УДК 004.056.55

Н. А. Молдовян
Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Д. С. Будчан
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Криптографические протоколы на основе решения кубических уравнений

Рассматриваются протоколы открытого и отрицаемого шифрования с формированием шифртекста в виде набора коэффициентов кубического сравнения по трудно факторизуемому модулю. Показан общий подход к построению аналогичных протоколов с использованием модульных вычислений над двоичными многочленами и рассмотрены особенности решения кубических уравнений в конечных двоичных полях. Показан общий подход к построению алгоритма решения кубических уравнений в конечных двоичных полях, который значительно упрощает процедуру решения уравнений и сокращает временные затраты на поиск корня. Предложен новый протокол электронной цифровой подписи с проверочным соотношением в виде кубического сравнения общего вида по трудноразложимому модулю, основанный на одновременном шифровании как секретного, так и фиктивного сообщений. В качестве дальнейших исследований предложено вычисление оценок стойкости разработанного алгоритма электронной цифровой подписи и алгоритмов, основанных на вычислениях над двоичными многочленами.

Криптография, шифрование, отрицаемое шифрование, электронная цифровая подпись, кубическое уравнение, конечное двоичное поле

Протоколы шифрования используются для решения различных задач в области обеспечения информационной безопасности (ИБ) информационно-телекоммуникационных систем. В частности, сравнительно новый вид шифрования – отрицаемое шифрование (ОШ) – лежит в основе ряда средств компьютерной безопасности, например BestCrypt (коммерческое приложение по шифрованию дисков для Windows), TrueCrypt (приложение для Windows, MACOS и Linux с возможностью шифрования дисков), StegFS (криптографическая файловая система для Linux), Off-the-RecordMessaging (криптографический протокол для систем мгновенного обмена сообщениями). Протоколы и алгоритмы ОШ решают также и ряд специфических задач в области ИБ [1].

Ранее был предложен способ открытого шифрования, основанный на генерации и решении кубических сравнений, заданных по трудно факторизуемому модулю. В [2] описан подробный алгоритм генерации шифртекста (зашифровывания сообщений по открытому ключу) в виде набора коэффициентов сравнения третьей степени и соответствующий алгоритм расшифровывания, включающий в качестве составной части процедуру решения кубических уравнений в простом конечном поле. На основе алгоритма открытого шифрования [1] был предложен протокол ОШ по открытому ключу, обеспечивающий защищенность информации от атак с принуждением к раскрытию ключа шифрования. Стойкость криптосхем, предложенных в [2], основана на вычислительной сложности факторизации чисел специального вида.

Представляет интерес дальнейшее развитие криптосхем, основанных на генерации и решении кубичных сравнений, в направлении построения протоколов электронной цифровой подписи

(ЭЦП) и реализации алгоритмов открытого шифрования, использующих вычисления над двоичными многочленами. Последнее обеспечит повышение скорости шифрования. Далее рассмотрено построение протокола ЭЦП, в котором в качестве проверочного соотношения используется кубичное сравнение, и особенности реализации криптосхем [2], заданных над двоичными многочленами.

Предметная область. Информационная безопасность включает в себя обеспечение доступности, целостности и конфиденциальности информации – так называемую AIC-триаду (availability, integrity, confidentiality). Для достижения требуемого уровня ИБ применяются различные типы алгоритмов и протоколов шифрования (симметричного, коммутативного, асимметричного), цифровой подписи (индивидуальная, коллективная, групповая, слепая), аутентификации (простая, строгая, с нулевым разглашением секрета) и контроля целостности данных. Для обеспечения секретности сообщений в случае атак с принуждением к раскрытию ключа шифрования используются алгоритмы и протоколы ОШ (с открытым ключом, с разделяемым секретным ключом, бесключевые). Области приложения отрицаемого шифрования включают защищенные распределенные вычисления [3], системы тайного электронного голосования [4] и средства компьютерной безопасности [5].

Перспективной представляется идея реализации алгоритмов ОШ в виде алгоритмов псевдовероятностного шифрования. Последние представляют собой подкласс алгоритмов ОШ, удовлетворяющих требованию вычислительной неразличимости по шифртексту от алгоритмов вероятностного шифрования [6]. Выполнение этого требования состоит в том, что в процессе псевдовероятностного шифрования формируется шифртекст, который мог бы быть сгенерирован алгоритмом вероятностного шифрования. Последний называется ассоциируемым алгоритмом вероятностного шифрования.

При построении протоколов ОШ с открытым ключом важным требованием является использование стандартной инфраструктуры открытых ключей. Это требование реализуется на основе включения в протокол шагов взаимной аутентификации пользователей, объединенных с одновременным выполнением замаскированной процедуры обмена разовыми открытыми ключами [7], [8]. Эта процедура должна выполняться таким образом, что для потенциального нарушителя вычислительно невозможно различить случаи, когда в ходе процесса взаимной аутентификации осуществлен обмен разовыми открытыми ключами, от случаев, когда такой обмен не осуществлялся. Используя разовые открытые ключи, отправитель и получатель формируют разовый разделяемый секретный ключ, по которому зашифровывают секретное сообщение. Полученный в ходе этой процедуры шифртекст используется как рандомизирующий параметр алгоритма вероятностного шифрования фиктивного сообщения. В случае принудительной атаки на обе стороны сеанса шифрованной связи (двусторонняя принуждающая атака) получатель и отправитель раскрывают фиктивное сообщение и личные секретные ключи, связанные с их открытыми ключами, однако атакующий не может выявить наличие в переданном шифртексте еще одного (секретного) сообщения, поскольку долговременный открытый ключ получателя не использовался для зашифровывания секретного сообщения. Кроме того, включение в протокол ОШ этапа взаимной аутентификации отправителя и получателя секретного сообщения обеспечивает защиту от активных принуждающих атак, когда злоумышленник, навязывая ложный сеанс связи, выдает себя за легального отправителя или получателя.

Построить протокол ОШ с замаскированной процедурой обмена разовыми открытыми ключами можно на основе различных алгоритмов открытого шифрования (Рабина, Эль-Гамаля, RSA и др.). Предложенный недавно способ открытого шифрования в виде процедуры генерации степенных сравнений общего вида также может быть использован в сочетании с процедурой замаскированного обмена открытыми ключами [2]. Специальный интерес представляет случай, относящийся к кубичным сравнениям, поскольку для него при соответствующем выборе параметров алгоритма устраняется неоднозначность выходного значения процедуры расшифровывания [9], которая не устранима для случая квадратных сравнений.

Построение протокола цифровой подписи. Протокол ОШ [9] описывается следующим образом. Личным секретным ключом владельца открытого ключа n является пара простых числа p и q, таких, что $n = pq$, $p^2 = 7 \bmod 9$, $q^2 = 7 \bmod 9$, причем ни одно из чисел $p - 1$ и $q - 1$ не делится на 3. Открытым ключом является пара чисел n и $N < n$, где N – квадратичный невычет по модулю p

и по модулю q. Открытое шифрование сообщения $M < n$ выполняется как генерации кубичного выражения в виде произведения выражений $x - M$ и $x^2 + Zx + Y$, где значения $Z < n$ и $Y < n$ берутся такими, что дискриминант многочлена второй степени является невычетом по модулю n:

1. Сформировать случайное число $Z < n$ и вычислить $Y = Z^2/4 - N \bmod n$.

2. Вычислить коэффициенты A, B и D уравнения $x^3 + Ax^2 + Bx + D \equiv 0 \bmod n$ по формулам $A = Z - M \bmod n$, $B = Y - MZ \bmod n$ и $D = -MY \bmod n$.

Данный алгоритм открытого шифрования лежит в основе схемы ОШ, в рамках которой осуществляется одновременное зашифровывание фиктивного $M < n$ и секретного $T < n$ сообщений, причем M преобразуется в соответствии с описанным алгоритмом по открытому ключу (N, n), а секретное сообщение – по формуле $Z = (1/2 - T)^2 \times \times \bmod n$ (обеспечивается стойкость к принудительной атаке на отправителя сообщения) или по формуле $Z = (T + U)U^{-1} \bmod n$ (обеспечивается стойкость к двухсторонней принудительной атаке), где U – разовый общий секретный ключ, формируемый с использованием скрытного распределения разовых открытых ключей. Фактически секретное сообщение встраивается в параметр Z, который в базовом алгоритме открытого шифрования имеет случайное значение, а в протоколе ОШ – псевдовероятностное значение. Расшифровывание шифртекста в виде набора коэффициентов (A, B, D) выполняется посредством вычисления корней кубического уравнения $x^3 + + Ax^2 + Bx + D = 0$ в конечных полях $GF(p)$ и $GF(q)$, по которым на основе китайской теоремы об остатках вычисляется корень M кубичного сравнения $x^3 + Ax^2 + Bx + D \equiv 0 \bmod n$. Стойкость рассмотренного протокола ОШ основана на вычислительной сложности задачи факторизации чисел вида n. В силу построения рассматриваемой криптосхемы ОШ корнем последнего сравнения является значение M, поэтому деление многочлена $x^3 + Ax^2 + Bx + D$ на $x - M$ даст многочлен $x^2 + Zx + Y$. По полученному значению Z владелец открытого ключа (n, N) может восстановить секретное сообщение T.

Рассмотрим построение схемы ЭЦП с проверочным соотношением в виде кубического сравнения:

$$S^3 + 2\rho S + 3H \equiv 0 \bmod n,$$

где ρ – случайно генерируемое 32-битовое число, играющее роль параметра рандомизации; H – значение хеш-функции от электронного документа M. Знание простых делителей числа n позволит вычислить кубичные корни последнего уравнения. При этом значения корней зависят от сообщения M (через значение хеш-функции H), а проверка правильности найденного корня S при заданном значении ρ легко осуществляется по известному открытому ключу n подстановкой цифровой подписи в проверочное соотношение. В качестве подписи задается пара чисел (ρ, S). При этом проверка подлинности ЭЦП должна включать также и условие $\rho < 2^{32}$, поскольку для произвольного значения S' легко вычисляется число $\rho' = -S^{-1}\left(S^3 + 3H\right)/2 \bmod n$, такое, что пара чисел (ρ', S') удовлетворяет проверочному соотношению. Однако без знания делителей модуля n нахождение значения S', при котором будет выполнено условие $\rho' < 2^{32}$, является вычислительно сложной задачей.

Формирование ЭЦП в рассматриваемой криптосхеме может быть выполнено владельцем открытого ключа генерацией 32-битовых случайных значений ρ, при которых проверочное кубическое уравнение имеет решения относительно неизвестного S, алгоритм нахождения которого детально описан в [9], [10]. Выбор в качестве личного секретного ключа простых чисел, удовлетворяющих соотношениям $p^2 = 7 \bmod 9$, $q^2 = 7 \bmod 9$, обеспечивает снижение вычислительной сложности процедуры генерации ЭЦП.

Особенности реализации протоколов ОШ с использованием вычислений над двоичными многочленами. С целью повышения производительности протоколов открытого шифрования и ОШ, основанных на формировании шифртекста в виде коэффициентов кубических сравнений, представляет интерес вопрос об оценке возможности использования вычислений в конечных кольцах двоичных многочленов. Этот вариант реализации предполагает выбор двух случайных неприводимых двоичных многочленов μ и λ достаточно большой степени в качестве секретного ключа, по которому вычисляется открытый ключ $\psi = \mu\lambda$. Алгоритм генерации неприводимых двоичных многочленов произвольной степени описан, например, в [11].

При таком модифицировании криптосхемы возникает вопрос о разработке метода решения кубических уравнений в конечных двоичных полях. Решение этой задачи может быть найдено на основе использования формулы Кардано, в которую входят выражения, описывающие корни квадратного уравнения. Однако в случае квадратных уравнений в двоичных полях корни не могут быть выражены в виде формулы. Отсюда следует, что и в случае кубических уравнений корни не могут быть выражены аналитически и их нахождение связано с использованием некоторого алгоритмического способа, который в обобщенном виде может быть представлен следующим образом:

1. Стандартной заменой переменных кубическое уравнение произвольного вида представить в виде

$$z^3 + \pi z + \gamma = 0, \qquad (1)$$

где γ – некоторый свободный член.

2. Используя алгоритмический способ нахождения корней квадратного уравнения

$$u^2 + \gamma u - \pi^3/27 = 0 \qquad (2)$$

установить корни последнего уравнения в поле $GF\left(\left(2^S\right)^2\right)$: $\alpha \in GF\left(\left(2^S\right)^2\right)$ и $\beta \in GF\left(\left(2^S\right)^2\right)$.

3. Вычислить корни $\sqrt[3]{\alpha}$ и $\sqrt[3]{\beta}$ (по 3 разных значения) в поле $GF\left(\left(2^S\right)^2\right)$.

4. Вычислить корни уравнения (1) как всевозможные суммы $\sqrt[3]{\alpha} + \sqrt[3]{\beta}$, удовлетворяющие условию $\alpha\beta = -\pi/3$.

5. Обратной заменой переменных выразить корни исходного кубического уравнения через найденные корни уравнения (1).

На шаге 2 рассмотренного алгоритма возникнет необходимость решать квадратное уравнение вида (2) в полях характеристики, в которых корни квадратного уравнения не могут быть выражены в виде формулы. Заменой переменных квадратное уравнение (2) приводится к виду

$$x^2 + x - a = 0.$$

Нахождение корней квадратного уравнения в полях характеристики осуществляется алгоритмическим способом, в котором используются такие теоретические понятия, как след и полуслед, имеющие важное значение в информационной технике (областях кодирования информации, передачи данных) и в различных областях математики. Функция следа позволяет организовывать эффективные вычисления и алгоритмы, оперирующие с элементами конечных полей. След – это линейная операция (функция), отображающая элементы одного поля в другое и обладающая свойствами идемпотентности, коммутативности, ассоциативности и дистрибутивности:

$$\mathrm{Tr}_{K/P}(z) = z + z^q + z^{q^2} + \ldots + z^{q^{m-1}},$$

где z – элемент из поля $K = GF(q^n)$, отображаемый в элемент поля $P = GF(q)$.

В бинарном конечном поле $GF\left(2^n\right)$ имеем $q = 2$ и формула вычисления следа элемента поля примет вид

$$\mathrm{Tr}(z) = z + z^2 + z^4 + \ldots + z^{2^{n-1}}.$$

Если след элемента конечного поля $GF(2^n)$ равен нулю при нечетном n, используется формула полуследа:

$$\mathrm{Sr}(z) = x = z + z^4 + z^{16} + \ldots + z^{2^{n-1}}.$$

В [12] представлено описание алгоритма решения квадратных уравнений в конечном поле характеристики два, в котором важным является следующее утверждение: формула полуследа дает решение квадратного уравнения с нулевым следом в поле $GF(2^n)$, где n – нечетное.

Существует ряд работ, в которых решение квадратного уравнения в полях $GF(2^n)$ с нечетным n сводится к системе линейных уравнений, однако вычисление такой системы уравнений достаточно громоздко и требует определенных временных затрат. Особенность вычислений в конечном поле состоит в необходимости выбора представления элементов – от выбранного представления зависит способ реализации, а следовательно, сложность алгоритма. Теоретически возможно использование различных представлений, но на практике в основном используются 2 варианта, а именно представления в стандартных базисах и нормальных базисах. В [12] предложена идея расширения полей и построения нормальных базисов следующего вида с помощью квадратичного симметричного расширения:

$$\left\{\beta,\ \beta^2,\ \beta^4,\ \beta^8,\ \ldots,\ \beta^{2^{n-1}}\right\},$$

где β – корни неприводимого многочлена степени n.

Такой метод позволит быстро находить корни квадратных уравнений вида

$$x^2 + x = a$$

в полях $GF(2^n)$ при любых n, что значительно упростит процедуру решения уравнений и сократит временные затраты на поиск корня.

Таким образом, алгоритм, предложенный в [12], может служить одной из базовых процедур алгоритма решения кубических уравнений в конечном поле характеристики два при разработке алгоритмов открытого шифрования и протоколов ОШ с использованием вычислений в конечных двоичных полях.

Таким образом, предложенный в данной статье протокол электронной цифровой подписи с поверочным соотношением в виде кубичного сравнения общего вида по трудноразложимому модулю расширяет функциональность криптосхемы [9], ранее предложенной для выполнения открытого шифрования и ОШ. Описанный в статье аналог криптосхемы обладает новизной, так как построен с использованием модульных вычислений над двоичными многочленами. Предложенный подход к построению алгоритма решения кубических уравнений в конечных двоичных полях представляет научный интерес, так как играет базовую роль в криптосхеме-аналоге. Особенностью решения кубических уравнений в двоичных полях является то, что корни не могут быть выражены аналитически через коэффициенты кубического уравнения, а находятся алгоритмическим путем.

Дальнейшее исследование по криптосхемам, связанным с решением кубических уравнений общего вида, предполагает выполнение оценок стойкости разработанного алгоритма ЭЦП и алгоритмов, основанных на вычислениях над двоичными многочленами.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-57-54002-Вьет_а.

СПИСОК ЛИТЕРАТУРЫ

1. Биричевский А. Р. Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем: автореф. дис. ... канд. техн. наук / СПИИРАН. СПб., 2017. 19 с.

2. Вайчикаускас М. А. Методы и протоколы псевдовероятностного защитного преобразования информации для технологии тайного электронного голосования: автореф. дис. ... канд. техн. наук / ПГУПС. СПб., 2017. 16 с.

3. Ishai Yu., Kushilevits E., Ostrovsky R. Efficient non-interactive secure computation // Advances in Cryptology – EUROCRYPT 2011. Lecture Notes Comp. Sci. 2011. Vol. 6632. P. 406–425.

4. Barakat M. T. A new sender-side public-key deniable encryption scheme with fast decryption // KSII Transactions on Internet and Information Systems. 2014. Vol. 8. P. 3231–3249.

5. Морозова Е. В., Мондикова Я. А., Молдовян Н. А. Способы отрицаемого шифрования с разделяемым ключом // Информационно-управляющие системы. 2013. № 6. С. 73–78.

6. Татчина Я. А. Методы и алгоритмы симметричных псевдовероятностных защитных преобразований для средств обеспечения информационной безопасности: автореф. дис. ... канд. техн. наук / СПбГЭТУ «ЛЭТИ». СПб., 2017. 16 с.

7. Молдовян Н. А., Вайчикаускас М. А. Расширение криптосхемы Рабина: алгоритм отрицаемого шифрования по открытому ключу // Вопр. защиты информации. 2014. № 2. С. 12–16.

8. Михтеев М. С., Молдовян Н. А. Гибридный протокол отрицаемого шифрования, основанный на процедуре аутентификации // Вопр. защиты информации. 2017. № 1. С. 12–17.

9. Молдовян Н. А., Молдовян Д. Н., Вайчикаускас М. А. Генерация кубических уравнений как способ открытого шифрования // Вопр. защиты информации. 2015. № 2. С. 3–7.

10. Moldovyan N. A., Moldovyan A. A., Shcherbacov V. A. Generating Cubic Equations as a Method for Public Encryption // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2015. Vol. 3 (79). P. 60–71.

11. Молдовян Н. А., Аль-Рахми Р. Я. Синтез алгебраических блочных шифров с использованием операции над двоичными многочленами // Вопр. защиты информации. 2012. № 1. С. 2–7.

12. Глуско Кр. Л., Титов С. С. Арифметический алгоритм решения квадратных уравнений в конечных полях характеристики два // Докл. Томского гос. ун-та систем управления и радиоэлектроники. 2012. Т. 1, № 2. С. 148–152.

N. A. Moldovyan
Saint Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
D. S. Budchan
Saint Petersburg Electrotechnical University «LETI»

CRYPTOGRAPHIC PROTOCOLS BASED ON SOLVING OF CUBIC EQUATIONS

There are considered protocols for public and deniable encryption with generating ciphertext in form of the set of the coefficients of cubic congruence modulo an integer that is difficult for factoring. It is proposed a general approach to constructing analogous protocols using modulo computations over binary polynomials. There are discussed peculiarities of solving cubic equations in finite binary fields. A general approach of the construction of an algorithm for solving cubic equations in finite binary fields is shown, which greatly simplifies the procedure of solving equations. It is proposed a novel digital signature protocol with cubic verification equation of general type, which is based on simultaneous encryption of both secret and fictitious messages. It is proposed to calculate the stability estimates of the developed algorithm of the electronic digital signature and algorithms based on calculations over binary polynomials.

Cryptography, encryption, deniable encryption, digital signature, cubic equation, binary finite field

УДК 004.272

В. В. Жариков, А. А. Пазников
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Адаптивный алгоритм барьерной синхронизации в стандарте MPI на основе модели параллельных вычислений LogP

Рассматривается задача разработки адаптивного алгоритма барьерной синхронизации ветвей параллельных MPI-программ в распределенных вычислительных системах. Предложен алгоритм барьерной синхронизации, обеспечивающий субоптимальный выбор схемы реализации барьерной синхронизации. В процессе выбора учитывается время выполнения информационных обменов в модели параллельных вычислений LogP. Построены аналитические оценки времени выполнения распространенных алгоритмов барьерной синхронизации в модели LogP. Предложенный адаптивный алгоритм реализован в стандарте MPI. Приводятся результаты натурных экспериментов на кластерных вычислительных системах. Результаты экспериментов позволяют проследить зависимость между параметрами модели LogP, числом процессов и выбором алгоритма реализации барьерной синхронизации. Разработанный адаптивный алгоритм позволит сократить среднее время выполнения барьерной синхронизации на 4 %, по сравнению с существующими распространенными алгоритмами.

Коллективные обмены, барьерная синхронизация, распределенные вычислительные системы, LogP, MPI, параллельное программирование

В настоящее время для решения сложных задач в области науки и производства применяются распределенные вычислительные системы (ВС). В архитектурном плане распределенная ВС представляется множеством элементарных машин (ЭМ), взаимодействующих между собой через коммуникационную среду [1]. ЭМ может быть представлена как процессорным ядром, так и многоядерным SMP/NUMA-узлом, укомплектованным специализированными ускорителями (например, графическими процессорами). Количество ЭМ в системе может достигать нескольких миллионов. Так, например, суперкомпьютер Sunway TaihuLight, возглавляющий рейтинг TOP500, включает в себя более 10 млн процессорных ядер. Для выполнения параллельных программ на таких