УДК 512.624: 003.26

Кр.Л. Глуско, С.С. Титов

Арифметический алгоритм решения квадратных уравнений в конечных полях характеристики два

Рассмотрены арифметические задачи в конечных полях характеристики два, которые могут иметь криптографические приложения. На основе построения нормальных базисов с помощью симметричного квадратичного расширения предложен алгоритм решения квадратных уравнений через обобщённую формулу полуследа. Рассмотрены примеры.

Ключевые слова: конечное поле характеристики два, нормальный базис, формула полуследа квадратное уравнение.

Задача решения квадратных уравнений в конечных полях

В современных каналах связи используются многобитовые последовательности, которые можно интерпретировать как элементы конечных полей. Поэтому важной задачей становится поиск решений уравнений в полях больших степеней и представление их в виде битовых строк.

В теории конечных полей одним из актуальных вопросов является решение квадратных уравнений, что нашло применение и в других областях дискретной математики. В эллиптической криптографии, к примеру, это позволяет в два раза уменьшить количество бит для хранения точек эллиптической кривой [1, 2] при реализации криптографических примитивов.

Имеется отличие в задачах решения квадратных уравнений в полях различной характеристики. Решение квадратных уравнений в простых полях нечётной характеристики приводит к задаче вычисления символа Лежандра [2]. Решение же квадратных уравнений в полях характеристики два имеет свою специфику, поскольку решаемое уравнение в стандартном виде оказывается линейным.

Рассмотрим алгоритм решения квадратных уравнений в конечных полях характеристики два. Для полноты изложения дальнейших рассуждений напомним некоторые теоретические понятия.

След – линейная операция $Tr_{F/K}$, 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 $GF(q)$, где $q = p^n$, формула абсолютного следа элемента поля имеет следующий вид: $Tr(z) = z + z^p + z^{p^n} + \ldots + z^{p^{n-1}} \in GF(q)$ и может принимать значения $\{0, 1, \ldots, p-1\}$.

Если поле $F = GF(q^m)$ является расширением поля $K = GF(q)$, то речь уже идет о вычислении относительного следа $Tr_{F/K}(z)$ элемента поля $GF(q^m)$. 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 – данный элемент этого поля; x – искомый корень [1, 2]. В книге [2, с. 80] представлен пример такого приведения для несуперсингулярных эллиптических кривых: уравнение вида $Y^2 + xY + f(x) = 0$ при подстановке $Y = xZ$ принимает вид $Z^2x^2 + x^2Z + f(x) = 0$, и при $x \neq 0$ оно эквивалентно уравнению $Z^2 + Z + \sigma = 0$, где $\sigma = f(x)/x^{-2}$.

Для решения такого квадратного уравнения при $Tr(z) = 0$ в конечных 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 $z^{2^n} = z$ [1, 2, 4].

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

В книге [1] решение квадратного уравнения в полях $GF(2^n)$, где n четное, сводится к системе линейных уравнений, вычисление которой довольно громоздко и требует временных затрат. Трудность задачи поиска формулы решения для четной степени иллюстрирует следующее

Утверждение 2. При четном n не существует линеаризированного многочлена вида $z = \sum_{s \in S} a^{2^s}$ (S – подмножество в $\{0, 1, \ldots, n-1\}$), дающего решение квадратного уравнения $z^2 + z = a$.

Можно ставить задачу и как поиск многочлена, корень которого является решением квадратного уравнения $z^2 + z = a$ в поле $GF(2^n)$ [5, 6], где n четное, при этом стоит еще раз отметить, что в бинарных полях квадратное уравнение является линейным.

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 можем найти формулу решения в поле $GF(2^{nk})$, $k = 2^r$, $r = 1, 2, 3, \ldots$.

Построение нормальных базисов с помощью квадратичного симметричного расширения

Решение уравнения может быть представлено в *стандартном базисе*, т.е. базисе вида $\{1, \lambda, \lambda^2, \lambda^3, \ldots, \lambda^{n-1}\}$, но мы воспользуемся разложением в *нормальном базисе*, т.е. базисе вида $\{\alpha, \alpha^2, \alpha^4, \alpha^8, \ldots, \alpha^{2^{n-1}}\}$, где λ и α – корни неприводимого многочлена степени n. Задача построения нормальных базисов является нетривиальной, например, требуется, чтобы $Tr(\beta) = 1$, поэтому для построения базиса $\{\alpha, \alpha^2, \alpha^4, \alpha^8, \ldots, \alpha^{2^{n-1}}\}$ используем операцию *симметричного квадратичного расширения*, формула которого такова: $\alpha = \beta + \beta^{-1}$, где α является элементом поля F, β является элементом поля K, а поле K является расширением поля F.

Необходимо рассмотреть алгоритм построения нормальных базисов при квадратичном симметричном расширении полей.

Возьмем нормальный базис $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$, $\alpha \in GF(2^n)$, примем $\beta \in GF(2^{2n})$ как результат симметричного квадратичного расширения поля $GF(2^n)$, то есть $\alpha = \beta + \beta^{-1}$; таким образом, β – корень квадратного уравнения $\beta^2 + \alpha\beta + 1 = 0$. Пусть α – корень многочлена $f(x)$ степени n. Из нормальности базиса вытекает, что $f(x)$ неприводим. Элемент β является корнем многочлена $F(x)$ степени $2n$, связанного с $f(x)$ соотношением $F(x) = x^n f(x + x^{-1})$. Многочлен $F(x) = x^n f(x + x^{-1})$ является самовозвратным. Исследуем вопрос: когда множество $\{\beta, \beta^2, \ldots, \beta^{2^{2n-1}}\}$ также будет нормальным базисом, но уже в поле $GF(2^{2n})$? Если $F(x)$ приводим, то все степени элемента β лежат в поле $GF(2^n)$ и поэтому не могут образовывать требуемый базис. Многочлен $F(x)$ будет неприводимым тогда и только тогда [7], когда след α^{-1} равен единице; в этом случае справедливо равенство $\beta^{-1} = \beta^{2^n}$. В таком случае потребуем от α равенства единице её антиследа, то есть следа α^{-1}: $Tr(\alpha^{-1}) = \alpha^{-1} + \ldots + \alpha^{-2^{n-1}} = 1 \neq 0$. Это требование является существенным.

Из определения нормальности базиса следует: $\alpha + \ldots + \alpha^{2^{n-1}} \neq 0$, т.е. (абсолютный) след элемента равен единице, более того, нормальность исходного базиса равносильна тому, что для любого подмножества $\{i, j, \ldots, k\}$ множества $\{0, 1, \ldots, n-1\}$ сумма $\alpha^{2^i} + \alpha^{2^j} + \ldots + \alpha^{2^k}$ не равна нулю. Предположим от противного, что элементы множества $\{\beta, \beta^2, \ldots, \beta^{2^{2n-1}}\}$ линейно зависимы над полем из двух элементов, т.е. $\beta^{2^i} + \beta^{2^j} + \ldots + \beta^{2^k} = 0$, где $\{i, j, \ldots, k\}$ – подмножество множества $\{0, 1, \ldots, 2n-1\}$. Возводя это равенство в степень 2^n, получим:

$$(\beta^{2^i})^{2^n} + (\beta^{2^j})^{2^n} + \ldots + (\beta^{2^k})^{2^n} = 0; \quad (1)$$

$$\beta^{-2^i} + \beta^{-2^j} + \beta^{-2^k} = 0. \quad (2)$$

Сложив выражение (2) и первоначальное $\beta^{2^i} + \beta^{2^j} + \ldots + \beta^{2^k} = 0$, получим $(\beta^{2^i} + \beta^{-2^i}) + (\beta^{2^j} + \beta^{-2^j}) + \ldots + (\beta^{2^k} + \beta^{-2^k}) = 0$. С учетом выражения $\alpha = \beta + \beta^{-1}$ оно приобретает вид $\alpha^{2^i} + \alpha^{2^j} + \ldots + \alpha^{2^k} = 0$.

Как известно, $\alpha^{2^n} = \alpha^{2^0} = \alpha$ для любого $\alpha \in GF(2^n)$. Значит, из-за линейной независимости степеней α числа $i, j, \ldots, k$ разбиваются на пары равных степеней по модулю n, т.е. для $\alpha \in GF(2^n)$ множество $\{i, j, \ldots, k\}$ преобразуется в $\{i_1, i_1 + n, \ldots, i_m, i_m + n\}$:

$$\alpha^{2^j} + \ldots + \alpha^{2^k} = (\alpha^{2^{i1}} + \alpha^{2^{i1+n}}) + (\alpha^{2^{j1}} + \alpha^{2^{j1+n}}) + \ldots + (\alpha^{2^{k1}} + \alpha^{2^{k1+n}}) = 0. \quad (3)$$

На основании свойств степеней для $\alpha \in GF(2^n)$ имеем равенство $\alpha^{2^{i+n}} = \alpha^{2^i \cdot 2^n} = (\alpha^{2^i})^{2^n} = \alpha^{2^i}$, поэтому в выражении (3) все суммы в скобках равны нулю.

Для β получим следующее равенство: $\beta^{2^i} + \beta^{2^j} + \ldots + \beta^{2^k} = (\beta^{2^{i1}} + \beta^{2^{i1+n}}) + \ldots + (\beta^{2^{im}} + \beta^{2^{im+n}})$.

Ввиду самовозвратности и неприводимости характеристического многочлена выражение примет вид $(\beta^{2^{i1}} + \beta^{2^{i1+n}}) + \ldots + (\beta^{2^{im}} + \beta^{2^{im+n}}) = (\beta^{2^{i1}} + \beta^{-2^{i1}}) + \ldots + (\beta^{2^{im}} + \beta^{-2^{im}}) = (\beta + \beta^{-1})^{2^{i1}} + (\beta + \beta^{-1})^{2^{im}} = \alpha^{2^{i1}} + \ldots + \alpha^{2^{im}} = 0$, где $\{i_1, \ldots, i_m\}$ – подмножество множества $\{0, 1, \ldots, n-1\}$, что противоречит утверждению о нормальности базиса $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$.

Таким образом, наше предположение неверно, и множество $\{\beta, \beta^2, \ldots, \beta^{2^{2n-1}}\}$ является нормальным базисом. Итак, доказана

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

Таким образом, взяв α корень многочлена $\alpha^2 + \alpha + 1 = 0$ в поле $GF(2^m)$, $m = 2^1$, можно последовательно построить нормальные базисы в полях $GF(2^m)$, где $m = 2^k$.

Выпишем [8] первые многочлены, определяющие эти нормальные базисы:

$D_1(x) = x + 1$;
$D_2(x) = x^2 + x + 1$;
$D_3(x) = x^4 + x^3 + x^2 + x + 1$;
$D_4(x) = x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$;
$D_5(x) = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$;
$D_6(x) = x^{32} + x^{31} + x^{30} + x^{28} + x^{27} + x^{26} + x^{24} + x^{22} + x^{17} + x^{16} + x^{15} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$.

Метод решение квадратных уравнений в конечных полях

Вернемся к решению квадратного уравнения $x^2 + x = a$.

Возьмем нормальный базис $\{\alpha, \alpha^2, \ldots, \alpha^{2^{k-1}}\}$ для разложения:

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

Сложим эти уравнения и вынесем общие множители α:

$\alpha(x_0 + a_0 + x_{k-1}^2) + \alpha^2(x_1 + a_1 + x_0^2) + \alpha^4(x_2 + a_2 + x_1^2) + \ldots + \alpha^{2^{k-1}}(x_{k-1} + a_{k-1} + x_{k-2}^2) = 0$.

Преобразуем систему (4), с учетом необходимого условия равенства нулю множителей степеней α

$$\begin{cases} x_0 + a_0 + x_{k-1}^2 = 0, \\ x_1 + a_1 + x_0^2 = 0, \\ x_2 + a_2 + x_1^2 = 0, \\ \ldots\ldots\ldots\ldots \\ x_{k-1} + a_{k-1} + x_{k-2}^2 = 0. \end{cases} \quad (5)$$

Общий вид таких множителей имеет вид $x_i + a_i + x_{i-1}^2 = 0$, $i-1 \pmod k$, $x_i, a_i \in GF(2^n)$, где n нечетное, $k = 2^r$, $r = 1, 2, 3, \ldots$.

Для примера возьмем $r = 2$, тогда $k = 4$.

$$\begin{cases} x_0 + a_0 + x_3^2 = 0, \\ x_1 + a_1 + x_0^2 = 0, \\ x_2 + a_2 + x_1^2 = 0, \\ x_3 + a_3 + x_2^2 = 0. \end{cases} \quad (6)$$

Выразим x_3 в 1-м уравнении из 4-го, затем x_2 из 3-го и x_1 из 2-го:

$x_0 = a_0 + x_3^2 = a_0 + [a_3 + x_2^2]^2 = a_0 + [a_3 + (a_2 + x_1^2)^2]^2 = a_0 + a_3^2 + a_2^4 + a_1^8 + x_0^{16}$;

$x_0^{16} + x_0 = b_0$, где $b_0 = a_0 + a_3^2 + a_2^4 + a_1^8$.

Приняв $F(x_0) = x_0^2 + x_0$, выражение $x_0^{16} + x_0$ можно представить как $F(F(F(F(x_0))))$.

Это подтверждает, что k должно является степенью 2, а не просто натуральным числом, чтобы сократились все степени, кроме 2^0 и 2^k. Представим это выражение в общем виде:

$$x_0 = a_0 + x_{k-1}^2 = a_0 + [a_{k-1} + x_{k-2}^2]^2 = \ldots = a_0 + a_{k-1}^2 + a_{k-2}^4 + \ldots + \alpha_1^{2^{k-1}} + x_0^{2^k} .$$

Таким образом, общий вид уравнения $x_0^{2^k} + x_0 = b_0$ и $b = F(F(F(\ldots(F(x)))))$, число итераций F равно k. Отсюда получаем формулу $x_0 = (F^{-1}(F^{-1}(F^{-1}(\ldots(F^{-1}(b_0))))))$, где $F^{-1}(x) = Sr(x)$.

В книге [2, с. 79] приведен пример решения квадратного уравнения суперсингулярной эллиптической кривой $Y^2 + Y = X^3 + X + 1$ над полем $GF(2^4) = GF(2)(\lambda)$, где λ есть корень неприводимого многочлена $1 + X + X^4$.

Отсюда получаем $1 + \lambda + \lambda^4 = 0$. Выразим $\lambda^4 = 1 + \lambda = (1, 0, 0, 0) + (0, 1, 0, 0) = (1, 1, 0, 0)$.

Авторы выбрали элемент $X = x = \{x_0, x_1, x_2, x_3\} = (1, 0, 0, 0)$. Подставим его в уравнение $X^3 + X + 1 = X^3 + X + (1, 0, 0, 0) = (1, 0, 0, 0)^3 + (1, 0, 0, 0) + (1, 0, 0, 0) = (1, 0, 0, 0)$. При подстановке $(1, 0, 0, 0)$ в выражение стандартного базиса λ получаем: $(1, 0, 0, 0) = 1 + 0\lambda + 0\lambda^2 + 0\lambda^3 = 1$.

Решение уравнения $y^2 + y = (1, 0, 0, 0)$ приведено в стандартном базисе $y = y_0 + y_1\lambda + y_2\lambda^2 + y_3\lambda^3$, полученные решения $(0, 1, 1, 0)$ и $(1, 1, 1, 0)$, т.е. $\lambda + \lambda^2$ и $1 + \lambda + \lambda^2$.

Решим это уравнение в нормальном базисе $\{\beta, \beta^2, \beta^4, \beta^8\}$, где β является корнем неприводимого многочлена $\beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0$, полученного с помощью симметричного квадратичного расширения многочлена $\alpha^2 + \alpha + 1 = 0$.

Итак, мы имеем уравнение $a_0\beta + a_1\beta^2 + a_2\beta^4 + a_3\beta^8 = 1$. Оно равносильно уравнению $\beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0$ в поле $GF(2^4)$, поэтому элементы $a_0 = a_1 = a_2 = a_3 = 1$.

Система (6) примет вид

$$\begin{cases} x_0 + x_3^2 = 1, \\ x_1 + x_0^2 = 1, \\ x_2 + x_1^2 = 1, \\ x_3 + x_2^2 = 1. \end{cases} \tag{7}$$

Решая ее в поле $GF(2)$, получаем два решения y_1 и y_2 этого уравнения, а именно $(0, 1, 0, 1)$ и $(1, 0, 1, 0)$, т.е. $y_1 = \beta^4 + \beta$, $y_2 = \beta^8 + \beta^2$.

Для проверки соответствия с [2] необходимо перевести полученные решения в стандартный базис $\{1, \lambda, \lambda^2, \lambda^3\}$. Порядок неприводимого многочлена $\beta^4 + \beta^3 + \beta^2 + \beta + 1$ равен пяти (ord = 5), а для многочлена $1 + X + X^4$ порядок ord = 15. Отсюда следует, что можно принять $\beta = \lambda^3$.

$y_1 = \beta^4 + \beta = \lambda^3 + \lambda^{12} = \lambda^3 + \lambda^3 + \lambda^2 + \lambda + 1 = \lambda^2 + \lambda + 1 = (1, 1, 1, 0)$;

$y_2 = \beta^8 + \beta^2 = \lambda^6 + \lambda^9 = \lambda^3 + \lambda^2 + \lambda^3 + \lambda = \lambda^2 + \lambda = (0, 1, 1, 0)$.

Этот результат совпадает с приведённым в [2].

Рассмотрим уравнение $y^2 + y = a$ при $n = 5$, $s = 2$, $k = 2^2 = 4$. Таким образом, решение будет лежать в поле $GF(2^{20})$, полученном расширением полей $GF(2^5)$ и $GF(2^4)$.

Необходимое и достаточное условие разрешимости уравнения в поле $GF(2^{20})$ есть $Tr(a) = a + a^2 + \ldots + a^{2^{19}} = (a_0\beta + a_1\beta^2 + a_2\beta^4 + a_3\beta^8) + (a_3^2\beta + a_0^2\beta^2 + + a_1^2\beta^4 + a_2^2\beta^8) + \ldots + (a_1^{16}\beta + + a_2^{16}\beta^2 + a_3^{16}\beta^4 + a_0^{16}\beta^8) = 0$. Сумма коэффициентов при степенях β будут соответственно равны следам элементов a_0, a_1, a_2 и a_3 а именно: $Tr(a_0) + Tr(a_1) + Tr(a_2) + Tr(a_3)$. В связи с линейной независимостью элементов базиса $\{\beta, \beta^2, \beta^4, \beta^8\}$ получаем: $Tr(a_0) + Tr(a_1) + Tr(a_2) + Tr(a_3) = 0$ в поле $GF(2^5)$, в силу того, что операция возведения в квадрат является автоморфизмом поля $GF(2^{20})$ (который называют автоморфизмом Фробениуса), $Tr(a_0 + a_1 + a_2 + a_3) = 0$. Отсюда имеем условие, что следы элементов a_0, a_1, a_2 и a_3 в сумме дают 0.

На основании теории, представленной выше, решение квадратного уравнения в нормальном базисе можно представить так: $x_0\beta + x_1\beta^2 + x_2\beta^4 + x_3\beta^8 = a$.

Последовательной подстановкой находим x_0:

$x_0 = Sr(b_0^2) = b_0 + b_0^2 + b_0^8 = a_0 + a_3^2 + a_2^4 + a_1^8 + a_0^2 + a_3^4 + a_2^8 + a_1^{16} + a_0^8 + a_3^{16} + a_2 + a_1^2$.

По аналогии находим другие значения: x_1, x_2, и x_3.

К примеру, $a_0 = k = (0, 1, 0, 0, 0)$; $a_1 = k^2 = (0, 0, 1, 0, 0)$; $a_2 = k = (0, 1, 0, 0, 0)$; $a_3 = k^3 = (0, 0, 0, 1, 0)$, где k – корень уравнения $k^5 + k^2 + 1 = 0$.

Найдем побитно решения первоначального квадратного уравнения:

$x_0 = k + k^6 + k^4 + k^{16} + k^2 + k^{12} + k^8 + k^{32}\ [=k] + k^8 + k^{48}\ [=k^{17}] + k + k^4 = (k^3 + k) + (k^4 + k^3 + k + 1) + + k^2 + (k^3 + k^2 + k) + (k^4 + k + 1) + k = k^3 + k = (0, 1, 0, 1, 0)$.

$x_1 = k^3 + k = (0, 1, 0, 1, 0)$, $x_2 = k^3 + k^2 = (0, 0, 1, 1, 0)$, $x_3 = k^4 + k + 1 = (1, 1, 0, 0, 1)$.

Таким образом, запишем корни уравнения $y^2 + y = a$ в поле $GF(2^{20})$ при $a_0 = k$, $a_1 = k^2$, $a_2 = k$, $a_3 = k^3$, где k – решение уравнения $k^5 + k^2 + 1 = 0$, как битовую строку: $y_1 = x_0\beta + x_1\beta^2 + x_2\beta^4 + x_3\beta^8 = = (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$.

Второй корень получим из условия линейной независимости элементов базиса путем инвертирования: $y_2 = (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$.

Заключение

Таким образом, описанный метод дает возможность быстро найти корни квадратных уравнений $x^2 + x = a$ в полях $GF(2^m)$ при любых m, что упрощает процедуру решения и сокращает временные затраты. После представления этих решений в виде битовых строк их можно передавать по каналам связи. Это позволяет унифицировать и оптимизировать процесс решения.

Итак, в данной статье рассмотрены арифметические алгоритмы, такие как построение нормальных базисов посредством симметричного квадратичного расширения конечных полей характеристики два и решение квадратных уравнений в этих полях, что имеет применение в криптографии и теории передачи информации.

Литература

1. Логачев О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. – М.: МЦНМО, 2004. – С. 41–53.

2. Болотов А.А. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – М.: КомКнига, 2006. – С. 76–81.

3. Лидл Р. Конечные поля / Р. Лидл, Г. Нидеррайтер. – В 2 т. – Т. 1: Пер. с англ. – М.: Мир, 1988. – С. 74–75.

4. Глуско Кр.Л. След и полуслед в конечных полях // Матер. науч.-техн. конф., посвящ. 55-летию УрГУПС: В 2 т. Т. 1: Екатеринбург, 2011. – вып. 97(180), – 1 электрон. опт. диск (CD-ROM). – С. 356–364.

5. Медведев Н.В. Почти-пороговые схемы разделения секрета на эллиптических кривых / Н.В. Медведев, С.С. Титов // Доклады ТУСУРа. – 2011. – № 1 (23), ч. 1. – С. 91–96.

6. Титов С.С. Генерация неприводимых многочленов, связанных степенной зависимостью корней / С.С. Титов, А.В. Торгашова // Доклады ТУСУРа. – № 2 (22), ч. 1. – С. 310–318.

7. Демкина О.Е. Рекуррентное вычисление неприводимых многочленов в задачах двоичного кодирования / О.Е. Демкина, С.С. Титов, А.В. Торгашова // Молодые ученые – транспорту: Тр. IV науч.-техн. конф. – Екатеринбург: УрГУПС, 2003. – С. 391–404.

8. Глуско К.Л. Специфика проблем связи и управления на транспорте / К.Л. Глуско, С.С. Титов // Инновационный транспорт. – Екатеринбург: УрГУПС. – 2012. – № 2 (3). – С. 44–50.

Глуско Кристина Леонидовна
Аспирант, ассистент каф. высшей и прикладной математики УрГУПСа, г. Екатеринбург
тел.: 8-922-608-52-21
Эл. почта: gluskokrl@rtural.ru

Титов Сергей Сергеевич
Д-р физ.-мат. наук, профессор каф. высшей и прикладной математики УрГУПСа
Тел.: 8-950-194-88-81
Эл. почта: sergey.titov@usaaa.ru

Glusko Kr.L., Titov S.S,

Arithmetic algorithm for solving quadratic equations in finite fields of characteristic two

The paper considers the problem of arithmetic in finite fields of characteristic two, which may have cryptographic applications. Based on the construction of normal bases by using a symmetric quadratic extension of an algorithm for solving quadratic equations by the generalized formula semitrace. Examples considered.
Keywords: finite field of characteristic two, normal basis, the formula semitrace, quadratic equation.