УДК 004.056.5

В. М. АМЕРБАЕВ, Р. Г. БИЯШЕВ, С. Е. НЫСАНБАЕВА

ПРИМЕНЕНИЕ ИНТЕРПОЛЯЦИОННОЙ ФОРМУЛЫ ЛАГРАНЖА В АЛГОРИТМЕ ФОРМИРОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ

Предлагается процедура формирования электронной цифровой подписи, разработанная на базе (n,k)-кодов Лагранжа. В этих кодах используется представление полиномов в виде интерполяционных формул Лагранжа в поле $GF(q)$.

В настоящее время криптографические методы и средства широко применяются не только для защиты государственных и военных интересов, но также частных лиц и коммерческих организаций. В связи с этим возникла необходимость иметь для электронных сообщений и документов подписи, эквивалентные используемым в бумажных документах. Такая электронная цифровая подпись (ЭЦП) для сообщения является идентификатором (числом), зависящим от самого сообщения и от некоторого секретного ключа. При этом предполагается, что ЭЦП должна быть легко проверяемой. Цифровая подпись позволяет решать следующие три задачи: 1) осуществлять аутентификацию (подлинность) источника сообщения, 2) устанавливать целостность сообщения, 3) обеспечивать невозможность отказа от факта подписи конкретного сообщения [1-3].

Для реализации схемы цифровой подписи необходимы два алгоритма: алгоритм формирования (вычисления) цифровой подписи и алгоритм ее проверки. В настоящее время применяются несколько принципиально различных подходов к созданию схем цифровой подписи. Их можно разделить на три группы: 1) схемы на основе систем шифрования с открытыми ключами; 2) схемы со специально разработанными алгоритмами вычисления и проверки подписи; 3) схемы на основе симметричных систем шифрования. Предлагаемая схема ЭЦП относится ко второй группе.

К известным системам ЭЦП относятся алгоритмы RSA, Эль Гамаля и DSA. Последний алгоритм предложен в США в 1991 году для использования в качестве стандарта цифровой подписи DSS (Digital Signature Standard). Российский стандарт ГОСТ Р 34.10-94 вступил в действие в 1995 году. Эти алгоритмы и стандарты разработаны на базе криптосистем с открытыми ключами. В государственном стандарте Республики Казахстан СТ РК 1073-2007 определены четыре уровня безопасности [4]. В соответствии с установленными в нем требованиями к средствам крип-тографической защиты информации первого, второго, третьего и четвертого уровня длина ключа электронной цифровой подписи должна быть не менее 60, 100, 150 и 200 бит соответственно.

Предложенная система электронной цифровой подписи (ЭЦП) создана на основе подхода, который был предложен при построении кодов с параллельной структурой, обнаруживающих и исправляющих ошибки [5]. Этот подход базируется на непозиционной мультипликативной композиции векторов и использует представление полиномов в виде интерполяционных формул Лагранжа в конечном поле $GF(q)$. В связи с этим указанные самокорректирующиеся коды названы (n,k)-кодами Лагранжа. В коде Лагранжа n символов составляют его длину, а любые k символов могут быть выбраны в качестве информационных. При этом процедура кодирования не искажает выбранный набор информационных символов. Код Лагранжа над полем $GF(q)$ имеет максимальную длину $n = q$, где $q = p$, m – степень неприводимого многочлена, порождающего конечное поле $GF(q)$. Таким образом, элементы поля $GF(q)$ представлены p-ичным кодом.

В поле $GF(q)$ рассматривается множество элементов I, расположенных в упорядоченном виде, пронумерованных целыми числами из интервала $[0,q)$ $I = \{\omega_0 < \omega_1 < ... < \omega_{q-1}\}$ и названных локаторами. Каждый локатор характеризуется порядком расположения «i» и величиной ω_i. Вводится также множество I_n, состоящее из n локаторов, $I_n \subseteq I$.

Пусть в поле $GF(q)$ задана некоторая упорядоченная последовательность элементов $(\alpha_1, \alpha_2, ..., \alpha_n)$. Требуется по этой последовательности элементов построить полином $f(x)$ следующим образом: для каждого локатора $\omega_i \in I_n$ выражение $f(\omega_i) = \alpha_i$ имеет единственное решение в классе полиномов степени не выше n-1 (при $n \le q-1$). Искомый полином задается интерполяционной формулой Лагранжа:

$$f(x) = \sum_{i=1}^{n} f(\omega_i) L_n^{(i)}(x), \qquad (1)$$

где

$$L_n^{(i)}(x) = \frac{(x-\omega_1)...(x-\omega_{i-1})(x-\omega_{i+1})...(x-\omega_n)}{(\omega_i-\omega_1)...(\omega_i-\omega_{i-1})(\omega_i-\omega_{i+1})(\omega_i-\omega_n)},$$

$$1 \le i \le n. \qquad (2)$$

Многочлены (2) называются фундаментальными полиномами Лагранжа. Вводятся следующие обозначения:

$$P_{I_n}(x) = \prod_{\omega_S \in I_n} (x-\omega_s), \quad P_{I_n}^{(s)}(x) = \frac{P_{I_n}(x)}{(x-\omega_s)},$$

$$P_{I_n}^{(s)}(\omega_s) =$$

$$= (\omega_s-\omega_1)...(\omega_s-\omega_{s-1})(\omega_s-\omega_{s+1})...(\omega_s-\omega_n),$$

тогда s-й фундаментальный многочлен Лагранжа запишется в виде $L_{I_n}^{(s)}(x) = \dfrac{P_{I_n}^{(s)}(x)}{P_{I_n}^{(s)}(\omega_s)}$. Для однозначного восстановления произвольного полинома $f(x)$ по его значениям в локаторах (узлах), взятых из поля $GF(q)$, необходимо рассматривать множество вычетов полинома $f(x)$ по модулю $P_{I_n}(x)$, которые представляются интерполяционными полиномами Лагранжа (1) [5]:

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

где

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

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 $GF(q)$: $g(x) \to (g(\omega_1), ..., g(\omega_n))$, и это отображение является биективным. Совокупность всех таких кодовых слов названа кодом Лагранжа. Опишем реализацию основных операций на языке кодовых векторов Лагранжа. Пусть

$g(x) \leftrightarrow (g_1, g_2, ..., g_n)$, $f(x) \leftrightarrow (f_1, f_2, ..., f_n)$,

$g_i \in F_q$, $f_i \in F_q$, $i = \overline{1,n}$,

тогда

$$< g(x) \pm f(x)|_{P_{I_n}(x)} =$$

$$= g(x) \pm f(x) \leftrightarrow (g_1 \pm f_1, ..., g_n \pm f_n) \qquad (5)$$

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

$$\alpha g(x) \leftrightarrow \alpha(g_1,...,g_2) = (\alpha g_1,...,\alpha g_n), \quad (6)$$

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

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

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

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. Вводятся дополнительные обозначения. I_q – множество всех элементов (локаторов) поля $GF(q)$, расположенных в «возрастающем» порядке (например, степени полиномов) $x_1 < x_2 < ... < x_q$. I_n – подмножество множества I_q, состоящее из n элементов, $P_{I_n}(x) = \prod_{x_i \in I_n}(x - x_i)$.

Аддитивная и мультипликативная композиции над кодовыми векторами Лагранжа

$$\bar{a} = (\alpha_1,\alpha_2,...,\alpha_n) \leftrightarrow a(x) \in <\bullet|_{P_{I_n}},$$

$$\bar{b} = (\beta_1,\beta_2,...,\beta_n) \leftrightarrow b(x) \in <\bullet|_{P_{I_n}}$$

выполняются по правилам:

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

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

Рассматривается код Лагранжа $(\alpha_1,\alpha_2,...,\alpha_n)$, в котором $\alpha_i \in GF(q)$, $i = \overline{1,n}$. Порождаемая им алгебра задается системой полиномов

$$<\bullet|_{P_{I_n}} = \{a(x) \mid a(x) = \sum_{i=1}^{n} \tilde{\alpha}_i P_{I_n}^{(i)}(x)\},$$

где $P_{I_n}^{(i)}(x) = \dfrac{P_{I_n}(x)}{(x - x_i)}$, $\tilde{\alpha}_i = \alpha_i[P_{I_n}^{(i)}(x_i)]^{-1}$.

Предполагается, что первые k символов $\alpha_1,\alpha_2,...,\alpha_k$ кодового слова (вектора) длины n ($k<n$) являются информационными. Избыточные символы $\alpha_{k+1},\alpha_{k+2},...,\alpha_{k+s}$ определяются посредством операции расширения

$$\alpha_{k+s} = \sum_{i=1}^{k} \tilde{\alpha}_i P_{I_k}^{(i)}(x_{k+s}), \quad s = \overline{1,\ n-k},$$

$$I_k = \{x_1,...,x_k\}. \quad (9)$$

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

В предлагаемом алгоритме формирования электронной цифровой подписи используется неприводимый многочлен степени m над полем $GF(2)$, который порождает конечное поле $GF(2^m)$. Элементы (символы) поля $GF(2^m)$ имеют одну и ту же длину m бит и представляются двоичным кодом Лагранжа, имеющим максимальную длину $N = 2^m$ бит.

Алгоритм формирования цифровой подписи для электронного сообщения включает три этапа:

1) представление электронного сообщения в виде кодовых векторов Лагранжа;

2) хэширование сообщения с помощью процедуры введения избыточных символов;

3) вычисление ЭЦП путем шифрования полученного хэш-значения.

На первом этапе подписываемое сообщение разбивается на блоки длиной N_m бит. Каждый блок интерпретируются как некоторый многочлен $F(x)$:

$$F(x) = (\alpha_1(x),\alpha_2(x),...,\alpha_k(x)), \quad (10)$$

где $\alpha_i(x)$, $i = \overline{1,k}$ значения полинома $F(x)$ в узлах x_i, $i = \overline{1,k}$, поля $GF(2^m)$. $\alpha_i(x)$, $i = \overline{1,k}$ являются полиномами над полем $GF(2)$, а также информационными символами в кодовых векторах Лагранжа из n символов.

В представлении (10) полагается, что первые l_1 бит – это коэффициенты многочлена (символа) $\alpha_1(x)$, следующие l_2 бит являются коэффициентами полинома $\alpha_2(x)$, и так далее, последние двоичные разряды l_k задают многочлен $\alpha_k(x)$. Напомним, что значения $l_i = m$, $i = \overline{1,k}$.

На втором этапе производится хэширование (сжатие) сообщения от длины N_m до длины N_k.

Для этого вводятся избыточные символы $\alpha_{k+1}(x), \alpha_{k+2}(x), ..., \alpha_n(x)$, которые определяются в соответствии с операцией расширения (9):

$$\alpha_{k+t} = \sum_{i=1}^{k} \tilde{\alpha}_i P_{I_k}^{(i)}(x_{k+t}),$$

$$t = \overline{1,\ n-k},\quad I_k = \{x_1, ..., x_k\}.$$

Количество избыточных элементов задается числом $t = n - k$. Длина N_k хэш-значения и электронной цифровой подписи определяется общей длиной избыточных символов: $N_k = m(n-k)$.

Таким образом, в результате выполнения первых двух этапов сформированы кодовые слова Лагранжа, размер которых задается блоком электронных сообщений из N_m бит и вычисленным хэш-значением из N_k бит: $N = N_m + N_k$.

Третий этап – вычисление ЭЦП. Для зашифрования полученного хэш-значения используется один из следующих нетрадиционных алгоритмов шифрования, разработанных на базе:

– непозиционных полиномиальных систем счисления [6, 7];

– (n,k)-кодов Лагранжа [8].

При получении сообщения адресат должен проверить электронную цифровую подпись, то есть удостовериться в ее достоверности. Для этого он определяет два хэш-значения. Одно хэш-значение вычисляется от полученного им сообщения, а другое находится в результате расшифрования ЭЦП.

Электронная цифровая подпись считается подлинной, если совпадают оба хэш-значения, найденные адресатом.

ЛИТЕРАТУРА

1. *Столлингс В.* Криптография и защита сетей: принципы и практика. 2-е изд. М., 2001. 672 с.

2. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии: учебное пособие для вузов. 2-е изд. испр. и допол. М., 2002. 480 с.

3. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тесты на языке Си. М., 2003. 816 с.

4. СТ РК 1073-2007. Средства криптографической защиты информации / Общие технические требования. Введ. 2009. 01.01. Астана, 2009.

5. *Амербаев В. М., Бияшев Р.Г.* Интерполяция и коды, исправляющие ошибки // Теория кодирования и информационное моделирование. Алма-Ата, 1973. С. 51-64.

6. *Нысанбаев Р.К.* Криптографический метод на основе полиномиальных оснований // Вестник Мин-ва науки и высшего образования и НАН РК. 1999. № 5. С. 63-65.

7. *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.

8. *Нысанбаев Р.К.* Разработка нетрадиционного криптографического алгоритма с возможностью обнаружения ошибок в криптограммах на основе (n,k)-кода Лагранжа // Вестник КазГУ. Сер. Математика, механика, информатика. 1999. № 3(17). С. 182-186.

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 бірмәнділігі көрсетілген. Сандық қолтаңба құрайтын алгоритмнің криптотұрақтылық формуласы анықталды.

Summary

Procedure of formation of the electronic digital signature developed on base of Lagranzh (n, k)-codes is offered. In these codes representation of polynoms in a kind of interpolational Lagranzh formula in the field $GF(q)$ is used.

ДГП «Институт проблем информатики и правления» РГП «ИМИМ» МОН РК, г. Алматы

Поступила 10.06.10 г.