Н. А. КАПАЛОВА

(Институт проблем информатики и управления, г. Алматы)

МОДИФИЦИРОВАННЫЙ АЛГОРИТМ ШИФРОВАНИЯ ЭЛЬ-ГАМАЛЯ НА БАЗЕ НЕПОЗИЦИОННЫХ ПОЛИНОМИАЛЬНЫХ СИСТЕМ СЧИСЛЕНИЯ

Аннотация

Представлены результаты модификации системы асимметричного шифрования по схеме Эль-Гамаля на базе непозиционных полиномиальных систем счисления (НПСС) и приведен контрольный пример. Использование НПСС при разработке и исследовании нетрадиционных алгоритмов и методов кодирования, шифрования и формирования электронной цифровой подписи и распределения криптографических ключей позволяет значительно повысить надежность и эффективность этих криптографических процедур. Схему Эль-Гамаля можно использовать как для цифровых подписей, так и для шифрования, криптографическая стойкость схемы основана на сложности проблемы дискретного логарифмирования в мультипликативной группе конечного поля. Она лежит в основе стандартов электронной цифровой подписи в США (DSA) и России. Надежность предлагаемого алгоритма повышается за счет выбора оснований НПСС и примитивных элементов. Все вычисления в НПСС производятся параллельно по модулям рабочих оснований, за счет этого сокращается время выполнения операций.

Ключевые слова: модификация, алгоритм, шифрование, системы счисления, Эль-Гамаль, цифровая подпись.

Кілт сөздер: модификация, алгоритм, шифрлау, есептеу жүйелері, Эль-Гамаль, сандық жазу.

Keywords: modification of the algorithm, encryption, number systems, El Gamal digital signature.

Введение. В 1976 г. У. Диффи и М. Хеллманом была опубликована работа, в которой изложены принципы криптографии с открытыми ключами. Рождение «новой криптографии» серьезно повлияло на дальнейшее развитие средств криптографии. Во-первых, алгоритмы криптографии с открытым ключом используют математические функции, отличные от подстановок и переста-новок. Во-вторых, методы криптографии с открытым ключом являются асимметричными – в них используются два разных ключа при зашифровании и расшифровании. Это отличает их от методов традиционного (симметричного) шифрования, где предполагается только один секретный ключ. Идея применения двух разных ключей повлекла глубокие изменения в подходах к обеспечению конфиденциальности. Алгоритмы шифрования с открытым ключом зависят от одного ключа для зашифрования и другого, связанного с первым, ключа для расшифрования. Эти алгоритмы имеют следующую важную особенность:

– с точки зрения вычислений нереально определить ключ расшифрования, зная только используемый криптографический алгоритм и ключ зашифрования;

– любой из этих двух связанных ключей может служить для зашифрования, и тогда другой ключ может применяться для расшифрования.

Известными примерами систем шифрования с открытым ключом являются системы RSA, Эль-Гамаля, Мак-Элиса. Одним из заблуждений, касающийся шифрования с открытым ключом, было мнение, что шифрование с открытым ключом оказывается более универсальным подходом, что делает традиционное симметричное шифрование устаревшим. Но оказалось, что это не так, поскольку

реализация схем шифрования с открытым ключом требует значительно больше вычислительных ресурсов, чем алгоритмы симметричных систем. Поэтому утверждения об отказе от схем традиционного шифрования явились необоснованными. Как отметил один из открывателей метода шифрования с открытым ключом Уитфилд Диффи, шифрование с открытым ключом нашло применение в сфере управления ключами и приложениях электронной цифровой подписи.

Использование непозиционных полиномиальных систем счисления (НПСС) при разработке и исследовании нетрадиционных алгоритмов и методов кодирования, шифрования и формирования электронной цифровой подписи (ЭЦП) и распределения криптографических ключей позволяет значительно повысить надежность и эффективность этих криптографических процедур, уменьшить длину ЭЦП и дополнить ЭЦП свойством обнаружения ошибок и исправления одиночной ошибки [1-3].

Криптографическая стойкость системы шифрования Эль-Гамаля с открытым ключом основана на сложности проблемы дискретного логарифмирования в мультипликативной группе конечного поля. Эта задача сложно реализуема для значений p, содержащих более 150 десятичных знаков. Рекомендуется выбирать p таким, чтобы число p-1 содержало большой простой делитель. Недостатком криптосистемы Эль-Гамаля является удвоение длины открытого текста при шифровании, а также необходимость использования различных значений рандомизатора для зашифрования различных открытых текстов.

Модифицированный алгоритм шифрования Эль-Гамаля на базе НПСС. Схему Эль-Гамаля можно использовать как для цифровых подписей, так и для шифрования. Алгоритм Эль-Гамаля не запатентован, он первый криптографический алгоритм с открытым ключом, пригодный для шифрования и цифровых подписей, применение которого не ограничено патентами США (срок патента Диффи-Хеллмана закончился 29.04.1997 г.). Схема Эль-Гамаля лежит в основе стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-2001).

В работе представлены результаты модификации системы асимметричного шифрования по схеме Эль-Гамаля. на базе НПСС. Разработанный нетрадиционный асимметричный алгоритм шифрования электронного сообщения M по схеме Эль-Гамаля осуществляется следующим образом [1-4].

1. Вначале формируется НПСС: ее основаниями (рабочими) выбираются неприводимые многочлены

$$p_1(x), p_2(x),..., p_S(x) \quad (1)$$

над полем $GF(2)$ степени m_1, m_2, …, m_S соответственно так, чтобы вычеты по этим основаниям покрывали длину подписываемого сообщения. Полиномы (1) с учетом порядка их расположения образуют одну систему оснований. В соответствии с Великой китайской теоремой об остатках все основания должны быть различными, в том числе и тогда, когда они имеют одну степень. Рабочий диапазон НПСС определяется многочленом (модулем) $P_S(x) = p_1(x)p_2(x)...p_S(x)$ степени $m = \sum_{i=1}^{S} m_i$. В этой системе любой многочлен $F(x)$, степени меньшей m, имеет единственное представление вида

$$F(x) = (z_1(x), z_2(x),..., z_S(x)), \quad (2)$$

где $F(x) \equiv z_i(x)(\mathrm{mod}(p_i(x))$, $i = \overline{1, S}$. По виду (2) восстанавливается позиционное представление $F(x)$ с использованием следующей формулы:

$$F(x) = \sum_{i=1}^{S} z_i(x) B_i(x), \text{ где } B_i(x) = \frac{P_S(x)}{p_i(x)} M_i(x) \equiv 1(\mathrm{mod}\ p_i(x)).$$

(3)

Затем сообщение *M* длиной *N* бит интерпретируется как последовательность остатков $z_1(x), z_2(x), ..., z_S(x)$ от деления некоторого многочлена *M*(*x*), степени меньше *m* на рабочие основания $p_1(x), p_2(x), ..., p_S(x)$ соответственно и записывается в непозиционном виде в виде последовательности вычетов:

$$M(x) = (z_1(x), z_2(x), ..., z_S(x)),$$

(4)

где $M(x) \in z_i(x)(\mathrm{mod}\ p_i(x))$, $i = \overline{1, S}$. Далее многочлен *M*(*x*) будет записываться без аргумента, т.е. в виде *M*.

Для каждого основания $p_i(x)$ выбирается примитивный элемент (многочлен) $\alpha_i(x)$ из полной системы вычетов по модулю $p_i(x)$, т. е. степени $\alpha_i(x)$ не превышают m_i, где $i = \overline{1, S}$. Тогда примитивный элемент нетрадиционного алгоритма шифрования интерпретируется как последовательность остатков от деления некоторого многочлена $\alpha(x)$ на основания $p_1(x)$, $p_2(x)$, …, $p_S(x)$ соответственно:

$$\alpha(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)),$$

где $\alpha(x) \in \alpha_i(x)(\mathrm{mod}\ p_i(x))$, $i = \overline{1, S}$. Выбранные рабочие основания и соответствующие им примитивные многочлены $\alpha_i(x)$ содержатся в секрете.

Далее определяются базисы НПСС по формуле (3) для восстановления результата в позиционном виде по его остаткам. Для этого вычисляются многочлены

$$\delta_i(x) \in \frac{P_S(x)}{p_i(x)} (\mathrm{mod}\ p_i(x))$$

и инверсные к ним полиномы $\delta_i^{-1}(x)$:

$$\delta_i^{-1}(x)\delta_i(x) \in 1(\mathrm{mod}\ p_i(x)).$$

Тогда базисы находятся по формуле

$$B_i(x) \delta= (_i^{-1}) x\ \frac{P_S(x)}{p_i(x)},$$

которые также являются секретными параметрами алгоритма.

2. Затем пользователи *A* и *B* независимо друг от друга выбирают соответственные личные (закрытые) ключи $1 < l_A, l_B < 2^m$.

3. Потом пользователи *A* и *B* вычисляют третий элемент открытого ключа соответственно:

$$\beta_A(x) = (\beta_{A_1}(x), \beta_{A_2}(x), ..., \beta_{A_S}(x)), \text{ где } \beta_A(x) \equiv \alpha_i^{l_A}(x)(\mathrm{mod}(p_i(x)), i = \overline{1, S};$$

$\beta_B(x) = (\beta_{B_1}(x), \beta_{B_2}(x), ..., \beta_{B_S}(x))$, где $\beta_B(x) \equiv \alpha_i^{l_B}(x)(\mathrm{mod}(p_i(x)), i = \overline{1,S}$.

Все операции возведения в степень вычисляются в непозиционной полиномиальной системе счисления, поэтому эти вычислении операций могут выполняться параллельно по модулям полиномов, выбранных в качестве оснований системы.

4. После этого стороны *A* и *B* обмениваются вычисленными значениями открытых ключей соответственно

$$K_A(x) = (P_S(x), \alpha(x), \beta_A(x)), \quad K_B(x) = (P_S(x), \alpha(x), \beta_B(x))$$

в двоичном представлении по незащищенному каналу.

5. Используя открытые ключи адресата пользователи *A* и *B* выполняют процесс шифрования сообщения *M* в виде (4) по аналогии с традиционной схемой Эль-Гамаля в соответствии с алгоритмом зашифрования E_k:

$$E_k(M) = (C_1, C_2), \text{ где } C_1 = \alpha^r(\mathrm{mod}(P_S(x)), \; C_2 = M \cdot \beta^r(\mathrm{mod}(P_S(x)),$$

где *r* – случайно выбираемое число (рандомизатор) и $0 \le r \le 2^m$.

6. Для расшифрования зашифрованного сообщения в соответствии с алгоритмом расшифрования D_k пользователи *A* и *B* используют свои личные ключи:

$$D_k(C_1, C_2) = C_2 \cdot (C_1^{l_i})^{-1} \bmod P_S(x) = M, \text{ где } i = A, B.$$

Все вычисления в НПСС производятся параллельно по модулям рабочих оснований $p_1(x)$, $p_2(x)$, …, $p_S(x)$, вследствие этого существенно возрастает скорость выполнения операций.

Рассмотрим пример. Пусть пользователь *A* вычисляет открытый ключ и публикует его для того, чтобы пользователь *B* мог писать ему сообщения. Затем пользователь *A* выполняет следующие действия.

1. Формирует НПСС: ее основаниями выбираются неприводимые многочлены: $p_1(x) = x^2 + x + 1$, $p_2(x) = x^4 + x^3 + 1$ и $p_3(x) = x^4 + x + 1$.

2. Для каждого основания $p_1(x)$, $p_2(x)$, …, $p_3(x)$ выбирает соответственно примитивный элемент (многочлен) $\alpha_1(x) = x^2+x$, $\alpha_2(x) = x^2$, $\alpha_3(x) = x^3+x+1$. Выбранные рабочие основания и соответствующие им примитивные многочлены держатся в секрете.

3. Затем выбирает личный (закрытый) ключ $l_A = 3$ так, что $1 < l_A < 2^m$.

4. Вычисляет третий элемент открытого ключа: $\beta_A(x) = (\beta_{A_1}(x), \beta_{A_2}(x), \beta_{A_3}(x))$, где

$$\beta_{A_1}(x) \equiv \alpha_1^{l_A}(x)(\mathrm{mod}(p_1(x)) = (x^2 + x)^3 \bmod(x^3 + x + 1) = x^2 + x + 1;$$

$$\beta_{A_2}(x) \equiv \alpha_2^{l_A}(x)(\mathrm{mod}(p_2(x)) = (x^2)^3 \bmod(x^4 + x^3 + 1) = x^3 + x^2 + x + 1;$$

$$\beta_{A_3}(x) \equiv \alpha_3^{l_A}(x)(\mathrm{mod}(p_3(x)) = (x^3 + x + 1)^3 \bmod(x^4 + x + 1) = x^3 + x^2.$$

5. После этого *A* публикует значения открытых ключей соответственно:

$$K_A(x) = \{ (p_1(x), p_2(x), p_3(x)); (\alpha_1(x), \alpha_2(x), \alpha_3(x)); (\beta_1(x), \beta_2(x), \beta_3(x)) \}.$$

Так как порядок и значения рабочих основании $p_1(x), p_2(x), p_3(x)$ и примитивные $\alpha_1(x), \alpha_2(x), \alpha_3(x)$ оговариваются между пользователями заранее, по незащищенному каналу передается только общий вид $P(x)$, $\alpha(x)$ и $\beta(x)$ в двоичном представлении.

Используя открытые ключи адресата A, пользователь B выполняет процесс зашифрования сообщения $M = \{10010110100\}$, которое представляется в виде последовательности вычетов по рабочим основаниям:

$$M_1 = \{100\} = x^2, M_2 = \{1011\} = x^3 + x + 1, M_1 = \{0100\} = x^2 .$$

6. Пользователь B выбирает случайные числа $r_1 = 4$, $r_2 = 4$ и $r_3 = 9$, где $0 \le r \le 2^{11}$. Сообщение шифруется следующим образом:

$$C_{1A_1} = \alpha_1^r(x) = x + 1,\ C_{1A_2} = \alpha_2^r(x) = x^3 + x^2 + x,\ C_{1A_3} = \alpha_3^r(x) = x^2 + x + 1,$$

$$C_{2A_1} = M_1 \cdot \beta_1^r(x) = x,\ C_{2A_2} = M_2 \cdot \beta_2^r(x) = x^3 + x^2,\ C_{2A_3} = M_3 \cdot \beta_3^r(x) = x^3 + x^2 + x .$$

Тогда зашифрованный текст выглядит так:

$$C_{1A} = \{x + 1,\ x^3 + x^2 + x,\ x^2 + x + 1\} = \{011,1110,0111\},$$

$$C_{2A} = \{x,\ x^3 + x^2, \mathrm{x}^3 + x^2 + x\} = \{010,1100,1110\} .$$

7. Для расшифрования зашифрованного сообщения пользователь A использует свои личные ключи:

$$\left(C_{1A_1}^{l_A}\right)^{-1} = (x+1)^{-1} \bmod p_1(x) = x,\ \left(C_{1A_2}^{l_A}\right)^{-1} = (x^2+1)^{-1} \bmod p_2(x) = x^3 + x^2 + x + 1,$$
$$\left(C_{1A_3}^{l_A}\right)^{-1} = (x^3 + x)^{-1} \bmod p_3(x) = x^3 + x^2 \text{ и } M_1 = C_{2A_1} \cdot (C_{1A_1}^{l_A})^{-1} = (x \cdot x) \bmod p_1(x) = x^2,$$
$$M_2 = C_{2A_2} \cdot (C_{1A_2}^{l_A})^{-1} = (x^3 + x^2)(x^3 + x^2 + x + 1) \bmod p_2(x) = x^3 + x + 1,$$

$$M_3 = C_{2A_3} \quad (C_{1A_3}^{l_A})^{\ 1} = (x^3 + x^2 + x) \quad (x^3 + x^2) \bmod p_3(x) = x^2 .$$

Таким образом, расшифрованное сообщение имеет вид:

$$M = \{M_1, M_2, M_3\} = \{x^2, x^3 + x + 1, x^2\} = \{10010110100\} .$$

Надежность предлагаемого алгоритма повышается за счет выбора оснований НПСС и примитивных элементов. Другое достоинство – сокращение времени выполнения операций возведения в степень за счет распараллеливания по модулям оснований НПСС. Криптостойкость алгоритма характеризуется выбором оснований НПСС и соответствующих им примитивных многочленов, базисов НПСС, личных ключей пользователей.

ЛИТЕРАТУРА

1 Бияшев Р.Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: Дис. ... докт. тех. наук. – М., 1985. – 328 с.

2 Капалова Н.А., Нысанбаева С.Е. Исследование нетрадиционного алгоритма открытого распределения ключей // Инфокоммуникационные технологии в науке, производстве и образовании: Третья Межд. науч.-практ. конф. – Ч. III. – г. Ставрополь, Северо-Кавказ. гос. техн. ун-т, 1-5 мая 2008. – С. 217-222.

3 Нысанбаева С.Е. Система электронной цифровой подписи с открытым ключом на базе модулярной арифметики // Математический журнал. – 2011. – № 2. – С. 58-63.

4 Капалова Н.А. Алгоритм шифрования на базе непозиционных полиномиальных систем счисления с использованием системы Эль-Гамаля // Инфокоммуникационные технологии в науке, производстве и образовании: Пятая Межд. науч.-практ. конф. – Ч. II. – г. Ставрополь, Северо-Кавказ. гос. техн. ун-т, 2-6 мая 2012. – С. 225-227.

REFERENCES

1 Biiashev R.G. Razrabotka i issledovanie metodov skvoznogo povysheniia dostovernosti v sistemakh obmena dannymi raspredelennykh ASU: Dis. ... dokt. tekh. nauk. – M., **1985**. – 328 s. (in Russ.)

2 Kapalova N.A., Nysanbaeva S.E. Issledovanie netraditsionnogo algoritma otkrytogo raspredeleniia kliuchei // Infokommunikatsionnye tekhnologii v nauke, proizvodstve i obrazovanii: Tret'ia Mezhd. nauch. prakt. konf. Ch. III. g. Stavropol', Severo Kavkaz. gos. tekhn. un t, 1-5 maia **2008**. – S. 217-222. (in Russ.)

3 Nysanbaeva S.E. Sistema elektronnoi tsifro¬voi podpisi s otkrytym kliuchom na baze moduliarnoi arifmetiki // Matematicheskii zhurnal. – **2011**. – № 2. – S. 58-63. (in Russ.)

4 Kapalova N.A. Algoritm shifrovaniia na baze nepozitsionnykh polinomial'nykh sistem schisleniia s ispol'zovaniem sistemy El'-Gamalia // Infokommunikatsionnye tekhnologii v nauke, proizvodstve i obrazovanii: Piataia Mezhd. nauch.-prakt. konf. Ch. II. g. Stavropol', Severo-Kavkaz. gos. tekhn. un-t, 2-6 maia **2012**. – S. 225-227. (in Russ.)

Резюме

Н. А. Капалова

(Информатика және басқару проблемалары институты, Алматы қ.)

ПОЗИЦИЯЛЫ ЕМЕС ПОЛИНОМДЫ САНАУ ЖҮЙЕСІ НЕГІЗІНДЕ

ЭЛЬ-ГАМАЛЬ ШИФРЛАУ АЛГОРИТМІНІҢ МОДИФИКАЦИЯСЫ

Позициялы емес полиномды санау жүйесі (ППСЖ) негізінде Эль-Гамаль асимметириялық шифрлау сызбасын модификациялау нәтижелері келтірілген. Дәстүрлі емес кодттау, шифрлау, электрондық сандық қолтаңбаларды құру және криптографиялық кілттерді тарату алгоритмдері мен әдістерін құру мен зерттеуде ППСЖ қолдану, осы криптографиялық шаралардың тұрақтылығы мен тиімділігін мейлінше арттырады. Эль-Гамаль сызбасын шифрлеуге, сондай-ақ электрондық сандық қолтаңбаларды құру үшін де қолдануға болады, оның тұрақтылығы ақырлы сақинаның мультипликативті тобында дискретті логарифмдеу мәселесінің қиындығына негізделген. Оны АҚШ пен Ресей электрондық сандық қолтаңба стандарттарының негізі ретінде алған. Ұсынылып отырған алгоритмның тұрақтылығы ППСЖ негіздері мен қарапайым элементтерін таңдау есебінен өседі. ППСЖ барлық есептеулер жұмысшы негіздерінің модулдері бойынша параллельді түрде орындалады, сондықтан амалдарды орындау уақыты қысқарады.

Кілт сөздер: модификация, алгоритм, шифрлау, есептеу жүйелері, Эль-Гамаль, сандық жазу.

Summary

N. A. Kapalova

(Institute for problems of informatics and control, Almaty)

THE MODIFIED ALGORITHM OF ENCRYPTION EL GAMAL

ON THE BASIS OF NOT POSITIONAL POLYNOMIAL NOTATIONS

This paper presents the results of modification of the system of asymmetric encryption scheme El Gamal based on not positional polynomial notations (NPPN) are and the control example is reduced. Using the NPPN in the development and research of innovative algorithms and methods for encoding, encryption and digital signature of formation and distribution of cryptographic keys can significantly increase the reliability and effectiveness of these cryptographic procedures. El Gamal scheme can be used for digital signatures and encryption, cryptographic security scheme based on the complexity of the discrete logarithm problem in the multiplicative group of a finite field. It is the basis of standards of digital signature in the U.S. (DSA) and Russia. The reliability of the proposed

algorithm is improved by selecting the grounds NPPN and primitive elements. All calculations are done in parallel to the NPPN on modules operating bases, due to this reduced running times.

Keywords: modification of the algorithm, encryption, number systems, El Gamal digital signature.

Поступила 1.02.1213г