УДК 004.056.5; 681.3

Р. Г. БИЯШЕВ, С. Е. НЫСАНБАЕВА

ИССЛЕДОВАНИЕ НАДЕЖНОСТИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В НЕПОЗИЦИОННОЙ ПОЛИНОМИАЛЬНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

Исследовано влияние на криптостойкость электронной цифровой подписи состава оснований непозиционной полиномиальной системы счисления, используемых при создании подписи.

Применение нетрадиционных методов и алгоритмов при создании систем шифрования и формирования электронной цифровой подписи (ЭЦП) позволяет значительно повысить их криптостойкость [1]. Термин «нетрадиционные» означает использование непозиционной полиномиальной системы счисления (НПСС), в которой основаниями выбираются неприводимые многочлены $p_1(x), p_2(x),..., p_S(x)$ над полем $GF(2)$ степени $m_1, m_2,..., m_S$ соответственно [2, 3]. Тогда многочлен $P_S(x) = p_1(x)p_2(x)...p_S(x)$ степени $m = \sum_{i=1}^{S} m_i$ определяет основной рабочий диапазон. В этой системе любой многочлен $F(x)$ степени, меньшей m, единственным образом представляется в виде

$$F(x) = (\alpha_1(x), \alpha_2(x),..., \alpha_S(x)), \qquad (1)$$

где $F(x) \equiv \alpha_i(x) (\mathrm{mod}\ p_i(x))$. Позиционное представление полинома $F(x)$ восстанавливается по его непозиционному виду (1) следующим образом:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x) B_i(x),$$

где $B_i(x) = \dfrac{\prod_{i=1}^{S} p_i(x)}{p_i(x)} M_i(x) \equiv 1 (\mathrm{mod}\ p_i(x))$,

а значения многочленов $M_i(x)$ выбираются для выполнения сравнения.

В НПСС электронное сообщение длиной N интерпретируется как последовательность *остатков отделения некоторого многочлена F(x)* на основания $p_1(x), p_2(x),..., p_S(x)$ степени не выше N, $S \le N$ соответственно, т.е. в виде (1). Эти основания называются рабочими и выбираются соответственно степени $m_1, m_2,..., m_S$ из условия выполнения уравнения

$$k_1 p^{m_1}(x) + k_2 p^{m_2}(x) + ... + k_S p^{m_S}(x) = N, \qquad (2)$$

где $0 \le k_i \le n_i$ – подлежащие определению не-

известные коэффициенты; n_i – количество всех неприводимых многочленов степени m_i; $p^{m_i}(x)$ – многочлен степени m_i; $1 \le m_i \le S$; $k = k_1 + k_2 + \ldots + k_S$ – количество рабочих оснований.

Алгоритм формирования ЭЦП длины N_1 бит *для электронного сообщения заданной длины N* бит реализуется при помощи процедур хэширования и шифрования: хэш-функция сжимает подписываемое сообщение до длины N_1, а затем полученное хэш-значение шифруется. Длина ЭЦП N_1 может быть значительно меньше N. Хэширование сообщения длины N до длины N_1 производится путем вычисления вычетов восстановленного многочлена $F(x)$ по избыточным (дополнительным) основаниям $p_{S+1}(x), p_{S+2}(x), \ldots, p_{S+U}(x)$, $1 \le U \le N_1$, выбираемым произвольно из всех неприводимых многочленов с двоичными коэффициентами степени не выше N_1. Вычеты $\alpha_{S+1}(x), \alpha_{S+2}(x), \ldots, \alpha_{S+U}(x)$ от деления $F(x)$ на дополнительные основания определяют длину хэш-значения N_1. Для шифрования полученного хэш-значения выбираются основания $r_1(x), r_2(x), \ldots, r_W(x)$, $1 \le W \le N_1$ из числа неприводимых многочленов с двоичными коэффициентами степени не выше N_1 и генерируется ключевая последовательность также длиной N_1. Все используемые системы оснований (рабочих, дополнительных и для шифрования хэш-значения) выбираются независимо друг от друга, причем некоторые из них могут совпадать. Важным явля-ется также и порядок распределения оснований.

Выражение, определяющее криптостойкость ЭЦП, имеет вид [1]

$$p_{sig} = 1/(2^{N_1} \sum_{k_1,k_2,\ldots,k_s} ((Z_1 \sum_{t_1,t_2,\ldots,t_U} Z_2) \sum_{v,v_2,\ldots,v_W} Z_3)), \quad (3)$$

где $Z_1 = (k_1 + k_2 + \ldots + k_s)!\, C_{n_1}^{k_1} C_{n_2}^{k_2} \ldots C_{n_S}^{k_s}$,

$Z_2 = (t_1 + t_2 + \ldots + t_U)!\, C_{d_1}^{t_1} C_{d_2}^{t_2} \ldots C_{d_U}^{t_U}$,

$Z_3 = (v_1 + v_2 + \ldots + v_W)!\, C_{l_1}^{v_1} C_{l_2}^{v_2} \ldots C_{l_W}^{v_W}$.

В формуле (3) суммирование:

– $\sum_{k_1,k_2,\ldots,k_s}$ осуществляется по всевозможным комбинациям коэффициентов $k_1, k_2, \ldots, k_S$, удовлетворяющих равенству (2), т. е. по всем выбранным системам оснований из числа неприводимых полиномов с двоичными коэффициентами сте-пени не выше N, запись вычетов по которым покрывает длину заданного сообщения N;

– $\sum_{t_1,t_2,\ldots,t_U}$ распространено на всевозможные комбинации коэффициентов $t_1, t_2, \ldots, t_U$ уравнения $t_1 p^{a_1}(x) + t_2 p^{a_2}(x) + \ldots + t_U p^{a_U}(x) = N_1$ (аналога уравнения (2)), где $a_1, a_2, \ldots, a_U$ и $d_1, d_2, \ldots, d_U$ – соответственно степени и число неприводимых многочленов, используемых при выборе избыточных оснований, $0 \le t_i \le d_i$, $p^{a_i}(x)$ – многочлен степени a_i, $1 \le a_i \le U$, $t = t_1 + t_2 + \ldots + t_U$ – число избыточных оснований; запись вычетов по которым покрывает хэш-значение длины N_1;

– $\sum_{v,v_2,\ldots,v_W}$ производится по всевозможным комбинациям коэффициентов $v_1, v_2, \ldots, v_W$ равенства $v_1 r^{b_1}(x) + v_2 r^{b_2}(x) + \ldots + v_W r^{b_W}(x) = N_1$, где $b_1, b_2, \ldots, b_W$ и $l_1, l_2, \ldots, l_W$ – степени и количество неприводимых многочленов соответственно, используемых при выборе оснований $r_1(x), r_2(x), \ldots, r_W(x)$, $0 \le v_i \le l_i$, $r^{b_i}(x)$ – много-член степени b_i, $1 \le b_i \le W$, $v = v_1 + v_2 + \ldots + v_W$ – число оснований, запись вычетов по которым покрывает хэш-значение.

Надежность ЭЦП зависит от составов и сочетания систем оснований на всех этапах ее формирования, которые могут отличаться и степенью и количеством (табл. 1). Возможные комбинации рабочих и избыточных оснований приведены в первых двух столбцах табл. 1. Формула (3) описывает общий случай формирования ЭЦП, в котором все системы оснований (рабочих, избыточных и для шифрования хэш-

значения) составлены из неприводимых многочленов различных степеней: вариант 1.1 в табл. 1. В вариантах 1, 2, 4, 5 не рассматриваются комбинации избыточных оснований, в которых их количество совпадает с числом рабочих оснований, вследствие пред- положения, что N_1 значительно меньше N.

Каждой из пяти приведенных комбинаций соответствуют определенные составы оснований $r_1(x), r_2(x), ..., r_W(x)$. Их степень, так же, как и дополнительных, не превышает значения N_1, поэтому возможные наборы оснований $r_1(x), r_2(x), ..., r_W(x)$ рассматриваются в сочетании с составом избыточных оснований. В каждой строке третьего столбца приведены соответствующие возможные комбинации оснований $r_1(x), r_2(x), ..., r_W(x)$.

Анализ криптостойкости ЭЦП проводится вначале для разных структур систем рабочих и избыточных оснований, т.е. для вариантов 1.1, 2.1, 3.1, 4.1, 5.1 (часть I), а затем от соотношения комбинаций дополнительных оснований и оснований, выбираемых для шифрования хэш-значения (часть II). Тогда в формуле (3) соответственно будет изменяться вид выражений Z_1, Z_2, Z_3.

По формуле (3) вычислены 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. Поэтому для подписываемого сообщения заданной длины получено не одно значение, а диапазон изменения криптостойкости ЭЦП: например, для N=16 бит этот диапазон составляет $3{,}6 \cdot 10^{-6}$ – $-5{,}6 \cdot 10^{-21}$ (первый столбец табл. 2). Таким образом, при нетрадиционном подходе к формированию ЭЦП возможно существенное уменьшение ее длины по сравнению с указанной в Государственном стандарте Республики Казахстан [4], при сохранении, а при необходимости и увеличении ее надежности. В стандарте максимальная длина ЭЦП составляет 512 бит.

Часть I. Вариант 1.1 описывается формулой (3), поэтому рассматриваются варианты 2.1, 3.1, 4.1, 5.1.

Вариант 2.1. Избыточные основания имеют одинаковые степени, поэтому $Z_2 = t_1! C_{d_i}^{t_i}$ и вторая сумма $\sum_{t_i}$ распространяется на всевозможные варианты выбора избыточных оснований одной и той же степени из числа неприводимых полиномов степени не выше N_1, удовлетворяющих уравнению $t_i p^{a_i}(x) = N_1$, a_i – степень оснований.

Вариант 3.1. Рабочие и избыточные основания имеют одинаковые и совпадающие степени, тогда $Z_1 = k_1! C_{n_i}^{k_i}$, $Z_2 = t_1! C_{n_i}^{t_i}$, а первая и вторая

Таблица 1

№ п/п	Степени		№ п/п	Основания $r_1(x), r_2(x), ..., r_W(x)$	
	рабочих оснований (РО)	избыточных оснований (ИО)		их степени	их количество
1	Различные (формула (3))	Различные (формула (3))	1.1	Различные (формула (3))	Отличается от числа ИО (формула (3))
			1.2	Различные	Совпадает с числом ИО
			1.3	Совпадают со степенью ИО	Совпадает с числом ИО
2	Различные	Одинаковые	2.1	Различные	Отличается от числа ИО
			2.2	Различные	Совпадает с числом ИО
			2.3	Одинаковые, но не совпадающие со степенью ИО	Не совпадает с числом ИО
			2.4	Одинаковые и совпадающие со степенью ИО	Совпадает с числом ИО
3	Одинаковые	Одинаковые и совпадающие со степенью РО	3.1–3.4	Совпадают с подпунктами 2.1 – 2.4	
4	Одинаковые	Одинаковые, но не совпадающие со степенью РО	4.1–4.4	Совпадают с подпунктами 2.1 – 2.4	
5	Одинаковые	Различные	5.1–5.3	Совпадают с подпунктами 1.1 – 1.3	

Таблица 2.

Длина сообщения N =16					
Длина ЭЦП – N_1 бит	Криптостойкость ЭЦП				
	Вариант 1.1	Вариант 2.1	Вариант 3.1	Вариант 4.1	Вариант 5.1
1	$3,6\cdot10^{-6}$	$3{,}6\cdot10^{-6}$	–	$5,8\cdot10^{-5}$	$5{,}8\cdot10^{-5}$
2	$1,8\cdot10^{-6}$	$1{,}8\cdot10^{-6}$	–	$2,9\cdot10^{-5}$	$2{,}9\cdot10^{-5}$
3	$5,6\cdot10^{-8}$	$1{,}1\cdot10^{-7}$	–	$1,8\cdot10^{-6}$	$9{,}1\cdot10^{-7}$
4	$7,0\cdot10^{-9}$	$1{,}4\cdot10^{-8}$	–	$2,3\cdot10^{-7}$	$1{,}1\cdot10^{-7}$
5	$8,7\cdot10^{-10}$	$2{,}3\cdot10^{-9}$	–	$3,8\cdot10^{-8}$	$1{,}4\cdot10^{-8}$
6	$6,7\cdot10^{-11}$	$1{,}0\cdot10^{-10}$	–	$4,0\cdot10^{-9}$	$1{,}0\cdot10^{-9}$
7	$7,9\cdot10^{-12}$	$3{,}7\cdot10^{-11}$	–	$6,0\cdot10^{-10}$	$1{,}2\cdot10^{-10}$
8	$7,6\cdot10^{-13}$	$4{,}0\cdot10^{-12}$	$7{,}8\cdot10^{-10}$	$6{,}5\cdot10^{-11}$	$1{,}2\cdot10^{-11}$
9	$7,6\cdot10^{-14}$	$2{,}0\cdot10^{-12}$	–	$9,3\cdot10^{-12}$	$1{,}2\cdot10^{-12}$
10	$6,7\cdot10^{-15}$	$4{,}5\cdot10^{-14}$	–	$7,4\cdot10^{-13}$	$1{,}1\cdot10^{-13}$
11	$6,6\cdot10^{-16}$	$6{,}3\cdot10^{-15}$	–	$1,0\cdot10^{-14}$	$1{,}1\cdot10^{-14}$
12	$6,4\cdot10^{-17}$	$5{,}9\cdot10^{-16}$	–	$9,6\cdot10^{-15}$	$1{,}0\cdot10^{-15}$
13	$6,0\cdot10^{-18}$	$7{,}4\cdot10^{-17}$	–	$1,2\cdot10^{-15}$	$9{,}7\cdot10^{-17}$
14	$5,3\cdot10^{-19}$	$6{,}7\cdot10^{-18}$	–	$1,1\cdot10^{-16}$	$8{,}5\cdot10^{-18}$
15	$5,5\cdot10^{-20}$	$8{,}6\cdot10^{-19}$	–	$1,4\cdot10^{-17}$	$9{,}0\cdot10^{-19}$
16	$5,6\cdot10^{-21}$	$9{,}0\cdot10^{-20}$	$1{,}8\cdot10^{-18}$	$1{,}5\cdot10^{-18}$	$9{,}0\cdot10^{-20}$

суммы $\sum_{k_i}$ и $\sum_{t_i}$ производят суммирование по всевозможным вариантам выбора соответственно рабочих и избыточных оснований одной и той же степени из числа неприводимых полиномов степени не выше N и N_1, удовлетворяющих соответственно уравнениям $k_i p^{m_i}(x) = N$ и $t_i p^{m_i}(x) = N_1$, m_i – степень оснований.

Вариант 4.1. Рабочие и избыточные основания имеют одинаковые, но не совпадающие степени, тогда $Z_1 = k_i! C_{n_i}^{k_i}$, $Z_2 = t_i! C_{d_i}^{t_i}$, а суммы $\sum_{k_i}$ и $\sum_{t_i}$ распространяются на всевозможные варианты выбора соответственно рабочих и избыточных оснований одной степени из числа неприводимых полиномов степени не выше N и N_1, удовлетворяющих соответственно уравнениям $k_i p^{m_i}(x) = N$ и $t_i p^{a_i}(x) = N_1$, m_i – степень рабочих оснований, a_i – степень избыточных оснований.

Вариант 5.1. Рабочие основания имеют одинаковые степени, тогда $Z_1 = k_i! C_{n_i}^{k_i}$, а суммирование $\sum_{k_i}$ осуществляется по всевозможным вариантам выбора рабочих оснований одинаковой степени из числа неприводимых полиномов степени не выше N, удовлетворяющих уравнению $k_i p^{m_i}(x) = N$, m_i – степень рабочих оснований.

Значения криптостойкости этих вариантов приведены в табл. 2: наибольшая надежность – у ЭЦП первого столбца, за ней следует ЭЦП второго столбца, а наименьшая криптостойкость – у ЭЦП в третьем столбце.

Часть II. Криптостойкость ЭЦП изучается для варианта 1 и подпунктов 1.1 – 1.3 при следующих трех комбинациях: 1) вначале в общем случае, 2) дополнительными основаниями являются полиномы только трех степеней a_1, a_2, a_3 и $t = t_1 + t_2 + t_3$, 3) дополнительных оснований всего три, т.е. $t_1 = t_2 = t_3 = 1$, $t = t_1 + t_2 + t_3 = 3$. Подпункты вариантов 2–4 табл. 1 могут быть получены по аналогии.

Комбинация 1.1.

1. Общий случай выбора оснований: описывается выражением (3).

2. В этом частном случае в выражении (3) $Z_2 = (t_1 + t_2 + t_3)!\, C_{d_1}^{t_1} C_{d_2}^{t_2} C_{d_3}^{t_3}$ и вторая сумма

Таблица 3

Длина сообщения N =16			
Длина ЭЦП – N_1 бит	Криптостойкость ЭЦП		
	Комбинация 1.1 (формула (3))	Комбинация 1.2	Комбинация 1.3
1	$3,6\cdot10^{-6}$	–	–
2	$1,8\cdot10^{-6}$	–	–
3	$5,6\cdot10^{-8}$	–	–
4	$7,0\cdot10^{-9}$	–	–
5	$8,7\cdot10^{-10}$	–	–
6	$6,7\cdot10^{-11}$	$2,3\cdot10^{-10}$	$2,3\cdot10^{-10}$
7	$7,9\cdot10^{-12}$	$3,7\cdot10^{-11}$	$3,7\cdot10^{-11}$
8	$7,6\cdot10^{-13}$	$2,0\cdot10^{-12}$	$2,0\cdot10^{-12}$
9	$7,6\cdot10^{-14}$	$1,8\cdot10^{-13}$	$2,0\cdot10^{-13}$
10	$6,7\cdot10^{-15}$	$1,7\cdot10^{-14}$	$1,7\cdot10^{-14}$
11	$6,6\cdot10^{-16}$	$1,7\cdot10^{-15}$	$2,0\cdot10^{-15}$
12	$6,4\cdot10^{-17}$	$1,5\cdot10^{-16}$	$1,7\cdot10^{-16}$
13	$6,0\cdot10^{-18}$	$1,4\cdot10^{-17}$	$1,9\cdot10^{-17}$
14	$5,3\cdot10^{-19}$	$1,4\cdot10^{-18}$	$1,7\cdot10^{-18}$
15	$5,5\cdot10^{-20}$	$1,4\cdot10^{-19}$	$1,8\cdot10^{-19}$
16	$5,6\cdot10^{-21}$	$1,5\cdot10^{-20}$	$1,8\cdot10^{-20}$

$\sum_{t_1,t_2,t_3}$ распространена на всевозможные способы выбора количества оснований трех степеней, т.е. коэффициентов t_1,t_2,t_3 уравнения $t_1 p^{a_1}(x)+t_2 p^{a_2}(x)+t_3 p^{a_3}(x)=N_1$.

3. Здесь Z_2=3! $d_1d_2d_3$ и суммирование $\sum_{a_1,a_2,a_3}$ производится по всевозможным комбинациям 3-х оснований степени a_1,a_2,a_3, удовлетворяющих *уравнению* $p^{a_1}(x)+p^{a_2}(x)+p^{a_3}(x)=N_1$.

В табл. (3) приведены значения криптостойкости, определенные для этих комбинаций: во втором и третьем столбцах они меньше величин криптостойкости общего случая (3) в среднем в 2,8 и 3,1 раза соответственно. Такая разница объясняется тем, что комбинаций выбора оснований с тремя степенями с увеличением длины ЭЦП становится больше, чем комбинаций с тремя избыточными основаниями (начиная с N_1=11). Отсутствие значений криптостойкости в первых пяти строках обусловлено тем, что таких комбинаций для ЭЦП длиной от 1 до 5 бит нет.

Комбинация 1.2. Число оснований $r_1(x),r_2(x),...,r_W(x)$ совпадает с количеством избыточных $p_{S+1}(x),p_{S+2}(x),...,p_{S+U}(x)$: $t=\nu$, но $U\neq W$ и $t_i\neq\nu_i$, так как число выбранных оснований каждой степени может быть разным.

1. Для общего случая Z_2 и Z_3 в выражении (3) будут иметь вид

$$Z_2=t!\ C_{d_1}^{t_1}C_{d_2}^{t_2}\dots C_{d_U}^{t_U},\ Z_3=t!\ C_{l_1}^{\nu_1}C_{l_2}^{\nu_2}\dots C_{l_W}^{\nu_W}. \quad (4)$$

2. Если среди избыточных оснований будут только неприводимые многочлены трех степеней, то из (4) получим

$$Z_2=t!\,C_{d_1}^{t_1}C_{d_2}^{t_2}C_{d_3}^{t_3},\ Z_3=t!\,C_{l_1}^{\nu_1}C_{l_2}^{\nu_2}\dots C_{l_W}^{\nu_W}, \quad (5)$$

где $t=\nu=t_1+t_2+t_3=\nu_1+\nu_2+\dots+\nu_W$.

3. В случае трех дополнительных оснований из (5) следует

$$Z_2=3!\,d_1d_2d_3,\ Z_3=3!\ C_{l_1}^{\nu_1}C_{l_2}^{\nu_2}\dots C_{l_W}^{\nu_W}.$$

Комбинация 1.3. Состав оснований $r_1(x),r_2(x),...,r_W(x)$ совпадает с составом избыточных $p_{S+1}(x),p_{S+2}(x),...,p_{S+U}(x)$ по количеству и степеням: $t=\nu$, U=W и $t_i=\nu_i$, но эти основания могут быть неодинаковыми для каждой их степени и отличаться порядком следования.

1. Для общего случая тогда в формуле (3)

$$Z_2=Z_3=(t_1+t_2+\dots+t_U)!\,C_{d_1}^{t_1}C_{d_2}^{t_2}\dots C_{d_U}^{t_U}.$$

2. При выборе избыточных оснований трех степеней

$$Z_2 = Z_3 = (t_1 + t_2 + t_3)!\, C_{d_1}^{t_1}\, C_{d_2}^{t_2}\, C_{d_3}^{t_3}.$$

3. В случае трех дополнительных оснований

$$Z_2 = Z_3 = 3!\, d_1 d_2 d_3 .$$

Полученные результаты показывают, что наибольшей надежностью обладает подпись, криптостойкость которой определяется выражением (3), т.е. при формировании которой все три системы оснований различны по структуре (степени, количеству и распределению). Наибольшая разница в значениях составляет два порядка, но криптостойкость при этом остается достаточно высокой. В связи с этим выбор систем оснований при создании ЭЦП зависит от предъявляемых к ней требований по обеспечению необходимой степени надежности.

ЛИТЕРАТУРА

1. *Амербаев В.М., Бияшев Р.Г., Нысанбаева С.Е.* Применение непозиционных систем счисления при криптографической защите информации // Изв. НАН РК. Сер. физ.-мат. наук. 2005. № 3. С. 84-89.

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

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

4. СТ РК 1073-2002 «Средства криптографической защиты информации»: Общие технические требования. Астана: Госстандарт РК, 2002.

Резюме

Қолтаңбаны құру кезінде қолданылатын позициялық емес полиномды санау жүйелерінің негіз құрамының электронды қолтаңбаның криптотұрақтылығына әсері зерттелген.

Summary

We investigate influence of the structure of the bases of non-positional polynomial notation, which is used for creating an electronic digital signature, on the signature cryptostability.

Институт проблем информатики и управления МОН РК, г. Алматы

Поступила 05.10.06г.

УДК 621.3