ПРИМЕНЕНИЕ КОЭФФИЦИЕНТОВ ОБОБЩЕННОЙ ПОЛИАДИЧЕСКОЙ СИСТЕМЫ В АДАПТИВНЫХ СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ

Калмыков И.А., Березкина М.В., Макарова А.В., Науменко Д.О.
Северо - Кавказский федеральный университет,
Институт информационных технологий и телекоммуникаций,
г.Ставрополь, Россия
alyonchikMav@yandex.ru

В данной работе рассмотрен алгоритм обратного преобразования для адаптивных средств защиты информации, функционирующих в расширенных полях Галуа $GF(p^v)$.

1. Введение

Развитие систем передачи и обработки информации, широкое использование вычислительных систем стало причиной всестороннего развития криптографических методов защиты информации (КМЗИ) от несанкционированного доступа (НДС). В настоящее время растет число конечных алгебраических систем, к которым применяются КМЗИ [1]. Использование полиномиальной системы остаточных классов (ПСОК), определяемой в полях Галуа является одним из наиболее эффективных методов КМЗИ от НСД. В этом случае задача криптозащиты информации от НСД состоит в необходимости выбрать из полного множества возможных некоторую ограниченную совокупность взаимнопростых полиномов, определяемых в полях Галуа и полученная совокупность не должна быть прозрачна для концептуального распознавания, проводимого при криптоанализе.

Самым приемлемым классом для построения алгоритма КМЗИ с использованием ПСОК являются неприводимые полиномы полей Галуа,

количество которых стремительно растет с ростом порядка и с увеличением характеристики поля $g > 2$ [1].

2. Постановка задачи исследования

Приведем процедуру зашифрования сообщения с использованием ПСОК. Соответствующее сообщение будет иметь вид двоичного кода, если отображение семантического знака представить в символах кодировки. Входная последовательность двоичных символов бьется на блоки L длиной по M разрядов,на следующем шаге определяется набор неприводимых

полиномов $p_1(z)$, $p_2(z),\ldots, p_n(z)$, удовлетворяющих условию:

$$\deg P(z) \geq M \ , \qquad (1)$$

где $P(z) = \prod_{i=1}^{n} p_i(z)$ полный диапазон ПСОК.

При этом каждому двоичному блоку L ставится в соответствие $L(z)$ – полиномиальная форма, а также вектор

$$L(z) = (\alpha_1(z), \alpha_2(z),\ldots,\alpha_n(z)), \qquad (2)$$

где $\alpha_i(z) \equiv L(z) \bmod p_i(z)$, $i = 1,2,\ldots,n$.

Двоичная ключевая последовательность K длиной M разрядов аналогичным образом представляется в полиномиальной форме $K(z)$, приводится к виду с использованием набора неприводимых полиномов

$p_1(z)$, $p_2(z),\ldots, p_n(z)$

$$K(z) = (k_1(z), k_2(z),..., k_n(z)), \quad (3)$$

где $k_i(z) \equiv K(z) \bmod p_i(z)$, $i = 1,2,...,n$.

Затем к значениям $L(z)$ и $K(z)$ применяется криптографическое преобразование

$$F(z) = E(L(z),K(z)), \quad (4)$$

которое определено в ПСОК и и ему обратное $D(z)$ такое, что

$$D(F(z),K(z)) = D(E(L(z),K(z)),K(z)) = L(z). \quad (5)$$

Зашифрованное сообщение, полученное согласно (4), передается на приемную сторону, дешифруется, согласно выражению (5). Для восстановления $L(z)$ на основе полученных остатков $(\alpha_1(z), \alpha_2(z),...,\alpha_n(z))$ следует применить коэффициенты обобщенной полиадической системы (ОПС) [3-4]

$$L(z) = a(z) + a_2(z)q_1(z) + ... + a_n(z)q_{n-1}(z), \quad (6)$$

где $a_i(z)$ – коэффициенты ОПС; $i = 1,2,...,n$,

$$q_1(z) = \prod_{j=1}^{l} p_j(z);\ l=1, \ldots, n-1.$$

В работе [5] представлено устройство, которое осуществляет вычисление коэффициентов ОПС на основе значений $(\alpha_1(z), \alpha_2(z),...,\alpha_n(z))$,

но реализация выражения (6) требует значительных аппаратурных затрат, потому что увеличение числа комбинаций неприводимых полиномов из

множества возможных оснований, удовлетворяющих условию (1), приводит к резкому возрастанию объема памяти, необходимой для хранения значений ортогональных базисов.

Следовательно, очевидна актуальность разработки высокоэффективного метода обратного преобразования из модулярного кода в позиционный на основе коэффициентов ОПС, характеризующийся минимальными затратами памяти.

Приведем процедуру вычисления коэффициентов ОПС с использованием китайской теоремы об остатках. Пусть задана ПСКВ с основаниями

$p_1(z)$, $p_2(z),\ldots, p_n(z)$, удовлетворяющих условию

$$\deg p_1(z) \le \deg p_2(z) \le ... \le \deg p_n(z).$$

Согласно китайской теореме об остатках

$$A(z) = \sum_{i=1}^{n} \alpha_i(z) B_i(z) \bmod P_{полн}(z) \quad (7)$$

где $B_i(z) = m_i(z)P(z)/p_i(z) \equiv 1 \bmod p_i(z)$ ортогональный базис ПСОК.

Представим ортогональные базисы в ОПС.

$$B_1(z) = \left[a_1^1(z), a_2^1(z),..., a_n^1(z)\right];$$

$$B_2(z) = \left[0, a_2^2(z),..., a_n^2(z)\right];$$

$$\begin{matrix} . \\ . \\ . \\ B_n(z)=[0,0,...,a_n^n(z)] \end{matrix} \quad (8)$$

Для этого воспользуемся алгоритмом, представленным в работе [1]. Вычислим значения коэффициентов ОПС для ортогонального базиса $B_1(z)$. Очевидно, что $B_1(z) \equiv \alpha_1(z) \bmod p_1(z)$. Значит $\alpha_1^1(z)=1$.

Разность исходного значения $B_1(z)$ и значения остатка $\alpha_1(z)$ будет без остатка делиться на $p_1(z)$, то есть

$$B_1^1(z)=\frac{B_1(z)-\alpha_1(z)}{p_1(z)} < p_2(z)p_3(z)...p_n(z)$$

значит, оно определяется своими последними цифрами. Тогда

$$B_1^1(z)=\frac{(1,0,...,0)-(1,1,...,1)}{p_1(z)}=(\alpha_2^1(z),...,\alpha_n^1(z))=(p_1^{-1}(z) \bmod p_2(z),..., p_1^{-1}(z) \bmod p_n(z))$$

где $p_1^{-1}(z)=1/\ p_1(z) \bmod p_j(z)=m_j^1(z)$ обратная величина $p_1(z)$, по модулю $p_j(z)$,

$j = 2,...,n$.

Последнее равенство можно записать как

$$B_1^1(z)=(m_2^1(z),m_3^1(z),...m_n^1(z)). \quad (9)$$

Следовательно, вторая цифра $a_2^1(z)=m_2^1(z)$. Аналогично определяем значение

$$B_1^2(z)=\frac{B_1^1(z)-m_2^1(z)}{p_2(z)}=(\alpha_3^2(z),...,\alpha_n^2(z))=\left(\left|\frac{m_3^1(z)-m_2^1(z)}{p_2(z)}\right|_{p_3}^{+}...\left|\frac{m_n^1(z)-m_2^1(z)}{p_2(z)}\right|_{p_n}^{+}\right) \quad (10)$$

Преобразуем выражение (10) к виду

$$B_1^2(z)=\left(\left|m_3^1(z)-m_2^1(z))m_3^2(z)\right|_{p_3(z)}^{+}...\left|m_n^1(z)-m_2^1(z))m_n^2(z)\right|_{p_n(z)}^{+}\right) \quad (11)$$

Значит, третий коэффициент ОПС базиса B_1 (z) равен

$$a_3^1(z)=\left|(m_3^1(z)-m_2^1(z))m_3^1(z)-m_2^1(z)m_3^2(z)\right|_{p_3(z)}^{+}.$$

Значение $a_1^2(z)=m_2^1(z)$. Тогда

$$a_3^1(z)=\left|(m_3^1(z)-a_2^1(z))(m_3^1(z)-a_2^1(z))m_3^2(z)\right|_{p_3(z)}^{+}. \quad (12)$$

Для *j*-го коэффициента ОПС базиса будет

$$B_1^{j-1}(z)=\frac{B_1^{j-2}(z)-a_j^1(z)}{p_j(z)}=(\alpha_j^{j-1}(z),...,\alpha_n^{j-1}(z)).$$

$$a_j^1(z)=\alpha_j^{j-1}(z)=((((m_j^1(z)+a_2^1(z))m_j^2(z)+...+a_j^{j-1}(z))m_j^{j-1}(z)) \bmod p_j(z)).$$

Для *n*-го коэффициента ОПС базиса B_1 (z)

$$B_1^{n-1}(z)=\frac{B_1^{n-2}(z)-a_j^{n-1}(z)}{p_j(z)}=\alpha_n^{n-1}(z).$$

$$a_n^1(z)=\alpha_n^{n-1}(z)=((((m_n^1(z)+a_2^1(z))m_n^2(z)+...+a_n^{n-1}(z))m_n^{n-1}(z)) \bmod p_n(z)).$$

Таким образом, осуществлен перевод первого ортогонального базиса $B_1(z)$ в смешанную систему оснований. Рассмотрим процедуру перевода второго ортогонального базиса $B2$ (z) в ОПС. Для этого необходимо воспользоваться приведенным выше алгоритмом рассмотренным выше алгоритмом. Так как

$$\mathrm{B}_2\ (\mathrm{z}) = (0,1,0...0),\ \text{то}\ a_1^2(z) = \alpha_1^1(z) = 0\,.$$

Определим значение второго коэффициента ОПС.

$$B_2^1(z) = \frac{(0,1...0) - (0,0...0)}{p_i(z)} = (\alpha_2^2(z),0...0) = \left(\left/ p_1(z) \bmod p_2(z),0...0\right.\right).$$

Преобразуя последнее равенство, получаем

$$B_2^1(z) = (m_2^1(z),0...0).\ \text{Тогда}\ a_2^2(z) = m_2^1(z).$$

Определим величину третьего коэффициента ОПС для ортогонального базиса $B_2(z)$.

$$B_2^2(z) = \frac{B_2^1(z) - a_2^2(z)}{p_2(z)} = (\alpha_3^2(z),...,\alpha_n^2(z)) = \left((m_2^1(z)m_3^2(z) \bmod p_3(z)...(m_2^1(z)m_n^2(z)) \bmod p_n(z)\right) \quad (13)$$

тогда $a_3^2(z) = \alpha_3^2(z) = \left((m_2^1(z)m_3^2(z) \bmod p_3(z) = (a_2^2(z)m_3^2(z))\right) \bmod p_3(z)$ Используя представленный выше алгоритм, получаем величину j-го коэффициента ОПС.

$$B_2^{j-1}(z) = \frac{B_2^{j-2}(z) - a_j^2(z)}{p_j(z)} = (\alpha_j^{j-1}(z),...,\alpha_n^{j-1}(z)).$$

$$a_j^2(z) = \alpha_j^{j-1}(z) = \left(\left(\left(\left(a_2^2(z) + m_j^2(z)\right)m_j^2(z) + ... + a_{j-1}^2(z)\right)m_j^{j-1}(z)\right) \bmod p_j(z)\right).$$

Для n-го коэффициента второго ортогонального базиса будет

$$B_1^{n-1}(z) = \frac{B_2^{n-2}(z) - a_{n-1}^2(z)}{p_j(z)} = \alpha_n^{n-1}(z).$$

$$a_n^2(z) = \alpha_j^{j-1}(z) = \left(\left(\left(\left(a_2^2(z)m_n^2(z) + a_3^2(z)\right)m_n^3(z) + ... + a_{n-1}^2(z)\right)m_n^{n-1}(z)\right) \bmod p_n(z)\right).$$

Тогда в виде коэффициентов ОПС второй ортогональный базис будет:

$$B_2(z) = [0, a_2^2(z)...a_n^2(z)].$$

Обобщим рассмотренный алгоритм для представления n-го ортогонального базиса, который представляется как $B_n(z) = (0,0,0,...1)$. Тогда

$$a_n^n(z) = 0; a_n^n(z) = \prod_{j=1}^{n-1} m_n^j(z) \bmod p_n(z), \quad (14)$$

где l = 1...n-1

Следовательно

$$B_n(z) = \left[0...a_n^n(z) = \prod_{j=1}^{n-1} m_n^j(z) \bmod p_n(z)\right]. \quad (15)$$

Если положить, что $a_1^1(z) = m_1^0(z) = 1$.то значения коэффициентов ОПС для i-го ортогонального базиса ПСКВ определяется выражением

$$a_n^2(z)= \begin{cases} 0 & j<1 \\ \prod_{l=1}^{i-1} m_j^l(z) \bmod p_j(z), & j=1 \\ \left(\left(a_i^i m_j^i(z)+a_{i+1}^i m_j^{i+1}(z)+\ldots+a_{j-1}^i\right)m_j^{j-1}(z)\right)\bmod p_j(z). & j>1 \end{cases} \quad (16)$$

Анализ выражения (16) показывает, что данная процедура описывается формулой Горнера и может быть успешна реализована на основе применения параллельно-конвейерной организации вычислений. Можно также отметить, что данная реализация носит последовательный итерационный характер и производится по правилам модулярной арифметики, когда значения последующих коэффициентов определяются величинами предыдущих коэффициентов.

Следовательно, очевидно, что величина коэффициентов ОПС определяется произведением величин обратных основаниям ПСОК $p_i(z)$ по

модулю $p_i(z)$. Значит, для реализации обратного преобразования на основе коэффициентов ОПС необходимо хранить не значения коэффициентов для всех возможных комбинаций неприводимых полиномов, а только величины $m_j^i(z)=p_i(z)^{-1} \bmod p_j(z)$, что позволяет в несколько раз сократить аппаратурные затраты.

Литература

1. Коблиц Н. Курс теории чисел в криптографии. Пер. с англ. М.: ТВП, 2001. – 254 с.

2. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003. – 328 с.

3. 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.

4. Червяков Н. И., Калмыков И. А., Галкина В. А., Щелкунова Ю. О., Шилов А. А. Элементы компьютерной математики и нейроноинфроматики. Под ред. Н. И. Червякова. М.:Физматлит, 2003. – 216 с.

5. Калмыков И. А., Лободин М. В., Алексишин Е. В., Щелкунова Ю. О. Нейронная сеть для вычисления коэффициентов обобщенной

полиадической системы, представленных в расширенных полях Галуа GF(2v) // Патент РФ № 2258956, бюл. № 23 от 20.08.2005.