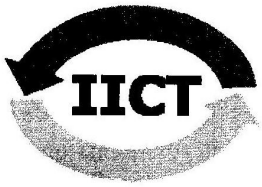
Институт информационных и вычислительных технологий
МОН РК



МАТЕРИАЛЫ

научной конференции

ИИВТ МОН РК

«Современные проблемы информатики и вычислительных технологий»

18-19 июня 2015 года

Алматы 2015

СОДЕРЖАНИЕ

РАЗРАБОТКА АСИММЕТРИЧНОЙ СИСТЕМЫ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ МОДУЛЯРНОЙ АРИФМЕТИКИ

Бияшев Р.Г., Нысанбаева С.Е., Бегимбаева Е.Е.
Институт информационных и вычислительных технологий МОН РК,
Алматы, Республика Казахстан
E-mail: brg@ipic.kz, sultasha1@mail.ru, enlik_89@mail.ru

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 криптосистемы и сократить длину ключа.

1 Введение

Нетрадиционные системы являются основой для создания предлагаемой модели асимметричной системы цифровой подписи (ЦП) на базе алгоритма DSA [1-3]. В классической системе в остаточных классах основаниями служат простые числа, а в НПСС основаниями являются неприводимые многочлены над полем $GF(2)$ [3]. Использование НПСС позволяет уменьшить длину ключей, повысить стойкость и эффективность непозиционных криптографических алгоритмов [4]. Повышение эффективности обеспечивается за счет правил НПСС, в которой все арифметические операции могут выполняться параллельно по модулям оснований НПСС.

В разработанных нетрадиционных криптографических алгоритмах формирование ЦП осуществляется для электронного сообщения заданной длины. В этих криптосистемах в качестве критерия криптостойкости используется криптостойкость самих алгоритмов формирования ЦП, которая характеризуется полным секретным ключом [3-5].

В работе [3] разработаны арифметика НПСС с полиномиальными основаниями и ее приложения к задачам повышения достоверности. Показано, что алгебра полиномов над некоторым полем по модулю неприводимого над этим полем многочлена является полем и представление полинома в непозиционном виде является единственным. Определены также правила выполнения арифметических операций в НПСС и восстановления многочлена по его остаткам. В соответствии с китайской теоремой об остатках все рабочие основания должны быть различными.

2 Формирование НПСС

Процесс формирование НПСС для подписываемого электронного сообщения M длины N бит происходит следующим образом. Выбираются системы рабочих оснований с двоичными коэффициентами

$$p_1(x), p_2(x), \ldots, p_S(x), \qquad (1)$$

где $p_i(x)$ – неприводимые многочлены над полем $GF(2)$ степени m_i соответственно $i = \overline{1,S}$. Основной рабочий диапазон НПСС представляется многочленом $P_S(x) = \prod_{i=1}^{S} p_i(x)$ степени $m = \sum_{i=1}^{S} m_i$. Все выбираемые рабочие основания должны отличаться друг от друга (согласно китайской теоремы 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 $p_1(x), p_2(x), \ldots, p_S(x)$ соответственно и оно является единственным:

$$F(x) = (\alpha_1(x), \alpha_2(x), \ldots, \alpha_S(x)), \quad (2)$$

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

$$F(x) = \sum_{i=1}^{S} \alpha_i(x) B_i(x),\ B_i(x) = \frac{P_S(x)}{p_i(x)} M_i(x) \equiv 1 (\mathrm{mod}\, p_i(x)), i = \overline{1,S}\ . \quad (3)$$

Многочлены $M_i(x)$ выбираются такие, чтобы выполнялось сравнение в (3).

В НПСС электронное сообщение длины N бит интерпретируется как последовательность остатков от деления некоторого многочлена (обозначим его также $F(x)$) соответственно на рабочие основания $p_1(x), p_2(x), \ldots, p_S(x)$ степени не выше N, т.е. в виде (2). Основания выбираются из числа всех неприводимых полиномов степени от m_1 до m_S из условия выполнения уравнения [6]:

$$k_1 m_1 + k_2 m_2 + \cdots + k_S m_S = N. \quad (4)$$

В уравнении (4) $0 \le k_i \le n_i$, $i = \overline{1,S}$ - неизвестные коэффициенты и число выбранных неприводимых многочленов степени m_i. Один конкретный набор этих коэффициентов является одним из решений (4) и задает одну систему рабочих оснований, n_i - количество всех неприводимых многочленов степени m_i, $1 \le m_i \le N$, $S = \sum_{i=1}^{S} k_i$ - число выбранных рабочих оснований. Уравнение (4) 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 [4-5].

В НПСС для получения ЦП используется хэш-значение от подписываемого сообщения.

3 Хэширование электронного сообщения в НПСС

Для хэширования сообщения M от длины N бит до N_k бит вводятся избыточные основания

$$p_{S+1}(x), p_{S+2}(x), \ldots, p_{S+U}(x). \quad (5)$$

Эти основания выбираются произвольно из всех неприводимых многочленов, степень которых не должны превышать N_k. Система избыточных оснований формируется независимо от выбора рабочих оснований. Среди U избыточных оснований могут быть и совпадающие с некоторыми из рабочих оснований. Пусть $a_1(x), a_2(x), \ldots, a_U(x)$

и $d_1(x), d_2(x), \ldots, d_U(x)$ степени и число неприводимых многочленов соответственно, используемых при их выборе. Число выбранных избыточных оснований в этом случае определяется из уравнения:

$$t_1 a_1 + t_2 a_2 + \cdots + t_U a_U = \mathrm{N}_k \,, \tag{6}$$

где $0 \le t_j \le d_j$, $0 \le a_j \le N_k$, $j = \overline{1,\mathrm{U}}$, t_j - количество выбранных избыточных оснований степени a_j $U = t_1 + t_2 + \cdots + t_U$ – число выбранных избыточных оснований, запись вычетов по которым покрывает хэш-значение длины N_k. Решение уравнения (6) определяет одну систему избыточных оснований.

Следующим этапов вычисления хэш-значения является вычисление избыточных вычетов

$$\alpha_{S+1}(x), \alpha_{S+2}(x), \ldots, \alpha_{S+U}(x) \tag{7}$$

от деления восстановленного многочлена $F(\mathrm{x})$ на избыточные основания (5). Тогда хэш-значение интерпретируется как последовательность этих вычетов:

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

где $h(\mathrm{F(x)}) \equiv \alpha_{S+j}(x) \bmod \mathrm{p}_{S+j}(x)), \mathrm{j} = \overline{1,U}$. Сумма длин избыточных вычетов (7) составляет длину хэш-значения и ЦП.

Для полученного хэш-значения будет построена непозиционная асимметричная система ЦП.

4 Асимметричная цифровая подпись на базе НПСС

Digital Signature Algorithm (DSA) - это схема цифровой подписи [7], которая была принята в 1994 году, как стандарт США и действовала до 2001 г. Схема является вариацией ЦП Эль-Гамаля и К.Шнорра. Надежность DSA основана на практической неразрешимости определенного частного случая задачи вычисления дискретного логарифма.

Суть схемы ЦП DSA состоит в следующем. Отправитель и получатель электронного документа используют при вычислении большие целые простые числа p и q, в диапазоне $2^{L-1} < p < 2^L$, $512 \le L \le 1024$, L кратно 64, $2^{159} < q < 2^{160}$, q - простой делитель $(p-1)$ и $g = h^{(p-1)/q} \bmod p$, где h любое целое число, $1 < h < p-1$ такое, что $h^{(\mathrm{p}-1)/\mathrm{q}} (\mathrm{mod\,p}) > 1$.

b является секретным ключом, который держится в секрете и случайно выбирается из диапазона $1 < b < q$. Вычисляется значение $\beta = g^b \bmod p$. Параметры (p,q,g) - открытые ключи, которые опубликовываются для всех пользователей системы информационного обмена с ЦП.

Процесс формирование ЦП для сообщения M состоит из следующих шагов:

1. вычисляется хэш-значение h от подписываемого сообщения M : $h = h(M)$;

2. выбирается хранящееся в секрете случайное целое число r, $1 \le r \le q$ и меняющееся от одной подписи к другой;

3. вычисляется значение: $\gamma = (g^r \bmod p) \bmod q$;

4. вычисляется $\delta = \left(r^{-1}\left(h + b\gamma\right)\right) mod\, q$, где r^{-1} удовлетворяет условию $\left(r^{-1} r\right) mod\, q = 1$;

5. ЦП для сообщения M являются пара чисел (γ, δ). Они передаются вместе с сообщением по открытым каналам связи.

Процесс проверки ЦП состоит из следующих шагов: (обозначим M', δ', γ' полученные версии M, δ, γ).

1. выполняется проверка условий $0 < \gamma, \delta < q$. Если не выполняется, хотя бы одно из условий ЦП, то ЦП считается недействительной.

2. вычисляется хэш-значение $h_1 = h(M')$ от полученного сообщения M'.

3. вычисляется значение $v = (\delta')^{-1} mod\, q$.

4. вычисляются значения выражений: $z_1 = (h_1 v) mod\, q$ и $z_2 = \left(\gamma' v\right) mod\, q$.

5. определяется значение: $u = \left(\left(g^{z_1}\, \beta^{z_2}\right) mod\, p\right) mod\, q$.

6. если выполняется равенство $\gamma' = u$, то ЦП принимается. Значит, при процессе передачи сообщения не нарушена целостность сообщения. В противном случае, подпись считается недействительной.

При построении непозиционной асимметричной системы ЦП вначале производится модификация алгоритма DSA: исключается второй модуль q, т.к. для вычисления ЦП будет использовано полученное выше хэш-значение в НПСС. Затем для построенного алгоритма DSA по одному модулю p будет разработана непозиционная система цифровой подписи длины N_k.

Полученный электронный документ (хэш-значение) длины N_k (8) рассматривается в непозиционной полиномиальной системе счисления, в которой и будет разработана непозиционная асимметричная система ЦП. Для этой НПСС выбираются полиномиальные основания

$$\eta_1(\mathrm{x}), \eta_2(\mathrm{x}), ..., \eta_W(\mathrm{x}), \tag{9}$$

по аналогии с выбором рабочих оснований в разделе 2. Пусть $q_1, q_2, ..., q_W$ и $l_1, l_2, ..., l_W$ степени и число неприводимых многочленов соответственно, используемых при их выборе. Число выбранных избыточных оснований в этом случае определяется из аналога уравнений (4) и (6).

Затем для оснований (9) находятся соответственные порождающие элементы (полиномы) $g_1(\mathrm{x}), g_2(\mathrm{x}), ..., g_W(\mathrm{x})$, которые являются аналогом примитивных элементов в алгоритме DSA.

Выбирается также секретный ключ отправителя b в диапазоне $[1, 2^q]$, где q является суммой степеней $q_1, q_2, ..., q_W$.

Вычисляется значение открытого ключа $\beta(\mathrm{x}) : \beta(\mathrm{x}) = (\beta_1(\mathrm{x}), \beta_2(\mathrm{x}), ..., \beta_w(\mathrm{x}))$ по модулю оснований (7).

Далее, выбирается случайное целое число r из диапазона $[1, 2^q]$.

Полиномы $\gamma(\mathrm{x})$ и $\delta(\mathrm{x})$) из модифицированного алгоритма DSA по одному модулю p представляются в непозиционном виде как последовательности вычетов от их деления на основания (9).

Цифровой подписью для сообщения M является пара многочленов $(\gamma(\mathrm{x}), \delta(\mathrm{x}))$.

4 Заключение

Особенность построения непозиционной асимметричной системы ЦП с использованием алгоритма DSA и НПСС заключается в том, что не все ее параметры могут быть использованы в качестве показателей степени. Это относится к полиномиальным основаниям НПСС.

Компьютерное моделирование модифицированных криптосистем на базе НПСС позволит выработать рекомендации по их надежному использованию и генерации полных секретных ключей.

Литература

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Советское радио, 1968.- 439 с.
2. Stallings W., Cryptography and Network Security (4th Edition), Prentice Hall, 2005.
3. Бияшев Р.Г. 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.
4. Biyashev, R.G. and Nyssanbayeva, S.E.: Algorithm for Creation a Digital Signature with Error Detection and Correction, Cybernetics and Systems Analysis. 4, 489-497 (2012).
5. Biyashev R., Nyssanbayeva S., Kapalova N.: The Key Exchange Algorithm on Basis of Modular Arithmetic. International Conference on Electrical, Control and Automation Engineering (ECAE2013), December 1-2, 2013, Hong Kong – Monami,S. 2014. – P.501-505.
6. Моисил Гр. К. Алгебраическая теория дискретных автоматических устройств / Пер. с рум. В.М.Остиану. Под ред. В.И. Шестакова. – М.: Изд-во иностранной литературы, 1963. - 680 с.
7. FIPS PUB 186. Digital Signature Standard (DSS).

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА ИЗЛУЧЕНИЯ РЕНТГЕНОРАДИОМЕТРИЧЕСКИМ МЕТОДОМ В КАРОТАЖНЫХ СТАНЦИЯХ

Дракунов Ю.М.[1], Тулешова А.А.[2]

[1] *Доктор технических наук, профессор кафедры «Механика» механико-математического факультета Казахского Национального Университета имени аль-Фараби, г. Алматы, Республика Казахстан, e-mail: drakunov50@mail.ru*

[2] *Докторант первого курса по специальности «Математическое и компьютерное моделирование» механико-математического факультета Казахского Национального Университета имени аль-Фараби, научный сотрудник Института информационных и вычислительных технологий Комитета науки, г. Алматы, Республика Казахстан, e-mail: a.shadyman@mail.ru*

В данном докладе речь идет о математическом моделировании процесса излучения породы ренгенорадиометрическим методом[2].

Геофизические исследования скважин (ГИС) методом каротажа являются одним из важных и ответственных этапов при определении состояния скважины, требующих больших материальных и временных затрат. Основной целью исследований является разработка метода и средств минимизации затрат на исследование скважин за счет интеграции в одной системе подсистемы сбора и регистрации данных с подсистемами оценки состояния скважины и подсистемой выбора оптимального режима проведения ГИС[1].