Секція 2. Зберігання, аналіз та захист даних в інформаційних системах

УДК 512.623.3

А.Я. Белецкий

Национальный авиационный университет, Киев

ОБОБЩЕННЫЕ ПРИМИТИВНЫЕ ПОЛИНОМЫ

В теории полей Галуа, составляющих основу алгебраической теории помехоустойчивого кодирования и современной теории криптографии, ключевым является понятие неприводимого полинома (НП). Полином

$$\varphi_n(x) = \sum_{i=0}^{n} \alpha_{n-i} x^{n-i}, \quad \alpha_i \in \{0,1\}, \qquad (1)$$

степени n над полем $GF(2^n)$ называется *неприводимым*, если он не делится ни на какой полином меньшей степени над данным полем [1].

Многочлен (1), записанный в *алгебраической* (полиномиальной) форме, может быть однозначно представлен бинарной строкой (двоичным вектором) своих коэффициентов (в *бинарной* форме)

$$\varphi_n = \{\alpha_n, \alpha_{n-1}, \ldots, \alpha_i, \ldots, \alpha_0\}, \quad \alpha_i \in \{0,1\}.$$

Например, бинарному вектору

$$\varphi_8 = 100011011$$

соответствует алгебраическая форма полинома

$$\varphi_8(x) = x^8 + x^4 + x^3 + x + 1. \qquad (2)$$

Введем одну из главных характеристик НП, называемую показателем полинома. *Показатель* неприводимого полинома равен наименьшему положительному числу e, при котором НП $\varphi_n(x)$ делит двучлен $x^e + 1$ без остатка [2]. Физический смысл такой характеристики состоит в том, что он определяет *порядок* мультипликативной группы, образованной степенями *примитивного элемента* θ группы по $\bmod \varphi_n$.

Множество неприводимых полиномов $\{\varphi_n\}$ содержит важное (например, для криптографических приложений) подмножество так называемых примитивных полиномов (ПрП). В алгебре, теории чисел и полей Галуа двоичный полином $\varphi_n(x)$ степени n называется *примитивным*, если он неприводим, а наименьший показатель e, при котором $\varphi_n(x)$ делит двучлен $\Phi(x) = x^e + 1$ без остатка, определяется выражением $e = 2^n - 1$ [2].

В теории полиномов постулируется утверждение, согласно которому все примитивные полиномы являются неприводимыми, тогда как обратное не всегда соблюдается, т.е. совсем не обязательно, чтобы каждый неприводимый полином обладал свойствами примитивности.

Основная задача данного исследования заключается в доказательстве того, что, во-первых, любой НП φ_n степени n соответствующим подбором образующих (примитивных) элементов $\boldsymbol{\omega}$ приводится к примитивному полиному $\varphi_n^{(\omega)}$ и, во-вторых, число элементов $\boldsymbol{\omega}$, доставляющих произвольному неприводимому полиному φ_n свойство примитивности, есть величина постоянная, определяемая функцией Эйлера аргумента $L_n = 2^n - 1$.

Приведенное ранее определение примитивного полинома $\varphi_n(x)$ можно отобразить такими эквивалентными соотношениями:

$$\varphi_n(x) \mid x^e - 1; \qquad (3)$$

$$x^e \equiv 1 \bmod \varphi_n(x) \qquad (4)$$

при условии, что

$$\min e = 2^n - 1. \qquad (5)$$

Предлагаемое обобщение понятия примитивного полинома сводится к следующему. Заменим основание x одночлена x^e в формулах (3) и (4) произвольным полиномом $\omega_m(x)$ степени m такой, что $1 \le m < n$. Тем самым представим данные выражения в виде:

$$\varphi_n^{(\omega)}(x) \mid [\omega_m(x)]^e - 1; \qquad (6)$$

$$[\omega_m(x)]^e \equiv 1 \bmod \varphi_n^{(\omega)}(x) \qquad (7)$$

при соблюдении условия (5).

Полином $\omega_m(x)$ назовем *образующим элементом* (ОЭ) ПрП, подобный ранее введенному образующему элементу θ. Дальнейшие пояснения упростятся, если от алгебраических форм полиномов $\varphi_n(x)$ и $\omega_m(x)$ перейти к их бинарным формам. В классическом варианте (3) или (4) одночлен x^e можно записать в виде числового (бинарного) эквивалента $(10)^e$, поскольку основание x есть полином первой степени с минимальным весом, т.е. $x = 10$. В то же время ОЭ ω_m может быть отличным от полинома $x = 10$ и принимать значения 11, 110, 101 и др.

Неприводимый полином (2) выбран разработчиками криптографического алгоритма Rijndael в качестве базового для построения примитива нелинейной подстановки (S-блока) в шифре AES [3].

Относительно НП (2) можно сказать следующее. Во-первых, этот полином не является примитивным; его показатель равен 51. Во-вторых, как справедливо отмечается в [4], полином $\varphi_8(x)$ заданный выражением (2), является первым НП восьмой степени, упоминающийся в большинстве справочников, т.е. его выбор достаточно произволен.

Как известно, S-блоки могут быть реализованы *только* на примитивных полиномах. Проблему непримитивности полинома авторы алгоритма Rijndael решили простой заменой одночлена x двучленом $x+1$. Такая замена привела к тому, что исходный непримитивный полином (2) показателя 51 приобрел свойство примитивности с показателем 255.

Проведенный краткий анализ неприводимых и примитивных полиномов как раз и подтверждает возможность и целесообразность перехода от классического представления примитивного полинома в виде соотношений (3) или (4) к обобщенному представлению выражениями (6) или (7) соответственно.

Основной результат данной работы состоит в том, что в ней введено понятие *обобщенного примитивного полинома*, расширяющее классический термин примитивного полинома. Это означает, в частности, что предлагается новая формулировка основного постулата теории неприводимых полиномов, согласно которой все НП $\varphi_n(x)$ приобретают свойство примитивности над образующими элементами $\omega_m(x)$, такими, что выполняется сравнение (7) при соблюдении условия (5). Таким образом, фактически термин обобщенные примитивные полиномы над допустимыми образующими элементами корреспондируется с мультипликативной группой максимального порядка, формируемой степенями ОЭ по модулю выбранного НП. В отличии от классических ПрП (и в общем случае НП) обобщенные ПрП не могут быть представлены ни в алгебраической, ни в векторной формах.

Показано, во-первых, что *все* неприводимые полиномы, в том числе и те, которые в классическом понимании не являются примитивными, приобретают свойство примитивности соответствующим выбором образующего элемента. Таким способом, в частности, разработчики криптоалгоритма Rijndael заменой образующего элемента $\omega = 10$ элементом $\omega = 11$ обратили выбранный ими для построения S-блока непримитивный полином (2) в примитивный. Во-вторых, число образующих элементов, посредством которых *все* неприводимые полиномы степени n становятся примитивными, есть величина постоянная, равная функции Эйлера аргумента L_n. Кроме того, предложен достаточно простой алгоритм синтеза образующих матриц Галуа и Фибоначчи, обладающих замечательными свойствами простоты и коммутативности. С помощью таких матриц непосредственно формируются мультипликативные группы порядка L_n по выбранным параметрам φ_n и ω.

В работе приведены примеры синтеза линейных регистров сдвига с линейными обратными связями, отвечающих обобщенным примитивным полиномам. Обсуждаются вопросы оптимизации S-блоков симметричных блочных шифраторов.

Показано, что полученные результаты могут быть продолжены не только на обобщенные примитивные полиномы с коэффициентами над полем Галуа простого аргумента, отличного от 2, но также и на обобщенные поля Галуа произвольной характеристики.

Список литературы

1. Лидл Р., Нидеррайтер Г. Конечные поля / Р. Лидл, Г. Нидеррайтер. – М.: Мир, 1988. – Т. 1. – 432 с.

2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванов. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

3. [Электронный ресурс]. – Режим доступ к ресурсу: csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

4. Зензин О.С. Стандарт криптографической защиты AES. Конечные поля / О.С. Зензин, М.А. Иванов; под ред. М.А. Иванова. – М.: КУДИЦ-ОБРАЗ, 2002. – 176 с.