

УДК 681.3.06

Г.З. Халимов

Харьковский национальный университет радиотехники, Харьков

## КРИВЫЕ ФЕРМА С БОЛЬШИМ ЧИСЛОМ ТОЧЕК В РАСШИРЕННЫХ КОНЕЧНЫХ ПОЛЯХ

*Представлено решение задачи построения кривых Ферма с большим числом точек в расширенных конечных полях степени три и выше.*

**Ключевые слова:** кривые Ферма, универсальное хеширование.

### Введение

Вероятность коллизии универсального хеширования по рациональным функциям алгебраических кривых определяется отношением значения полюса базисных функций к числу точек кривой над конечным полем. Наилучший результат хеширования достигается на максимальных кривых большого рода. Максимальной кривой Ферма наибольшего рода является кривая Эрмита. Исследования по кривым Ферма широко представлены в работах [1 – 4]. В работах [1, 2] рассмотрены условия максимальной кривых Ферма, в [3, 4] – оценки параметров кривых Ферма для универсального хеширования в простом и в квадратичном поле. Максимальные плоские кривые существуют только в квадратичных полях. Актуальным является оценка параметров кривых Ферма в расширениях конечных полей степени три и выше.

**Целью статьи** является построение кривых Ферма с большим числом точек в расширенном конечном поле степени три и выше. В разделе 1 рассмотрены основные свойства кривых Ферма в кубическом поле и асимптотические границы. В разделе 2 приведены наилучшие кривые Ферма и асимптотические результаты в расширенном поле степени выше трёх.

### 1. Оценка параметров кривых Ферма в кубическом поле

Важные классы кривых Ферма для кубического поля представлены в следующих теоремах.

**Теорема 1.** Кривая

$$X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1} = 0$$

над полем  $F_q$  имеет число точек

$$N = (q-2)(q^2+q+1)^2 + 3(q^2+q+1). \quad (1)$$

**Доказательство.** Образующий элемент  $a$  поля  $F_q$  имеет порядок  $q^3-1$  и все степени  $\alpha^{q^2+q+1}$  образуют подполе порядка  $q-1$ . Решениями урав-

нения  $X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1} = 0$  будут значения  $x, y, z$ , которые удовлетворяют условиям  $Z^{q^2+q+1} = 0$ ,  $Y^{q^2+q+1} = \delta$ ,  $X^{q^2+q+1} = \eta$ ,  $\delta + \eta = 0$  или  $Z^{q^2+q+1} = 1$ ,  $Y^{q^2+q+1} = \delta$ ,  $X^{q^2+q+1} = \eta$ ,  $\delta + \eta + 1 = 0$ , где  $\delta, \eta \in F_q$ . Первое условие выполняется, если  $(\delta, \eta) = (1, -1) = (\beta^0, \beta^{(q-1)/2})$ , где  $\beta = \alpha^{q^2+q+1}$  и число решений для этой пары равно  $3(q^2+q+1)$ .

Рассмотрим решения  $(\delta, \eta) = (\beta^i, \beta^j)$ , которые определяются вторым условием. Если характеристика поля  $p \neq 2$ , тогда существуют решения  $(\delta, \eta) = ((q-1)/2, (q-1)/2)$  и их число равно  $(q^2+q+1)^2$ , из-за отсутствия перестановок. Остаются ещё  $(q-1)/2-1$  пар  $(\delta, \eta) = (\beta^i, \beta^j)$ , удовлетворяющих  $\delta + \eta + 1 = 0$  во втором условии. Число решений по этой группе с учетом перестановок по координатам будет равно

$$2((q-1)/2-1)(q^2+q+1)^2.$$

Общее число решений будет равно

$$N = (q-2)(q^2+q+1)^2 + 3(q^2+q+1).$$

Если характеристика поля  $p=2$ , тогда не существуют решения  $(\delta, \eta) = ((q-1)/2, (q-1)/2)$  и нет решения вида  $(\delta, \eta) = (1, -2)$ , удовлетворяющего условию  $Z^{q^2+q+1} = 1, Y^{q^2+q+1} = 1, X^{q^2+q+1} = -2$ . Остаются только  $(q-2)/2$  пар  $(\delta, \eta) = (\beta^i, \beta^j)$ , удовлетворяющих условию  $\delta + \eta + 1 = 0$ .

Число решений по этой группе с учетом перестановок по координатам будет равно

$$2((q-2)/2)(q^2+q+1)^2 = (q-2)(q^2+q+1)^2.$$

Общее число решений будет равно

$$N = 3(q^2+q+1) + (q-2)(q^2+q+1)^2,$$

что совпадает с (1).  $\diamond$

**Замечание 1.**

1. Кривая  $X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1} = 0$  впервые рассмотрена в [5]. Доказательство является новым.

2. Кривая имеет большое число точек, является одной из лучших в кубическом поле, но она не является максимальной кривой и имеет не очень хорошие асимптотические свойства.

**Утверждение 1.** Асимптотическая граница для отношения максимального числа точек  $N_g(q^3)$  к роду  $g$  для кривой

$$X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1} = 0$$

в кубическом поле определяется выражением

$$\limsup_{g \rightarrow \infty} N_g(q^3)/g = 2q - 4. \quad (2)$$

**Доказательство.** Род кривой по теореме Римана-Роха равен

$$g = (q^2+q)(q^2+q-1)/2.$$

Число точек определяется выражением (1)

$$N = (q-2)(q^2+q+1)^2 + 3(q^2+q+1).$$

Отношение числа точек к роду при движении  $q \rightarrow \infty$  приводит к требуемому результату.

**Утверждение 2.** Асимптотическая граница отношения максимального числа точек  $N_g(q)$  для кривой  $X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1} = 0$  в кубическом поле к максимальному числу точек по границе Хассе-Вейля определяется выражением

$$\limsup_{g \rightarrow \infty} N_g(q^3)/N_g(q^3)_{HV} = 1/\sqrt{q}. \quad (3)$$

Подставив выражение для рода  $g = (q^2+q)(q^2+q-1)/2$  в выражение Хассе-Вейля для числа точек максимальных кривых  $N_g(q^3)_{HV} = q^3 + 1 + 2g\sqrt{q^3}$ , получим выражение для

$$N_g(q)_{HV} = q^5\sqrt{q} + 2q^4\sqrt{q} - q^2\sqrt{q} + q^3 + 1.$$

Отношение числа точек кривой к максимальному числу точек по границе Хассе-Вейля при  $q \rightarrow \infty$  даёт соотношение (3).  $\diamond$

Следующая теорема определяет новую кривую Ферма с большим числом точек в кубическом поле.

**Теорема 2.** Кривая

$$X^{(q^2+q+1)/3} + Y^{(q^2+q+1)/3} + Z^{(q^2+q+1)/3} = 0$$

над полем  $F_{q^3}$  имеет число точек

$$N = (q-2)(q^2+q+1)^2/9 + (q^2+q+1). \quad (4)$$

**Доказательство.** Все степени элемента

$\gamma = a^{(q^2+q+1)/3}$ , где  $a$  – образующий элемент поля  $F_{q^3}$ , образуют мультипликативную подгруппу  $1, \gamma, \gamma^2, \dots, \gamma^{3(q-1)-1}$  порядка  $3(q-1)$ .

Так как элементы подгруппы  $\gamma^{3i}$  принадлежат подполю  $F_q$ , решениями уравнения  $X^{(q^2+q+1)/3} + Y^{(q^2+q+1)/3} + Z^{(q^2+q+1)/3} = 0$  будут те же значения  $x, y, z$ , что и для уравнения  $X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1} = 0$ , определяемые параметрами  $\delta, \eta \in F_q$ .

Других пар  $(\delta, \eta) \in \{\gamma^{3i+1}\} \cup \{\gamma^{3i+2}\}$  которые

удовлетворяли бы условиям  $Z^{(q^2+q+1)/3} = 0$ ,  $Y^{(q^2+q+1)/3} = \delta$ ,  $X^{(q^2+q+1)/3} = \eta$ ,  $\delta + \eta = 0$  или  $Z^{(q^2+q+1)/3} = 1$ ,  $Y^{(q^2+q+1)/3} = \delta$ ,  $X^{(q^2+q+1)/3} = \eta$ ,  $\delta + \eta + 1 = 0$  не существует. Покажем это.

Рассмотрим следующие возможности. Пусть условиям  $\delta + \eta = 0$  и  $\delta + \eta + 1 = 0$  удовлетворяют  $\delta = \gamma^{3i+1}$  и  $\eta = \gamma^{3j+1}$ . Подставим  $\delta, \eta$  в первое условие, получим  $\gamma^{3i+1} + \gamma^{3j+1} = 0$  и  $\gamma^{3i} + \gamma^{3j} = 0$ , что соответствует тому, что  $\delta, \eta \in F_q$ .

Подставим  $\delta, \eta$  во второе условие, получим  $\gamma^{3i} + \gamma^{3j} = -\gamma^{-1}$ . Последнее равенство не имеет места, так как  $\gamma^{-1} \notin F_q$ .

Следующая возможность определяется тем, что условиям  $\delta + \eta = 0$  и  $\delta + \eta + 1 = 0$  удовлетворяют решения  $\delta = \gamma^{3i+1}$  и  $\eta = \gamma^{3j+2}$ . Подставим  $\delta, \eta$  в первое условие, получим  $\gamma^{3i} + \gamma^{3j+1} = 0$ , что не может быть, так как  $\gamma^{3j+1} \notin F_q$ .

Подставим  $\delta, \eta$  в условие  $\delta + \eta + 1 = 0$ , получим  $\gamma^{3i+1} + \gamma^{3j+2} + 1 = 0$ . Для мультипликативной подгруппы  $1, \gamma, \gamma^2, \dots, \gamma^{3(q-1)-1}$  порядка  $3(q-1)$  справедливо равенство  $1 + \gamma + \gamma^2 = \gamma^4$  и имеем  $\gamma^{3i} + \gamma^{3i+1} + \gamma^{3i+2} = \gamma^{3(i+1)}$ . Выразим  $\gamma^{3i+1}$  из по-

следнего выражения и подставим в  $\gamma^{3i+1} + \gamma^{3j+2} + 1 = 0$ . Имеем  $\gamma^{3j+2} + \gamma^{3(i+1)} - \gamma^{3i} - \gamma^{3i+2} = 0$ . После преобразования получим  $(\gamma^{3j+2} - \gamma^{3i+2}) + (\gamma^{3(i+1)} - \gamma^{3i}) = 0$ . Первая скобка в выражении равна  $(\gamma^{3j+2} - \gamma^{3i+2}) = \gamma^2(\gamma^{3j} - \gamma^{3i}) = \gamma^2\gamma^{3k}$ , вторая  $(\gamma^{3(i+1)} - \gamma^{3i}) = \gamma^{3t}$ . Окончательно получим  $\gamma^{3k+2} + \gamma^{3t} = 0$ . Последнее равенство не имеет места, так как  $\gamma^{3k+2} \notin F_q$ .

Таким образом, решениями уравнения

$$X^{(q^2+q+1)/3} + Y^{(q^2+q+1)/3} + Z^{(q^2+q+1)/3} = 0$$

являются только пары  $\delta, \eta$ , которые принадлежат подполю  $F_q$ . Аналогично, как и в случае теоремы 1 получим число решений

$$N = (q-2)(q^2+q+1)^2/9 + (q^2+q+1). \quad \diamond$$

Асимптотические свойства кривой

$$X^{(q^2+q+1)/3} + Y^{(q^2+q+1)/3} + Z^{(q^2+q+1)/3} = 0$$

определяются утверждениями 3, 4.

**Утверждение 3.** Асимптотическая граница для отношения максимального числа точек  $N_g(q^3)$  к роду  $g$  для кривой

$$X^{(q^2+q+1)/3} + Y^{(q^2+q+1)/3} + Z^{(q^2+q+1)/3} = 0$$

в кубическом поле определяется выражением

$$\limsup_{g \rightarrow \infty} N_g(q^3)/g = 2q - 4. \quad (5)$$

Так как род кривой равен

$$g = (q^2 + q - 2)(q^2 + q - 5)/18,$$

соотношение (5) получается как предел отношения  $N_g(q^3)/g$ .  $\diamond$

**Утверждение 4.** Асимптотическая граница отношения максимального числа точек  $N_g(q^3)$  для кривой

$$X^{(q^2+q+1)/3} + Y^{(q^2+q+1)/3} + Z^{(q^2+q+1)/3} = 0$$

в кубическом поле к максимальному числу точек по границе Хассе-Вейля определяется выражением

$$\limsup_{g \rightarrow \infty} N_g(q^3)/N_{HV}(q^3) = 1/\sqrt{q}. \quad (6)$$

Доказательство результата определяется простой подстановкой.

**Замечание 2.**

1. Асимптотические свойства кривых

$$X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1} \text{ и } X^{(q^2+q+1)/3} + Y^{(q^2+q+1)/3} + Z^{(q^2+q+1)/3}$$

являются одинаковыми.

2. Кривые

$$X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1} \text{ и } X^{(q^2+q+1)/3} + Y^{(q^2+q+1)/3} + Z^{(q^2+q+1)/3}$$

имеют большое число точек, больше чем кривые Эрмита в квадратичном поле такой же мощности.

**Пример 1.** Пусть задано поле  $F_{7^3}$  и кривая

$$X^{19} + Y^{19} + Z^{19}.$$

Число точек

$$N = (q-2)(q^2+q+1)^2/9 + (q^2+q+1) = 5(7^2+7+1)^2/9 + (7^2+7+1) = 1862.$$

Точные вычисления также дают  $N = 1862$ .

**Выводы.**

1. В кубическом поле не существуют максимальные кривые Ферма, за исключением тривиального случая второй степени.

2. Для уравнений большой степени наилучший асимптотический результат достигается для кривых вида

$$X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1} \text{ и } X^{(q^2+q+1)/3} + Y^{(q^2+q+1)/3} + Z^{(q^2+q+1)/3}.$$

Универсальное хеширование в кубическом поле по кривым

$$X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1}$$

является эффективным из-за большого числа точек кривой.

**2. Кривые Ферма для расширенного поля**

Рассмотрим расширения поля выше третьего и свойства кривых Ферма в таких полях. Для уравнений Ферма степени  $m$ , когда степени элемента  $a^m$  образуют подполе ( $a$  – образующий элемент поля  $F_{q^n}$ ), существуют точные выражения для числа точек.

Практический подход к анализу кривых заключается в том, что сначала необходимо определить все разложения поля  $F_{q^n}$  по подполям меньшей размерности. В результате анализ сводится к оценкам числа решений для этих подполей, наиболее интересными случаями, являются простое поле, квадратичное и кубическое. Общий результат формулируется в теореме 3.

**Теорема 3.** Пусть задана кривая

$$X^{(q^n-1)/(q^m-1)} + Y^{(q^n-1)/(q^m-1)} + Z^{(q^n-1)/(q^m-1)} = 0$$

над полем  $F_{q^n}$  и  $q^m - 1$  является делителем  $q^n - 1$ .

Тогда число точек на кривой равно

$$N = (q^m - 2) \left( (q^n - 1)/(q^m - 1) \right)^2 + 3(q^n - 1)/(q^m - 1). \quad (7)$$

**Доказательство.** Образующий элемент  $\alpha$  поля  $F_{q^n}$  имеет порядок  $q^n - 1$  и все степени  $\alpha^{(q^n-1)/(q^m-1)}$  образуют подполе порядка  $(q^n - 1)/(q^m - 1)$ .

Решениями уравнения

$$X^{(q^n-1)/(q^m-1)} + Y^{(q^n-1)/(q^m-1)} + Z^{(q^n-1)/(q^m-1)} = 0$$

будут значения  $x, y, z$ , которые удовлетворяют условиям

$$\begin{aligned} Z^{(q^n-1)/(q^m-1)} &= 0, \quad Y^{(q^n-1)/(q^m-1)} = \delta, \\ X^{(q^n-1)/(q^m-1)} &= \eta, \quad \delta + \eta = 0, \text{ и} \\ Z^{(q^n-1)/(q^m-1)} &= 1, \quad Y^{(q^n-1)/(q^m-1)} = \delta, \\ X^{(q^n-1)/(q^m-1)} &= \eta, \quad \delta + \eta + 1 = 0, \end{aligned}$$

где  $\delta, \eta \in F_{q^{m-1}}$ .

Так как пары  $\delta, \eta$  принадлежат подполю  $F_{q^{m-1}}$  порядка  $(q^n - 1)/(q^m - 1)$ , применим тот же анализ, как и в случае теоремы 1. Для характеристики поля  $p \neq 2$ , число решений будет равно

$$\begin{aligned} N &= 3(q^n - 1)/(q^m - 1) + 2 \left( (q^m - 1)/2 - 1 \right) \times \\ &\quad * \left( (q^n - 1)/(q^m - 1) \right)^2 + \left( (q^n - 1)/(q^m - 1) \right)^2 = \\ &= (q^m - 2) \left( (q^n - 1)/(q^m - 1) \right)^2 + 3(q^n - 1)/(q^m - 1). \end{aligned}$$

В случае характеристики  $p=2$ , получим этот же результат.  $\diamond$

**Замечание 3.** Пусть  $n = 3$  и  $m = 1$ . Тогда имеем

$$X^{(q^3-1)/(q-1)} + Y^{(q^3-1)/(q-1)} + Z^{(q^3-1)/(q-1)} = 0$$

в поле  $F_{q^3}$  и получим  $X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1}$ .

Число точек  $N = (q-2) \left( (q^3-1)/(q-1) \right)^2 + 3(q^3-1)/(q-1) = (q-2)(q^2+q+1)^2 + 3(q^2+q+1)$  и это равно выражению (1).

Асимптотические свойства кривой

$$X^{(q^n-1)/(q^m-1)} + Y^{(q^n-1)/(q^m-1)} + Z^{(q^n-1)/(q^m-1)} = 0$$

определяются утверждениями 5, 6.

**Утверждение 5.** Асимптотическая граница для отношения максимального числа точек  $N_g(q^n)$  к

роду  $g$  для кривой  $X^{(q^n-1)/(q^m-1)} + Y^{(q^n-1)/(q^m-1)} + Z^{(q^n-1)/(q^m-1)} = 0$  над конечным полем  $F_{q^n}$ , где

$q^m - 1 \mid q^n - 1$ , определяется выражением

$$\limsup_{g \rightarrow \infty} N_g(q^n)/g = 2(q^m - 2). \quad (8)$$

Род кривой равен  $g = (q^n - q^m)(q^n - 2q^m + 1)/\left(2(q^m - 1)^2\right)$ , соотношение (8) получается как предел отношения  $N_g(q^n)/g$ .  $\diamond$

**Утверждение 6.** Асимптотическая граница отношения максимального числа точек  $N_g(q^n)$  для кривой

$$X^{(q^n-1)/(q^m-1)} + Y^{(q^n-1)/(q^m-1)} + Z^{(q^n-1)/(q^m-1)} = 0$$

над конечным полем  $F_{q^n}$ , где  $q^m - 1 \mid q^n - 1$  к максимальному числу точек по границе Хассе-Вейля определяется выражением

$$\limsup_{g \rightarrow \infty} N_g(q^n)/N_g(q^n)_{HV} = q^{m-n/2}. \quad (9)$$

Действительно, подставляя в выражение для границы Хассе-Вейля значение рода, получим, что для максимальной кривой

$$N_g(q^n)_{HV} = (q^m - 1)^{-2} (q^{5n/2} - 3q^{3n/2+m} + q^{3n/2} + \dots).$$

Выражение (9) следует из подстановки  $N_g(q^n) = (q^m - 2) \left( (q^n - 1)/(q^m - 1) \right)^2 + 3(q^n - 1)/(q^m - 1)$  и  $N_g(q^n)_{HV}$  в выражение  $N_g(q^n)/N_g(q^n)_{HV}$  и предела отношения при  $g \rightarrow \infty$ .  $\diamond$

### Выводы

1. Не существуют максимальные кривые Ферма в кубических полях, за исключением тривиального случая кривой второй степени, и в квадратичных полях степени большей корня квадратного размерности поля [1].

2. Наилучшими кривыми большой степени в расширенном поле являются кривые степени  $(q^n - 1)/(q^m - 1)$ , которые имеют плохие асимптотические свойства.

3. Наилучший результат по кривым Ферма в кубическом поле достигается на кривых (см. теоремы 1, 2)

- $X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1}$ ,
- $X^{(q^2+q+1)/3} + Y^{(q^2+q+1)/3} + Z^{(q^2+q+1)/3}$ .

Число точек для кривой

$$X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1}$$

над  $F_{q^3}$  равно

$$N = (q-2)(q^2+q+1)^2 + 3(q^2+q+1),$$

что больше чем для кривых Эрмита в квадратичном поле такой же мощности.

4. Асимптотические свойства кривых определяются утверждениями 1 – 4. Асимптотическая граница для отношения максимального числа точек  $N_g(q^3)$  к её роду  $g$  для кривых равна

$$\limsup_{g \rightarrow \infty} N_g(q^3)/g = 2q - 4,$$

а отношение к максимальному числу точек по границе Хассе-Вейля определяется

$$\limsup_{g \rightarrow \infty} N_g(q^3)/N_{g,HV}(q^3) = 1/\sqrt{q}.$$

По асимптотическим границам кривые Ферма в кубическом поле лучше кривых вида

$$X^{(q-1)/3} + Y^{(q-1)/3} + Z^{(q-1)/3} = 0$$

над простым полем и проигрывают кривой Эрмита для квадратичного поля. Универсальное хеширование в кубическом поле по кривым

$$X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1}$$

является эффективным из-за большого числа точек кривой.

5. Для расширения поля выше третьего наилучшими кривыми Ферма являются кривые степени  $(q^n - 1)/(q^m - 1)$ . Число точек кривой определяется теоремой 3

$$N = (q^m - 2) \left( (q^n - 1)/(q^m - 1) \right)^2 + 3(q^n - 1)/(q^m - 1).$$

### КРИВІ ФЕРМА З ВЕЛИКИМ ЧИСЛОМ ТОЧОК В РОЗШИРЕНИХ КІНЦЕВИХ ПОЛЯХ

Г.З. Халімов

Представлено рішення задачі побудови кривих Ферма з великим числом точок в розширених кінцевих полях ступеня три і вище.

**Ключові слова:** криві Ферма, універсальне гешивання.

### FERMAT CURVES WITH LARGE NUMBER OF POINTS IN EXTENDED FINITE FIELDS

G.Z. Khalimov

A solution of the problem of constructing curves farm with a large number of points in the extended finite fields, grade three and above.

**Keywords:** Fermat curves, universal hashing.

Наилучший результат по числу точек достигается на кривой

$$X^{(q^n-1)/(q-1)} + Y^{(q^n-1)/(q-1)} + Z^{(q^n-1)/(q-1)} = 0.$$

Асимптотические границы представлены утверждениями 5, 6. Асимптотическая граница для отношения максимального числа точек  $N_g(q^n)$  к роду  $g$  для кривых равна

$$\limsup_{g \rightarrow \infty} N_g(q^n)/g = 2(q^m - 2),$$

а отношение к максимальному числу точек по границе Хассе-Вейля определяется

$$\limsup_{g \rightarrow \infty} N_g(q^n)/N_{g,HV}(q^n) = q^{m-n/2}.$$

Универсальное хеширование в расширенном поле по кривым степени  $(q^n - 1)/(q^m - 1)$  является эффективным из-за большого числа точек кривой.

### Список литературы

1. Torres F. Plan maximal curves / F. Torres // *Acta Arithmetica*. – 2001. – Vol. 98, No. 2. – P. 165-179.

2. Lachaud G. Sommes d'Eisenstein et nombre de points de certaines courbes algebriques sur les corps finis / G. Lachaud // *C.R. Academia Science, Paris*. – 1987. – V.305, Serie 1. – P. 729-732.

3. Халімов Г.З. Оценки параметров кривых ферма для универсального хеширования в простом поле / Г.З. Халімов // *Научно-техническая конференция с международным участием. Компьютерное моделирование в наукоемких технологиях (часть 2). КМНТ Харьков, 18-21 мая 2010*. – С. 266

4. Халімов Г.З. Оценка параметров кривых Ферма в расширенном поле для универсального хеширования / Г.З. Халімов, А.В. Ленишин // *Защита информации: сборник научных трудов НАУ*. – К., 2010. – Вып. 17. – С. 116-120.

5. Pellikan R. The Klein quartic, the Fano plan and curves representing design / R. Pellikan // *In Codes, Curves and Signals: Common Threads in Communications*, (A. Vardy Ed.), *Kluwer Acad. Publ., Dordrecht*. – 1998. – P. 9-20.

Поступила в редколлегию 8.04.2011

**Рецензент:** д-р техн. наук, проф. И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков.