УДК 004.056.5

Р.Г. Бияшев[1], С.Е. Нысанбаева[1], Е.Е. Бегимбаева[2]
([1]Институт информационных и вычислительных технологий КН МОН РК,
Казахский национальный университет им. ал-Фараби,
Казахстан, г. Алматы, enlik_89@mail.ru)

МОДИФИЦИРОВАННАЯ АСИММЕТРИЧНАЯ СИСТЕМА ЦИФРОВОЙ ПОДПИСИ

Аннотация. В статье описывается модель асимметричной нетрадиционной системы цифровой подписи. Нетрадиционными, непозиционными или модулярными называются криптосистемы, разработанные на базе непозиционных полиномиальных систем счисления (НПСС). Модель подписи строится на основе схемы цифровой подписи Digital Signature Algorithm (DSA) и НПСС. Применение НПСС позволит повысить криптостойкость криптосистем и сократить длину ключа.

Ключевые слова: Цифровая подпись, асимметричная схема, непозиционныеполиномиальные системы счисления, криптостойкость.

В системах безопасности информационного обмена для защиты данных при передаче и обмене данными используются криптографические системы цифровой подписи (ЦП). В связи с их широким применением в настоящее время тщательно исследованы многие аспекты теории и практики цифровых подписей с открытым ключом. Основы криптографии с открытыми ключами были выдвинуты У.Диффи (Whitfield Diffie), М.Хеллманом (Martin Hellman) и была впервые представлена в работе [1]. Криптосистемы с открытым ключом нашли применения в сфере приложения ЭЦП. В асимметричных схемах цифровой подписи подписание документа производится с применением закрытого ключа, а проверка подписи - открытого. Системы ЭЦП с открытым ключом включают три процесса: генерация ключевой пары для подписи и ее проверки, формирование цифровой подписи и проверка подлинности подписи.

Основой для создания предлагаемой модели ЦП являются разработанные нетрадиционные системы цифровой подписи [2,3]. Эти системы разработаны на базе алгебраического подхода с использованием непозиционных полиномиальных систем счисления (НПСС) или полиномиальных систем счисления в остаточных классах (полиномиальных СОК). В классической СОК в качестве системы оснований выбираются положительные целые числа $(p_1, p_2, \ldots, p_n)$, и в ней целое положительное число A представляется в виде последовательности вычетов

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n) \quad (1)$$

от деления на систему оснований $(p_1, p_2, \ldots, p_n)$ [4]. Построение СОК основано на использовании китайской теоремы об остатках. В соответствии с этой теоремой представление числа A в виде последовательности вычетов является единственным, если основания $(p_1, p_2, \ldots, p_n)$ будут попарно просты между собой. Цифры α_i образуются следующим образом:

$$\alpha_i = A - [A/p_i]p_i \,, \; i = \overline{1,n} \,, \quad (2)$$

где $[A/p_i]$ - целая часть от деления A на p_i. Из (2) следует, что цифра *i*-го разряда α_i числа A это наименьший положительный остаток от деления A на p_i и $\alpha_i < p_i$. Объем диапазона представимых чисел в этом случае равен $P = p_1 p_2 \cdots p_n$. Здесь, диапазон представимых чисел растет как произведение оснований, а разрядность чисел растет как сумма разрядностей тех же оснований.

В отличие от классических СОК, где основаниями служат простые числа, в НПСС основаниями служат неприводимые многочлены над полем $GF(2)$ [2]. Использование НПСС позволяет уменьшить длину ключей, повысить стойкость и эффективность непозиционных криптографических алгоритмов [3]. Повышение эффективности обеспечивается за счет правил НПСС, где все арифметические операции могут выполняться параллельно по модулям оснований НПСС. В разработанных нетрадиционных криптографических алгоритмах формирование цифровой подписи осуществляется

для электронного сообщения заданной длины. В непозиционных криптосистемах в качестве критерия криптостойкости используется криптостойкость самих алгоритмов формирования цифровой подписи, которая характеризуется полным секретным ключом. Криптостойкость определяется не только длиной секретной ключевой последовательности, но и выбранными системами полиномиальных оснований. С ростом порядка неприводимых многочленов с двоичными коэффициентами их количество стремительно растет [5]. Ввиду этого возможен широкий выбор полиномиальных оснований. Криптостойкость предложенных алгоритмов формирования цифровой подписи с использованием НПСС существенно возрастает с увеличением длины электронного сообщения [3,6].

Формирование НПСС для подписываемого электронного сообщения M длины N бит происходит путем выбора системы рабочих оснований с двоичными коэффициентами[2,3,6]

$$p_1(x), p_2(x), \dots, p_S(x), \tag{3}$$

где $p_i(x)$ – неприводимые многочлены над полем $GF(2)$ степени m_i, $i = \overline{1,S}$соответственно. Основной рабочий диапазон НПСС представляетсямногочленом $P_S(x) = \prod_{i=1}^{S} p_i(x)$ степени $m = \sum_{i=1}^{S} m_i$. Все выбираемые рабочие основания должны отличаться друг от друга (согласно китайской теореме об остатках), даже если они являются неприводимыми полиномами одной степени.

В НПСС любой многочлен $F(x)$, степень которого меньше m, имеет непозиционное представление в виде последовательности вычетов от его деления на основания $p_1(x), p_2(x), \dots, p_S(x)$и оно является единственным:

$$F(x) = (a_1(x), a_2(x), \dots, a_S(x), \tag{4}$$

где $F(x) \equiv (a_i(x) (\mathrm{mod} p_i(x))$, $i = 1,S$. По виду (4) восстанавливается позиционное представление многочлена $F(x)$[2,3]:

$$F(x) = \sum_{i=1}^{S} a_i(x) B_i(x), B_i(x) = \frac{P_S(x)}{p_i(x)} M_i(x) \equiv 1 (\mathrm{mod}\, p_i(x)), i = 1,S \tag{5}$$

Многочлены $M_i(x)$выбираются такие, чтобы выполнялось сравнение (5).

В НПСС электронное сообщение длины N бит интерпретируется как последовательность остатков от деления некоторого многочлена (обозначим его также F(x)) соответственно на рабочие основания $p_1(x), p_2(x), \dots, p_S(x)$ степени не выше N, т.е. в виде (4). Основания выбираются из числа всех неприводимых полиномов степени от m_1 до m_S из условия выполнения уравнения[4]:

$$k_1 m_1 + k_2 m_2 + \cdots + k_S m_S = N \tag{6}$$

В уравнении (6) $0 \le k_i \le n_i, i = \overline{1,S}$- неизвестные коэффициенты и число выбранных неприводимых многочленов степениm_i. Один конкретный набор этих коэффициентов является одним из решений (6) и задает одну систему рабочих оснований, n_i - количество всех неприводимых многочленов степениm_i, $1 \le m_i \le N$, $S = \sum_{i=1}^{S} k_i$ - число выбранных рабочих оснований. В системе рабочих оснований учитывается также порядок расположения оснований. Уравнение (6) определяет количество S рабочих оснований, вычеты по которым покрывают длину N заданного сообщения. Полные системы вычетов по модулям многочленов степени m_i включают в себя все полиномы степени не выше $m_i - 1$, для записи которых необходимы m_i бит. С увеличением степени неприводимых многочленов их количество стремительно растет, в связи с этим также значительно увеличивается количество решений уравнения (6).

При формировании симметричной ЦП в НПСС вводится избыточность:подписываемое сообщениеM расширяется на избыточные основания $p_{S+1}(x), p_{S+2}(x), \dots, p_{S+U}(x)$. Они выбираются произвольно из всех неприводимых многочленов степени, не превышающей значенияN_k, где $j = \overline{1,U}$. Система избыточных оснований формируется независимо от выбора рабочих оснований $p_i(x), i = \overline{1,S}$,но среди U избыточных оснований могут быть и совпадающие с некоторыми из рабочих оснований. Пусть $a_1, a_2, \dots, a_U$ и $d_1, d_2, \dots, d_U$степени и число

неприводимых многочленов соответственно, используемых при их выборе. Число выбранных избыточных оснований в этом случае определяется из уравнения (аналога уравнения (6)):

$$t_1 a_1 + t_2 a_2 + \cdots + t_U a_U = N_k, \quad (7)$$

где $0 \le t_j \le d_j$, $0 \le a_j \le N_k, j = \overline{1,U}$, t_j - количество выбранных избыточных оснований степени $a_j, U = \sum_{i=1}^{U} t_i$– число выбранных избыточных оснований, запись вычетов по которым покрывает хэш-значение длины N_k. Решение уравнения (7) определяет одну систему избыточных оснований.

Далее, вычисляются избыточные вычеты $\alpha_{S|1}(x), \alpha_{S|2}(x), \ldots, \alpha_{S|U}(x)$ от деления восстановленного многочлена $F(x)$ на избыточные основания $p_{S+j}(x)$, $j = \overline{1,U}$. Тогда хэш-значение интерпретируется как последовательность этих вычетов:

$$h(F(x)) = (\alpha_{S+1}(x), \alpha_{S+2}(x), \ldots, \alpha_{S+U}(x)) \quad (8)$$

где $h(F(x)) \equiv \alpha_{S+j}(x) \bmod p_{S+j}(x)), j = \overline{1,U}$. Сумма длин избыточных вычетов составляет длину хэш-значения и ЭЦП.

Схема цифровой подписи Эль-Гамаля [8] основана на трудности вычисления дискретных логарифмов в конечном поле. Алгоритм цифровой подписиDSAпредставляет собой вариацию цифровой подписи схемы Эль-Гамаля и К.Шнорра. Его надежность основана на практической неразрешимости определенного частного случая задачи вычисления дискретного логарифма. Современные методы решения этой задачи имеют приблизительно ту же эффективность, что и методы решения задачи факторизации, в связи с этим предлагается использовать ключи длиной от 512 до 1024 бит с теми же характеристиками надежности, что и в системе RSA. Длина подписи в системе DSA меньше, чем в RSA, и составляет 320 бит.DSA является одним из алгоритмов, рекомендованных стандартом США для формирования ЦП [9].

Алгоритм DSA является “классическим” примером схемы ЦП на основе использования хэш-функции и асимметричного алгоритма шифрования. Стойкость системы в целом основана на сложности нахождения дискретных логарифмов в конечных полях.

Суть схемы электронной подписи DSA состоит в следующем. Пусть отправитель и получатель электронного документа используют при вычислении большие целые простые числа p иq: $2^{L-1} < p < 2^L, 512 \le L \le 1024, L$ кратно 64, $2^{159} < q < 2^{160}$, $q -$ простойделитель $(p-1)$и $g = h^{(p-1)/q} \bmod p$, гдеhлюбоецелоечисло, $1 < h < p-1$ такое, что$h^{\frac{p-1}{q}} (\bmod p) > 1$.

Секретный ключ b, случайно выбирается из диапазона $1 \le b \le q$ и держится в секрете. Вычисляется значение $\beta = g^b \bmod p$. Параметры p, q, g являются открытыми ключами и опубликовываются для всех пользователей системы информационного обмена с ЭЦП.

Рассмотрим формирование ЭЦП для сообщения M:

1. определяется хэш-значение hот подписываемого сообщения M: $h = h(M)$;
2. выбирается случайное целое число $r, 1 \le r \le q$, хранящееся в секрете и меняющееся от одной подписи к другой;
3. определяется значение: $\gamma = (g^r \bmod p) \bmod q$;
4. с использованием секретного ключа отправителя сообщениянаходится $\delta = (r'(h + b\gamma)) \bmod q$, где r' удовлетворяет условию $(r'r) \bmod q = 1$;
5. цифровой подписью для сообщения M являются пара чисел (γ, δ), которые передаются вместе с сообщением по открытым каналам связи.

Рассмотрим проверку ЭЦП: обозначим M', δ', γ'полученные версии M, δ, γ.

1. Проверяется выполнение условий $0 < \delta < q$ и $0 < \gamma < q$. При невыполнении хотя бы одного из условий цифровая подпись считается недействительной.
2. Вычисляется хэш-значение $h_1 = h(M')$ от полученного сообщения M'.
3. Находится значение $v = (\delta')^{-1} \bmod q$.
4. Вычисляются значения выражений: $z_1 = (h_1 v) \bmod q$ и $z_2 = (\gamma' v) \bmod q$.
5. Определяется значение: $u = ((g^{z_1} \beta^{z_2}) \bmod p) \bmod q$.

6. Если выполняется равенство $\gamma' - u$, то ЭЦП принимается, т.е. в процессе передачи не нарушена целостность сообщения:$M' - M$. При невыполнении этого равенства подпись считается недействительной.

Стойкость схемы DSAв первую очередь зависит от размера параметров p и q (в случае атаки «грубая сила»). Соответственно криптостойкость на параметр p в случае 512 и 160 бит будет равна 2^{160}. Успешная атака на параметр qвозможна только в том случае, если злоумышленник может вычислять дискретные логарифмы в полях Галуа $GF(2^{512})$.

Одной из теоретически возможных атак на схему DSA является компрометация параметра r. Для каждой подписи требуется новое значение r, которое должно быть выбрано случайным образом. Если злоумышленник найдет значение r, то секретный ключ b может быть раскрыт. Другой возможный вариант - две подписи были сгенерированы на одном значении r. В этом случае злоумышленник тоже в состоянии восстановить b. Следовательно, одним из факторов, повышающих безопасность использования схем ЭЦП, является наличие надежного генератора случайных чисел.

В DSA длина модуля преобразования составляет порядка 1024 битов. До такой же длины увеличены длины ключей. В связи с этим увеличивается вычислительная сложность криптографических преобразований, но уменьшается скорость вычислений. Сокращение длины ключа и повышение скорости вычислений возможно при разработке модификации этой схемы ЦП на базе НПСС.

Проводятся работы по созданию модулярной системы ЦП с открытым ключом, при создании которой будет использован модифицированный алгоритм DSA на базе НПСС. Вначале алгоритм DSA записывается в виде, в котором отсутствует второй модуль q и все вычисления производятся только по одному модулю p. Затем разрабатывается модификация этой схемы на базе НПСС.

Признательность, благодарность

Исследования проводятся в рамках грантового финансирования Министерства образования и науки Республики Казахстан.

ЛИТЕРАТУРА

[1] Diffi W., Hellman M. Privacy and Authentication: An Introduction to Cryptography // Proc. of the IEEE [Russian Translation]. – 1979. № 3, 71–109 p.

[2] Р.Г. Бияшев, Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: Дис. на соискание уч. степ. докт. тех. наук. - М., 1985. - 328 с.

[3] Biyashev R.G., Nyssanbayeva S.E. Algorithm for Creation a Digital Signature with Error Detection and Correction // Cybernetics and Systems Analysis. 4, 489-497 (2012).

[4] Акушский, И.Я., Юдицкий. Д.И. Машинная арифметика в остаточных классах. - М.: Советское радио, 1968. - 439 с.

[5] Бияшев Р.Г., Нысанбаева С.Е., Капалова Н.А. Секретные ключи для непозиционных криптосистем. Разработка, исследование и применение // LAP LAMBERT. Academ-ic Pablishing. - Germany, 2014. – 126 С.

[6] Нысанбаева С.Е. Разработка и исследование криптографических систем на базе непозиционных полиномиальных систем счисления: Дис. на соискание уч. степ. докт. тех. наук. – Алматы, 2009. – 240 с.

[7] Моисил Гр. К. Алгебраическая теория дискретных автоматических устройств. - М: Издательство иностранной литературы, 1963 . – 680 с.

[8] T. ElGamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory, v. IT-31, n. 4, 1985. P. 469-472.

[9] FIPS PUB 186. Digital Signature Standard (DSS).

REFERENCES

[1] Diffi W., Hellman M. Privacy and Authentication: An Introduction to Cryptography // Proc. of the IEEE [Russian Translation]. – 1979. № 3, 71–109 p.

[2] R.G. Biyashev, Razrabotka I issledovaniye metodov skvoznogo povysheniya dostovernosti v sistemah obmena dannymi raspredelennyh ASU: Doctoral Dissertation in Technical Sciences, Moscow, 1985. -M., 1985. - 328 p.

[3] Biyashev R.G., Nyssanbayeva S.E. Algorithm for Creation a Digital Signature with Error Detection and Correction // Cybernetics and Systems Analysis. 4, 489-497 (2012).

[4] Akushskii, I.Ya, Juditskii, D.I. Machine Arithmetic in Residue Classes [in Russian], Sov. Radio, Moscow (1968).

[5] Biyashev R.G., Nyssanbayeva S.E., Kapalova N.A. Sekretnye kluchi dlya nepozicionnyh kriptosistem. Razrabotka, issledovaniye I primeneniye // LAP LAMBERT. Academic Pablishing. - Germany, 2014. – 126 p.

[6] Nyssanbayeva S.E. Razrabotka i issledovaniye kriptographicheskih system na baze nepozicionnyh polinomialnyh system schisleniya: Doctoral Dissertation in Technical Sciences. – Almaty, 2009. -

[7] Moisil Gr.C. Algebraic Theory of Discrete Automatic Devices [Russian translation]. Inostr. Lit., Moscow (1963).

[8] T. ElGamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory, v. IT-31, n. 4, 1985. P. 469-472.

[9] FIPS PUB 186. Digital Signature Standard (DSS).

Р.Г. Бияшев, С.Е. Нысанбаева, Е.Е. Бегимбаева

Сандық қолтаңбаның модификацияланған асимметриялық жүйесі

Түйіндеме. Мақалада дәстүрлі емес сандық қолтаңба жүйесінің түрленген моделі қарастырылады. Позициялы емес полиномды санау жүйесі (ППСЖ) негізінде құралған криптожүйелер дәстүрлі емес, позициялы емес немесе модулдік деп аталады. Digital Signature Algorithm (DSA) сандық қолтаңба сұлбасы негізінде сандық колтаңба моделі құрылады. ППСЖ синонимі – классикалық қалындылар класындағы санау жүйесі (ҚКСЖ), модулді арифметика.

Негізгі сөздер: Сандық қолтаңба, позициялы емес полиномды санау жүйесі, криптотұрақтылық.

Р.Г. Бияшев, С.Е. Нысанбаева, Е.Е. Бегимбаева

Модифицированная асимметричная система цифровой подписи

Резюме. Описана модель модификаций нетрадиционной системы цифровой подписи. Нетрадиционными, непозиционными или модулярными называются криптосистемы, разработанные на базе непозиционных полиномиальных систем счисления (НПСС). Модель цифровой подписи строится на основе схемы цифровой подписи Digital Signature Algorithm (DSA) и НПСС. Применение НПСС позволят повысить криптостойкость криптосистем. Синонимы НПСС - классические системы счисления в остаточных классах (СОК), модулярная арифметика.

Ключевые слова: Цифровая подпись, непозиционные полиномиальные системы счисления, криптостойкость.

R.G. Biyashev, S.E. Nyssanbayeva, Ye.Ye. Begimbayeva

Modified asymmetric system of digital signature

Summary. A model of modification of unconventional system of digital signature are describes. Cryptosystems which developed on the basis of nonpositional polynomial notations (NPNs) are called unconventional, nonpositional or modular. Digital signature model based on the digital signature scheme of Digital Signature Algorithm (DSA) and NPNs. Application NPNs will allow improving cryptographic strength of the cryptosystems. Synonyms of NPNs - classical notations in residue number system (RNS), polynomial notations systems in RNS, modular arithmetic.

Key words: Digital signature, nonpositional polynomial notations, cryptostrength.

ӘОЖ 51(07)372.851

[1]Біргебаев А.Б., [2]Кокажаева А.Б., [3]Турлыбекова А.Т.

(Абай атындағы Қазақ Ұлттық педагогикалық Университеті

Қазақ мемлекеттік қыздар педагогикалық университеті.

Қ.И.Сәтбаев атындағы Қазақ Ұлттық техникалық университеті. Қазақстан Республикасы)

ЕНГІЗУЛЕР ТЕОРЕМАСЫ МЕН ОПЕРАТОРЛАР ТЕОРИЯСЫН ОҚЫТУДЫҢ ПСИХОЛОГИЯЛЫҚ АСПЕКТІЛЕРІ

Аннотация: Жұмыста функциональдық анализдің қолданбалы бөлімдерінің психалогиялық аспектілері сипатталады. Белгілі психолог және педагог мамандардың, сол сияқты математик ғалымдардың психологияның фундамаментальды мәселелері туралы ойлары талданады.Математикалық модельдеу және оны зерттеу мәселелерін сыртқы әлемді санаға барлық көпбейнелілігімен емес, ішкі және сыртқы толыққанды байланысымен емес, жуықтап бейнелейтін психологиялық деңгейде қарастырылатыны белгілі. Нақты құбылыс туралы ұғыну, сезіну арналары арқылы немесе бұрыннан белгілі білімге сүйеніп, жинақтаған толық емес ақпарат модель ретінде көріністер мен образдардың жүйесі сол күйде біздің санамыздан орын алады. Соның нәтижесінде біздің қоршаған орта туралы көзқарасымыз ұстанымдық түрде модельдік сипатталады. Қарастырылып отырған жұмыста белгілі бір саланың моделі ретінде берілген дифференциалдық теңдеулерді функциональдық анализдің әдістерімен, нақтырақ айтқанда операторлар теориясының әдістерімен шешудің психологиялық мәселелері талданған. Функциональдық анализдің әдістерімен шешілген дифференциалдық теңдеулер шешімдерінің оқу-тәрбие үрдісіндегі орны көрсетіледі.

Тірек сөздер: *операторлар, енгізулер теоремасы, интегралдық қосынды, математикалық моделдеу.*