УДК 004.056.5

МОДЕЛИРОВАНИЕ СХЕМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В НЕПОЗИЦИОННОЙ ПОЛИНОМИАЛЬНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

***Сауле Еркебулановна Нысанбаева**, д.т.н., гнс*
Тел.: 8727 272 8005, e-mail: sultasha1@mail.ru
***Нурсулу Алдажаровна Капалова**, к.т.н., внс*
Тел.: 8727 272 4559, e-mail: kapalova@ipic.kz
Институт проблем информатики и управления, Республика Казахстан
http//www.ipic.kz

Разработаны две модели программной реализации алгоритма формирования электронной цифровой подписи (ЭЦП) на базе непозиционных полиномиальных систем счисления с заданной криптостойкостью. Эти модели различаются процедурами вычисления секретных ключей алгоритма. Определены основные компоненты этих моделей.

Ключевые слова: электронная цифровая подпись, криптостойкость, непозиционная полиномиальная система счисления, программная реализация

Введение


С.Е. Нысанбаева

В статье представляются результаты, полученные при разработке моделей программной реализации алгоритма формирования электронной цифровой подписи, разработанного с использованием непозиционных полиномиальных систем счисления с заданной криптостойкостью. Этот комплекс программ будет являться частью создаваемой системы криптографической защиты информации (СКЗИ). СКЗИ будет состоять из трёх частей (блоков): формирования полных секретных ключей реализуемых криптотоалгоритмов, модулярных систем шифрования электронных сообщений и электронной цифровой подписи с заданной криптостойкостью [1-6].

Схема цифровой подписи включает два алгоритма:

- алгоритм формирования подписи;
- алгоритм проверки подписи.

В настоящее время предложены принципиально различные подходы для создания схем цифровой подписи, которые можно разделить на три группы:

- схемы на основе систем шифрования с открытым ключом;
- схемы со специально разработанными алгоритмами формирования и проверки цифровой подписи;
- схемы на основе симметричных систем шифрования.


Н.А. Капалова

Реализуемую схему ЭЦП, построенную на базе непозиционных полиномиальных систем счисления, можно отнести ко второй группе схем цифровой подписи. При моделировании этой схемы (или системы) цифровой подписи должны быть реализованы процессы:

- выбора полного ключа схемы ЭЦП;
- формирования (или вычисления) ЭЦП;
- проверки ЭЦП.

Входными данными в блоке электронной цифровой подписи являются длина блока подписываемого сообщения, длина подписи и требуемая (задаваемая) криптостойкость нетрадиционного алгоритма формирования ЭЦП.

Нетрадиционность означает использование непозиционной полиномиальной системы счисления. Синонимы НПСС - системы счисления в остаточных классах, системы остаточных классов (СОК). В классической системе счисления в остаточных классах (СОК) в качестве системы оснований выбираются положительные целые числа, и в ней целое положительное число представляется своими остатками (вычетами) от деления на эту систему оснований [5].В отличие от классических СОК основаниями в НПСС выбираются неприводимые многочлены над полем *GF*(2), то есть с двоичными коэффициентами [6].Построение непозиционных систем счисления основано на использовании китайской теоремы об остатках, доказанной в I веке китайским математиком Сун Це. В соответствии с этой теоремой представление числа в виде последовательности вычетов является единственным, если основания будут попарно просты между собой. Свое развитие они начали после выхода в свет в 1955 году первых работ чешских исследователей - инженера М. Валаха и математика А. Свободы. В 1955 году исследования в этой области были начаты также в СССР. Это новое научное направление было названо модулярной арифметикой [4,5].

Построение НПСС

Построение НПСС – это выбор ее оснований, называемых рабочими. Пусть такими основаниями выбраны некоторые неприводимые многочлены [7]:

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

Их степени обозначим m_1, $m_2,...,m_S$ соответственно. Полиномы (1) с учётом порядка их расположения образуют одну систему оснований. Основной рабочий диапазон НПСС- это многочлен $P(x) = p_1(x)p_2(x)\cdots p_S(x)$ степени $m = \sum_{i=1}^{S} m_i$.

В НПСС любой многочлен $F(x)$, степень которого меньше m, имеет единственное непозиционное представление в виде последовательности вычетов от его деления на основания (1):

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

где $F(x) \equiv \alpha_i(x) (\mathrm{mod}\, p_i(x))$, i= 1,2,..,S. Позиционное представление$F(x)$ восстанавливается по его непозиционному виду (2) [5-7]:

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

Многочлены $M_i(x)$ выбираются такие, чтобы выполнялось сравнение в (3). Формула (3) применяется при обработке, хранении и передаче информации. В случае только передачи и хранения информации восстановление позиционного видаполинома $F(x)$ осуществляется по формуле:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x) P_i(x), \quad \text{где} \quad P_i(x) = \frac{P_S(x)}{p_i(x)}. \quad (4)$$

В [6] разработаны арифметика непозиционных систем счисленияс 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 виде (2) является единственным (аналог китайской теоремы об остатках для многочленов). 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.

Нетрадиционные криптосистемы разрабатывались для электронных сообщений, длина которых имеет заданное количество бит. В НПСС сообщение (или его блок) заданной длины N бит интерпретируется как последовательность остатков от деления не-

которого многочлена (обозначим его также $F(x)$) соответственно на рабочие основания (1), то есть в виде (2). Остатки $\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)$ выбираются так, чтобы первым l_1 битам сообщения соответствовали двоичные коэффициенты остатка $\alpha_1(x)$, следующим l_2 битам – двоичные коэффициенты остатка $\alpha_2(x)$ и так далее, последним l_S двоичным разрядам – двоичные коэффициенты вычета $\alpha_S(x)$.

Каждое рабочее основание должно иметь степень не выше значения N. Основания (1) выбираются из числа всех неприводимых полиномов степени от m_1 до m_S из условия выполнения уравнения [8]:

$$k_1 m_1 + k_2 m_2 + ... + k_S m_S = N. \quad (5)$$

В уравнении (5) $0 \le k_i \le n_i, i = 1,2,..,S$- неизвестные коэффициенты и число выбранных неприводимых многочленов степени m_i, один конкретный набор этих коэффициентов является одним из решений (5) и задаёт одну систему рабочих оснований, n_i- количество всех неприводимых многочленов степени $m_i, 1 \le m_i \le N$, $S = k_1 + k_2 + ... + k_S$ - число выбранных рабочих оснований. 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 растёт (таблица 1), в связи с этим также значительно увеличивается количество решений уравнения (5).

Таблица 1

Зависимость числа неприводимых многочленов от их степени

Степень неприводимых многочленов	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Количество неприводимых многочленов	1	1	2	3	6	9	18	30	56	99	186	335	630	1161	2182	4080

Выверенная таблица неприводимых многочленов над полем $GF(2)$ для степеней, указанных в таблице 1, опубликована в № 1 журнала «Известия научно-технического общества «КАХАК» (2013 год, Республика Казахстан).

Алгоритм формирования ЭЦП по модулям нескольких избыточных полиномиальных оснований

Алгоритм формирования ЭЦП для электронного сообщения заданной длины Nбит в непозиционной полиномиальной системе счисления реализуется в три этапа:

1. построение НПСС;
2. хэширование (сжатие) сообщения длины N до длины N_1 путём экстраполяции на избыточные основания;
3. шифрование хэш-значения: выбор системы полиномиальных основанийи их размещения, генерация ключевой последовательности.

Первый этап описан выше.

Для проведения процедуры хэширования из всех неприводимых многочленов степени, не превышающей N_1, выбираются произвольно избыточные основания $p_{S+1}(x), p_{S+2}(x), ..., p_{S+U}(x)$, $1 \le U \le N_1$. Хэширование сообщения длины N до длины N_1 производится путем вычисления вычетов $F(x)$ по дополнительным основаниям. Полученные при делении избыточные вычеты $\alpha_{S+1}(x), \alpha_{S+2}(x), ..., \alpha_{S+U}(x)$ определяют длину хэш-значения N_1.

Шифрование хэш-значения осуществляется выбором системы полиномиальных оснований $r_1(x), r_2(x), ..., r_W(x)$, $1 \le W \le N_1$, из числа неприводимых многочленов с двоичными коэффициентами степени не выше N_1 с учётом их размещения, а также генерации ключевой гаммы длиной N_1 [7,9].

Основания на каждом этапе создания цифровой подписи выбираются независимо друг от друга, но среди них могут быть и одинаковые.

Криптостойкость алгоритма формирования ЭЦП определяется выражением:

$$p_{sig1} = 1/(2^{N_1} \sum_{k_1,k_2,...k_s} (((k_1 + k_2 + ... + k_s)!\ C_{n_1}^{k_1}\ C_{n_2}^{k_2} \dots C_{n_S}^{k_S} \times$$
$$\times \sum_{t_1,t_2,...t_U} (t_1 + t_2 + ... + t_U)!\ C_{d_1}^{t_1}\ C_{d_2}^{t_2} \dots C_{d_U}^{t_U}) \times \qquad (6)$$
$$\times \sum_{v,v_2,...y_W} (v_1 + v_2 + ... + v_W)!\ C_{l_1}^{v_1}\ C_{l_2}^{v_2} \dots C_{l_W}^{v_W})).$$

В формуле (6) суммирование

- $\sum_{k_1,k_2,...k_s}$ осуществляется по всевозможным комбинациям коэффициентов $k_1, k_2, ..., k_S$, то есть на все выборы систем оснований из числа неприводимых полиномов с двоичными коэффициентами степени не выше N, запись вычетов по которым покрывает длину заданного сообщения N;

- $\sum_{t_1,t_2,...t_U}$ распространено на всевозможные комбинации коэффициентов $t_1, t_2, ..., t_U$ уравнения $t_1 a_1 + t_2 a_2 + ... + t_U a_U = N_1$ (аналога уравнения (5)),где $a_1, a_2, ..., a_U$ и $d_1, d_2, ..., d_U$ - соответственно степени и число неприводимых многочленов, используемых при выборе избыточных оснований, $0 \le t_i \le d_i$ - число выбранных избыточных оснований степени a_i, $1 \le a_i \le N_1$, $t = t_1 + t_2 + ... + t_U$ - число избыточных оснований; запись вычетов по которым покрывает хэш-значение длины N_1;

- $\sum_{v,v_2,...y_W}$ производится по всевозможным комбинациям коэффициентов $v_1, v_2, ..., v_W$ равенства $v_1 b_1 + v_2 b_2 + ... + v_W b_W = N_1$ (аналога уравнения (5)),где $b_1, b_2, ..., b_W$ и $l_1, l_2, ..., l_W$ - степени и число неприводимых многочленов соответственно, используемых при выборе оснований $r_1(x), r_2(x), ..., r_W(x)$, $0 \le v_i \le l_i$ – неизвестные коэффициенты иличисло выбранных оснований степени b_i, $1 \le b_i \le N_1$, $v = v_1 + v_2 + ... + v_W$ - числооснований, запись вычетов по которым покрывает хэш-значение.

По формуле (6) рассчитаны значения криптостойкости ЭЦП в зависимости от длины подписываемого сообщения, при этом длина ЭЦП задавалась от N_1=1 до N_1=N с интервалом 1 бит (модельные расчёты). Поэтому для подписываемого сообщения получено не одно значение, а диапазон изменения криптостойкости ЭЦП: например, для N=16 бит этот диапазон составляет $3{,}6*10^{-6}$ - $5{,}6*10^{-21}$ (таблица 2). Таким образом, при нетрадиционном подходе к формированию ЭЦП возможно уменьшение её длины, по сравнению с указанными в Государственном стандарте Республики Казахстан [10].

Таблица 2

Криптостойкость алгоритма формирования ЭЦП

Длина сообщения (или блока)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Криптостойкость алгоритма формирования ЭЦП	$5{,}0\cdot10^{-1}$	$5{,}0\cdot10^{-1}$	$1{,}3\cdot10^{-1}$	$6{,}3\cdot10^{-2}$	$3{,}1\cdot10^{-2}$	$1{,}2\cdot10^{-2}$	$6{,}0\cdot10^{-3}$	$2{,}6\cdot10^{-3}$	$1{,}2\cdot10^{-3}$	$4{,}9\cdot10^{-4}$	$2{,}2\cdot10^{-4}$	$9{,}6\cdot10^{-5}$	$4{,}1\cdot10^{-5}$	$2{,}0\cdot10^{-5}$	$7{,}9\cdot10^{-6}$	$3{,}6\cdot10^{-6}$
	$-5{,}0\cdot10^{-1}$	$-0{,}3\cdot10^{-1}$	$-2{,}0\cdot10^{-3}$	$-1{,}2\cdot10^{-4}$	$-7{,}6\cdot10^{-6}$	$-2{,}3\cdot10^{-7}$	$-1{,}3*10^{-8}$	$-5{,}5\cdot10^{-10}$	$-2{,}5\cdot10^{-11}$	$-9{,}1\cdot10^{-13}$	$-4{,}0\cdot10^{-14}$	$-1{,}7\cdot10^{-15}$	$-6{,}9\cdot10^{-17}$	$-4{,}0\cdot10^{-18}$	$-1{,}2\cdot10^{-19}$	$-5{,}6\cdot10^{-21}$

Программное моделирование алгоритма формирования ЭЦП

Для реализации схемы цифровой подписи рассмотрены две модели. В первой модели криптостойкость алгоритма формирования подписи будет определяться непосредственно в блоке системы ЭЦП. Во второй модели эта криптостойкость будет вычисляться в блоке формирования ключей и храниться в базе данных (БД) полных ключей. Создание различных моделей реализации для нетрадиционных криптографических систем позволяет построить такую систему криптографической защиты информации, которую было бы несложно трансформировать при изменении модели реализуемых криптографических алгоритмов.

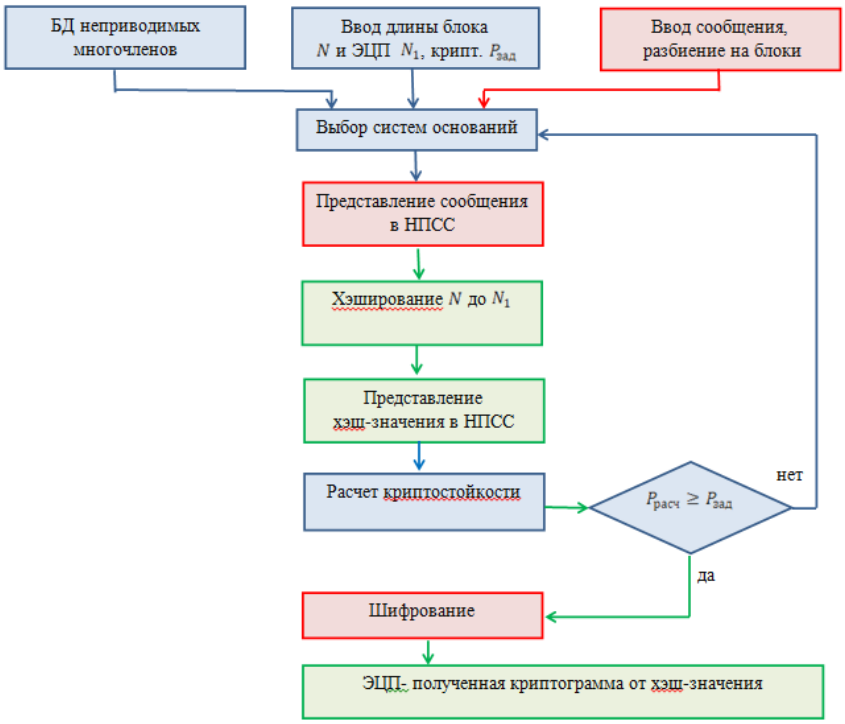

Рисунок. Структурная схема реализации нетрадиционного алгоритма формирования электронной цифровой подписи

Структурная схема первой модели реализации нетрадиционного алгоритма формирования электронной цифровой подписи приведена на рисунке. Эта схема отражает структуру основных этапов и алгоритма формирования ЭЦП и его программной реализации.

Выбор систем рабочих и избыточных оснований и оснований для шифрования хэш-значения, то есть на каждом из этапов алгоритма формирования ЭЦП, производится из базы данных неприводимых многочленов с двоичными коэффициентами. По выбранным системам оснований вычисляется криптостойкость, которая сравнивается с заданной $\boldsymbol{p}_{зад}$.Если рассчитанная по формуле (6) криптостойкость $\boldsymbol{p}_{расч}$ окажется больше $\boldsymbol{p}_{зад}$., то будут выбираться другие системы оснований. Когда необходимый набор указанных систем оснований будет найден, вычисляется цифровая подпись путем зашифрования полученного хэш- значения.

Преимущество этой модели состоит в том, что полный ключ находится в момент формирования цифровой подписи. Это естественно снижает скорость формирования ЭЦП. Увеличить скорость получения подписи по этой модели можно за счет распарал-

леливания вычислительных операций, заложенных в самом алгоритме формирования подписи, то есть по выбранным основаниям каждой из трех систем.

Во второй модели схемы цифровой подписи полный ключ будет выбираться в блоке «Формирование полных ключей» (соответственно по длинам сообщения и электронной цифровой подписи) и храниться в базе данных полных ключей. Составными частями полного ключа являются система рабочих оснований, система избыточных оснований, а также псевдослучайная последовательность (традиционный секретный ключ) и инверсный (обратный) для ПСП ключ для шифрования хэш-значения. Затем для систем полных ключей системы ЭЦП будет вычисляться значение криптостойкости, которое будет записано в базу данных. Кроме этих составных частей в БД будет храниться информация о другой необходимой информации.

Заключение

Работы по разработке, анализу и реализации отечественных средств криптографической защиты информации для Республики Казахстан являются актуальными, поскольку Казахстан активно интегрируется в мировое информационное сообщество.

Литература

1 *Бияшев Р.Г., Нысанбаева С.Е., Капалова Н.А, Хакимов Р.А.* Разработка системы криптографической защиты на базе модулярной арифметики // ИБ-2013: материалы XIII междунар. науч.-практ. конф. – Таганрог: изд-во ЮФУ, 2013. Ч. I. С. 215-220.

2 *Нысанбаева С.Е., Бияшев Р.Г., Капалова Н.А., Хакимов Р.А.* Генерация полных ключей для модулярных полиномиальных систем // Проблемы оптимизации сложных систем: труды IX междунар. Азиатской школы – семинара. – Алматы, 2013. С. 241-244.

3 *Бияшев Р.Г., Нысанбаева С.Е., Капалова Н.А* Разработка систем криптографической защиты информации с заданными характеристиками // Проблемы информатики. – Новосибирск, 2013. №2 (19). С. 30-36.

4 *Свобода А.* Развитие вычислительной техники в Чехословакии//Системы счисления в остаточных классах:кибернетический сб. − М.,1963. № 8. С. 115-149.

5 *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. – М.: Советское радио, 1968.− 439 с.

6 *Бияшев Р.Г.*Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: дисс. докт. тех. наук: 05.13.06: защищена 09.10. 1985: утв. 28.03.1986. − М., 1985. − 328 с.

7 *Бияшев Р.Г., Нысанбаева С.Е.* Алгоритм формирования электронной цифровой подписи с возможностью обнаружения и исправления ошибки // Кибернетика и системный анализ. 2012. Т. 48. № 4. С. 14-23.

8 *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.

9 *Нысанбаев Р.К.*Криптографический метод на основе полиномиальных оснований // Вестник Министерства науки и высшего образования и Национальной академии наук Республики Казахстан. 1999. № 5. С. 63-65.

10 СТ РК 1073-2007. Средства криптографической защиты информации / Общие технические требования: утв. 1 января 2009.

Simulation of the digital signature schemein nonpositional polynomial notation

Saule Yerkebulanovna Nyssanbayeva, doctoroftechnicalsciences, chief researcher

Nursulu Aldazharovna Kapalova, candidate of technical sciences, leadingresearcher
Institute of Informatics and Control Sciences

Two models for computer programs realization of algorithm for creating a digital signature (DS) on the basis of nonpositional polynomial notations with preset cryptostrength, are developed. These models differ with calculation procedures of algorithm secret keys. Thebasiccomponentsofthesemodelsaredefined.

Keywords: digital signature, cryptostrength, nonpositional polynomial notation, computer programme realization