

ПРИМЕНЕНИЕ ПОЛИНОМИАЛЬНОЙ СИСТЕМЫ КЛАССОВ ВЫЧЕТОВ ДЛЯ ПОВЫШЕНИЯ СКОРОСТИ ФУНКЦИОНИРОВАНИЯ СПЕЦПРОЦЕССОРА АДАПТИВНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Калмыков И.А., Хайватов А.Б., Тимошенко Л.И., Гахов В.Р.

Ставропольский военный институт связи Ракетных войск,
Северо-Кавказский государственный технический университет

г. Ставрополь, Россия

kia762@yandex.ru , xab_x@mail.ru

Проблема исследований: В ближайшем будущем роль компьютерных систем будет всемерно усиливаться. При этом возникают новые задачи по разработке и созданию адаптивных средств защиты информации (АСЗИ) в вычислительных сетях от несанкционированного доступа (НСД).

Решение проблемы:

В последние годы наблюдается тенденция все более всестороннего применения алгебраических систем, определяемых в расширенных полях Галуа, при построении адаптивных средств защиты информации. Это обуславливает возможность использования следующих криптографических преобразований:

- сложение элементов по модулю порождающего полинома $g(z)$;
- умножение элементов поля по модулю порождающего полинома $g(z)$;
- возведение элементов в степень по модулю $g(z)$.

Применение полиномиальной системы классов вычетов (ПСКВ) позволяет повысить эффективность данных систем с точки зрения обеспечения высокой скорости работы криптографического устройства.

Если в качестве оснований алгебраической системы выбрать минимальные многочлены $p_i(z)$ поля $GF(p^n)$, то полином $A(z)$, удовлетворяющий условию $A(z) \in P_{пол}$, где $P_{пол} = \prod_{i=1}^n p_i(z) = z^{p^n-1} - 1$, представляется в виде вектора

$$A(z) = (a_1(z), a_2(z), \dots, a_n(z)), \quad (1)$$

где $a_i(z) = \text{rest}(A(z)/p_i(z))$, $i = 1, 2, \dots, n$.

Для двух полиномов, принадлежащих полному диапазону $A(z) = (a_1(z), a_2(z), \dots, a_n(z))$ и $B(z) = (b_1(z), b_2(z), \dots, b_n(z))$, справедливо [1,2]:

$$\begin{aligned} |A(z) + B(z)|_{p(z)}^+ &= (|a_1(z) + b_1(z)|_{p_1(z)}^+, \dots, |a_n(z) + b_n(z)|_{p_n(z)}^+) = \\ &= \left(I_0^1 \oplus g_0^1, \sum_i (I_{m_2-i}^2 \oplus g_{m_2-i}^2) z^i, \sum_j (I_{m_2-j}^3 \oplus g_{m_2-j}^3) z^j, \dots, \sum_w (I_{m_2-w}^n \oplus g_{m_2-w}^n) z^w \right), \end{aligned} \quad (2)$$

$$\begin{aligned} |A(z) - B(z)|_{p(z)}^+ &= (|a_1(z) - b_1(z)|_{p_1(z)}^+, \dots, |a_n(z) - b_n(z)|_{p_n(z)}^+) = \\ &= \left(I_0^1 \circ g_0^1, \sum_i (I_{m_2-i}^2 \circ g_{m_2-i}^2) z^i, \sum_j (I_{m_2-j}^3 \circ g_{m_2-j}^3) z^j, \dots, \sum_w (I_{m_2-w}^n \circ g_{m_2-w}^n) z^w \right), \end{aligned} \quad (3)$$

$$\begin{aligned} |A(z) \cdot B(z)|_{p(z)}^+ &= (|a_1(z) \cdot b_1(z)|_{p_1(z)}^+, \dots, |a_n(z) \cdot b_n(z)|_{p_n(z)}^+) = \\ &= (I_0^1 g_0^1, \sum_{l=0}^{2m_2-2} q_{2m_2-2-l}^2 z^{2m_2-2-l}, \mathbf{K}; \sum_{j=0}^{2m_n-2} q_{2m_n-2-j}^n z^{2m_n-2-j}), \end{aligned} \quad (4)$$

где $q_s^i = \sum_{k=0}^s I_k^i g_{s-k}^i$ - линейная свертка; $s = 0, \dots, 2m_i - 2$, $i = 0, \dots, n$.

Следовательно, ПСКВ может быть использована при реализации криптографических преобразований.

Пусть для выработки М-последовательности задан порождающий полином $L(z) = z^{255} + z^{127} + z^{63} + z^{31} + z^{15} + z^3 + 1$, а для реализации криптографических преобразований в поле $GF(2^7)$ - порождающий полином $g(z) = z^7 + z + 1$. Тогда для одновременного обеспечения информационной скрытности и высокой скорости работы спецпроцессора АСЗИ будут использоваться 7-разрядные элементы поля $GF(2^7)$. В этом случае сформированная последовательность символов в виде двоичных векторов длиной 7 бит является псевдослучайной последовательностью (ПСП) элементов конечного поля $GF(2^7)$. Так как сформированная последовательность является последовательностью элементов мультипликативной группы расширенного поля Галуа $GF(2^7)$, то к ним возможно применение криптографических преобразований.

Пусть криптографические преобразования определяются выражением

$$s(z) g_1(z) + g_2(z) \equiv f(z) \text{ mod } g(z). \quad (2)$$

В таблице представлено состояние первых 15 ячеек памяти генератора двоичной ПСП, задаваемой порождающим полиномом $L(z) = z^{255} + z^{127} + z^{63} + z^{31} + z^{15} + z^3 + 1$.

Таблица 1

№	Ячейки памяти генератора М-последовательности														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	0	0	1	1	0	0	1	1	0	0	1	1	0
2	1	1	0	0	0	1	1	0	0	1	1	0	0	1	1

Так как для реализации (2) необходимо две ПСП элементов поля $GF(2^7)$, то значение первой ПСП снимаем с первой по седьмую ячеек, согласно выражения

$$g_1(z) = (a_7x^6 + a_6x^5 + a_5x^4 + a_4x^3 + a_3x^2 + a_2x + a_1x^0) \bmod g(z), \quad (3)$$

а значение второй ПСП с восьмой по четырнадцатую ячеек генератора М-последовательности

$$g_2(z) = (a_{14}x^6 + a_{13}x^5 + a_{12}x^4 + a_{11}x^3 + a_{10}x^2 + a_9x + a_8x^0) \bmod g(z). \quad (4)$$

Тогда имеем следующие элементы поля $GF(2^7)$ на первых двух тактах работы генератора:

$$\begin{aligned} 1 \text{ такт} \quad g_1^1(z) &= 0110001 = z^5 + z^4 + 1; & g_2^1(z) &= 1100110 = z^6 + z^5 + z^2 + z; \\ 2 \text{ такт} \quad g_1^2(z) &= 1100011 = z^6 + z^5 + z + 1; & g_2^2(z) &= 1001100 = z^6 + z^3 + z^2; \end{aligned}$$

Пусть в качестве открытого текста используется 7-битовая последовательность

$$s(z) = 0000011 = z + 1.$$

Проведем преобразования согласно (2). Получаем

$$\begin{aligned} f(z) &\equiv (s(z)g_1(z) + g_2(z)) \bmod g(z) = \\ &= ((z + 1)(z^5 + z^4 + 1) + z^6 + z^5 + z^2 + z) \bmod z^7 + z + 1 = \\ &= z^5 + z^4 + z^2 + 1 \end{aligned}$$

В качестве ПСКВ выберем алгебраическую систему, определяемую основаниями: $p_1(z) = z + 1$; $p_2(z) = z^2 + z + 1$; $p_3(z) = z^4 + z^3 + z^2 + z + 1$;

$p_4(z) = z^4 + z^3 + 1$, $p_5(z) = z^4 + z + 1$. Тогда рабочий диапазон составляет

$$P_{\text{раб}}(z) = \prod_{i=1}^5 p_i(z) = z^{15} + 1. \text{ Представим исходные последовательности в коде}$$

ПСКВ и проведем соответствующие преобразования

Операнды	$\alpha_1(z)$	$\alpha_2(z)$	$\alpha_3(z)$	$\alpha_4(z)$	$\alpha_5(z)$
$s(z) = z + 1$	0	$z + 1$	$z + 1$	$z + 1$	$z + 1$
$g_1^1(z) = z^5 + z^4 + 1$	x 1	0	$z^3 + z^2 + z + 1$	$z + 1$	z^2

$s(z)g_1(z) \bmod g(z)$	0	0	z^3+z^2+z	z^2+1	z^3+z^2
$g_2^1(z)=z^6+z^5+z^2+z$	$+$	0	$z+1$	z^2+1	z
$s(z)g_1(z) + g_2(z) \bmod g(z)$	0	$z+1$	z^3+z+1	z^2+z+1	0

Таким образом, имеем

$$f(z) = z^5 + z^4 + z^2 + 1 = (0, z+1, z^3+z+1, z^2+z+1, 0)$$

Следовательно, применение ПСКВ позволяет обеспечить следующие преимущества [1,3]:

- операции выполняются над остатками независимо по каждому из модулей $p_i(z)$, что позволяет повысить быстродействие вычислительной системы;
- операции проводятся над малоразрядными операндами, что позволяет не только повысить быстродействие системы, но и сократить аппаратные затраты.

Литература

1. Калмыков И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов/ Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2005. - 276 с.
2. Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Бережной В.В. Математическая модель нейронных сетей для исследования ортогональных преобразований в расширенных полях Галуа/Нейрокомпьютеры: разработка, применение. №6, 2003. с.61-68с.
3. Элементы применения компьютерной математики и нейроинформатики /Н.И. Червяков, И.А. Калмыков И.А., В.А. Галкина, Ю.О. Щелкунова, А.А. Шилов; Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2003. – 216с.