УДК 621.391.15 : 519.7 **DOI:10.30837/rt.2021.4.207.03**

А.В. БЕССАЛОВ, д-р техн. наук, О.В. ЦЫГАНКОВА, канд. техн. наук, С.В. АБРАМОВ

ОЦЕНКА ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ АЛГОРИТМА CSIDH НА СУПЕРСИНГУЛЯРНЫХ СКРУЧЕННЫХ И КВАДРАТИЧНЫХ КРИВЫХ ЭДВАРДСА

Введение

В статье приведены новые исследования в теме предыдущей работы [1]. Задачи постквантовой криптографии (PQC) сегодня успешно решаются различными алгоритмами, среди которых перспективными, зарекомендовали себя алгоритмы на изогениях суперсингулярных эллиптических кривых [2, 3]. Эффективной альтернативой протоколу SIDH [2] (Supersingular Isogeny Diffi-Hellman) является алгоритм CSIDH [3] (Commutative SIDH) с минимальной из известных длиной ключа. Взамен расширенного поля F_{p^2} в SIDH операции в CSIDH выполняются в простом поле F_p, что для данного p вдвое снижает длину элементов поля и размеры ключей.

Реализации алгоритмов SIDH и CSIDH ранее базировались на быстрой арифметике изогений кривых в форме Монтгомери. В работе [4] предложен новый эффективный метод вычисления изогений нечетных степеней для кривых Эдвардса на основе w-координат Фарашахи – Хоссейни [5]. Эта работа, в свою очередь, базируется на методе Монтгомери дифференциального сложения точек и адаптирует его к кривым Эдвардса. Оптимизация арифметики изогений на кривых Эдвардса в проективных координатах $(W:Z)$ в [4] значительно ускорила алгоритмы их предыдущей работы [6] и позволила авторам получить выигрыш 20 % в скорости выполнения операций по сравнению с реализацией алгоритма на кривых в форме Монтгомери. Формулы вычисления изогений нечетных степеней кривых Эдвардса [7] также содержат компоненты дифференциального сложения точек, что послужило основой метода, предложенного в [4]. Вычисления в классических проективных координатах, как показал наш анализ для изогений малых степеней [8], существенно усложняются с ростом степени изогении и проигрывают по стоимости $(W:Z)$-координатам.

Полные кривые Эдвардса E_d с одним параметром d ($\chi(d)=-1$), определенные в работе [9], имеют хорошо известные преимущества: высокая скорость экспоненцирования точки, универсальность закона сложения точек, аффинные координаты нейтрального элемента группы точек. Введение второго параметра a a кривой $E_{a,d}$ в работе [10] расширило класс кривых в форме Эдвардса и породило, согласно принятой в [11, 12] классификации, два новых класса: скрученные и квадратичные кривые Эдвардса. Они образуют пары квадратичного кручения, которые используются в данной статье для имплементации алгоритма CSIDH.

Вычисление изогений нечетных степеней для полных и квадратичных кривых Эдвардса E_d осуществляется по формулам, определенным теоремами 2 – 4 работы [7]. В предыдущей работе [1] мы обобщили теоремы [7] на кривые в обобщенной форме Эдвардса с двумя параметрами a и d, что позволило в данной статье применить скрученные и квадратичные кривые Эдвардса над полем F_p для имплементации модели CSIDH.

Наш анализ опирается на свойства скрученных и квадратичных кривых Эдвардса, связанных как пары квадратичного кручения [13, 14]. Суперсингулярные кривые этих классов с одинаковым порядком $N_E = p+1 = p+1 = 2^m n, m \geq 3,$ (n – нечетное) существуют лишь при $p \equiv 3 \bmod 4$. Минимальный четный кофактор порядка таких кривых равен 8, тогда для алгоритма CSIDH с нечетным $n = \prod_{i=1}^{K} l_i$. модуль поля F_p следует выбирать как $p = 8n-1$.

С целью адаптации определений для арифметики изогений кривых Эдвардса и кривых в форме Вейерштрасса мы используем модифицированный закон сложения точек [11, 12].

В разд. 1 дан краткий обзор свойств скрученных и квадратичных суперсингулярных кривых Эдвардса (СКЭ) [13 – 15]. В разд. 2 рассматриваются специфичные аспекты имплементации модели алгоритма CSIDH на скрученных и квадратичных СКЭ, приводится модификация алгоритма [3], рассчитаны и табулированы параметры изогенных кривых модели, приведен пример вычислений Алисы и Боба в схеме разделения секрета Диффи – Хеллмана. В разд. 3 дан сравнительный анализ стоимости вычисления параметра d' изогенной кривой E' с использованием $(W:Z)$-координат [4] и классических проективных координат $(X:Y:Z)$[11]. Обсуждается дискуссионный вопрос об отказе от вычисления изогенной функции $\phi(R)$ случайной точки R кривой в алгоритме CSIDH.

1. Свойства скрученных и квадратичных суперсингулярных кривых Эдвардса

Рассмотрим некоторые специфические свойства суперсингулярных кривых Эдвардса (СКЭ) [13, 14]. Эллиптическая кривая *в обобщенной форме Эдвардса* [11] определяется уравнением

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

При квадратичном характере $\chi(ad) = -1$, кривая (1) изоморфна *полной кривой* Эдвардса [9] с одним параметром d:

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

В случае $\chi(ad) = 1, \chi(a) = \chi(d) = 1$ имеет место изоморфизм кривой (1) с *квадратичной кривой Эдвардса* [11]:

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

имеющей, в отличие от (2), параметр d, определенный как квадрат. Для обеих кривых (2) и (3) обычно принимают $a = 1$. В работе [10] кривая (3) и кривая (2) названы *кривыми Эдвардса*. Вместе с тем различие квадратичных характеров этих кривых ведет к кардинально различным их свойствам [11, 12].

Скрученная кривая Эдвардса определена в работе [11] как частный случай кривой (1) при $\chi(ad) = 1, \chi(a) = \chi(d) = -1$.

Мы определяем пару скрученной и квадратичной кривой Эдвардса [11] как пару квадратичного кручения с параметрами $\chi(ad) = 1, a' = ca, d' = cd, \chi(c) = -1$. Так как СКЭ существуют лишь при $p \equiv 3 \bmod 4$[11], то можно принять $c = -1, a' = -a = -1, d' = -d$, где a,d – параметры квадратичной кривой, соответственно a', d' – скрученной кривой. Иначе говоря, переход от квадратичной к скрученной кривой кручения и обратно можно определить как $E_d = E_{1,d} \leftrightarrow E_{-1,-d}$. Соответственно, уравнение скрученной СКЭ при $p \equiv 3 \bmod 4$ из (1) можно записать как

$$E_{-1,-d}: \quad x^2 - y^2 = 1 - dx^2y^2, \quad d \in F_p^*, \quad d \neq 1., \chi(d) = 1. \tag{4}$$

Порядок N_E эллиптической кривой над простым полем F_p определяется на основе следа t характеристического уравнения Фробениуса $\varphi^2 + t\phi + p = 0$ как $N_E = p + 1 - t$. Для кривой квадратичного кручения E^t соответствующий порядок будет равным $N_E{}^t = p + 1 + t$. Эллиптическая кривая является суперсингулярной тогда и только тогда, когда над любым расширением простого поля F_p след уравнения Фробениуса $t \equiv 0 \bmod p$, при этом

$\varphi^2 = -p,\ \varphi = \pm\sqrt{-p}$. [14,15]. Иными словами, в алгебраическом замыкании $\overline{F}_p$ суперсингулярная кривая не содержит точек порядка p. Над простым полем F_p такая кривая всегда имеет порядок $N_E = p+1$.

Итак, скрученные и квадратичные СКЭ как пара квадратичного кручения имеют одинаковый порядок $N_E = p+1$, но разную структуру. Кроме двух точек $(0,\pm 1)$, все их точки различны, поэтому изогении одинаковых степеней имеют разные ядра и вычисляются независимо. Обе кривые являются нециклическими в отношении точек четного порядка (содержат по три точки 2-го порядка, две из которых – особые точки $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ [11]). Квадратичная СКЭ, кроме того, содержит две особые точки 4-го порядка $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$.. Наличие трех точек 2-го порядка ограничивает числом 8 минимальный четный кофактор порядка $N_E = 8n, (n - \textit{нечетное})$ скрученных и квадратичных кривых Эдвардсах [11]. Максимальный порядок точек этих кривых равен $N_E / 2$. Важно, что точки четных порядков в вычислениях алгоритма CSIDH не участвуют.

Для кривой (1) J -инвариант [13, 15]

$$J(a,d) = \frac{16(a^2 + d^2 + 14ad)^3}{ad(a-d)^4}, \quad ad(a-d) \neq 0\,. \tag{5}$$

Этот параметр различает изогенные (с разными J -инвариантами) и изоморфные (с равными J -инвариантами) кривые. Так как J -инвариант сохраняет свое значение для всех изоморфных кривых и пар квадратичного кручения, он одинаков для пары скрученных и квадратичных СКЭ ($a = \pm 1$), поэтому в дальнейшем будем пользоваться J -инвариантом $J(d)$. Он является полезным инструментом как при поиске суперсингулярных кривых, так и при построении графов цепочек изогений. Одним из свойств J -инварианта $J(d)$ является

$$J(d) = J(d^{-1})\,.$$

Для рассматриваемых классов СКЭ замена $d \to d^{-1}$ дает изоморфизм, а для полных кривых Эдвардса – квадратичное кручение.

2. Модификация алгоритма csiidh на скрученных и квадратичных кривых Эдвардса

Алгоритм PQC CSIDH (Commutative SIDH) предложен авторами [3] для решения той же задачи обмена ключами (SIDH [2]), но на основе изогенных отображений эллиптических кривых в целом как аддитивных абелевых групп. Такое отображение над простым полем F_p определено как класс групповой операции (the class group action) и является коммутативным. В сравнении с известной оригинальной схемой CRS (Couveignes (1997), Rostovtsev, Stolbunov (2004)) на несуперсингулярных кривых использование изогений суперсингулярных кривых позволило кардинально ускорить алгоритм и получить наименьший из известных размер ключа (512 бит в [3]).

Пусть кривая E порядка N_E содержит точки малых нечетных порядков $l_i, i = 1,2,...,K$. Тогда существует изогенная кривая E' того же порядка N_E как отображение степени l_i: $E \to E' = [l_i] * E$. Повторение этой операции e_i раз будем обозначать $[l_i^{e_i}] * E$. Значения экспонент изогений $e_i \in Z$ определяют длину цепочки изогений степени l_i. В работе [3] принят интервал значений экспонент $[-m \le e_i \le m], m = 5, K = 74$, что обеспечивает уровень безопасности 128 бит при атаках квантового компьютера. Отрицательные значения экспоненты e_i означают переход к суперсингулярной кривой квадратичного кручения.

Имплементация алгоритма CSIDH в основном использует быструю арифметику эллиптических кривых Монтгомери $y^2 = x^3 + Cx^2 + x,\ C \neq \pm 2$, содержащих две точки 4-го порядка и, соответственно, имеющие порядок $N_E = 4n(n - \text{нечетное})$ [9]. В работе [4] алгоритм строится на полных СКЭ того же порядка. В настоящей работе мы впервые предлагаем использовать в алгоритме CSIDH скрученные и квадратичные СКЭ, имеющие те же рекордные показатели быстродействия, что и полные кривые Эдвардса [11]. Такая возможность возникает на основе доказанных нами в [1] теорем. При минимальном кофакторе 8 порядок скрученных и квадратичных СКЭ $N_E = 8n$. Таким образом, для этих классов СКЭ с порядком $N_E = 8n = p + 1, \quad n = \prod_{i=1}^{K} l_i.$ модуль поля в алгоритме CSIDH следует выбирать как $p \equiv -1 \bmod 8$.

Не интерактивный обмен ключами по схеме Диффи – Хеллмана включает этапы [3]:

1. **Выбор параметров.** Для малых простых нечетных l_i вычисляется $n = \prod_{i=1}^{K} l_i.$, где значение K определяется уровнем безопасности, и выбирается подходящий модуль поля $p = 2^m \prod_{i=1}^{K} l_i. - 1,\ m \geq 3$ и стартовая эллиптическая кривая E_0.

2. **Вычисление открытых ключей.** Алиса с помощью своего секретного ключа $\Omega_A = (e_1, e_2, .., e_K)$ строит изогенное отображение $\Theta_A = [l_1^{e_1}, l_2^{e_2}, .., l_K^{e_K}]$ и вычисляет изогенную кривую $E_A = \Theta_A * E_0$ как свой открытый ключ. Боб на основе секретного ключа Ω_B и функции Θ_A выполняет те же вычисления и получает свой открытый ключ $E_B = \Theta_B * E_0$. Эти кривые определяются их параметрами с точностью до изоморфизма.

3. **Обмен ключами**. Здесь протокол подобен п.2 с заменой $E_0 \to E_B$ для Алисы и $E_0 \to E_A$ для Боба. Зная открытый ключ Боба, Алиса вычисляет $E_{BA} = \Theta_A * E_B = \Theta_A \Theta_B * E_0$ Аналогичные действия Боба дают результат $E_{AB} = \Theta_B * E_A = \Theta_B \Theta_A * E_0$**,** совпадающий с первым в силу коммутативности групповой операции. В качестве разделенного секрета берется J -инвариант кривой E_{AB} (E_{BA}).

Ниже приводим модификацию алгоритма вычислений Алисы согласно п.2 [3] с использованием изогений скрученных и квадратичных СКЭ.

Algorithm 1: Evaluating the class-group action on twisted and quadratic SEC.

Input: $d_A \in E_A, \chi(d) = 1$ *and a list of integers* $\Omega_A = (e_1, e_2, ...e_K)$.

Output: d_B *such that* $[l_1^{e_1}, l_2^{e_2}, ...l_K^{e_K}] * E_A = E_B$, *where* $E_{A,B}$: $x^2 + y^2 = 1 + d_{A,B} x^2 y^2$,

1. **While** *some* $e_i \neq 0$ **do**
   2. *Sample a random* $x \in F_p$,
   3. Set $a \leftarrow 1, \quad E_A : x^2 + y^2 = 1 + d_A x^2 y^2$ **if** $(1 - x^2)/(1 - dy^2)$ *is a square in* F_p,
   4. **else** $a \leftarrow -1, \quad E_A : x^2 - y^2 = 1 - d_A x^2 y^2$,
   5. *Let* $S = \{i \mid ae_i > 0\}$. **If** $G = \varnothing$ *then start over to line 2 while* $a \leftarrow -a$,
   6. *Let* $k = \prod_{i \in G} k_i, \quad$ *and compute* $R \leftarrow [(p+1)/2k, \quad P = (x, y)$,
   7. **For** e*ach* $i \in S$ **do**
      8. *Compute* $Q \leftarrow [k / l_i] R$
      9. **If** $Q \neq (1,0)$ *Compute an isogeny* $\phi : E_A \to E_B$ *with* $\ker \phi = Q$,
      10. ***Set*** $d_A \leftarrow d_B$, $R \leftarrow \phi(R)$, $e_i \leftarrow e_i - a$ **,**
      11. *Skip* i *in* S *and* $k \leftarrow k / l_i$ **if** $e_i = 0$,
12. **Return** d_A**.**

В сравнении с алгоритмом 2 в работе [3] в нашем алгоритме 1, адаптированном к скрученным и квадратичным СКЭ, сделаны модификации:

1. Проверка квадратичности y^2 в п.3 выполняется для уравнения квадратичной кривой Эдвардса (3)

2. При порядке скрученной кривой Эдвардса $N_E = 8n = p+1$ с максимальным порядком точки $N_E/2 = 4n$ для получения точки порядка n достаточно двукратного удвоения случайной точки P. В п.6 это свойство учтено уменьшением одного удвоения в скалярном произведении точки R.

3. Скорректирован п.9 (нельзя сбрасывать индекс i до обнуления e_i в п.10).

4. Обновление числа $k \leftarrow k/l_i$ вместе со сбросом i в п.11 следует делать после обнуления e_i.

Согласно п.10 для каждого l_i вычисляется ровно e_i изогений до обнуления экспоненты e_i. В зависимости от ее знака изогении вычисляются в классе квадратичных ($e_i > 0$) или скрученных СКЭ ($e_i < 0$).

В основе построения изогений нечетных простых степеней для квадратичных кривых Эдвардса лежит теорема 2 [7], а для скрученных кривых Эдвардса – теорема 1 [1]. В последней работе впервые приведены формулы отображений $\phi(P)$ для кривой (1), зависящие от двух параметров a и d. Теорема формулируется ниже.

Теорема 1 [1]. Пусть $G = \{(1,0), \pm Q_1, \pm Q_2, ..., \pm Q_s\}$ – подгруппа нечетного простого порядка $l = 2s+1$ точек $\pm Q_i = (\alpha_i, \pm\beta_i)$, кривой $E_{a,d}$ (1) над полем F_p.

Определим

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

Тогда $\phi(x, y)$ – l-изогения с ядром G из кривой $E_{a,d}$ в кривую $E_{a',d''}$ с параметрами

$$a' = a^l,\ d' = d^l A^8,\ \ A = \prod_{i=1}^{s} \alpha_i, \tag{6}$$

и отображающей функцией

$$\phi(x, y) = \left(\frac{x}{A^2} \prod_{ii=1}^{s} \frac{(\alpha_i x)^2 - (a\beta_i y)^2}{1 - (d\alpha_i \beta_i xy)^2}, \frac{y}{A^2} \prod_{i=1}^{s} \frac{(\alpha_i y)^2 - (\beta_i x)^2}{1 - (d\alpha_i \beta_i xy)^2} \right), \tag{7}$$

или

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

Доказательство теоремы приведено в [1].

Рассмотрим простую модель имплементации алгоритма CSIDH на скрученных и квадратичных СКЭ, образующих пары квадратичного кручения с одинаковым порядком. Такие кривые существуют лишь при $p \equiv -1 \bmod 8$ и имеют порядок $N_E = N_E{}^t = p+1 = cn\ (n - odd),\ c \equiv 0 \bmod 8$. Пусть такая пара кривых содержит ядра 3-го и 5-го порядка при наименьшем значении $n = 15$, тогда минимальное простое $p = 239$ и порядок этих кривых $N_E = 16n = 240$. Параметр d всего семейства 118 квадратичных кривых Эдвардса можно принять как квадраты $d = r^2 \bmod p, r = 2..119$. Из них найдено 30 пар квад-

ратичных и скрученных СКЭ с параметрами $a=\pm 1$ и $\chi(ad)=1$. Квадратичную СКЭ (3) обозначаем E_d, а скрученную СКЭ (4) – как $E_{-1,-d}$. В табл. 1 приведены значения параметра d для пар квадратичных и скрученных СКЭ. Они записаны как квадраты $d=r^2 \bmod p,, r=5..119.$ в порядке нарастания r.

Таблица 1

Значения параметра d квадратичных и скрученных СКЭ $(a=\pm 1)$ при $p=239$ и $N_E=240$

25	64	121	196	50	183	5	10	87	176
24	153	11	110	48	187	120	193	27	160
213	44	2	201	61	3	206	192	80	62

Для первой скрученной кривой $E_{-1,-25}=E_{-1,-d}{}^{(0)}$ из табл. 1 можно построить 3- и 5-изогении и найти параметры $d^{(i)}$ цепочки изогенных кривых $E_{-1,-d}{}^{(i)}, i=1,2,...,\pi$, таких что $E_{-1,-d}{}^{(\pi)}=E_{-1,-d}{}^{(0)}$. Параметр a всех изогенных скрученных СКЭ можно зафиксировать как квадратичный невычет $a=-1$ (см. (6)).

Скрученная кривая $E_{-1,-25}$ над полем F_{239} содержит точку 3-го порядка $Q_1=(149,64)$, тогда согласно теореме 3 [7] $A=\prod_{k=1}^{s}\alpha_k=149$, $A^8=8$, $d^{(1)}=A^8(d^{(0)})^3=3$. Вычисленные параметры $d^{(i)}$ цепочки 3-изогенных кривых со стартовым значением $d=d^{(0)}=25$ можно записать как последовательность $d^{(i)}\in\{25,\ 3,\ 10,\ 50,\ 110,25\}$ периода 5. Период цепочки $\pi=5$ делит число всех скрученных СКЭ, равное 30. Задавая другое стартовое значение $d=2$ из табл. 1, можно получить другую последовательность параметров $d^{(i)}\in\{2,61,62,193,5,2\}$. Эти данные используются для скрученных СКЭ при построении функции $[l_1^{e_1}, l_2^{e_2}], l_1=3, e_1<0$.

При положительных значениях экспонент $e_1>0$ результаты аналогичных вычислений для квадратичных СКЭ с другими ядрами $<Q_1>3$-го порядка отличаются от приведенных выше лишь реверсным порядком элементов последовательности $d^{(i)}\in\{25,110,50,10,3,25\}$.

Ядром 5-изогении на скрученной кривой $E_{-1,-25}$ является подгруппа точек 5-го порядка $Q_1=(\alpha_1,\beta_1)=(-95,28)$, $2Q_1=Q_2=(\alpha_2,\beta_2)=(-72,-119)$, $3Q_1=-2Q_1=(\alpha_2,-\beta_2)$, $4Q_1=-Q_1=(\alpha_1,-\beta_1)$, $5Q_1=O=(1,0)$. Она однозначно определяется координатами α_1,α_2 двух точек и уравнением (4). Используя формулу (6) и координаты ядер, можно вычислить элементы последовательности $d^{(i)}\in\{25,\ 2,11,\ 50,193,187,3,61,183,110,5,121,10,62,\ 201,\ 25\}$ параметров цепочки 5-изогенных скрученных СКЭ периода $\pi=15$. Для квадратичных кривых эта последовательность записывается в обратном порядке.

Примем секретные ключи экспонент изогений $\{e_i\}$ Алисы и Боба $\Omega_A=(-1,2),\ \ \Omega_B=(4,-3)$, их функции изогенных отображений соответственно $\Theta_A=[3^{-1},5^2]$, $\Theta_B=[3^4,5^{-3}]$. Вычислим их отрытые ключи $d_A,\ \ d_B$. В качестве стартовой кривой цепочки изогений примем кривую $E^{(0)}=E_{-1,-25}$. Алиса вычисляет параметры 3-х изогенных кривых $E^{(i)}$: одну 3-изогенную скрученную СКЭ и две 5-изогенных квадратичных СКЭ в произвольном порядке. Ее вычисления порождают цепочку изогенных кривых

$E^{(0)} = E_{-1,-25} \to E_{-1,-3} \Rightarrow E_3 \to E_{187} \to E_{193}$. Итак, открытый ключ Алисы $d_A = 193$. Аналогичные вычисления Боба с секретным ключом $\Omega_B = (4,-3)$:

$$E^{(0)} = E_{-1,-25} \Rightarrow E_{25} \to E_{110} \to E_{50} \to E_{10} \to E_3 \Rightarrow E_{-1,-3} \to E_{-1,-61} \to E_{-1,-183} \to E_{-1,-110}$$

дают значение его открытого ключа $d_B = 110$.

Далее, в схеме разделения секретов Алиса, зная открытый ключ Боба, вычисляет изогенную кривую $E_{BA} = [3^{-1}, 5^2] * E_{-1,-110} = E_{-1,-62}$. Тот же результат с помощью функции $E_{AB} = [3^4, 5^{-3}] * E_{-1,-193} = E_{-1,-62}$ получает Боб. Разделенным секретом есть параметр $d_{AB} = 62$.

Отображение (8) точек $P = (x, y)$ кривой $E_A = E_{-1,-25}$ с ядром 3-изогении $G = \{(1,0), \pm Q = (149, \pm 64)\}$ имеет вид

$$\phi_3(x, y) = \left(\frac{x}{149^2} \frac{x^2 + 64^2}{1 + 25 \cdot 64^2 x^2}, \frac{y}{149^2} \frac{x^2 - 149_i^{\,2}}{1 - 25 \cdot 149^2 x^2} \right).$$

Точка максимального нечетного 15-го порядка $P = (-44, -12)$ кривой $E_{-1,-25}$ отображается в точку $P' = (221, 125)$ 5-го порядка кривой $E_{-1,-3}$, точка 5-го порядка $P = (144, 28)$ отображается в точку $P' = (25, 183)$ 5-го порядка, а точка 3-го порядка $P = (149, 64)$ отображается в нейтральный элемент группы – точку $P' = (1, 0) = O$. Как видим, функция $\phi_3(x, y)$ втрое снижает порядки точек прообраза, кратных 3, и не меняет порядки других точек.

Для кривой $E_{-1,-25}$ с ядром 5-го порядка $G = \{(1,0), \pm Q_1 = (-95, \pm 28), \pm Q_2 = (-72, \pm 119)\}$ 5-изогения в форме (8) записывается как

$$\phi_5(x, y) = \left(\frac{x}{155} \frac{x^2 + 28^2}{1 + 25 \cdot 28^2 x^2} \frac{x^2 + 119^2}{1 + 25 \cdot 119^2 x^2}, \frac{y}{155} \frac{x^2 - 95_i^{\,2}}{1 - 25 \cdot 95^2 x^2} \frac{x^2 - 72_i^{\,2}}{1 - 25 \cdot 72^2 x^2} \right).$$

Точка 15-го порядка $P = (-44, -12)$ кривой $E_{-1,-25}$ отображается этой функцией в точку $P' = (-18, 7)$ 3-го порядка кривой $E'_{-1,-2}$, точка 3-го порядка $P = (149, 64)$ отображается в точку $P' = (-18, -7)$ 3-го порядка изогенной кривой, точка 5-го порядка $P = (-95, 28)$ отображается в точку $P' = (1, 0) = O$. Здесь функция $\phi_5(x, y)$ снижает порядки точек прообраза, кратных 5, в пять раз, без изменения порядков других точек.

3. Оценка стоимости вычислений алгоритма csiidh на скрученных и квадратичных кривых Эдвардса в координатах (W:Z) и (X:Y:Z)

Значительный прогресс в эффективности вычисления изогений нечетных степеней СКЭ достигнут в работе [4] на основе использования проективных координат Фарашахи – Хоссейни [5]. Вместе с тем, некоторые оценки стоимости вычислений алгоритма Edwards-CSIDH в [4] не полны и учитывают лишь часть вычислений. В данной статье мы даем более корректный анализ ряда вычислительных затрат в координатах (W:Z) со сравнительной оценкой их в координатах (X:Y:Z).

3.1. Оценка стоимости вычислений изогенной функции

В работе [4] доказана теорема 1, определяющая изогенное отображение нечетной степени $l = 2s + 1$ кривой Эдвардса E_d в кривую $E_d{}'$ в координатах Фарашахи – Хоссейни $w(x, y) = dx^2 y^2$ (или $w(x, y) = x^2 / y^2$). Как и в работе [7], она доказана лишь для кривой Эдвардса E_d ($a = 1$), и неизвестно, применимы ли ее результаты в классе скрученных кривых

Эдвардса $E_{a,d}$ ($\chi(a)=\chi(d)=-1$). Ниже приводим эту теорему для всех кривых в обобщенной форме $E_{a,d}$ (1), которая доказана нами в работе [1]. Вместо взятой за основу формулы (7) в работе [4] мы исходим из более лаконичной формулы (8), полученной нами в теореме 1.

Теорема 2 [1]. Пусть $G=\{(1,0),\pm Q_1,\pm Q_2,...,\pm Q_s\}$ – подгруппа нечетного простого порядка $l=2s+1$ точек $\pm Q_i=(\alpha_i,\pm\beta_i)$, кривой $E_{a,d}$ над полем F_p, и $w_i=d\alpha_i^2\beta_i^2$, $w=dx^2y^2$, $P=(x,y)\in E_{a,d}$. Тогда $w(\phi(x,y))=w(x',y')$ $w(\phi(x,y))=w(x',y')$ есть l-изогения с ядром G из кривой $E_{a,d}$ в кривую $E_{a',d'}$ с параметрами $a'=a^l$, $d'=d^lA^8$, $A=\prod_{i=1}^{s}\alpha_i$, и отображающей функцией

$$w(\phi)=w\prod_{i=1}^{s}\frac{(w-w_i)^2}{(1-ww_i)^2}. \tag{9}$$

Доказательство этой теоремы дано в работе [1].

Подчеркнем, что изогения (9) для w-координаты кривой $E_{a,d}$ (1) не зависит от параметра a и в равной степени справедлива для квадратичных и скрученных кривых Эдвардса, образующих пары квадратичного кручения [11]. Иными словами, функция (9) отображает точки кривой одного из этих двух классов в точки кривой того же класса.

Реализация вычислений изогений (9) для полных кривых Эдвардса дана в работе [4]. Для вычисления параметров $d^{(i)}$ цепочки изогений в проективных координатах вводится дополнительный параметр С в уравнение кривой E_d (2). Для пары квадратичной и скрученной СКЭ (3), (4) при $p\equiv 3 \bmod 4$ мы принимаем $a=\pm 1$, $d=ar^2 \bmod p$, $r\in[2,...,(p-1/2)]$ и определим кривую

$$E_{C,D}:\ \ Cx^2+aCy^2=C+aDx^2y^2,\quad D=dC,\quad \chi(d)=1. \tag{10}$$

При $a=\pm 1$ получаем проективное уравнение соответственно квадратичной (3) и скрученной (4) СКЭ как пары квадратичного кручения..

Переход к проективным координатам $(W:Z)$ позволяет избежать инверсий в формуле (9), при этом для кривой (10) при С=1:

$$W'=W\prod_{i=1}^{s}(WZ_i-W_iZ)^2,$$

$$Z'=Z\prod_{i=1}^{s}(ZZ_i-WW_i)^2.$$

Здесь для каждого s выполняется $4sM+2M+2S$ операций в поле ($M=$ умножение, S – возведение в квадрат). Если ввести промежуточные формулы

$$H=(W+Z)(W_i-Z_i),\qquad J=(W-Z)(W_i+Z_i),$$

$$2W'=W\prod_{i=1}^{s}(H_i-J_i)^2,$$

$$2Z'=Z\prod_{i=1}^{s}(H_i+J_i)^2,$$

то требуется всего $4sM+2S$ операций при вычислении одной изогенной функции (9). Подчеркнем, что в этой оценке, приведенной в [4], не учтены стоимости вычислений параметров $(W_i,Z_i,)$ ядер изогений. Они определены ниже.

3.2. Вычисление точек ядра изогении и параметра d' изогенной кривой в координатах (W:Z)

Для каждой изогенной кривой E' прямое вычисление параметра d' согласно теоремам [7] осуществляется по формуле (6) $d' = d^l (\prod_{i=1}^{s} \alpha_i)^8$.

В работе [4] для расчета d' в *w*-координатах используется формула

$$d' = d^l \prod_{i=1}^{s} \frac{(1+w_i)^8}{4^4}, \quad w_i = d\alpha_i^2\beta_i^2. \tag{11}$$

На первый взгляд, вычисления по формуле (6) проще, так как не требуют для каждого i дополнительно $2M+S$ операций для расчета $w_i = d\alpha_i^2\beta_i^2$ в (11). Однако в первом случае вычисления выполняются на основе рекуррентного удвоения точек ядра в классических проективных координатах $(X:Y:Z)$, а во втором – в координатах $(W:Z)$, что потребовало сравнительного анализа стоимости вычислений при двух подходах.

В проективных *w*-координатах $(D':C')$ имеем

$$D' = D^l \prod_{i=1}^{s} (Z_i + W_i)^8 \tag{12}$$

$$C' = C^l \prod_{i=1}^{s} (2Z_{i\,i})^8, \quad d' = D'/C' \tag{13}$$

Авторы [4] оценивают стоимость вычислений (12), (13) как $2M(s-1)+6S$. В эту оптимистичную оценку не входят стоимости вычислений d^l, W_i, Z_i. В соответствии с п.8 алгоритма 1 известной после SM случайной точки R является лишь одна точка ядра $Q_1 = (\alpha_1, \beta_1)$, с помощью которой рекуррентно вычисляются точки $Q_i = (\alpha_i, \beta_i), i = 2,3,...,s,$ и координаты $w_i = d\alpha_i^2\beta_i^2$. Оценим эти затраты.

Для расчета координат $(W_i, Z_i,)$ ядер простых нечетных порядков l_i достаточно $(s-1)$ раз удвоить точку $Q_1 = (\alpha_1, \beta_1)$ с координатами $(W_1, 1)$. Используя уравнение кривой (1), закон удвоения запишем как [10, 11]

$$2(\mathrm{x}_1, \mathrm{y}_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2} \right) = \left(\frac{x_1^2 - ay_1^2}{1 - w_1}, \frac{2x_1y_1}{1 + w_1} \right) = (\mathrm{x}_2, \mathrm{y}_2).$$

Отсюда

$$w_2 = d\left(\frac{x_1^2 - ay_1^2}{1 - w_1} \cdot \frac{2x_1y_1}{1 + w_1} \right)^2 = 4w_1 \left(\frac{(x_1^2 - ay_1^2)}{(1 - w_1^{\,2})} \right)^2$$

В последней формуле сомножитель в числителе преобразуется к виду

$$(x_1^2 - ay_1^2)^2 = (x_1^2 + ay_1^2)^2 - 4ax_1^2y_1^2 = (1 + w_1)^2 - 4ad^{-1}w_1 .$$

В итоге

$$w_2 = \frac{4w_1(d(1 + w_1)^2 - 4aw_1)}{d(1 - w_1^2)^2} .$$

В проективных координатах $(W_i, Z_i,)$ можно записать

$$W_2 = 4W_1(d(Z_1 + W_1)^2 - 4aW_1),$$

$$Z_2 = d(Z_1 + W_1)^2(Z_1 - W_1)^2.$$

Рекуррентное удвоение с учетом $d = D/C$ дает

$$W_{i+1} = 4W_i(d(Z_i + W_i)^2 - 4aW_i), \quad i = 1,2,...,s-1, \tag{14}$$

$$Z_{i+1} = d(Z_i + W_{i1})^2(Z_i - W_i)^2. \tag{15}$$

Стоимость вычислений (14), (15) с учетом стоимости расчета W_1 составляет $(4M + 2S)(s-1) + 2M + S$. В итоге вместе с вычислениями (12), (13) суммарную стоимость вычислений можно оценить равной $(6M + 2S)(s-1) + 2M + 7S$.

3.3. Вычисление точек ядра изогении и параметра d' изогенной кривой в проективных координатах (X:Y:Z)

Используя уравнение кривой (1), закон удвоения запишем в форме, не зависящей от параметра d [11]:

$$2(\mathrm{x}_1, \mathrm{y}_1) = \left(\frac{x_1^2 - ay_1^2}{2 - x_1^2 - ay_1^2}, \frac{2x_1y_1}{x_1^2 + ay_1^2} \right)$$

Подсчет числа возведений в квадрат и умножений в поле и с учетом $a = \pm 1$ дает суммарную стоимость удвоения точки в координатах (X:Y:Z) $4M + 3S$ [10, 11].

Рекуррентное удвоение точки ядра $Q_i = (\alpha_i, \beta_i),$, после замены обозначений $\alpha_i \to \mathrm{x}_i$, $\beta_i \to \mathrm{y}_i$, определяется формулами:

$$X_{i+1} = (X_i^2 - aY_i^2)(X_i^2 + aY_i^2), \; i = 1,2,...,s-1, \tag{16}$$

$$Y_{i+1} = 2X_iY_i(2Z_i^2 - X_i^2 - aY_i^2), \tag{17}$$

$$Z_{i+1} = (2Z_i^2 - X_i^2 - aY_i^2)(X_i^2 + aY_i^2), \tag{18}$$

Заметим, что для каждого X_i и Z_i возведение в квадрат осуществляется в следующей итерации, что позволяет соответствующие произведения квадратов возводить в 4-ю степень вместо 8-й. Стоимость вычислений (16) – (18) составляет $(4M + 3S)(s-1)$.

Взамен формул (12), (13) расчета параметра d' в проективных координатах получаем:

$$D' = D^l \left(\prod_{i=1}^{s} X_i^2 \right)^4, \tag{19}$$

$$C' = C^l \left(\prod_{i=1}^{s} Z_i^2 \right)^4, \tag{20}$$

Стоимость вычислений (19), (20) составляет $2M(s-1) + 4S$. Вместе с удвоением точек ядра (16) – (18) суммарная стоимость равна $(6M + 3S)(s-1) + 4S$.

Можно заключить, что вычисления параметра d' в w-координатах (стоимость равна ($(6M + 2S)(s-1) + 2M + 7S$)) более эффективны в сравнении с координатами (X:Y:Z) с экономией sS для больших s числа полевых операций возведений в квадрат. Ясно, что это связано с более эффективным удвоением точек ялра в w-координатах. Вблизи верхней границы степеней изогений $l_{\max} = 587, s = 293$ [3] этот выигрыш близок к 300S.

Дискуссионным является вопрос о необходимости вычисления изогенной функции $R' = \phi(R)R$ в п.10 алгоритма 1. Для изогении $\phi(R)$ степени l_i точка $R' \in E'$ имеет порядок, не содержащий сомножителя l_i, и, таким образом, бесполезна для нахождения следующего ядра в цепочке изогений данной степени. Для этой цели следует вновь найти случайную точку R'

кривой E′, содержащей точку точку порядка l_i. Это осуществляется с помощью скалярного умножения (SM) во внешнем цикле алгоритма 1.

Конечной целью алгоритма разделения секретов CSIDH является нахождение общего параметра d_{AB} кривой E_{AB}. Для каждого шага в цепочке изогений $E \to E'$ необходим лишь расчет параметра $d' = \psi(d, Q)$ на основе параметров d и ядра $< Q >$ домена E. Этот расчет вовлекает два SM случайных точек R и $(s-1)$ рекуррентных удвоений точек $< Q >$. Таким образом, построение и вычисление достаточно сложной функции $\phi(R)$ не является необходимым для реализации алгоритма CSIDH. Она используется лишь в конце цепочки изогений при $R = Q, \phi(Q) = (1,0)$, однако это известное свойство не требует проверки. Часть вычислений в алгоритме, связанных с расчетом функции $\phi(R)$, можно сэкономить.

Результаты имплементации модели Эдвардс-CSIDH [4] в проективных координатах $(W : Z)$ утверждают, что он не быстрее модели Монтгомери-CSIDH в координатах $(X : Z)$ на 20 %. Заметим, что эта модель построена на полных кривых Эдвардса с порядком. $N_E = p + 1 = 4n$ (n – нечетное). На основе теорем 1 и 2 [1], в данной работе мы показали, как реализовать такую модель на скрученных и квадратичных СКЭ, образующих пары квадратичного кручения. Преимуществом этих классов кривых перед полными кривыми Эдвардса является отсутствие трудоемкой инверсии параметра $d \to d^{-1}$, необходимой при переходе к полной кривой квадратичного кручения. Это лишь ускоряет выполнение алгоритма. Однако при одинаковом максимальном порядке точки $4n$ порядок этих кривых $N_E = 8n$ вдвое больше в сравнении с полными, что вряд ли существенно.

Можно заключить, что метод вычисления изогений нечетных степеней в координатах $(W : Z)$, предложенный в [4], с использованием полных и скрученных СКЭ, позволяет реализовать наиболее быстрые на сегодня вычисления при построении PQC протокола CSIDH и подобных. Доказанные в работе [1] теоремы открывают для их имплементации классы скрученных и квадратичных кривых Эдвардса.

В статье впервые приведены пример такой имплементация для простой модели алгоритма CSIDH и оценки стоимости вычислений параметров изогенных кривых. Наибольшие вычислительные затраты в алгоритме CSIDH связаны со скалярным умножением SM случайных точек, которые требуют скорее экспериментальной оценки. Много научных работ сегодня посвящены теме Constant time CSIDH [16, 17 и др.] и предлагают различные алгоритмы защиты от атак побочного канала. Нами планируются дальнейшие исследования в этой теме.

Список литературы:

1. Bessalov A., Sokolov V., Skladannyi P., Zhyltsov O. Computing of odd degree isogenies on supersingular twisted Edwards curves // CEUR Workshop Proceedings. 2021. 2923, pp. 1–11. (2021).
2. Jao and L. de Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies // Post-Quantum Cryptography, pp. 19-34 (2011).
3. Castryck W., Lange T., Martindale C., Panny L., Renes J. CSIDH: An efficient post-quantum commutative group action // Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology {ASIACRYPT 2018. pp. 395{427. Springer International Publishing, Cham (2018).
4. Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. Security and Communication Networks, 2019.
5. Farashahi R.R., Hosseini S.G. Differential addition on twisted Edwards curves. In: Pieprzyk, J., Suriadi, S. (eds.) Information Security and Privacy. pp. 366{378. Springer International Publishing, Cham (2017).
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.
7. 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).
8. A. Bessalov V. Sokolov P. Skladannyi. Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves // Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS’2020), June 2–3, 2020: abstracts. No. I, vol. 2631. Aachen : CEUR, 2020. P. 30–39.

9. 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.

10. 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. 1-1.

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

12. Bessalov A.V., Tsygankova O.V. Number of curves in the generalized Edwards form with minimal even cofactor of the curve order // Problems of Information Transmission. Vol. 53, Is. 1 (2017). P. 92-101. doi:10.1134/S0032946017010082.

13. Bessalov A.V., Kovalchuk L.V. Supersingular Twisted Edwards Curves Over Prime Fields. I. Supersingular Twisted Edwards Curves with j-Invariants Equal to Zero and 12^3 // Cybernetics and Systems Analysist. 2019. 55(3). P. 347–353.

14. Bessalov A.V., Kovalchuk, L.V.Supersingular Twisted Edwards Curves over Prime Fields.* II. Supersingular Twisted Edwards Curves with the j-Invariant Equal to 66^3 // Cybernetics and Systems Analysist. 2019. 55(5). P. 731–741.

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

16. H. Onuki, Y. Aikawa, T. Yamazaki, T. Takagi. A Faster Constant-time Algorithm of CSIDH keeping Two Points. ASIACRYPT, 2020.

17. A. Jalali, R. Azarderakhsh, M. M. Kermani, D. Jao. Towards optimized and constant-time CSIDH on embedded devices // IACR Cryptology ePrint Archive 2019/297; https://eprint.iacr.org/2019/297. (to apper at COSADE 2019).

Поступила в редколлегию 01.11.2021

Сведения об авторах:

Бессалов Анатолий Владимирович – д-р техн. наук, профессор, Киевский университет имени Бориса Гринченко, профессор кафедры информационной и кибернетической безопасности, факультет информационных технологий и управления, Украина; email: bessalov@ukr.net; ORCID: https://orcid.org/0000-0002-6967-5001

Цыганкова Оксана Валентиновна – канд. техн. наук, Національний Технічний Університет України «Київський Політехнічний Інститут», Фізико-технічний Інститут, старший преподаватель кафедры математических методов защиты информации, Украина; email: oksana.valent@gmail.com

Абрамов Сергей Вадимович – Киевский университет имени Бориса Гринченко, аспирант кафедры информационной и кибернетической безопасности, факультет информационных технологий и управления, Украина; ORCID: https://orcid.org/0000-0002-5145-2782