УДК 681.3.06

 *А.В. Бессалов, д-р техн. наук, О.В. Цыганкова*

**СУПЕРСИНГУЛЯРНЫЕ ПОЛНЫЕ КРИВЫЕ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ**

Дан анализ условий существования суперсингулярных полных кривых Эдвардса над простым полем. сформулированы и доказаны 3 теоремы об условиях существования суперсингулярных кривых с j-инвариантами, равными

*Ключевые слова*: суперсингулярная кривая, полная кривая Эдвардса, скрученная кривая Эдвардса, квадратичная кривая Эдвардса, пара кручения, порядок точки, символ Лежандра, квадратичный вычет, квадратичный невычет

 **Введение**

Эллиптические кривые в форме Эдвардса над простым полем наиболее перспективны для современных криптосистем. Производительность операции экспоненцирования точки такой кривой в среднем более чем в 1.5 раза выше, чем для кривой в форме Вейерштрасса [1]. Арифметика этих кривых и ее программирование существенно упрощаются в связи с наличием нейтрального элемента группы как аффинной точки кривой О = (1,0).

Суперсингулярные эллиптические кривые, интерес к которым сначала был потерян в начале 90-х годов в связи с уязвимостью к MOV-атаке изоморфизма [2], в начале нынешнего столетия стали основой криптографии на спаривании точек эллиптической кривой [3]. Несомненные технологические преимущества кривых в форме Эдвардса делают актуальной задачу исследования свойств суперсингулярных кривых этого типа.

В настоящей работе дан анализ свойств суперсингулярных кривых одного из классов кривых в обобщенной форме Эдвардса [1] над простым полем – полных кривых Эдвардса. В разделе 1 вводятся основные понятия и определения в соответствии с новой классификацией кривых Эдвардса [1]. В разделе 2 сформулированы и доказаны 3 теоремы об условиях существования суперсингулярных кривых с j-инвариантами, равными

1. **Кривые в обобщенной форме Эдвардса и суперсингулярные кривые**

В работе [4] *скрученные кривые Эдвардса* (*twisted Edwards curves*) определены как обобщение кривых Эдвардса *х*2 + *у*2 = 1 + *dx*2*y*2 [5] путем ввода нового параметра *a* в уравнение

E*a*,*d* : *ах*2 + *у*2 = 1 + *dx*2*y*2 , *a,d* ∈Fp\*, *d* ≠ 1, *a ≠ d* , *p* ≠ 2.

 Наряду с вводом параметра *а* авторы [4] сняли ограничения на пару параметров *a* и *d*, допуская любые значения Здесь и далее символ Лежандра элемента [3]. При *а* = 1 такая кривая получила в [4] название *кривой Эдвардса*, а если у нее *d –* квадратичный невычет (т.е. ),то – *полной кривой Эдвардса*. Этот термин связан с полнотой закона сложения точек кривой [5]. В работе [6] мы предложили поменять местами координаты *х* и *у* в форме кривой Эдвардса с целью сохранения горизонтальной симметрии обратных точек, принятой в теории эллиптических кривых. Опираясь на это свойство, определим *кривую в обобщенной форме Эдвардса* уравнением

: , *a,d* ∈Fp\*, *d*(*d – a*)≠ 0, *d* ≠ 1, *p* ≠ 2. (1)

Тогда модифицированный универсальный закон сложения точек имеет вид

 . (2)

При совпадении двух точек получим из (2) закон удвоения точек

 . (3)

Определяя теперь обратную точку как – *Р =* (*x*1, –*y*1), получаем согласно закона (2) координаты нейтрального элемента группы (*x*1, *y*1) + (*x*1, –*y*1) = О = (1, 0). На оси *х* также всегда лежит точка *D*0= (–1, 0) второго порядка, для которой в соответствии с (3) 2*D*0= (1, 0) = О. В зависимости от свойств параметров *a* и *d* можно получить еще 2 особые точки второго порядка и 2 особые точки 4-го порядка. Как следует из (1), на оси *y* могут также лежать не особые точки 4-го порядка ±*F*0 **=** (0, ±1/), для которых ±2*F*0 = *D*0= (–1, 0). Эти точки существуют над полем , если параметр *а* является квадратом (квадратичным вычетом).

Согласно нашей классификации кривых в форме (1), обоснованной в работах [1,7,8], скрученная кривая имеет параметры *a* и *d* со свойствами квадратичных невычетов тогда как при *a* = 1 определены полные кривые Эдвардса с параметром *d*, являющимся квадратичным невычетом и квадратичные кривые Эдвардса, для которых Полные кривые Эдвардса являются циклическими в отношении точек четных порядков и не содержат особых точек. Важно, что нециклические скрученные и квадратичные кривые Эдвардса образуют пары квадратичного кручения, параметры которых связаны линейным преобразованием [1,8]. Этим свойством удобно пользоваться при анализе суперсингулярных кривых этих классов, для которых можно принять и ограничиться одним параметром со свойством . Другими словами, анализ суперсингулярных кривых двух классов – скрученных и квадратичных кривых Эдвардса – сводится к анализу последних с одним параметром

Порядок эллиптической кривой над конечным полем определяется на основе следа уравнения Фробениуса как Для кривой квадратичного кручения соответствующий порядок будет равным . Эллиптическая кривая является суперсингулярной тогда и только тогда, когда над любым расширением простого поля . . Иными словами, в алгебраическом замыкании суперсингулярная кривая не содержит точек порядка . Над простым полем такая кривая всегда имеет порядок а над любым расширением этого поля

 Для кривой

 *E*: (4)

в форме Вейерштрасса с j-инвариантом

 (5)

характерными являются значения при и при . Эти значения j-инварианта часто (но не всегда) порождают суперсингулярную кривую.

Изоморфизм кривых в формах (1) и (4) достигается лишь приблизительно для четверти всех кривых в форме Вейерштрасса, содержащих одну иди 3 точки 2-го порядка. Порядок таких кривых Наиболее удобной формой их представления является кривая в форме Монтгомери [4]

  , , , , , (6)

Как частный случай канонической кривой (4) в форме Вейерштрасса, уравнение (6) часто используется при анализе свойств кривой в обобщенной форме Эдвардса (1). Так как кривые (1) и (6)) изоморфны () [1,4], доказательства условий существования таких суперсингулярных кривых равнозначны.

Для кривой (1) j-инвариант равен

 , . (7)

Так как j–инвариант сохраняет свое значение для всех изоморфных кривых и пар квадратичного кручения , он является полезным инструментом при поиске суперсингулярных кривых. Как отмечалось, для этих целей параметр в (7) является избыточным, т.е. можно принять и рассматривать свойства лишь полных и квадратичных кривых Эдвардса. Если квадратичная кривая – суперсингулярная, то и соответствующая ей скрученная кривая (как нара квадратичного кручения) – также суперсингулярная. В этой связи в дальнейшем мы принимаем и будем пользоваться j-инвариантом

 Одним из свойств j-инварианта является

 (8)

Это свойство легко доказать, обращая элемент в (7) и умножая числитель и знаменатель на после чего можно получить равенство (8) Как известно, инверсия параметра дает кривую квадратичного кручения для полной кривой Эдвардса [5], и изоморфную – для квадратичной кривой Эдвардса [1].

1. **Условия существования суперсингулярных полных кривых Эдвардса**

Порядок кривых Эдвардса поэтому суперсингулярные кривые в форме Эдвардса с порядком существуют лишь при . Поэтому в данной работе мы рассматриваем лишь этот случай.

Полная кривая Эдвардса определена в работах [4,5] как частный случай кривой (1)

E1,*d* : , *d* ∈Fp\*, *d*(*d –* 1)≠ 0,  (9)

Характерными свойствами этого класса кривых являются цикличность группы точек четного порядка и отсутствие особых точек (или полнота закона сложения точек) [5].

**2.1. Суперсингулярные полные кривые Эдвардса с нулевым j–инвариантом**

Такие кривые изоморфны подклассу кривых (4) в форме Вейерштрасса вида с j-инвариантом (5), равным 0. Хотя любая кривая этого вида имеет нулевой j-инвариант, не все они являются суперсингулярными. Кроме того, не любая из этих кривых сводится к форме Монтгомери (6).

**Теорема 1.** *При* *полная кривая Эдвардса над простым полем с нулевым j–инвариантом* и *с параметрами является суперсингулярной.*

**Доказательство.** При нулевом значении j-инварианта (7) решения для параметра кривой определяются корнями квадратного уравнения

 (10)

Отсюда следует, что кривые с нулевым j-инвариантом существуют лишь при существовании элемента простого поля Элемент 3 является квадратичным вычетом при [11]. При имеет место сравнение при этом кривые Эдвардса несуперсингулярны. Итак, в условиях теоремы кривая с параметрами (10) имеет нулевой инвариант .

Докажем, что порядок кривой в условиях теоремы Сначала покажем, что при выполнении сравнения выполняется и условие . Действительно, из следует Далее, любая кривая с нулевым j-инвариантом (5) изоморфна кривой (4) вида При выполнении условия теоремы справедливо также сравнение , тогда порядок мультипликативной группы поля не делится на 3. При этом группа не содержит подгруппы (и, соответственно, элементов) 3-го порядка и НОД( [12]. Если примитивный элемент мультипликативной группы поля , то и –также примитивный элемент. В уравнении для всех правая часть уравнения при любом *В* пробегает все те же значения. Из них квадратичных вычетов, которые дают ровно точек кривой, элемент 0 из множества значений дает одну точку 2-го порядка, тогда с добавлением точки на бесконечности получаем порядок кривой Подчеркнем, что данная кривая циклическая с одной точкой 2-го порядка и двумя точками 4-го порядка (т.к. при имеет место 4|и, следовательно, она изоморфна полной кривой Эдвардса, при этом все корни в (10) – квадратичные невычеты. Таким образом, в условиях теоремы кривая (1), изоморфная кривой в форме Вейерштрасса имеет порядок и, следовательно, является суперсингулярной.

Если в уравнении принять = можно получить изоморфную кривой (4) кривую (6) в форме Монтгомери вида

Делением на она приводится к виду (6)

Тогда с учетом уравнения (6) из равенства получаем

и два решения для этого параметра

 . (11)

Эти значения совпадают с решениями (10), в чем можно убедиться умножением числителя и знаменателя в (11) на тогда . Аналогично получаем и второе решение для инверсии В произведении один из сомножителей – квадратичный вычет, другой – квадратичный невычет, так как и [9]. Это доказывает, что параметры (10) – квадратичные невычеты и кривая входит в класс полных кривых Эдвардса . Теорема доказана. ▲

В таблице 1 в качестве примера приведены значения в первой сотне чисел, для которых справедливы условия теоремы, вместе со взаимно обратными значениями вычисленными согласно (10). Они определяют все суперсингулярные полные кривые Эдвардса с нулевым j-инвариантом и порядком .

 Таблица 1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 11 | 23 | 47 | 59 | 71 | 83 |
|  | (2, 6) | (11,21) | (39,41) | (8,37) | (23,34) | (24,45) |

Все полные кривые Эдвардса с нулевым j-инвариантом при (при этом ) являются несуперсингулярными. Это очевидно, так как в этом случае не делится на 4.

**2.2. Суперсингулярные полные кривые Эдвардса с j–инвариантом**

Приведем условия существования суперсингулярных кривых этого класса.

**Теорема 2.** *При* *полная кривая Эдвардса над простым полем с j-инвариантом* и *с параметром является суперсингулярной.*

**Доказательство. Д**ля кривой в форме Вейерштрасса (4) вида согласно (5) получаем Изоморфизм с полной кривой Эдвардса здесь существует лишь в случае, если тогда кривая (4) сводится к форме Монтгомери (6). Разделим правую часть уравнения (4) при на , тогда после замены приходим к кривой (6) вида , при этом Отсюда следует, что Это значение есть квадратичный невычет при , и изоморфная кривой (6) кривая (1) – полная кривая Эдвардса.

С другой стороны, суперсингулярные кривые над простым полем со следом Фробениуса изоморфны своему квадратичному кручению: Переход к кривой кручения в классе полных кривых Эдвардса достигается, как отмечалось, обращением параметра Тривиальным примером суперсингулярной кривой в этом классе является значение , найденное выше для кривой в форме Монтгомери. В этом случае пара квадратичного кручения вырождается в одну кривую, след Фробениуса и порядок кривой . Теорема доказана. ▲

Для пары согласно (7) получим

 .

Заметим, что кривая (4) при может оказаться нециклической (с тремя точками 2-го порядка), но всегда является суперсингулярной при [9].

В общем случае для нахождения кривой Эдвардса с j-инвариантом в соответствии с (7) следует решить уравнение 6-й степени

 (11)

Уравнение (11) может дать до 6 корней или 3 пары взаимно-обратных значений Пары корней, являющихся квадратичными невычетами, отвечают полной кривую Эдвардса, в противном случае – квадратичной кривой. Как следует из приведенного выше анализа, существует единственная полная кривая Эдвардса с j-инвариантом при (этот корень уравнения (11) имеет кратность 2).

Значениями не исчерпываются все суперсингулярные кривые. В работах [1,6] мы обнаружили и привели доказательство теоремы об условии существования полной суперсингулярной кривой с параметрами . Здесь мы дадим новое строгое доказательство этой теоремы.

**2.3. Суперсингулярные полные кривые Эдвардса с j–инвариантом**

Принимая разделим уравнение (9) на тогда получим

 (12)

Иногда это уравнение удобней записать в форме

Для квадратичной кривой Эдвардса отсюда сразу определяются координаты особых точек

 После исключения 4-х базовых точек () суперсингулярные кривые следует искать на основе нахождения числа решений уравнения (12) со значениями параметра , дающими одинаковое число решений (это справедливо для полных кривых, у которых замена дает пару квадратичного кручения [5] ).

Уравнение (12) можно использовать для поиска параметров суперсингулярных кривых, для которых подмножества левой и правой части уравнения, включающие квадратичные вычеты и невычеты, пересекаются, т.е. содержат одинаковые элементы. Такой подход требует изучения свойств множества c учетом структуры полных кривых Эдвардса (без особых точек) и квадратичных кривых Эдвардса (с особыми точками 2-го и 4-го порядков). В данной работе мы рассматриваем лишь первый класс этих кривых. Подобный же анализ для квадратичных и скрученных кривых Эдвардса мы дадим в следующей работе.

Обозначим множество всех элементов в знаменателе (12) как

 }. (13)

Мощность этого множества

Пусть

 –

множество всех ненулевых квадратов, и, соответственно, – множество всех квадратичных невычетов. При очевидно, = –.

Множество (13) является суммой непересекающихся подмножеств квадратичных вычетов из множества

 } (14)

и невычетов

 } (15)

с элементами из множества квадратичных невычетов. Мы рассматриваем множества как наборы элементов поля , вычисленных при различных значениях

Для доказательства теоремы нам потребуются доказать следующие леммы.

**Лемма 1.** *При р* ≡ 3mod4 *мощности множеств ненулевых квадратов*  } и квадратичных невычетов } одинаковы и равны . .

**Доказательство.** Число решений уравнения определяется числом квадратов в правой части. Подобная задача была нами рассмотрена в работе [13]. Согласно лемме 2 этой работы при *р* ≡ 3mod4 число ненулевых квадратичных вычетов в множестве элементов равно (*p* – 3)/4. При (, не входящий в число вычетов, поэтому число ненулевых квадратичных вычетов равно (*p* – 3)/4. Так как по условию то множество всех элементов мощности (*p* – 3)/2 содержит равное число (*p* – 3)/4 квадратичных вычетов и невычетов, т.е. . Лемма доказана.

Очевидно, что утверждение леммы инвариантно к замене

**Лемма 2.** *При р* ≡ 3mod8 *множество ненулевых квадратов*  и множество квадратичных невычетов содержат *ровно по* *пар взаимно-обратных элементов.*

**Доказательство.** Пусть для некоторого существует элемент из множества такой, что . Тогда элементы взаимно-обратны. Уравнение для можно записать как

 ,

или

 (16)

Согласно лемме 1 число решений этого уравнения для всех равно (*p* – 3)/4. При *р* ≡ 3mod8 для каждого квадрата из множества квадратов найдется элемент этого множества, обратный первому. Так как при *р* ≡ 3mod8 элемент [9], то Другими словами, множество не содержит 1. Таким образом, множество в условиях леммы включает ровно (*p* – 3)/8 пар взаимно-обратных элементов. В множестве все квадратичные вычеты множества становятся невычетами с сохранением свойства обратимости (но уже только для квадратичных невычетов) и числа элементов. Лемма доказана.

**Лемма 3.** *При р* ≡ 3mod8 *подмножество множества не содержит пар взаимно-обратных элементов.*

**Доказательство.** Допустим обратное и справедливо уравнение (16) для квадратичных невычетов подмножества. Тогда

 (17)

Правая часть равенства согласно допущению есть квадратичный невычет, а левая – квадрат. Для половины квадратов множества дает согласно лемме 2 решений, тогда как для половины невычетов таких решений нет. Следовательно, все элементы в подмножественеобратимы (т.е. не содержит пар мультипликативно обратных элементов). Лемма доказана.

С другой стороны, если допустить обратимость элементов то вместе с обратимостью элементов это даст (*p* – 3)/2 решений уравнения (12) и 2(*p* – 3) точек кривой, что невозможно.

**Лемма 4.** *При р* ≡ 3mod8 *множества*  } *и* *содержат по* (*p –* 3)*/*8 *одинаковых квадратичных вычетов и невычетов, и мощность их пересечения* *равна* (*p* – 3)/4.

**Доказательство.** Обозначим пересечение множеств и как . Тогда оно имеет подмножества квадратичных вычетов и квадратичных невычетов, причем . Одинаковые элементы этих множеств определяются из равенства

 .

Как и в лемме 1, это уравнение имеет (*p* – 3)/4 решений [13], а множество является суммой подмножеств квадратов и квадратичных невычетов равной мощности (*p* – 3)/8. Это следует из того, что множество также содержит 2 непересекающихся подмножества и с числом элементов по (*p* – 3)/8. Таким образом, ровно половина всех квадратов множества и невычетов этого множества совпадают с соответствующими подмножествами множества при этом . Тогда общее число совпадающих элементов этих множеств равно . Это доказывает утверждение леммы.

**Лемма 5.** *При р* ≡ 3mod8 для каждойпары взаимно-обратных квадратов множества существует единственный элемент множества невычетов , равный

**Доказательство.** Как следует из леммы 2, множества вычетов и невычетов состоят из пар взаимно-обратных элементов. Вместе с тем согласно лемме 4 множества невычетов и пересекаются лишь наполовину и содержат одинаковых элементов. Требуется доказать, что из каждой пары взаимно-обратных элементов множества лишь один элемент попадает в множество .

Пусть – пара квадратов множества Предположим, что существует квадратичный невычет , такой, что справедливо

1.
2. =

Поскольку при *р* ≡ 3mod8, элемент [12], правая часть равенств а) и b) не равна 0 (это тождественно отсутствию особых точек деления на 0 у полной кривой Эдвардса (12) при ). По условию элемент является квадратичным невычетом. Отсюда ясно, что существует единственное решение для невычета или множеств и , так как при выполнении равенства а) не выполняется равенство b) и наоборот. Лемма доказана.

**Теорема 3.** *При р* ≡ 3mod8  *полная кривая Эдвардса над* **F***p с параметрами*  *является суперсингулярной.*

**Доказательство.** Из выполнениясравнения *р* ≡ 3mod8сразу следует *р* ≡ 3mod4, так как редукция первого сравнения по модулю 4 дает второе.Следовательно, 4|(*p* + 1) и порядок кривой делится на 4. При выполнении сравнения *р* ≡ 3mod8 элемент 2 поля F*p*является квадратичным невычетом, т.е. [12], тогда при имеем полную кривую Эдвардса. Требуется доказать, что при *d =* 2 порядок кривой (9) равен *p* + 1 и кривая суперсингулярная.

При уравнение (12) имеет вид

 (18)

Как следует из леммы 1, одинаковые множества и содержат по квадратичных вычетов и невычетов, что составляет ровно половину всех вычетов (без элемента 1) и невычетов (без элемента -1). В соответствии с (18) надо найти число совпадающих элементов множества и множества обратных элементов

Свойства множеств квадратов и квадратичных невычетов (леммы 2 и 3) сводятся к тому, что множество состоит из пар взаимно-обратных квадратов, тогда как множество не содержит таких пар.

Лемма 4 утверждает, что пересечение множеств и содержит подмножества квадратичных вычетов и квадратичных невычетов с мощностями Тогда согласно лемме 5 для каждой пары квадратов существует единственный квадратичный невычет из пары который принадлежит множеству квадратичных невычетов .

С учетом этих свойств существует одно из двух альтернативных подмножеств или из 4-х элементов

 , (19)

 (20)

из которых первые два являются парой взаимно-обратных квадратов, а последние – парой необратимых квадратичных невычетов Необратимость последних невычетов следует из леммы 3. Последний элемент в (19) или (20) может быть любым отличным от первого невычетом множества . Умножая все его элементы на и обращая каждый из них, получим одно из подмножеств

 ,

Отсюда следует, что их пересечение с подмножествами соответственно (19) и (20) имеет две альтернативы:

 или

 Каждая из них содержит ровно 2 элемента, один из которых – квадратичный вычет, а другой – невычет. Так как все множество согласно лемме 2 содержит пар взаимно-обратиых квадратов, то можно построить то же число его подмножеств (или ), элементы которых определены подмножествами (19) или (20). Тогда мощность пересечения двух множеств равна

 .

Итак, имеется ровно решений уравнения (18), из которых половину решений дают квадратичные вычеты, половину – невычеты. Так как каждое решение уравнения (18) дает по 4 точки () кривой (9), получаем (*p* – 3) точек, удовлетворяющих уравнению (18). Добавляя 4 отброшенные при анализе точки О = (1, 0), *D* = (– 1, 0) и , получаем при порядок кривой (9) .Такая кривая является суперсингулярной со следом Фробениуса поэтому пара квадратичного кручения с параметром Теорема доказана. ▲

**Пример**. При в таблице 1 представлены элементы всех множеств, используемых в теореме 3.

 Таблица 1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|  | 4 | 9 | 16 | 6 | 17 | 11 | 7 | 5 |
|  | 3 | 8 | 15 | 5 | 16 | 10 | 6 | 4 |
|  |  |  |  | 5 | 16 |  | 6 | 4 |
|  | 3 | 8 | 15 |  |  | 10 |  |  |
|  | 16 | 11 | 4 | 14 | 3 | 9 | 13 | 15 |
|  | 6 | 7 | 5 | 15 | 13 | 17 | 3 | 14 |
|  | 16 | 11 | 4 |  |  | 9 |  |  |
|  |  |  |  | 14 | 3 |  | 13 | 15 |
|  | 16 |  | 4 |  | 3 |  |  | 15 |
|  | 16 |  | 4 |  |  |  |  |  |
|  |  |  |  |  | 3 |  |  | 15 |
|  | 3 |  | 15 | 5 |  |  | 6 |  |

Здесь два подмножества (19) или (20) можно построить как:

Тогда

а пересечения соответствующих подмножеств включают элементы:

.

Итак, получены решения уравнения (18), причем два из них для квадратичных вычетов, и два – для невычетов, что отвечает теореме 3. Приведенный пример дает наиболее простую иллюстрацию схемы доказательства.

При j-инвариант (7) полной суперсингулярной кривой Эдвардса равен

При уравнения кривой (12) при для пары квадратичного кручения имеют вид:

 . (21)

Так как элементы (–1) и 2 – квадратичные невычеты, то в соответствии с леммой 1 в правой части уравнений имеется равное число квадратичных вычетов и невычетов. Такое же соотношение их для левых частей уравнений. Из доказанной теоремы 3 следует, что при *р* ≡ 3mod8 ровно половина всех квадратичных вычетовмножеств в левой и правой части этих уравнений совпадают. Такое же утверждение справедливо для квадратичных невычетов.

Интересно заметить, что для суперсингулярной кривой с параметром и j–инвариантом два уравнения (12) для пары квадратичного кручения вырождаются в одно уравнение

,

совпадающее с (21) после замены

Существуют ли другие суперсингулярные полные кривые Эдвардса, кроме рассмотренных выше? Вопрос открытый. Пока нам удалось установить c помощью вычислений на компьютере, что в первой сотне значений модуля других кривых этого класса не существует.

 Литература

1. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография: монография/ А.В.Бессалов. – Киев: КПИ им. Игоря Сикорского, изд-во «Политехника», 2017. – 272с.
2. *Menezes A.J, Okamoto T., Vanstone S. A.* Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. University of Waterloo, sep. 1990. And //IEEE Transactions on Information Theory, V39, 1993. – PP 1639-1646.
3. L. C. Washington. Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.
4. Bernstein Daniel J., Birkner Peter , Joye Marc , Lange Tanja, Peters Christiane. Twisted Edwards Curves. IST Programme under Contract IST–2002–507932 ECRYPT,and in part by the National Science Foundation under grant ITR–0716498, 2008, РР. 1-17.
5. Bernstein Daniel J., Lange Tanja.Faster Addition and Doubling on Elliptic Curves // Advancesin Cryptology—ASIACRYPT’2007 (Proc. 13th Int. Conf. On the Theory and Applicationof Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. PP. 29–50.
6. Бессалов А.В., Цыганкова О.В. Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем. Проблемы передачи информации, - Том 51, вып 4, 2015. C.92-98.
7. Бессалов А.В., Цыганкова О.В. Классификация кривых в форме Эдвардса над простым полем. Прикладная радиоэлектроника: научно-техн. журнал. – 2015. – Том 14. – №4. – С.197 – 203.
8. Бессалов А.В., Цыганкова О.В. Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой. Проблемы передачи информации, - Том 53, вып 1, 2017. – С.101-111.
9. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.
10. Morain F. Edwards curves and CM curves. ArXiv 0904/2243v1 [Math.NT] Apr.15, 2009.
11. Дэвенпорт Г. Высшая арифметика: введение в теорию чисел // Пер. с англ. под редакцией Ю.В.Линника. – М: «Наука», 1965. – 176с.
12. Ковальчук Л.В., Беспалов О.Ю, Огнєв П.І. Рекурентні алгоритми обчислення кореня довільного степеню у кільці лишків. Правове нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2013, вип.1(25). – С.58 – 67.
13. Бессалов А.В., Ковальчук Л.В. Точное число эллиптических кривых в канонической форме, изоморфных кривым Эдвардса над простым полем. Кибернетика и системный анализ, т.51, №2, 2015. – С.3-12.