4. *Babenko L.K., Ishchukova E.A., Maro E.A.* Research about Strength of GOST 28147-89 Encryption Algorithm. – Proceedings of the 5th international conference on Security of information and networks (SIN 2012). – ACM, New York, NY, USA, 2012. – P. 138-142.
5. *Babenko L.K., Ishchukova E.A.* Differential Analysis of GOST Encryption Algorithm. – Proceedings of the 3rd International Conference of Security of Information and Networks (SIN 2010). – ACM, New York, NY, USA,2010. – P. 149-157.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: blk@fib.tsure.ru; 347928, г. Таганрог, ул. Чехова, 2, корпус "И"; тел.: 88634312018; кафедра безопасности информационных технологий; профессор.

Ищукова Евгения Александровна – e-mail: jekky82@mail.ru; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

Babenko Lyudmila Klimentevna – Southern Federal University; e-mail: blk@fib.tsure.ru; Block "I", 2, Chehov street, Taganrog, 347928, Russia; phone: +78634312018; the department of security of information technologies; professor.

Ischukova Evgeniya Aleksandrovna – e-mail: jekky82@mail.ru; phone: +78634371905; the department of security of information technologies; associate professor.

УДК 681.3.06

А.В. Бессалов, А.А. Дихтенко, О.В. Цыганкова

ПЛОТНОСТЬ КАНОНИЧЕСКИХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ СО СВОЙСТВОМ ИЗОМОРФИЗМА К ФОРМЕ ЭДВАРДСА

Кривые в форме Эдвардса наиболее интересны с точки зрения практических приложений. Удобство программирования и рекордная производительность – главные преимущества кривых данного класса перед прочими известными формами представления эллиптических кривых. В работе поставлена задача определения точного числа канонических кривых изоморфных кривым Эдвардса над простым полем. Для ее решения предложен прием, основанный на замене параметров (a, b) канонической кривой парой параметров (a, c), где c – единственный в поле корень кубического уравнения. Таким образом, найдены условия существования канонических кривых, изоморфных кривым в форме Эдвардса над простым полем. Также доказаны две леммы в теории квадратичных вычетов, построенной на схеме Гаусса. На основе полученных условий и доказанных лемм приведены точные формулы расчета числа эллиптических кривых с ненулевыми параметрами a и b, изоморфных кривым Эдвардса. Доказано, что для больших полей плотность таких кривых близка к 0,25.

Каноническая эллиптическая кривая; кривая Эдвардса; кривая кручения; параметры кривой; изоморфизм; квадратичный вычет; квадратичный невычет.

A.V. Bessalov, A.A. Dikhtenko, O.V. Tsygankova

DENSITY OF THE CANONICAL ELLIPTIC CURVES HAVING A PROPERTY OF THE ISOMORPHISM TO AN EDWARDS FORM

Edwards curves are the most interesting in terms of practical applications. The ease of programming and the best performance are their main advantages before other known forms of elliptic curves representation. A problem of determining the precise number of canonical elliptic curves which are isomorphic to Edwards curves over a prime field is posed in the paper. An approach is proposed by authors in order to solve the problem. The approach is based on substitution of canonical curve parameters (a, b) by a parameters pair (a, c), where c – is the cubic equation unique root in a field. As a result the conditions for existence canonical curves isomorphic to

Edwards curves over a prime field are found. Additionally two lemmas are proved in a quadratic residues theory, which is constructed on the Gauss scheme. The precise formulas are given in the paper for counting the number of elliptic curves with non-zero a and b parameters which are isomorphic to Edwards curves. It is proved that density of such curves for large fields is close to 0,25.

Canonical elliptic curve; Edwards curve; twisted curve; curve parameters; isomorphism; quadratic residue; quadratic non-residue.

Введение. Перспективным классом эллиптических кривых сегодня являются кривые в форме Эдвардса [1–5], рекордные по быстродействию и удобные для программирования. Двойная симметрия их в координатах поля характеристики $p > 2$ порождает четырехкратную избыточность по числу точек N_E. Так как $N_E \equiv 0 \; mod \; 4$, циклические кривые Эдвардса всегда содержат одну точку 2-го порядка и 2 точки 4-го порядка. Кривых в канонической форме с таким свойством сравнительно немного, поэтому для построения изоморфных им кривых Эдвардса следует решить задачу поиска кривых в форме Вейерштрасса с двумя точками 4-го порядка.

В работе впервые решена задача расчета точного числа эллиптических кривых в канонической форме, изоморфных кривым Эдвардса. С этой целью мы ввели зависимый от традиционных параметров (a, b) канонической кривой параметр c как единственный в поле F_p корень кубического уравнения. Далее получена системы линейных уравнений для неизвестных параметров a и c^2 с решениями, выраженными через квадратичные вычеты и невычеты. Для нахождения точного числа канонических кривых, изоморфных форме Эдвардса, потребовалось сформулировать и доказать 2 леммы о числе решений уравнений, связывающих суммы вычетов и невычетов. Доказательства опираются на схему Гаусса распределения квадратичных вычетов [6]. В итоге удалось найти формулы расчета точного числа кривых с заданными свойствами для любых $p \equiv 3 \; mod \; 4$ и $p \equiv 1 \; mod \; 4$. Кроме того, предложен алгоритм поиска изоморфных форме Эдвардса кривых, полезных для криптографии.

1. Условия, порождающие 2 точки 4-го порядка канонической кривой. Каноническая кривая над полем характеристики $p \neq 2, 3$ описывается известным уравнением [7]

$$E_p: \; y^2 = x^3 + ax + b, \; 4a^3 + 27b^2 \neq 0, a, b \; \in F_p. \qquad (1)$$

Далее потребуется операция удвоения точки $P = (x_1, y_1)$, которая дает координаты точки $2P = (x_3, y_3)$, равные:

$$\begin{cases} x_3 = v^2 - 2x_1 \\ y_3 = -y_1 - v(x_3 - x_1) \end{cases} \quad v = \frac{3\,{x_1}^2 + a}{2y_1}. \qquad (2)$$

Пусть c – единственный в поле F_p корень кубического уравнения $x^3 + ax + b = 0$. Тогда вместо (1) можем записать

$$y^2 = (x - c)(x^2 + cx + a + c^2), \qquad b = -c^3 - ac, \; c \in F_p. \qquad (3)$$

Парабола в правой части (3) не имеет корней в поле F_p, если дискриминант квадратного уравнения является квадратичным невычетом, т.е.

$$c^2 - 4(a + c^2) = -(3c^2 + 4a) \neq A^2. \qquad (4)$$

Это условие гарантирует существование единственной точки 2-го порядка кривой (3), определяемой как $D = (c, 0)$. Условие $A^2 \neq 0$, входящее в (4), исключает появление кратных корней кубического уравнения и, тем самым, сингулярные кривые [7].

Пусть $P = (x_1, y_1)$ – точка 4-го порядка. Ее удвоение в соответствии с (2) дает координаты точки $D = (c, 0)$:

$$\begin{cases} x_3 = \left(\frac{3\,{x_1}^2 + a}{2y_1}\right)^2 - 2x_1 = c; \\ y_3 = -y_1 - \left(\frac{3\,{x_1}^2 + a}{2y_1}\right)(c - x_1) = 0. \end{cases} \qquad (5)$$

Из этой системы после сокращения сомножителя $(3\,{x_1}^2 + a)$ получим квадратное уравнение для координаты x_1 точки 4-го порядка

$$ {x_1}^2 - 2cx_1 - (2c^2 + a) = 0. $$

Корни этого уравнения находятся из

$$ x_1 = c \pm \sqrt{\delta} = c \pm \sqrt{3c^2 + a}, \quad \delta = 3c^2 + a. \tag{6} $$

Из двух решений в (6) выбирается значение x_1, принадлежащее точке кривой E_p. Из (5) можно также получить формулу для вычисления координаты y_1 точки 4-го порядка

$$ {y_1}^2 = \delta(\pm 2\sqrt{\delta} + 3c). \tag{7} $$

Из (6) следует, что точка 4-го порядка существует, если дискриминант квадратного уравнения 4δ является квадратом в поле , т.е.

$$ \delta = 3c^2 + a = B^2 \neq 0. \tag{8} $$

Здесь $B^2 \neq 0$, так как иначе, согласно (7), $y_1 = 0$ и получаем еще одну точку 2-го порядка. Теперь условия существования точек 2-го и 4-го порядков (4) и (8) можно выразить через символы Лежандра как

$$ \text{a)} \left(\frac{-(3c^2+4a)}{p}\right) = -1; \text{ b)} \left(\frac{\delta}{p}\right) = \left(\frac{(3c^2+a)}{p}\right) = 1. \tag{9} $$

Возникает вопрос: для какого числа канонических кривых существует изоморфизм с кривыми Эдвардса при любых значениях порядка поля p и какова плотность таких кривых? Иными словами, какое точное число кривых Эдвардса над простым полем?

2. Точное число кривых в канонической форме, изоморфных кривым Эдвардса. Для определения точного числа эллиптических кривых в форме Вейерштрасса (1), имеющих ровно 2 точки 4-го порядка, необходимо обратиться к некоторым результатам теории чисел. Г. Дэвенпорт в своей работе [6] приводит блестящее доказательство распределения квадратичных вычетов, полученное Гауссом. Рассмотрим схему Гаусса и итоги его анализа.

Произведение $n(n+1) mod\, p,\ n = 1, 2, 3, \dots, p-1,$ включает составляющие BB (оба сомножителя – квадратичные вычеты) с общим числом (BB), HH (оба сомножителя – квадратичные невычеты) с числом (HH), и смешанные пары BH и HB с числом (BH) и (HB). Гаусс доказал, что имеет место система уравнений:

$$ (BB) + (BH) = \frac{p-2-\varepsilon}{2}, \quad \varepsilon = (-1)^{\frac{p-1}{2}}, \tag{10} $$

$$ (HB) + (HH) = \frac{p-2+\varepsilon}{2}, \tag{11} $$

$$ (BB) + (HB) = \frac{p-3}{2}, \tag{12} $$

$$ (BH) + (HH) = \frac{p-1}{2}, \tag{13} $$

$$ (BB) + (HH) - (BH) - (HB) = -1. \tag{14} $$

Здесь первые 4 уравнения не являются линейно независимыми (суммы первой и второй пар уравнений совпадают), поэтому добавлено 5-е уравнение. Из этой системы легко найти любую из 4-х неизвестных. Комбинируя (10)-(14), можно получить:

$$ (BB) = \frac{p-4-\varepsilon}{4}, \quad (BH) = \frac{p-\varepsilon}{4}, \tag{15} $$

$$ (HB) = (HH) = \frac{p-2+\varepsilon}{4}, \quad \varepsilon = (-1)^{\frac{p-1}{2}}. \tag{16} $$

Сумма всех сочетаний вычетов и невычетов равна

$(BB) + (HH) + (BH) + (HB) = p - 2$, так как для сомножителя $(n+1)$ в произведении $n(n+1)$ последний элемент равен 0 (он исключается из решений). В нашей задаче потребуются два результата, которые докажем как две приведенные ниже леммы.

Лемма 1. *Уравнение* $X^2 - C^2 = Y^2 mod\ p$ *при всех ненулевых квадратах* X^2, C^2 *и* Y^2 *и фиксированном* C^2 *имеет ровно* $\frac{p-4-(-1)^{\frac{p-1}{2}}}{4}$ *решений для квадратов.*

Доказательство. Воспользуемся схемой Гаусса для сомножителей $n(n+1) mod\ p$. Очевидно, что все результаты обобщаются на произведение $n(n+C)$ при любом C. Уравнение $X^2 - C^2 = Y^2$ можно записать как $\left(\left(\frac{X}{C}\right)^2 - 1\right) = \left(\frac{Y}{C}\right)^2$. Оно отвечает схеме Гаусса при $n = \frac{X}{C}$. Когда $\frac{X}{C}$ пробегает все ненулевые значения $1, 2, \ldots\ p-1$, их квадраты являются квадратичными вычетами $n^2 = 1, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$. Как следует из уравнения, значения $\left(\left(\frac{X}{C}\right)^2 - 1\right)$ при этом должны быть также квадратичными вычетами. Эта ситуация отвечает событиям BB в схеме Гаусса, а их число (BB) определяется формулой (15). Оно же определяет число $\frac{p-4-(-1)^{\frac{p-1}{2}}}{4}$ ненулевых решений для квадратов уравнения $X^2 - C^2 = Y^2$. Лемма 1 доказана.

Лемма 2. *Уравнение* $X^2 + C = Y^2 mod\ p$ *при всех ненулевых квадратах* X^2 *и* Y^2 *и фиксированном квадратичном невычете* C *имеет ровно* $\frac{p-2+(-1)^{\frac{p-1}{2}}}{4}$ *решений для квадратов.*

Доказательство. После замены $Z = X^{-1}$, $V = YX^{-1}$, $X \neq 0$, уравнение примет вид $CZ^2 + 1 = V^2$. В схеме Гаусса, если CZ^2 пробегает все $\frac{p-1}{2}$ значений квадратичных невычетов, элементы $(CZ^2 + 1)$ согласно нашему уравнению должны быть вычетами. Приходим к ситуации HB в схеме Гаусса с числом $(HB) = \frac{p-2+(-1)^{\frac{p-1}{2}}}{4}$, которое определяется формулой (16). Лемма 2 доказана.

Перейдем теперь к вычислению числа кривых с ненулевыми параметрами *a* и *b*, изоморфных кривым Эдвардса.

Утверждение. Число кривых (1) в канонической форме с параметрами $a \neq 0$ и $b \neq 0$ над полем F_p с двумя точками 4-го порядка определяется формулами:

I. При $p = 3\ mod\ 4$

(α) $M_\propto = \frac{(p-1)(p-7)}{4}$, если $\left(\frac{3}{p}\right) = 1$;

(β) $M_\beta = \frac{(p-1)(p-3)}{4}$, если $\left(\frac{3}{p}\right) = -1$;

II. При $p = 1\ mod\ 4$

(γ) $M_\gamma = \frac{(p-1)^2}{4}$.

Доказательство.

I. Пусть $p = 3\ mod\ 4$, тогда (-1) – квадратичный невычет [7], т.е. $\left(\frac{-1}{p}\right) = -1$, и для (9а) невычет заменяем квадратичным вычетом

$$\left(\frac{-1}{p}\right)\left(\frac{(3c^2 + 4a)}{p}\right) = \left(\frac{-1}{p}\right) \quad \Rightarrow \quad \left(\frac{(3c^2 + 4a)}{p}\right) = 1.$$

Аргументы символов Лежандра (9) являются линейными функциями параметров *a* и c^2, следовательно, имеем невырожденную систему двух линейных уравнений над полем F_p с решениями:

$$\begin{cases} 3c^2 + 4a = A^2 \\ 3c^2 + a = B^2 \end{cases} \Rightarrow \begin{cases} a = 3^{-1}(A^2 - B^2) \\ c^2 = 9^{-1}(4B^2 - A^2) \end{cases} \qquad (17)$$

Для кривых с параметрами $a \neq 0$ и $b \neq 0$ квадратичные вычеты $A^2 \neq B^2$ и, кроме того, $4B^2 \neq A^2$ (нулевые вычеты c^2 отбрасываются, так как из $c = 0 \Rightarrow b = -c^3 - ac = 0$). Из (9) следует, что $A^2 \neq 0$ и $B^2 \neq 0$.

Построим квадратную таблицу из упорядоченных $\frac{p-1}{2}$ значений всех B^2 (по столбцам) и A^2 (по строкам). В клетки таблицы запишем значения $(4B^2 - A^2)$ из (17), так что на главной диагонали оказываются элементы $3A^2$, которые по условию $A^2 \neq B^2$ отбрасываются из искомых решений. Кроме того, в каждой строке имеем ровно один 0, который также отбрасывается. Требуется найти число ν ненулевых недиагональных квадратов в строке, что дает решения для значений c^2 в (17). Общее число решений по всем строкам, очевидно, равно $\mu = \nu\frac{p-1}{2}$. Для примера приведено такое построение для $p = 11$, табл. 1.

Таблица 1

Возможные значения величины $(4B^2 - A^2)$ при $p = 11 \equiv 3\ mod\ 4$

A^2 \ B^2	**1**	**4**	**9**	**5**	**3**
1	3	4	2	8	0
4	0	1	10	5	8
9	6	7	5	0	3
5	10	0	9	4	7
3	1	2	0	6	9

Из доказанной леммы 1 следует, что число ненулевых квадратов в каждой строке таблицы при $p \equiv 3\ mod\ 4$ равно $\frac{p-3}{4}$. В табл. 1 таких квадратов по 2 в каждой строке. На главной диагонали со значениями $3A^2$ имеем квадратичные вычеты, если 3 – квадрат в поле, и невычеты в противном случае. Поскольку диагональные элементы отбрасываются из решений, в каждой строке остается $\nu = \frac{(p-3)}{4} - 1 = \frac{p-7}{4}$ при $\left(\frac{3}{p}\right) = 1$ либо $\nu = \frac{(p-3)}{4}$ при $\left(\frac{3}{p}\right) = -1$. Общее число решений для ненулевых квадратов по всем строкам, таким образом, составляет

$$\mu_{\propto} = \frac{(p-1)(p-7)}{8}, \text{ при } \left(\frac{3}{p}\right) = 1 \text{ и } \mu_{\beta} = \frac{(p-1)(p-3)}{8}, \text{ при } \left(\frac{3}{p}\right) = -1.$$

Число эллиптических кривых M_{α}, M_{β} с заданными свойствами вдвое выше этих значений, так как каждому решению для c^2 отвечают два корня кубика $\pm c$ и, соответственно, два коэффициента кривой $\pm b$. Две первые формулы утверждения доказаны. Заметим, что $\left(\frac{3}{p}\right) = 1$ для всех $p \equiv \pm 1\ mod\ 12$ [6]. В частности, 3 является квадратичным вычетом при $p = 11, 13, 23, 47$ и др.

II. Пусть теперь $p = 1\ mod\ 4$, тогда (-1)– квадратичный вычет, т.е. $\left(\frac{-1}{p}\right) = 1$ [7]. Тогда для (9а), принимая A невычетом в системе уравнений, можно найти ее единственное решение

$$\begin{cases} 3c^2 + 4a = A \\ 3c^2 + a = B^2 \end{cases} \left(\frac{A}{p}\right) = -1 \Rightarrow \begin{cases} a = 3^{-1}(A - B^2); \\ c^2 = 9^{-1}(4B^2 - A^2). \end{cases} \quad (18)$$

Здесь, как видим, нулевые решения для a и c^2 невозможны. Остается лишь найти число квадратов в таблице ненулевых значений $(4B^2 - A)$. Если принять $B^2 = 0$, в формуле для c^2 вновь получим невычет в правой части, поэтому и в данном случае учитываем лишь ненулевые элементы A и B^2.

Подобно п.1 построим квадратную таблицу из $\frac{p-1}{2}$ значений всех B^2 (по столбцам) и невычетов A (по строкам). В клетки таблицы запишем значения $(4B^2 - A)$ из (18), все не равные 0. Необходимо найти число ν квадратов в строке,

что дает решения для значений c^2 в (18), и умножить это значение на число строк. Пример такого построения для $p = 13$ дан в табл. 2.

Из леммы 2 следует, что уравнение $4B^2 - A = Y^2$ с ненулевыми вычетами и фиксированным невычетом A имеет $\nu_\gamma = \frac{p-2+(-1)^{\frac{p-1}{2}}}{4}$ решений. Это значение равно числу квадратов в каждой строке таблицы, тогда с учетом $(-1)^{\frac{p-1}{2}} = 1$ при $p \equiv 1\ mod\ 4$ получаем общее число решений уравнения

$$\mu_\gamma = \nu_\gamma \frac{p-1}{2} = \frac{(p-1)^2}{8}.$$

Таблица 2

Возможные значения величины $(4B^2 - A)$ при $p = 13 \equiv 1\ mod\ 4$

A \ B^2	**1**	**4**	**9**	**3**	**12**	**10**
2	2	1	8	10	7	12
5	12	11	5	7	4	9
6	11	10	4	6	3	8
7	10	9	3	5	2	7
8	9	8	2	4	1	6
11	6	5	12	1	11	3

Как отмечалось выше, число кривых M_γ с заданными свойствами вдвое превосходит μ_γ. Итак, сформулированное утверждение доказано. Важно отметить, что формулы утверждения определяют точное число кривых Эдвардса над простым полем.

Замечание. За формулировку и доказательство лемм 1 и 2 и утверждения берет на себя ответственность первый автор статьи.

Рассчитанные по формулам (α), (β), (γ) мощности семейств кривых, изоморфных кривым Эдвардса при значениях $p = 7, 11, 13, \ldots, 47$ приведены в табл. 3.

Таблица 3

Мощности семейств кривых, изоморфных кривым Эдвардса

p	7	11	13	17	19	23	29	31	37	41	43	47
M	6	10	36	64	72	88	196	210	324	400	420	529

Пример. Требуется найти кривую с двумя точками 4-го порядка над полем F_{11}. Примем с учетом данных табл. 1 $A^2 = 1$, $B^2 = 4$, тогда согласно (17) $c^2 = 9$ – квадрат в поле, $a = 10$ и $b = \pm c(c^2 + a) = \pm 2$. Получили пару кривых кручения $y^2 = x^3 + 10x \pm 2$ с порядками $N_E = 8$ и $N_{E^t} = 16$. Их точки второго порядка $D = (-3, 0)$ и $D^t = (3, 0)$, а координаты точки 4-го порядка первой кривой в соответствии с (6), (7) равны $x_1 = c \pm \sqrt{\delta} = -3 \pm 2$, $x_1 = 6$, $y_1 = \pm 5$. Здесь решения, не лежащие на кривой, отбрасываются. Вообще нал полем F_{11} существует, как следует из табл. 3, 10 кривых с ненулевыми параметрами a и b и двумя точками 4-го порядка.

Так как общее число всех кривых с ненулевыми a и b за вычетом редких сингулярных кривых с нулевым дискриминантом близко $(p-1)^2$, плотность кривых, изоморфных кривым Эдвардса, для больших полей практически равна четверти всех эллиптических кривых. Формулы (17), (18) конструктивны, так как позволяют рассчитывать параметры a и $\pm c$ кривой (и, соответственно, $\pm b$) при заданных значениях пар (A^2, B^2) или (A, B^2). На основе условий (9) и формул (17), (18) можно предложить следующий алгоритм построения канонических кривых с двумя точками 4-го порядка:

1. В поле F_p задаются произвольное значение пары квадратичных вычетов (A^2, B^2) или пары (A, B^2) и согласно (17) или (18) рассчитываются параметры a и c^2. Если вычисленное значение c^2 – невычет, меняем параметр B^2 и повторяются расчеты.

2. Если c^2 – квадратичный вычет, находятся 2 кривые с параметрами $(a, \pm c)$ и $(a, \pm b)$. Значение параметра b рассчитываются в соответствии с (3).

3. Находятся координаты точки 4-го порядка (для построения изоморфной кривой Эдвардса).

4. Вычисляется порядок одной из кривых и, в случае неприемлемого порядка, рассчитывается порядок кривой кручения. Если решение не найдено, используется другая пара значений (A^2, B^2) или (A, B^2) (возвращаемся в п.1).

В предложенном виде алгоритм достаточно быстро приводит к кривой с двумя точками 4-го порядка. Далее, как описано в [3], строится изоморфная кривая в форме Эдвардса.

Выводы. Показано, что задача поиска кривой Эдвардса сводится к задаче построения изоморфной канонической кривой с единственной точкой 2-го порядка и двумя точками 4-го порядка. Получены точные формулы расчета числа эллиптических кривых, изоморфных кривым Эдвардса над простым полем. Они определяют точное число кривых Эдвардса. Приведен простой алгоритм поиска канонических кривых, изоморфных кривым Эдвардса над простым полем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Edwards H.M.* A normal form for elliptic curves // Bulletin of the American Mathematical Society. – July 2007. – Vol. 44, № 3. – P. 393-422.
2. *Bernstein Daniel J., Lange Tanja.* Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007. – P. 1-20.
3. *Бессалов А.В.* Число изоморфизмов и пар кручения кривых Эдвардса над простым полем // Радиотехника. – 2011. – Вып. 167. – С. 203-208.
4. *Бессалов А.В., Гурьянов А.И., Дихтенко А.А.* Кривые Эдвардса почти простого порядка над расширениями малых простых полей // Прикладная радиоэлектроника. – 2012. – Т. 11, № 2. – С. 225-227.
5. *Бессалов А.В., Дихтенко А.А.* Криптостойкие кривые Эдвардса над простыми полями // Прикладная радиоэлектроника. – 2013. – Т. 12, № 2. – С. 285-291.
6. *Дэвенпорт Г.* Высшая арифметика: введение в теорию чисел: Пер. с англ. / Под ред. Ю.В. Линника. – М.: Наука, 1965. – 176 с.
7. *Бессалов А.В., Телиженко А.Б.* Криптосистемы на эллиптических кривых: Учеб. пособие. – Киев: ІВЦ «Політехніка», 2004. – 224 с.

Статью рекомендовал к опубликованию к.т.н. Б.К. Третьяков.

Бессалов Анатолий Владимирович – ФТИ НТУУ «КПИ»; e-mail: bessalov@ukr.net; 03056, Киев, пр. Победы, 37; тел.: +380509765173; кафедра ММЗИ; д.т.н.; профессор.

Цыганкова Оксана Валентиновна – e-mail: oksana.valent@gmail.com; тел.: +380664046054; кафедра ММЗИ; аспирантка.

Дихтенко Алиса Анатольевна – Донецкий национальный университет; e-mail: alice.dikhtenko@gmail.com; 83001, Украина, Донецк, ул. Университетская, 24; тел.: +380665628864; кафедра ТУ и ВМ; аспирантка.

Bessalov Anatoliy Vladimirovich – FTI NTUU “KPI”; e-mail: bessalov@ukr.net; 57, pr. Pobedy’, Kiev, 03056, Ukraine; phone: +380509765173; the department of MMIS; dr. of eng. sc.; professor.

Tsygankova Oksana Valentinovna – e-mail: oksana.valent@gmail.com; phone: +380664046054; the department of MMIS; postgraduate student.

Dikhtenko Alisa Anatol’evna – Donetsk National University; e-mail: alice.dikhtenko@gmail.com; 24, Universitetskaya street, Donetsk, 83001, Ukraine; phone: +380665628864; the department of the ET and CM; postgraduate student.