МЕТОДЫ И МОДЕЛИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

УДК621.391.15 : 519.7

2-ИЗОГЕНИИ ПОЛНЫХ И КВАДРАТИЧНЫХ КРИВЫХ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

А. В. БЕССАЛОВ

Дан анализ условий существования 2-изогений полных и квадратичных кривых Эдвардса над простым полем. Дан обзор свойств трех классов кривых в обобщенной форме Эдвардса: полных, скрученных и квадратичных кривых Эдвардса. Для корректной записи отображающих функций и определения степени изогении предложено использовать модифицированный закон сложения точек. Обсуждаются проблемы нахождения дуальных 2-изогений между классами полных, квадратичных и скрученных кривых Эдвардса.

Ключевые слова: кривая в обобщенной форме Эдвардса, скрученная кривая Эдвардса, квадратичная кривая Эдвардса, порядок кривой, порядок точки, изоморфизм, изогения, квадратичное кручение, квадратичный вычет, квадратичный невычет.

ВВЕДЕНИЕ

Одной из известных перспектив постквантовой криптографии являются изогении суперсингулярных эллиптических кривых с возможно большим числом подгрупп их точек. Проблема дискретного логарифмирования классической эллиптической криптографии заменяется проблемой поиска одной из изогений великого множества подгрупп такой нециклической кривой, достаточно стойкой к атакам виртуального квантового компьютера. На сегодняшний день нарастающий интерес к изогениям связывается с наименьшей длиной ключа в предлагаемых алгоритмах в сравнении с другими известными кандидатами постквантовой криптографии при заданном уровне стойкости.

Свойства изогений для кривых в форме Веерштрасса достаточно хорошо изучены. Значительно меньше нам известны эффективные методы построения и свойства изогений перспективных классов кривых в форме Эдвардса.

Кривые Эдвардса с одним параметром, определенные в работе [1], имеют очень привлекательные для криптографии преимущества: максимальная скорость экспоненцирования точки, полнота и универсальность закона сложения точек, аффинные координаты нейтрального элемента группы точек, повышенная безопасность в отношении атак побочного канала. Программирование групповых операций становится более эффективным и ускоряется в связи с отсутствием особой точки на бесконечности как нуля абелевой группы точек. Введение второго параметра кривой в работе [2] расширило класс кривых в форме Эдвардса и породило кривые с новыми свойствами, интересными для криптографических приложений. В данной статье обсуждаются свойства 2-изогений двух классов этих кривых, в частности, условия их существования над простым полем.

Среди многочисленных работ по этой проблематике выделим статьи [3, 4], в которых впервые получены формулы изогений для двух классов кривых в форме Эдвардса. Наш анализ в данной работе опирается на их результаты.

В разделе 1 статьи приводятся основные определения для изоморфных кривых в форме Монтгомери и Эдвардса, законы сложения и удвоения точек последних с модификацией, адаптированной к горизонтальной симметрии обратных точек. Дан краткий обзор свойств трех классов кривых в обобщенной форме Эдвардса в соответствии с принятой в [5, 6] классификацией. В разделе 2 дается детальный анализ одного из методов получения 2-изогений для двух классов полных и квадратичных кривых Эдвардса, приводятся примеры и обсуждаются условия существования 2-изогений в этих классах над простым полем.

1. ИЗОМОРФИЗМЫ И СВОЙСТВА КРИВЫХ ЭДВАРДСА

Анализ изогений кривых Эдвардса часто опирается на кривые в форме Вейерштрасса и их частные случаи изоморфных кривых в форме Монтгомери или Лежандра. Запишем кривую форме Монтгомери над полем $F_q, q = p^m$, уравнением [2]

$$E_{C,D} : Dv^2 = u^3 + Cu^2 + u, \quad C = 2\frac{a+d}{a-d},$$

$$D = \frac{4}{a-d}, \quad a = \frac{C+2}{D}, \quad d = \frac{C-2}{D}, \quad C^2 \neq 4. \qquad (1)$$

Эта кривая рациональным преобразованием координат

$$y=\frac{u}{v},\quad x=\frac{u-1}{u+1},\quad \Rightarrow\quad u=\frac{1+x}{1-x},\, v=\frac{u}{y}. \qquad (2)$$

отображается в бирационально эквивалентную кривую *в обобщенной форме Эдвардса* [2,6] с уравнением

$$E_{a,d}:\ \begin{array}{c} x^2+ay^2=1+dx^2y^2, \\ a,d\in F_p^*, d\neq 1, a\neq d,\, p\neq 2 \end{array}. \qquad (3)$$

В отличие от уравнения этой кривой в [2] здесь мы параметр a умножаем на y^2 вместо x^2. Если квадратичный характер $\chi(ad)=-1$, кривая (3) изоморфна *полной кривой* Эдвардса [1] с одним параметром d

$$E_d:\ x^2+y^2=1+dx^2y^2, \chi(d)=-1, d\neq 0,1, \qquad (4)$$

В случае $\chi(ad)=1$, и $\chi(a)=\chi(d)=1$ имеет место изоморфизм кривой (3) с *квадратичной кривой Эдвардса* [6]

$$E_d:\ x^2+y^2=1+dx^2y^2, \chi(d)=1, d\neq 0,1, \qquad (5)$$

имеющей, в отличие от (4), параметр d, определенный как квадрат. Это отличие ведет к кардинально различным свойствам кривых (4) и (5) [6], которые резюмируются ниже. Несмотря на это, в мировой литературе эти классы кривых объединены общим термином *кривые Эдвардса* [2].

В работе [7] мы предложили поменять местами x и y координаты в форме кривой Эдвардса. Тогда модифицированный универсальный закон сложения точек имеет вид

$$(x_1,y_1)+(x_2,y_2)=$$

$$=\left(\frac{x_1x_2-ay_1y_2}{(1-dx_1x_2y_1y_2)},\frac{x_1y_2+x_2y_1}{(1+dx_1x_2y_1y_2)}\right). \qquad (6)$$

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

$$2(x_1,y_1)=\left(\frac{x_1^2-ay_1^2}{\left(1-dx_1^2y_1^2\right)},\frac{2x_1y_1}{\left(1+dx_1^2y_1^2\right)}\right). \qquad (7)$$

Использование модифицированных законов (6), (7) позволяет сохранить общепринятую горизонтальную симметрию (относительно оси x) обратных точек. Определяя теперь обратную точку как $-P=(x_1,\,-y_1)$, получим согласно (6) координаты нейтрального элемента группы точек $O=(x_1,y_1)+(x_1,\,-y_1)=(1,\,0)$. Кроме нейтрального элемента О на оси x также всегда лежит точка $D_0=(-1,\,0)$ второго порядка, для которой в соответствии с (7) $2D_0=(1,\,0)=O$. В зависимости от свойств параметров a и d можно получить еще 2 особые точки 2-го порядка и 2 или 4 точки 4-го порядка. Как следует из (3), на оси y могут лежать точки $\pm F_0=\left(0,\,\pm 1/\sqrt{a}\right)$ 4-го порядка, для которых $\pm 2F_0=D_0=(-1,\,0)$. Эти точки существуют над простым полем F_p, если параметр a является квадратом (квадратичным вычетом).

Из уравнения (3) определим квадраты:

$$x^2=\frac{1-ay^2}{1-dy^2},\ y^2=\frac{1-x^2}{a-dx^2},$$

порождающие особые точки на бесконечности (знак "∞"мы ставим при делении на 0):

$$D_{1,2}=\left(\pm\sqrt{\frac{a}{d}},\infty\right),\pm F_{11}=\left(\infty,\pm\frac{1}{\sqrt{d}}\right). \qquad (8)$$

Они возникают в случаях $\chi(ad)=1$ и $\chi(d)=1$ соответственно. Это, например, всегда выполняется в расширении поля F_{p^2}. По правилам предельного перехода и закона удвоения (7) можно проверить, что $2D_{1,2}=O,\ \pm 2F_1=D_0=(-1,\,0)$. Иными словами, при выполнении условий их существования особые точки $D_{1,2}$ есть точки 2-го порядка, а особые точки $\pm F_1$ – точки 4-го порядка.

Кроме перечисленных, точки 4-го порядка могут существовать как не особые при ненулевых координатах x и y.

Теорема 1. *Не особые точки 4-го порядка*

$$\pm F_2=\left(\sqrt[4]{\frac{a}{d}},\pm\sqrt{\frac{-1}{\sqrt{ad}}}\right),\ \pm F_3=\left(-\sqrt[4]{\frac{a}{d}},\pm\sqrt{\frac{-1}{\sqrt{ad}}}\right)$$

кривой в форме (1) при $x\neq 0$ существуют тогда и только тогда, когда выполняются условия:

(i) *при* $p\equiv -1 mod 4$: $\chi(a)=\chi(d)=-1$;

(ii) *при* $p\equiv 1 mod 4$: $\chi(a)=\chi(d)=1,\ ad=c^4$.

Доказательство теоремы 1 дано в работе [5]. Заметим, что с учетом 4-х корней 4-й степени из элемента поля число точек 4-го порядка для кривой (5), определенных теоремой 1, обычно равно 8 (для каждой точки (x_1,y_1) существует точка (y_1,x_1)).

Точки $\pm F_{2,3}$ можно рассматривать как точки деления на 2 особых точек 2-го порядка $D_{1,2}/2$ [6].

Пример 1. Для кривой $x^2-y^2=(1+3x^2y^2) mod 7$ (здесь $a=-1$, $d=3$ – квадратичные невычеты при $p=7\equiv 3\bmod 4$ и выполняются условия (i) теоремы 1)

точки 4-го порядка согласно теореме 1 имеют координаты $\pm F_{2,3} = (\pm 2, \pm 2)$. При удвоении их согласно (7) получим $2F_2 = (\pm 3, \infty) = D_{1,2}$. Порядок N_E этой кривой, включающей точки $O, \pm F_{2,3}, D_{0,1,2}$, равен 8, группа точек нециклическая с типом $T = (2, 2^2)$.

Пример 2. В условиях (ii) теоремы 1 рассмотрим кривую $x^2 + y^2 = (1 + 3x^2 y^2) mod 13$ (здесь $a = 1$, $d = 3$ – квадратичные вычеты при $p = 13$). Согласно теореме 1 находим точки 4-го порядка $\pm F_{2,3} = (\pm 6, \pm 4)$, $\pm F_{4,5} = (\pm 4, \pm 6)$. Кроме того, кривая имеет две точки 4-го порядка $\pm F_0 = (0, \pm 1)$ и две особые точки (8) 4-го порядка $\pm F_1 = (\infty, \pm 3)$. Удвоение точек $F_{2,3}$ согласно (7) дает точки $2F_2 = \left(\pm\sqrt{\frac{a}{d}}, \infty\right) = (\pm 3, \infty) = D_{1,2}$. Эта кривая, таким образом, содержит 12 точек 4-го порядка, имеет порядок $N_E = 16$ и является нециклической с типом $T = (2^2, 2^2)$. Точки 4-го порядка являются ключевыми при нахождении 2-изогений кривых Эдвардса.

С использованием правил предельного перехода в (6) для особых точек, можно найти координаты сумм:

$$
\begin{aligned}
&(x_1, y_1) + (-1, 0) = (-x_1, -y_1) = (x_1, y_1)^*, \\
&(x_1, y_1) + \left(\sqrt{\frac{a}{d}}, \infty\right) = \left(\sqrt{\frac{a}{d}} x_1^{-1}, \frac{1}{\sqrt{ad}} y_1^{-1}\right), \\
&(x_1, y_1) + \left(-\sqrt{\frac{a}{d}}, \infty\right) = \left(-\sqrt{\frac{a}{d}} x_1^{-1}, -\frac{1}{\sqrt{ad}} y_1^{-1}\right), \\
&(x_1, y_1) + \left(\infty, \frac{1}{\sqrt{d}}\right) = \left(-\frac{1}{\sqrt{d}} y_1^{-1}, \frac{1}{\sqrt{d}} x_1^{-1}\right), \qquad (9) \\
&(x_1, y_1) + \left(\infty, -\frac{1}{\sqrt{d}}\right) = \left(\frac{1}{\sqrt{d}} y_1^{-1}, -\frac{1}{\sqrt{d}} x_1^{-1}\right).
\end{aligned}
$$

Все найденные суммы удовлетворяют уравнению (1) при подстановке, т.е. являются точками кривой.

Подчеркнем, что использование правил предельного перехода сохраняет операцию сложения любых пар точек, включая особые. Это позволяет говорить об изоморфизме кривых в форме Монтгомери и Эдвардса [6,8].

Обоснование новой классификации кривых в обобщенной форме Эдвардса дано в работах [6, 8]. Ниже даны определения 3-х классов этих кривых и перечень фундаментальных свойств кривых разных классов.

В зависимости от свойств параметров a и d кривые в обобщенной форме Эдвардса (1) разбиваются на 3 непересекающиеся класса:

- *полные кривые Эдвардса* (с условием C1: $\chi(ad) = -1$;
- *скрученные кривые Эдвардса* (с условиями C2.1: $\chi(a) = \chi(d) = -1$;
- квадратичные кривые Эдвардса (с условиями C2.2: $\chi(a) = \chi(d) = 1$.

Основные свойства этих классов кривых [6–8]:

1. В отношении точек 2-го порядка первый класс полных кривых Эдвардса над простым полем является классом *циклических* кривых, скрученные же и квадратичные кривые Эдвардса образуют классы *нециклических* кривых. Максимальный порядок точек кривых последних классов не превышает $N_E / 2$.

2. Класс полных кривых Эдвардса не содержит особых точек.

3. Скрученные кривые Эдвардса содержат лишь две особых точки 2-го порядка $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$.

4. Квадратичные кривые Эдвардса содержат две особые точки 2-го порядка $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ и две особые точки 4-го порядка $\pm F_{11} = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$.

5. Скрученные и квадратичные кривые Эдвардса образуют пары квадратичного кручения на основе преобразования параметров: $\tilde{a} = ca$, $\tilde{d} = cd$, $\chi(c) = -1$.

6. В классах скрученных и квадратичных кривых Эдвардса замена $a \leftrightarrow d$ дает изоморфизм $E_{a,d} \sim E_{d,a}$.

7. Полные и квадратичные кривые Эдвардса изоморфны кривым с параметром $a = 1$: $E_{a,d} \sim E_{1.,d/a}$. Введение нового параметра a в уравнение кривой (1) оправдано лишь для класса скрученных кривых Эдвардса.

8. Скрученные кривые Эдвардса при $p \equiv 1 \bmod 4$ не имеют точек 4-го порядка.

9. Для точек нечетного порядка закон сложения точек (6) всегда является полным (т.е. сумма любой пары точек не дает особой точки).

2. 2-ИЗОГЕНИИ ПОЛНЫХ И КВАДРАТИЧНЫХ КРИВЫХ ЭДВАРДСА

Изогения эллиптической кривой $E(K)$ над полем K в кривую $E'(K)$ есть гомоморфизм $\phi(E(\bar{K})) \to E'(\bar{K})$, задаваемый рациональными функциями. Это значит, что для всех $P, Q \in E(K)$, $\phi(P + Q) = \phi(P) + \phi(Q)$ и существуют рациональные функции [9]

$$\phi(x,y)=\left(\frac{p(x)}{q(x)},y\frac{f(x)}{g(x)}\right)=(x',y'),$$

отображающие точки кривой E в точки кривой E'. Степенью изогении называется максимальная из степеней $\alpha=\deg\phi(x,y)=\max\{\deg p(x),\deg q(x)\}$, а ее ядром – подгруппа $G\subseteq E$ порядка α, точки которой отображаются функцией $\phi(x,y)$ в нейтральный элемент группы О. Изогения сжимает точки кривой E в α раз и является сюръекцией (α точек кривой E отображаются в одну точку кривой E'). При $G=E$ изогения становится изоморфизмом.

Вычисление изогений обычно осуществляется по формулам Велю [9] для кривых в форме Вейерштрасса. В работах [3, 4] получены формулы изогений второй (2-изогении) и нечетных степеней, адаптированные, в частности, к кривым в форме Эдвардса (4) и (5) с одним параметром d. Проанализируем и расширим некоторые из их результатов с акцентом на анализ условий существования 2-изогений над простым полем.

Построение 2-изогений в [3] производится в 3 этапа:

1. Изоморфное преобразование $\psi_1(x,y)=(u,v)$ кривой Эдвардса в форму Монтгомери.
2. Построение 2-изоогений $\psi_2(u,v)=(U,V)$.
3. Обратная трансформация $\psi_3(U,V)=(x,y)$ изогенной кривой в форме Монтгомери в форму Эдвардса.

В итоге находится композиция $\phi(x,y)=$ $=\psi_1\circ\psi_2\circ\psi_3$ трех отображений между кривой E и изогенной кривой E'.

На первом этапе $E_d\to E_{C,D}$ кривая Эдвардса $x^2+y^2=1+dx^2y^2$ рациональным преобразованием (2)

$$\psi_1(x,y)=((a-d)\frac{1+u}{1-u},(a-d)\frac{2u}{v})$$

трансформируется в бирационально эквивалентную форму Монтгомери

$$v^2=u^3+2(a+d)u^2+(a-d)^2u \qquad (10)$$

кривой, изоморфной (1). Точка (0,0) есть точка 2-го порядка этой кривой, которая вместе с точкой на бесконечности как нейтральным элементом группы образует ядро 2-изогении. Требуется найти параметры $\bar a$ и $\bar d$ изогенной кривой E' с уравнением (10) и рациональную функцию $\psi_2(u,v)=(U,V)$.

Для кривой Монтгомери общего вида

$$v^2=u^3+cu^2+bu \qquad (11)$$

нахождение 2-изогений хорошо известно [9]. На основе формул Велю, использующих законы сложения точек кривой в общей форме Веерштрасса, для кривой (11) можно получить 2-изогению ([9], пример 12.4)

$$\psi_2(u,v)=\left(\frac{u^2+cx+b}{u},\frac{u^2-b}{u^2}v\right)=(U,V) \qquad (12)$$

и уравнение изогенной кривой

$$V^2=U^3-2cU^2+(c^2-4b)U. \qquad (13)$$

Дискриминант квадратного уравнения в правой части (12) равен $\Delta=16b$, и, в зависимости от значения $\chi(b)$, кривая (13) имеет одну или 3 точки 2-го порядка. В первом случае можно построить одну 2-изогению, во втором – 3 (для трех ядер как подгрупп 2-го порядка).

Ключевым в данной работе является вопрос о существовании 2-изогений в 3-х классах кривых Эдвардса над простым полем. Как следует из (10) и (11), к форме Монтгомери (1) или (10) (и, соответственно, к форме Эдвардса) можно привести лишь те кривые (11) общего вида, параметр b которых является квадратом: $\chi(b)=1$. Это связано с существованием на кривой (11) точек 4-го порядка $F=(u_1,v_1)$, таких, что $2F=(0,0)$. Тогда, принимая $b=u_1^2$, уравнение (11) приводится к виду

$$v^2=u^3+cu_1u^2+u_1^2u \qquad (14)$$

или изоморфной (1) (или ее квадратичному кручению) кривой

$$c=2\frac{a+d}{a-d}. \qquad (15)$$

Эта кривая бирационально эквивалентна кривой (3) в обобщенной форме Эдвардса (при $v^2\to Dv^2$). Уравнение (14) эквивалентно (10) при $u_1^2=(a-d)^2$ и $cu_1=2(a+d)$.

Таким образом, 2-изогенная кривая (13) с дискриминантом $\Delta=16u_1^2$ в этом случае имеет 3 точки 2-го порядка, и соответствующие изогении могут находиться лишь в классах квадратичных и скрученных кривых Эдвардса, образующих пары квадратичного кручения. В то же время кривая E, для которой строится изогения, может иметь одну точку 2-го порядка и 2 точки 4-го порядка (класс полных кривых Эдвардса), так и принадлежать другим классам кривых Эдвардса с тремя точками 2-го порядка. Например, при $p\equiv 3\bmod 4$ суперсингулярная кривая $v^2=u^3+u$ (для нее $\chi(c^2-4b)=-1$) имеет одну точку 2-го порядка и 2 точки 4-го порядка и изоморфна полной кривой Эдвардса. Ее 2-изогенная кривая (13)

$V^2 = U^3 - 4U$ имеет 3 точки 2-го порядка и попадает в классы квадратичных и скрученных кривых Эдвардса с одним порядком $p+1$ этих кривых. Однако элемент (–4) есть квадратичный невычет и кривая Эдвардса, изоморфная кривой $V^2 = U^3 - 4U$, не существует. Однако, принимая $U \to U - 2$, получим изоморфную кривую, $V^2 = U^3 + 6U^2 + (2\sqrt{2})^2 U$ для которой изоморфизм с кривой Эдвардса при $p \equiv 3 \bmod 8$ существует. Таким образом, исходная кривая E вида (11) с адаптацией к кривым Эдвардса может иметь одну или 3 точки второго порядка и, следовательно, над простым полем принадлежит одному из классов полных, скрученных или квадратичных кривых Эдвардса. Все эти кривые в расширении F_{p^2}, в котором все элементы подполя F_p становятся квадратами, становятся квадратичными кривыми Эдвардса. В расширениях F_{p^n}, разумеется, также можно строить как полные, так и скрученные кривые Эдвардса.

Далее рассмотрим полные и квадратичные кривые (5) с одним параметром d, $a = 1$. В этом случае уравнения (10) и (11) тождественны при $c = 2(1+d)$, $b = (1-d)^2$ тогда $c^2 - 4b = 16d$ и уравнение изогенной кривой (13) в форме Монтгомери имеет вид

$$M1: \quad V^2 = U^3 - 4(1+d)U^2 + 16dU. \qquad (16)$$

Ее дискриминант $\Delta = 16(1-d)^2$, а соответствующие корни определяются как $2(1+d) \pm 2(1-d) = \{4, 4d\}$. Ее, следовательно, можно записать как

$$V^2 = U(U-4)(U-4d).$$

Кривая (16) с точностью до изоморфизма совпадает с изогенной кривой в форме (10), но с параметром $\bar{d}$

$$V^2 = U^3 + 2(1+\bar{d})U^2 + (1-\bar{d})^2 U. \qquad (17)$$

Из (14) – (17) можно получить равенства

$$2\frac{(1+\bar{d})}{(1-\bar{d})}U_1 = -4(1+d), \quad U_1^2 = 16d.$$

Отсюда после подстановки $U_1 = \pm 4\sqrt{d}$ получим

$$\frac{(1+\bar{d})}{(1-\bar{d})} = \frac{\mp(1+d)}{2\sqrt{d}} \Rightarrow \quad \bar{d}_1^{\pm 1} = \left(\frac{1-\sqrt{d}}{1+\sqrt{d}}\right)^2. \quad (18)$$

Итак, для кривой две изогенные кривые имеют два взаимно-обратных параметра изоморфных квадратичных кривых Эдвардса.

Формула (18) справедлива лишь для одной из 3-х точек 2-го порядка (0,0) кривой (13). Линейное смещение координаты $U \to \{U-4, U-4d\}$ в другие значения корней кубики в (16) приводит к двум альтернативным уравнениям изогенных кривых в форме Монтгомери:

$$M2: \quad V^2 = U^3 - 4(d-2)U^2 + 16(1-d)U.$$

$$M3: \quad V^2 = U^3 + 4(2d-1)U^2 - 16d(1-d)U.$$

На основе (14), (15) и этих уравнений можно получить еще две формулы для параметров $\bar{d}_{2,3}$ изогенных кривых, которые приведены ниже в теореме 1.

Обратное преобразование изогенных кривых в форме Монтгомери (M1, M2 и M3) в форму Эдвардса производится на основе рациональных функций (2) с учетом различных значений координат точек 4-го порядка $\pm U_1 \in \{4\sqrt{d}, 4\sqrt{1-d}, 4\sqrt{d(d-1)}\}$ или $\pm U_1 = 1 - \bar{d}$ с помощью функции

$$\psi_3(U,V) = \left(\frac{U-U_1}{U+U_1}, \frac{2U}{V}\sqrt{\frac{U_1}{1-\bar{d}}}\right) = (x,y).$$

Подстановка этих рациональных функций вида (2) в уравнения кривой в форме Монтгомери дает изогенную кривую Эдвардса $x^2 + y^2 = 1 + \bar{d}x^2y^2$.

Композиция $\phi(x,y) = \psi_1 \circ \psi_2 \circ \psi_3$ трех преобразований дает формулы 2-изогений для кривых в форме Эдвардса, приведенные ниже.

В работе [3] доказана теорема 1, которую мы приводим с учетом модификации законов сложения точек кривых Эдвардса и замены $(x \leftrightarrow y)$.

Теорема 1 [3]. Пусть E_d – кривая Эдвардса и определены элементы (возможно, в расширении) поля K $\delta^2 = d, \gamma^2 = 1-d, i^2 = -1$. Тогда существуют 2-изогении $E_d \to E'_d$, заданные функциями ϕ_1, ϕ_2, ϕ_3:

$$\phi_1(x,y) = \left(\frac{d \mp \delta}{d \pm \delta}\frac{\delta x^2 \pm 1}{\delta x^2 \mp 1}, i(\delta \mp 1)xy\right),$$

отображающей E_d в $E'_d : x^2 + y^2 = 1 + \bar{d}_1 x^2 y^2$ с параметрами

$$\bar{d}_1^{\pm 1} = \left(\frac{1-\delta}{1+\delta}\right)^2;$$

$$\phi_2(x,y) = \left(\frac{(\gamma \mp 1)x^2 \pm 1}{(\gamma \pm 1)x^2 \mp 1}, (\gamma \mp 1)xy\right),$$

отображающей E_d в $E'_d : x^2 + y^2 = 1 + \bar{d}_2 x^2 y^2$ с параметрами

$$\bar{d}_2^{\pm 1} = \left(\frac{1-\gamma}{1+\gamma}\right)^2;$$

$$\phi_3(x,y)=\left(-\frac{\delta x^2 \mp i\gamma-\delta}{\delta x^2 \pm i\gamma-\delta},(i\gamma\pm\delta)\frac{y}{x}\right),$$

отображающей E_d в $E'_d: x^2+y^2=1+\bar{d}_3 x^2y^2$ с параметрами

$$\bar{d}_3^{\pm 1}=\left(\frac{i\gamma\mp\delta}{i\gamma\pm\delta}\right)^2.$$

Здесь следует заметить, что общепринятым определением степени изогении является старшая из степеней $\frac{p(x)}{q(x)}$ первой рациональной функции преобразования $\phi(x,y)$ [9]. Оно справедливо для кривых в форме Вейерштрасса. Если обратиться к оригинальной теореме 1 [3], то приходим к парадоксальному результату: степень 2-изогении равна1. Принятый нами модифицированный закон сложения (6) точек кривой Эдвардса с симметрией обратных точек $\pm(x_1,y_1)=(x_1,\pm y_1)$ снимает этот парадокс ($\alpha=\deg(\phi)=2$).

Из формул теоремы 1 следует, что над простым полем существуют 2-изогении кривых E из классов полных (функция $\phi_2(x,y)$ при $\chi(1-d)=1$) и квадратичных кривых (все функции $\phi_{1,2,3}(x,y)$ при $\chi(d)=1$ и $\chi(-1)=1$, или $\chi(1-d)=1$, или $\chi(d)=1$ и $\chi(d-1)=1$). Изогенная кривая E' во всех случаях лежит в классе квадратичных кривых Эдвардса.

Пример 3. Пусть $p=11$ и задана полная кривая Эдвардса $E=E_7: x^2+y^2=1+7x^2y^2$, где $\chi(d=7)=-1$, $\chi(1-d=4)=1$ и порядком $N_E=16$. Согласно теореме 1 существует лишь пара 2-изогенных квадратичных кривых Эдвардса $E'=E_4$ и $E'=E_3$ с параметрами $d_{1,2}=\bar{d}^{\pm 1}=\{4,3\}$ и отображением $\phi_2(x,y)$. Они имеют тот же порядок $N_E=16$ (что отвечает известной теореме Тейта [9]), изоморфны между собой, но вместо одной имеют уже 3 точки 2-го порядка (кривые являются нециклическими) и 12 точек 4-го порядка. Среди них по две особых точки 2-го и 4-го порядков. Точки исходной полной кривой E обозначим P_i, а точки двух изогенных кривых E' как Q_i Как и при удвоении точек, отображение $\phi_2(x,y)$ сжимает прообраз (кривую E) вдвое, т.е. отображает пару точек кривой E в одну точку кривой E'. В отличие от удвоения, 2-изогения не обязательно уменьшает вдвое порядок точки четного порядка.

На кривой E имеем точки $(\pm1,0)$, $(0,\pm1)$, $(\pm2,\pm4)$, $(\pm3,\pm3)$, $(\pm4,\pm2)$. Пусть $P_1=(2,4)$ – точка 16-го порядка кривой. $P_2=(3,3)=6P_1$ – точка 8-го порядка, $P_3=(4,2)=11P_1$. На изогенной кривой $E'=E_4$, кроме базовых точек $O=(1,0)$ $D_0=(-1,0)$, $\pm F_0=(0,\pm1)$, имеем особые точки $D_{1,2}=(\pm5,\infty)$, $\pm F_1=(\infty,\pm5)$, и точки 4-го порядка $(\pm2,\pm3)$, $(\pm3,\pm2)$. Обозначим $Q_1=(2,3)$, $Q_2=(3,2)$. $P^*=P+D_0$. С помощью первого значения функции $\phi_2(x,y)$ вычисляем:

$$\pm\phi_2(P_1,P_1^*)^{(1)}=(3,\pm2)=\pm Q_2,$$

$$\pm\phi_2(P_3,P_3^*)^{(1)}=(-3,\pm2)=\mp Q_2^*,$$

$$\pm\phi_2(P_2,P_2^*)^{(1)}=(\infty,\pm5)=\pm F_1,$$

$$\phi_2(\pm F_0)^{(1)}=(-1,0)=D_0,$$

$$\phi_2(D_0.O)^{(1)}=(1,0)=O.$$

Вторая изогенная кривая $E'=E_3$ с параметром $d=3$, кроме базовых точек, имеет особые точки $D_{1,2}=(\pm2,\infty)$, $\pm F_1=(\infty,\pm2)$, и точки 4-го порядка $(\pm4,\pm4),(\pm5,\pm5)$. Пусть $R_1=(4,4)$, $R_2=(5,5)$. Согласно второго значения функции $\phi_2(x,y)^{(2)}$ получаем:

$$\pm\phi_2(P_1,P_1^*)^{(2)}=(4,\mp4)=\mp R_1,$$

$$\pm\phi_2(P_3,P_3^*)^{(2)}=(-4,\mp4)=\pm R_1^*,$$

$$\pm\phi_2(P_2,P_2^*)^{(2)}=(0,\pm1)=\pm F_0,$$

$$\phi_2(\pm F_0)^{(2)}=(-1,0)=D_0,$$

$$\phi_2(D_0.O)^{(2)}=(1,0)=O.$$

Итак, функция $\phi_2(x,y)$ отображает пару точек одинаковых порядков кривой в одну точку кривой E' (т.е. функция $\phi_2(x,y)$ – сюръекция), причем одна полная кривая Эдвардса отображается в две изоморфные квадратичные кривые.

Рассмотрим изогении квадратичных кривых. Для отображения $\phi_2(x,y)$ справедливо свойство

$$1-\bar{d}_2^{\pm1}=1-\left(\frac{1\mp\gamma}{1\pm\gamma}\right)^2=\frac{\pm4\gamma}{(1\pm\gamma)^2}.$$

Отсюда следует, что из пары изогенных кривых для одной кривой $\chi(1-\bar{d}_2)=1$ и можно вновь пользоваться функцией $\phi_2(x,y)$.

Пример 4. Построим изогению для квадратичной кривой $E=E_3$ из примера 3 с параметрами $d=3, 1-d=9, \gamma=3$. Одна из изогенных кривых при отображении $\phi_2(x,y)$ имеет тот же параметр $d=3$ и

те же точки $R_1=(4,4)$, $R_2=(5,5)$, $D_{1,2}=(\pm 2,\infty)$, $\pm F_1=(\infty,\pm 2)$, $\pm F_0=(0,\pm 1)$, $D_0, O.$ Отображение $\phi_2(x,y)^{(2)}$ этой кривой дает точки кривой E'

$$\pm\phi_2(R_1,R_1^*)^{(2)}=(\infty,\mp 2)=\pm F_1,$$

$$\pm\phi_2(R_2,R_2^*)^{(2)}=(0,\mp 1)=\mp F_0,$$

$$\phi_2(\pm \mathrm{F}_1,)^{(2)}=(2,\infty)=D_1,$$

$$\phi_2(D_1,D_2\ )^{(2)}=(-2,\infty,)=D_2,$$

$$\phi_2(\pm F_0)^{(2)}=(-1,0)=D_0,$$

$$\phi_2(D_0.O)^{(2)}=(1,0)=O.$$

Если повторно применить функцию $\phi_2(x,y)^{(2)}$ к точкам изогенной кривой E', получим точки кривой E'':

$$\phi_2(D_0.O)^{(2)}=(1,0)=O,$$

$$\phi_2(\pm F_0)^{(2)}=(-1,0)=D_0,$$

$$\phi_2(\pm F_1,)^{(2)}=(2,\infty)=D_1,$$

$$\phi_2(D_1,D_2\ )^{(2)}=(-2,\infty,)=D_2.$$

Таким образом, вторая изогения возвращает нас в точки исходной кривой ($E''=E$), причем за 2 шага отображаемые точки кривой E удваиваются (умножаются на α: точки 4-го порядка отображаются в точки 2-го порядка, а точки 2-го порядка – в точку O). Это пример дуальной 2-изогении $\hat{\phi}_2=\phi_2(x,y)^{(2)}$ для квадратичной кривой над простым полем.

В общем случае для изогении $\phi: E\to E'$ существует дуальная изогения $\hat{\phi}: E'\to E$, такая, что $\phi\circ\hat{\phi}=[\deg(\phi)=\alpha]$, [9]. Формулы теоремы 1 доказывают, что над полем F_p для полных кривых Эдвардса дуальная изогения не существует, но она существует в расширении F_{p^2}. В этом расширении параметр d полной кривой E становится квадратом и она становится квадратичной. Для нахождения дуальной изогении $\hat{\phi}: E'\to E$, например, к функции $\phi_1(x,y)$ со значениями параметра изогенной кривой

$$\overline{d}_1^{\pm 1}=\left(\frac{1-\delta}{1+\delta}\right)^2$$

требуется решить обратную задачу: по известному значению d_1 кривой E надо вычислить одно из подходящих значений параметра $\overline{\delta}$ кривой E', которое определяется похожей формулой

$$\overline{\delta}^{\pm 1}=\left(\frac{1\mp\sqrt{d_1}}{1\pm\sqrt{d_1}}\right).$$

Отсюда видно, что отображение в полную кривую Эдвардса E с квадратичным невычетом d_1 существует лишь в расширении F_{p^2} .

Скрученные кривые Эдвардса лежат за пределами отображений теоремы 1. За исключением суперсингулярных кривых, скрученная кривая как квадратичное кручение квадратичной кривой Эдвардса имеет другой порядок и соответствующие изогении не существуют. Если, однако, кривой E является полная кривая Эдвардса, то обращением ее параметра $d\to d^{-1}$ получаем ее квадратичное кручение, а соответствующая ее изогения (квадратичная кривая) будет иметь порядок соответствующей скрученной кривой. Известным преимуществом скрученной кривой перед квадратичной является наличие лишь двух особых точек вместо четырех [5, 6]. Остается открытым вопрос: как построить прямую 2-изогению из класса полных в класс скрученных кривых над простым полем. Для этого следует модифицировать отображения теоремы 1 с учетом двух параметров a и d. Этот вопрос будет рассмотрен в следующей работе. Пока можно утверждать, что в связи с отсутствием точек 4-го порядка в классе скрученных кривых Эдвардса при $p\equiv 1 \bmod 4$ 2-изогений в этом классе над простым полем не существует.

Литература

[1] *Bernstein D.J., Lange T.* Faster Addition and Doubling on Elliptic Curves // 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.

[2] *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, PP. 1-17.

[3] *Moody D.,, Shumow D. Analogues of Velus formulas for isogenies on alternate models of elliptic curves.* Cryptology ePrint Archive, Report 2011/430, http://eprint.iacr.org/, 2011.

[4] O. *Ahmadi O.,, and Granger R, On isogeny classes of Edwards curves over finite fields*, J. Number Theory, 132 (6), pp. 1337-1358, (2012).

[5] *Бессалов А.В.* Уникальные криптографические свойства нециклических скрученных кривых Эдвардса. Прикладная радиоэлектроника: научно-техн. журнал. – 2018. – Том 17. – №1, 2. – С. 49–54.

[6] *Бессалов А.В.* Эллиптические кривые в форме Эдвардса и криптография. Монография. «Политехника», Киев, 2017. – 272 с.

[7] *Бессалов А.В., Цыганкова О.В.* Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем. Проблемы передачи информации. – Том 51, вып 4, 2015. –С. 92–98.

[8] *Бессалов А.В., Цыганкова О.В.* Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой. Проблемы передачи информации, - Том 53 (1). – 2017. –С.101–111.

[9] *Washington L.C.* Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.

Поступила в редколлегию 16.10.2018

Бессалов Анатолий Владимирович, доктор технических наук, профессор, профессор НТУУ «КПИ им. Игоря Сикорского». Область научных интересов – асимметричная криптография.

УДК 621.391.15:519.7

Бессалов А. В. **2-ізогенії повних і квадратичних кривих Едвардса над простим полем** / А. В. Бессалов // Прикладная радиоэлектроника: науч. – техн. журнал. – 2018. – Том 17, № 3, 4. – С. 152–159.

Дано аналіз умов існування 2-ізогеній повних і квадратичних кривих Едвардса над простим полем. Дано огляд властивостей трьох класів кривих в узагальненій формі Едвардса: повних, скручених і квадратичних кривих Едвардса. Для коректного запису відображаючох функцій і визначення степеню 2-ізогеній запропоновано застосовувати модифікований закон складання точок. Обговорюються проблеми знаходження дуальних 2-ізогеній між класами повних квадратичних і скручених кривих Едвардса.

Ключові слова: крива в узагальненій формі Едвардса, скручена крива Едвардса, квадратична крива Едвардса, порядок кривої, порядок точки, ізоморфізм, ізогенія, квадратичне кручення, квадратичний лишок, квадратичний нелишок.

Бібліогр. 09 найм.

UDC 621.391.15:519.7

Bessalov A. V. **2-isogenies of complete and quadratic Edwards curves over prime field** / A. V. Bessalov // Applied Radio Electronics: Sci. Journ. – 2018. – Vol. 17, № 3, 4. – P. 152–159.

An analysis of the conditions for the existence of 2-isogenies of complete and quadratic Edwards curves over a prime field is given. An overview of the properties of the three classes of curves in the generalized Edwards form (complete, twisted, and quadratic Edwards curves) is considered. To correctly record the mapping functions and determine the degree of isogeny, the use of the modified law of addition of points is proposed. The problems of finding dual 2-isogenies between classes of complete, quadratic and twisted Edwards curves are discussed.

Keywords: curve in a generalized Edward form, twisted Edwards curve, quadratic Edwards curve, curve order, points order, addition of points, isomorphism, quadratic twist, square, non-square.

Ref.: 09 items.