



**Аннотация.** Дан анализ условий существования суперсингулярных скрученных кривых Эдвардса над простым полем. Сформулированы и доказаны теоремы об условиях существования суперсингулярных кривых с  $j$ -инвариантами, равными нулю и  $12^3$ , в разных классах кривых. На основании этих результатов получены конкретные параметры для некоторых суперсингулярных кривых. Приведено обобщение полученных ранее результатов, использующее изоморфизм кривых в формах Вейерштрасса и Эдвардса.

**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]. Программирование арифметики этих кривых существенно упрощается в связи с тем, что нейтральный элемент этой группы является аффинной точкой  $O = (1, 0)$ . Универсальность закона сложения точек делает их более безопасными к атакам отводного канала [2].

Суперсингулярные эллиптические кривые, интерес к которым ослаб в 90-е годы в связи с уязвимостью к MOV-атаке изоморфизма [3], в начале нынешнего столетия стали основой криптографии на спаривании точек эллиптической кривой [4]. Кроме того, изогении таких кривых могут быть перспективны для задач постквантовой криптографии [5–7]. Технологические преимущества кривых в форме Эдвардса делают актуальной задачу исследования свойств суперсингулярных кривых этого типа.

В настоящей работе проведен анализ свойств суперсингулярных кривых в обобщенной форме Эдвардса [1] над простым полем. Статья состоит из трех разделов. В разд. 1 вводятся основные обозначения, а также понятия и определения в соответствии с новой классификацией кривых Эдвардса [1]. В разд. 2 и 3 доказаны теоремы об условиях существования суперсингулярных кривых Эдвардса с  $j$ -инвариантами, равными нулю и  $12^3$ .

## 1. КРИВЫЕ В ОБОБЩЕННОЙ ФОРМЕ ЭДВАРДСА И СУПЕРСИНГУЛЯРНЫЕ КРИВЫЕ

В работе [8] скрученные кривые Эдвардса (twisted Edwards curves) определены как обобщение кривых Эдвардса  $x^2 + y^2 = 1 + dx^2y^2$  [2] путем ввода нового параметра  $a$  в уравнение:

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2, \quad a, d \in F_p^*, \quad d \neq 1, \quad a \neq d, \quad p \neq 2.$$

Наряду с вводом параметра  $a$  в [8] были сняты ограничения на параметр  $d$ , допуская любые значения  $\left(\frac{ad}{p}\right) = \pm 1$  (здесь  $\left(\frac{ad}{p}\right)$  — символ Лежандра произведения  $a \cdot d$  [4]). При  $a = 1$  такая кривая получила в [8] название кривой Эдвардса, а если ее параметр  $d$  — квадратичный невычет (т.е.  $\left(\frac{d}{p}\right) = -1$ ), то она называется полной кривой Эдвардса. Этот термин был предложен в связи с полнотой закона сложения точек кривой [2]. В работе [9] предложено поменять местами координаты  $x$  и  $y$  в форме кривой Эдвардса в целях сохранения горизонтальной симметрии обратных точек, принятой в теории эллиптических кривых. Опираясь на это свойство, определим кривую в обобщенной форме Эдвардса в виде уравнения

$$E_{a,d} : x^2 + ay^2 = 1 + dx^2y^2, \quad a, d \in F_p^*, \quad d(d-a) \neq 0, \quad d \neq 1, \quad p \neq 2. \quad (1)$$

Тогда модифицированный универсальный закон сложения точек имеет вид

$$(x_1, y_1) + (x_2, y_2) = \left( \frac{x_1x_2 - ay_1y_2}{(1 - dx_1x_2y_1y_2)}, \frac{x_1y_2 + x_2y_1}{(1 + dx_1x_2y_1y_2)} \right). \quad (2)$$

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

$$2(x_1, y_1) = \left( \frac{x_1^2 - ay_1^2}{(1 - dx_1^2y_1^2)}, \frac{2x_1y_1}{(1 + dx_1^2y_1^2)} \right). \quad (3)$$

Определяя теперь обратную точку как  $P = (x_1, -y_1)$ , получаем согласно закону (2) координаты нейтрального элемента группы:  $(x_1, y_1) + (x_1, -y_1) = O = (1, 0)$ , который лежит на оси  $OX$ , где также всегда лежит точка  $D_0 = (-1, 0)$  второго порядка, для которой  $2D_0 = (1, 0) = O$  согласно (3). В зависимости от свойств параметров  $a$  и  $d$  можно получить еще две особые точки второго порядка и две особые точки четвертого порядка. Как следует из (1), на оси  $OY$  могут также лежать неособые точки четвертого порядка  $\pm F_0 = (0, \pm 1/\sqrt{a})$ , для которых  $\pm 2F_0 = D_0 = (-1, 0)$ . Эти точки существуют над полем  $F_p$ , если параметр  $a$  является квадратичным вычетом.

Согласно классификации кривых в форме (1), обоснованной в работах [1, 10, 11], скрученная кривая имеет параметры  $a$  и  $d$ , которые являются квадратичными невычетами:  $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$ . А при  $a = 1$  определены полные кривые Эдвардса

с параметром  $d$ , являющимся квадратичным невычетом:  $\left(\frac{d}{p}\right) = -1$ , и квадратичные кривые Эдвардса, для которых  $\left(\frac{d}{p}\right) = 1$ . Полные кривые Эдвардса являются циклическими и не содержат особых точек, а нециклические скрученные и квадра-

тичные кривые имеют по три точки второго порядка, две из которых — особые. Следует отметить, что скрученные и квадратичные кривые Эдвардса образуют пары квадратичного кручения, параметры которых связаны линейным преобразованием  $a' = ca$ ,  $d' = cd$ , где  $\left(\frac{c}{p}\right) = -1$  (см. [1, 11]). Воспользуемся этим свойством при анализе суперсингулярных кривых таких классов, для которых примем  $a = 1$ , и ограничимся одним параметром  $d$ , для которого  $\left(\frac{d}{p}\right) = 1$ ,  $d \neq 1$ . Другими словами, анализ суперсингулярных кривых двух классов — скрученных и квадратичных кривых Эдвардса сводится к анализу последних с одним параметром  $d$ .

Порядок  $N_E$  эллиптической кривой над конечным полем  $F_q$ ,  $q = p^m$ , определяется на основе следа уравнения Фробениуса  $t$ :  $N_E = q + 1 - t$ . Для кривой квадратичного кручения  $E^t$  соответствующий порядок определяется как  $N_E^t = q + 1 + t$ . Эллиптическая кривая является суперсингулярной тогда и только тогда, когда над любым расширением простого поля  $F_p$  имеем след  $t \equiv 0 \pmod{p}$  [4]. Иными словами, в алгебраическом замыкании поля  $\overline{F_p}$  суперсингулярная кривая не содержит точек порядка  $p$ . Над простым полем  $F_p$  такая кривая всегда имеет порядок  $N_E = p + 1$ , а над любым расширением этого поля  $N_E \equiv 1 \pmod{p}$ .

Для кривой

$$E: Y^2 = X^3 + AX + B \quad (4)$$

в канонической форме Вейерштрасса с  $j$ -инвариантом [4, 12]

$$j(E) = \frac{12^3 \cdot 4A^3}{4A^3 + 27B^2} \quad (5)$$

характерными являются значения  $j(E) = 0$  при  $A = 0$  и  $j(E) = 12^3$  при  $B = 0$ . Эти значения  $j$ -инварианта часто (при выполнении известных условий для модуля  $p$ ) порождают суперсингулярную кривую.

Изоморфизм кривых в формах (1) и (4) достигается лишь приблизительно для четвертой части всех кривых в форме Вейерштрасса, содержащих одну или три точки второго порядка. Порядок  $N_E$  таких кривых всегда кратен четырем. Наиболее удобной формой их представления является кривая в форме Монтгомери [5]:

$$E_{C,D}: Dv^2 = u^3 + Cu^2 + u, \quad C = 2 \frac{a+d}{a-d}, \\ D = \frac{4}{a-d}, \quad a = \frac{C+2}{D}, \quad d = \frac{C-2}{D}, \quad C^2 \neq 4. \quad (6)$$

Как частный случай канонической кривой (4) в форме Вейерштрасса, уравнение (6) часто используется при анализе свойств кривой в обобщенной форме Эдвардса (1). Поскольку кривые (1) и (6) изоморфны  $(E_{a,d} \sim E_{C,D})$  [1, 8], условия существования таких суперсингулярных кривых эквивалентны.

Для кривой (1) имеем  $j$ -инвариант [13]

$$j(a, d) = \frac{16(a^2 + d^2 + 14ad)^3}{ad(a-d)^4}, \quad ad(a-d) \neq 0. \quad (7)$$

Так как  $j$ -инвариант сохраняет свое значение для всех изоморфных кривых и пар квадратичного кручения [4], он является полезным инструментом при поиске суперсингулярных кривых. Поэтому параметр  $a$  в (7) является избыточным,

т.е. можно принять  $a = 1$  и рассматривать свойства лишь полных и квадратичных кривых Эдвардса. Если квадратичная кривая — суперсингулярная, то и соответствующая ей скрученная кривая (как пара квадратичного кручения) также суперсингулярная. Исходя из этого в дальнейшем будем использовать  $j$ -инвариант  $j(1, d)$ . Одним из его свойств является

$$j(1, d) = j(1, d^{-1}). \quad (8)$$

Чтобы доказать это свойство, достаточно элемент  $d$  в (7) заменить на  $d^{-1}$  и умножить числитель и знаменатель на  $d^6$ . В результате получаем равенство (8). Как известно, обращение параметра  $d \rightarrow d^{-1}$  дает кривую квадратичного кручения для полной кривой Эдвардса [2] и изоморфную кривую — для квадратичной кривой Эдвардса [1].

**Замечание 1.** Поскольку порядок  $N_E$  кривой Эдвардса  $E$  над полем  $F_p$  всегда делится на четыре, то суперсингулярные кривые в форме Эдвардса с порядком  $N_E = p+1$  существуют лишь при  $p \equiv 3 \pmod{4}$ . Действительно, из условия  $p+1 = 4k$  следует условие  $p = 4k - 1$  или  $p \equiv 3 \pmod{4}$ . Поэтому в настоящей статье рассматриваем лишь кривые над полями  $F_p$ , где  $p \equiv 3 \pmod{4}$ , поскольку это условие является необходимым для существования суперсингулярных кривых Эдвардса.

Скрученная кривая Эдвардса определена в работе [1] как частный случай кривой (1):

$$E_{a,d} : x^2 + ay^2 = 1 + dx^2y^2, \quad d \in F_p^*, \quad d(d-a) \neq 0, \quad \left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1.$$

Для анализа условий существования суперсингулярных кривых этого класса достаточно провести такой анализ в классе квадратичных кривых Эдвардса:

$$E_{1,d} : x^2 + y^2 = 1 + dx^2y^2, \quad d \in F_p^*, \quad d(d-1) \neq 0, \quad \left(\frac{d}{p}\right) = 1.$$

Характерными свойствами этого класса кривых являются нециклическая структура подгрупп точек четного порядка и наличие четырех особых точек второго и четвертого порядков [8].

## 2. СУПЕРСИНГУЛЯРНЫЕ КРИВЫЕ ЭДВАРДСА С НУЛЕВЫМ $j$ -ИНВАРИАНТОМ

Поскольку при изоморфных преобразованиях эллиптических кривых значение  $j$ -инварианта не изменяется, то кривые Эдвардса с нулевым  $j$ -инвариантом будут изоморфны кривым (4) в форме Вейерштрасса с  $j$ -инвариантом (5), равным нулю. Из (5) следует, что эти кривые имеют вид  $Y^2 = X^3 + B$ . Хотя любая кривая этого вида имеет нулевой  $j$ -инвариант, не все они суперсингулярны. Кроме того, не любая из этих кривых сводится к форме Монтгомери (6) и, следовательно, изоморфна кривой в форме Эдвардса.

**Теорема 1.** Пусть кривая (1) над полем  $F_p$  с параметром  $a = 1$  имеет  $j$ -инвариант  $j(1, d) = 0$ . Тогда при  $p \equiv -1 \pmod{12}$  она является полной суперсингулярной кривой Эдвардса с параметром  $d = -(2 \pm \sqrt{3})^2$ .

**Доказательство.** Согласно (7) из условия  $j(1, d) = 0$  следует равенство

$$d^2 + 14d + 1 = 0. \quad (9)$$

Это возможно тогда и только тогда, когда дискриминант левой части является квадратичным вычетом множества  $Q_p$ , т.е. при условии

$$D = 14^2 - 4 = 3 \cdot 8^2 \in Q_p,$$

что эквивалентно условию  $3 \in Q_p$ . Согласно [14] это возможно лишь при  $p \equiv \pm 1 \pmod{12}$ . Но при  $p \equiv 1 \pmod{12}$  имеет место сравнение  $p \equiv 1 \pmod{4}$ , а тогда согласно замечанию 1 не существует суперсингулярных кривых Эдвардса над полем  $F_p$ . Поэтому остается возможным только условие  $p \equiv -1 \pmod{12}$ ; одно из утверждений теоремы доказано. Заметим, что в этом случае имеем решения уравнения (9):

$$d_{1,2} = -7 \pm 4\sqrt{3}.$$

Далее, поскольку  $j$ -инвариант не изменяется при переходе от одной формы кривой к другой, то  $j$ -инвариант (5) этой кривой в форме Вейерштрасса  $y^2 = x^3 + Ax + B$  тоже будет равен нулю, т.е. выполнено равенство  $A = 0$ , и эта кривая в форме Вейерштрасса будет иметь вид

$$y^2 = x^3 + B. \quad (10)$$

Из условия  $p \equiv -1 \pmod{12}$  следует  $p \equiv -1 \pmod{3}$ , откуда вытекает, что  $|F_p^*| = p - 1$  не делится на три. Следовательно, отображение  $\varphi: F_p \rightarrow F_p^*$ ,  $\varphi(x) = x^3$ , является биекцией. Поэтому, когда  $x$  пробегает все значения из  $F_p^*$ , правая часть (10) также пробегает все эти значения. Среди этих значений существует точно  $\frac{p-1}{2}$  квадратичных вычетов, для каждого из них имеем два значения  $y$ -координаты точки кривой. Таким образом, с учетом точки  $(\sqrt[3]{B}, 0)$  и точки на бесконечности получаем, что количество точек кривой равно  $2 \cdot \frac{p-1}{2} + 1 + 1 = p + 1$ , т.е.  $N_E = p + 1$  и кривая является суперсингулярной.

Докажем, что  $E_{1,d}$  — полная кривая Эдвардса. Заметим, что при  $p \equiv 3 \pmod{4}$  элемент  $-1$  является квадратичным невычетом. Согласно (9) параметр этой кривой определяется формулой

$$d_{1,2} = -(7 \mp 4\sqrt{3}) = -(2^2 \mp 2 \times 2 \times \sqrt{3} + (\sqrt{3})^2) = -(2 \mp \sqrt{3})^2. \quad (11)$$

Поскольку выражения в правой части (11) являются квадратичными невычетами, т.е.  $d_{1,2} \notin Q_p$ , то кривая является полной кривой Эдвардса.

Теорема доказана.

**Следствие 1.** Среди кривых Эдвардса с нулевым  $j$ -инвариантом не существует скрученных и квадратичных кривых.

Действительно, как доказано в теореме 1, любая кривая Эдвардса с нулевым  $j$ -инвариантом при  $p \equiv 3 \pmod{4}$  согласно (11) является полной.

### 3. СУПЕРСИНГУЛЯРНЫЕ СКРУЧЕННЫЕ КРИВЫЕ ЭДВАРДСА С $j$ -ИНВАРИАНТОМ, РАВНЫМ $12^3$

Рассмотрим условия существования суперсингулярных кривых с  $j$ -инвариантом, равным  $12^3$ . Для дальнейшего изложения понадобится следующее утверждение, доказанное в [12].

**Утверждение 1** [12]. Пусть  $p$  — простое,  $p \equiv 3 \pmod{4}$ ,  $E$  — эллиптическая кривая над  $F_p$ , заданная уравнением  $y^2 = x^3 + Ax$ , для некоторого  $A \in F_p$ . Тогда  $N_E = p + 1$ , т.е.  $E$  является суперсингулярной кривой.

С использованием этого утверждения получим два следующих результата.

**Утверждение 2.** Пусть  $p$  — простое,  $p \equiv 3 \pmod{4}$ ,  $E_{a,d}$  — кривая Эдвардса над  $F_p$  с параметрами  $a$  и  $d$ , заданная уравнением  $x^2 + ay^2 = 1 + dx^2y^2$ , причем  $j(a,d) = 12^3$ . Тогда кривая  $E_{a,d}$  — суперсингулярная.

**Доказательство.** Для любой кривой  $E$  в форме Эдвардса существует кривая  $E'$  в форме Вейерштрасса, ей изоморфная и заданная уравнением (4). При этом  $j$ -инварианты изоморфных кривых сохраняют свое значение, поэтому инвариант кривой  $E'$ , заданный согласно (5), также равен  $12^3$ :

$$j = \frac{12^3 \cdot 4A^3}{4A^3 + 27B^2} = 12^3.$$

Отсюда получаем  $4A^3 = 4A^3 + 27B^2$ , т.е.  $B = 0$ , и кривая  $E'$  задана уравнением  $y^2 = x^3 + Ax$ , а такая кривая согласно утверждению 1 является суперсингулярной.

Утверждение 2 доказано.

В следующей теореме приводятся некоторые суперсингулярные кривые в классе скрученных кривых Эдвардса.

**Теорема 2.** Пусть  $p \equiv 7 \pmod{8}$ . Тогда скрученная кривая Эдвардса над полем  $F_p$  с параметрами  $a = -1$  и  $d_{1,2} = -(3 \pm 2\sqrt{2})^2$  имеет  $j$ -инвариант, равный  $12^3$ , и является суперсингулярной.

**Доказательство.** Вначале покажем, что теорема сформулирована корректно, т.е. указанные параметры  $d_{1,2}$  действительно являются элементами поля  $F_p$  и кривая с такими параметрами является скрученной.

Так, при  $p \equiv 7 \pmod{8}$  элемент 2 является квадратичным вычетом, поскольку в этом случае  $p = 8k + 7$  для некоторого  $k \in N$  и согласно квадратичному закону взаимности Гаусса

$$\left(\frac{2}{p}\right) = (-1)^{\frac{(8k+6)(8k+8)}{8}} = 1.$$

Следовательно, параметры  $d_{1,2}$  определены корректно.

Далее, если  $p \equiv 7 \pmod{8}$ , то  $p \equiv 3 \pmod{4}$ , откуда  $-1 \notin Q_p$ . Поэтому  $a \notin Q_p$ ,  $d_{1,2} \notin Q_p$  и кривые с этими параметрами являются скрученными согласно классификации в [1, 10, 11].

Докажем суперсингулярность таких кривых. Для этого согласно утверждениям 1 и 2 достаточно показать, что  $j$ -инварианты таких кривых равны  $12^3$ .

Заметим, что в силу изоморфизма соответствующих кривых

$$j(a,d) = j(-a,-d), \quad a, d \in F_p.$$

Поэтому достаточно вычислить инварианты  $j(1, -d_{1,2})$ .

Пусть  $d_1 = -(3 + 2\sqrt{2})^2$ ,  $d_2 = -(3 - 2\sqrt{2})^2$ . Обозначим  $t_1 = -d_1 = (3 + 2\sqrt{2})^2$ ,  $t_2 = -d_2 = (3 - 2\sqrt{2})^2$  и вычислим инварианты  $j(1, t_1)$ ,  $j(1, t_2)$ .

Путем несложных преобразований получаем равенства

$$t_1 = (3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2}, \quad t_1 + 1 = 18 + 12\sqrt{2} = 6(3 + 2\sqrt{2}) = 6\sqrt{t_1},$$

откуда  $(t_1 + 1)^2 = 36t_1$ .

Аналогично  $t_1 - 1 = 6\sqrt{t_1} - 2$ , откуда

$$(t_1 - 1)^2 = 36t_1 - 24\sqrt{t_1} + 4 = 36t_1 + 4 - 4(t_1 + 1) = 32t_1.$$

Тогда

$$j(1, t_1) = \frac{16((t_1 + 1)^2 + 12t_1)^3}{t_1(t_1 - 1)^4} = \frac{16(36t_1 + 12t_1)^2}{t_1(32t_1)^2} = \frac{16 \cdot 48^3}{32^2} = 12^3.$$

Аналогичными расчетами получаем равенство  $j(1, t_2) = 12^3$ . Следовательно,  $j(-1, d_1) = j(-1, d_2) = 12^3$  и кривые с параметрами  $a = -1$  и  $d = d_{1,2}$  являются суперсингулярными. Теорема доказана.

Заметим, что в классе полных кривых Эдвардса  $j$ -инвариант  $j(1, d) = 12^3$  порождается единственным значением параметра  $d = -1$  при  $p \equiv 3 \pmod{8}$  [см. 15]. Таким образом, всего имеется шесть корней уравнения  $j(1, d) = 12^3$  (см. (7)): по два корня для квадратичных и скрученных кривых и по одному корню  $d = -1$  кратности 2 для полных кривых Эдвардса.

#### ЗАКЛЮЧЕНИЕ

В статье сформулированы и доказаны условия существования суперсингулярных кривых Эдвардса при некоторых дополнительных условиях для  $j$ -инварианта кривой. Эти условия позволяют получать все суперсингулярные кривые с фиксированным значением  $j$ -инварианта. Отметим, что значениями  $j(1, d) = 0$  и  $j(1, d) = 12^3$  не исчерпываются все суперсингулярные кривые Эдвардса. В частности, в работах [1, 12] были обнаружены полные суперсингулярные кривые с  $j$ -инвариантом, равным  $66^3$ , а также приведены основные тезисы доказательства теоремы о суперсингулярности таких кривых с параметрами  $d = 2^{\pm 1}$ . В продолжение этой работы (часть 2, разд. 4) будет приведено более полное доказательство существования скрученных и квадратичных суперсингулярных кривых Эдвардса с  $j$ -инвариантом, равным  $66^3$ .

#### СПИСОК ЛИТЕРАТУРЫ

1. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Киев: КПИ имени Игоря Сикорского. Изд-во «Политехника», 2017. 272 с.
2. Bernstein D.J., Lange T. Faster addition and doubling on elliptic curves. In: *Advances in Cryptology — ASIACRYPT'2007* (Proc. 13th Int. Conf. on the Theory and Application of Cryptology and Information Security. Kuching, Malaysia (December 2–6, 2007)). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. P. 29–50.
3. 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*. 1993. Vol. 39. P. 1639–1646.
4. Washington L.C. *Elliptic curves. Number theory and cryptography*. Second Edition. CRC Press. Taylor and Francis Group. A Chapman and Hall Book, 2008. 513 p.
5. Tanushree Banerjee, Anwar Hasan M. Energy efficiency analysis of elliptic curve based cryptosystems. URL: <http://cacr2018-04 DH-Isogenies>.
6. Adj G., Cervantes-Vazquez D., Chi-Dominguez J.-J., Menezes A., Rodriguez-Henriquez F. On the cost of computing isogenies between supersingular elliptic curves. URL: <http://cacr2018-03 Menezes Isogenies on SSC>.
7. Youngho Y., Azarderakhsh R., Jalali A., Jao D., Soukharev V. A post-quantum digital signature scheme based on supersingular isogenies. *Cryptology ePrint Archive*, Report 2017/186, 2017. URL: <http://eprint.iacr.org/2017/186>. 18 p.
8. Bernstein D.J., Birkner P., Joye M., Lange T., Peters Ch. Twisted Edwards curves. IST Programme under Contract IST-2002-507932 ECRYPT, and in part by the National Science Foundation under grant ITR-0716498, 2008. P. 1–17.



9. Бессалов А.В., Цыганкова О.В. Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем. *Проблемы передачи информации*. 2015. Т. 51, вып. 4. С. 92–98.
10. Бессалов А.В., Цыганкова О.В. Классификация кривых в форме Эдвардса над простым полем. *Прикладная радиоэлектроника*. 2015. Т. 14, № 4. С. 197–203.
11. Бессалов А.В., Цыганкова О.В. Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой. *Проблемы передачи информации*. 2017. Т. 53, вып. 1. С. 101–111.
12. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых. Киев: ІВЦ «Політехніка», 2004. 224 с.
13. Morain F. Edwards curves and CM curves. ArXiv 0904/2243v1 [Math.NT] Apr. 15, 2009. 15 p.
14. Дэвенпорт Г. Высшая арифметика: введение в теорию чисел. Пер. с англ. (под ред. Линника Ю.В.). Москва: Наука, 1965. 176 с.
15. Бессалов А.В., Цыганкова О.В. Суперсингулярные полные кривые Эдвардса над простым полем. *Радиотехника*. 2017. № 191. С. 88–98.

Надійшла до редакції 15.05.2018

**А.В. Бессалов, Л.В. Ковальчук**

**СУПЕРСИНГУЛЯРНІ СКРУЧЕНІ КРИВІ ЕДВАРДСА НАД ПРОСТИМ ПОЛЕМ.**

**1. СУПЕРСИНГУЛЯРНІ СКРУЧЕНІ КРИВІ ЕДВАРДСА**

**З  $j$ -ІНВАНІАНТАМИ, ЯКІ ДОРІВНЮЮТЬ НУЛЮ ТА  $12^3$**

**Анотація.** Проаналізовано умови існування суперсингулярних скручених кривих Едвардса над простим полем. Сформульовано та доведено теореми про умови існування суперсингулярних кривих з  $j$ -інваріантами, які дорівнюють нулю та  $12^3$ , в різних класах кривих. На базі цих результатів отримано конкретні параметри для деяких суперсингулярних кривих. Наведено узагальнення отриманих раніше результатів, що використовує ізоморфізм кривих у формах Вейерштрасса та Едвардса.

**Ключові слова:** суперсингулярна крива, повна крива Едвардса, скручена крива Едвардса, квадратична крива Едвардса, пара кручення, порядок точки, символ Лежандра, квадратичний лишок, квадратичний нелишок.

**A.V. Bessalov, L.V. Kovalchuk**

**SUPERSINGULAR TWISTED EDWARDS CURVES OVER PRIME FIELDS.**

**1. SUPERSINGULAR TWISTED EDWARDS CURVES WITH  $j$ -INVARIANTS 0 AND  $12^3$**

**Abstract.** The analysis is given of the conditions of the existence of supersingular twisted Edwards curves over prime fields. Theorems are formulated and proved about these conditions for supersingular twisted Edwards curves with  $j$ -invariants 0 and  $12^3$ , for different classes of curves. Parameters for some supersingular curves are obtained using these results. Generalization of some previously obtained results is given, using isomorphism of curves in Weierstrass form and Edwards form.

**Keywords:** supersingular curve, complete Edwards curve, twisted Edwards curve, quadratic Edwards curve, twisted pair, order of point, Legendre symbol, quadratic residue, quadratic non-residue.

**Бессалов Анатолий Владимирович,**

доктор техн. наук, профессор, профессор кафедры Физико-технического института НТУУ «КПИ имени Игоря Сикорского», Киев, e-mail: bessalov@ukr.net.

**Ковальчук Людмила Васильевна,**

доктор техн. наук, профессор, профессор кафедры Физико-технического института НТУУ «КПИ имени Игоря Сикорского», Киев, e-mail: lusi.kovalchuk@gmail.com.