УДК 004.056+621.3.019.3

Г.Н. Гулак

МЕТОД ПОСТРОЕНИЯ ПРИМИТИВНЫХ ПОЛИНОМОВ ДЛЯ КРИПТОГРАФИЧЕСКИХ ПОДСИСТЕМ ГАРАНТОСПОСОБНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Ключевые слова: подсистема криптографической защиты, примитивный полином, неприводимый полином, минимальный полином элемента, примитивный элемент, конечное поле, фактор-кольцо, критерий Рабина.

Введение

В ходе проектирования различных компьютерных сетей и радиотехнических систем широко используются примитивные полиномы над полем порядка 2^k, где $k \geq 2$. В частности, такие полиномы применяются при построении подсистем криптографической защиты для реализации элементов криптографических схем, включая генераторы псевдослучайных чисел, модули гарантированного периода преобразования, блоки (подстановки) замены и т.д. [1, 2]. Таким образом, возникает задача генерации (построения) примитивных полиномов с заданными характеристиками.

В то же время в специализированных изданиях даются таблицы неприводимых полиномов и образцы примитивных полиномов над полем порядка 2^k только для некоторых значений k [3–5]. В статье предложен метод построения примитивных полиномов над полем порядка 2^k для произвольного целого числа $k \geq 2$ на основе известных примитивных полиномов над полем из двух элементов, что актуально с точки зрения используемых в современных компьютерных системах форматов представления данных.

В разд. 1 приведены определения основных понятий и вспомогательные результаты, используемые для обоснования алгоритма, на котором базируется предложенный метод, и полезные при его практической реализации. В разд. 2 дано детальное описание алгоритма, а в разд. 3 представлен пример его применения.

1. Определения основных понятий и некоторые вспомогательные результаты

В дальнейшем термин «поле» используется как синоним термина «конечное поле из 2^n элементов». Это поле обозначается символом F_{2^n} и обычно задается с помощью неприводимого полинома $f(x)$ степени n над полем F_2: $F_{2^n} = F_2[x]/(f(x))$. Элементами поля F_{2^n} являются полиномы $g(x) \in F_2[x]$ степени, меньше n, а сложение и умножение таких полиномов в поле происходит по модулю полинома $f(x)$.

Обозначим символом α элемент x поля $F_{2^n} = F_2[x]/(f(x))$. Тогда полином $f(x)$ в поле F_{2^n} имеет n разных корней α^{2^i}, $i \in \overline{0, n-1}$ [6, 7].

Элемент β поля F_{2^n} называется примитивным, если $F_{2^n} \setminus \{0\} = \{\beta^k : k \in \overline{0, 2^n - 1}\}$. Унитарный полином $g(x)$ степени $m > 1$ над полем F_{2^n} — примитивным над этим полем, если он неприводим над ним и имеет корень β в поле $F_{2^{nm}} = F_{2^n}[x]/(g(x))$, который является примитивным элементом последнего.

Для проверки неприводимости или примитивности полиномов можно использовать известные критерии.

Утверждение 1 (критерий Рабина) [8]. Пусть полином $g(x) \in F_{2^n}[x]$, его степень $\deg(g(x)) = m > 1$. Тогда полином $g(x)$ является неприводимым над полем F_{2^n} тогда и только тогда, когда

а) он делит полином $x^{2^{nm}} - x$: $g(x) \mid x^{2^{nm}} - x$;

б) для любого простого делителя p числа m полиномы $g(x)$ и $x^{2^{\frac{nm}{p}}} - x$ взаимно просты.

Следствие. Полином $g(x) \in F_2[x]$ степени 2^t является неприводимым над полем F_2 тогда и только тогда, когда он делит полином $x^{2^{2^t}} - x$ и является взаимно простым с полиномом $x^{2^{2^{t-1}}} - x$.

В [8] описан алгоритм проверки неприводимости полиномов степени m над полем F_{2^n}, который базируется на критерии Рабина и имеет сложность $O(m^2 + nm)$ операций в этом поле.

Утверждение 2 [9]. Неприводимый полином $g(x) \in F_{2^n}[x]$ степени $m > 1$ является примитивным над полем F_{2^n} тогда и только тогда, когда для любого простого делителя p числа $2^{nm} - 1$ полином $g(x)$ не делит полином $x^{\frac{2^{nm}-1}{p}} - 1$.

Утверждение 3 [10]. Неприводимый полином $g(x) \in F_{2^n}[x]$ степени $m > 1$ является примитивным над полем F_{2^n} тогда и только тогда, когда полином $\dfrac{x^{2^{nm}-1} - 1}{(x-1)g(x)}$ имеет ровно $2^{n(m-1)}(2^n - 1) - 1$ ненулевых членов.

Пусть E, F — поля, при этом $E \subseteq F$ и $a \in F$. Унитарный полином наименьшей степени над полем E, корнем которого является элемент a, называется минимальным полиномом элемента a над полем E и обозначается $m_{a,E}(x)$. Этот полином неприводим над полем E и раскладывается на линейные множители над полем F: $m_{a,E}(y) = \prod_{i=0}^{n-1} (x + a^{q^i})$, где $q = |F|$, $n = [F : E]$ — степень расширения F над полем E [7].

Нахождение коэффициентов полинома $m_{a,E}(x) = x^n + \sum_{j=0}^{n-1} c_j x^j$ для известных полей E, F и элемента a сводится к решению системы линейных уравне-

ний $a^{q^i n} + \sum_{j=0}^{n-1} c_j a^{q^i j} = 0$, $i \in \overline{0, n-1}$, над полем F относительно неизвестных $c_0, \ldots, c_{n-1} \in E$. Эта система имеет единственное решение, которое можно найти, выполнив $O(n^2)$ операций в поле F [11]. В случае $n = 2^t$, $t \in \mathbf{N}$, можно воспользоваться алгоритмом быстрой интерполяции, сложность которого оценивается величиной $O(n \log^2 n \log\log n)$ указанных операций [8].

2. Алгоритм построения примитивных полиномов над непростыми полями по известным примитивным полиномам над полем F_2

Пусть $f(x)$ — примитивный полином степени kl над полем F_2, где $k, l > 1$.

Требуется построить:

— примитивный полином $h(y) \in F_2[y]$ степени k, определяющий поле $F_{2^k} = F_2[y]/(h(y))$;

— примитивный полином $g(x) \in F_{2^k}[x]$ степени l, такой, что $g(x) \mid f(x)$.

Метод решения поставленной задачи состоит в следующем.

Обозначим α корень полинома $f(x)$ в поле $F_{2^{kl}} = F_2[x]/(f(x))$ и положим

$$\beta = \alpha^{\frac{2^{kl}-1}{2^k-1}}, \tag{1}$$

$$h(y) = m_{\beta, F_2}(y), \; g(x) = m_{\alpha, F_{2^k}}(x). \tag{2}$$

Поскольку α — примитивный элемент поля $F_{2^{kl}}$, то β — примитивный элемент его подполя $F' = \{a \in F_{2^{kl}} : a^{2^k} = a\}$ порядка 2^k. Отсюда следует, что неприводимый полином $h(y)$ имеет степень k и является примитивным над полем F_2. Далее $g(x)$ — неприводимый полином над полем F_{2^k}, корнем которого есть примитивный элемент α поля $F_{2^{kl}}$. Итак, $\deg(g(x)) = l$, и, поскольку $f(\alpha) = 0$, то $g(x) \mid f(x)$. Таким образом, полиномы (2) удовлетворяют указанным выше условиям.

Для вычисления коэффициентов этих полиномов воспользуемся уравнениями

$$h(y) = \prod_{j=0}^{k-1} (y + \beta^{2^j}), \tag{3}$$

$$g(x) = \prod_{i=0}^{l-1} (x + \alpha^{2^{ki}}), \tag{4}$$

а также применим один из критериев, указанных в разд. 1.

Заметим, что коэффициенты полинома (3) принадлежат полю F_2, в то время как коэффициенты полинома (4) являются элементами подполя F' поля $F_{2^{kl}}$, которые задаются векторами их координат в стандартном базисе $B = (\alpha^0, \alpha^1, \ldots, \alpha^{kl-1})$. Поэтому для нахождения искомого представления полинома $g(x)$ как элемента фактор-кольца $F_{2^k} = F_2[y]/(h(y))$ необходимо разложить коэффициенты полинома (4) по базису $(\beta^0, \beta^1, \ldots, \beta^{l-1})$.

Рассмотрим базис B' поля $F_{2^{kl}}$, который состоит из элементов $\alpha^i\beta^j$, $i \in \overline{0, l-1}$, $j \in \overline{0, k-1}$, и обозначим C матрицу перехода от базиса B к базису B', т.е. квадратную матрицу порядка kl над полем F_2, удовлетворяющую условию $B'^{\downarrow} = CB^{\downarrow}$. Матрица C обратима; при этом векторы координат $\vec{u}$ и $\vec{u'}$ произвольного элемента $u \in F_{2^{kl}}$ в базисах B и B' соответственно связаны соотношением $\vec{u'} = \vec{u}\, C^{-1}$.

Пусть $u = \sum\limits_{s=0}^{kl-1} u_s \alpha^s$ является произвольным элементом поля F', который задается вектором его координат $\vec{u} = (u_0, \ldots, u_{kl-1})$ в базисе B. Тогда для нахождения вектора координат этого элемента в базисе $(\beta^0, \beta^1, ..., \beta^{l-1})$, достаточно вычислить вектор $\vec{u}C^{-1} = (u(i, j): \ i \in \overline{0, l-1}, \ j \in \overline{0, k-1})$. Поскольку $u \in F'$, то $u(i, j) \neq 0$ только при $i = 0$; значит, $u = \sum\limits_{j=0}^{k-1} u(0, j)\beta^j$ — искомое разложение элемента u по базису $(\beta^0, \beta^1, ..., \beta^{l-1})$.

На основе приведенных рассуждений получим следующий алгоритм решения поставленной задачи.

Алгоритм

Вход. Примитивный полином $f(x)$ степени kl над полем F_2; $k, l > 1$.

1. Вычислить элемент β по формуле (1).
2. Вычислить коэффициенты полиномов (3), (4).
3. Для любых $i \in \overline{0, l-1}$, $j \in \overline{0, k-1}$ вычислить координаты $c_s(i, j)$ элемента $\alpha^i\beta^j = \sum\limits_{s=0}^{kl-1} c_s(i, j)\alpha^s$ в базисе B; построить матрицу $C = (c_s(i, j))$ порядка kl, строки которой пронумерованы парами (i, j), а столбцы — числами $s \in \overline{0, kl-1}$.
4. Вычислить матрицу $D = C^{-1}$, используя алгоритм Гаусса.
5. Для каждого коэффициента $u \in F'$ полинома (4), который задается вектором его координат $\vec{u}$ в базисе B, вычислить вектор $\vec{u}D = (u(i, j): i \in \overline{0, l-1}, j \in \overline{0, k-1})$ и установить $u = \sum\limits_{j=0}^{k-1} u(0, j)\beta^j$.

3. Пример применения алгоритма

Пусть $k = l = 2$, $f(x) = x^4 + x^3 + 1$. Тогда $\alpha^4 = \alpha^3 + 1$, $\beta = \alpha^5 = \alpha^3 + \alpha + 1$, и поскольку $\beta^2 = \beta + 1$, то $h(y) = (y + \beta)(y + \beta^2) = y^2 + y + 1$.

Кроме того, $g(x) = (x + \alpha)(x + \alpha^4) = x^2 + (\alpha^3 + \alpha + 1)x + (\alpha^3 + \alpha + 1)$.

Далее матрица перехода от базиса $B = (1, \alpha, \alpha^2, \alpha^3)$ к базису $B' = (1, \beta, \alpha, \alpha\beta)$ поля F_{2^4} имеет такой вид:

$$C = \begin{pmatrix} 1000 \\ 1101 \\ 0100 \\ 1111 \end{pmatrix},$$

а матрица, обратная к C, равна

$$D = \begin{pmatrix} 1000 \\ 0010 \\ 0101 \\ 1110 \end{pmatrix}.$$

Умножая вектор коэффициентов $u = (1101)$ элемента $\alpha^3 + \alpha + 1$ в базисе B на матрицу D, получаем вектор $uD = (0100)$. Итак, $\alpha^3 + \alpha + 1 = \beta$ и $g(x) = x^2 + \beta x + \beta$.

Заключение

Предложенный метод построения примитивных полиномов использован для создания элемента криптографической схемы, а именно, источника псевдослучайных чисел с заданными характеристиками.

Применение алгоритма построения примитивного полинома на основе известного примитивного полинома над полем из двух элементов, позволило существенно сократить общее время на проектирование и исключить трудоемкие вычислительные операции.

Дальнейшие исследования в данном направлении целесообразно направить на изучение особенностей использования предложенного метода применительно к проектированию различных криптографических приложений.

Г.М. Гулак

МЕТОД ПОБУДОВИ ПРИМІТИВНИХ ПОЛІНОМІВ ДЛЯ КРИПТОГРАФІЧНИХ ПІДСИСТЕМ ГАРАНТОЗДАТНИХ АВТОМАТИЗОВАНИХ СИСТЕМ

Запропоновано метод побудови примітивних поліномів, які використовуються під час проектування радіотехнічних систем, підсистем криптографічного захисту інформації в гарантоздатних автоматизованих системах перетворення інформації та управління на об'єктах критичної інфраструктури, а також в інших суспільно значущих інформаційних системах. Зокрема, такі поліноми можуть застосовуватися для створення елементів криптографічних схем, включаючи джерела псевдовипадкових чисел, вузли гарантованого періоду, вузли (підстановки) заміни. Із застосуванням критерію Рабіна для незвідних поліномів та рекурсивної конструкції запропоновано метод побудови на основі відомих примітивних поліномів над полем із двох елементів примітивних поліномів над полями порядку 2^k, де $k \geq 2$. Для обчислення коефіцієнтів поліномів наведено необхідні рівності. Цей метод є актуальним у випадку створення підсистем криптографічного захисту інформації у сучасних комп'ютерних системах, що використовують мікроконтролери та мікропроцесори на основі 32- або 64-бітних форматів подання даних. Вказаний метод побудови примітивних поліномів над непростими полями за відомими примітивними поліномами над полем із двох елементів має поліноміальну складність. Наведено означення основних понять, а також необхідні допоміжні результати, що використовуються при обгрунтуванні алгоритму, на якому базується пропонований метод, та можуть бути корисними при його реалізації, надано детальний опис алгоритму та наведено приклад його застосування.

Ключові слова: підсистема криптографічного захисту, примітивний поліном, незвідний поліном, мінімальний поліном елемента, примітивний елемент, скінченне поле, фактор-кільце, критерій Рабіна.

G.N. Gulak

METHOD FOR CONSTRUCTING PRIMITIVE POLYNOMIALS FOR CRYPTOGRAPHIC SUBSYSTEMS OF DEPENDABLE AUTOMATED SYSTEMS

The paper proposes a method for constructing primitive polynomials that are used in the design of radio engineering systems, subsystems of cryptographic information protection in reliable automated information processing and control systems at critical infrastructure facilities, as well as in other socially significant information systems. In particular, such polynomials can be used to create elements of cryptographic schemes, including pseudo-random number generators, guaranteed period nodes, substitution nodes (substitution). Using the Rabin criterion for irreducible polynomials and a recursive construction, the paper proposes a method for constructing, based on well-known primitive polynomials over a field of two elements, primitive polynomials over fields of order 2^k, where $k \geq 2$. The necessary equalities for calculating the coefficients of polynomials are given. This method is relevant in the case of creating subsystems for cryptographic protection of information in modern computer systems that use microcontrollers and microprocessors based on 32 or 64 bit data presentation formats. The indicated method for constructing primitive polynomials over non-simple fields based on the known primitive polynomials over a field of two elements has polynomial complexity. The article provides definitions of the basic concepts, as well as the necessary auxiliary results, which are used to substantiate the algorithm on which the proposed method is based, which can be useful in its implementation, a detailed description of the algorithm is presented and an example of its application is given.

Keywords: subsystem of cryptographic security, primitive polynomial, irreducible polynomial, minimal polynomial of an element, primitive element, finite field, factor ring, Rabin's criterion.

1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М. : КУДИЦ-ОБРАЗ, 2001. 368 с.
2. Rueppel R.A. Analysis and design of stream ciphers. Springer communications and control engineering series, 1986. 244 p.
3. Гилл А. Линейные последовательностные машины. Анализ, синтез и применение. Пер. с англ. М. : Наука, 1974. 288с.
4. Берлекэмп Э. Алгебраическая теория кодирования. М. : Мир, 1971. 480 с.
5. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М. : Мир, 1986. 576 с.
6. Ленг С. Алгебра. М. : Мир, 1968. 564 с.
7. Лидл Р., Нидеррайтер Г. Конечные поля: в 2-х т. М. : Мир, 1988. Т. 1. 430 с.; Т. 2. 390 с.
8. Von zur Gathen J., Gerhard J. Modern computer algebra. New-York : Cambridge Univ. Press, 1999. **40.** 755 p.
9. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра: в 2-х т. Т.II. М. : Гелиос АРВ, 2003. 416 с.
10. Fitzgerald R.W. A characterization of primitive polynomials over finite fields. *Finite Fields and Their Appl*. 2003. **9**. P. 117–121.
11. Валицкий Ю.Н. Один способ решения системы линейных уравнений с матрицей Вандермонда. *Научно-методический сборник «Математика сегодня»*. Киев : Вища школа, 1989. С. 39–47.

Получено 09.09.2020