УДК 621.391.15:519.7 **DOI:10.30837/rt.2020.1.200.04**

А.В. БЕССАЛОВ

АЛГОРИТМЫ И ОЦЕНКИ СЛОЖНОСТИ ВЫЧИСЛЕНИЙ 3- И 5-ИЗОГЕНИЙ СУПЕРСИНГУЛЯРНЫХ КРИВЫХ ЭДВАРДСА

Введение

Одной из известных перспектив постквантовой криптографии (PQC) являются алгоритмы, построенные на изогениях суперсингулярных эллиптических кривых (*supersingular isogenies Diffi-Hellman* – SIDH[1]). Сегодня интерес к изогениям связывается с наименьшей длиной ключа в предлагаемых алгоритмах в сравнении с другими известными кандидатами PQC.

Кривые Эдвардса с одним параметром, определенные в работе [2], имеют привлекательные для криптографии преимущества: максимальная скорость экспоненцирования точки, универсальность закона сложения точек, аффинные координаты нейтрального элемента группы точек, повышенная безопасность в отношении атак побочного канала. Введение второго параметра кривой в работе [3] расширило класс *s* кривых Эдвардса и породило кривые с новыми интересными для криптографии свойствами.

Наряду с отмеченными свойствами кривые в форме Эдвардса оказались наиболее быстрой технологией при вычислении изогений. В работе [4] приводятся экспериментальные оценки скорости вычисления изогений на кривых Эдвардса, более чем втрое превышающие показатели для кривых в форме Вейерштрасса. Так как процедура нахождения изогенной точки обычно включает скалярное произведение точки, общий выигрыш в быстродействии алгоритмов на кривых Эдвардса может стать значительным.

Известные реализации алгоритма SIDH используют в основном кривые в форме Вейерштрасса и Монтгомери. Попытка программной реализации алгоритма SIDH с помощью 2- и 3-изогений кривых в форме Эдвардса столкнулась с проблемой наличия четырех особых точек на бесконечности 2-го и 4-го порядков в классе квадратичных кривых Эдвардса. Эти точки имеются во всех подгруппах четных порядков, число которых близко половине всех подгрупп кривой. Чтобы обойти эту проблему, предлагается использовать изогении минимальных нечетных степеней 3 и 5 для точек нечетного порядка кривой. Хотя переход от 2- к 5-изогении усложняет алгоритм вычислений, подобная гладкая реализация алгоритма представляется перспективной.

Среди многочисленных работ по этой проблематике выделим статьи [4 – 6], в которых впервые получены формулы изогений для кривых в форме Эдвардса. Наш анализ опирается на их результаты с использованием свойств суперсингулярных кривых [7, 8]. С целью адаптации определений для арифметики изогений кривых Эдвардса и кривых в форме Вейерштрасса мы используем модифицированный закон сложения точек [9, 10].

В данной статье построены алгоритмы и получены оценки сложности вычислений 3- и 5-изогений двух классов кривых Эдвардса. В разд. 1 дается краткий обзор свойств трех классов кривых Эдвардса согласно новой классификации. В разд. 2 даны определения и доказывается формула для изогений нечетных степеней, выраженная рациональными функциями одной переменной. В разд. 3, 4 построены алгоритмы и получены оценки сложности вычисления 3- и 5-изогений в проективных координатах. В разд. 5 приводятся алгоритмы вычисления 3- и 5-изогений. Наконец, в разд. 6 определены условия существования 3- и 5-изогений и требования к параметрам кривой для алгоритма SIDH [1].

1. Классы кривых в обобщенной форме Эдвардса

Эллиптическая кривая *в обобщенной форме Эдвардса* [9] определяется уравнением

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

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

$$E_d: \quad x^2 + y^2 = 1 + dx^2y^2,\ \chi(d) = -1,\ d \neq 0,1, \tag{2}$$

В случае $\chi(ad) = 1$, и $\chi(a) = \chi(d) = 1$ имеет место изоморфизм кривой (1) с *квадратичной кривой Эдвардса* [9]:

$$E_d: \quad x^2 + y^2 = 1 + dx^2y^2,\ \chi(d) = 1,\ d \neq 0,1, \tag{3}$$

имеющей, в отличие от (2), параметр d, определенный как квадрат. Это отличие ведет к кардинально различным свойствам кривых (2) и (3) [9], которые резюмируются ниже. Несмотря на это, в статье [3] эти классы кривых объединены общим термином *кривые Эдвардса.*

Кривые с различными значениями a, d изоморфны, если они имеют одинаковый j-инвариант, равный для кривой (1)

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

Этот параметр является базовым в структуре графа изогенных кривых, вершины которого задают классы изоморфных кривых.

В работе [9] мы предложили поменять местами x и y координаты в форме кривой Эдвардса. Тогда модифицированный универсальный закон сложения точек кривой (1) имеет вид

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{(1 - dx_1x_2y_1y_2)}, \frac{x_1y_2 + x_2y_1}{(1 + dx_1x_2y_1y_2)} \right). \tag{4}$$

При совпадении двух точек получим из (4) закон удвоения точек

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{(1 - dx_1^2y_1^2)}, \frac{2x_1y_1}{(1 + dx_1^2y_1^2)} \right). \tag{5}$$

Использование модифицированных законов (4), (5) позволяет сохранить общепринятую горизонтальную симметрию (относительно оси X) обратных точек. Определяя обратную точку как $-P = (x_1, -y_1)$, получим согласно (4) координаты нейтрального элемента группы точек $O = (x_1, y_1) + (x_1, -y_1) = (1, 0)$. Кроме нейтрального элемента О на оси X всегда лежит точка $D_0 = (-1, 0)$ второго порядка, для которой в соответствии с (5) $2D_0 = (1, 0) = O$. В зависимости от свойств параметров a и d можно получить еще две особые точки 2-го порядка и две или более точек 4-го порядка. Как следует из (1), 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 (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):

$$D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right), \pm F_{11} = \left(\infty, \pm\frac{1}{\sqrt{d}}\right). \tag{6}$$

Они возникают в случаях $\chi(ad) = 1$ и $\chi(d) = 1$ соответственно. Это, например, всегда выполняется в расширении поля.

В зависимости от свойств параметров a и d кривые в обобщенной форме (1) разбиваются на три непересекающиеся (неизоморфных) класса [9, 10]:

- *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 [9]:

1. В отношении точек 2-го порядка первый 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 три точки 2-го порядка). 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 $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$, 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. В классах скрученных и квадратичных кривых Эдвардса замена $a \leftrightarrow d$ дает изоморфизм $E_{a,d} \sim E_{d,a}$.

6. 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.

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

Подчеркнем, что в расширении F_{p^2} простого поля F_p все три класса кривых Эдвардса, заданные над простым полем, приобретают свойства квадратичных кривых (3). Поэтому далее мы рассматриваем в основном кривые E_d вида (2) и (3) с одним параметром.

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 рациональная функция [11]

$$\phi(x, y) = \left(\frac{p(x)}{q(x)}, y\frac{f(x)}{g(x)}\right) = (x', y'), \tag{7}$$

отображающая 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 O 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 (4) 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 $d' = A^8 d^l$, $A = \prod_{i=1}^{s} \alpha_i$, и отображающей функцией

$$\phi(x,y) = \left(\frac{x}{A^2} \prod_{i=1}^{s} \frac{(\alpha_i x)^2 - (\beta_i y)^2}{1 - (d\alpha_i\beta_i xy)^2}, \frac{y}{A^2} \prod_{i=1}^{s} \frac{(\alpha_i y)^2 - (\beta_i x)^2}{1 - (d\alpha_i\beta_i xy)^2} \right). \quad (8)$$

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 (8) для функции $\phi(x,y)$ прямо следует из определения $\phi(P)$ в формулировке теоремы, закона (4) сложения точек $(x_P, y_P) = (x,y)$ с точками $\pm Q_i = (\alpha_i, \pm\beta_i)$, при этом для пар координат имеем:

$$\frac{x_{P+Q_i}}{x_{Q_i}} \frac{x_{P-Q_i}}{x_{-Q_i}} = \frac{1}{\alpha_i^2} \frac{(\alpha_i x)^2 - (\beta_i y)^2}{1 - (d\alpha_i\beta_i xy)^2}, \qquad \frac{y_{P+Q_i}}{x_{Q_i}} \frac{y_{P-Q_i}}{x_{-Q_i}} = \frac{1}{\alpha_i^2} \frac{(\beta_i x)^2 - (\alpha_i y)^2}{1 - (d\alpha_i\beta_i xy)^2}.$$

Сомножители x и y перед произведениями в координатах функции $\phi(x,y)$ учитывают нейтральный элемент $O = (1_i, 0)$ ядра изогении. Из (8) 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 (8) можно привести к виду (7), тогда определение степени изогении становится очевидным. Из (2) и (3) выразим $y^2 = (1-x^2)/(1-dx^2)$ и подставим это значение в (8). Тогда в числителе первой координаты (8)

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

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

Аналогично преобразуем знаменатель первой координаты (8)

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

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

После сокращения общих сомножителей получаем

$$\frac{(\alpha_i x)^2-(\beta_i y)^2}{1-(d\alpha_i\beta_i xy)^2} = \frac{x^2-\beta_i^{\,2}}{1-d\beta_i^{\,2}x^2}.$$

Аналогичные выкладки можно провести со второй координатой (8). В итоге функцию (8) можно записать в эквивалентной форме

$$\phi(x,y) = \left(\frac{x}{A^2}\prod_{i=1}^{s}\frac{x^2-\beta_i^{\,2}}{1-d\beta_i^{\,2}x^2}, \frac{-y}{A^2}\prod_{i=1}^{s}\frac{x^2-\alpha_i^{\,2}}{1-d\alpha_i^{\,2}x^2}\right), \tag{9}$$

отвечающей классическому виду (7). Эта форма приведена в работе [4] без доказательства. Очевидным ее преимуществом перед (8) является простота и минимальная вычислительная сложность. Кроме этого, степень изогении как максимальная степень полинома $p(x)$ в (7) сразу определяется как $l = 2s+1.$

Рассмотрим пример 3-изогении полной суперсингулярной кривой Эдвардса.

Пример 1. Пусть E_d – полная суперсингулярная кривая Эдвардса (2) при $p = 23, d = -1.$ с j-инвариантом $j = 12^3$ [6]. Она имеет порядок $N_E = 24$ и содержит точки $(\pm1,0), (0,\pm1), (\pm2,\pm2), (\pm3,\pm6), (\pm6,\pm3), (\pm9,\pm10), (\pm10,\pm9)$. Обозначим $P_1 = (3,6)$, $P_2 = (6,3)$ – точки 24-го порядка кривой. $P_3 = (2,2)$ – точка 8-го порядка, $P_4 = (9,10)$ – точка 12-го порядка, $P_3 = (10,9)$ – точка 6-го порядка и $Q = (-10,9)$ – точка 3-го порядка, и для любой точки $P = (x_1, y_1)$ $P^* = P + D_0 = (-x_1, -y_1)$. Заметим, что сумма точек 2-го и 3-го порядка дает точку 6-го порядка, поэтому x-координаты точек 3-го и 6-го порядков имеют обратные знаки. Итак, ядро 3-изогении содержит точки $(1,0)$, $(-10,\pm9)$, т.е. $\alpha = -10$, $\beta = 9$, $A^2 = 8,$ и согласно теореме 2 [4] параметр изогенной кривой $E_{d'}$ равен, $d' = -8^4 = -2$. Эта суперсингулярная кривая с j-инвариантом $j = 3$, кроме точек $O = (1,0)$ $D_0 = (-1,0)$, $\pm F_0 = (0, \pm1)$, имеет точки первого квадранта: $R_1 = (3,5)$ $R_2 = (5,3)$ – точки 24-го порядка кривой. $R_3 = (7,7)$ – точка 8-го порядка, $R_4 = (9,11)$ – точка 6-го порядка и $R_5 = (11,9)$ – точка 12-го порядка и $Q' = (-9,11)$ – точка 3-го порядка. С помощью функции (9)

$$\phi(x,y) = \left(\frac{x}{8}\cdot\frac{x^2-9^2}{1+9^2x^2}, \frac{-y}{8}\frac{x^2-10^2}{1+10^2x^2}\right)$$

получим:

$$\phi(\pm P_1 = (3,\pm6)) = \left(\frac{3}{8}\cdot\frac{3^2-9^2}{1+9^2\cdot3^2}, \frac{\mp6}{8}\frac{3^2-10^2}{1+10^2\cdot3^2}\right) = (-7,\pm7) = \mp R_3^*, \qquad \phi(P_2 = (6,3)) = (7,-7) = -R_3,$$

$$\phi(P_3 = (2,2)) = (7,7) = R_3,$$

$$\phi(P_4 = (9,\pm10)) = (0,\mp1) = \mp F_0,$$

$\phi(P_5 = (10,9)) = (-1,0) = D_0,$

$\phi(\pm Q = (-10,\pm 9)) = (1,0) = O, \phi(O = (1,0)) = (1,0) = O.$

Для преобразования других точек можно использовать свойство функции (9) $\phi(\pm x, \pm y) = (\pm x', \pm y')$ Здесь имеет место отображение «3 в 1» со сжатием E_d в три раза (24 точки кривой E_d отображаются в восемь точек изогенной кривой $E_{d'}{}'$). В частности, восемь точек 24-го порядка вместе с четырьмя точками 8-го порядка отображаются в четыре точки 8-го порядка, четыре точки 12-го порядка вместе с двумя точками 6-го порядка отображаются в две точки 4-го порядка, точки 4-го порядка и 2-го порядков отображаются в точку 2-го порядка, и, наконец, точки ядра отображаются в О. Все преобразования отвечают умножению точек на 3, подобно эндоморфизму $E \to 3E$.

Рассмотрим пример 5-изогении на полной суперсингулярной кривой Эдвардса.

Пример 2. При $p = 19$ и $d = -1$ полная суперсингулярная кривая Эдвардса E_{18} (2) имеет порядок $N_E = 20$ и содержит точки 1-го квадранта: $P_1 = (2,8)$, $P_2 = (4,6)$ – точки 20-го порядка кривой, $P_3 = (8,2)$ – точка 10-го порядка, и $Q_1 = (6,4)$ – точка 5-го порядка. Тогда $Q_2 = 2Q_1 = (-8,-2)$ и ядро 5-изогении содержит точки $\{(1,0),(6,\pm 4),(-8,\pm 2)\}$. Итак, $\alpha_1 = 6, \beta_1 = 4, \alpha_2 = -8, \beta_2 = -2, A = \alpha_1\alpha_2 = 9, A^2 = 5,$ и параметр изогенной суперсингулярной кривой $d' = -5^4 = -2$. Она содержит точки 1-го квадранта: $R_1 = (4,5)$, $R_2 = (7,9)$ – точки 20-го порядка кривой $E_{d'}{}'$,. $R_3 = (5,4)$, $R_4 = (9,7)$ – точки 10-го порядка. 5-изогения (9) здесь имеет вид

$$\phi(x,y) = \left(\frac{x}{5} \cdot \frac{x^2 - 4^2}{1 + 4^2 x^2} \frac{x^2 - 2^2}{1 + 2^2 x^2}, \frac{-y}{5} \cdot \frac{x^2 - 6^2}{1 + 6^2 x^2} \cdot \frac{x^2 - 8^2}{1 + 8^2 x^2} \right).$$

Тогда

$$\phi(P_1 = (2,8)) = \left(\frac{2}{5} \cdot \frac{2^2 - 4^2}{1 + 4^2 2^2} \frac{2^2 - 2^2}{1 + 2^2 2^2}, \frac{-8}{5} \cdot \frac{2^2 - 6^2}{1 + 6^2 2^2} \cdot \frac{2^2 - 8^2}{1 + 8^2 2^2} \right) = (0,1) = F_0$$

$\phi(P_2 = (4,6)) = (0,-1) = -F_0,$

$\phi(P_3 = (8,2)) = (-1,0) = D_0,$

$\phi(\pm Q_1 = (6,\pm 4)) = (1,0) = O, \quad \phi(O = (1,1)) = (1,0) = O.$

Это отображение «5 в 1» преобразует подмножества из пяти точек кривой E_d в одну из четырех точек изогенной кривой 4-го, 2-го порядка или точку O. Здесь функция (9) действует подобно эндоморфизму $E_d \to 5E_d$, снижающему порядки точек порядков, кратных 5, в пять раз.

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 $p+1 = 4 \cdot 3^m \cdot 5^n$ для защиты от квантового компьютера составляло величину более 760 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 1,5 КБит). 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, 11], 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 (9). Для первой координаты 3-изогении после замены $\beta^2 = (1-\alpha^2)/(1-d\alpha^2)$ имеем:

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

Для точек ядра $\pm Q = (\alpha, \pm\beta)$ 3-го порядка из равенства $2Q = -Q$ и формулы (5) легко получить уравнение для полинома деления $2\alpha + 1 - d\alpha^3(2+\alpha) = 0$, откуда $d = (2\alpha+1)/\alpha^3(2+\alpha)$ [11]. 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

$$(X' : Z') = (X(X^2 Z_1^2 + X_1^2 Z^2 + 2X_1 Z_1 Z^2) : Z(X^2 Z_1^2 + X_1^2 Z^2 + 2X_1 Z_1 X^2)). \quad (10)$$

Подобное выражение найдено в работе [11], 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]

$$d' = A^8 d^3, A = \alpha. \tag{11}$$

Определяя здесь параметр $d = (2\alpha + 1)/\alpha^3(2+\alpha)$, в проективных координатах, равенство (11) принимает вид

$$d' = \frac{Z_1}{X_1} \cdot \frac{(2X_1 + Z_1)^3}{(2Z_1 + X_1)^3}. \tag{12}$$

Чтобы избежать инверсии при вычислении параметра d', в работе [11] предложено использовать проективные координаты изоморфной (2) кривой

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

Тогда, согласно (12),

$$D' = Z_1(2X_1 + Z_1)^3 = (2X_1Z_1 + Z_1^2)(4X_1^2 + Z_1^2 + 4X_1Z_1), \tag{13}$$

$$C' = X_1(2Z_1 + X_1)^3 = (2X_1Z_1 + X_1^2)(4Z_1^2 + X_1^2 + 4X_1Z_1). \tag{14}$$

Так как $2X_1Z_1 = (X_1 + Z_1)^2 - X_1^2 - Z_1^2$, вычисления по формулам (13), (14) имеют стоимость $2M + 3S$

Вычисление координаты (10) точки изогенной кривой $E_{d'}'$ можно выполнить с помощью формул [11]:

$$F = (X' + Z') = (X_1Z + Z_1X)^2(X + Z), \tag{15}$$

$$G = (X' - Z') = (X_1Z - Z_1X)^2(X - Z). \tag{16}$$

Тогда $2X' = F + G$, $2Z' = F - G$. Вычисления по формулам (15), (16) имеют стоимость $4M + 2S$. Суммарная стоимость вычисления 3-изогении в проективных координатах равна $6M + 5S$.

4. Вычисление 5-изогений в проективных координатах

Для первой координаты 5-изогении (9) после замены $\beta_{1,2}^2 = (1 - \alpha_{1,2}^2)/(1 - d\alpha_{1,2}^2)$ получим:

$$\frac{X'}{Z'} = \frac{x}{(\alpha_1\alpha_2)^2} \cdot \frac{x^2 + \alpha_1^2 - d\alpha_1^2x^2 - 1}{d(x^2 + \alpha_1^2) - d\alpha_1^2x^2 - 1} \cdot \frac{x^2 + \alpha_2^2 - d\alpha_2^2x^2 - 1}{d(x^2 + \alpha_2^2) - d\alpha_2^2x^2 - 1}. \tag{17}$$

Оценим вычислительную сложность выражения (17) в проективных координатах (алгоритм 1), тогда после замены $x \to \frac{X}{Z}$, $\alpha_{1,2} \to \frac{X_{1,2}}{Z_{1,2}}$ получим

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

Соответственно,

$$X' = XZ_1^2Z_2^2[X^2(Z_1^2 - dX_1^2) + \mathrm{Z}^2(X_1^2 - \mathrm{Z}_1^2)][X^2(Z_2^2 - dX_2^2) + \mathrm{Z}^2(X_2^2 - \mathrm{Z}_2^2)], \tag{18}$$

$$Z' = ZX_1^2X_2^2[dX^2(Z_1^2 - X_1^2) + \mathrm{Z}^2(dX_1^2 - \mathrm{Z}_1^2)][dX^2(Z_2^2 - X_2^2) + \mathrm{Z}^2(dX_2^2 - \mathrm{Z}_2^2)]. \tag{19}$$

Алгоритм 1: вычисления по формулам (18), (19). Вычисления X' согласно алгоритму 1 требуют $6S$ возведений в квадрат всех координат, $3M$ умножений X -координат на параметр

d, и $8M$ остальных умножений. Вместе с $8M$ умножений при вычислении Z' получим оценку стоимости расчета координат $(X':Z')$ 5-изогении, равную $19M+6S$.

Параметр d' изогенной кривой определяется как $d'=A^8d^5, A=\alpha_1\alpha_2$. Параметры изоморфной кривой $E_{C',D'}$ при этом

$$D'=(X_1^2X_2^2\cdot d)^4\cdot d, \tag{20}$$

$$C'=(Z_1^2Z_2^2)^4 \tag{21}$$

Вычисления по формулам (20), (21), с учетом уже известных $X_1^2X_2^2$ и $Z_1^2Z_2^2$, имеют стоимость $2M+4S$. Общая стоимость вычисления 5-изогении согласно алгоритму 1 составляет $21M+10S$.

Обратимся далее к методам, подобным методам предыдущего раздела. Использование полинома деления 24-й степени для точек 5-го порядка здесь не дает такого эффекта, как для 3-изогений. Вместе с тем, нам удалось выразить параметр d как функцию $d(\alpha_1,\alpha_2)$. Для точек Q ядра 5-го порядка справедливо $2Q=(\alpha_2,\beta_2), 4Q=-Q=(\alpha_1,-\beta_1)$. Другими словами, координата α_2 вычисляется по формуле удвоения точки Q, а координата α_1- по формуле удвоения точки $2Q$. Тогда, согласно (5) и (2),

$$\alpha_2=\frac{\alpha_1^2-\beta_1^2}{1-d\alpha_1^2\beta_1^2}=\frac{\alpha_1^2-\dfrac{\alpha_1^2-1}{d\alpha_1^2-1}}{1-d\alpha_1^2\dfrac{\alpha_1^2-1}{d\alpha_1^2-1}}=\frac{d\alpha_1^4-2\alpha_1^2+1}{-d\alpha_1^4+2d\alpha_1^2-1},\quad \alpha_1=\frac{d\alpha_2^4-2\alpha_2^2+1}{-d\alpha_2^4+2d\alpha_2^2-1}.$$

Отсюда

$$d=\frac{2\alpha_1^2-(\alpha_2+1)}{\alpha_1^2[(\alpha_2+1)\alpha_1^2-2\alpha_2]}=\frac{2\alpha_2^2-(\alpha_1+1)}{\alpha_2^2[(\alpha_1+1)\alpha_2^2-2\alpha_1]}$$

Подстановка этих выражений в (17) после ряда сокращений дает не зависящую от параметра d формулу

$$\frac{X'}{Z'}=x\cdot\frac{\{x^2(\alpha_2-1)+\alpha_1^2(\alpha_2+1)-2\alpha_2\}}{\{x^2(\alpha_2+1-2\alpha_1^2)+\alpha_1^2(1-\alpha_2)\}}\cdot\frac{\{x^2(\alpha_1-1)+\alpha_2^2(\alpha_1+1)-2\alpha_1\}}{\{x^2(\alpha_1+1-2\alpha_2^2)+\alpha_2^2(1-\alpha_1)\}} \tag{22}$$

Для числителей $F_{1,2}$ и знаменателей $G_{1,2}$ этой рациональной функции запишем:

$$F_{1,2}=x^2\alpha_{2,1}-x^2+\alpha_{1,2}^2\alpha_{2,1}+\alpha_{1,2}^2-2\alpha_{2,1}, \tag{23}$$

$$G_{1,2}=x^2\alpha_{2,1}+x^2-\alpha_{1,2}^2\alpha_{2,1}+\alpha_{1,2}^2-2x^2\alpha_{1,2}^2. \tag{24}$$

Тогда

$$U_{1,2}=F_{1,2}+G_{1,2}=2\{x^2\alpha_{2,1}+\alpha_{1,2}^2-(\alpha_{2,1}+x^2\alpha_{1,2}^2)\}=2(x^2-1)(\alpha_{2,1}-\alpha_{1,2}^2), \tag{25}$$

$$V_{1,2}=F_{1,2}-G_{1,2}=2\{\alpha_{1,2}^2\alpha_{2,1}+x^2-(\alpha_{2,1}-x^2\alpha_{1,2}^2)\}=2(\alpha_{1,2}^2-1)(\alpha_{2,1}+x^2). \tag{26}$$

В проективных координатах имеем

$$U_{1,2}=2\left(\left(\frac{X}{Z}\right)^2-1\right)\left(\left(\frac{X_{1,2}}{Z_{1,2}}\right)^2-\left(\frac{X_{2,1}}{Z_{2,1}}\right)\right)=2\left(Z_{2,1}Z_{1,2}^2Z^2\right)^{-1}\left(X^2-Z^2\right)\left(X_{1,2}^2Z_{2,1}-X_{2,1}Z_{1,2}^2\right) \tag{27}$$

$$V_{1,2}=2\left(\left(\frac{X_{1,2}}{Z_{1,2}}\right)^2-1\right)\left(\left(\frac{X}{Z}\right)^2+\left(\frac{X_{2,1}}{Z_{2,1}}\right)\right)=2\left(Z_{2,1}{Z_{1,2}}^2Z^2\right)^{-1}\left({X_{1,2}}^2-{Z_{1,2}}^2\right)\left(X^2Z_{2,1}+X_{2,1}Z^2\right). \quad (28)$$

Альтернативные формулы без учета общих сомножителей имеют вид

$$U'_{1,2}=\left(X^2-Z^2\right)\left[-\left(X_{2,1}+Z_{2,1}\right)\left({X_{1,2}}^2-{Z_{1,2}}^2\right)+\left(X_{2,1}-Z_{2,1}\right)\left({Z_{1,2}}^2+{X_{1,2}}^2\right)\right], \quad (29)$$

$$V'_{1,2}=\left({X_{1,2}}^2-{Z_{1,2}}^2\right)\left[\left(X_{2,1}+Z_{2,1}\right)\left(X^2+Z^2\right)-\left(X_{2,1}-Z_{2,1}\right)\left(X^2-Z^2\right)\right]. \quad (30)$$

С учетом $2F_{1,2}=U_{1,2}+V_{1,2}$ и $2G_{1,2}=U_{1,2}-V_{1,2}$ (формулы (27),(28)) можно получить

$$2F_{1,2}=\left[Z^2\left(X_{2,1}+Z_{2,1}\right)\left({X_{1,2}}^2-{Z_{1,2}}^2\right)+Z_{1,2}^2\left(X_{2,1}-Z_{2,1}\right)\left(X^2-Z^2\right)\right] \quad (31)$$

$$2G_{1,2}=\left[-X^2\left(X_{2,1}+Z_{2,1}\right)\left({X_{1,2}}^2-{Z_{1,2}}^2\right)+X_{1,2}^2\left(X_{2,1}-Z_{2,1}\right)\left(X^2-Z^2\right)\right] \quad (32)$$

Итак, функцию (22) на основе (25), (26) можно записать как

$$\frac{X'}{Z'}=\frac{X}{Z}\cdot\frac{F_1}{G_1}\cdot\frac{F_2}{G_2}=\frac{X}{Z}\cdot\frac{U_1+V_1}{U_1-V_1}\cdot\frac{U_2+V_2}{U_2-V_2}. \quad (33)$$

Алгоритм 2: вычисления по формулам (27), (28). После сокращения общих сомножителей функция (22) имеет вид

$$\frac{X'}{Z'}=\frac{X}{Z}\cdot\frac{\left(X^2-Z^2\right)\left(X_1^2Z_2-X_2Z_1^2\right)+\left({X_1}^2-Z_1^2\right)\left(X^2Z_2+X_2Z^2\right)}{\left(X^2-Z^2\right)\left(X_1^2Z_2-X_2Z_1^2\right)-\left({X_1}^2-Z_1^2\right)\left(X^2Z_2+X_2Z^2\right)}\cdot\frac{\left(X^2-Z^2\right)\left(X_2^2Z_1-X_1Z_2^2\right)+\left({X_2}^2-Z_2^2\right)\left(X^2Z_1+X_1Z^2\right)}{\left(X^2-Z^2\right)\left(X_2^2Z_1-X_1Z_2^2\right)-\left({X_2}^2-Z_2^2\right)\left(X^2Z_1+X_1Z^2\right)}$$

Вычислительная стоимость числителя X' здесь составляет, $14M+6S$, а знаменателя Z' – $2M$, в итоге затраты вычисления координат изогенной точки равны $16M+6S.$

Алгоритм 3: вычисления по формулам (29), (30). В числителе (33) выполняется 10 умножений M, а в знаменателе – $6M$, в итоге вновь вычислительные затраты оцениваются величиной $16M+6S.$

Алгоритм 4: вычисления по формулам (31), (32). На основе формул (31) и (32) для пар $2F_{1,2}, 2G_{1,2}$ и (33) рассчитываются по два общих сомножителя ($4M$), к этому добавляется по $6M$ умножений в числителе и знаменателе (33). Общая стоимость вычислений остается неизменной и равна $16M+6S.$ Этот алгоритм приводится в следующем разделе.

Иначе говоря, все три возможных алгоритма вычисления координат $(X':Z')$ изогенной точки согласно (22) имеют равноценную сложность.

Параметр d' изогенной кривой определяется как $d'=A^8d^5, A=\alpha_1\alpha_2.$ Параметры изоморфной кривой $E_{C',D'}$ при этом:

$$D'=(X_1^2\cdot X_2^2\cdot d)^4\cdot d, \quad (34)$$

$$C'=(Z_1^2\cdot Z_2^2)^4 \quad (35)$$

Вычисления по формулам (34), (35) имеют стоимость $4M+4S$. В сравнении с алгоритмом 1 здесь добавляются два умножения $X_1^2\cdot X_2^2$ и $Z_1^2\cdot Z_2^2$. Общая стоимость вычисления 5-изогении согласно алгоритмам 2 – 4 составляет $20M+10S$.

Известная средняя оценка соотношения стоимостей M и S определяется как $M \cong \frac{2}{3}S$ [2]. При этом оценка стоимости вычисления 3-изогении составляет $6M + 5S \cong 9,3M$, а 5-изогении $20M + 10S \cong 26,7M$. Эти оценки отличаются практически втрое.

Следует заметить, что найденные в работе оценки сложности вычисления 3- и 5-изогений справедливы не только для суперсингулярных кривых Эдвардса, но и для всех кривых классов полных и квадратичных кривых Эдвардса.

5. Алгоритмы вычисления 3- и 5-изогений кривых Эдвардса

Вычисление 3- и 5-изогений кривых Эдвардса (2) согласно формулам (13) – (18) и расчету параметра $d' = A^8 d^l$ изогенной кривой осуществляется с помощью приведенных ниже алгоритмов со стоимостью $6M + 5S$ и $20M + 10S$ соответственно.

Вход: точка $P = (X : Z)$ и точка 3-го порядка $Q_1 = (X_1 : Z_1)$, ядра кривой. E_d с параметром d

1. $s_1 \leftarrow X_1^2$
2. $s_2 \leftarrow Z_1^2$
3. $t_1 \leftarrow (X + Z_1)^2 - s_0 - s_2$
4. $t_2 \leftarrow t_1 + s_1$
5. $t_3 \leftarrow t_1 + s_2$
6. $t_4 \leftarrow 2t_1$
7. $t_5 \leftarrow 4s_1 + s_2 + t_4$
8. $t_6 \leftarrow 4s_2 + s_1 + t_4$
9. $D' \leftarrow t_3 \cdot t_5$
10. $C' \leftarrow t_2 \cdot t_6$
11. $u_1 \leftarrow X_1 \cdot Z$
12. $u_2 \leftarrow X \cdot Z_1$
13. $u_3 \leftarrow (u_1 + u_2)^2$
14. $u_4 \leftarrow (u_1 - u_2)^2$
15. $F \leftarrow (X + Z) \cdot u_3$
16. $G \leftarrow (X - Z) \cdot u_4$
17. $2X' \leftarrow F + G$
18. $2Z' \leftarrow F - G$

Выход: точка кривой $E'_{d'}$ $P' = (X' : Z')$ и параметры $(D' : C')$ изогенной кривой $C'E_{d'}{}'$

Алгоритм вычисления 3-изогении кривой Эдвардса

Вход: точка $P = (X : Z)$ и точки 5-го порядка $Q_1 = (X_1 : Z_1)$, , $Q_2 = (X_2 : Z_2)$ ядра кривой E_d с параметром d

1. $s_0 \leftarrow X^2$
2. $s_1 \leftarrow X_1^2$
3. $s_2 \leftarrow X_2^2$
4. $r_0 \leftarrow Z^2$
5. $r_1 \leftarrow Z_1^2$

6. $r_2 \leftarrow Z_2^{\,2}$
7. $t_0 \leftarrow s_0 - r_0$
8. $t_1 \leftarrow s_1 - r_1$
9. $t_2 \leftarrow s_2 - r_2$
10. $u_1 \leftarrow X_1 + Z_1$
11. $u_2 \leftarrow X_2 + Z_2$
12. $v_1 \leftarrow X_1 - Z_1$
13. $v_2 \leftarrow X_2 - Z_2$
14. $f_1 \leftarrow u_2 \cdot t_1$
15. $e_1 \leftarrow v_2 \cdot t_0$
16. $F_1 \leftarrow r_o \cdot f_1 + r_1 \cdot e_1$
17. $G_1 \leftarrow -s_o \cdot f_{11} + r_1 \cdot e_1$
18. $f_2 \leftarrow u_1 \cdot t_2$
19. $e_2 \leftarrow v_1 \cdot t_0$
20. $F_2 \leftarrow r_o \cdot f_2 + r_2 \cdot e_2$
21. $G_1 \leftarrow -s_o \cdot f_2 + r_2 \cdot e_2$
22. $X' \leftarrow X \cdot F_1 \cdot F_2$
23. $Z' \leftarrow Z \cdot G_1 \cdot G_2$
24. $L_1 \leftarrow s_1 \cdot s_2$
25. $L_2 \leftarrow r_1 \cdot r_2$
26. $D \leftarrow L_1 \cdot d$
27. $D \leftarrow D^2$
28. $D \leftarrow D^2$
29. $D' \leftarrow D \cdot d$
30. $C \leftarrow L_2^{\,2}$
31. $C' \leftarrow C^2$

Выход: точка кривой $E'_{d'}$ $P' = (X' : Z')$ и параметры $(D' : C')$ изогенной кривой $C'E_{d'}{}'$

Алгоритм вычисления 5-изогении кривой Эдвардса (алгоритм 4)

Эти алгоритмы отличаются наибольшей простотой и сравнительно малой стоимостью вычислений. В отличие от приведенного в работе [6] алгоритма вычисления 3-изогении мы используем вместо (8) более простое выражение (9) для функции $\phi(x, y)$ вместе с более простой формулой для параметра $d' = A^8 d^l$. Фактически при вычислении 3-изогении мы используем алгоритм, близкий к предложенному в работе [6], с той же эффективностью $6M + 5S$ стоимости вычислений. Оригинальные алгоритмы вычисления 5-изогений, как показал наш анализ, требуют втрое больших вычислительных затрат, чем для 3-изогений. Возрастание в $\frac{3}{2}$ раза числа переменных ($4 \rightarrow 6$) в 2,5 раза увеличивает число смежных произведений $\left(\frac{C_6^2}{C_4^2} = \frac{5}{2}\right)$, что дает грубую завышенную оценку (3.75 раза) выявленной пропорции.

6. Требования к параметрам криптосистемы

Поиск подходящего значения характеристики поля p в задаче SIDH с использованием 3- и 5-изогений кривых Эдвардса должен отвечать ряду необходимых условий.

Утверждение 1. 3- и 5-изогении существуют для суперсингулярных полных и квадратичных кривых Эдвардса E_d соответственно при $p \equiv -1 \bmod 60$ $p \equiv -1 \bmod 120$.

Доказательство. Точки 3-го и 5-го порядков существуют на полной суперсингулярной кривой Эдвардса порядка $p+1 = 4 \cdot 3^m \cdot 5^n$ при выполнении условий $p \equiv -1 \bmod 4$, $p \equiv -1 \bmod 3$ и $p \equiv -1 \bmod 5$, которые сводятся к одному условию $p \equiv -1 \bmod 60$. Минимальным четным кофактором порядка N_E квадратичной кривой Эдвардса является число 8 [7], при этом $p+1 = 8 \cdot 3^m \cdot 5^n$ и справедливо условие $p \equiv -1 \bmod 120$.

Утверждение 2. При нечетном $l = 2s+1$ l-изогении точек P нечетного порядка кривой есть точки нечетного порядка.

Доказательство. Кривая Эдвардса E_d порядка $N_E = 2^c \cdot n, c \geq 2$, содержит точки P нечетного порядка $n = l \cdot m$. Тогда существует l-изогения и изогенная кривая E' того же порядка N_E. l-изогения есть гомоморфизм, сжимающий в l раз точки $< P >$ в подгруппу точек нечетного порядка m кривой E'. Эта подгруппа не содержит точек четного порядка. При $m = 1$ l-изогения отображает все точки $< P >$ в нейтральный элемент O порядка 1.

Утверждение 3. При $p \equiv 1 \bmod 4$ суперсингулярных кривых Эдвардса не существует.

Доказательство. При $p \equiv 1 \bmod 4$ порядок суперсингулярной кривой $p+1 \equiv 2 \bmod 4$, тогда как для любой кривой Эдвардса число 4 делит порядок кривой [7].

Значение модуля p поля определяется требованиями безопасности. В произведении $3^m \cdot 5^n$ оба сомножителя имеют одинаковый порядок при $3^m \approx 5^n$, тогда $m \approx 1.465n$. Это уравновешивает число соответствующих циклических подгрупп. Квантовый уровень безопасности 128 бит с оценкой сложности $\sqrt[6]{p}$ (вместо $\sqrt[4]{p}$ для обычного компьютера) обеспечивается при длине модуля $\log_2 p = 6 \cdot 128 = 768$ бит. В поле F_{p^2} каждая координата точки имеет длину $2\log_2 p = 1536$ бит. Оценка длины ключа в системе SIDH составляет $6 \cdot \log_2 p = 6 \cdot 768 = 4608$ бит. Квантовый уровень безопасности 256 бит удваивает все эти оценки.

Заключение

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, позволяют реализовать наиболее быстрые алгоритмы постквантовой криптографии.

Список литературы:

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

2. 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.

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. P. 1-17.

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

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

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

7. 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.

8. Бессалов А.В., Ковальчук Л.В. Суперсингулярные скрученные кривые Эдвардса над простым полем. II. Суперсингулярные скрученные кривые Эдвардса с *j*-инвариантом, равным 66^3. // Кибернетика и системный анализ. 2019. Т. 55. №5. С. 35–46.

9. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Киев : Политехника, 2017. 272с.

10. Бессалов А.В., Цыганкова О.В. Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой // Проблемы передачи информации. 2017. Т. 53 (1). С.101-111. doi:10.1134/S0032946017010082.

11. Washington L.C. Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.

Киевский Университет имени Бориса Гринченко *Поступила в редколлегию 12.01.2020*