УДК 681.3

А. Н. Березин, Н. А. Молдовян

ПОСТРОЕНИЕ КРИПТОСХЕМ НА ОСНОВЕ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ ПО ТРУДНО РАЗЛОЖИМОМУ МОДУЛЮ

Дано обоснование построения алгоритмов и протоколов с открытым ключом на основе задачи дискретного логарифмирования по трудно разложимому модулю с целью повышения уровня безопасности. В качестве модуля предлагается использовать произведение двух сильных простых чисел, с отношением размеров 2:1. Данный подход дает альтернативные решения по синтезу криптосхем, основанных на вычислительной трудности одновременного решения задач факторизации и дискретного логарифмирования по простому модулю, обеспечивая снижение размера подписи в протоколах электронной цифровой подписи и повышение производительности криптосхем.

Криптографический протокол, цифровая подпись, слепая коллективная подпись, задача факторизации, задача дискретного логарифмирования, открытый ключ

Вычислительная сложность задачи дискретного логарифмирования (ЗДЛ), определяемой над конечными циклическими группами, широко используется для синтеза криптосхем с открытым ключом. Важнейшие практически используемые алгоритмы электронной цифровой подписи (ЭЦП) основаны на ЗДЛ на эллиптической кривой (ЭК), заданной над конечными полями. Существующие общие методы решения ЗДЛ, которые абстрагируются от конкретного вида групповой операции и элементов группы, имеют экспоненциальную трудоемкость. Наибольшая трудоемкость соответствует случаю, когда порядок группы является простым числом. Трудоемкость общих методов решения ЗДЛ (метод Полларда, метод больших и малых шагов) определяется наибольшим простым делителем порядка группы. Для решения ЗДЛ в конечном простом поле известны специальные методы решения, имеющие субэкспоненциальную сложность (метод вычисления индексов).

Практически отсутствуют публикации, посвященные синтезу криптосхем над ЗДЛ по трудно разложимому модулю $n = rq$. Известно, что ЗДЛ по модулю n имеет одинаковый порядок с суммарной трудностью задачи факторизации (ЗФ) числа n, ЗДЛ по модулю q и ЗДЛ по модулю r [1]. Лучший известный алгоритм факторизации числа n имеет субэкспоненциальную сложность, и при одинаковом размере чисел p и n трудоемкость ЗФ и трудоемкость ЗДЛ по модулю p имеют одинаковый порядок. Трудоемкость ЗДЛ по модулю q и ЗДЛ по модулю r на много порядков меньше трудоемкости ЗФ числа n, поскольку размер простых чисел q и r в 2 раза меньше размера n. Таким образом, реализация криптосхем над ЗДЛ по модулю n не дает выигрыша в стойкости, что предопределило сравнительно малый интерес к синтезу таких криптосхем.

В настоящей статье обосновывается возможность построения алгоритмов и протоколов с открытым ключом, основанных на трудности ЗДЛ по составному модулю n и обеспечивающих более высокий уровень безопасности.

Особенности задачи дискретного логарифмирования по составному модулю. Задача факторизации и ЗДЛ по простому модулю являются независимыми, тогда как ЗФ составного числа n и ЗДЛ по модулю связаны между собой, а именно алгоритм решения

последней имеет трудоемкость не ниже трудоемкости факторизации n (см. [1], с. 114), поскольку алгоритм решения ЗДЛ по модулю при случайно выбранном основании α может быть полиномиально модифицирован в алгоритм факторизации числа n (трудоемкость получаемого таким образом алгоритма полиномиально выражается через трудоемкость ЗДЛ по модулю n). Действительно, пусть для заданного значения y, принадлежащего циклической подгруппе, генерируемой степенями числа α, известен алгоритм вычисления числа x, такого, что выполняются условия $y = \alpha^x \bmod n$, $x < n$. Этот алгоритм может быть использован для факторизации n следующим образом.

Сгенерируем случайное число $X < n$ $(n - X << n)$, вычислим значение $y = \alpha^X \bmod n$, а затем с помощью рассматриваемого алгоритма – значение, такое, что $y = \alpha^x \bmod n$. Очевидно, что порядок числа α делит разность $X - x : \omega \mid X - x$. Последнее означает, что значение ω может быть найдено как один из делителей числа $X - x$. Если сильные простые числа q и r (делители числа n) не генерируются специальным образом, то число $X - x$ с вероятностью, близкой к 1, можно будет достаточно легко факторизовать, т. е. найти все его простые делители d_i, среди которых будут содержаться и все простые делители порядка ω. Если делитель d_i выбран достаточно большого размера, он с высокой вероятностью будет делить либо $q-1$, либо $r-1$, но не будет одновременно делить $q-1$ и $r-1$. Пусть $\omega \mid q-1$. Тогда число $\beta = \alpha^{(X-x)/d_i} \bmod n$ легко вычисляется и имеет порядок по модулю q, равный d_i, т. е. $\beta^{d_i} \equiv 1 \bmod q$. Также справедливо соотношение $\beta^{d_i} \equiv 1 \bmod n \rightarrow \beta^{d_i} \equiv 1 \bmod r$. Поскольку d_i не является порядком числа β по модулю r, то $\beta \equiv 1 \bmod r \rightarrow \beta^{d_i} \equiv 1 \bmod r \rightarrow r \mid \beta - 1$. Последнее соотношение показывает, что число n может быть факторизовано вычислением наибольшего общего делителя чисел n и $\beta - 1$. Таким образом, эффективный алгоритм решения ЗДЛ по модулю n модифицируется в эффективный алгоритм факторизации числа n. Однако это не касается частных специальных случаев, когда 1) функция Эйлера от числа n содержит 2 больших простых множителя и 2) числа $q-1$ и $r-1$ содержат одинаковый простой множитель γ, имеющий достаточно большой размер (160 бит и более), а число α имеет порядок по модулю n, равный γ. В первом случае делители числа n имеют вид $q = N_q q' + 1$ и $r = N_r r' + 1$, где q' и r' – простые числа размером не менее 512 бит; N_q и N_r – достаточно большие четные числа. В качестве α берется число, порядок которого $\omega = q'r'$. Решение ЗДЛ по модулю n позволит вычислить значение ω, однако нахождение делителей числа ω является ЗФ, имеющей субэкспоненциальную сложность. Таким образом, для факторизации n после решения ЗДЛ снова требуется решить ЗФ, но уже по отношению к числу ω меньшего размера. Однако выбранные размеры делителей ω таковы, что разложить ω на множители – практически невыполнимая задача при использовании лучшего известного алгоритма факторизации. Требование выбора в качестве N_q и N_r достаточно больших четных чисел связано с тем, чтобы сделать практически невыполнимым нахождение значения функции Эйлера

$\phi(n) = N_q N_r q'r'$ путем подбора возможных значений N_q и N_r при известном значении $\omega = q'r'$. По значению $\phi(n)$ легко вычисляются делители числа n (см. [2], с. 142). При размере чисел N_q и $\tilde{E} = F_H(M, \tilde{R}) \bmod \gamma$ равном 64 бит и более нахождение значения $\phi(n)$ описанным способом вычислительно невыполнимо. Во втором случае делители числа n имеют вид $q = N_q\gamma + 1$ и $r = N_r\gamma + 1$, где γ – простое число размером не менее 160 бит. В качестве α берется число, порядок которого равен $\omega = \gamma$ и для которого выполняются соотношения $\alpha \bmod q \neq 1$ и $\alpha \bmod r \neq 1$. Решение ЗДЛ по модулю n позволит вычислить значение γ, однако этого недостаточно для нахождения делителей числа n, поскольку $\text{НОД}\left(\alpha^i - 1, n\right) = 1$ для всех значений $i \in \{1, 2, ..., \gamma - 1\}$.

Построение криптосхем. Строить криптосхемы с использованием трудности ЗДЛ по трудно разложимому модулю n можно по аналогии с известными криптосхемами, основанными на трудности ЗДЛ по простому модулю. Однако следует учесть особенности, рассмотренные ранее. Также следует учесть то, что при выборе составного модуля длиной 1024 бит ЗДЛ будет практически сводиться к ЗФ модуля, поскольку ЗДЛ по простому модулю длиной 512 бит решается сравнительно легко. Поэтому для того, чтобы ЗДЛ по модулю n была независимой от ЗФ, требуется использовать значение n, содержащее по крайней мере один простой делитель q такого размера, чтобы ЗДЛ по модулю q была практически невыполнимой. В этом случае для взлома криптосистем, основанных на трудности ЗДЛ по модулю n, найти прорывное решение ЗФ будет недостаточно.

Из изложенного вытекает следующий подход к синтезу криптосхем с 80-битовой стойкостью, который состоит в реализации известных типов криптосхем с открытым ключом, основанных на сложности ЗДЛ, над конечным кольцом вычетов по составному модулю $n = rq$, где размер числа r равен 1024 бит, а размер числа q – 512 бит. При таком подходе существенно используется принципиальное отличие ЗДЛ по составному модулю от ЗФ и ЗДЛ по простому модулю. Известные криптосхемы, основанные на ЗДЛ по простому модулю, используются как аналоги, по которым строятся криптосхемы, использующие трудность ЗДЛ по модулю n размером 1536 бит. Последняя задача принципиально отличается от ЗДЛ по простому модулю. Для решения ЗДЛ по составному модулю могут быть использованы общие методы дискретного логарифмирования [1], [3], имеющие экспоненциальную сложность, и метод сведения к ЗДЛ по простому модулю (имеющий субэкспоненциальную сложность) путем факторизации составного модуля и использования китайской теоремы об остатках [1], [3]. Однако в последнем методе требуется вычислить дискретный логарифм по простым модулям r и q. Это показывает, что появление прорывного метода решения ЗФ или ЗДЛ по простому модулю не приведет к взлому криптосистемы, основанной на ЗДЛ по модулю n, один из простых делителей которого имеет длину 1024 бит.

Действительно, если будут найдены прорывные решения ЗФ, то ЗДЛ по составному модулю n потребует решения ЗДЛ по простым модулям q и r. Так как размер числа r в 2 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 по модулю r равна 280 операциям 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, следовательно, они обладают существенно более высоким уровнем безопасности в смысле значительного снижения (на многие порядки) вероятности их взлома за счет появления прорывных атак.

Особенности криптосхем на основе сложности дискретного логарифмирования по составному модулю. Модуль n и связанные с ним параметры криптосхем могут быть выработаны некоторым доверительным центром, который уничтожит делители q и r после выработки значения n. В этом случае может быть построен более широкий ряд криптосхем различного типа, основанных на трудности одновременного решения ЗФ и ЗДЛ по простому модулю. Однако процедура замены значения модуля (при появлении такой необходимости) в значительной степени теряет гибкость. Последний недостаток устраняется при использовании значения модуля n и связанных с ним параметров в качестве открытого ключа. В обоих случаях появляется дополнительная возможность синтеза схем обычной и слепой электронной цифровой подписи (ЭЦП) над конечными группами с многомерной цикличностью [4], [5].

В криптосхемах, основанных на трудности ЗДЛ по модулю n, в сравнении с их соответствующими аналогами наблюдается увеличение временной сложности вычислительных процедур примерно в 2,25 раза, если в исходных схемах не выбираются значения простых модулей со специальной структурой их двоичного представления. Если в исходных схемах используются простые модули со специальной структурой, то сложность увеличивается в десятки раз. Это связано с тем, что значение составного модуля не может быть выбрано таким, чтобы устранить операцию арифметического деления при выполнении операции модульного умножения. Однако в сравнении со схемами [6]–[8], основанными на трудности одновременного решения ЗФ и ЗДЛ, в предлагаемых схемах наблюдается некоторое снижение сложности используемых вычислительных процедур. При этом в случае протоколов ЭЦП значительно сокращается размер подписи при заданном уровне стойкости. Технические вопросы, связанные с особыми требованиями к модулю n, используемому в предлагаемых криптосхемах, рассматривались ранее в книгах [2], [9] при описании ряда алгоритмов ЭЦП, основанных на сложности ЗФ.

Рассмотрим алгоритм 240-битовой ЭЦП, основанный на ЗДЛ с двойным основанием по модулю n. Открытый ключ представляет собой набор значений $(n, \alpha, \beta, \gamma, y)$, где элемент y вычисляется по формуле $y = \alpha^x \beta^w \bmod n$; a, β – числа, имеющие порядок, равный 80-битовому простому числу γ, и принадлежащие разным циклическим подгруппам. Секретным ключом является набор чисел (r, q, x, w), где x и w – случайные 80-битовые числа $(x < \gamma, w < \gamma)$; простые числа q и r являются секретными значениями и имеют следующую структуру: $r = N_r\gamma^2 + 1$ и $q = N_q\gamma^2 + 11$, где N_r и N_q – 2 больших четных числа. Процедура генерации ЭЦП включает в себя следующие шаги:

1. Сгенерировать случайные числа $k < \gamma$ и $t < \gamma$ и вычислить значение $R = \alpha^k \beta^t \bmod n$.

2. Используя некоторую специфицированную 160-битовую хеш-функцию F_H, вычислить значение $F_H(M)$, где M – документ, который требуется подписать. Представить значение $F_H(M)$ в виде конкатенации двух 80-битовых чисел: $F_H(M) = H_1 \| H_2$.

3. Вычислить первый 80-битовый элемент ЭЦП $E = F_H(M, R) \bmod \gamma$.

4. Вычислить второй 80-битовый элемент ЭЦП $S = ((k + xE) / H_1) \bmod \gamma$.

5. Вычислить третий 80-битовый элемент ЭЦП $U = ((t + wE) / H_2) \bmod \gamma$.

В результате выполнения данной процедуры генерируется 240-битовая ЭЦП в виде тройки 80-битовых чисел (E, S, U). Процедура проверки ЭЦП включает в себя следующие шаги:

1. Вычислить значение $F_H(M) = H_1 \| H_2$.

2. Вычислить значения $\tilde{R} = y^{-E} \alpha^{SH_1} \beta^{UH_2} \bmod n$ и $\tilde{E} = F_H(M, \tilde{R}) \bmod \gamma$.

3. Сравнить значения $\tilde{E}$ и E. Если $\tilde{E} = E$, то ЭЦП признается подлинной.

Корректность работы протокола ЭЦП доказывается подстановкой корректно сформированной подписи в процедуру проверки ее подлинности. Данная подстановка дает следующее:

$$\tilde{R} \equiv y^{-E} \alpha^{SH_1} \beta^{UH_2} \equiv \alpha^{-Ex} \beta^{-Ew} \alpha^{H_1 \frac{k+Ex}{H_1}} \beta^{H_2 \frac{t+Ew}{H_2}} \equiv \alpha^{-Ex} \beta^{-Ew} \alpha^{k+Ex} \beta^{t+Ew} \equiv$$
$$\equiv \alpha^k \beta^t \equiv R \bmod n \Rightarrow \tilde{R} = R \Rightarrow \tilde{E} = E.$$

Таким образом, процедура проверки ЭЦП выполняется, если подпись сформирована правильно. Это доказывает корректность протокола ЭЦП.

Принципиальное отличие ЗДЛ по простому от ЗДЛ по трудно разложимому модулю дает свидетельствует о целесообразности синтеза криптосхем различного типа, основанных на ЗДЛ второго типа. Такие криптосхемы могут быть отнесены к схемам, взлом которых требует одновременного решения двух независимых вычислительно трудных задач – ЗФ и ЗДЛ по простому модулю. При этом для протоколов ЭЦП, относящихся к криптосхемам последнего типа, 80-битовая стойкость достигается при длине подписи, равной 320 и даже 240 бит, что существенно меньше размера подписи для известных схем ЭЦП, основанных на ЗФ (криптосистема Рабина, RSA), а также для схем ЭЦП, основанных на двух трудных задачах [7], [10].

СПИСОК ЛИТЕРАТУРЫ

1. Menezes A. J., Vanstone S.A. Handbook of Applied Cryptography. CRC Press, 1996.

2. Молдовян Н. А., Молдовян А. А. Введение в криптосистемы с открытым ключом. СПб.: БХВ-Петербург, 2005.

3. Молдовян Н. А. Теоретический минимум и алгоритмы цифровой подписи. СПб.: БХВ-Петербург, 2010.

4. Молдовян Н. А. Алгоритмы аутентификации информации в АСУ на основе структур в конечных векторных пространствах // Автоматика и телемеханика. 2008. № 12. С. 163–177.

5. Молдовян Н. А. Аутентификация информации в АСУ на основе конечных групп с многомерной цикличностью // Автоматика и телемеханика. 2009. № 8. С. 177–190.

6. Повышение производительности процедур коммутативного шифрования / П. А. Молдовяну, Д. Н. Молдовян, Е. В. Морозова, С. В. Пилькевич // Вопр. защиты информации. 2009. № 4. С.24–31.

7. Дернова Е. С., Молдовян Н. А. Синтез алгоритмов цифровой подписи на основе нескольких вычислительно трудных задач // Вопр. защиты информации. 2008. № 1. С. 22–26.

8. 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.

9. Молдовян Н. А. Практикум по криптосистемам с открытым ключом. СПб.: БХВ-Петербург, 2007.

10. 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. P. 1–9.

A. N. Berezin, N. A. Moldovyan

CRYPTOSCHEME DESIGN BASED ON THE PROBLEM OF DISCRETE LOGARITHM MODULO A NUMBER DIFFICULT FOR FACTORING

In order to improve security, a justification have been given for designing the public-key algorithms and protocols based on difficulty of finding discrete logarithm modulo in case of using a composite number that is difficult for factoring. It is proposed to use the product of two strong primes as the modulo, with their sizes relation 2:1. This approach provides an alternative solution for construction of the cryptoschemes, based on difficulty of simultaneous solving both the discrete logarithm modulo prime problem and the factoring problem. The approach provides reducing the signature size in digital signature protocols and increasing the rate of the cryptoschemes.

Cryptographic protocol, digital signature, blind collective signature, factoring problem, discrete logarithm problem, public key

УДК 658.512.22

Р. И. Сольницев, До Суан Чо, Б. И. Шапошинков

К ОЦЕНКЕ ТОЧНОСТИ ОБРАБОТКИ МЕТЕОРОЛОГИЧЕСКИХ ДАННЫХ В ЗАМКНУТОЙ СИСТЕМЕ УПРАВЛЕНИЯ «ПРИРОДА – ТЕХНОГЕНИКА»

Рассматриваются вопросы построения подсистемы САПР метеорологической поддержки (МП) замкнутой системы управления «природа – техногеника» (ЗСУ ПТ). Представлены алгоритмы оценки точности обработки метеорологических данных в ЗСУ ПТ. Приведены численные результаты такой оценки.

Экология, загрязняющие вещества, метеорологическое обеспечение, алгоритм, оценка точности, нестационарный случайный процесс, подсистема САПР

В предыдущих работах [1], [2] проведен анализ основных подходов к построению ЗСУ ПТ с целью минимизации загрязняющих веществ (ЗВ) в атмосфере, рассмотрено решение задач синтеза управлений, разработки САПР ЗСУ ПТ. В частности, в [2] рассмотрены вопросы метеорологической поддержки ЗСУ ПТ. Для управления в ЗСУ ПТ необходимо обеспечить поступление метеоданных в ЗСУ ПТ в режиме реального времени.

Известно, что метеорологические данные по ветру, температуре, давлению, влажности (v, T, p, W), полученные из Центра метеорологической информации района, промзоны, в общем случае являются нестационарными случайными процессами (НСП). Однако при оценках статистических характеристик реализаций в процессе обработки метеоданных непосредственное использование этих данных затруднено вследствие малого количества реализаций, полученных на практике.

С целью приближения алгоритмов обработки метеоданных и формирования управляющих воздействий в ЗСУ ПТ к хорошо разработанным и удобным характеристикам стационарных эргодических процессов обработка и ввод в ЗСУ ПТ метеоданных проводятся по эквивалентным статистическим характеристикам стационарных процессов с оценками этих характеристик на стационарность и эргодичность.