Протокол выработки общего ключа на основе аппарата изогений суперсингулярных эллиптических кривых (проект)

С. Гребнев[1], П. Ключарёв[2], А. Коренева[3], Д. Кошелев[4], О. Тараскин[5], А. Тулебаев[3]

[1]QAPP

[2]МГТУ им. Н.Э. Баумана

[3]Код безопасности

[4]ИнфоТеКС

[5]Waves

Москва, 2020

Содержание

Введение

В настоящем отчете излагаются результаты исследований возможностей создания протокола выработки общего ключа на основе механизма изогений суперсингулярных эллиптических кривых.

Дадим краткую характеристику предлагаемой схемы.

- Схема – типа SIDH [8].
- Только эфемерные ключи.
- Три уровня квантовой стойкости — 80, 128 и 256 битов
- Стартовая кривая специального вида E_{19}.
- Представление кривых в форме Монтгомери.
- Отказ от компрессии открытых ключей в пользу быстродействия.

1. Основные определения

В данном разделе кратко приводятся основные сведения о математическом аппарате изогений эллиптических кривых, более подробно см. монографии [18, 21].

1.1. Базовые определения

Рассмотрим эллиптическую кривую над полем K, $\mathrm{char}\, K \neq 2,3$, заданную в *краткой форме Вейерштрасса*: $E_{a,b}(K) : y^2 = x^3 + ax + b$.

Определение 1. *Кольцо регулярных функций* на кривой: факторкольцо

$$\overline{K}[E_{a,b}] = \overline{K}[x,y]/(y^2 - x^3 - ax - b).$$

Так как $(y^2 - x^3 - ax - b)$ неприводим, то в кольце регулярных функций нет делителей нуля. Его поле частных $\overline{K}_{a,b}(x,y)$ – *поле рациональных функций* на $E_{a,b}$.

Определение 2. Пусть $E_{a,b}, E_{a_1,b_1}$ – эллиптические кривые над K. *Рациональное отображение* (*морфизм*) $E_{a,b}$ в E_{a_1,b_1} – отображение вида

$$\psi = \psi(x,y) = (f_1(x,y), f_2(x,y)),$$

где $f_1(x,y), f_2(x,y) \in \overline{K}(E_{a,b})$, такое, что для любой точки $(x_0,y_0) \in E_{a,b}$ такой, где функции определены, верно $(f_1(x_0,y_0), f_2(x_0,y_0)) \in E_{a_1,b_1}$.

Определение 3. Если ψ – рациональное отображение и $\psi(\mathscr{O}) = \mathscr{O}_1$, то ψ – *изогения*. Если такое отображение существует, то соответствующие кривые называются *изогенными*.

Теорема 1. *(Тэйт). Две кривые над конечным полем K изогенны тогда и только тогда, когда порядки их групп равны.*

Согласно [21, 2.9], рациональное отображение $\psi(x,y)$, $\psi : E_{a,b} \to E_{a_1,b_1}$ может быть записано в канонической форме $\psi(x,y) = (r_1(x), yr_2(x))$, где r_1, r_2 – рациональные функции. Под *степенью* изогении будем понимать степень r_1 как рациональной функции. Изогении степени l будем также называть l-изогениями.

Определение 4. Изогения называется *сепарабельной*, если $r_1'(x) \neq 0$.

Далее рассматриваются только сепарабельные изогении.

Известно, что для любой изогении $\psi : E \to E'$ существует единственная *дуальная* изогения $\hat{\psi} : E' \to E$ такая, что $\hat{\psi} \circ \psi = [m]_E$ и $\psi \circ \hat{\psi} = [m]_{E'}$, где m – степень изогении.

Если рассмотреть три эллиптические кривые E, E', E'' и изогении ϕ, ψ: $\phi : E \mapsto E'$, $\psi : E' \mapsto E''$, то определены *композиции* изогений $\psi \circ \phi : E \mapsto E''$, и $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$, а также $\deg \psi \circ \phi = \deg \psi \deg \phi$.

С практической точки зрения под изогенией φ достаточно понимать пару рациональных функций

$$\frac{N(x)}{D(x)} = \frac{x^n + \cdots + n_1 x + n_0}{x^{n-1} + \cdots + d_1 x + d_0},$$

где $D(x)$ обращается в 0 на ядре изогении $\ker(\varphi)$.

Определение 5. *Графом изогений* называется граф, множеством вершин которого является множество классов изоморфизма эллиптических кривых. Две различных вершины этого графа соединены ребром тогда и только тогда, когда представители соответствующих классов изоморфизма изогенны.

1.2. Суперсингулярные эллиптические кривые

Определение 6. Морфизм эллиптической кривой в себя – *эндоморфизм*. Эндоморфизмы эллиптической кривой $E(K)$, определенной над полем K, образуют кольцо относительно операций сложения (поточечного) и композиции, оно обозначается $End(E)$.

Пример 1. 1. $E(_{a,b}(GF(p))$, *эндоморфизм Фробениуса*: $(x,y) \mapsto (x^p, y^p)$

2. $E_{a,b}(K)$, $P = (x,y) \mapsto -P = (x,-y)$ – эндоморфизм

3. $E_{a,b} \to E_{a,b}, P \mapsto mP$ – изогения (и эндоморфизм), обозначается $[m]$.

Пусть $K = GF(q)$, $\mathrm{char}(K) = p$. Для $m \in \mathbb{N}$ обозначим $E_{a,b}[m]$ множество точек $(x,y) \in E_{a,b}(\overline{K})$ таких, что $mP = \mathcal{O}$ – *группу кручения* кривой $E_{a,b}$.

Теорема 2. *1. Если $(m,p) = 1$, то $E_{a,b}[m]$ изоморфна $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*

2. Группа $E_{a,b}[p^e]$ либо равна $\{\mathcal{O}\}$ для всех $e = 1,2,\ldots$, либо для всех e изоморфна $\mathbb{Z}/p^e\mathbb{Z}$.

Определение 7. В случае, если группа $E_{a,b}[p^e]$ равна $\{\mathcal{O}\}$ для всех $e = 1,2,\ldots$, кривая называется *суперсингулярной*.

Определение 8. Если кольцо эндоморфизмов $End(E)$, рассматриваемое как $\mathbb{Z}$-модуль, имеет ранг 4, то кривая $E(K)$ называется *суперсингулярной*.

Для случая $GF(p)$ суперсингулярные кривые определяются условием $\#E = p+1$.

Все суперсингулярные кривые определены над $GF(p^2)$, их количество приблизительно равно $p/12$.

Граф l-изогений при простом $l \neq p$ между суперсингулярными эллиптическими кривыми обладает следующими свойствами [16, 17]:

- он $(l+1)$-регулярный;
- содержит единственную связную компоненту, состоящую из всех суперсингулярных эллиптических кривых;
- экспандер (конечный ненаправленный мультиграф, в котором любое подмножество вершин, не являясь «слишком большим», имеет «сильную» связность).

1.3. Вычисление изогений

Для построения изогений заданной степени можно воспользоваться формулами Велю [20].

Итак, пусть имеется эллиптическая кривая $E_{a,b}(K)$, заданная в форме Вейерштрасса ($y^2 = x^3 + ax + b$) над полем K характеристики, отличной от 2 и 3. Пусть F – подгруппа $E_{a,b}(K)$ порядка l. Тогда изогения с ядром F строится по следующему алгоритму.

1. Разобьем $F \setminus \{\mathscr{O}\}$ на три непересекающихся множества, $F = F_2 \cup R_+ \cup R_-$, где F_2 – множество точек четного порядка, а R_+ и R_- – разбиение множества точек нечетного порядка так, что $R \in R_+$ тогда и только тогда, когда $-R \in R_-$.
2. Определим множество S: $S = F_2 \cup R_+$.
3. Для каждой точки $Q \in S$ будем вычислять
$$g_Q^x = 3x^2 x_Q + a, g_Q^y = -2y_Q$$
(здесь (x_Q, y_Q) – координаты точки Q); если $Q = -Q$, то $v_Q = g_Q^x$, иначе $v_Q = 2g_Q^x$;
$$u_Q = (g_Q^x)^2$$
4. Вычислим
$$v = \sum_{Q \in S} v_Q;$$

$$w = \sum_{Q \in S} (u_Q + x_Q v_Q).$$

5. Коэффициенты изогенной кривой определяются как

$$a' = a - 5v;$$

$$b' = b - 7w.$$

6. Формулы преобразования координат $(x, y) \mapsto (x', y')$ имеют вид

$$x' = x + \sum_{Q \in S} \left(\frac{v_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right),$$

$$y' = y + \sum_{Q \in S} \left(u_Q \frac{2y}{(x - x_Q)^3} + v_Q \frac{y - y_Q}{(x - x_Q)^2} - \frac{g_Q^x g_Q^y}{(x - x_Q)^2} \right).$$

Трудоемкость алгоритма Велю пропорциональна степени изогении l.

Для случая подгруппы F, имеющей порядок l^e, можно вычислить соответствующую изогению как композицию e изогений степени l: пусть $F = \langle G \rangle$, тогда $\varphi = \varphi_{l-1} \circ \varphi_{l-2} \circ \cdots \circ \varphi_0$,

$$\varphi_0 : E \to E_1 = E / \left\langle l^{e-1} G \right\rangle, G_1 = \varphi_0(G);$$

$$\varphi_i : E_i \to E_{i+1} = E_i / \left\langle l^{e-i-1} G_i \right\rangle, G_{i+1} = \varphi_i(G_i).$$

Учитывая сказанное, приведем формулы Велю для случаев $l = 2, 3$.

Случай $l = 2$

Пусть $P = (X_P, y_P)$ – точка порядка 2 на $E_{a,b}(GF(p^2))$. Положим $v = 3X_P^2 + a$, $a' = a - 5v$, $b' = b - 7vX_P$; тогда $E_{a',b'}(GF(p^2)) : Y^2 = X^3 + a'X + b'$ – 2-изогенная $E_{a,b}$ кривая, и отображение

$$(x, y) \mapsto \left(\frac{v}{x - X_P} + X_P, Y - \frac{vY}{(X - X_P)^2} \right)$$

задает 2-изогению из $E_{a,b}$ в $E_{a',b'}$ с ядром $\langle P \rangle$.

Случай $l = 3$

Пусть $P = (X_P, y_P)$ – точка порядка 3 на $E_{a,b}(GF(p^2))$. Положим $v = 3X_P^2 + a$, $u = 4Y_P^3$, $a' = a - 5v$, $b' = b - 7(u + vX_P)$; тогда $E_{a',b'}(GF(p^2)) : Y^2 = X^3 + a'X + b'$ – 3-изогенная $E_{a,b}$ кривая, и отображение

$$(x,y) \mapsto \left(\frac{v}{x - X_P} + \frac{u}{(X - X_P)^2} + X_P, Y\left(1 - \frac{v}{(X - X_P)^2} + \frac{2u}{(X - X_P)^3}\right)\right)$$

задает 3-изогению из $E_{a,b}$ в $E_{a',b'}$ с ядром $\langle P \rangle$.

1.4. Изогении между суперсингулярными кривыми

Напомним, что у двух изоморфных кривых одинаковый j-инвариант. Из-за того, что построение изоморфизма между кривыми особой сложности не представляет, задача изогений по сути является задачей про нахождение изогений между различными классами изоморфных кривых (а каждый из этих классов можно представить соответствующим j-инвариантом).

1.5. Кривые Монтгомери

Математический аппарат эллиптических кривых в форме Монтгомери [14] показал себя наиболее эффективным при реализации схем, основанных на изогениях, поэтому в настоящем разделе мы кратко напомним некоторые их свойства.

Кривая Монтгомери задается уравнением

$$M_{A,B}(GF(p)) : By^2 = x^3 + Ax^2 + x, \text{ где } A, B \in GF(p), B(A^2 - 4) \neq 0. \tag{1}$$

Выполним замену координат $(x,y) \mapsto \left(\frac{x}{B} + \frac{A}{3B}, \frac{y}{B}\right)$, положим $a = 1/B^2 - A^2/(3B^2)$, $b = -A^3/(27B^3) - aA/(3B)$ – получим преобразование к краткой форме Вейерштрасса $E_{a,b}$.

Теорема 3. *Эллиптическая кривая, заданная в краткой форме Вейерштрасса $E_{a,b}$, может быть преобразована в форму Монтгомери тогда и только тогда, когда многочлен $x^3 + ax + b$ имеет корень α в $GF(p)$ и $(3\alpha^2 + a)$ есть квадратичный вычет $mod p$.*

Если условия этой теоремы выполнены, то положим $A = 3\alpha s$, $B = s$, где s – квадратный корень из $(3\alpha^2 + a)^{-1}$, и определим замену координат по формуле $(x, y) \mapsto (x/s + \alpha, y/s)$.

На таких кривых точка $(0, 0)$ имеет порядок 2, и $\#M_{A,B}$ делится на 4.

j-инвариант кривой Монтгомери вычисляется по формуле

$$j(M_{A,B}) = \frac{256(A^2-3)^3}{A^2-4}. \tag{2}$$

Операции на кривых Монтгомери задаются следующими формулами:

$$(x_1, y_1) + (x_2, y_2) = \left(B\frac{(y_2-y_1)^2}{(x_2-x_1)^2} - A - x_1 - x_2, \frac{(2x_1+x_2+A)(y_2-y_1)}{(x_2-x_1)} - B\frac{(y_2-y_1)^3}{(x_2-x_1)^3 - y_1)} \right)$$

при $(x_1, y_1) \neq (x_2, -y_2)$;

$$[2](x_1, y_1) = \left(\frac{(x_1^2-1)^2}{4x_1(x_1^2+Ax_1+1)}, y_1\frac{(x_1^2-1)(x_1^4+2Ax_1^3+6x_1^2+2Ax_1+1)}{8x_1^2(x_1^2+Ax_1+1)^2} \right);$$

$$[3](x_1, y_1) = \left(\frac{(x_1^4-4Ax_1-6x_1^2-3)^2 x_1}{(3x_1^4+4Ax_1^3+6x_1^2-1)^2}, \right.$$
$$\left. y_1\frac{(x_1^4-4Ax_1-6x_1^2-3)(x_1^8+4Ax_1^7+28x_1^6+28x_1^5+(16A^2+6)x_1^4+28Ax_1^3+28x_1^2+4AX_1+1))}{(4Ax_1^3+3x_1^4+6x_1^2-1)^3} \right)$$

Точка (x, y) на кривой Монтгомери (1) представляется в *проективных координатах* в виде пары $(X : Z)$ такой, что $x = X/Z$. Подобное представление позволяет использовать эффективные алгоритмы сложения и удвоения [1, 14], вычисляющие только X-координату точки, что в ряде случаев является достаточным.

Пусть $m > n > 0$, $P = (X_1 : Y_1 : Z_1) \in M_{A,b}$, известны кратные точки $P_n = [n]P$, $P_m = [m]P$, $P_{m-n} = [(m-n)]P$. Тогда имеют место формулы

$$X_{m+n} = Z_{m-n}((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n))^2$$
$$Z_{m+n} = X_{m-n}((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n))^2$$

$$4X_nZ_n = (X_n + Z_n)^2 - (X_n - Z_n)^2$$
$$X_{2n} = (X_n + Z_n)^2(X_n - Z_n)^2$$
$$Z_{2n} = 4X_nZ_n((X_n - Z_n)^2 + ((A+2)/4)(4X_nZ_n))$$

1.6. Вычисление изогений на кривых Монтгомери

TODO!!!

1.7. Арифметика в $GF(p^2)$

Пусть $p \equiv 3 \pmod 4$, тогда $GF(p^2) = GF(p)(\iota)$, где $\iota^2 + 1 = 0$. Элементы поля представляются в виде $u = u_0 + u_1 \cdot \iota$, $u_0, u_1 \in GF(p)$. Операции в поле $GF(p^2)$ задаются естественным образом.

- Сложение: $u + v = (u_0 + v_0) + (u_1 + v_1) \cdot \iota$.
- Аддитивная инверсия: $-u = -u_0 + (-u_1) \cdot \iota$
- Умножение: $uv = (u_0 v_0 - u_1 v_1) + (u_0 v_1 + u_1 v_0) \cdot \iota$.
- Мультипликативная инверсия: $u^{-1} = (u_0)(u_0^2 + u_1^2)^{-1} + (-u_1)(u_0^2 + u_1^2)^{-1} \cdot \iota$.

2. Протокол выработки общего ключа

В протоколе принимают участие два абонента: *инициатор A* и *ответчик B*.

Параметры протокола

Параметрами протокола являются:

- простое число p вида $p = l_A^{e_A} l_B^{e_B} \cdot f - 1$, где l_A, l_B – маленькие простые (например, 2 и 3), $(l_A, f) = (l_B, f) = 1$;
- поле $GF(p^2)$;
- суперсингулярная кривая $E_0(GF(p^2))$, мощность группы точек которой равна $(l_A^{e_A} l_B^{e_B} \cdot f)^2$ (*стартовая кривая*). По построению (см. [8]), $E[l_A^{e_A}]$ содержит $l_A^{e_A - 1}(l_A + 1)$ циклических подгрупп порядка $l_A^{e_A}$, каждая из которых определяет собственную изогению (т.е. ядром которой она является), аналогичное замечание верно и для $E[l_B^{e_B}]$.

В основе протокола лежит следующая коммутативная диаграмма:

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E/\langle P\rangle \\ \psi\Big\downarrow & & \Big\downarrow \\ E/\langle Q\rangle & \longrightarrow & E/\langle P,Q\rangle \end{array} \tag{3}$$

где φ,ψ – случайные пути в графах изогений степеней l_A, l_B соответственно. Протокол представляет собой вариант схемы Диффи-Хеллмана, реализованный над диаграммой (3). Идея его состоит в том, чтобы абонент A выбирал φ, а B выбрал ψ. Стойкость протокола основана на сложности нахождения пути, соединяющего две вершины в графе.

Протокол выработки общего ключа

Фиксируем открытые параметры протокола:

- простое число $p = l_A^{e_A} l_B^{e_B} \cdot f - 1$, где l_A, l_B – маленькие простые (например, 2 и 3), $(l_A, f) = (l_B, f) = 1$;
- стартовую кривую $E_0(GF(p^2))$;
- базисы $\{P_A, Q_A\}$ и $\{P_B, Q_B\}$, которые порождают, соответственно, $E_0[l_A^{e_A}]$ и $E_0[l_B^{e_B}]$, т.е. $\langle P_A, Q_A\rangle = E_0[l_A^{e_A}]$ и $\langle P_B, Q_B\rangle = E_0[l_B^{e_B}]$.

Абонент A выбирает случайный элемент $n_A \in_R \mathbb{Z}/l_A^{e_A}\mathbb{Z}$ и строит изогению $\varphi_A : E_0 \to E_A$ с ядром $K_A := \langle P_A + [n_A]Q_A\rangle$. Абонент A также вычисляет образ $\{\varphi_A(P_B), \varphi_A(Q_B)\}$ и посылает эти точки абоненту B вместе с эллиптической кривой E_A (т.е. ее описанием).

Аналогично, абонент B выбирает случайный элемент $n_B \in_R \mathbb{Z}/l_B^{e_B}\mathbb{Z}$ и строит изогению $\varphi_B : E_0 \to E_B$ с ядром $K_B := \langle P_B + [n_B]Q_B\rangle$. Абонент B также вычисляет образ $\{\varphi_B(P_A), \varphi_B(Q_A)\}$ и посылает эти точки абоненту A вместе с эллиптической кривой E_B (т.е. ее описанием).

Получив от абонента B набор $E_B, \varphi_B(P_A), \varphi_B(Q_A)$, абонент A строит изогению $\varphi_A' : E_B \to E_{AB}$ с ядром $\langle\varphi_B(P_A) + [n_A]\varphi_B(Q_A)\rangle$; абонент b выполняет аналогичные действия. В качестве общего ключа используется j-инвариант кривой

$$E_{AB} = \varphi_B'(\varphi_A(E_0)) = \varphi_A'(\varphi_B(E_0)) = E_0/\langle P_A + [n_A]Q_A, P_B + [n_B]Q_B\rangle .$$

3. Анализ стойкости

В рамках этого раздела считаем, что $p = l_A^{e_A} \cdot l_B^{e_B} \cdot f - 1$ – сбалансированное простое (т.е. $l_A^{e_A} \approx l_B^{e_B} \approx p^{1/2}$), $E_0(GF(p^2))$ – суперсингулярная эллиптическая кривая, базисы $\{P_A, Q_A\}$ и $\{P_B, Q_B\}$ порождают, соответственно, $E_0[l_A^{e_A}]$ и $E_0[l_B^{e_B}]$, т.е. $\langle P_A, Q_A \rangle = E_0[l_A^{e_A}]$ и $\langle P_B, Q_B \rangle = E_0[l_B^{e_B}]$.

Иногда, для краткости, мы будем опускать индексы A, b и использовать обозначения l^e.

3.1. Формальный анализ

Основная вычислительная задача, на предположение о сложности которой опирается стойкость предлагаемого протокола, состоит в следующем [8].

Задача 1. *Вычислительная задача суперсингулярных изогений, Computational Supersingular Isogeny — CSSI*: пусть $\phi_1 : E_0 \to E_1$ – изогения с ядром $R_1 + [n]S_1$, где n выбрано случайно равновероятно из $\mathbb{Z}/l^e\mathbb{Z}$. По E_1 и значениям образов $\phi_1(R_2), \phi_1(S_2)$ найти порождающий элемент группы $\langle R_1 + [n]S_1 \rangle$.

Можно сформулировать и аналог вычислительной задачи Диффи–Хеллмана для изогений суперсингулярных эллиптических кривых.

Задача 2. *Вычислительная задача Диффи–Хеллмана для суперсингулярных изогений, Supersingular Computational Diffie–Hellman — SSCDH*: пусть $\phi_A : E_0 \to E_A$ – изогения с ядром $\langle P_A + [n_A]Q_A \rangle$, где n_A выбрано случайно равновероятно из $\mathbb{Z}/l_A^{e_A}\mathbb{Z}$, и пусть $\phi_B : E_0 \to E_B$ – изогения с ядром $\langle P_B + [n_B]Q_B \rangle$, где n_B выбрано случайно равновероятно из $\mathbb{Z}/l_B^{e_B}\mathbb{Z}$, По E_A, E_B и значениям образов $\phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A)$ найти порождающий элемент группы $\langle P_A + [n_A]Q_A, P_B + [n_B]Q_B \rangle$.

Далее, сформулируем аналог распознавательного варианта задачи Диффи–Хеллмана:

Задача 3. *Распознавательная задача суперсингулярных изогений, Supersingular Decisonal Diffie–Hellman — SSDDH*: пусть задан набор , выбранный с вероятностью $1/2$ из одного из следующих распределений

- $(E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A), E_{AB})$, где $(E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A))$ – как в предыдущем определении,

$$E_{AB} \cong E_0 / \langle P_A + [n]Q_A, P_B + [n]Q_B \rangle ;$$

- $(E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A), E_C)$, где $(E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A))$ – как в предыдущем определении,

$$E_C \cong E_0 / \left\langle P_A + [n']Q_A, P_B + [n']Q_B \right\rangle$$

  где n' выбрано случайно из $\mathbb{Z}/l_B^{e_B}\mathbb{Z}$);

определить, из какого распределения выбран указанный набор.

Редукция задачи SSCDH к SSCI очевидна, в обратном направлении – неизвестна, как и в случае с задачей Диффи–Хеллмана и дискретного логарифмирования в абелевой группе.

Далее, напомним, следуя [8], основные положения модели Канетти–Кравчика из [5].

Рассмотрим конечное множество абонентов $P_1, \ldots, P_n$, моделируемых вероятностными алгоритмами. Противник $\mathscr{I}$, который также моделируется вероятностным алгоритмом, контролирует все коммуникации между абонентами (с тем исключением, что противник не может вставлять или модифицировать сообщения – кроме сообщений от нечестных абонентов). Любое сообщение может быть доставлено лишь один раз. Абоненты передают исходящие сообщения противнику, который контролирует их доставку, через запрос `Send`. Абоненты активируются запросом `Send`, и таким образом противник контролирует создание сеансов протокола. Два сеанса s и s' являются *соответствующими (matching)*, если исходящие сообщения одного сеанса являются входящими для другого, и наоборот.

Противник получает доступ к запросам $\mathtt{SessionStateReveal}$, $\mathtt{SessionKeyReveal}$, $\mathtt{Corrupt}$.

Запрос $\mathtt{SessionStateReveal}(\mathfrak{s})$ позволяет противнику получить состояние текущего сеанса $\mathfrak{s}$, в том числе любую секретную информацию. Запрос фиксируется, и сеанс не выдает выходной информации.

Запрос $\mathtt{SessionKeyReveal}(\mathfrak{s})$ выдает противнику сеансовый ключ для заданного сеанса $\mathfrak{s}$.

Запрос $\mathtt{Corrupt}(P_i)$ передает противнику контроль над абонентом P_i, в том числе всю информацию в памяти абонента, включая сохраненные сеансовые ключи и другую информацию о сеансах. Захваченный абонент не производит более выходной информации.

Назовем сеанс $\mathfrak{s}$ с владельцем P_i *локально раскрытым*, если противник выполнил один из запросов $\mathtt{SessionStateReveal}(\mathfrak{s})$, $\mathtt{SessionKeyReveal}(\mathfrak{s})$, $\mathtt{Corrupt}(P_i)$, до того, как сеанс завершился. Скажем, что сеанс *раскрыт*, если локально раскрыт сеанс или соответствующий ему, иначе назовем сеанс *свежим*.

Далее, противнику $\mathscr{I}$ разрешается единственный запрос $\mathtt{Test}(\mathfrak{s})$, который может быть применен на любом этапе к завершенному свежему сеансу $\mathfrak{s}$. Выбирается случайный бит b. Если $b = 0$, то оракул раскрывает сеансовый ключ, иначе, если $b = 1$, оракул вырабатывает случайное значение из пространства сеансовых ключей. Затем противник может выполнять любые запросы, за исключением того, что он не может пытаться раскрыть тестовый сеанс $\mathfrak{s}$. В любой момент противник может попытаться угадать b. Обозначим $\mathrm{GoodGuess}^{\mathscr{I}}(k)$ событие, состоящее в том, что $\mathscr{I}$ угадал b, и определим *преимущество*

$$\mathrm{Adv}^{\mathscr{I}}(k) = \max\left\{0, \left|\Pr[\mathrm{GoodGuess}^{\mathscr{I}}(k)] - \frac{1}{2}\right|\right\},$$

где k – параметр стойкости.

Определение 9. Протокол выработки общего ключа Π с параметром стойкости k является стойким относительно задачи определения сеансового ключа в модели Канетти–Кравчика, если выполнено следующее:

1. если два честных абонента завершили совпадающие сеансы, то соответствующие сеансовые ключи совпадают;
2. $\mathrm{Adv}^{\mathscr{I}}(k)$ – пренебрежимо малая величина.

Теорема 4. *В предположении о сложности задачи SSDDH, протокол из раздела 2 является стойким относительно задачи определения сеансового ключа в модели Канетти–Кравчика.*

Доказательство. Поскольку наш протокол является вариантом протокола из [8], то доказательство в точности повторяет рассуждения из [8, Theorem 6.1]. Для полноты изложения приведем эти рассуждения.

Два честных абонента в совпадающих сеансах вырабатывают одинаковый общий ключ, поэтому первая часть Определения 9 выполнена.

Для доказательства второй части предположим, что существует полиномиальный противник $\mathscr{I}$ с преимуществом ε, не являющимся пренебрежимо малой величиной. Тогда Алгоритм 1 является полиномиальным различителем для задачи SSDDH.

Algorithm 1 Различитель для SSDDH

Require: $E_A, E_B, \phi_A(P_B), \phi_A Q_B, \phi_B(P_A), \phi_B(Q_A)$

Ensure: d

$r \xleftarrow{R} \{1, \ldots, k\}$, где k – максимальное количество активируемых $\mathscr{I}$ сеансов

Вызвать $\mathscr{I}$ и симулировать протокол для $\mathscr{I}$б за исключением r-го активированного сеанса

Для r-го сеанса: A отправляет $A, i, E_A, \phi_A(P_B), \phi_A(Q_B)$, а B отправляет $B, i, E_B, \phi_B(P_A), \phi_A(P_B)$, где i – идентификатор сеанса

if r-й сеанс выбран $\mathscr{I}$ в качестве тестового сеанса **then**

    Установить $\mathscr{I}$ как ответ на тестовый запрос

    $d \leftarrow$ вывод $\mathscr{I}$

else

    $d \xleftarrow{R} \{0, 1\}$

end if

return d

Полиномиальность алгоритма очевидна, осталось доказать, что он имеет преимущество, не являющееся пренебрежимо малой величиной. Если r-й сеанс не является тестовым, то Алгоритм 1 выдает случайный бит и, таким образом, его преимущество равно 0. Иначе, $\mathscr{I}$ успешно завершится с вероятностью ε, поскольку симулированный протокол для $\mathscr{I}$ неотличим от действительного. Последний случай имеет место с вероятностью $1/k$, следовательно, преимущество различителя для задачи SSDDH равно ε/k, что не является пренебрежимо малой величиной. □

3.2. Практический анализ

Дадим несколько упрощенную формулировку SSCI, достаточную для наших целей. Итак, пусть задана (секретная) l^e-изогения $\phi : E_0 \to E/\langle G\rangle$. По кривой $E/\langle G\rangle$ и образам $\varphi(P), \varphi(Q)$ найти порождающий элемент подгруппы G или, что эквивалентно, изогению $\phi : E \to E/G$).

Тотальный перебор

Поскольку у любой суперсингулярной кривой $E(GF(p^2))$ имеется $(l+1)l^{e-1}$ циклических подгрупп порядка l^e, то тотальный перебор требует $O(l^e)$ или $O(p^{1/2})$ опробований.

Метод “встречи посередине”

Пусть для простоты e четное.

Построим два дерева таких, что листья первого определяют классы изоморфизмов кривых, $l^{e/2}$-изогенных E; листья второго – классы изоморфизмов кривых, $l^{e/2}$-изогенных E/G.

В каждом наборе по $(l+1)l^{e/2-1}$ классов; с большой вероятностью единственный класс, заданный представителями E' и E'' из первого и второго наборов соответственно, содержится в их пересечении. Найдя его, строим ϕ как композицию изогении из $\phi_1 : E \to E'$, изоморфизма $\psi : E' \to E''$ и двойственной к изогении из E/G: $\phi_2 : E/\langle G\rangle \to E''$.

Требуемый объем памяти — $O(p^{1/4})$ ячеек, время — $O(p^{1/4})$ операций.

Квантовый вычислитель

Claw-finding алгоритм из [19] для заданных функций $g_1 : X_1 \to Y$, $g_2 : X_2 \to Y$ определяет такие $(x_1, x_2) \in X_1 \times X_2$: $g_1(x_1) = g_2(x_2)$.

Пусть при этом $\#X_1 \approx \#X_2 \approx N$, $\#Y \gg N$, тогда время работы составляет $O(N^{2/3})$ операций при требованиях к памяти $O(N^{2/3})$.

В нашем случае X_1 – множество $l^{e/2}$-изогений из $E = E_1$; X_2 – множество $l^{e/2}$-изогений из $E/G = E_2$, $g_i(\phi) = j(\phi(E_i))$. Имеем $\#X_1 = \#X_2 \approx p^{1/4}$, отсюда время – $O(p^{1/6})$ (и память $O(p^{1/6})$).

Метод Гровера, примененный к задаче CSSI в [11], требует $O(p^{1/4})$ операций, необходимая память – $O(1)$.

В работе [11] проведен сравнительный анализ квантовых алгоритмов, из которого следует, что в реалистичной модели квантового вычислителя (с ограниченным объемом памяти, не превосходящим 2^{64} ячеек) метод Гровера является более эффективным.

Параллельный поиск коллизий

Параллельный метод поиска коллизий (метод Винера–ван Ооршота) из [15] эффективно применяется к задаче CSSI в [3, 7], коэффициент распараллеливания при этом близок к 100%.

Наиболее эффективные методы поиска коллизий псевдослучайной функции f являются итерационными в том смысле, что они основаны на вычислении последовательностей вида $x_i = f(x_{i-1})$, $i \in \mathbb{N}$, откуда следует, что функция f должна быть такой, что множество ее значений содержится в множестве, на котором она определена.

Идея метода состоит в том, что каждый процессор вырабатывает свою последовательность $x_i = f(x_{i-1})$ до появления *выделенной точки* x_d, удовлетворяющей некоторому легко проверяемому условию (например, фиксированное число нулевых старших битов), x_d записывается в общую для всех процессоров память по адресу, вычисляемому как некоторая взаимно однозначная функция точки, и начинает выработку новой последовательности.

Если одна и та же выделенная точка встречается дважды – найдена коллизия f. Каждый процессор вместе с последовательностью x_i вычисляет значения $(x^{(i)}, y^{(i)})$ и сохраняет их для каждой выделенной точки, совпадение выделенных точек x^d и $x'_{d'}$, означает, что $((x^{(d)}, y^{(d)}), (x^{(d')}, y(d')))$ – коллизия.

Среднее время работы алгоритма приближенно равно

$$\left(\sqrt{\frac{\pi\#S}{2p}}/m + \frac{\alpha}{\theta}\right)t,$$

где

- f – случайное отображение,
- p – вероятность того, что случайно выбранная коллизия f является *полезной*,
- θ – доля выделенных точек в множестве S,
- t – время одной итерации.

Пусть $S = \{0,1\} \times \{0,\ldots,(l+1)l^{e/2-1} - 1\}$, $E_0 = E$, $E_1 = E/G$. Каждая пара $(i,y) \in S$ задает подгруппу эллиптической кривой E_i.

Пример 2. Для $l = 2$ в [3] соответствие задается между парами $(i,y) = (i,(b,k)) \in \{0,1\} \times \{0,1,2\} \times \{0,\ldots,l^{e/2-1} - 1\}$ и циклическими подгруппами $\langle R_i \rangle \subset E_i$, где

$$R_i = \begin{cases} P_i + [b2^{e/2-1}k, & \text{если } b = 0,1 \\ [2k]P_i + Q_i, & \text{если } b = 2, \end{cases}$$

где $\langle P_i, Q_i \rangle = E_i[2^{2/2-1}]$.

Пусть $h : S \to E_0(GF(p^2)) \cup E_1(GF(p^2))$, $h : (i,y) \mapsto R_i$, и пусть итерационная функция $f : S \to S$ – функция, которая по входной паре (i,y) вычисляет изогению степени $l^{e/2}$ с ядром $\langle R_i \rangle$, вычисляет j-инвариант $j(E_i/\langle R_i \rangle)$ и отображает его в S при помощи некоторой псевдослучайной функции $g : GF(p^2) \to S$.

Существует единственная полезная коллизия для f, которая и решает задачу CSSI.

Таким образом, итоговые оценки трудоемкости параллельного метода поиска коллизий применительно к задаче CSSI:

$$T = \frac{2.5}{m}\sqrt{|S|^3/w} \cdot t; \tag{4}$$

m – количество процессоров, $|S|$ – мощность множества определения итерационной функции, w – объем памяти, t – трудоемкость итерационной функции.

В нашем случае $|S| \approx p^{1/2}$, и таким образом оценка стойкости составляет

$$O\left(\frac{p^{3/8}}{m\, w^{1/2}}\right) \tag{5}$$

операций вычисления итерационной функции (в нашем случае – вычисления l-изогении).

Несбалансированные делители и слабые стартовые кривые

В работе [12] предлагается атака на имплементации SIDH со специально подобранными параметрами, трудоемкость которой меньше, чем у рассмотренных методов. Для противодействия указанной атаке мы будем использовать хорошо сбалансированные простые p: $p = 2^{e_2}3^{e_3}f - 1$ так, что множители $2, 3$ сбалансированы: $e_2 \approx e_3 \cdot \log_2 3$, а множитель f – малое простое число, и стартовую кривую специального вида из [22].

Долговременные ключи

Отметим, что эффективная атака, предложенная в [9], позволяет определить долговременный ключ абонента за $O(\log p)$ сеансов, поэтому использование долговременных ключей, равно как и повторное использование эфемерных ключей, протоколом не допускается.

Выводы

Следуя рассуждениям работ [3, 11], можно заключить, что наилучший классический метод решения задачи CSSI — параллельный метод поиска коллизий, наилучший квантовый метод решения указанной задачи — метод Тани.

Соответственно, при расчете параметров мы будем ориентироваться на трудоемкость указанных методов.

4. Выбор параметров

Простое число p выбирается в виде $p = 2^{e_2}3^{e_3}f - 1$ так, что множители $2, 3$ сбалансированы: $e_2 \approx e_3 \cdot \log_2 3$, а множитель f – малое простое число. При этом для p требуется, чтобы $\left(\frac{-19}{p}\right) = -1$ (см. далее).

В соответствии с оценками раздела 3, предлагаются следующие наборы параметров.

Число	Формула	Классическая стойкость	Квантовая стойкость
p_{485}	$2^{242} \cdot 3^{152} \cdot 5 - 1$	173	80
p_{772}	$2^{386} \cdot 3^{242} \cdot 7 - 1$	281	128
p_{1532}	$2^{776} \cdot 3^{496} - 1$	566	255

Замечание 1. Классическая стойкость рассчитана по формуле (4) для параметров суперкомпьютера Fugaku, возглавляющего текущую редакцию списка Top500 [2] с $\approx 2^{23}$ вычислительными ядрами и $\approx 2^{49}$ ячеек памяти при $t = 2^{22}$.

Стартовая кривая протокола может фиксироваться, например, как $E_0(GF(p^2)) : y^2 = x^3 + x$. Однако мы предлагаем использовать кривую $E_{19}(GF(p))$:

$$E_{19} : y^2 = x^3 - 2^3 19x + 2 \cdot 19^2 \tag{6}$$

с j-инвариантом $-2^{15}3^3$. Ее выбор мотивирован в [22]. В частности, E_{19} не обладает эндоморфизмами степени 2 и 3, то есть петлями в графах 2- и 3-изогений. Также у нее отсутствуют кратные дуги в графах 2- и 3-изогений, в отличие от кривых, использованных в SIKE [10].

По теореме Дойринга (см., например, [4, Теорема 2.1]) для суперсингулярности кривой E_{19} необходимо и достаточно, чтобы $\left(\frac{-19}{p}\right) = -1$.

Эллиптические кривые задаются в форме Монтгомери (1).

Для построения базиса $\{P_A, Q_A\}$ будем действовать следующим образом. Будем перебирать случайные точки $P \in_R E_0$ и вычислять $P' = [(l_B^{e_B} \cdot f)^2]P$; с большой вероятностью это точка порядка $((l_A)^{e_A})^2$ (проверяем, умножая на степени l_A), и тогда $P_A = P'$. Аналогично вычислим Q_A порядка $((l_B)^{e_B})^2$.

Проверка независимости: *спаривание Вейля* $e(P_A, Q_A)$ в $E[l_A^{e_A}]$ должно иметь порядок $l_A^{e_A}$ (с большой вероятностью это так).

Аналогично выберем базис $\{P_B, Q_B\}$.

Замечание 2. Предполагается заменить данную процедуру на детерминированную, аналогично тому, как сделано в SIKE [10].

5. Реализация

TODO!!!

Заключение

Основные результаты работы подгруппы на данном этапе:

- предложен постквантовый протокол выработки общего ключа двумя абонентами на основе протокола SIDH;
- выбраны параметры протокола, в том числе, стартовая кривая, характеристики поля и т.д.
- разработан прототип программной реализации на языке Python с использованием библиотеки SAGE.

Основные задачи для дальнейшей работы:

- исследование криптографической стойкости протокола;
- разработка оптимизированной программной реализации протокола.

Список литературы

[1] Explicit-Formulas Database. XZ coordinates for Montgomery curves. http://hyperelliptic.org/EFD/g1p/auto-montgom-xz.html. — 2020.

[2] Supercomputer Fugaku. https://www.top500.org/system/179807/. — 2020.

[3] Adj G., Cervantes-Vázquez D., Chi-Domínguez J-J., Menezes A., Rodríguez-Henríquez F. On the cost of computing isogenies between supersingular elliptic curves. http://eprint.iacr.org/2018/313. — 2018.

[4] Bröker R. *Constructing supersingular elliptic curves*. // Journal of Combinatorics and Number Theory, 2009. Vol. 1(3). P. 269–273.

[5] Canetti R., Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels// EUROCRYPT 2001, LNCS 2045. — N. Y.: Springer-Verlag. — 2001. — P. 453–474.

[6] Costello C., Longa P., Naehrig M. Efficient algorithms for supersingular isogeny Diffie-Hellman. http://eprint.iacr.org/2016/413 (2016).

[7] Costello C., Longa P., Naehrig M., Renes J., Virdia F. Improved Classical Cryptanalysis of SIKE in Practice. http://eprint.iacr.org/2019/298 (2019).

[8] De Feo L., Jao D., Plût J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. // Journal of Math. Cryptology, 2014. Vol. 8(3). P. 209–247.

[9] Galbraith S., Petit C., Shani B., Yan Bo Ti. On the Security of Supersingular Isogeny Cryptosystems. — Cryptology ePrint Archive: Report 2016/859. — https://eprint.iacr.org/2016/859. — 2016.

[10] Jao D. et al. Supersingular Isogeny Key Encapsulation. https://sike.org — 2017.

[11] Jaques S., Schanck J.M. Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE.// Cryptology ePrint Archive: Report 2019/103. — https://eprint.iacr.org/2019/103. — 2019.

[12] Kutas P., Martindale C., Panny L., Petit C., Stange K.E. Weak instances of SIDH variants under improved torsion-point attacks. http://eprint.iacr.org/2020/633. — 2020.

[13] Miller V. The Weil Pairing, and Its Efficient Calculation. J. Cryptology. 17. 235-261. — 2004.

[14] Montgomery P. L. Speeding the Pollard and elliptic curve methods of factorization// Math. Comp. — 1987. — **48**. — pp. 243–264.

[15] van Oorschot P., Wiener M. Parallel Collision Search with Cryptanalytic Applications. J. Cryptology 12, 1–28 (1999).

[16] Pizer A. Ramanujan graphs and Hecke operators. Bull. Amer. Math. Soc. (N.S.), 23(1):127–137, 1990.

[17] Pizer A. Ramanujan graphs. In Computational perspectives on number theory (Chicago, IL, 1995), volume 7 of AMS/IP Stud. Adv. Math., pages 159–178. Amer. Math. Soc., Providence, RI, 1998.

[18] Silverman J.H. The Arithmetic of Elliptic Curves. — Springer:2009.

[19] Seiichiro Tani. Claw Finding Algorithms Using Quantum Walk. `http://arxiv.org/abs/0708.2584`. — 2008.

[20] Velú J. Isogénies entre courbes elliptiques, C.R. Acad. Sc. Paris, Serie A., 273, pp. 238–241 (1971).

[21] Washington L.C. Elliptic curves, number theory and cryptography: CRC. — 2008.

[22] Кошелев Д. *Стартовая суперсингулярная эллиптическая кривая для криптографии на изогениях*, `https://www.researchgate.net/profile/Dimitri_Koshelev`, 2020.

A. Контрольные примеры

TODO!!!