Генерация степенных сравнений как способ открытого шифрования и протокол отрицаемого шифрования

Молдовян Н. А.
Санкт-Петербургский институт
информатики и автоматизации РАН
Санкт-Петербург, Россия
nmold@mail.ru

Вайчикаускас М. А.
Санкт-Петербургский государственный
электротехнический университет «ЛЭТИ»
Цюрих, Швейцария
m.vaichikauskas@gmail.com

Аннотация. **Представлен новый способ открытого шифрования, в котором процесс зашифровывания выполняется путем генерации коэффициентов кубичного уравнения, а процесс расшифровывания заключается в решении данного уравнения. Безопасность данного метода основывается на сложности задачи факторизации, а именно на сложности факторизации составного модуля, который служит открытым ключом. Секретный ключ представляет собой пару чисел p и q, таких что $n = pq$. Процесс расшифровывания выполняется путем решения кубичного сравнения по модулю n. Первым шагом данного процесса является нахождение корней уравнения в полях $GF(p)$ и $GF(q)$. В работе предлагается метод решения кубичных уравнений в простых конечных полях. Предложенный способ открытого шифрования применен для построения протокола отрицаемого шифрования, стойкого к двусторонним принуждающим атакам.**

Ключевые слова: **криптография, шифрование, открытое шифрование, отрицаемое шифрование, открытый ключ, вероятностное шифрование, задача факторизации, кубичные уравнения, простое конечное поле.**

Введение

Новый способ открытого шифрования состоит в генерации шифртекста в виде набора коэффициентов уравнений второй, третьей и четвертой степеней [1, 2]. Он позволяет одновременно шифровать два, три и четыре сообщения в одну криптограмму, благодаря чему может быть реализовано отрицаемое шифрование (ОШ), которое представляет собой криптографический механизм, обеспечивающий защиту информации в случае принуждающих атак. Подробно концепция ОШ и некоторые области его применения рассмотрены в работах [3, 4]. В [5] обоснована состоятельность ОШ с разделяемым секретным ключом как нового самостоятельного механизма защиты информации от несанкционированного доступа, перспективного для применения в средствах обеспечения компьютерной безопасности, использующихся в том числе для защиты телекоммуникаций в информационно-вычислительных системах на железнодорожном транспорте.

Способ открытого шифрования, основанный на генерации степенных уравнений и включающий одновременное шифрование двух и более сообщений, предполагает неоднозначность процедуры расшифровывания. В данной статье рассматривается способ открытого шифрования с использованием кубичных уравнений, свободный от неоднозначности расшифровывания шифртекста, что является его существенным преимуществом по сравнению с аналогичными способами. Также предложен способ отрицаемого шифрования, в основу которого положен разработанный способ открытого шифрования.

Новый способ открытого шифрования

Так же, как в алгоритме шифрования [1], личным секретным ключом владельца открытого ключа n является пара сильных простых чисел p и q [6], таких, что $n = pq$, $p^2 = 7 \bmod 9$, $q^2 = 7 \bmod 9$, и число 3 не делит ни одно из чисел $(p-1)$ и $(q-1)$.

Идея обеспечения однозначности процедуры расшифровывания, состоящей в решении кубичного уравнения над конечным кольцом классов по модулю n, состоит в генерации кубичного выражения, которое представляется в виде произведения многочлена первой степени $(x - M)$, где M – шифруемое сообщение $(M < n)$, и многочлена второй степени $(x^2 + Zx + Y)$, не имеющего корней в указанном кольце. При этом случайные значения $Z < n$ и $Y < n$ генерируются так, что дискриминант многочлена второй степени является невычетом. Однако шифрование выполняется лицами, которым неизвестны делители трудно факторизуемого числа n, поэтому требуется расширить открытый ключ, включив в него некоторый квадратичный невычет $N < n$, который генерируется владельцем открытого ключа после генерации личного секретного ключа. Для этого владелец открытого ключа генерирует случайное значение, для которого выполняются следующие два условия:

$$N^{\frac{p-1}{2}} \equiv -1 \bmod p;$$
$$N^{\frac{q-1}{2}} \equiv -1 \bmod q.$$

Открытым ключом является пара чисел N и n.

Алгоритм шифрования сообщения M по открытому ключу описывается следующим образом:

1) сформировать случайное число $Z < n$ и вычислить значение по формуле

$$Y = Z^2/4 - N \bmod n;$$

2) вычислить коэффициенты A, B и D кубичного уравнения

$$x^3 + Ax^2 + Bx + D = 0 \bmod n, \qquad (1)$$

используя формулы $A = Z - M \bmod n$, $B = Y - MZ \bmod n$ и $D = -MY \bmod n$, которые вытекают из условия $x^3 + Ax^2 + Bx + D = (x - M)(x^2 + Zx + Y)$.

Таким образом, сложность процедуры формирования шифртекста $C = (A, B, D)$ примерно равна трем операциям умножения по модулю n. Криптограмма C направляется по открытому каналу владельцу открытого ключа (N, n), который расшифровывает ее с использованием своего личного секретного ключа. Процедура расшифровывания состоит в решении кубичного уравнения (1), заданного коэффициентами A, B и D, т. е. в нахождении единственного его корня, равного значению M.

Решение уравнения (1) выполняется следующим образом. Решаются следующие два кубичных уравнения:

$$x^3 + Ax^2 + Bx + D \equiv 0 \bmod p; \quad (2)$$

$$x^3 + Ax^2 + Bx + D \equiv 0 \bmod q \quad (3)$$

в простых конечных полях $GF(p)$ и $GF(q)$, соответственно. Каждое из этих уравнений имеет единственный корень в простом конечном поле. Пусть корень уравнения (2) равен M_p, а уравнения (3) – M_q. Тогда корень уравнения (1) находится как решение системы линейных сравнений

$$\begin{cases} M \equiv M_p \bmod p \\ M \equiv M_q \bmod q \end{cases}. \quad (4)$$

В соответствии с греко-китайской теоремой об остатках решением системы (4) является значение

$$M = \left[M_p q \left(q^{-1} \bmod p \right) + M_q p \left(p^{-1} \bmod q \right) \right] \bmod pq. \quad (5)$$

Трудоемкость расшифровыванию задает решение уравнений (2) и (3). Рассмотрим, как можно решить кубичное уравнение в конечном поле, например уравнения (2).

По аналогии со способом решения кубичных уравнений в поле действительных чисел [7] путем замены переменной по формуле $x = z - A/3 \bmod p$ перейдем к решению следующего уравнения, свободного от квадрата неизвестного:

$$z^3 + Pz + Q = 0 \bmod p, \quad (6)$$

где

$$P = B - \frac{A^2}{3} \bmod p;$$

$$Q = \frac{2A^3}{27} - \frac{AB}{3} + D \bmod p.$$

Поскольку заведомо известно, что есть решение уравнения (6), вывод формулы для корней кубичного уравнения, приведенный в [7, с. 234–238], можно применить и в рассматриваемом случае. Такой подход дает следующую формулу для корней (6):

$$z = \alpha + \beta, \quad (7)$$

где

$$\alpha = \sqrt[3]{-\frac{Q}{2} + \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}} \bmod p;$$

$$\beta = \sqrt[3]{-\frac{Q}{2} - \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}} \bmod p. \quad (8)$$

При этом при наличии нескольких значений кубичного корня в формулах (8) следует выбирать такие пары, которые удовлетворяют соотношению

$$\alpha\beta = -\frac{P}{3}. \quad (9)$$

Поскольку при открытом шифровании используются случайные значения, т. е. этот процесс является вероятностным, под квадратным корнем в выражениях (8) может оказаться значение, которое является как квадратичным вычетом, так и квадратичным невычетом. В первом случае значение квадратного корня имеется, и его можно легко вычислить (см., например, [8]). При этом из-за условия выбора простых чисел в качестве секретного ключа (число 3 не делит ни одно из чисел $p - 1$ и $q - 1$) есть единственный кубичный корень из любого значения, поэтому существует единственный корень уравнения (6), который вычисляется непосредственно по формулам (7) и (8).

Во втором случае, чтобы найти решение уравнения (6), требуется перейти в поле $GF(p^2)$, выполнить вычисления по формулам (7) и (8) и взять в качестве искомых значений те, которые лежат в поле $GF(p)$, вложенном в поле $GF(p^2)$. В качестве поля $GF(p^2)$ удобно выбрать поле двоичных векторов, заданных над полем $GF(p)$ [8, 9] при определении операций сложения и умножения векторов $\boldsymbol{V} = (a, b) \in GF(p^2)$ и $\boldsymbol{U} = (c, d) \in GF(p^2)$ по формулам

$$\boldsymbol{V} + \boldsymbol{U} = (a, b) + (c, d) = (a + c \bmod p, b + d \bmod p); \quad (10)$$

$$\boldsymbol{VU} = (a, b)(c, d) = (ac + kbd \bmod p, bc + ad \bmod p), \quad (11)$$

где $k \in GF(p)$ – некоторый заданный квадратичный невычет.

Вместо уравнения (6) будем рассматривать уравнение над конечным полем двоичных векторов вида:

$$\boldsymbol{Z}^3 + \boldsymbol{PZ} + \boldsymbol{Q} = (0, 0), \quad (12)$$

где

$$P = (P, 0) = (B, 0) - \frac{(A, 0)^2}{3};$$

$$Q = (Q, 0) = \frac{2}{27}(A, 0)^3 - \frac{(A, 0)(B, 0)}{3} + (D, 0).$$

Если заведомо известно, что есть решение уравнения (6), то есть и решения уравнения (12), тогда имеем формулу для корней (12)

$$\boldsymbol{Z} = \boldsymbol{A} + \boldsymbol{B}, \quad (13)$$

где

$$\boldsymbol{A} = \sqrt[3]{-\frac{Q}{2} + \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}}; \quad \boldsymbol{B} = \sqrt[3]{-\frac{Q}{2} - \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}}. \quad (14)$$

При этом при наличии нескольких значений кубичного корня в формулах (8) следует выбирать такие пары, которые удовлетворяют соотношению

$$AB = -\frac{P}{3}. \quad (15)$$

Заметим, что имеются следующие положения.

Утверждение 1. Пусть $a \in GF(p)$ есть квадратичный невычет, тогда для $(a, 0) \in GF(p^2)$ выполняется

$$\sqrt{(a,0)} = (0, \pm\sqrt{k^{-1}a}),$$

где k – квадратичный невычет, заданный в формуле (11), определяющей правило выполнения операции умножения в поле двоичных векторов.

Доказательство. В соответствии с формулой (12) получаем

$$(0, \pm\sqrt{k^{-1}a})^2 = \sqrt{(a,0)}. \quad \Diamond$$

Утверждение 2. В поле $GF(p^2)$, где $p > 3$, из произвольного кубичного вычета $\boldsymbol{A}$ есть три разных кубичных корня.

Доказательство. Любое простое число $p > 3$ представимо в виде $p = 6t \pm 1$ при некотором натуральном числе t, поэтому порядок мультипликативной группы поля $GF(p^2)$ представим в виде $p^2 - 1 = 36 \pm 12t$, т. е. число 3 – порядок этой конечной группы. Последняя является циклической, поэтому в ней есть ровно два элемента, имеющих порядок, равный 3. Пусть это будут элементы $\boldsymbol{E}$ и $\boldsymbol{E}^2$. Последние являются нетривиальными корнями из единичного элемента $(1,0) \in GF(p^2)$. Если $\boldsymbol{B}$ является кубичным корнем из $\boldsymbol{A}$, то $\boldsymbol{EB}$ и $\boldsymbol{E}^2\boldsymbol{B}$ – также кубичные корни из $\boldsymbol{A}$: $(\boldsymbol{EB})^3 = \boldsymbol{E}^3\boldsymbol{B}^3 = \boldsymbol{B}^3 = \boldsymbol{A}$ и $(\boldsymbol{E}^2\boldsymbol{B})^3 = \boldsymbol{E}^6\boldsymbol{B}^3 = \boldsymbol{B}^3 = \boldsymbol{A}$.

Предположение о существовании четвертого корня $B' = \sqrt[3]{A}$ приводит к наличию в конечной циклической группе более двух элементов, имеющих порядок 3. Это противоречие доказывает, что в поле $GF(p^2)$ имеются ровно три разных кубичных корня из каждого кубичного вычета.

Утверждение 3. В поле $GF(p^2)$ при $p^2 \equiv 7 \bmod 9$ один из кубичных корней $\boldsymbol{B}$ из кубичного вычета $\boldsymbol{A}$ может быть найден по формуле

$$B = A^{\frac{p^2+2}{9}}. \quad (16)$$

Доказательство. Поскольку $\boldsymbol{A}$ – кубичный вычет, есть некоторый элемент $\boldsymbol{X} \in GF(p^2)$, для которого выполняется $\boldsymbol{X}^3 = \boldsymbol{A}$, поэтому имеем

$$A^{\frac{p^2-1}{3}} = X^{p^2-1} = (1,0).$$

Следовательно,

$$B^3 = A^{\frac{p^2+2}{3}} = AA^{\frac{p^2-1}{3}} = A.$$

В силу того, что уравнение (12) заведомо имеет решения, вычисляемые по формулам (13) и (14), под кубичным корнем в (14) будут присутствовать кубичные вычеты. Вычисление кубичных корней в выражениях (14) может быть выполнено по формуле (16).

В целом в сравнении с процедурой зашифровывания расшифровывание имеет существенно более высокую вычислительную сложность, однако при использовании быстрого алгоритма возведения в большую степень в конечных полях $GF(p)$ и $GF(p^2)$ она выполняется достаточно быстро – в полтора-два раза медленнее процедуры расшифровывания в протоколе открытого шифрования Эль-Гамаля [10]. Однако в последнем процедура зашифровывания имеет вычислительную сложность в сотни раз более высокую, чем сложность зашифровывания в описанном способе открытого шифрования.

Протокол отрицаемого шифрования

Предложенный способ шифрования по открытому ключу может быть использован в протоколе ОШ, стойком к двухсторонним принуждающим атакам. Алгоритм ОШ строится следующим образом. Фиктивное сообщение $M < n$ зашифровывается по способу ОШ, описанному ранее, а секретное сообщение встраивается в значение параметра Z. Это встраивание выполняется с помощью разового разделяемого секретного ключа U, который согласовывается на этапе взаимной аутентификации пользователей путем умножения секретного сообщения T на ключ U по модулю n: $Z = TU \bmod n$. При восстановлении фиктивного сообщения одновременно восстанавливается и значение псевдослучайного параметра Z. Затем вычисляется секретное сообщение по формуле $T = U^{-1}Z \bmod n$.

Для взаимной аутентификации пользователей воспользуемся генерацией случайного запроса одним пользователем и вычислением ответа на этот запрос другим пользователем. В качестве ответа зададим значение цифровой подписи пользователя к полученному случайному запросу. В качестве специфицируемой схемы цифровой подписи выберем криптосистему RSA, поскольку трудноразложимый модуль уже имеется в качестве одного из элементов открытого ключа. Чтобы выполнять процедуры формирования и проверки подлинности цифровой подписи в рамках криптосхемы RSA, открытый ключ должен быть дополнен третьим элементом – числом e, таким, что $e < \varphi(n)$ и НОД $(e, \varphi(n)) = 1$. При этом личный секретный ключ также дополняется третьим элементом – числом $d = e^{-1} \bmod (p-1)(q-1)$.

Такая криптосхема реализована в следующем протоколе ОШ, в котором предполагается, что отправитель сообщения владеет открытым ключом (n_1, e_1, N_1), а получатель – открытым ключом (n_2, e_2, N_2).

1. Отправитель генерирует случайное число k_1, удовлетворяющее условию $0 < k_1 < N_1 - 1$, и вычисляет значение

$$R_1 = N_2^{k_1} \bmod n_2.$$

Затем формирует свою подпись

$$S_1 = S_1(R_1) = R_1^{d_1} \bmod n_1$$

к значению R_1 и направляет значения R_1 и $S_1(R_1)$ получателю.

2. Получатель, используя открытый ключ (n_1, e_1, N_1), проверяет подлинность подписи $S_1(R_1)$. Если подпись подлинная, то он генерирует случайное число k_2, удовлетворяющее условию $0 < k_2 < p - 1$, и вычисляет значение

$$R_2 = N_2^{k_2} \bmod n_2.$$

Затем формирует свою подпись $S_2(R_1)$ к значению R_1 и свою подпись $S_2(R_2)$ к значению R_2 и направляет значения R_2, $S_2(R_1)$ и $S_2(R_2)$ отправителю.

3. Отправитель, используя открытый ключ (n_2, e_2, N_2), проверяет подлинность подписи $S_2(R_1)$ к случайному значению,

которое он направлял получателю, и подлинность подписи S_2 (R_2) к разовому открытому ключу R_2 получателя. Если подпись подлинная, то он зашифровывает и передает секретное сообщение T ($T < n_2$) получателю, выполняя следующие шаги (в противном случае он прерывает сеанс связи):

3.1) генерирует фиктивное сообщение $M < n_2$;

3.2) вычисляет значение

$$U = R_2^{k_1} \bmod n_2,$$

легко заметить, что

$$U = N_2^{k_2 k_1} \bmod n_2,$$

и, используя значение U в качестве разового секретного ключа, вычисляет маскируемый под случайное число шифртекст $Z = UT \bmod n_2$;

3.3) вычисляет значение

$$Y = Z^2/4 - N_2 \bmod n_2$$

и криптограмму $C = (A, B, D)$, используя формулы $A = (Z - M) \bmod n$, $B = (Y - MZ) \bmod n$ и $D = -MY \bmod n$;

3.4) вычисляет свою подпись $S_1(C)$ к криптограмме $C = (A, B, D)$ и направляет значения $S_1(C)$ и C получателю;

4. Получатель проверяет подлинность подписи $S_1(C)$. Если подпись ложная, он игнорирует шифртекст C и прерывает сеанс связи. Если подпись подлинная, то он восстанавливает секретное сообщение T следующим путем:

4.1) подставляет в уравнение (1) значения коэффициентов A, B и D и, используя известные ему значения p и q, вычисляет целочисленный корень (1), который равен фиктивному сообщению M;

4.2) вычисляет значение Z по формуле $Z = (A + M) \bmod n$;

4.3) вычисляет значение разового секретного ключа

$$U' = R_1^{k_2} \bmod n_2,$$

легко заметить, что

$$U' = N_2^{k_1 k_2} \bmod n_2 = U;$$

4.4) Вычисляет секретное сообщение $T = U'^{\,1}Z \bmod n_2$.

5. Подвергаясь двухсторонней принуждающей атаке, отправитель раскрывает фиктивное сообщение M, а получатель раскрывает свой личный секретный ключ (p, q, d_2).

Атакующий расшифровывает криптограмму по ключу (p, q, d_2) и убеждается, что значение M раскрыто правильно. Он может также вычислить и псевдослучайное значение Z, однако раскрыть секретное сообщение он не сможет, так как для этого надо знать разовый общий секретный ключ, который не зависит от личных секретных ключей участников сеанса секретной связи.

Чтобы уличить пользователей в обмане, атакующий должен решить задачу дискретного логарифмирования по трудноразложимому модулю n_2. Последняя задача не проще, чем факторизация числа n_2. На этом основано предположение: атакующий не сможет доказать, что случайные значения R_1 и R_2 были использованы как разовые открытые ключи в процедуре согласования разового общего секрета U, т. е. то, что пользователи скрытно использовали криптосхему Диффи – Хеллмана.

В случае активных принуждающих атак нарушитель, выдающий себя за получателя сообщения, обнаруживается на шаге 3 описанного протокола, а нарушитель, выдающий себя за отправителя сообщения, – на шаге 4, где проверяется подлинность подписи отправителя к криптограмме C.

Односторонний алгоритм отрицаемого шифрования

Если в модели потенциального нарушителя не предусматривается принуждающая атака на получателя сообщения и рассматриваются только пассивные атаки, то алгоритм ОШ может быть построен без скрытного использования схемы открытого согласования общего секретного ключа. Построение такого алгоритма может быть выполнено с использованием базового кубичного уравнения (1) и открытого ключа (n, N) получателя на основе включения в протокол следующих шагов.

1. Отправитель секретного сообщения $T < n$ генерирует фиктивное сообщение $M < n$ и вычисляет криптограмму $C = (A, B, D)$ следующим путем:

1.1) вычисляет псевдослучайное значение $Z = (2^{\,1} - T)^2 \bmod n$ и значение

$$Y = Z^2/4 - N \bmod n;$$

1.2) вычисляет коэффициенты A, B и D, при которых уравнение (1) имеет единственный корень, по следующим формулам:

$$A = (Z - M) \bmod n;$$

$$B = (Y - MZ) \bmod n;$$

$$D = -MY \bmod n;$$

1.3) отправляет криптограмму $C = (A, B, D)$ получателю.

2. Получатель, используя свой личный секретный ключ, решает кубичное уравнение (1) и находит корень M – фиктивное сообщение. Затем он вычисляет секретное сообщение T, выполняя следующие шаги:

2.1) вычисляет значение Z по формуле $Z = (A + M) \bmod n$;

2.2) вычисляет значения

$$T_i = 2^{\,1} - \sqrt{Z} \bmod n,$$

где $i = 1, 2, 3, 4$;

2.3) отбрасывает три случайных значения T_i, а оставшееся осмысленное сообщение берет в качестве восстановленного секретного сообщения T.

В случае принуждения отправителя сообщения к раскрытию использованных параметров шифрования он предоставляет атакующему фиктивное сообщение M и число Z, ссылаясь на последнее как на случайное значение. Выполнив шифрование M по открытому ключу (N, n) при использовании предоставленного «случайного» значения Z, атакующий получит криптограмму $C = (A, B, D)$.

Если она совпадает с шифртекстом, переданным по открытому каналу и по предположению известным атакующему, то последний вынужден признать, что ему честно раскрыли переданное сообщение. Чтобы раскрыть обман, атакующему нужно восстановить секретное сообщение по известному значению Z, однако это требует вычисления квадратного корня по модулю n, что не менее сложно, чем решение задачи факторизации числа n [11, 12]. На вычислительной трудности последней задачи построено достаточно большое число раз-

личных криптосхем, например, RSA [13], открытый шифр Рабина [12], схемы цифровой подписи [1, 14].

Заключение

Предложен способ открытого шифрования, заключающийся в формировании шифртекста в виде набора коэффициентов кубичного уравнения. В отличие от известного способа шифрования с формированием шифртекста в виде набора коэффициентов квадратного уравнения [1], в предложенном способе решена проблема неоднозначности текста, восстанавливаемого при выполнении процедуры расшифровывания. Основным шагом процедуры расшифровывания в предложенном способе является решение кубичных уравнений в простом конечном поле $GF(p)$. Чтобы найти корни таких уравнений в общем случае, предложено решать их в поле $GF(p^2)$, заданном в виде конечного поля двоичных векторов.

Описанный в статье способ открытого шифрования может быть использован для построения протокола ОШ, включающего одновременное шифрование секретного и фиктивного сообщений. При этом фиктивное сообщение восстанавливается как корень кубичного уравнения, а секретное – путем преобразования одного из коэффициентов неразложимого в поле $GF(p)$ квадратного трехчлена.

Литература

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

2. Moldovyan N. A., Moldovyan A. A., Shcherbacov V. A. Provably Sender-Deniable Encryption Scheme // Proc. «The Third Conference of Mathematical Society of the Republic of Moldova» (IMCS-50). Chisinau, 19-23 Aug. 2014, Inst. Mathematics and Computer Science, Academy of Sciences of Moldova. 2014, P. 134-141.

3. Canetti R., Dwork C., Naor M., Ostrovsky R. Deniable Encryption // Advances in Cryptology – CRYPTO 1997. Proc. P. 90-104.

4. Ibrahim M. H. Receiver-Deniable Public-Key Encryption // Int. J. Network Security. 2009. Vol. 8, № 2. P. 159-165.

5. Березин А. Н., Биричевский А. Р., Молдовян Н. А., Рыжков А. В. Способ отрицаемого шифрования // Вопр. защиты информации. 2013. № 2. С. 18-21.

6. Gordon J. Strong primes are easy to find // Advances in cryptology – EUROCRYPT'84. Springer-Verlag LNCS. 1985. Vol. 209. P. 216-223.

7. Курош А. Г. Курс высшей алгебры. – М.: Наука, 1971. 431 с.

8. Молдовян Н. А. Теоретический минимум и алгоритмы цифровой подписи. – СПб.: Петербург-БХВ, 2010. 304 с.

9. Moldovyan N. A., Moldovyanu P. A. Vector form of the finite fields GF (pm) // Bull. Acad. de Stiinte a Republicii Moldova. Matematica. 2009. № 3. P. 57-63.

10. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory. 1985. Vol. IT-31, № 4. P. 469-472.

11. Moldovyan N. A., Moldovyan A. A. Class of Provably Secure Information Authentication Systems // Springer Verlag CCIS 4th Int. Workshop MMM-ANCS'07 Proc. 13-15 Sept. 2007. 2007. Vol. 1. P. 147-152.

12. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М.: Постмаркет, 2001. – 323 с.

13. Rabin M. O. Digitalized signatures and public key functions as intractable as factorization // Technical report MIT/LCS/TR-212, MIT Laboratory for Computer Sci. 1979.

14. Moldovyan A. A., Moldovyan N. A., Shcherbakov V. A. Short signatures from difficulty of the factoring problem // Bull. Acad. de Stiinte a Republicii Moldova. Matematica. 2013. № 2-3. P. 27-36.

Generation of Polynomial Equations as a Method for Public Key Encryption and Deniable Encryption Protocol

Moldovyan N.A.
Saint-Petersburg Institute for Informatics and Automation of RAS
St. Petersburg, Russia
nmold@mail.ru

Vaichikauskas M.A.
Saint-Petersburg State Electrotechnical University "LETI"
Zurich, Switzerland.
m.vaichikauskas@gmail.com

Abstract. **The paper introduces a new method for public encryption in which the enciphering process is performed as a generation of the coefficients of some cubic equation and the deciphering process is solving the equation. Security of the method is based on a difficulty of the factoring problem, namely, difficulty of factoring a composite number n that serves as a public key. The private key is the pair of primes p and q such that $n = pq$. The deciphering process is performed as solving cubic congruence modulo n. Finding roots of cubic equations in the fields $GF(p)$ and $GF(q)$ is the first step of the decryption. The paper also describes a method for solving cubic equations defined over prime finite fields. Introduced method of public encryption is applied for development of deniable encryption protocol, which is resistant against two-sided coercive attacks.**

Keywords: **cryptography, encryption, public key encryption, deniable encryption, public key, probabilistic encryption, factorization problem, cubic equation, prime finite field.**

References

1. Moldovan N.A., Vaichikauskas M.A. Rabin Cryptoscheme Expansion: Public-key Deniable Encryption Algorithm [Rasshirenie Kriptoskhemy Rabina: Algoritm otritsaemogo shifrovaniya po otrkrytomu klyuchu]. *Information Security Questions [Voprosy Zashchity Informatsii]*, 2014, no. 2, pp. 12-16. (In Russ.)

2. Moldovyan N.A., Moldovyan A.A., Shcherbacov V.A. Provably Sender-Deniable Encryption Scheme. *Proc. "The Third Conference of Mathematical Society of the Republic of Moldova" (IMCS 50)*. Chisinau, 19-23 Aug. 2014, Institute of Mathematics and Computer Science, Academy of Sciences of Moldova. 2014. P. 134-141.

3. Canetti R., Dwork C., Naor M., Ostrovsky R. Deniable Encryption. *Advances in Cryptology – CRYPTO 1997.* Proc. Pp. 90-104.

4. Ibrahim M.H. Receiver-Deniable Public-Key Encryption. *Int. J. Network Security*, 2009, Vol. 8, no. 2, pp. 159-165.

5. Berezin A.N., Birichevskiy A.R., Moldovyan N.A., Ryzgkov A.V. Method for Deniable Encryption [Sposob otritsaemogo shifrovaniya]. *Items of Information Protection [Voprosy zashchity informatsii]*, 2013, no. 2, pp. 18-21. (In Russ.)

6. Gordon J. Strong primes are easy to find. *Advances in cryptology – EUROCRYPT'84. Springer Verlag LNCS*, 1985, Vol. 209, pp. 216-223.

7. Kurosh A.G. High Algebra Course [Kurs Vysshey Algebry]. Moscow, Nauka, 1971. 431 p. (In Russ.)

8. Moldovyan N.A. Theoretical Minimum and Algorithms of Digital Signature [Teoreticheskiy Minimum i Algoritmy Tsifrovoy Podpisi]. St. Petersburg, Peterburg-BHV, 2010. 304 p. (In Russ.)

9. Moldovyan N.A., Moldovyanu P.A. Vector form of the finite fields GF (pm). *Bulletinul Academiei de Stiinte a Republicii Moldova. Matematica*, 2009, no. 3, pp. 57-63.

10. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 1985, Vol. IT-31, no. 4, pp. 469-472.

11. Moldovyan N.A., Moldovyan A.A. Class of Provably Secure Information Authentication Systems. *Springer Verlag CCIS.* 4th Int. Workshop MMM-ANCS'07 Proc. September 13-15, 2007. 2007, vol. 1. P. 147-152

12. Koutinho S. Introduction to Number Theory. RSA Algorithm [Vvedenie v Teoriyu Chisel. Algoritm RSA]. Moscow, Postmarket, 2001. 323 p. (In Russ.)

13. Rabin M.O. Digitalized signatures and public key functions as intractable as factorization. *Technical report MIT/LCS/TR 212, MIT Laboratory for Computer Sci.*, 1979.

14. Moldovyan A.A., Moldovyan N.A., Shcherbakov V.A. Short signatures from difficulty of the factoring problem. *Bull. Acad. de Stiinte a Republicii Moldova. Matematica*, 2013, no. 2-3, pp. 27-36.