УДК 621.391.15 : 519.7

А.В. БЕССАЛОВ, Л.В. КОВАЛЬЧУК

СУПЕРСИНГУЛЯРНЫЕ СКРУЧЕННЫЕ КРИВЫЕ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ[1]. II. СУПЕРСИНГУЛЯРНЫЕ СКРУЧЕННЫЕ КРИВЫЕ ЭДВАРДСА С *j*-ИНВАРИАНТОМ, РАВНЫМ 66^3

Аннотация. В продолжение результатов, полученных в [1], сформулированы и доказаны теоремы об условиях существования суперсингулярных кривых Эдвардса над простым полем с *j*-инвариантом, равным 66^3, и с другими значениями *j*-инвариантов. Приведено обобщение полученных ранее результатов, использующее изоморфизм кривых в формах Лежандра и Эдвардса.

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

ВВЕДЕНИЕ

Эллиптические кривые в форме Эдвардса над простым полем наиболее перспективны для современных криптосистем [1]. Производительность операции экспоненцирования точки такой кривой в среднем более чем в 1,5 раза выше, чем для кривой в форме Вейерштрасса [2]. Программирование арифметики этих кривых существенно упрощается в связи с наличием нейтрального элемента группы как аффинной точки кривой O = (1,0). Универсальность закона сложения точек делает их более безопасными к атакам бокового канала [3].

Суперсингулярные эллиптические кривые, интерес к которым ослаб в 90-е годы в связи с уязвимостью к MOV-атаке изоморфизма [4], в начале нынешнего столетия стали основой криптографии на спаривании точек эллиптической кривой [5]. Кроме того, изогении таких кривых могут быть перспективны для задач постквантовой криптографии [6–8]. Технологические преимущества кривых в форме Эдвардса делают актуальной задачу исследования свойств суперсингулярных кривых этого типа.

В настоящей статье дан анализ свойств двух классов суперсингулярных кривых в обобщенной форме Эдвардса [2] над простым полем — квадратичных и скрученных кривых Эдвардса. В разд. 1 вводятся основные понятия и определения в соответствии с новой классификацией кривых Эдвардса [2]. В разд. 2 дан анализ условий существования суперсингулярных кривых Эдвардса с *j*-инвариантом, равным 66^3. В разд. 3 дано обобщение некоторых результатов для суперсингулярных кривых Эдвардса с другими *j*-инвариантами на основе их изоморфизма с кривыми в форме Лежандра [5].

[1] Продолжение. Начало в № 3, 2019

1. КРИВЫЕ ЭДВАРДСА В ОБОЩЕННОЙ ФОРМЕ. ОБЗОР ИЗВЕСТНЫХ РЕЗУЛЬТАТОВ

Используем основные обозначения и свойства кривых, приведенные в [1].

В работе [9] скрученные кривые Эдвардса (twisted Edwards curves) определены как обобщение кривых Эдвардса $x^2 \quad y^2 \quad 1 \quad dx^2 y^2$ [3] путем ввода нового параметра a в уравнение кривой:

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

В работе [10] предложено поменять местами координаты x и y в форме кривой Эдвардса в целях сохранения горизонтальной симметрии обратных точек и определить кривую в обобщенной форме Эдвардса, используя уравнение

$$E_{a,d} : x^2 \quad ay^2 \quad 1 \quad dx^2 y^2, \; a, d \quad F_p^*, \; d \quad 1, \; d(d \quad a) \quad 0, \; p \quad 2 . \qquad (1)$$

Тогда модифицированный универсальный закон сложения точек имеет вид

$$(x_1, y_1) \quad (x_2, y_2) \quad \frac{x_1 x_2 \quad a y_1 y_2}{1 \quad d x_1 x_2 y_1 y_2}, \frac{x_1 y_2 \quad x_2 y_1}{1 \quad d x_1 x_2 y_1 y_2} . \qquad (2)$$

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

$$2(x_1, y_1) \quad \frac{x_1^2 \quad a y_1^2}{1 \quad d x_1^2 y_1^2}, \frac{2 x_1 y_1}{1 \quad d x_1^2 y_1^2} . \qquad (3)$$

Определяя точку $P \quad (x, \; y)$, обратную к точке $P \quad (x, y)$, получаем согласно закону (2) координаты нейтрального элемента группы $(x, y) \quad (x, \quad y) \quad O \quad (1,0)$.

Согласно классификации кривых в форме (1), обоснованной в работах [2, 10–12], скрученная кривая имеет параметры a и d, которые являются квадратичными невычетами: $\frac{a}{p} \quad \frac{d}{p} \quad 1$, тогда как при $a \quad 1$ определены полные кривые Эдвардса с параметром d, являющимся квадратичным невычетом: $\frac{d}{p} \quad 1$, и квадратичные кривые Эдвардса, для которых $\frac{d}{p} \quad 1$.

Для кривой E, заданной уравнением

$$Y^2 \quad X^3 \quad AX \quad B \qquad (4)$$

в канонической форме Вейерштрасса с j-инвариантом [5, 13]

$$j(E) \quad \frac{12^3 \quad 4A^3}{4A^3 \quad 27B^2},$$

характерными являются значения $j(E) \quad 0$ при $A \quad 0$ и $j(E) \quad 12^3$ при $B \quad 0$. Эти значения j-инварианта часто (при выполнении известных условий для модуля p) порождают суперсингулярную кривую. В [1] были изучены суперсингулярные кривые с такими же значениями j-инварианта.

Изоморфизм кривых в формах (1) и (4) достигается лишь приближенно для четверти всех кривых в форме Вейерштрасса. Порядок таких кривых составляет $N_E \quad 0 (\mathrm{mod} 4)$. Наиболее удобной формой их представления является кривая $E_{C,D}$ в форме Монтгомери [9]:

$$Dv^2 \quad u^3 \quad Cu^2 \quad u,\ C \quad 2\frac{a \quad d}{a \quad d},\ D \quad \frac{4}{a \quad d},\ a \quad \frac{C \quad 2}{D},\ d \quad \frac{C \quad 2}{D},\ C^2 \quad 4. \quad (5)$$

Так как кривые (1) и (5) изоморфны ($E_{a,d} \sim E_{C,D}$) [2, 9], условия существования таких суперсингулярных кривых эквивалентны.

Для кривой (1) j-инвариант имеет вид [14]

$$j(a, d) \quad \frac{16(a^2 \quad d^2 \quad 14ad)}{ad(a \quad d)^4},\ ad(a \quad d) \quad 0. \quad (6)$$

Так как j-инвариант сохраняет свое значение для всех изоморфных кривых и пар квадратичного кручения [5], он является полезным инструментом при поиске суперсингулярных кривых. Как отмечалось в [1], для этих целей параметр a в (6) является избыточным, т.е. можно принять $a \quad 1$ и рассматривать свойства лишь полных и квадратичных кривых Эдвардса. В дальнейшем будем использовать j-инвариант $j(1, d)$. Одним из свойств j-инварианта является $j(1, d) \quad j(1, d^{\ 1})$.

Скрученная кривая Эдвардса определена в работе [2] как частный случай кривой (1)

$$E_{a,d}: x^2 \quad ay^2 \quad 1 \quad dx^2y^2,\ d \quad F_p^*,\ d(d \quad a) \quad 0,\ \frac{a}{p} \qquad \frac{d}{p} \qquad 1.$$

Для анализа условий существования суперсингулярных кривых этого класса достаточно провести такой анализ в классе квадратичных кривых Эдвардса $E_{1,d}$:

$$x^2 \quad y^2 \quad 1 \quad dx^2y^2,\ d \quad F_p^*,\ d(d \quad 1) \quad 0,\ \frac{d}{p} \quad 1. \quad (7)$$

2. СУПЕРСИНГУЛЯРНЫЕ СКРУЧЕННЫЕ КРИВЫЕ ЭДВАРДСА С j-ИНВАРИАНТОМ $j(1, d) \quad 66^3$

Проанализируем свойства квадратичной кривой Эдвардса (7). Как отмечалось, последующий переход к скрученной кривой сводится к умножению ее параметров $(1, d)$ на квадратичный невычет: $(1, d) \quad (c, cd)$, $\frac{c}{p} \quad 1$.

При $x, y \quad 0, \ 1, \ \frac{1}{\sqrt{d}}$ разделим левую и правую части уравнения (7) кривой $E_{1,d}$ на x^2, y^2:

$$\frac{1}{y^2} \quad \frac{1}{x^2} \quad \frac{1}{x^2y^2} \quad d,$$

откуда получаем

$$y^{\ 2} \quad 1 \quad \frac{1 \quad d}{1 \quad x^{\ 2}},\ x, y \quad 0, \ 1, \ \frac{1}{\sqrt{d}}. \quad (8)$$

Если (8) переписать в виде

$$y^{\ 2} \quad 1 \quad \frac{d \quad x^{\ 2}}{1 \quad x^{\ 2}},$$

то получим особые точки кривой $E_{1,d}$: $D_{1,2} \qquad \frac{1}{\sqrt{d}}$; — особые точки второго порядка; $F_{1,2} \qquad ; \ \frac{1}{\sqrt{d}}$ — особые точки четвертого порядка,

причем $F_1 \quad F_2$. Отметим также, что кривая содержит и другие (неособые) точки малых порядков: нейтральный элемент группы O , точку второго порядка D_0 и две точки четвертого порядка F_0 .

Будем искать такие значения параметра d , при которых уравнение (7) задает суперсингулярную кривую. Для этого в уравнении (8) сделаем замену переменных

$$u \quad x^{1}, \; v \quad y^{1}$$

и перепишем это уравнение как

$$v^2 \quad 1 \quad \frac{1 \quad d}{1 \quad u^2}. \tag{9}$$

Необходимо найти такие значения d , при которых количество пар (x, y) , являющихся решениями (8), было бы равно $p \quad 1$. Если исключить из этого множества решений точки малых порядков (особые и неособые), т.е. точки, у которых одна из координат равна нулю или , то останется $p \quad 1 \quad 8 \quad p \quad 7$ точек. Иными словами, кривая $E_{1,d}$ будет суперсингулярной тогда и только тогда, если количество пар (u, v) , являющихся решениями (9), для которых $u, v \quad 0, \; 1, \; \sqrt{d}, \;$, равно $p \quad 7$.

Для формулировки и доказательства основного результата необходимо ввести ряд обозначений и доказать несколько вспомогательных утверждений.

Для произвольного простого числа p будем использовать следующие обозначения, которые можно назвать стандартными: $Q_p \quad \{x \quad Z_p^* \mid y \quad Z_p^*: x \quad y^2 \pmod p\}$ — множество приведенных квадратичных вычетов по модулю p ; $Q_p \quad \{ \; x \mid x \quad Q_p\}$; $\overline{Q_p} \quad Z_p^* \setminus Q_p$ — множество приведенных квадратичных невычетов по модулю p .

Для дальнейшего изложения необходимо определить следующие множества:

$$U \quad x^2 \quad 1 \mid x \quad 2, 3, \ldots, \frac{p \quad 1}{2} \quad ; \tag{10}$$

$$S \quad U \quad Q_p \tag{11}$$

— множество элементов из U , являющихся квадратичными вычетами;

$$\bar{S} \quad U \quad \overline{Q_p} \tag{12}$$

— множество элементов из U , являющихся квадратичными невычетами;

$$S \quad \{ \; x \mid x \quad S\}. \tag{13}$$

Заметим, что при условии $p \quad 3 \pmod 4$ выполнено равенство $\overline{Q_p} \quad Q_p$, поскольку в этом случае $1 \quad \overline{Q_p}$. Поэтому для таких значений p выполняется условие $S \quad S \quad$.

Легко увидеть, что в обозначениях (10)–(12) выполнено равенство $U \quad \{x^2 \quad 1 \mid x \quad Z_p^* \setminus \{ \; 1\}\}$, т.е. $|U| \quad |Q_p| \quad 1 \quad \frac{p \quad 3}{2}$, и при этом

$$U \quad S \quad \bar{S} \text{ и } S \quad \bar{S} \quad , \tag{14}$$

поскольку $Q_p \quad \overline{Q_p} \quad$.

Для доказательства основной теоремы необходимы следующие леммы.

Лемма 1. Пусть $p \quad 3(\mathrm{mod}4)$. Тогда $|S| \quad |\bar{S}| \quad \frac{p \quad 3}{4}$.

Доказательство. Согласно (10) и (11) количество элементов множества S равно количеству квадратичных вычетов среди элементов вида $x^2 \quad 1$. Задача нахождения количества таких квадратичных вычетов решалась в лемме 2 работы [15] и затем обобщена и решена в работе [16], в которой $|S| \quad rr_1$ — количество пар вида $(a, a \quad 1) \quad Q_p \quad Q_p$. Тогда согласно следствию 2 из [16] и с учетом того, что $1 \quad Q_p, \quad 1 \quad Q_p$, получаем

$$rr_1 \quad \frac{p \quad 3 \quad \frac{1}{p} \quad \frac{1}{p}}{4} \quad \frac{p \quad 4 \quad 1}{4} \quad \frac{p \quad 3}{4},$$

откуда $|S| \quad \frac{p \quad 3}{4}$.

В силу равенства $|U| \quad \frac{p \quad 3}{2}$ и с учетом (14) получаем

$$|\bar{S}| \quad |U| \quad |S| \quad \frac{p \quad 3}{4}.$$

Лемма 1 доказана.

Лемма 2. Пусть p — простое. Тогда:

1) для любого $u \quad Z_p^*$ имеем $u \quad S \quad u^{\quad 1} \quad S$;

2) для любого $u \quad Z_p^*$ имеем $u \quad S \quad u^{\quad 1} \quad S$.

Доказательство . 1. Вначале докажем импликацию $u \quad S \quad u^{\quad 1} \quad S$ для любого $u \quad Z_p^*$.

Пусть $u \quad S$. Согласно (10) и (11) это означает, что существует такое $x \quad 2, 3, \ldots, \frac{p \quad 1}{2}$, что

$$u \quad x^2 \quad 1. \tag{15}$$

Следует доказать, что

$$y \quad 2, 3, \ldots, \frac{p \quad 1}{2} \; : u^{\quad 1} \quad y^2 \quad 1.$$

В уравнении (15) разделим левую и правую части на u^2:

$$u^{\quad 1} \quad \frac{x^2}{u^2} \quad \frac{1}{u^2} \quad 1 \quad 1 \quad \frac{x^2 \quad 1 \quad u^2}{u^2} \quad 1 \quad \frac{u \quad u^2}{u^2} \quad 1$$
$$\frac{u(u \quad 1)}{u^2} \quad 1 \quad \frac{ux^2}{u^2} \quad 1 \quad \frac{x^2}{u} \quad 1. \tag{16}$$

Поскольку $u \quad S$, то согласно (10) имеем $u \quad Q_p$; следовательно, $z \quad Z_p^*: u \quad z^2$. Тогда (16) можно переписать как

$$u^{\quad 1} \quad \frac{x^2}{z^2} \quad 1 \quad \frac{x}{z}^{\quad 2} \quad 1.$$

При этом $\frac{x}{z}$ 1, так как u^{1} 0. Полагая y $\frac{x}{z}$, получаем (15), что и требовалось доказать.

Обратная импликация доказывается с использованием уже доказанной. Пусть для некоторого u Z_p^* выполнено условие u^{1} S. Тогда на основании доказанного имеем $(u^{1})^{1}$ S, т.е. u S. Первое утверждение доказано.

2. Пусть u S. Тогда согласно (13) u S. Из первого утверждения леммы 2 следует, что $(u)^{1}$ S, т.е. u^{1} S, откуда u^{1} S. Лемма 2 доказана.

Следствие 1. Пусть p $7(\mathrm{mod}\,8)$. Тогда:

1) множество S состоит из элемента 1 и пар элементов вида (a, a^{1}) для некоторых a $Q_p \setminus \{1\}$, причем число таких пар равно $\frac{p\ 7}{8}$;

2) множество S состоит из элемента 1 и пар элементов вида (a, a^{1}) для некоторых a $\overline{Q_p} \setminus \{1\}$, причем число таких пар равно $\frac{p\ 7}{8}$.

Доказательство. 1. Заметим, что при условии p $7(\mathrm{mod}\,8)$ выполняется условие 2 Q_p. Поэтому когда x пробегает все значения вида $2,3,\ldots,\frac{p\ 1}{2}$, то выражение x^2 пробегает все значения из $Q_p \setminus \{1\}$; в частности, $x: x^2$ 2. Тогда $x: x^2$ 1 1, причем 1 Q_p, следовательно 1 S.

Далее, из конгруэнции p $7(\mathrm{mod}\,8)$ следует конгруэнция p $3(\mathrm{mod}\,4)$; следовательно, 1 Q_p, а значит 1 S.

Таким образом, для всех таких a S, что a 1, выполнено условие a^{1} a, а значит пары вида (a, a^{1}) при a 1 состоят из разных элементов. Согласно п. 1 леммы 2 множество S помимо элемента 1 содержит пары вида (a, a^{1}). Тогда количество таких пар равно $\frac{|S|\ 1}{2}$ $\frac{\frac{p\ 3}{4}\ 1}{2}$ $\frac{p\ 7}{8}$; п. 1 следствия 1 доказан.

2. Поскольку согласно п. 1 1 S, имеем 1 S. Далее доказательство выполняется аналогично доказатеьству п. 1 следствия 1 с использованием п. 2 леммы 2.

Следствие 1 полностью доказано.

Лемма 3. Пусть p $3(\mathrm{mod}\,4)$. Тогда для любого a Z_p^* справедливо условие a $\overline{S}$ a^{1} $\overline{S}$.

Доказательство. Предположим обратное: пусть существует такое u Z_p, для которого u $\overline{S}$ и u^{1} $\overline{S}$. Тогда согласно (12)

$$x\ \ Z_p: u\ \ x^2\ \ 1;\quad z\ \ Z_p: u^{1}\ \ z^2\ \ 1.$$

Отсюда x^2 u 1 $u(1\ u^{1})$ z^2 и u x^2 $(z^{1})^2$ $(x\ z^{1})^2$. Однако тогда u Q_p, что противоречит определению (12) множества $\overline{S}$ как состоящего из квадратичных невычетов. Лемма 3 доказана.

Лемма 4. Пусть $p \equiv 3 \pmod 4$. Тогда справедливо следующее утверждение: из любой пары вида (u, u^{-1}), где $u \in \overline{Q} \setminus \{-1\}$, в точности один элемент (либо u, либо u^{-1}) принадлежит множеству $\overline{S}$.

Доказательство. Из леммы 3 следует, что из любой пары вида (u, u^{-1}), где $u \in \overline{Q} \setminus \{-1\}$, не более одного элемента принадлежит множеству $\overline{S}$. Осталось показать, что из каждой такой пары по крайней мере один элемент принадлежит множеству $\overline{S}$.

По определению (12) множество $\overline{S}$ содержит только квадратичные невычеты и не содержит элемента -1. Далее, согласно лемме 1 имеем $|\overline{S}| = \frac{p-3}{4}$, в то время как все множество квадратичных невычетов $\overline{Q_p}$ состоит из $\frac{p-1}{2}$ элементов. Это множество содержит элемент -1 (поскольку $p \equiv 3 \pmod 4$) и непересекающиеся пары элементов вида (a, a^{-1}), где $a \neq a^{-1}$ и $a, a^{-1} \in \overline{Q_p} \setminus \{-1\}$. Очевидно, что число таких пар составляет $\frac{\frac{p-1}{2}-1}{2} = \frac{p-3}{4}$. Согласно лемме 3 из каждой такой пары в множестве $\overline{S}$ может находиться не более одного элемента.

Пусть t — количество пар, элементы которых (по одному из пары) принадлежат множеству $\overline{S}$. Поскольку другие элементы в этом множестве отсутствуют, то $t = |\overline{S}| = \frac{p-3}{4}$, т.е. это количество равно количеству всех возможных таких пар. Следовательно, из каждой пары вида (a, a^{-1}), где $a \neq a^{-1}$ и $a, a^{-1} \in \overline{Q_p} \setminus \{-1\}$, в множество $\overline{S}$ попадает в точности один элемент, что и требовалось доказать. Лемма 4 доказана.

Следствие 2. Пусть $p \equiv 3 \pmod 4$. Тогда для любого $u \in S \setminus \{1\}$ в точности один элемент из пары (u, u^{-1}) будет принадлежать множеству $\overline{S}$.

Доказательство. Согласно (13) множество S состоит из квадратичных вычетов. Далее, поскольку $p \equiv 3 \pmod 4$ и $-1 \in Q_p$, то из $u \in S$ следует $u, u^{-1} \in Q_p$. Кроме того, при $u \in S \setminus \{1\}$ выполнены условия $u \neq 1$, $u^{-1} \neq 1$. Тогда $u \neq u^{-1}$ и согласно лемме 4 в точности один элемент из пары u, u^{-1} будет принадлежать множеству $\overline{S}$. Следствие 2 доказано.

Следствие 3. Пусть $p \equiv 7 \pmod 8$. Тогда $|S \cap \overline{S}| = \frac{p-7}{8}$.

Доказательство. Согласно следствию 1 представим множество S в виде

$$S = \{1\} \cup \{a_1, a_1^{-1}\} \cup \ldots \cup \{a_l, a_l^{-1}\}$$

для некоторых $a_i \in \overline{Q_p}$, $i \in \overline{1, l}$, где $l = \frac{p-7}{8}$.

Согласно следствию 2 из каждой пары a_i, a_i^{-1} в точности один элемент принадлежит множеству $\overline{S}$. Кроме того, $1 \notin \overline{S}$, так как $1 \in U$, т.е. точно $\frac{p-7}{8}$ элементов множества S принадлежат множеству $\overline{S}$. Следствие 3 полностью доказано.

Теорема 1. При $p \equiv 7 \pmod 8$ квадратичные кривые Эдвардса над F_p с параметрами $a = 1$ и $d = -2^{-1}$, а также скрученные кривые Эдвардса с параметрами $a = -1$ и $d = -2^{-1}$ являются суперсингулярными. Для этих значений a и d выполнено условие $j(a,d) = 66^3$.

Доказательство. Из сравнения $p \equiv 7 \pmod 8$ непосредственно следует сравнение $p \equiv 3 \pmod 4$, так как редукция выражения $8k - 7$, $k \in Z$, по модулю 4 дает выражение $4k - 3$, $k \in Z$. Следовательно, $p - 1$ делится на 4 и условие $p \equiv 7 \pmod 8$ не противоречит существованию суперсингулярной кривой Эдвардса над F_p.

Рассмотрим квадратичную кривую Эдвардса с одним параметром $d = -2$, причем при $p \equiv 7 \pmod 8$ справедливо [13]. Если кривая суперсингулярная, то суперсингулярными будут изоморфная ей кривая с параметром $d = -2^{-1}$ и ее пара квадратичного кручения — скрученная кривая Эдвардса с параметрами $a = -1$ и $d = -2^{-1}$. Поэтому для доказательства теоремы достаточно доказать, что при $d = -2$ порядок кривой (8) имеет вид $N_E = p + 1$ и, следовательно, кривая является суперсингулярной, или, что то же самое, доказать, что количество решений (9), у которых координаты не равны нулю или ∞, равно $p + 7$.

При $d = -2$ уравнение (9) примет вид

$$v^2 = 1 - \frac{1}{(u^2 - 1)}, \tag{17}$$

где с учетом исключения особых и неособых точек малых порядков $u, v = 0, 1, \sqrt{2}, \infty$.

Левая часть уравнения (17) принимает значения из множества U, для которого согласно (14) выполнены условия $U = S \cup \overline{S}$ и $S \cap \overline{S} = \varnothing$. Далее рассмотрим два случая — когда значение левой части (17) принадлежит множеству S и когда оно принадлежит множеству $\overline{S}$.

Для некоторой пары (u,v), являющейся решением (17), обозначим $a = v^2 + 1 \in U$. Тогда $u^2 + 1 = a^{-1}$, но при этом $u^2 + 1 \in U$. Поэтому для поиска количества решений (17) достаточно найти количество таких элементов $a \in U$, чтобы при этом выполнялось условие $a^{-1} \in U$.

Рассмотрим два случая.

Случай 1. Пусть $a \in S$. Тогда справедливы следующие эквивалентности:

$$a \in U \Leftrightarrow a^{-1} \in U \Leftrightarrow a \in S \Leftrightarrow a^{-1} \in U \overset{(1)}{\Leftrightarrow}$$

$$\overset{(1)}{\Leftrightarrow} a^{-1} \in S \Leftrightarrow a^{-1} \in U \setminus S \overset{(2)}{\Leftrightarrow} a^{-1} \in S \setminus \overline{S},$$

где равносильность $\overset{(1)}{\Leftrightarrow}$ выполнена ввиду п. 2 следствия 1, а равносильность $\overset{(2)}{\Leftrightarrow}$ выполнена вследствие того, что $S = -S$, поскольку при $p \equiv 3 \pmod 4$ выполнено условие $-1 \notin Q_p$.

Далее, согласно следствию 3 имеем $|S \setminus \overline{S}| = \frac{p+7}{8}$, т.е. существует точно $\frac{p+7}{8}$ таких значений $a \in S$, что выполняется условие $a^{-1} \in U$.

Случай 2. Пусть $a \quad \overline{S}$. Тогда вследствие выполнения условия $1 \quad Q_p$ также выполнено условие $a \quad Q_p$, а значит, и $a^{\ 1} \quad Q_p$. Если при этом также выполнено условие $a^{\ 1} \quad U$, то также выполнено и условие $a^{\ 1} \quad S$. Тогда, обозначив $a^{\ 1} \quad b$ и соответственно $a \quad b^{\ 1}$, получим условия из случая 1, т.е. при $a \quad \overline{S}$ также существует точно $\frac{p \quad 7}{8}$ таких значений a, что $a^{\ 1} \quad U$.

Следовательно, всего существует $\frac{p \quad 7}{8} \quad \frac{p \quad 7}{8} \quad \frac{p \quad 7}{4}$ таких значений $a \quad U$, для которых выполнено условие $a^{\ 1} \quad U$. Для каждого такого значения $a \quad U$ существует только два значения: $u \quad \sqrt{a \quad 1}$ и $v \quad \sqrt{a^{\ 1} \quad 1}$, при которых выполняется условие (9). Следовательно, всего существует $4 \ \frac{p \quad 7}{4} \quad p \quad 7$ таких пар (u, v), являющихся решениями (9), при этом $u, v \quad 0, \ 1, \ \sqrt{2}, \quad$. Тогда соответствующие им пары (x, y) будут решениями (8) при $d \quad 2$. Добавляя к множеству решений восемь точек малых порядков, получаем $p \quad 7 \quad 8 \quad p \quad 1$ пар, являющихся решениями уравнения (8) при $d \quad 2$, поэтому квадратичная кривая $E_{1,2}$ является суперсингулярной. Как было замечено ранее, при этом также суперсингулярными будут квадратичная кривая $E_{1,2^{\ 1}}$ и скрученные кривые $E_{\ 1,\ 2}$ и $E_{\ 1,\ 2^{\ 1}}$.

Теорема 1 доказана.

Пример 1. Проверить, что кривая

$$E_{1,2} : x^2 \quad y^2 \quad 1 \quad 2x^2 y^2$$

над полем F_{23} является суперсингулярной. Найти ее точки.

Поскольку $23 \quad 2 \ 8 \quad 7$, то согласно теореме 1 кривая должна быть суперсингулярной. Запишем уравнение кривой в форме (9):

$$y^{\ 2} \quad 1 \quad \frac{1}{x^{\ 2} \quad 1}$$

и выделим восемь точек малых порядков:

$$O \quad (1,0), \ D_0 \quad (\ 1,0), \quad F_0 \quad (0, \quad 1), \ D_{1,2} \quad (\ 14, \quad), \ F_{1,2} \quad (\ , \quad 14). \quad (18)$$

Построим множество значений, которые принимает левая часть уравнения (8):

$$U \quad \{y^{\ 2} \quad 1 \mid y \quad F_{23}^{*} \setminus \{\ 1\}\},$$

и множество значений, которые принимает правая часть уравнения (8):

$$U^{\ 1} \quad \frac{1}{x^{\ 2} \quad 1} \mid x \quad F_{23}^{*} \setminus \{\ 1\} \quad .$$

Для удобства элементы множеств U и $U^{\ 1}$ занесем в табл. 1.

Таблица 1

Значения $x^{\ 1}$ и $y^{\ 1}$	2	3	4	5	6	7	8	9	10	11
Значения $y^{\ 2}$	4	9	16	2	13	3	18	12	8	6
Значения $y^{\ 2} \quad 1$	3	8	15	1	12	2	17	11	7	5
Значения $\frac{1}{x^{\ 2} \quad 1}$	15	20	3	22	21	11	19	2	13	9

Заметим, что третья и четвертая строки таблицы содержат множества U и U^{1} соответственно. Пересечение этих множеств состоит из четырех элементов:

$$U \quad (U^{1}) \quad \{2, 3, 11, 15\},$$

и это отражено в доказательстве теоремы 1: $\frac{23 \quad 7}{4} \quad 4$.

Для каждого $a \quad U \quad (U^{1})$ получаем по два значения $x \quad F_{23}^{*} \setminus \{1\}$ таких, что $\frac{1}{x^{2} \quad 1} \quad a$, и по два значения $y \quad F_{23}^{*} \setminus \{1\}$ таких, что $y^{2} \quad 1 \quad a$. Поэтому каждому значению $a \quad U \quad (U^{1})$ соответствует четыре точки кривой $E_{1,2}$. В табл. 2 приведены эти значения.

Таблица 2

Значения координат точек кривой $E_{1,2}$, соответствующие параметру a	$a \quad 2$	$a \quad 3$	$a \quad 11$	$a \quad 15$
Значения x: $\frac{1}{x^{2} \quad 1} \quad a$, при которых выполняются условия	± 9	± 4	± 7	± 2
Значения y: $y^{2} \quad 1 \quad a$, при которых выполняются условия	± 7	± 2	± 9	± 4

В результате получаем 16 точек кривой:

$$(9, \quad 7); (4, \quad 2); (7, \quad 9); (2, \quad 4). \qquad (19)$$

Множества (18) и (19) содержат все 24 точки кривой, которая является суперсингулярной с порядком $p \quad 1$.

При $d \quad 2^{1}$ j-инвариант (6) квадратичной суперсингулярной кривой Эдвардса равен $j(1,2) \quad 2^{3} \quad 3^{3} \quad 11^{3} \quad 66^{3}$. Такое же значение имеет j-инвариант скрученной суперсингулярной кривой Эдвардса $j(1, \quad 2) \quad 66^{3}$.

При $x, y \quad 0,1$ уравнения кривой (8) при $d \quad 2^{1}$ для пары изоморфных квадратичных кривых имеют вид

$$E_{1,d}: \quad y^{2} \quad 1 \quad \frac{1}{x^{2} \quad 1}; \quad E_{1,d^{1}}: \quad y^{2} \quad 1 \quad \frac{2^{1}}{x^{2} \quad 1}, \quad x \quad 2,3,\ldots,\frac{p \quad 1}{2}. \qquad (20)$$

Так как элемент 1 — квадратичный невычет, а 2 — вычет, то в соответствии с леммой 1 среди значений, которые принимают правые части уравнений (20), имеется точно $\frac{p \quad 3}{2}$, одинаковое для квадратичных вычетов и столько же квадратичных невычетов. Такое же соотношение сохраняется и для левых частей уравнений (20). Из доказанной теоремы 1 следует, что при $p \quad 7 \pmod 8$ ровно половина всех квадратичных вычетов, имеющихся среди значений левой и правой частей этих уравнений, совпадают. Такое же утверждение справедливо для квадратичных невычетов.

Следует отметить, что для полной суперсингулярной кривой с параметром $d \quad 1$ и j-инвариантом $j(1, \quad 1) \quad 12^{3}$ два уравнения для пары квадратичного кручения вырождаются в одно:

$$E_{1,d\ 1}:\ y^{\ 2}\ \ 1\ \ \frac{2}{x^{\ 2}\ \ 1},\quad x\ \ 2,3,\ldots,\frac{p\ \ 1}{2},$$

совпадающее с (8) после замены $2\ \ 2^{\ 1}$.

3. СУПЕРСИНГУЛЯРНЫЕ СКРУЧЕННЫЕ КРИВЫЕ ЭДВАРДСА С ДРУГИМИ ЗНАЧЕНИЯМИ *j*-ИНВАРИАНТА

В работе [5] определены все суперсингулярные кривые в классе кривых в форме Лежандра с одним параметром λ:

$$E_\lambda:\ y^2\ \ x(x\ \ 1)(x\ \ \lambda),\ \lambda\ \ 0,1 \tag{21}$$

и *j*-инвариантом

$$j(\lambda)\ \ \frac{2^8(\lambda^2\ \ \lambda\ \ 1)^3}{\lambda^2(\lambda\ \ 1)^2}, \tag{22}$$

а также доказана следующая теорема (см. [5, теорема 4.34]).

Пусть p — нечетное простое число. Определим полином

$$H(z)\ \ \sum_{i\ \ 0}^{(p\ \ 1)/2}\binom{(p\ \ 1)/2}{i}z^i. \tag{23}$$

Тогда эллиптическая кривая (21) с $\lambda\ \ F_p$ является суперсингулярной тогда и только тогда, когда $H(\lambda)\ \ 0$.

Если $\lambda\ \ Q_p$ и существует такое $e\ \ F_p$, что $\lambda\ \ e^2$, то кривая (21) после замены $\frac{x}{e}\ \ u$, $\frac{y^3}{e^3}\ \ Dv^2$ сводится к форме Монтгомери (5):

$$Dv^2\ \ u^3\ \ \frac{1\ \ e^2}{e}u^2\ \ u. \tag{24}$$

Приравнивая коэффициенты $\frac{1\ \ e^2}{e}\ \ 2\frac{1\ \ d}{1\ \ d}$ при u^2 в уравнении (24) и уравнении (5), получаем

$$d\ \ \left(\frac{1\ \ e}{1\ \ e}\right)^2\ \ \left(\frac{1\ \ \sqrt{\lambda}}{1\ \ \sqrt{\lambda}}\right)^2. \tag{25}$$

Отсюда следует, что изоморфизм между кривыми в форме Лежандра (21) и Эдвардса (1) достигается лишь для квадратичных кривых Эдвардса (7) при $\lambda\ \ e^2$. Согласно примеру 4.14 из [4] при $p\ \ 23$ факторизация полинома (23) 11-й степени имеет вид

$$\begin{aligned}H(z)\ \ &(z\ \ 3)(z\ \ 8)(z\ \ 21)(z\ \ 11)(z\ \ 13)(z\ \ 16)\\ &(z\ \ 2)(z\ \ 12)(z\ \ 1)(z^2\ \ z\ \ 1).\end{aligned} \tag{26}$$

Здесь первые шесть сомножителей содержат пары взаимно-обратных корней $\lambda_1^{\ 1}$, $(1\ \ \lambda_1)^{\ 1}$, $\left(\frac{\lambda_1}{1\ \ \lambda_1}\right)^{\ 1}$, $\lambda_1\ \ 3$, порождающих изоморфные суперсингулярные кривые с одинаковым значением *j*-инварианта (22), равным $j(3)\ \ 66^3 \bmod 23\ \ 19$. Они записаны в первой строке табл. 3. Во второй строке таблицы представлены значения параметра d изоморфных суперсингулярных квадратичных кривых Эдвардса, вычисленных согласно формуле (2), где

$\sqrt{3}$ 7, $\sqrt{13}$ 6. Корни полинома (z), являющиеся квадратичными невычетами, исключаются при построении квадратичных кривых Эдвардса. В результате в табл. 3 остались две пары параметров d $\{2^{1}, 13^{1}\}$.

Таблица 3

Корни полинома	λ_1	$\lambda_1{}^1$	1 λ_1	1 $\lambda_1{}^1$	$\frac{\lambda_1}{\lambda_1 \quad 1}$	$\frac{\lambda_1}{\lambda_1 \quad 1}^{1}$
Значение корня λ	3	8	21	11	13	16
Соответствующие значения параматра *d*	12	2	–	–	13	16

Следующие три корня полинома (26) порождают суперсингулярные кривые в форме Лежандра с *j*-инвариантом (22), равным $j(2) \quad 12^3 \bmod 23 \quad 3$. Квадратичным вычетам $\lambda \quad 2^{1}$ согласно (25) соответствуют параметры $d \quad 3^{1}$ изоморфных суперсингулярных квадратичных кривых Эдвардса. Тот же результат получаем с помощью формулы (12) из работы [1] для кривых с $j(1, d) \quad 12^3$.

Итак, при $p \quad 23$ имеется шесть суперсингулярных квадратичных кривых Эдвардса с параметрами $d \quad \{2, 12, 13, 16, 3, 8\}$ со значениями *j*-инвариантов $j(1, d) \quad \{66^3, 12^3\}$. Их квадратичное кручение образует шесть суперсингулярных скрученных кривых Эдвардса с параметрами $a \quad 1$ и d. Других суперсингулярных кривых Эдвардса в этих классах над простым полем при $p \quad 23$ не существует. В разложении (26) полинома $H(z)$ последний сомножитель имеет два корня в расширении F_{p^2}, в котором согласно (29) возникают суперсингулярные скрученные кривые Эдвардса с нулевым *j*-инвариантом. Над простым полем в соответствии с утверждением 1 из [1] и факторизацией $H(z)$ (26) в данном примере их не существует.

Как следует из теоремы 4.34 из [4], число суперсингулярных кривых растет пропорционально модулю p. Например, при $p \quad 47$ имеется 10 суперсингулярных квадратичных кривых (9) с параметрами $d \quad \{2^{1}, 7^{1}, 4^{1}, 9^{1}, 17^{1}\}$, из которых только первые три пары значений определены теоремой 2 из [1] и теоремой 1 настоящей статьи. Эти теоремы позволяют легко найти суперсингулярные скрученные кривые Эдвардса при любых значениях p, тогда как в области криптографических приложений поиск других суперсингулярных кривых с помощью теоремы 4.34 из [4] и формулы (26) становится практически нереализуемым.

ЗАКЛЮЧЕНИЕ

В настоящей статье определены условия существования суперсингулярных скрученных кривых Эдвардса над простым полем с *j*-инвариантом, равным 66^3. Также построены суперсингулярные скрученные кривые с другими значениями *j*-инварианта и обобщены некоторые полученные ранее результаты, использующие изоморфизм кривых в формах Лежандра и Эдвардса. Приведены примеры построения суперсингулярных кривых Эдвардса с использованием полученных результатов.

СПИСОК ЛИТЕРАТУРЫ

1. Бессалов А.В., Ковальчук Л.В. Суперсингулярные скрученные кривые Эдвардса над простым полем. I. Суперсингулярные скрученные кривые Эдвардса с j-инвариантами, равными нулю и 12^3. *Кибернетика и системный анализ*. 2019. Т. 55, № 3. С. 3–10.
2. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Киев: КПИ имени Игоря Сикорского. Изд-во Політехніка, 2017. 272 с.
3. Bernstein D.J., Lange T. Faster addition and doubling on elliptic curves. In: *Advancesin 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. Vol. 4833. Berlin: Springer, 2007. P. 29–50.
4. 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.
5. Washington L.C. Elliptic curvres. Number theory and cryptography. Second Edition. CRC Press, 2008. 513 p.
6. De Feo L., Jao D., Plût J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Mathematical Cryptology*. 2014. Vol. 8, N 3. P. 209–247.
7. Unruh D. Non-interactive zero-knowledge proofs in the quantum random oracle model. Berlin; Heidelberg: Springer, 2015. P. 755–784.
8. Yoo 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. http://eprint.iacr.org/2017/186. 18 p.
9. 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.
10. 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.
11. Бессалов А.В., Цыганкова О.В. Классификация кривых в форме Эдвардса над простым полем. *Прикладная радиоэлектроника.* 2015. Т. 14. № 4. С. 197–203.
12. 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.
13. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых. Киев: ІВЦ «Політехніка», 2004. 224 с.
14. Morain F. Edwards curves and CM curves. ArXiv 0904/2243v1 [Math.NT] Apr.15, 2009. 15 p.
15. Бессалов А.В., Ковальчук Л.В. Точное число эллиптических кривых в канонической форме, изоморфных кривым Эдвардса над простым полем. *Кибернетика и системный анализ*. 2015. Т. 51, № 2. С. 3–12.
16. Беспалов О. Узагальнення леми Гаусса про характери пар елементів простого скінченного поля. Зб. наук. праць Інституту кібернетики ім. В.М. Глушкова НАН України та Кам'янець-Подольського національного університету ім. І. Огієнка. 2017. Випуск 15. С. 26–31.

Надійшла до редакції 15.05.2018

А.В. Бессалов, Л.В. Ковальчук

СУПЕРСІНГУЛЯРНІ СКРУЧЕНІ КРИВІ ЕДВАРДСА НАД ПРОСТИМ ПОЛЕМ. II. СУПЕРСІНГУЛЯРНІ СКРУЧЕНІ КРИВІ ЕДВАРДСА З *j*-ІНВАРІАНТОМ, ЯКИЙ ДОРІВНЮЄ 66^3

Анотація. В продовження результатів, отриманих в [1], сформульовано і доведено теореми про умови існування суперсінгулярних кривих Едвардса над простим полем з *j*-інваріантом, який дорівнює 66^3, і з іншими значеннями *j*-інваріантів. Наведено узагальнення отриманих раніше результатів, що використовує ізоморфізм кривих в формах Лежандра і Едвардса.

Ключові слова: суперсінгулярна крива, повна крива Едвардса, скручена крива Едвардса, квадратична крива Едвардса, пара квадратичного крутіння, порядок точки, символ Лежандра, квадратичне лишок квадратичний нелишок.

A.V. Bessalov, L.V. Kovalchuk

SUPERSINGULAR TWISTED EDWARDS CURVES OVER A SIMPLE FIELD. II. SUPERSINGULAR TWISTED EDWARDS CURVES WITH AN *j*-INVARIANT, EQUAL 66^3

Abstract. In continuation of the results obtained in [1], theorems on the existence conditions for Edwards super singular curves over a simple field with an *j*-invariant and with other values of the invariants were formulated and proved. A generalization of the previously obtained results using the isomorphism of curves in the Legendre and Edwards forms is given.

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

Бессалов Анатолий Владимирович,
доктор техн. наук, профессор, профессор кафедры Киевского университета имени Бориса Гринченко,, 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.