МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ

«АКТУАЛЬНЫЕ ПРОБЛЕМЫ МАТЕМАТИКИ И МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ»

ТЕЗИСЫ ДОКЛАДОВ

Алматы-2015

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
КОМИТЕТ НАУКИ
ИНСТИТУТ МАТЕМАТИКИ И МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ

«АКТУАЛЬНЫЕ ПРОБЛЕМЫ МАТЕМАТИКИ И МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ»

посвящается 50-летию создания
Института математики и механики АН КазССР

Алматы 1–5 июня 2015 года

ТЕЗИСЫ ДОКЛАДОВ

Алматы – 2015

однозначно разрешима относительно $\tilde{\omega}_i^k$, *то решение дискретной обратной задачи* (12)-(14) *существует и единственно.*

В теоремах 1 и 2 сеточная функция $\tilde{\omega}_i^k$ определяется по формуле

$$\tilde{\omega}_i^k = \omega_i^k - \frac{1}{2}(\delta_{k+i}^h + \delta_{k-i}^h),$$

а сеточная функция ω_i^k является решением следующей вспомогательной задачи:

$$\frac{\omega_i^{k+1} - 2\omega_i^k + ?_i^{k-1}}{h^2} = \frac{\omega_{i+1}^k - 2\omega_i^k + \omega_{i-1}^k}{h^2} - q_i\omega_i^k, \quad i \geq 1, \quad k \in Z$$

$$\omega_0^k = \delta_k^h, \qquad \omega_1^k = \frac{1}{2}\left(\delta_{k+1}^h + \delta_{k-1}^h\right) + \frac{h^2}{2}q_0\delta_k^h, \qquad k \in Z$$

Литература

1. *Романов В. Г., Кабанихин С. И.* Обратные задачи геоэлектрики. – М.: Наука, 1991. – 304 с.
2. *Романов В. Г.* Обратные задачи математической физики. – М.: Наука, 1984. – 264 с.
3. *Самарский А. А.* Теория разностных схем. – М.: Наука, 1983. – 616 с.
4. *Кабанихин С. И.* Проекционно-разностные методы определения коэффициентов гиперболических уравнений. – Новосибирск: Наука. Сиб. отд-ние, 1988. – 167 с.

УДК 004.056.5

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

Институт информационных и вычислительных технологий КН МОН РК, Алматы, Казахстан

e-mail: brg@ipic.kz, snyssanbayeva@gmail.com, enlik_89@mail.ru

Модификация схемы цифровой подписи DSA

Одним из способов повышения криптостойкости алгоритмов шифрования и цифровой подписи (ЦП) является увеличение размеров общесистемных параметров для этих алгоритмов. На сегодняшний день рассмотрены различные предложения и модели криптографических систем, в частности с открытым ключом. Они имеют практическую значимость.

В докладе представляется модифицированная система цифровой подписи, построенная на базе алгоритма DSA и непозиционных полиномиальных систем счисления (НПСС). В известных в литературе моделях цирофой подписи длина модуля преобразования составляет порядка 1024 бит, вместе с ним увеличивается длина ключа до такой же длины. В связи с этим увеличивается вычислительная сложность криптографических преобразований, но уменьшается скорость вычислений. Решение задачи повышения скорости вычисления и умепьшения длины ключа возможно при разработке модификации схемы ЦП с открытым ключом на базе НПСС.

Система счисления в остаточных классах или полиномиальные системы счисления в остаточных классах (полиномиальных СОК), модулярная арифметика являются синонимами НПСС. Отличие НПСС от классических СОК состоит в том, что в НПСС основаниями выбираются неприводимые многочлены над полем GF(2),т.е.с двоичными коэффициентами. В работе [1] разработаны арифметика НПСС с полиномиальными

основаниями и ее приложения к задачам повышения достоверности. Определены правила выполнения арифметических операций в НПСС и восстановления многочлена по его остаткам.

Вначале производится модификация алгоритма DSA, в которой вместо двух модулей используется один модуль (простое число) p. Затем разрабатывается модифицированная схема цифровой подписи на базе НПСС. Использование НПСС позволяет уменьшить длину ключей, повысить стойкость и эффективность непозиционных криптографических алгоритмов [2]. Формируется НПСС с рабочими основаниями $p_1(x), p_2(x), \ldots, p_S(x)$, степени которых равны соответственно $m_1, m_2, \ldots, m_S$. В соответствии с китайской теоремой об остатках все эти основания должны быть различными, в том числе и тогда, когда они имеют одну степень. Основной диапазон в НПСС определяется многочленом степени m, равным произведению всех рабочих оснований. Степень m есть сумма степеней m_i рабочих оснований, где $i = 1, 2, \ldots, S$. Для каждого из рабочих оснований выбираются соответственные порождающие полиномы $g_1(x), g_2(x), \ldots, g_S(x)$. Порождающие полиномы являются аналогом примитивных элементов в конечном поле по модулю простого числа. Секретный ключ отправителя b выбирается из диапазона $[1, 2^m]$. Вычисляется значение открытого ключа $\beta(x) : \beta(x) := (\beta_1(x), \beta_2(x), \ldots, \beta_S(x))$. В алгоритме DSA процедура вычисления хэш-значения по алгоритму SHA, в модифицированном алгоритме ЦП на базе НПСС будет использована процедура вычисления хэш-значения в НПСС. Полиномы γ(x) и σ(x) представляются в непозиционном виде как последовательности вычетов от их деления на основания НПСС:

$$\gamma(x) = (\gamma_1(x), \gamma_2(x), \ldots, \gamma_S(x)), \sigma(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_S(x)).$$

Цифровой подписью для сообщения M является пара многочленов $(\gamma(x), \sigma(x))$.

Для разработанного модифицированного алгоритма формирования ЦП разработан соответствующий ему алгоритм проверки цифровой подписи [3].

Модификация алгоритма асимметричной системы цифровой подписи с использованием НПСС позволит повысить криптостойкость алгоритма и увеличить эффективность вычислений. Полученные результаты компьютерного моделирования модифицированных криптосистем на базе НПСС позволят выработать рекомендации по их надежному использованию и генерации полных секретных ключей.

Литература

1. *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.

2. *Bijashev R.G., Nyssanbayeva S.E.* Algorithm for Creation a Digital Signature with Error Detection and Correction // Cybernetics and Systems Analysis. - 2012. № 4. -PP. 489-497

3. *FIPS* FIPS PUB 186, Digital Signature Standard (DSS)., 2009. - 119 p.

УДК 004.056.5

Бияшев Р. Г., Нысанбаева С. Е., Капалова Н.А., Хакимов Р.А.

Институт информационных и вычислительных технологий МОН РК, Алматы, Казахстан

e-mail: brg@ipic.kz, sultasha1@mail.ru, kapalova@ipic.kz, relesssar@gmail.com

Моделирование программной реализации непозиционного алгоритма шифрования

Описывается модель программной реализации системы симметричного шифрования с заданной криптостойкостью. Эта криптосистема разработана на базе непозиционных полиномиальных систем счисления (НПСС) и предназначена для использования в инфокоммуникационных системах при хранении и передаче информации [1-4]. Синонимы НПСС - модулярная арифметика, системы счисления в остаточных классах (СОК). В НПСС основания - это неприводимые многочлены над полем $GF(2)$. Система шифрования включает два алгоритма - зашифрования (получения криптограммы) и расшифрования. Суть разработанной непозиционной криптосистемы состоит в следующем. При шифровании открытого электронного сообщения (или его блока) заданной длины N бит формируется вначале НПСС. Для этого из множества всех неприводимых многочленов степени не выше значения N выбираются полиномиальные основания

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

над полем $GF(2)$ степени $m_1, m_2, ..., m_S$ соответственно. Все эти основания должны быть различными. Основным рабочим диапазоном этой непозиционной системы является многочлен $P_S(x) = p_1(x)p_2(x)...p_S(x)$ степени $m = m_1 + m_2 + ... + m_S$. В НПСС любой многочлен $F(x)$ степени меньше m имеет единственное представление в виде последовательности остатков (вычетов) от его деления на основания (1):

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

где $F(x) \equiv \alpha_i(x)(\mod p_i(x))$, $i = 1, 2, .., S$. Позиционное представление этого многочлена при хранении и передаче информации восстанавливается по его непозиционному виду (2)[3].

Затем сообщение длины N бит интерпретируется как последовательность остатков от деления некоторого многочлена (который обозначим также $F(x)$) соответственно на основания НПСС (1) степени не выше N. Эти основания выбираются из числа всех неприводимых полиномов степени от m_1 до m_S из условия выполнения уравнения:

$$k_1m_1 + k_2m_2 + ... + k_Sm_S = N. \quad (3)$$

В уравнении (3) число оснований степени m_i, $i = 1, 2, .., S$ определяются неизвестными коэффициентами k_i, $0 \le k_i \le n_i$, n_i - количество всех неприводимых многочленов степени m_i, $0 \le m_i \le N$, $S = k_1 + k_2 + ... + k_S$ - число всех выбранных оснований НПСС. Каждое решение (3) задает одну систему оснований НПСС, в которой учитывается также порядок расположения оснований.

В предложенном алгоритме шифрования процедуре зашифрования предшествуют этапы формирования НПСС и генерации ключа (псевдослучайной последовательности - ПСП) длины N бит. Затем шифруемое сообщение интерпретируется в виде (2). ПСП также интерпретируется как последовательность $G(x) = (\beta_1(x), \beta_2(x), \ldots, \beta_S(x))$, $G(x) \equiv \beta_i(x)(\mod p_i(x))$, $i = 1, 2, \ldots, S$. Тогда криптограмма рассматривается как некоторая функция $H(F(x), G(x))$: $H(x) = (\omega_1(x), \omega_2(x), \ldots, \omega_S(x))$, где $H(x) \equiv \omega_i(x)(\mod p_i(x))$, $i = 1, 2, \ldots, S$. Секретность нетрадиционного алгоритма шифрования характеризуется полным ключом, который определяется всевозможными вариантами