РЕШЕНИЕ КВАДРАТНЫХ УРАВНЕНИЙ В КОНЕЧНЫХ ПОЛЯХ ХАРАКТЕРИСТИКИ ДВА

Глуско Кр.Л., Титов С.С.
e-mail: sonniger@inbox.ru

В современных каналах связи используются многобитовые последовательности, которые можно интерпретировать как элементы конечных полей характеристики два, поэтому важной задачей становится использование многочленов больших степеней, задающих эти поля. Вычисление элементов неприводимых многочленов так же необходимы для решения квадратных уравнений в конечных полях характеристики два, что нашло применение в эллиптической криптографии: это позволяет в 2 раза уменьшить количество бит для хранения точек эллиптической кривой.

Различают понятия абсолютного и относительного следа элемента поля.

В произвольном поле $GF(p)$ формула будет выглядеть следующим образом: $q = p^n => Tr(z) = z + z^p + z^{p^2} + \ldots + z^{p^{n-1}}$.

$Tr(z) \in GF(p)$ и может принимать значения $0, 1, \ldots, p-1$.

Если поле $GF(q^m)$ является расширением поля $GF(q)$, то речь уже идет о вычислении относительного следа элемента поля $GF(q^m)$. Известно, что относительный след - единственная линейная операция, отображающая элементы поля F в элементы поля K, обладающая свойствами идемпотентности, коммутативности, ассоциативности и дистрибутивности [1].

Для решения уравнения $x^2 + x = z$ в полях $GF(2^n)$ при нечетном n используется так называемая формула полуследа:

$Sr(z) = x = z + z^4 + z^{16} + \ldots + z^{2^{n-1}}$; причём $z^{2^n} = z$.

Утверждение 1. *Формула полуследа дает решение квадратного уравнение с нулевым следом в поле $GF(2^n)$, где n нечетное.*

В книге [2] вычисление решения квадратного уравнения в полях $GF(2^n)$, где n четное, сводится к системе линейных уравнений.

Однако на основании исследований можно сформулировать следующее утверждение.

Утверждение 2. *При четном n не существует многочлена вида, дающего решение квадратного уравнения $z^2 + z = a$.*

В многочленах четных степеней появятся две степени подряд, поэтому при сложении $z+z^2$ некоторые позиции сократятся и не дадут полной формулы, аналогичной для многочленов нечетной степени.

Можно ставить задачу как поиск многочлена, корень которого является решением квадратного уравнения z^2+z в поле $GF(2^n)$, где n четное.

Для поиска решения уравнения больших степеней можно использовать идею расширения полей: зная формулу решения квадратного уравнения в полях $GF(2^n)$, где n нечетно, и, зная формулу решения этого уравнения в полях $GF(2^k)$, мы сможем найти формулу решения в поле $GF(2^{nk}), k = 2, 4, 8, 16, \ldots$ (см. рис. 1).

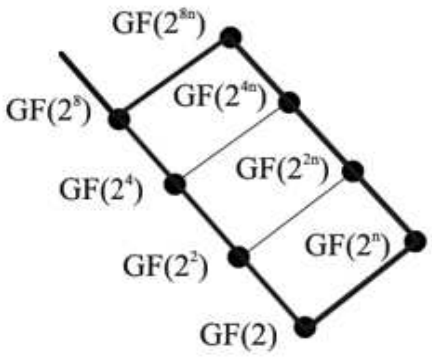

Рис. 1: Схема расширения полей

Решение квадратного уравнения при четном n можно выразить следующим образом:

$z \in GF(2^n) \Longleftrightarrow z = x + \alpha y, x, y \in GF(2^n)$

$Tr(z) = z+z^2+z^4+\ldots+z^{2^{2^n-1}} = (z+z^4+z^{16}+z^{2^{2^n-2}}+(z^2+z^8+\ldots+z^{2^{2^n-1}}) = (x+x^2+\ldots+x^{2^{n-1}})+\alpha(y+y^4+y^{16}+\ldots+y^{2^{n-1}})+\alpha^2(y^2+y^8+y^{32}+\ldots+y^{2^n})$.

$z^2+z+z_1 \Longrightarrow (x^2+\alpha^2y^2)+(x+\alpha y)+(x_1+\alpha y_1)$, где $\alpha^2 = \alpha+1$.

$(x^2+x+y^2)+\alpha(y^2+y) = x_1+\alpha y_1$.

Отсюда следует:

$$\begin{cases} Tr(y_1) = 0, \\ Tr(x_1+y^2) = 0. \end{cases}$$

При n нечетном $Tr(Sr(a)) = 0$, если $Tr(a) = 0$.

Одно из решений при условии, если $Tr(x_1) = 0$:

$y = Sr(y_1) = y_1 + y_1^4 + y_1^{16} + \ldots + y_1^{2^{n-1}}$.

$y^2 = [Sr(y_1)]^2 = y_1^2 + y_1^8 + y_1^{32} + \ldots + y_1^{2^{n-2}} + y^{2^n} = y_1 + y_1^2 + y_1^8 + y_1^{32} + \ldots + y_1^{2^{n-2}}$.

Сложив эти выражения, получим: $y + y^2 = y_1 = Tr(y_1) + y_1 \Longrightarrow Tr(y_1) = 0$.

Если $Tr(x_1) = 1$, то

$Tr(x_1 + y^2) = Tr(x_1) + Tr(y^2) = Tr(x_1) + Tr(y) = Tr(x_1)$, что противоречит начальным утверждениям.

Поэтому условия таковы: $Tr(x_1) = Tr(y_1) = 0$, а формула - такова:

$$\begin{cases} y = Sr(y_1) + Tr(x_1), \\ x = Sr(x_1 + y^2) = Sr(x_1) + Sr(y_1^2) = Sr(x_1) + Tr(x_1) + Sr(y_1^2). \end{cases}$$

Но нас интересует универсальная формула для нахождения корня квадратного уравнения для многочленов как нечетной, так и четной степени. Таким образом, возникает вопрос выбора базиса.

На основании проведенных исследований можно сказать, что надо выбирать базис $GF(2^s), s = 2^k$ через симметричный, или самовозвратный многочлен. Это связано с тем, что нормальный базис при последовательном возведении в степень создает цикл, что упрощает расчеты.

В заключении можно сделать вывод, что такая процедура решения квадратных уравнений является очень эффективной и сокращает временные затраты на вычисления.

Литература

[1] Конечные поля: в 2–х т. Т. 1. Лидл Р., Нидеррайтер Г. Пер. с англ. – М.: Мир, 1988. С. 71–72.

[2] Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы. Болотов А.А., Гашков С.Б., Фролов А.Б. – М.: КомКнига, 2006. С. 49–50, 60–62.