Секция 1

# ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.62

## О РЕШЕНИИ КВАДРАТНЫХ УРАВНЕНИЙ В БИНАРНЫХ ПОЛЯХ

К. Л. Глуско, С. С. Титов

Передача информации в современных каналах связи основана на использовании многобитовых последовательностей, которые можно интерпретировать как элементы конечных полей. Поэтому решение задач в бинарных полях больших степеней и представление этих решений в виде битовых строк является важной проблемой. Решение квадратных уравнений в конечных полях используется в разных областях математики и защиты информации. В эллиптической криптографии, к примеру, это позволяет в два раза уменьшить количество бит для хранения точек эллиптической кривой при реализации криптографических примитивов [1, 2].

След — линейная операция $\mathrm{Tr}_{F/K}$, отображающая элементы поля $F$ в элементы поля $K$, обладающая свойствами идемпотентности, коммутативности, ассоциативности и дистрибутивности [3].

Различают понятия абсолютного и относительного следа элемента поля. В поле $\mathrm{GF}(q)$, где $q = p^n$, $\mathrm{Tr}(z) \in \mathrm{GF}(q)$ и может принимать значения 0, 1, ..., $p-1$, формула абсолютного следа элемента поля имеет вид

$$\mathrm{Tr}(z) = z + z^p + z^{p^2} + \ldots + z^{p^{n-1}}.$$

Значение следа элемента часто является определяющим для выполнения тех или иных условий. Любое квадратное уравнение в поле характеристики два приводится к стандартному виду $x^2 + x = z$, где $z$ — элемент данного поля, $x$ — искомый корень [1]. Для решения такого квадратного уравнения при $\mathrm{Tr}(z) = 0$ в конечных полях $\mathrm{GF}(2^n)$ при нечётном $n$ используется так называемая формула полуследа:

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

**Утверждение 1.** Формула полуследа дает решение квадратного уравнения с нулевым следом в поле $\mathrm{GF}(2^n)$, где $n$ нечётное.

**Утверждение 2** [1, 4]. При чётном $n$ не существует линеаризированного многочлена вида $z = \sum\limits_{s \in S} a^{2^s}$ ($S$ — подмножество в $\{0, 1, \ldots, n-1\}$), дающего решение квадратного уравнения $z^2 + z = a$.

Решение квадратного уравнения может быть представлено в стандартном базисе, т. е. в базисе вида $\{1, \lambda, \lambda^2, \lambda^3, \ldots, \lambda^{n-1}\}$, но мы воспользуемся разложением в нормальном базисе, т. е. в базисе вида $\{\beta, \beta^2, \beta^4, \beta^8, \ldots, \beta^{2^{n-1}}\}$, где $\lambda$ и $\beta$ — корни неприводимых многочленов степени $n$ [2]. Отметим, что построение нормальных базисов является задачей нетривиальной.

Для построения базиса $\{\beta, \beta^2, \beta^4, \beta^8, \ldots, \beta^{2^{n-1}}\}$ используем операцию симметричного квадратичного расширения $\alpha = \beta + \beta^{-1}$, где $\alpha$ является элементом поля $F$, $\beta$ — элементом поля $K$, а поле $K$ — расширением поля $F$ [5].

**Теорема 1.** Если множество $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ является нормальным базисом в поле $\mathrm{GF}(2^n)$, след $\alpha^{-1}$ равен единице и $\alpha = \beta + \beta^{-1}$ в поле $\mathrm{GF}(2^{2^n})$, то множество $\{\beta, \beta^2, \ldots, \beta^{2^{2n-1}}\}$ также является нормальным базисом в поле $\mathrm{GF}(2^{2^n})$ [4].

Разложим квадратное уравнение $x^2 + x = a$ в нормальном базисе $\{\alpha, \alpha^2, \ldots, \alpha^{2^{k-1}}\}$:

$$\begin{cases} x = \alpha x_0 + \alpha^2 x_1 + \alpha^4 x_2 + \ldots + \alpha^{2^{k-1}} x_{k-1}, \\ a = \alpha a_0 + \alpha^2 a_1 + \alpha^4 a_2 + \ldots + \alpha^{2^{k-1}} a_{k-1}, \\ x^2 = \alpha^2 x_0 + \alpha^4 x_1 + \alpha^8 x_2 + \ldots + \alpha^{2^k} x_{k-1}. \end{cases}$$

Просуммируем эти уравнения и с учётом необходимого условия равенства нулю множителей при степенях $\alpha$ получим

$$\begin{cases} x_0 + a_0 + x_{k-1}^2 = 0, \\ x_1 + a_1 + x_0^2 = 0, \\ x_2 + a_2 + x_1^2 = 0, \\ \ldots \quad \ldots \quad \ldots \\ x_{k-1} + a_{k-1} + x_{k-2}^2 = 0. \end{cases}$$

Решив систему, получим формулу для $x_0$:

$$x_0 = (\mathrm{Sr}(\mathrm{Sr}(\mathrm{Sr}(\ldots(\mathrm{Sr}(b_0)))))),$$

где $b_0 = x_0^{2^k} + x_0$ и число операций Sr равно $k$.

Аналогично находим остальные элементы корней.

Описанный метод дает возможность быстро найти корни квадратных уравнений $x^2 + x = a$ в полях $\mathrm{GF}(2^m)$ при любых $m$ и представить эти решения в виде битовых строк.

## ЛИТЕРАТУРА


1. *Болотов А. А., Гашков С. В., Фролов А. Б.* Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006. С. 76–81.
2. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. С. 41–63.
3. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988. С. 74–75.
4. *Глуско К. Л.* След и полуслед в конечных полях // Материалы науч.-техн. конф., посв. 55-летию УрГУПС. Екатеринбург: Уральский государственный университет путей сообщения, 2011. Т. 1. Вып. 97(180) С. 356–364.
5. *Демкина О. Е., Титов С. С., Торгашева А. В.* Рекуррентное вычисление неприводимых многочленов в задачах двоичного кодирования // Молодые учёные — транспорту: Труды IV науч.-техн. конф. Екатеринбург: Уральский государственный университет путей сообщения, 2003. С. 391–404.