Р. Г. Бияшев, С. Е. Нысанбаева

МОДУЛЯРНАЯ СХЕМА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ КОДОВ ЛАГРАНЖА

Рассматриваются результаты построения алгоритма формирования электронной цифровой подписи, в котором применен подход, предложенный при разработке самокорректирующихся (n,k)-кодов Лагранжа и базирующийся на непозиционной мультипликативной композиции векторов и представлении полиномов в виде интерполяционных формул Лагранжа в конечном поле $FG(q)$ [1]. Поле $FG(q)$ порождается неприводимым многочленом $p(x)$ степени m над полем $FG(q)$ и его элементы представляются ρ-ичным кодом. В коде Лагранжа $n = q$ ($q = p^m$) символов составляют его максимальную длину, а любые k символов могут быть информационными. В процессе кодирования не происходит искажения выбранного набора информационных символов.

Рассмотрим основные положения алгебры полиномов над полем $FG(q)$, обладающих свойством однозначного восстановления полинома по его значениям в узлах, взятых из этого поля [1]. Множество элементов поля $FG(q)$, названных локаторами, пронумеровано целыми числами из интервала $[0,q)$ и расположено в упорядоченном виде: $I = \{\mathsf{w}_0 < \mathsf{w}_1 < \ldots < \mathsf{w}_{q-1}\}$. Каждый локатор характеризуется порядком расположения «i» и величиной w_i. Задается также множество I_n, состоящее из n локаторов, $I_n \subseteq I$.

Пусть в поле $FG(q)$ задана некоторая упорядоченная последовательность элементов (α_1, α_2, ..., α_n). Требуется построить полином $f(x)$, такой, что для каждого локатора $\mathsf{w}_i \in I_n$ выражение $f(\mathsf{w}_i) = \alpha_i$ имеет единственное решение в классе полиномов степени не выше $n-1$ (при $n \le q-1$). Искомый полином задается интерполяционной формулой Лагранжа:

$$f(x) = \sum_{i=1}^{n} f(\mathsf{w}_i) L_n^{(i)}(x), \tag{1}$$

где

$$L_n^{(i)}(x) = \frac{(x-\omega_1)\ldots(x-\omega_{i-1})(x-\omega_{i+1})\ldots(x-\omega_n)}{(\omega_i-\omega_1)\ldots(\omega_i-\omega_{i-1})(\omega_i-\omega_{i+1})(\omega_i-\omega_n)}, \quad 1 \le i \le n. \tag{2}$$

Многочлены (2) — фундаментальные полиномы Лагранжа. Вводится также система обозначений:

$$P_{I_n}(x) = \prod_{\mathsf{w}_s \in I_n} (x - \mathsf{w}_s), \quad P_{I_n}^{(s)}(x) = \frac{P_{I_n}(x)}{(x-\mathsf{w}_s)},$$

$$P_{I_n}^{(s)}(\omega_s) = (\omega_s-\omega_1)\ldots(\omega_s-\omega_{s-1})(\omega_s-\omega_{s+1})\ldots(\omega_s-\omega_n).$$

Тогда s-й фундаментальный многочлен Лагранжа запишется в виде $L_{I_n}^{(s)}(x) = \dfrac{P_{I_n}^{(s)}(x)}{P_{I_n}^{(s)}(\mathsf{w}_s)}$.

Для однозначного восстановления произвольного полинома $f(x)$ по его значениям в локаторах (узлах), взятых из поля $FG(q)$, необходимо рассматривать множество вычетов полинома $f(x)$ по модулю $P_{I_n}(x)$, которые представляются интерполяционными полиномами Лагранжа (1):

$$f(x) = < f(x) \big|_{P_{I_n}(x)} + q(x) P_{I_n}(x), \tag{3}$$

где

$$< f(x) \big|_{P_{I_n}(x)} = \sum_{\omega_s \in I_n} f(\omega_s) L_{I_n}^{(s)}(x). \tag{4}$$

Обозначения $< f(x)|_{P_{I_n}(x)}$ в (3)—(4) и $< \bullet|_{P_{I_n}}$ представляют множество всех многочленов, степень которых меньше степени полинома $P_{I_n}(x)$.

Важнейшая особенность алгебры $< \bullet|_{P_{I_n}}$ — каждый элемент (полином) $g(x) \in < \bullet|_{P_{I_n}}$ может быть однозначно представлен кодовым вектором размерности n с компонентами из поля $FG(q)$: $g(x) \to (g(\mathsf{w}_1),...,g(\mathsf{w}_n))$, и это отображение является биективным. Совокупность всех таких кодовых слов названа кодом Лагранжа. Рассмотрим реализацию основных операций на языке кодовых векторов Лагранжа. Пусть $g(x) \leftrightarrow (g_1, g_2,..., g_n)$, $f(x) \leftrightarrow (f_1, f_2,..., f_n)$, $g_i \in GF(q)$, $f_i \in GF(q)$, $i = \overline{1,n}$, тогда

$$< g(x) \pm f(x)|_{P_{I_n}(x)} = g(x) \pm f(x) \leftrightarrow (g_1 \pm f_1,..., g_n \pm f_n), \tag{5}$$

и для любого элемента $\alpha \in GF(q)$

$$\alpha g(x) \leftrightarrow \alpha(g_1,..., g_2\} = (\alpha g_1,..., \alpha g_n), \tag{6}$$

$$< g(x) \cdot f(x)|_{P_{I_n}(x)} \leftrightarrow (g_1 \cdot f_1,..., g_n \cdot f_n). \tag{7}$$

На языке кодов Лагранжа все операции (5)—(7) алгебры $< \bullet|_{P_{I_n}}$ осуществляются покомпонентно, следовательно, коды Лагранжа обладают параллельной структурой. При выполнении условия

$$\deg g(x) + \deg f(x) < \deg P_{I_n}(x) \tag{8}$$

имеет место равенство $< g(x) \cdot f(x)|_{P_{I_n}(x)} = g(x) \cdot f(x)$, т. е. при условии выполнения (8) коды Лагранжа распараллеливают операцию обычного умножения полиномов.

Избыточность в кодах Лагранжа задается следующим образом. Пусть I_q — множество всех элементов (локаторов) поля $FG(q)$, упорядоченных некоторым образом, т. е. $x_1 < x_2 < ... < x_q$, $F_q[x]$ — кольцо многочленов над полем $FG(q)$ степени не выше q — 1, I_n — подмножество множества I_q, состоящее из n элементов, $P_{I_n}(x) = \prod_{i \in IN}(x - x_i)$, IN— множество индексов элементов множества I_n. Отметим, что элементы всех выбранных подмножеств множества I_q расположены в «возрастающем» порядке в соответствии с принятой упорядоченностью.

Рассматривается код Лагранжа (α_1, α_2, ..., α_n), в котором $\alpha_i \in GF(q)$, $i = \overline{1,n}$. Порождаемая им алгебра задается системой полиномов $< \bullet|_{P_{I_n}} = \{a(x) \mid a(x) = \sum_{i=1}^{n} \widetilde{\alpha}_i P_{I_n}^{(i)}(x)\}$, $P_{I_n}^{(i)}(x) = \dfrac{P_{I_n}(x)}{(x - x_i)}$, $\widetilde{\alpha}_i = \alpha_i [P_{I_n}^{(i)}(x_i)]^{-1}$.

Аддитивная и мультипликативная композиции над векторами Лагранж $\overline{a} = (\alpha_1, \alpha_2, ..., \alpha_n) \leftrightarrow a(x) \in < \bullet|_{\rho_{I_n}}$, $\overline{b} = (\beta_1, \beta_2, ..., \beta_n) \leftrightarrow b(x) \in < \bullet|_{\rho_{I_n}}$ выполняются по правилам:

$$\overline{a} + \overline{b} = (\alpha_1 + \beta_1,..., \alpha_n + \beta_n) \leftrightarrow a(x) + b(x) \in < \bullet|_{P_{I_n}},$$

$$\overline{a} * \overline{b} = (\alpha_1 \cdot \beta_1,..., \alpha_n \cdot \beta_n) \leftrightarrow < a(x)b(x)|_{P_{I_n}}.$$

Предполагается, что первые k символов α_1, α_2, ..., α_k кодового слова (вектора) длины n $(k < n)$ являются информационными. Избыточные символы α_{k+1}, α_{k+2}, ..., α_n определяются посредством операции расширения

$$\alpha_{k+s} = \sum_{i=1}^{k} \widetilde{\alpha}_i P_{I_k}^{(i)}(x_{k+s}),\ s = \overline{1, n-k},\ I_k = \{x_1,..., x_k\}. \tag{9}$$

Таким образом, получен (n,k)-код, в котором любые $(n\text{-}k)$ символов могут считаться избыточными или проверочными.

В предлагаемом алгоритме электронная цифровая подпись формируется в конечном поле $FG(q)$, $q = 2^m$, $p = 2$. Алгоритм формирования цифровой подписи для электронного сообщения включает следующие этапы.

1-й этап. Конечное поле $GF(2^m)$ порождается неприводимым многочленом $p(x)$ степени m. Это поле содержит $n = 2^m$ элементов (символов). Элементы поля имеют запись в m бит, сообщение представляется в двоичной записи, содержащей $N = m \cdot n$ бит. Затем из n элементов выбираются t_j элементов в качестве избыточных локаторов (узлов). Их количество определяется требованиями, предъявляемыми к формируемой цифровой подписи. В этих узлах вычисляются избыточные символы (хэш-значение) кодового слова, из которых формируется ЭЦП. Оставшиеся $k_j = n - t_j$ элементов поля являются информационными узлами. Расположение всех элементов поля $FG(q)$ упорядочивают: например, для удобства вначале располагаются информационные локаторы, а за ними следуют избыточные: $x_1, x_2, ..., x_{k_j}, x_{k_{j+1}}, x_{k_{j+2}}, ..., x_n$.

Количество t_j, $j = 1,2,...,S$ избыточных узлов может быть разным в зависимости как от длины электронного сообщения, так и от предъявляемых к ЭЦП требований. Таким образом, для одного сообщения возможно создание S подписей, каждая длиной $N_{k_j} = m \cdot t_j$ бит, $j = 1,2,...,S$. Каждому t_j отвечает конкретное количество k_j информационных узлов.

2-й этап. Представление электронного сообщения в виде кодовых векторов Лагранжа. Подписываемое сообщение разбивается на блоки длиной N_{m_j} бит. Каждый блок интерпретируется как некоторый многочлен $F(x)$:

$$F(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_k(x)), \tag{10}$$

где $\alpha_i(x)$, $i = \overline{1,k}$ являются элементами поля $GF(2^m)$ и полагаются значениями полинома $F(x)$ в информационных узлах x_i, $i = \overline{1,k}$, т. е. они — информационные символы в кодовых векторах Лагранжа из n символов. В представлении (10) полагается, что первые l_1 бит являются коэффициентами многочлена (символа) $\alpha_1(x)$, следующие l_2 бит — коэффициенты полинома $\alpha_2(x)$ и так далее, последние двоичные разряды l_k задают многочлен $\alpha_k(x)$. Напомним, что значения $l_i = m$, $i = \overline{1,k}$.

3-й этап. На этом этапе производится хэширование (сжатие) блока сообщения от длины N_{m_j} до длины N_{k_j}: для этого вычисляются избыточные символы $\alpha_{k+1}(x)$, $\alpha_{k+2}(x)$, ..., $\alpha_{k_j+t_j}(x)$ в соответствии с операцией расширения (9):

$$\alpha_{k_j+u} = \sum_{i=1}^{k_j} \tilde{\alpha}_i P_{I_{k_j}}^{(i)}(x_{k_j+u}),\ u = \overline{1, n\text{-}k_j},\ I_{k_j} = \{x_1, ..., x_{k_j}\}\ . \tag{11}$$

Таким образом, первые три этапа формируют кодовые слова Лагранжа длиной $N = N_{m_j} + N_{k_j}$ бит.

4-й этап — вычисление ЭЦП. Хэш-значение зашифровывается одним из нетрадиционных алгоритмов шифрования непозиционных полиномиальных систем счисления [2—5].

При получении сообщения адресат проверяет цифровую подпись. Для этого он определяет два хэш-значения. Одно хэш-значение вычисляется от полученного им сообщения, а другое находится в результате расшифрования ЭЦП. Подпись считается подлинной, если совпадают оба хэш-значения, найденные адресатом.

Рассмотрим пример вычисления ЭЦП. Пусть кодовое слово формируется из элементов поля $GF(2^3)$, $n = 8$. Ими являются следующие многочлены, приведенные в порядке возрастания их степени: 0, 1, x, $x+1$, x^2, x^2+1, x^2+x, x^2+x+1 . В двоичном представлении эти элементы записываются соответственно следующим образом: 000, 001, 010, 011, 100, 101, 110, 111. В такой же последовательности обозначим локаторы поля $GF(2^3)$: $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$.

Элементы поля имеют одну и ту же длину $m = 3$ бита, тогда кодовое слово (информационные символы плюс избыточные) состоит из 8 символов длиной N—24 бит. Избыточными

узлами выберем последние три локатора x_6, x_7, x_8, тогда информационными узлами будут x_1, x_2, x_3, x_4, x_5: $t_j = 3$, $k_j = 5$, $N_{k_j} = 9$ бит, $N_{m_j} = 15$ бит. Пусть подписывается сообщение длиной 30 бит: (010001100101001111000110011101). Оно разбивается на два равных блока по 15 бит. Первый и второй блоки интерпретируются соответственно как некоторые многочлены $F_1(x) = (\alpha_{11}(x), \alpha_{21}(x), \alpha_{31}(x), \alpha_{41}(x), \alpha_{51}(x))$ и $F_2(x) = (\alpha_{12}(x), \alpha_{22}(x), \alpha_{32}(x), \alpha_{42}(x), \alpha_{52}(x))$, где $\alpha_{ij}(x)$, $i = 1,5$, $j = 1,2$ — значения полиномов $F_j(x)$, $j = 1,2$, в узлах x_i, $i = \overline{1,5}$. Эти многочлены в двоичном представлении имеют вид: $F_1(x) = (010001100101001)$, $F_2(x) = (111000110011101)$.

Информационными символами в первом блоке будут многочлены $\alpha_{11}(x) = x$, $\alpha_{21}(x) = 1$, $\alpha_{31}(x) = x^2$, $\alpha_{31}(x) = x^2 + 1$, $\alpha_{51}(x) = 1$, а во втором блоке — $\alpha_{21}(x) = x^2 + x + 1$, $\alpha_{22}(x) = 0$, $\alpha_{32}(x) = x^2 + x$, $\alpha_{42}(x) = x^2 + 1$, $\alpha_{52}(x) = x^2 + 1$.

Три избыточных символа определяются по формуле (11):

$$\alpha_{5+t,j} = \sum_{i=1}^{5} \tilde{\alpha}_i P_{I_5}^{(i)}(x_{5+t}),\ t = \overline{1,3},\ j = 1,2,\ I_5 = \{x_1, x_2, x_3, x_4, x_5\},\ \tilde{\alpha}_i = \alpha_i [P_{I_5}^{(i)}(x)]^{-1},\ P_{I_5}^{(i)}(x) = \frac{P_{I_5}(x)}{x - x_i},$$

$$P_{I_5}(x) = (x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5),\ i = \overline{1,5}\ .$$

Если неприводимым многочленом выбрать $x^3 + x + 1$, то в результате вычислений будут получены: $\rho^{(i)}{}_{I_5}(x_i)$ и инверсные к ним величины $\rho^{(1)}{}_{I_5}(x_1) = 101$; $[\rho^{(1)}{}_{I_5}(x_1)]^{-1} = 010$; $\rho^{(2)}{}_{I_5}(x_2) = 011$; $[\rho^{(2)}{}_{I_5}(x_2)]^{-1} = 110$; $\rho^{(3)}{}_{I_5}(x_3) = 010$; $[\rho^{(3)}{}_{I_5}(x_3)]^{-1} = 101$; $\rho^{(4)}{}_{I_5}(x_4) = 100$; $[\rho^{(4)}{}_{I_5}(x_4)]^{-1} = 111$; $\rho^{(5)}{}_{I_5}(x_5) = 011$; $[\rho^{(5)}{}_{I_5}(x_5)]^{-1} = 110$; значения $\rho^{(i)}{}_{I_5}(x)$ в избыточных узлах x_6, x_7, x_8 и $\tilde{\alpha}_i = \alpha_i [\rho^{(i)}{}_{I_5}(x)]^{-1}$: $\rho^{(1)}{}_{I_5}(x_6) = 010$; $\rho^{(2)}{}_{I_5}(x_6) = 111$; $\rho^{(3)}{}_{I_5}(x_3) = 111$; $\rho^{(4)}{}_{I_5}(x_6) = 101$; $\rho^{(5)}{}_{I_5}(x_6) = 011$; $\rho^{(1)}{}_{I_5}(x_7) = 001$; $\rho^{(2)}{}_{I_5}(x_7) = 101$; $\rho^{(3)}{}_{I_5}(x_7) = 100$; $\rho^{(4)}{}_{I_5}(x_7) = 111$; $\rho^{(5)}{}_{I_5}(x_7) = 011$; $\rho^{(1)}{}_{I_5}(x_8) = 010$; $\rho^{(2)}{}_{I_5}(x_8) = 100$; $\rho^{(3)}{}_{I_5}(x_8) = 001$; $\rho^{(4)}{}_{I_5}(x_8) = 110$; $\rho^{(5)}{}_{I_5}(x_8) = 011$; $\tilde{\alpha}_{1_1} = 100$, $\tilde{\alpha}_{2_1} = 110$, $\tilde{\alpha}_{3_1} = 010$, $\tilde{\alpha}_{4_1} = 110$, $\tilde{\alpha}_{5_1} = 110$; $\tilde{\alpha}_{1_2} = 101$, $\tilde{\alpha}_{2_2} = 000$, $\tilde{\alpha}_{3_2} = 011$, $\tilde{\alpha}_{4_2} = 010$, $\tilde{\alpha}_{5_2} = 011$; избыточные символы блоков: $\alpha_{6_1}(x) = 000$, $\alpha_{7_1}(x) = 001$, $\alpha_{8_1}(x) = 111$; $\alpha_{6_2}(x) = 100$, $\alpha_{7_2}(x) = 010$, $\alpha_{8_2}(x) = 000$; хэш-значения двух блоков: $h_1 = (\alpha_{6_1}, \alpha_{7_1}, \alpha_{8_1}) = (000001111)$ и $h_2 = (\alpha_{6_2}, \alpha_{7_2}, \alpha_{8_2}) = (100010000)$. За хэш-значение сообщения принимается их поразрядная сумма $h = h_1 \oplus h_2$: $h(x) = (\alpha h_1(x), \alpha h_2(x), \alpha h_3(x)) = (100011111)$. Зашифровав хэш-значение, получим цифровую подпись. Для шифрования может быть использован один из указанных выше нетрадиционных алгоритмов шифрования.

Для определения криптостойкости алгоритма построения ЭЦП находится количество всех возможных способов формирования полного секретного ключа. Полный ключ определяется многочленом $p(x)$ степени m, числом избыточных узлов, распределением избыточных и информационных локаторов, полным ключом алгоритма шифрования хэш-значения.

Выбор неприводимого полинома $p(x)$ производится из числа Z всех неприводимых многочленов степени m и определяется числом сочетаний $C_Z^1 = Z$. Этот полином порождает конечное поле и кодовый вектор Лагранжа из n элементов (локаторов). Длина цифровой подписи задается t_j, $j = 1,2,...,S$ избыточными узлами, выбираемыми из n локаторов с учетом их перестановок. Возможные варианты выбора избыточных локаторов описываются выражением $t_j! \cdot C_n^{t_j}$, а информационных узлов — $(n - t_j)!$, $j = 1,2,...,S$.

Тогда возможные способы хэширования блока сообщения от конкретной длины N_{m_j} бит до длины N_{k_j} бит находятся из выражения $Z_{h_j} = Z \cdot t_j! \cdot C_n^{t_j} \cdot (n - t_j)!$, где $C_n^{t_j} = \dfrac{n!}{t_j \cdot (n - t_j)!}$. После преобразования Z_{h_j} получим:

$$Z_h = Z \cdot n! \qquad (12)$$

В обозначении возможных способов хэширования отсутствует индекс «j», так как процедура хэширования, как видно из (12), характеризуется выбором конечного поля. Обратная величина (12) определяет криптостойкость процедуры хэширования:

$$p_h = 1/Z_h . \qquad (13)$$

Для зашифрования хэш-значения используется нетрадиционный алгоритм шифрования на базе непозиционных полиномиальных систем счисления [3, 4]. Надежность этого алгоритма при шифровании хэш-значения длиной N_{m_j} бит характеризуется всевозможными способами Z_{kr_j} получения полного секретного ключа. Каждой длине хэш-значения отвечает определенное значение криптостойкости шифрования $\rho_{kr_j} = 1/ Z_{kr_j}$. В таблице 1 приведены значения криптостойкости алгоритма шифрования, существенно возрастающей с увеличением длины сообщения.

Число возможных способов построения цифровой подписи длиной N_{k_j} для блока сообщения длины N_{m_j} и ее криптостойкость определяются следующими формулами соответственно (один вариант выбора длины ЭЦП — частный случай):

$$Z_{SL_j} = Z \cdot n! \cdot Z_{kr_j} = Z_h \cdot Z_{kr_j}, \quad p_{SL_j} = 1/Z_{SL_j} = p_h \cdot p_{kr_j} . \qquad (14)$$

Поскольку может быть построено S электронных цифровых подписей для одного кодового слова Лагранжа, получим с учетом (12)—(14) следующую формулу криптостойкости алгоритма формирования ЭЦП на базе кодов Лагранжа (несколько вариантов выбора длин ЭЦП — общий случай):

$$p_{SL} = \frac{1}{Zn! \sum\limits_{t_1,t_2,\ldots,t_S} Z_{kr_j}} . \qquad (15)$$

Суммирование в (15) распространено на всевозможные способы построения S вариантов цифровых подписей или на все выборы избыточных узлов из общего числа всех элементов кодового вектора Лагранжа.

Таблица 1. Криптостойкость нетрадиционного алгоритма шифрования

Длина сообщения N в битах	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Криптостойкость шифрования, ρ_{kr}	$5{,}0\cdot10^{-1}$	$2{,}5\cdot10^{-1}$	$3{,}1\cdot10^{-2}$	$7{,}8\cdot10^{-3}$	$2{,}0\cdot10^{-3}$	$3{,}8\cdot10^{-4}$	$9{,}3\cdot10^{-5}$	$2{,}0\cdot10^{-5}$	$4{,}5\cdot10^{-6}$	$9{,}1\cdot10^{-7}$	$2{,}1\cdot10^{-7}$	$4{,}8\cdot10^{-8}$	$1{,}0\cdot10^{-8}$	$2{,}4\cdot10^{-9}$	$4{,}8\cdot10^{-10}$	$1{,}1\cdot10^{-10}$

Рассмотрим некоторые примеры определения криптостойкости.

Пример 1. В приведенном выше примере для формирования ЭЦП были выбраны 3 избыточных узла из 8 элементов поля $GF(2^3)$. Можно построить еще одну подпись из 2 избыточных узлов. Пусть $t_1 = 3$, $N_{k_1} = 9$ бит, $t_2 = 2$, $N_{k_2} = 6$ бит, $N = 24$ бита, $S = 2$, $Z = 2$. Для каждого из двух частных случаев найдем значения криптостойкости по формуле (13) и для общего случая — по формуле (15). Частный случай. $\rho_h = 1/Z_h = 1/(2\cdot8!) \approx 1{,}2\cdot10^{-5}$, $\rho_{SL_1} = \rho_h \cdot \rho_{kr1} \approx 5{,}7\cdot10^{-11}$, $\rho_{SL_1} = \rho_h \cdot \rho_{kr2} \approx 4{,}7\cdot10^{-9}$. Общий случай. $p_{SL} = 1/[Z \cdot n!(1/p_{kr_1} + 1/p_{kr_{21}})] \approx 5{,}6\cdot10^{-11}$.

В государственном стандарте Республики Казахстан СТ РК 1073-2007 определены четыре уровня безопасности [6]. В соответствии с установленными в нем требованиями к средствам криптографической защиты информации первого, второго, третьего и четвертого уровней, длина ключа электронной цифровой подписи должна быть не менее 60, 100, 150 и 200 бит соответственно.

Пример 2. В поле $GF(2^3)$ определим криптостойкость алгоритма при построении ЭЦП длиной $N_{k_1} = 256$ бит ($n = 256$, $t_1 = 32$, $S = 1$, $Z = 30$). Для шифрования хэш-значения выбираем непозиционную полиномиальную систему счисления, в которой основаниями являются неприводимые многочлены 16-й степени над полем $GF(2)$ [4, 5]. Криптостойкость процедуры хэширования и алгоритма нетрадиционного шифрования равны: $\rho_h \approx 4 \cdot 10^{-509}$ и $\rho_{kr_1} \approx 5 \cdot 10^{-104}$. Тогда $\rho_{SL_1} \approx 10^{-648}$.

Результаты расчетов рассмотренных примеров показывают, что

- надежность алгоритма формирования ЭЦП на базе кодов Лагранжа можно качественно оценивать по криптостойкости ЭЦП наибольшей длины;
- с увеличением длины кодового слова надежность процедуры хэширования существенно влияет на криптостойкость ЭЦП. В таблице 2 приведены данные, иллюстрирующие нелинейный рост значений криптостойкости с повышением степени полеобразующего полинома;
- чем больше длина кодового вектора, тем выше криптостойкость ЭЦП и больше вариантов выбора цифровых подписей различной длины.

Таблица 2. Криптостойкость процедуры хэширования

Поле $GF(2^m)$	**n**	**N (бит)**	**Z**	p_h
3	8	24	2	10^{-5}
m = 4	16	64	3	10^{-14}
m = 5	32	160	6	10^{-37}
m = 6	64	256	9	10^{-90}
m = 7	128	896	18	10^{-217}
m = 8	256	2048	30	10^{-509}
m = 9	512	4608	56	10^{-1168}
Поле $GF(2^m)$	**n**	**N (бит)**	**Z**	p_h
3	8	24	2	10^{-5}
m = 4	16	64	3	10^{-14}
m = 5	32	160	6	10^{-37}
m = 6	64	256	9	10^{-90}
m = 7	128	896	18	10^{-217}
m = 8	256	2048	30	10^{-509}
m = 9	512	4608	56	10^{-1168}

СПИСОК ЛИТЕРАТУРЫ:

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. *Нысанбаев Р. К.* Криптографический метод на основе полиномиальных оснований // Вестник Мин-ва науки и высшего образования и Нац. акад. наук Республики Казахстан. 1999. № 5. С. 63–65.
3. *Бияшев Р. Г., Нысанбаева С. Е.* Исследование надежности корректирующей электронной цифровой подписи // Управление защитой информации. Мн.; М., 2007. Т. 11. № 4. С. 447–453.
4. *Бияшев Р. Г., Нысанбаева С. Е.* Моделирование генерации ключей в непозиционной полиномиальной системе счисления // Изв. ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность». Таганрог: Изд-во ТТИ ЮФУ, 2007. № 1. С.193–198.
5. *Амербаев В. М., Бияшев Р. Г., Нысанбаева С. Е.* Применение непозиционных систем счисления при криптографической защите информации. // Известия Национальной академии наук Республики Казахстан. Сер. физ.-мат. наук. 2005. № 3. С. 84–89.
6. СТ РК 1073-2007. Средства криптографической защиты информации / Общие технические требования. Введ. 2009. 01.01. Астана: 2009.