УДК 004.056.5

С. Е. НЫСАНБАЕВА

АЛГОРИТМ ФОРМИРОВАНИЯ КОРРЕКТИРУЮЩЕЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Рассмотрена процедура формирования электронной цифровой подписи в непозиционной полиномиальной системе счисления. Подпись создается по модулю одного избыточного основания и обладает дополнительными проверяющими свойствами. Показана однозначность алгоритма выявления и исправления одиночной ошибки. Получена формула криптостойкости алгоритма создания цифровой подписи.

В работе приводится нетрадиционный алгоритм формирования электронной цифровой подписи (ЭЦП) повышенной надежности, особенностью которого является дополнительная, проверяющая, функция выявления многократных ошибок и исправления одиночных ошибок. Нетрадиционность алгоритма означает использование при его создании непозиционной полиномиальной системы счисления (НПСС) или системы остаточных классов, в которой в качестве оснований берутся не простые числа, а неприводимые полиномы над полем $GF(2)$ [1-4].

При создании непозиционной полиномиальной системы счисления (НПСС) ее 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. Эти полиномы с учетом порядка их расположения образуют системы оснований и называются рабочими или информационными. В соответствии с Великой китайской теоремой об остатках все основания должны быть различными, в том числе и тогда, когда они имеют одну степень. Основным рабочим диапазоном в НПСС является многочлен $P_S(x) = p_1(x)p_2(x)...p_S(x)$ степени $m = \sum_{i=1}^{S} m_i$ и любой полином $F(x)$, степени меньшей m, имеет единственное представление вида

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

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

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

где $B_i(x) = \dfrac{P_S(x)}{p_i(x)} M_i(x) \equiv 1 (\mathrm{mod}\ p_i(x))$. (2)

Многочлены $M_i(x)$ выбираются такие, чтобы выполнялось сравнение в (2). Эта формула восстановления $F(x)$ применяется при обработке, хранении и передаче информации. Если же рассматриваются только процессы передачи и хранения непозиционной информации, то восстановление позиционного вида многочлена $F(x)$ осуществляется по формуле [2-4]:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x) P_i(x), \text{ где } P_i(x) = \frac{P_S(x)}{p_i(x)}. \qquad (3)$$

При разработке криптосистем электронное сообщение длиной N бит в НПСС интерпретируется как последовательность остатков от деления некоторого многочлена, например также $F(x)$, соответственно на рабочие основания $p_1(x), p_2(x),..., p_S(x)$ степени не выше N, то есть в виде (1). Система этих оснований выбирается из числа всех неприводимых полиномов степени от m_1 до m_S из условия выполнения уравнения [5]

$$k_1 p^{m_1}(x) + k_2 p^{m_2}(x) + ... + k_S p^{m_S}(x) = N, \qquad (4)$$

из которого находятся неизвестные коэффициенты k_i, $i = 1,2,..,S$ и где $0 \le k_i \le n_i$, n_i - количество всех неприводимых многочленов степени m_i, $p^{m_i}(x)$ - многочлен степени m_i, $1 \le m_i \le m_S \le N$, $S = k_1 + k_2 + ... + k_S$ - число выбранных оснований. Полные системы вычетов по модулям многочленов степени m_i включают в себя все полиномы степени не выше $m_i - 1$, для записи которых нужны m_i бит. С ростом степени неприводимых многочленов их количество стремитель-

но увеличивается и соответственно значительно растет количество решений уравнения (4) [3].

Процедура создания ЭЦП для электронного сообщения заданной длины N бит состоит из 3-х этапов. Вначале производится восстановление $F(x)$ по формуле (3), для этого производится формирование системы рабочих оснований в соответствии с уравнением (4). Этот первый этап описан выше. На 2-м этапе осуществляется сжатие (хэширование) сообщения до длины N_k путем введения избыточных или дополнительных оснований из числа всех неприводимых многочленов степени не выше N_k и вычисление избыточных вычетов по модулям этих оснований. Эти вычеты составляют хэш-значение длиной N_k. На третьем этапе хэш-значение шифруется, в результате получаем ЭЦП длиной N_k. При шифровании выбирается система оснований степени не выше N_k и порядок их расположения, а также генерируется ключевая последовательность длиной N_k [3, 4]. Все используемые на 1-м и 3-м этапах основания выбираются независимо друг от друга, но среди них могут быть и совпадающие. Условия выбора дополнительных оснований зависят от процедуры хэширования, которая и определяет различные алгоритмы формирования подписи: один из предложенных алгоритмов описан в [4]. Выбор оснований на всех этапах производится из созданной базы данных неприводимых многочленов.

В предлагаемом алгоритме при хэшировании выбирается одно избыточное основание $p_{S+1}(x)$ из числа всех неприводимых многочленов степени меньше N_k. Затем формируются три избыточных вычета $\alpha_{S+1}(x)$, $\alpha_{S+2}(x)$, $\alpha_{S+3}(x)$, которые и определяют хэш-значение из N_k бит. Эти вычеты используются не только для создания ЭЦП, но и для обнаружения и коррекции одиночной ошибки и выявления многократной ошибки. Первый вычет – это остаток по модулю дополнительного основания $p_{S+1}(x)$ от суммирования произведений рабочих вычетов и их порядковых номеров:

$$\alpha_{S+1}(x) = \sum_{i=1}^{S} \left| i\alpha_i(x) \right|_{p_{S+1}(x)}, \qquad (5)$$

где знак суммы $\sum$ означает поразрядное сложение по модулю 2, $\left| i\alpha_i(x) \right|_{p_{S+1}(x)}$ - вычет по модулю $p_{S+1}(x)$. Второй из дополнительных вычетов определяется как сумма всех рабочих вычетов по модулю 2:

$$\alpha_{S+2}(x) = \sum_{i=1}^{S} \alpha_i(x). \qquad (6)$$

Третий остаток вычисляется по модулю дополнительного основания от позиционного представления многочлена $F(x)$ по формуле (3):

$$\alpha_{S+3}(x) = \sum_{i=1}^{S} \left| \alpha_i(x) P_i(x) \right|_{p_{S+1}(x)}. \qquad (7)$$

Корректирующие функции алгоритма создания ЭЦП заключаются в обнаружении ошибок и исправления одиночной ошибки. При расширении многочлена $F(x)$ на избыточные вычеты выражение (1) примет вид:

$$F(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_j(x), ..., \alpha_S(x),$$
$$\alpha_{S+1}(x), \alpha_{S+2}(x), \alpha_{S+3}(x)).$$

При наличии одной ошибки в информационных вычетах (например, по j-му рабочему основанию $p_j(x)$) избыточные вычеты (5)–(7) изменят свои значения на $\alpha^*_{S+1}(x)$, $\alpha^*_{S+2}(x)$, $\alpha^*_{S+3}(x)$. Ошибка - это любое искажение $\alpha_j(x)$ по модулю $p_j(x)$, и ее величина может быть равна любому элементу из полной системы вычетов по модулю $p_j(x)$, $1 \le j \le S$. Тогда $F(x)$ представится в виде

$$F(x) = (\alpha_1(x), \alpha_2(x), ..., \overline{\alpha}_j(x), ..., \alpha_S(x),$$
$$\alpha^*_{S+1}(x), \alpha^*_{S+2}(x), \alpha^*_{S+3}(x)),$$

$\overline{\alpha}_j(x)$ принадлежит полной системе вычетов по модулю основания $p_j(x)$.

Выявление и коррекция одиночной ошибки осуществляется двумя избыточными вычетами [1,2]. В рассматриваемом алгоритме для этого используются вычеты (5) и (6). Пусть $\overline{\alpha}_j(x) = \alpha_j(x) + \Delta_j(x)$, где $\Delta_j(x)$ - величина ошибки. Если в хранимом или передаваемом сообщении произошла ошибка $\Delta_j(x)$, то система (5)–(6) запишется в виде

$$\alpha^*_{S+1}(x) = \sum_{i=1}^{S} \left| i\alpha_i(x) \right|_{p_{S+1}(x)} \oplus \left| j\Delta_j(x) \right|_{p_{S+1}(x)},$$

$$\alpha^*_{S+2}(x) = \sum_{i=1}^{S} \alpha_i(x) \oplus \Delta_j(x), \qquad (8)$$

где "⊕" - операция поразрядного сложения по модулю 2. Вычитая (5) из первого уравнения (8), а (6) - из второго уравнения (8), получим

$$\alpha^*_{S+1}(x) \oplus \alpha_{S+1}(x) = \left| j\Delta_j(x) \right|_{p_{S+1}(x)},$$

$$\alpha^*_{S+2}(x) \oplus \alpha_{S+2}(x) = \Delta_j(x). \qquad (9)$$

Обозначим невязки, то есть левые части (8), соответственно $\xi(x)$ и $\eta(x)$. Тогда система (9) перепишется в виде

$$\xi(x) = \left| j\Delta_j(x) \right|_{p_{S+1}(x)}, \ \eta(x) = \Delta_j(x). \qquad (10)$$

Как видно, величина ошибки определяется вторым уравнением (10). Номер ошибочного основания находится из первого уравнения (10), для этого необходимо определить инверсный для $\Delta_j(x)$ многочлен $\Delta_j^{-1}(x)$.

Для проверки того, была ли ошибка одиночной, вычисляются значения вычета $\alpha_{S+3}(x)$ до и после обнаружения и коррекции ошибки: если эти значения не совпадают, то выявленная ошибка является многократной.

Покажем, что каждой ошибке $\Delta_j(x)$ соответствует одна и только одна пара невязок (10).

Предложение 1. Каждой ошибке $\Delta_j(x)$ соответствует одна пара невязок $\xi(x)$, $\eta(x)$.

Предположим обратное, то есть одной ошибке $\Delta_j(x)$ отвечают две пары невязок $\xi(x)$, $\eta(x)$ и $\xi'(x)$, $\eta'(x)$. Тогда, кроме системы (10), будет иметь место также и система

$$\xi'(x) = \left| j\Delta_j(x) \right|_{p_{S+1}(x)}, \ \eta'(x) = \Delta_j(x). \qquad (11)$$

При вычитании (10) из (11) получим, что $\xi'(x) \oplus \xi(x) = 0$, $\eta'(x) \oplus \eta(x) = 0$, откуда следует, что $\xi'(x) = \xi(x)$ и $\eta'(x) = \eta(x)$. Предположение оказалось ошибочным.

Предложение 2. Каждой паре невязок $\xi(x)$, $\eta(x)$ соответствует одна ошибка $\Delta_j(x)$.

Допустим противоположное. Пусть одной паре невязок $\xi(x)$, $\eta(x)$ соответствуют две ошибки, например, $\Delta_j(x)$ и $\Delta_t(x)$ соответственно по основаниям $p_j(x)$ и $p_t(x)$. В этом случае получим, кроме системы (10), еще одну систему:

$$\xi(x) = \left| t\Delta_t(x) \right|_{p_{S+1}(x)}, \ \eta(x) = \Delta_t(x). \qquad (12)$$

Вычтем (10) из (12), результатом будет система:

$$0 = \left| t\Delta_t(x) \oplus j\Delta_j(x) \right|_{p_{S+1}(x)},$$

$$0 = \Delta_t(x) \oplus \Delta_j(x), \qquad (13)$$

откуда следует, что $\Delta_t(x) = \Delta_j(x)$. Тогда из первого уравнения (12) вытекает, что $\left| (t-j)\Delta_j(x) \right|_{p_{S+1}(x)} = 0$. Так как $\Delta_j(x) \neq 0$, то $t = j$, а это означает, что допущение было неправильным.

Чтобы алгоритм обнаружения и исправления ошибок был однозначным (удовлетворял предложениям 1 и 2), множества ошибок и множества невязок должны быть изоморфны: общее число ошибок не может превышать общего количества всех невязок, а это определит условия выбора $p_{S+1}(x)$.

Введем обозначение $\|\varphi\|_{p_i(x)}$ - число элементов в полной системе вычетов по модулю основания $p_i(x)$, $i = 1,2,\ldots,S+1$. Упорядочим расположение рабочих оснований в порядке увеличения их степеней $m_1 \le m_2 \le \ldots \le m_S$, то есть здесь и далее m_1 - наименьшая их степень, а m_S - наибольшая. Тогда для полных систем вычетов по модулям рабочих оснований можно записать

$$\|\varphi\|_{p_1(x)} \le \|\varphi\|_{p_2(x)} \le \ldots \le \|\varphi\|_{p_S(x)}$$

или

$$2^{m_1} \le 2^{m_2} \le \ldots \le 2^{m_S}. \qquad (14)$$

Общее число ошибок есть сумма элементов полных систем вычетов по всем основаниям. Число всех невязок определяется произведением числа элементов полной системы вычетов по модулю избыточного основания и количества элементов полной системы вычетов по модулю информационного основания наибольшей степени $\|\varphi\|_{p_{S+1}(x)} \cdot \|\varphi\|_{p_S(x)}$, что следует из (10). Тогда требуемое условие ограничения на избыточное основание $p_{S+1}(x)$ запишется в виде неравенства

$$\sum_{i=1}^{S} \|\varphi\|_{p_i(x)} \le \|\varphi\|_{p_{S+1}(x)} \cdot \|\varphi\|_{p_S(x)}. \qquad (15)$$

Расписывая (15) через число элементов в полной системе вычетов с учетом (14), получим

$$2^{m_{S+1}+m_S-m_1} \geq S. \qquad (16)$$

Неравенство (16) определяет условия выбора степени избыточного основания $p_{S+1}(x)$ в общем случае и характеризует ее зависимость от наибольшей и наименьшей степеней конкретной системы рабочих оснований и их количества S. Если же все основания, рабочие и дополнительное, будут иметь одинаковые степени, то в этом случае из (16) получим неравенство

$$2^{m_{S+1}} \geq S, \qquad (17)$$

показывающее, что степень избыточного основания m_{S+1} не должна превышать количества всех информационных оснований S. В случае, когда все рабочие основания имеют одну степень, а степень основания m_{S+1} будет отличаться от нее, то из (16) также следует (17).

Предположим теперь, что избыточное основание имеет степень $m_{S+1} < m_S$, а ошибка произошла по рабочему основанию, степень которого больше m_{S+1}. В этом случае ошибочный вычет может совпасть с $p_{S+1}(x)$ и тогда невозможно определение его номера из выражения

$$j = \left|\Delta_j(x)\Delta_j^{-1}(x)\right|_{p_{S+1}(x)} = \left|\Delta_j(x)\Delta_j^{-1}(x)\right|_{\Delta_j(x)}.$$

Из этого следует, что степень $p_{S+1}(x)$ должна быть не меньше наибольшей степени рабочих оснований:

$$m_{S+1} \geq m_S. \qquad (18)$$

Таким образом, избыточное основание выбирается таким, чтобы выполнялись одновременно два налагаемых на него условия (16) и (18).

Рассмотрим возможные ошибки по дополнительным вычетам.

1. Ошибочно одно из двух первых вычетов $\alpha_{S+1}(x)$ и $\alpha_{S+2}(x)$.

При проверке ЭЦП окажется отличной от нуля невязка по ошибочному вычету, другие две невязки будут равны нулю. После проверки ЭЦП ошибочный вычет исправляется заменой вновь вычисленным. Если при этом ошибка произошла также по третьему дополнительному вычету, то ошибочные вычеты заменяются вновь вычисленными.

2. Ошибочными являются оба первых вычета $\alpha_{S+1}(x)$ и $\alpha_{S+2}(x)$.

Поскольку по этим вычетам обе невязки отличны от нуля, то получаем вариант ошибки в информационном вычете. Поэтому ищем ошибку как одиночную по рабочему основанию. Ошибочный вычет выявляем и исправляем, то есть правильный заменяем на неверный и вносим третью ошибку. Затем вычисляем $\alpha_{S+3}(x)$, который покажет, что ошибка не одиночна. Если неверны все три избыточных вычета, то поступаем также.

При формировании ЭЦП ее длина $N_k << N$. Длина ЭЦП формируется избыточными вычетами, поэтому для записи вычетов $\alpha_{S+1}(x)$ и $\alpha_{S+3}(x)$ по модулю $p_{S+1}(x)$ нужно m_{S+1} бит, а вычета $\alpha_{S+2}(x)$ - m_S бит, поэтому

$$N_k = 2m_{S+1} + m_S < N. \qquad (19)$$

Тогда степень избыточного вычета определяется неравенством

$$(N_k - m_S)/2 < m_{S+1} < (N - m_S)/2. \qquad (20)$$

Из (19) и (20) следует более сильное ограничение на длину ЭЦП и степень $p_{S+1}(x)$:

$$3m_S < N_k < 3m_{S+1} < N. \qquad (21)$$

Как показано выше, выбор избыточного основания зависит от наибольшей степени информационных оснований. Для сообщения длины N возможно конкретное число всех систем рабочих оснований, покрывающих его. В каждой из этих систем рабочих оснований имеется свое конкретное наибольшее значение их степени, поэтому для сообщения длиной N степень m_S принимает значения из конкретного диапазона возможных наибольших степеней. Тогда, как следует из выражений (20) и (21), по описанному алгоритму могут быть сформированы несколько ЭЦП с различными длинами N_k, k=1,2,…,K, где K – число всех возможных цифровых подписей

Криптостойкость алгоритма определяется количеством всевозможных способов выбора оснований на всех этапах формирования ЭЦП: 1) системы рабочих оснований из множества неприводимых многочленов степени не выше N; 2) избыточного основания из множества неприводимых многочленов степени не выше N_k с учетом условий (16) и (18); 3) полного ключа шифрования полученного хэш-значения длиной N_k.

Определим количество таких способов для каждого этапа

1) Число возможных систем из S выбранных рабочих оснований $p_1(x), p_2(x),..., p_S(x)$ степени от m_1 до m_S определяется уравнением (4) с учетом всех перестановок рабочих оснований [3]:

$$Z_1 = (k_1 + k_2 + ... + k_s)!\, C_{n_1}^{k_1} C_{n_2}^{k_2} ... C_{n_s}^{k_s}. \quad (22)$$

2) Количество способов выбора одного избыточного основания $p_{S+1}(x)$ равно числу n_{S+1} всех неприводимых многочленов степени m_{S+1}:

$$Z_2 = C_{n_{S+1}}^{1} = n_{S+1}. \quad (23)$$

Тогда все способы выбора дополнительного основания для одной конкретной системы рабочих оснований равно произведению $Z_1 Z_2$.

3) На этапе шифрования хэш-значения длиной N_k формируется полный ключ из системы оснований $r_1(x), r_2(x),..., r_W(x)$ с учетом их перестановок и генерируемой псевдослучайной последовательности [3]. Обозначим степени и число неприводимых многочленов, используемых при выборе оснований $r_1(x), r_2(x),..., r_W(x)$, соответственно $b_1, b_2,..., b_W$ и $l_1, l_2,..., l_W$. Из аналога уравнения (4)

$$v_1 r^{b_1}(x) + v_2 r^{b_2}(x) + ... + v_W r^{b_W}(x) = N_k, \quad (24)$$

где $0 \le v_i \le l_i$ - неизвестные коэффициенты, $r^{b_j}(x)$ - многочлен степени b_j, $1 \le b_j \le b_W \le N_k$, $W = v_1 + v_2 + ... + v_W$, находятся W оснований системы, запись вычетов по которым покрывает шифруемое хэш-значение длины N_k.

Шифрование производится реализацией некоторой функции $H_1(F_1(x), G_1(x))$, где $G_1(x)$ - ключевая последовательность длины N_k, $F_1(x)$ - полученная последовательность двоичных символов хэш-значения. Тогда количество комбинаций полных ключей определится соотношением

$$Z_3' = 2^{N_k} (v_1 + v_2 + ... + v_W)!\, C_{l_1}^{v_1} C_{l_2}^{v_2} ... C_{l_W}^{v_W}.$$

Все варианты выбора различных систем оснований и ключевой последовательности получим из выражения

$$Z_3 = \quad (25)$$

$$= 2^{N_k} \sum_{v_1, v_2, ..., v_W} (v_1 + v_2 + ... + v_W)!\, C_{l_1}^{v_1} C_{l_2}^{v_2} ... C_{l_W}^{v_W}.$$

В (25) суммирование производится по всевозможным комбинациям целых положительных чисел $v_1, v_2, ..., v_W$, удовлетворяющих уравнению (24) [3]. Для одной системы рабочих оснований при конкретных значениях m_S и m_{S+1} все способы формирования проверяющей подписи будут определяться произведением $Z_1 Z_2 Z_3$. Тогда всевозможные варианты формирования ЭЦП длины N_k должны учитывать все системы рабочих оснований, определяемых уравнением (4), т. е. описываться формулой $Z_k = \sum_{k_1, k_2, ..., k_S} Z_1 Z_2 Z_3$. Все же способы формирования ЭЦП с проверяющими функциями для сообщения определенной длины N есть сумма всех Z_k, а ее обратная величина является искомой криптостойкостью:

$$p_{sig} = 1/ [\sum_{k=1}^{K} 2^{N_k} n_{S+1} \times \quad (26)$$

$$\times (\sum_{k_1, k_2, ..., k_S} (k_1 + k_2 + ... + k_s)!\, C_{n_1}^{k_1} C_{n_2}^{k_2} ... C_{n_S}^{k_S} \times$$

$$\times \sum_{v_1, v_2, ..., v_W} (v_1 + v_2 + ... + v_W)!\, C_{l_1}^{v_1} C_{l_2}^{v_2} ... C_{l_W}^{v_W})] .$$

Например. 1) Пусть сообщение имеет длину 16 бит. Минимальное значение наибольшей степени рабочих оснований $m_S = 4$, так как при меньших его значениях не существует систем рабочих оснований, покрывающих 16 бит. В таблице приведены все системы рабочих оснований, которые могут быть здесь использованы. Из неравенства (18) следует, что возможны 2 варианта значений m_S, для которых получаем следующие ограничения на дополнительное основание m_{S+1}: 1) $m_S = 4$, $m_{S+1} \le 6$; 2) $m_S = 5$, $m_{S+1} \le 5$. Тогда допустимыми будут варианты; 1) $m_S = 4$, $m_{S+1} = 4$, $N_1 = 12$; 2) $m_S = 4$, $m_{S+1} = 5$, $N_1 = 14$; 3) $m_S = 5$, $m_{S+1} = 5$, $N_1 = 15$. Из (26) получим: $p_{sig} \approx 10^{-14}$.

2) Пусть N = 256 байт = 2048 бит. Найдем криптостойкость для одной системы рабочих оснований. Выберем 80 многочленов 16-й степени, 60 многочленов 12-й степени и 6 многочленов 8-й степени: S=146 и $Z_1 \approx 5 \cdot 10^{529}$. Избыточное основание - многочлен 16-й степени: $Z_2 = 7749$.

Возможные системы рабочих оснований

Степень рабочих оснований	Системы оснований							
1	1		1		1		1	1
2		1		1	1		1	
3	1	2			1	1		2
4	3	2		1		2	2	1
5			3	2	2	1	1	1
S – число выбранных оснований	5	5	4	4	5	4	5	5

Тогда $N_k = 48$. Для шифрования хэш-значения выбираем полиномы 15-й, 14-й, 13-й и 6-й степени, тогда $W = 4$ и $Z_3' \approx 4 \cdot 10^{26}$, откуда $p_{sig} \approx 10^{-561}$.

Таким образом, в представленном нетрадиционном алгоритме длина и надежность формируемой подписи определяется длиной подписываемого сообщения, выбором системы рабочих оснований и процедурой хэширования, а ее криптостойкость достигает достаточно высоких значений.

ЛИТЕРАТУРА

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

2. *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.

3. *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.

4. *Бияшев Р. Г., Нысанбаева С. Е* Исследование надежности электронной цифровой подписи в непозиционной полиномиальной системе счисления // Изв. НАН РК. Сер. физ.-мат. наук. 2006. № 5. С. 56-61.

5. *Моисил Гр. К.* Алгебраическая теория дискретных автоматических устройств. М.: ИЛ, 1963. 680 с.

Резюме

Позициялы емес полиномды санау жүйесінде электрондық сандық қолтаңба түзетін процедура қарастырылған. Қолтаңба бір артылымды негіз модулі бойынша құрылады және қосымша тексеру қасиеттеріне ие. Жалғыз қателерді табу мен түзету процедурасының бір-мәнділігі көрсетілген. Сандық қолтаңба құрайтын алгоритмнің криптотұрақтылық формуласы анықталды.

Summary

A procedure of the formation an electronic digital signature in the non-positional polynomial notation is considered. The signature is created modulo one surplus base and given additional controlling properties. It has been determined that the procedure of discovering and correcting solitary error is one-valued. A formula of cryptostability for algorithm of creation digital signature is obtained.

Институт проблем информатики и управления МОН РК, г. Алматы

Поступила 20.09.07г.