УДК 681.3

Я. А. Мондикова, М. А. Вайчикаускас

Криптосхемы над задачей дискретного логарифмирования по трудноразложимому модулю

Предложен механизм построения новых криптосхем на основе трудности одновременного решения двух вычислительно-сложных задач. Представлены алгоритмы открытого шифрования, основанные на задаче дискретного логарифмирования по трудноразложимому модулю.

Криптографические протоколы, трудная задача, задача дискретного логарифмирования, вычислительно - трудная задача, задача факторизации

Криптографические методы защиты информации постоянно развиваются и совершенствуются, появляются новые криптографические примитивы, более стойкие, а потому более надежные. Однако стоит отметить, что в настоящее время безопасность большинства криптографических систем базируется на решении некоторой вычислительно-трудной задачи [1] (под вычислительно-трудной задачей понимается задача, которая имеет решение, однако его нахождение связано с большими вычислительными ресурсами и временными затратами). Это связано с текущим состоянием теории вычислительной сложности. Следует отметить, что не доказано, что не существует эффективных способов решить ту или иную сложную задачу. Таким образом, можно утверждать, что безопасность криптосистемы также базируется на малой вероятности того, что будут разработаны такие способы. Но не стоит забывать о бурных темпах развития компьютерной техники и технологий. Существует вероятность того, что теоретические достижения могут снизить уровень безопасности систем ниже критического.

Понятие безопасности криптографических алгоритмов и протоколов отражает следующие 2 факта: 1) известные алгоритмы их взлома вычислительно нереализуемы и 2) вероятность появления в обозримом будущем прорывных подходов к их взлому является пренебрежимо малой. Обычно двухключевые криптосхемы построены на одной вычислительно трудной задаче, способы решения которой задают уровень стойкости (число операций некоторого типа, которые требуется выполнить для взлома криптосхемы). Понятие стойкости относится к первому факту, а ее повышение обеспечивается увеличением размера параметров криптосхемы. Однако это не затрагивает второй факт, т. е. при появлении прорывного алгоритма взлома криптосистемы увеличение размера параметров не предотвратит критического снижения стойкости. Для увеличения безопасности криптосхем путем снижения вероятности их взлома за счет появления прорывных решений трудных задач был предложен подход к использованию трудности одновременного решения двух независимых трудных задач. В рамках данного подхода криптосхема разрабатывается таким образом, что ее взлом требует одновременного решения двух трудных задач. При этом значение стойкости криптосхемы увеличивается несущественно, но уровень безопасности увеличивается значительно за счет существенно более низкой вероятности одновременного появления прорывных решений двух независимых трудных задач. В качестве последних обосновано использование задачи дискретного логарифмирования (ЗДЛ) и задачи факторизации (ЗФ) [2].

В данной статье развивается подход к построению криптосхем, основанных на сложности ЗДЛ по трудноразложимому модулю, и показывается, что их взлом требует одновременного решения ЗФ и ЗДЛ по простому модулю. При этом обеспечивается универсальность построения, а именно, все типы криптосхем, разработанные ранее на основе трудности ЗДЛ по простому модулю, могут быть естественным способом преобразованы в схемы, взлом которых требует одновременного решения ЗДЛ и ЗФ по простому модулю.

Предлагаемый подход состоит в модифицировании известных криптосхем с открытым ключом, основанных на сложности ЗДЛ в конечном простом поле, заменой последней задачи на ЗДЛ в конечном кольце вычетов по составному модулю $n = rq$, равному произведению двух простых чисел r и q. Размер числа r равен 1024 бит, а размер числа q – 512 бит. Известные криптосхемы на основе ЗДЛ реализуются над кольцом вычетов по модулю p размером 1024 бит. Переход от простого модуля к составному означает, что в модифицированных криптосхемах используется трудность ЗДЛ по составному модулю. Последняя задача принципиально отличается от ЗДЛ по простому модулю. Для решения ЗДЛ по составному модулю могут быть применены общие методы дискретного логарифмирования [1], имеющие экспоненциальную сложность, или метод сведения к ЗДЛ по простому модулю, имеющий субэкспоненциальную сложность и включающий факторизацию составного модуля и использование китайской теоремы об остатках [2]. Можно также показать, что алгоритм вычисления дискретного логарифма по составному модулю n может быть использован для факторизации числа n. Кроме того алгоритм решения ЗДЛ по составному модулю n может быть использован для решения ЗДЛ и ЗФ по простому модулю. Это подтверждает принципиальное различие ЗДЛ по простому и составному модулям.

При нахождении прорывных решений ЗФ решение ЗДЛ по составному модулю n все еще будет требовать 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 простому 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.

В криптосхемах, создаваемых в рамках предложенного подхода, используется открытый ключ, представляемый тройкой чисел $\{n, \alpha, y\}$, где y вычисляется по следующей формуле:

$$y = \alpha^x \pmod n. \qquad (1)$$

Личным секретным ключом пользователя является тройка чисел (r, q, x), где $n = rq$, r – простое 1024-битовое число, q – простое 512-битовое число, x – случайное число, $x < \gamma$, где γ – порядок числа α по модулю n. При этом числа r, q и α не должны удовлетворять одному из следующих двух требований для обеспечения сложности задачи факторизации:

1. Простые числа r и q имеют следующую структуру: $r = N_r\gamma + 1$, $q = N_q\gamma + 1$, где N_r и N_q – 2 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 – 2 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.

Рассмотрим модифицированную схему распределения ключей.

В данной криптосхеме каждый абонент выбирает случайный секретный ключ x и вырабатывает открытый ключ y в соответствии с формулой (1).

Все абоненты размещают свои открытые ключи в общедоступном справочнике, который должен быть заверен специально созданным доверительным центром [3], чтобы исключить возможные нападения путем подмены открытых ключей или навязывания ложных открытых ключей.

Если 2 абонента A и B хотят установить секретную связь, то они поступают следующим образом. Абонент A берет из справочника открытый ключ абонента B и, используя свой секретный ключ, вычисляет общий секретный ключ:

$$Z_{AB} = (y_B)^{x_A} = (a^{x_B})^{x_A} = a^{x_B x_A} \pmod n,$$

где y_B – открытый ключ абонента B; x_A и x_B – соответствующие секретные ключи.

Абонент B аналогичным способом вычисляет значение Z_{AB}:

$$Z_{AB} = (y_A)^{x_B} = (a^{x_A})^{x_B} = a^{x_A x_B} \pmod n,$$

где y_A – открытый ключ абонента A.

Рассмотрим второй вариант модифицированной схемы Диффи–Хеллмана [1], [2]:

1. Абонент *A* генерирует модуль *n* и случайный секретный ключ x_A, вырабатывает открытый ключ y_A: $y_A = \alpha^{x_A} (\mathrm{mod}\, n_A)$.

2. Абонент *B* генерирует модуль *n* и случайный секретный ключ x_B, вырабатывает открытый ключ y_B: $y_B = \alpha^{x_B} (\mathrm{mod}\, n_B)$.

3. Абоненты размещают свои открытые ключи в общедоступном справочнике.

4. Абонент *A* генерирует вспомогательный ОК по открытым элементам a_B, n_B абонента *B*: $R_A = \alpha_B{}^{x_A} (\mathrm{mod}\, n_B)$ и первый вспомогательный общий секрет: $Z_A = y_B{}^{x_A} (\mathrm{mod}\, n)$.

5. Абонент *A* отсылает значение R_A абоненту *B*.

6. Абонент *B* генерирует вспомогательный ОК по открытым элементам a_A, n_A абонента *A*: $R_B = \alpha_A{}^{x_B} (\mathrm{mod}\, n_A)$ и вспомогательный общий секрет: $Z_B = y_A{}^{x_B} (\mathrm{mod}\, n)$.

7. Абонент *B* отсылает значение R_B абоненту *A*.

8. Пользователь *A* вычисляет общий секрет по формуле $Z_{\text{общ}} = Z_A[(R_B)^{x_A} \bmod n_A]$.

9. Пользователь *B* вычисляет общий секрет по формуле $Z_{\text{общ}} = Z_B[(R_A)^{x_B} \bmod n_B]$.

Рассмотрим модифицированный алгоритм открытого шифрования Эль-Гамаля [4]. В данной криптосхеме выбор параметров для вычисления открытого ключа *y* происходит по аналогии модифицированной схемы открытого распределения ключей Диффи–Хеллмана.

Каждый пользователь сети выбирает секретный ключ *x*; вычисляет открытый ключ по формуле (1); помещает *y* в заверенный справочник. Шифрование сообщения *T*, отправляемого пользователю *i*:

1. Выбрать случайное число *k*, которое является секретным ключом отправителя.

2. Вычислить $R = \alpha^k (\mathrm{mod}\, n)$ – разовый открытый ключ отправителя.

3. Используя открытый ключ получателя, вычислить $C = y^k\, T (\mathrm{mod}\, n)$.

4. Отправить блок шифротекста (*R*, *C*) получателю *i*.

Расшифровка:

1. Вычислить значение $Z = R^x (\mathrm{mod}\, n)$, которое по своей сути является разовым общим секретом (Z_{AB}) получателя и отправителя.

2. Вычислить значение $Z^{-1} = (R^x)^{-1} (\mathrm{mod}\, n)$.

3. Расшифровать криптограмму *C*: $T = CZ^{-1} (\mathrm{mod}\, n)$.

Таким образом, в данной статье описаны разработанные авторами алгоритмы открытого распределения ключей, взлом которых требует решения вычислительно-трудной задачи факторизации и задачи дискретного логарифмирования. К основным достоинствам данных схем можно отнести повышение стойкости схемы к взлому и уменьшение вероятности появления в обозримом будущем прорывных решений сразу двух трудных задач, положенных в основу данного алгоритма.

Также разработан алгоритм открытого шифрования, взлом которого требует решения вычислительно-трудной задачи факторизации и задачи дискретного логарифмирования. К основным достоинствам данной схемы можно отнести повышение стойкости схемы к взлому и уменьшение вероятности появления в обозримом будущем прорывных решений сразу двух трудных задач, положенных в основу данного алгоритма. Среди недостатков разработанного алгоритма самым существенным является увеличившееся количество операций, требуемых для выработки трудноразложимого модуля.

СПИСОК ЛИТЕРАТУРЫ

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

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

3. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. М.: Гелиос АРВ, 2002.

4. Дернова Е. С., Молдовян Н. А., Молдовян Д. Н. Криптографические протоколы. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2010.

I. A. Mondikova, M. A. Vaichikauskas

CRYPTO SCHEMES BASED ON DIFFICULT DESCRETE LOGARITHM TASK

It is proposed algorithms and protocols, cracking of wich is required solving two hard computational tasks simultaneously: discrete logarithm task and factorization task. In compare of existing schemes, which could be cracked by solving one hard computational task, these schemes provide higher level of security, because of requirement of solving two hard computational tasks of different types simultaneously.

Cryptographic protocols, hard task, discrete logarithm task, hard computational (mathematichal) task, factorization task

УДК 681.5

Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской, Р. А. Нечитайленко

Формирование математического описания многоуровневой адаптивной автоматизированной системы управления производством на стадии планирования

Рассмотрены требования к методам описания трехуровневых адаптивных автоматизированных систем управления производством (ААСУП). Проведен анализ локальных методов описания, предложены глобальные математические методы исследования ААСУП.

Адаптивное управление, анализ методов, выбор методов, формирование, глобальное описание, планирование, требования к методам

Адаптивные автоматизированные системы управления производством начали развиваться как новый класс систем на рубеже столетий [1]. Особый интерес к таким системам проявляется после перехода России к рыночным отношениям. Вместе с тем этот класс адаптивных систем является специфическим, и для его формального системного описания не подходят существующие теоретические методы ни автоматизированного, ни автоматического управления. Потребовалось сформировать новые методы на основе исследования известных методов. Такая процедура потребовала применения системного анализа к изучению адаптивных систем, включающего процедуры определения системной цели функционирования, структуры и ее функционального наполнения.

Первые две процедуры рассмотрены в публикации [2], продолжением которой является настоящая статья.

Постановка задачи. Провести системное функциональное наполнение трехуровневой структуры [2] адаптивной системы. Для этого необходимо сформулировать требования к математическому описанию, провести анализ известных методов и построить новый метод, пригодный для исследования адаптивных систем.

Решение задачи. Особенности воздействия среды и автоматизированного управления предъявили специфические и порой жесткие требования к методам математического описания процессов:

1. Достаточная адекватность описания процессов, происходящих в реальной системе.

2. Учет многоуровневого характера структуры систем с изменением масштабов описания по времени и координатам.

3. Системность и наглядность метода математического описания и простота алгоритма приложения.