкости. Примеры такого доказательства приведены в работе [17].

Общее обсуждение предложенных криптосхем

Во всех криптографических протоколах и алгоритмах, описанных в предыдущем разделе, составной модуль n может быть сформирован доверительным центром. Для некоторых криптосхем это условие является обязательным (протоколы коллективной подписи, открытого распределения ключей, коллективной слепой ЭЦП), для других — альтернативным вариантом реализации (протоколы обычной и слепой подписи, алгоритм открытого шифрования, протокол с нулевым разглашением). Следует отметить, что в криптосхемах последнего типа генерация трудно разложимого модуля самими пользователями является предпочтительным вариантом использования, поскольку в этом случае устраняются атаки с участием недобросовестного доверительного центра. При этом параметры n и α являются уникальными для каждого пользователя и должны быть включены в состав ОК, чтобы предоставить к ним доступ другим пользователям. В результате размер ОК увеличивается.

При индивидуальной генерации модуля n и числа α значение γ может оставаться секретным. Для последнего случая можно использовать как простое 160-битовое значение γ, так и составное значение γ, равное произведению двух 80-битовых простых чисел γ' и γ''. В случае генерации модуля n и числа α доверительным центром последний должен также вычислить и сделать общедоступным значение порядка числа γ, поэтому вариант составного числа γ является неприемлемым. (Это связано с тем, что значение γ выбирается сравнительно малого размера, поэтому его можно разложить на множители, использование которых дает возможность достаточно просто факторизовать модуль n.)

В рассмотренных криптосхемах размеры их параметров выбирались с учетом обеспечения минимально приемлемой стойкости, оцениваемой как 2^{80} модульных умножений. Для обеспечения более высокого уровня стойкости размер параметров должен быть соответствующим образом увеличен.

В предложенных схемах ЭЦП обеспечивается достаточно малый размер подписи (≈ 240 бит). Производительность криптосхем примерно в 2,25 раза меньше производительности аналогичных известных криптосхем, использующих вычисления по простому 1024-битовому модулю. Однако, поскольку последние обладают высоким быстродействием, то это снижение производительности не является существенным для практического применения.

Заключение

В данной работе описан и обоснован подход к построению криптосхем на основе трудности ЗДЛ по трудно разложимому модулю. Показано, что в рамках предложенного подхода повышается безопасность криптосхем по сравнению со схемами, использующими ЗФ или ЗДЛ по простому модулю. Производительность разработанных схем снижается незначительно. По сравнению с ранее известными подходами к синтезу криптосхем, основанными на трудности одновременного решения ЗФ и ЗДЛ по простому модулю, предложенный подход обеспечивает существенное со-

кращение размера подписи в протоколах обычной, коллективной и слепой ЭЦП. Кроме того, он может быть использован для разработки других типов криптографических протоколов, взлом которых требует одновременного решения ЗФ и ЗДЛ по простому модулю.

В предложенных криптосхемах применяется циклическая подгруппа мультипликативной группы кольца вычетов по составному модулю. Значительный интерес представляет синтез криптосхем, построенных на нециклических подгруппах, а именно мультипликативных подгруппах с двухмерной цикличностью, т. е. подгруппах, базис которых содержит два элемента α и β, имеющих один и тот же простой порядок γ. В последнем случае элемент ОК y вычисляется по формуле $y = \alpha^x \beta^w \bmod n$, где значения x и w являются элементами ЛСК. Применение нециклических подгрупп такого типа описано в работах [18–20] для построения протокола слепой ЭЦП со сравнительно малым размером подписи, основанной на трудности задачи факторизации. Однако использование таких подгрупп для построения алгоритмов и протоколов, основанных на сложности одновременного решения ЗФ и ЗДЛ, не рассматривалось и представляет собой предмет отдельного обсуждения.

Работа выполняется при финансовой поддержке РФФИ (проект № 12-07-31164 мол_а).

Литература

1. **Дернова Е. С., Молдовян Н. А.** Синтез алгоритмов цифровой подписи на основе нескольких вычислительно трудных задач // Вопросы защиты информации. 2008. № 1. С. 22–26.
2. **Дернова Е. С., Молдовян Н. А.** Протоколы коллективной цифровой подписи, основанные на сложности решения двух трудных задач // Безопасность информационных технологий. 2008. № 2. С. 79–85.
3. **Tahat N. M. F., Shatnawi S. M. A., Ismail E. S.** New Partially Blind Signature Based on Factoring and Discrete Logarithms // J. of Mathematics and Statistics. 2008. Vol. 4(2). P. 124–129.
4. **Tahat N. M. F., Ismail E. S., Ahmad R. R.** A New Blind Signature Scheme Based on Factoring and Discrete Logarithms // Intern. J. of Cryptology Research. 2009. Vol. 1(1). P. 1–9.
5. **Кишмар Р. В., Молдовяну П. А., Новикова Е. С., Сухов Д. К.** Протоколы слепой подписи на основе сложности одновременного решения двух трудных задач // Изв. СПбГЭТУ «ЛЭТИ». 2011. № 4. С. 44–48.
6. **Молдовян Д. Н., Кишмар Р. В., Васильев И. Н.** Двухключевые криптосхемы на основе комбинирования задач факторизации и дискретного логарифмирования // Вопросы защиты информации. 2011. № 4. С. 2–5.
7. **Menezes A. J., Vanstone S. A.** Handbook of Applied Cryptography. — CRC Press, 1996. — 780 p.
8. **Коблиц Н.** Курс теории чисел и криптографии. — М.: ТВП, 2001. — 254 с.
9. **Moldovyan A. A., Moldovyan D. N., Gortinskaya L. V.** Cryptoschemes based on new signature formation mechanism // Computer Science J. of Moldova. 2006. Vol. 14. N 3(42). P. 397–411.
10. **Camenisch J. L., Piveteau J.-M., Stadler M. A.** Blind Signatures Based on the Discrete Logarithm Problem // Advances in Crypology — EUROCRYPT'94. Proc. / Lecture Notes in Computer Science. Springer Verlang, 1995. Vol. 950. P. 428–432.
11. **Молдовян А. А., Молдовян Н. А.** Новые алгоритмы и протоколы для аутентификации информации в АСУ // Автоматика и телемеханика. 2008. № 7. С. 157–169.
12. **Молдовян А. А., Молдовян Н. А.** Коллективная ЭЦП — специальный криптографический протокол на основе новой трудной задачи // Вопросы защиты информации. 2008. № 1. С. 14–18.
13. **Moldovyan N. A., Moldovyan A. A.** Blind Collective Signature Protocol Based on Discrete Logarithm Problem // Intern. J. of Network Security. 2010. Vol. 11. N 2. P. 106–113.
14. **Moldovyan N. A.** Blind Signature Protocols from Digital Signature Standards // Intern. J. of Network Security. 2011. Vol. 13. N 1. P. 22–30.
15. **Молдовян Н. А., Дернова Е. С., Молдовян Д. Н.** Протоколы слепой и коллективной подписи на основе стандарта ЭЦП ДСТУ 4145-2002 // Вопросы защиты информации. 2011. № 2. С. 14–18.
16. **ElGamal T.** A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory. 1985. Vol. IT-31. N 4. P. 469–472.
17. **Молдовян А. А., Молдовян Д. Н., Васильев И. Н., Головачев Д. А.** Протоколы с нулевым разглашением секрета и обоснование безопасности схем цифровой подписи // Вопросы защиты информации. 2011. № 4. С. 6–11.
18. **Молдовян Д. Н., Васильев И. Н., Латышев Д. М., Сухов Д. К.** Построение схемы 240-битовой цифровой подписи // Вопросы защиты информации. 2011. № 3. С. 6–10.
19. **Васильев И. Н., Краснова А. И., Молдовян Д. Н.** Схема слепой 240-битовой цифровой подписи // Информационно-управляющие системы. 2011. № 6(55). С. 49–53.
20. **Moldovyan A., Moldovyan N., Novikova E.** Blind 384-bit Digital Signature Scheme: 6th Intern. Conf. MMM-ACNS'12. St.-Petersburg, Russia, Oct. 17–20 // Springer LNCS. 2012. Vol. 7531. P. 77–83.