УДК 621.391.15: 519.7
DOI: 10.31673/2409-7292.2019.046369

А.В. Бессалов, А.Н. Котенко, Д.Б. Третьяков

СЛОЖНОСТЬ ВЫЧИСЛЕНИЯ 3- И 5-ИЗОГЕНИЙ СУПЕРСИНГУЛЯРНЫХ КРИВЫХ ЭДВАРДСА

Дан анализ свойств 3- и 5-изогений полных и квадратичных суперсингулярных кривых Эдвардса. Для алгоритма инкапсуляции ключей SIDH предложено использовать изогении малых нечетных степеней 3 и 5. Получены формулы расчета изогений и верхних оценок сложности вычислений 3- и 5-изогений в проективных координатах.

Ключевые слова: кривая в обобщенной форме Эдвардса, полная кривая Эдвардса, скрученная кривая Эдвардса, квадратичная кривая Эдвардса, порядок точки, изоморфизм, изогения, степень изогении, квадратичный вычет, квадратичный невычет.

Введение

На сегодняшний день нарастающий интерес к изогениям связывается с наименьшей длиной ключа в предлагаемых алгоритмах (в частности, алгоритм инкапсуляции ключей SIDH[1]) в сравнении с другими известными кандидатами постквантовой криптографии (PQC) при заданном уровне стойкости.

В данной статье обсуждаются свойства 3- и 5-изогений двух классов кривых Эдвардса [2,3]. Предложено взамен 2- и 3-изогений строить алгоритм SIDH на 3- и 5-изогениях, что позволяет обойти особые точки 2-го и 4-го порядков [3,7]. В разделе 1 дается краткий обзор свойств трех классов кривых Эдвардса согласно новой классификации [7]. В разделе 2 доказывается формула для изогений нечетных степеней, выраженная рациональными функциями одной переменной. В 3-м и 4-м разделах получены оценки сложности вычисления 3- и 5-изогений в проективных координатах.

Среди многочисленных работ по этой проблематике выделим статьи [4,5,9], в которых получены формулы изогений для кривых в форме Эдвардса. Наш анализ в данной работе опирается на их результаты с использованием свойств суперсингулярных кривых [6]. С целью адаптации определений для арифметики изогений кривых Эдвардса и кривых в форме Вейерштрасса мы используем модифицированный закон сложения точек [7].

1. Классы кривых в обобщенной форме Эдвардса

Эллиптическая кривая *в обобщенной форме Эдвардса* [6,7] определяется уравнением:

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

В работе [7] мы предложили поменять местами x и y координаты в форме кривой Эдвардса. Тогда модифицированный универсальный закон сложения точек кривой (1) имеет вид:

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

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

Из уравнения (1) определим квадраты:

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

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

$$D_{1,2}=\left(\pm\sqrt{\frac{a}{d}},\infty\right),\qquad \pm F_{11}=\left(\infty,\pm\frac{1}{\sqrt{d}}\right). \tag{3}$$

Они возникают в случаях $\chi(ad)=1$ и $\chi(d)=1$ соответственно. Это, например, всегда выполняется в расширении поля F_{p^2}.

В зависимости от свойств параметров a и d кривые в обобщенной форме Эдвардса (1) разбиваются на 3 непересекающиеся (неизоморфных) класса [7]:

- *полные кривые Эдвардса* с условием С1: $\chi(ad)=-1$;
- *скрученные кривые Эдвардса* с условиями С2.1: $\chi(a)=\chi(d)=-1$;
- *квадратичные кривые Эдвардса* с условиями С2.2: $\chi(a)=\chi(d)=1$.

Основные свойства этих классов кривых [7]:

1. В отношении точек 2-го порядка класс полных кривых Эдвардса над простым полем является классом *циклических* кривых (с одной точкой 2-го порядка), скрученные же и квадратичные кривые Эдвардса образуют классы *нециклических* кривых (по 3 точки 2-го порядка).

2. Класс полных кривых Эдвардса не содержит особых точек.

3. Скрученные кривые Эдвардса содержат лишь две особых точки 2-го порядка $D_{1,2}=\left(\pm\sqrt{\frac{a}{d}},\infty\right)$, а квадратичные кривые Эдвардса, кроме них – еще две особые точки 4-го порядка $\pm F_{11}=\left(\infty,\pm\frac{1}{\sqrt{d}}\right)$.

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

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

Подчеркнем, что в расширении F_{p^2} простого поля F_p все 3 класса кривых Эдвардса, заданных над простым полем, приобретают свойства квадратичных кривых. Поэтому далее мы рассматриваем кривые E_d с параметром $a=1$.

2. Изогении нечетных степеней 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 существует функция [8]:

$$\phi(x,y)=\left(\frac{p(x)}{q(x)},y\frac{f(x)}{g(x)}\right)=(x',y'), \tag{4}$$

отображающаяие точки кривой E в точки кривой E'. Степенью изогении называется максимальная из степеней $l=\deg\phi(x,y)=\max\{\deg p(x),\deg q(x)\}$, а ее ядром $\ker\phi=G$ – подгруппа $G\subseteq E$, точки которой отображаются функцией $\phi(x,y)$ в нейтральный элемент О группы E'. Степень сепарабельной изогении равна порядку l ее ядра. Изогения сжимает точки кривой E в l раз (l точек кривой E отображаются в одну точку кривой E'). При $G=O$ изогения становится изоморфизмом со степенью 1.

В основе построения изогений нечетных простых степеней для кривых Эдвардса лежит теорема 2 [4]. Сформулируем ее с учетом модификации (2) закона сложения точек кривой (1) при $a=1$.

Теорема 2 [4]. Пусть $G=\{(1,0),\pm Q_1,\pm Q_2,...,\pm Q_s\}$ – подгруппа нечетного порядка $l=2s+1$ точек $\pm Q_i=(\alpha_i,\pm\beta_i)$ кривой E_d.

Определим $\phi(P)=\left(\prod_{Q\in G}\frac{x_{P+Q}}{x_Q},\prod_{Q\in G}\frac{y_{P+Q}}{x_Q}\right)$.

Тогда $\phi(x,y)$ есть l-изогения с ядром G из кривой E_d в кривую $E_{d'}$ с параметром $d'=A^8d^l$, $A=\prod_{i=1}^{s}\alpha_i$, и отображающей функцией:

$$\phi(x,y)=\left(\frac{x}{A^2}\prod_{i=1}^{s}\frac{(\alpha_i x)^2-(\beta_i y)^2}{1-(d\alpha_i\beta_i xy)^2},\frac{y}{A^2}\prod_{i=1}^{s}\frac{(\alpha_i y)^2-(\beta_i x)^2}{1-(d\alpha_i\beta_i xy)^2}\right). \quad (5)$$

Доказательство ее дано в [4]. Важным ее следствием является то, что изогенные кривые лежат в тех же классах, что и кривые E_d (т.е. полные кривые Эдвардса отображаются в полные, а квадратичные кривые – в квадратичные). Это существенно отличает изогении нечетных степеней от 2-изогений (для них полные кривые Эдвардса отображаются в квадратичные).

Формула (5) для функции $\phi(x,y)$ прямо следует из определения $\phi(P)$ в формулировке теоремы, закона (2) сложения точек $(x_P,y_P)=(x,y)$ с точками $\pm Q_i=(\alpha_i,\pm\beta_i)$, при этом для пар координат имеем $\frac{x_{P+Q_i}}{x_{Q_i}}\frac{x_{P-Q_i}}{x_{-Q_i}}=\frac{1}{\alpha_i^2}\frac{(\alpha_i x)^2-(\beta_i y)^2}{1-(d\alpha_i\beta_i xy)^2}$, $\frac{y_{P+Q_i}}{x_{Q_i}}\frac{y_{P-Q_i}}{x_{-Q_i}}=\frac{1}{\alpha_i^2}\frac{(\beta_i x)^2-(\alpha_i y)^2}{1-(d\alpha_i\beta_i xy)^2}$.

Сомножители x и y перед произведениями в координатах функции $\phi(x,y)$ учитывают нейтральный элемент $O=(1_i,0)$ ядра изогении. Из (5) очевидно выполнение свойства $\phi(1,0)=(1,0)$, т.е. нейтральный элемент отображается в себя. Для всех точек ядра также справедливо $\phi(\pm Q_i=(\alpha_i,\pm\beta_i))=(1,0)$.

Отображение (5) можно привести к виду (4), тогда определение степени изогении становится очевидным. Из (1) выразим $y^2=(1-x^2)/(1-dx^2)$, и подставим это значение в (5). Тогда в числителе первой координаты (5):

$$\alpha_i^2x^2-\beta_i^2y^2=\alpha_i^2x^2-\beta_i^2\frac{1-x^2}{1-dx^2}=\frac{(\alpha_i^2+\beta_i^2)x^2-\beta_i^2-d\alpha_i^2x^4}{1-dx^2}=\frac{(1+d\alpha_i^2\beta_i^2)x^2-\beta_i^2-d\alpha_i^2x^4}{1-dx^2}=$$
$$=\frac{x^2-\beta_i^2-d(\alpha_i^2x^4-\alpha_i^2\beta_i^2x^2)}{1-dx^2}=\frac{(x^2-\beta_i^2)(1-d\alpha_i^2x^2)}{1-dx^2}.$$

Аналогично преобразуем знаменатель первой координаты (5):

$$1-(d\alpha_i\beta_i xy)^2=1-d^2\alpha_i^2\beta_i^2x^2\frac{1-x^2}{1-dx^2}=\frac{1-dx^2-d^2\alpha_i^2\beta_i^2x^2+d^2\alpha_i^2\beta_i^2x^4}{1-dx^2}=\frac{1-d(\alpha_i^2+\beta_i^2)x^2+d^2\alpha_i^2\beta_i^2x^4}{1-dx^2}=$$
$$=\frac{(1-d\alpha_i^2x^2)(1-d\beta_i^2x^2)}{1-dx^2}.$$

После сокращения общих сомножителей получаем $\frac{(\alpha_i x)^2-(\beta_i y)^2}{1-(d\alpha_i\beta_i xy)^2}=\frac{x^2-\beta_i^2}{1-d\beta_i^2x^2}$.

Аналогичные выкладки можно провести со второй координатой (5). В итоге функцию (5) можно записать в эквивалентной форме:

$$\phi(x,y)=\left(\frac{x}{A^2}\prod_{i=1}^{s}\frac{x^2-\beta_i^2}{1-d\beta_i^2x^2},\frac{-y}{A^2}\prod_{i=1}^{s}\frac{x^2-\alpha_i^2}{1-d\alpha_i^2x^2}\right), \quad (6)$$

отвечающей классическому виду (4). Эта форма приведена в работе [4] без доказательства. Очевидным ее преимуществом перед (5) является простота и минимальная вычислительная сложность. Кроме этого, степень изогении как максимальная степень полинома $p(x)$ в (4) сразу определяется как $l=2s+1$.

Важно отметить, что строить изогении составного порядка (к примеру, 15-го) практически бессмысленно. Достаточно построить более простые 3-изогению и 5-изогению и пользоваться свойством их композиции, основанном на гомоморфизме отображения ϕ. Так как подгруппа точек 15-го порядка есть прямая сумма подгрупп простых 3-го и 5-го порядков, т.е. $G_{15}=G_3\oplus G_5$, то и для соответствующих изогений справедливо $\phi_{15}=\phi_3\oplus\phi_5$. Это свойство кардинально снижает сложность вычисления изогений составных степеней.

Для построения изогений степеней l^k, $l=3,5,..,k=2,3,..,m$, используется очевидное свойство группы: любая циклическая группа точек $<G_k>$ порядка l^k содержит подгруппу точек $<G_{k-1}>$ порядка l^{k-1}и подгруппу $<G_1>$ порядка l. Точка порядка l из $<G_k>$ находится скалярным произведением $l^{k-1}G_k$. Тогда, начиная со старшей степени m, можно построить последовательность l-изогений $\{\phi_{m-i}\}$, композиция которых $\phi_{m-t}=\phi_{m-1}\oplus\phi_{m-2}\oplus..\oplus\phi_{m-t+1}$ дает l^k-изогению при $t=m-k$. Такой алгоритм, выполняемый максимум за m шагов, имеет полиномиальную сложность.

Безопасность алгоритма SIDH [1] требует, чтобы число подгрупп кривой E_d порядка $p+1=4\cdot3^m\cdot5^n$ для защиты от квантового компьютера составляло величину более760 бит. Для эффективного решения этой задачи кривые E_d и $E_{d'}'$ рассматриваются над расширением F_{p^2} поля F_p (причем кривая E_d задается над простым полем). Порядок суперсингулярной кривой над расширением F_{p^2} равен $(p+1)^2$, в соответствующей пропорции возрастает число подгрупп кривой (порядка 1,5КБит).. Каждая циклическая подгруппа порядка n суперсингулярной кривой над F_p трансформируется над расширением F_{p^2} в нециклическую подгруппу порядка n^2, содержащую $(n+1)$ циклических подгрупп порядка n. Соответственно, число ядер для 3-изогений равно 4, а для 5-изогений – 6. Нахождение генератора одной из таких подгрупп (или ядра изогении) является одной из сложных задач PQC.

3. Вычисление 3-изогений в проективных координатах

Перспективным решением задачи повышения эффективности вычислений изогений является переход к однокоординатной изогении $(X':Z')$ [1, 9], тогда как вторая координата

точки с точностью до знака при необходимости определяется уравнением изогенной кривой. В этом случае лучшие результаты можно получить с использованием изогении формы (6). Для первой координаты 3-изогении после замены $\beta^2 = (1-\alpha^2)/(1-d\alpha^2)$ имеем:

$$\frac{X'}{Z'} = \frac{x}{\alpha^2}\cdot\frac{x^2-\beta^2}{1-d\beta^2x^2} = \frac{x}{\alpha^2}\cdot\frac{x^2-\frac{1-\alpha^2}{1-d\alpha^2}}{1-dx^2\cdot\frac{1-\alpha^2}{1-d\alpha^2}} = \frac{-x}{\alpha^2}\cdot\frac{x^2+\alpha^2-d\alpha^2x^2-1}{d(x^2+\alpha^2)-d\alpha^2x^2-1}$$

Для точек ядра $\pm Q = (\alpha, \pm\beta)$ 3-го порядка из равенства $2Q = -Q$ и формулы (2) легко получить уравнение для полинома деления $2\alpha+1-d\alpha^3(2+\alpha)=0$, откуда $d = (2\alpha+1)/\alpha^3(2+\alpha)$ [9]. Подставляя это значение в последнее равенство, приходим к рациональной функции $\frac{X'}{Z'} = x\cdot\frac{x^2+\alpha^2+2\alpha}{x^2+\alpha^2+2\alpha x^2}$.

Важно, что здесь 3-изогения определена лишь *x*-координатами точек *P* и *Q* и не зависит от параметра d. В проективных координатах после замены $x \to \frac{X}{Z}$, $\alpha = \frac{X_1}{Z_1}$ получим:

$$(X' : Z') = (X(X^2Z_1^2 + X_1^2Z^2 + 2X_1Z_1Z^2) : Z(X^2Z_1^2 + X_1^2Z^2 + 2X_1Z_1X^2)) \qquad (7)$$

Подобное выражение найдено в работе [9], в которой вместо изогении, определяемой теоремой 2, за основу взята теорема 3[4]. Эти теоремы дают разные определения для параметра d' изогенной кривой $E_{d'}$.Согласно теореме 2[4]:

$$d' = A^8d^3, A = \alpha. \qquad (8)$$

Определяя здесь параметр $d = (2\alpha+1)/\alpha^3(2+\alpha)$, в проективных координатах равенство (8) принимает вид:

$$d' = \frac{Z_1}{X_1}\cdot\frac{(2X_1+Z_1)^3}{(2Z_1+X_1)^3} \qquad (9)$$

$$E_{C',D'}: \quad C'(x^2+y^2) = C' + D'x^2y^2, D' = d'C'.$$

Тогда согласно (9):

$$D' = Z_1(2X_1+Z_1)^3 = (2X_1Z_1+Z_1^2)(4X_1^2+Z_1^2+4X_1Z_1), \qquad (10)$$

$$C' = X_1(2Z_1+X_1)^3 = (2X_1Z_1+X_1^2)(4Z_1^2+X_1^2+4X_1Z_1). \qquad (11)$$

Чтобы избежать инверсии при вычислении параметра d', в работе [9] предложено использовать проективные координаты изоморфной (1) кривой.

Так как $2X_1Z_1 = (X_1+Z_1)^2 - X_1^2 - Z_1^2$, вычисления по формулам (10), (11) имеют сложность $2M+3S$.

Вычисление координаты (10) точки изогенной кривой $E_{d'}{}'$ можно выполнить с помощью формул [9]:

$$F=(X'+Z')=(X_1Z+Z_1X)^2(X+Z),\qquad G=(X'-Z')=(X_1Z-Z_1X)^2(X-Z) \tag{12}$$

Тогда $2X'=F+G$, $2Z'=F-G$. Вычисления по формулам (12), имеют стоимость $4M+2S$. Суммарная стоимость вычисления 3-изогении равна $6M+5S$.

4. Вычисление 5-изогений в проективных координатах

Для первой координаты 5-изогении (6) после замены $\beta_{1,2}{}^2=(1-\alpha_{1,2}{}^2)/(1-d\alpha_{1,2}{}^2)$ получим: $\dfrac{X'}{Z'}=\dfrac{x}{(\alpha_1\alpha_2)^2}\cdot\dfrac{x^2+\alpha_1{}^2-d\alpha_1{}^2x^2-1}{d(x^2+\alpha_1{}^2)-d\alpha_1{}^2x^2-1}\cdot\dfrac{x^2+\alpha_2{}^2-d\alpha_2{}^2x^2-1}{d(x^2+\alpha_2{}^2)-d\alpha_2{}^2x^2-1}$.

Для этого случая полином деления для точек 5-го порядка имеет степень 12. Использование полинома деления здесь не дает такого эффекта, как для 3-изогений.

В проективных координатах после замены $x\to\dfrac{X}{Z}$, $\alpha_{1,2}\to\dfrac{X_{1,2}}{Z_{1,2}}$ имеем

$$\frac{X'}{Z'}=\frac{X(\mathrm{Z}_1\mathrm{Z}_2)^2}{Z(X_1X_2)^2}\cdot\frac{(XZ_1)^2+(X_1\,\mathrm{Z})^2-d(X_1X)^2-(\mathrm{Z}_1\mathrm{Z})^2}{d((XZ_1)^2+(X_1\,\mathrm{Z})^2)-d(X_1X)^2-(\mathrm{Z}_1\mathrm{Z})^2}\cdot\frac{(XZ_2)^2+(X_2\,\mathrm{Z})^2-d(X_2X)^2-(\mathrm{Z}_2\mathrm{Z})^2}{d((XZ_2)^2+(X_2\,\mathrm{Z})^2)-d(X_2X)^2-(\mathrm{Z}_2\mathrm{Z})^2}$$

Соответственно:

$$X'=XZ_1{}^2Z_2{}^2[X^2(Z_1{}^2-dX_1{}^2)+\mathrm{Z}^2(X_1{}^2-\mathrm{Z}_1{}^2)][X^2(Z_2{}^2-dX_2{}^2)+\mathrm{Z}^2(X_2{}^2-\mathrm{Z}_2{}^2)] \tag{13}$$

$$Z'=ZX_1{}^2X_2{}^2[dX^2(Z_1{}^2-X_1{}^2)+\mathrm{Z}^2(dX_1{}^2-\mathrm{Z}_1{}^2)][dX^2(Z_2{}^2-X_2{}^2)+\mathrm{Z}^2(dX_2{}^2-\mathrm{Z}_2{}^2)] \tag{14}$$

Вычисления по формулам (13), (14) требуют $19M+6S$ операций. Параметр d' изогенной кривой определяется квк $d'=A^8d^5, A=\alpha_1\alpha_2$. Параметры изоморфной кривой $E_{C',D'}$ при этом равны:

$$D'=(X_1^2X_2^2)^4\cdot(d^2)^2\cdot d,\qquad C'=(Z_1{}^2Z_2{}^2)^4 \tag{15}$$

Вычисления по формулам (15)) имеют стоимость $2M+6S$ Таким образом, общая стоимость вычисления 5-изогении составляет $21M+12S$.

Вывод

Итак, использование 3- и 5-изогений кривых Эдвардса для точек нечетного порядка при фиксированной стойкости к атакам квантового компьютера позволит обойти проблемы особых точек, свойственных 2-изогениям этих кривых. Оценки сложности вычисления 3- и 5-изогений кривых Эдвардса, соизмеримые со сложностью групповых операций, полезны для реализации наиболее быстрых алгоритмов постквантовой криптографии.

Литература

1 .D.Jao, and L. de Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, Post-Quantum Cryptography pp. 19-34 (2011).

2. Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advances in Cryptology—ASIACRYPT’2007 Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. P. 29–50.

3. 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.

4. Moody D., Shumow D. Analogues of Velus formulas for isogenies on alternate models of elliptic curves. Mathematics of Computation, vol. 85, no. 300, pp. 1929–1951, 2016.

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

6.Бессалов А.В., Ковальчук Л.В. Суперсингулярные скрученные кривые Эдвардса над простым полем. Кибернетика и системный анализ, №5, 2019.– С.35-46.

7. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Монография. «Политехника», Киев, 2017. - 272с. ISBN 978-966-622-808-9.

8. WashingtonL,C.. Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.

9. Suhri Kim, Kisoon Yoon, Jihoon Kwon, Seokhie Hong , and Young-Ho Park Efficient Isogeny Computations on Twisted Edwards Curves Hindawi Security and Communication Networks Volume 2018, Article ID 5747642, 11 pages https://doi.org/10.1155/2018/5747642.

Надійшла: 29.10.2019 Рецензент: д.т.н., професор Барабаш О.В.