

Криптосистема на категории изогенных эллиптических кривых и квантовый компьютер

В основе большинства известных алгоритмов криптографии с открытым ключом лежит одна и та же математическая структура: конечные абелевы группы. На этой структуре основаны задача определения строения и порядка группы и задача вычисления индекса. Эти задачи оказываются уязвимыми по отношению к квантовому компьютеру. Предлагается новая структура: категория алгебраических групп, третий тип задачи: вычисление морфизма между алгебраическими группами и криптосистема, основанная на задаче вычисления изогении между парой эллиптических кривых. Данный тип криптосистем представляется более стойким по отношению к квантовому компьютеру, чем используемые ранее.

1. Математические задачи и квантовый компьютер

В основе безопасности криптосистем с открытым ключом лежат сложные математические задачи. Для построения криптосистем эти задачи должны позволять встраивать потайной ход: создать такую частную задачу и лазейку, что если эта лазейка известна, то задача может быть решена с полиномиальной сложностью, а если не известна, то сложность решения задачи сверхполиномиальная.

В настоящее время для построения обобщенных криптосистем с открытым ключом используются следующие классы унифицированных задач.

1. Задача об укладке ранца над суммируемым множеством.
2. Задача определения порядка и структуры конечной абелевой группы.
3. Задача определения индекса элемента конечной абелевой группы.

Примером этих задач являются соответственно задача об укладке ранца над \mathbf{Z} (криптосистема Шора — Ривеста [3]); задача определения структуры и порядка группы $(\mathbf{Z}/n\mathbf{Z})^*$, эквивалентная разложению составного числа n над \mathbf{Z} (криптосистемы RSA, Фиата — Шамира [6]); задача логарифмирования в мультипликативной группе конечного поля (криптосистемы Эль-Гамала [5], DSS [7], ГОСТ Р 34. 10–94). Некоторые криптосистемы основаны на смешанных классах задач. Например, криптосистема на группе классов числового поля [9] основана на обеих задачах пп. 2, 3.

Несмотря на NP-полноту задачи об укладке ранца, все ранцевые криптосистемы оказались нестойкими. Это обусловлено спецификой выбора подкласса задач об укладке ранца: для маскировки исходных элементов ранца используется ограниченный набор преобразований — перестановки и сложения.

Остальные унифицированные классы задач основаны на свойствах конечных абелевых групп. Отметим, что практически единственной зада-

чей определения порядка и структуры группы, которая позволяет встраивать потайной ход, является задача разложения составного числа. Сложность этой задачи в настоящее время составляет примерно $S = \exp(1,52\sqrt{\ln n(\ln \ln n)^2})$ по отношению к методу общего решета числового поля [2]. Неприятным фактом является и то, что сложность задачи разложения аномально быстро падает. Снижение сложности обусловлено развитием математических методов разложения.

Определим скорость s снижения стойкости по формуле

$$s(t) = \frac{\log S(T) - \log S(T + t)}{t \log S(T)},$$

где $S(T)$ — сложность задачи в момент времени T . Применительно к задаче вскрытия ключа шифра DES сложность за 15 лет снижалась со средней скоростью 0,023. Примерно так же снижалась стойкость и некоторых других симметричных шифров. Однако скорость снижения сложности задачи разложения значительно больше. Для числа длиной 1000 бит она составляет 0,05, а для числа длиной 2000 бит — 0,055. Учитывая то, что скорость снижения стойкости криптоалгоритмов в течение указанного срока была примерно постоянной, представляется обоснованной экстраполяция этой скорости на будущее. В этом случае легко заметить неперспективность использования задачи разложения. Те же наблюдения и рассуждения справедливы и для задачи дискретного логарифмирования в простом конечном поле.

Таким образом, подавляющее большинство оставшихся задач принадлежат третьему классу. Вид группы может быть существенно различен: мультипликативная группа конечного поля, группа классов числового поля, якобиан алгебраической кривой и т. п. Если порядок и структура группы могут быть вычислены, то наиболее сложной задачей в этом классе задач является задача вычисления индекса в циклической группе простого порядка, называемая задачей логарифмирования.

Для логарифмирования в циклической группе простого порядка r наилучшими являются алгоритм Полларда, обладающий сложностью $O(\sqrt{r})$ и не допускающий распараллеливания, и алгоритм встречи на случайном лесе [15], обладающий сложностью $O(\sqrt{r \log r})$ и допускающий распараллеливание. Такую оценку имеют задачи логарифмирования на эллиптической кривой и на якобиане алгебраической кривой невысокого рода. Сложность логарифмирования в мультипликативной группе конечного поля асимптотически равна сложности разложения.

В последние годы за рубежом ведутся бурные исследования в области квантовых компьютеров, финансируемые спецслужбами [9, 10]. Квантовый компьютер позволяет реализовать ряд операций, требующих экспоненциальных времени и памяти на обычном компьютере. В частности, за-

дачи разложения и логарифмирования на произвольной группе, а также задача об изоморфизме графов оказываются разрешимыми с полиномиальной сложностью [11].

Вывод информации в квантовом компьютере осуществляется с помощью квантовых преобразований Фурье или Адамара. По принципу работы квантовые компьютеры ориентированы на выявление скрытых периодов функций. Например, для решения задачи разложения нужно найти число x такое, что $a^x \equiv a \pmod{n}$. Тогда нетривиальный делитель числа n с

большой вероятностью имеет вид $\text{НОД}\left(a^{\frac{x-1}{2}} - 1, n\right)$. Наибольший общий

делитель вычисляется на обычном компьютере.

По состоянию на 1998 г. квантовые компьютеры позволяют работать с квантовыми регистрами размера около 50 бит и программировать порядка 10^5 логических операций [10, 11]. Сложности обусловлены тем, что увеличение разрядности квантового регистра на один бит ведет к снижению мощности сигнала вдвое. Разложение составного числа длиной 512 бит требует регистра длиной 2564 бит и 10^9 логических операций. Однако прогресс в этой области техники идет быстро.

Изложенное показывает, что актуальной является проблема расширения класса универсальных задач, положенных в основу криптографических алгоритмов.

2. Категория изогенных эллиптических кривых

Категорией называется множество объектов и множество морфизмов, отображающее один из объектов в другой [14]. На множестве морфизмов определена ассоциативная операция композиции, существует единственный морфизм, сохраняющий объект неподвижным.

Примером категории является категория абелевых групп. В ней объектами являются абелевы группы, а морфизмами — гомоморфизмы групп.

Для построения алгоритмов аутентификации предлагается использовать категорию изогенных эллиптических кривых. По-видимому, предложенный метод справедлив и для алгебраических групп, определяемых алгебраическими кривыми более высоких степеней.

Эллиптическая кривая $E(\mathbb{F}_p)$ над простым полем \mathbb{F}_p задается уравнением

$$y^2 = x^3 + ax^2 + bx + c, \quad (1)$$

где многочлен в правой части не имеет кратных корней.

Точки эллиптической кривой задают абелеву группу по сложению. Эта группа либо циклична, либо изоморфна прямой сумме двух циклических групп. Число точек эллиптической кривой (1) конечно.

На кривой (1) можно определить кольцо аффинных координат $\mathbf{F}_p[E]$ как кольцо классов вычетов $\mathbf{F}_p[x, y]/(y^2 - x^3 - ax^2 - bx - c)$. Поле частных этого кольца образуют поле рациональных функций $\mathbf{F}_p(E)$ — квадратичное расширение поля функций одной переменной.

Между двумя эллиптическими кривыми может существовать *изогения* — отображение, отображающее бесконечно удаленную точку в бесконечно удаленную точку и задаваемое парой рациональных функций [12]. Такие кривые называются *изогенными*. Из уравнения (1) следует, что изогения $\varphi: E_1(\mathbf{F}_p) \rightarrow E_2(\mathbf{F}_p)$ задается функциями $\varphi = (f, g)$ из $\mathbf{F}_p(E)$.

Степенью изогении называется число $l = [\mathbf{F}_p(E_1) : \mathbf{F}_p(E_2)]$.

Изогения φ имеет дуальную (но не обратную) изогению $\hat{\varphi}: E_2(\mathbf{F}_p) \rightarrow E_1(\mathbf{F}_p)$. При этом отображение $\hat{\varphi}\varphi$ соответствует умножению точки кривой E_1 на целое число l , а изогения $\varphi\hat{\varphi}$ — умножению точки кривой E_2 на это же число. Дуальные изогении имеют одинаковые степени.

Изогении определены для кривых над произвольными полями. В случае кривой над \mathbf{C} изогения задает гомоморфизм фундаментальных параллелограммов, определяющих эллиптические кривые. Таким образом, ядро изогении — точки кривой, обращающиеся в бесконечно удаленную точку — имеет мощность l , это же справедливо и для алгебраически замкнутого конечного поля. Если кривая рассматривается над \mathbf{F}_p , то ядро изогении имеет степень l . Для существования изогении степени l необходимо, чтобы число точек на кривой делилось на l .

Изогении задают морфизмы эллиптических кривых и их гомоморфизмы как абелевых групп и, следовательно, являются морфизмами категории изогенных эллиптических кривых.

Эллиптическая кривая характеризуется дискриминантом Δ и j -инвариантом. Если характеристика поля больше 3, то уравнение кривой можно привести к виду

$$y^2 = x^3 + Ax + B. \quad (2)$$

В этом случае $\Delta = 4A^3 + 27B^2$, $j = \frac{1728 \cdot 4A^3}{4A^3 + 27B^2}$. Обратимая аффинная замена переменных, сохраняющая вид уравнения кривой, сохраняет и j -инвариант [12].

Изогенные кривые полностью характеризуется своими j -инвариантами. Для каждой эллиптической кривой существует не более l изогенных кривых, где l — степень изогении. Инварианты кривых, изогенных кривой с данным j , определяются как корни над \mathbf{F}_p модулярного уравнения [8]. Для этого нужно вместо одной из переменных подставить j . Если кривая E_1 с инвариантом j_1 изогенна кривой E_2 с инвариантом j_2 , то кривая E_2 изогенна E_1 , и j_1 является корнем модулярного уравнения при подстановке j_2 вместо одной из переменных. Если модулярное уравнение имеет

кратный корень, то это соответствует комплексному умножению, задаваемому изогенией. Комплексное умножение можно рассматривать как единичный морфизм, отображающий кривую в себя.

Модулярное уравнение имеет вид $\Phi_l(u, v) = 0$, где Φ_l — модулярный симметрический многочлен над \mathbf{Z} степени $l + 1$. Число слагаемых в Φ_l равно $O(l^2)$. Размер коэффициентов модулярного многочлена быстро растет с ростом l . Модулярный многочлен для изогении степеней 2 и 3 имеет вид [8]:

$$\begin{aligned}\Phi_2(u, v) &= u^3 + v^3 - u^2v^2 + 1488uv(u + v) - 162000(u^2 + v^2) + 40773375 uv + \\ &\quad 8748000000(u + v) - 157464000000000; \\ \Phi_3(u, v) &= u^4 + v^4 - u^3v^3 + 2232u^2v^2(u + v) - 1069956uv(u^2 + v^2) + 36864000(u^3 \\ &\quad + v^3) + 2587918086u^2v^2 + 8900222976000uv(u + v) + 452984832 \cdot 10^6(u^2 + v^2) - \\ &\quad 770845966336 \cdot 10^6 uv + 1855425871872 \cdot 10^9(u + v).\end{aligned}$$

Уравнение $\Phi_l(u, j) = 0$ имеет 0, 1, 2 или $l + 1$ корень в поле \mathbf{F}_p [8]. Если j_1, j_2 — инварианты изогенных эллиптических кривых, то $\Phi_l(j_1, j_2) = 0$ тогда и только тогда, когда между этими кривыми существует изогения степени l [8]. Из симметричности многочлена $\Phi_l(u, v)$ следует, что для каждой неединичной изогении существует дуальная.

Таким образом, граф изогений, вершинами которого являются инварианты кривых, а ребрами — изогении степени l , является неориентированным.

В работе [4] говорится, что этот граф представляет собой дерево. Каждая вершина имеет или $l + 1$ инцидентное ей ребро, два или одно ребро. При этом почти все вершины имеют одно ребро (листья) или $l + 1$ ребро. Однако нами найден контрпример, показывающий, что внутри “дерева” изогений простой степени l могут содержаться циклы. Например, эллиптическая кривая $y^2 = x^3 + x + 85 \pmod{251}$ имеет $j = 75$, граф изогений степени 2 содержит цикл длины 6, с каждой вершиной цикла связан единственный лист.

Наличие цикла изогений степени l говорит о том, что их произведение в кольце эндоморфизмов дает 1. Действительно, изогении индуцируют гомоморфизмы эллиптических кривых как абелевых групп. Поскольку в этом случае существуют две разных изогении (и, следовательно, сколь угодно много изогений) между двумя эллиптическими кривыми, которые действуют одинаково, то произведение изогений, задающих цикл, должно давать единицу.

3. Изогении степеней 2 и 3

Простейшие изогении $\varphi: E_1(\mathbf{F}_p) \rightarrow E_2(\mathbf{F}_p)$ имеет степень 2 и 3. Для этого кривая $E_1(\mathbf{F}_p)$ должна иметь соответственно точку порядка 2 и 3. В

первом случае аффинной заменой переменной x можно получить уравнение (1) с коэффициентом $c = 0$. Обозначим кривую (1) через $E[a, b]$.

Изогения $\varphi: E[a, b] \rightarrow E[-2a, a^2 - 4b]$ степени 2 имеет вид [12]:

$$\varphi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2} \right), \quad (3)$$

дуальная изогения $\hat{\varphi}: E[-2a, a^2 - 4b] \rightarrow E[a, b]$ имеет вид [12]:

$$\hat{\varphi}(x, y) = \left(\frac{y^2}{4x^2}, \frac{y(x^2 - a^2 + 4b)}{8x^2} \right). \quad (4)$$

Кривая $E(a, b)$ имеет j -инвариант $j = \frac{256(a^2 - 3b)^3}{b^2(a^2 - 4b)}$. Если j -

инвариант под действием изогений (3, 4) остается неподвижным, то это соответствует комплексному умножению. Если $a = -4t$, $b = 2t^2$, то изогении (2, 3) соответствуют комплексному умножению на $\sqrt{-2}$, при этом $j = 20^3$.

Если $a = 3k$, $b = 2k$, $k = -\frac{5^3}{3^3 \cdot 7}$, то изогении (3, 4) соответствуют комплексному умножению на $\frac{\pm 1 \pm \sqrt{-7}}{2}$ [15]. При этом $j = -15^3$.

Ядром изогении (3, 4) являются точки порядка 2, т. е. $(0, 0) \cup P_\infty$. Если число точек на кривой является удвоенным простым числом r , то изогения степени 2 является взаимно однозначным отображением точек порядка r .

Формулы для изогении степени 3 могут быть получены по методике [13]. Кривая (2) с точкой $R = (x_R, y_R)$ порядка 3 изогенна кривой $Y^2 = X^3 + A_1X + B_1$. Изогения задается системой уравнений

$$X = \frac{-x^3 + 2x^2x_R + x(2A + 5x_R^2) + 4B + 2Ax_R - 2x_R^3}{(x - x_R)^2},$$

$$Y = y \frac{-x^3 + 3x^2x_R - x(2A + 9x_R^2) - 8B - 6Ax_R - x_R^3}{(x - x_R)^3},$$

$$A_1 = -9A - 30x_R^2;$$

$$B_1 = -27B - 70x_R^3 - 42Ax_R.$$

Инвариант кривой (2) равен $j = \frac{1728 \cdot 4A^3}{4A^3 + 27B^2}$.

Изогении более высоких степеней описываются более сложными уравнениями. Для построения криптосистемы достаточно наличия двух или более изогений малых степеней $\{l_i\}$. При этом граф изогений может содержать циклы.

Для существования изогении степени l достаточно, чтобы число точек кривой делилось на l . Однако, если число точек не делится на l^2 , то обычно для кривой существует единственная изогения степени l . Соответственно связный граф изогений оказывается небольшим. Если же число точек делится на l^2 , то связный граф изогений увеличивается. Если число точек делится на $(l_1 l_2)^2$, то связный граф изогений может быть максимальным, с числом вершин, равным $O(\sqrt{p})$.

Например, для эллиптической кривой $y^2 = x^3 + x + 18$ над полем из 1009 элементов число точек равно $2^2 \cdot 3^2 \cdot 29$, $j = 117$. Связный граф изогений содержит 42 вершины.

Задача нахождения изогении между двумя изогенными кривыми сводится к задаче нахождения цепочки j -инвариантов под действием изогений степеней l_i . Эта задача является частным случаем задачи нахождения пути между двумя вершинами на неориентированном графе.

Если граф обусловлен действием изогений степеней 2 и 3, то каждая вершина имеет в среднем 2–3 ребра.

Задание изогении цепочкой несложных изогений не позволяет использовать для решения модулярных уравнений функции со скрытыми периодами, поскольку на каждом шаге коэффициенты уравнения меняются.

Теоретически можно использовать периодичность для вскрытия изогении, если вычислить модулярное уравнение степени l^n . Однако временная и емкостная сложности нахождения коэффициентов этого уравнения экспоненциальны, поэтому задача программирования квантового компьютера становится недопустимо сложной. Это позволяет предположить, что задача вычисления изогении между двумя эллиптическими кривыми является сложной для квантового компьютера.

Очевидно, что вместо изогении степени 2 можно использовать и другие изогении простых степеней.

4. Криптографические протоколы и примитивы на изогенных кривых

В основу безопасности протокола опознавания положена задача нахождения цепочки изогений степени l между двумя изогенными эллиптическими кривыми.

В исходном состоянии верификатор и претендент знают две изогенных кривых $E_1(\mathbf{F}_p)$ и $E_2(\mathbf{F}_p)$ и точки на них $Q_1 \in E_1(\mathbf{F}_p)$, $Q_2 \in E_2(\mathbf{F}_p)$. Эта ин-

формация является открытым ключом аутентификации. Секретный ключ претендента — цепочка изогений степени l между указанными кривыми.

Протокол 1. Диалоговое опознавание на изогенных эллиптических кривых.

Вход претендента. Секретный ключ.

Вход верификатора. Открытый ключ.

Результат. Опознавание претендента.

Метод.

1. Верификатор генерирует случайный логарифм z , вычисляет точку $P_1 = zQ_1$ на кривой E_2 и посылает эту точку претенденту.
2. Претендент вычисляет точку P_2 на кривой E_2 с помощью цепочки изогений и возвращает верификатору.
3. Верификатор проверяет, что выполняется равенство $P_2 = zQ_2$. В случае выполнения равенства опознавание считается успешным. ■

Безопасность протокола определяется следующей теоремой.

Теорема 2. Безопасность протокола 1 основана на следующих независимых задачах: задаче вычисления изогении между кривыми E_1 и E_2 в течение срока действия ключа опознавания и задаче логарифмирования на эллиптической кривой в реальном масштабе времени.

Доказательство. Предположим, что нарушитель, знающий открытый ключ, может найти изогению. Тогда он может найти ключ претендента и успешно пройти опознавание.

Предположим, что нарушитель может вычислить логарифм z на кривой E_1 для пары точек Q_1 и P_1 . Тогда он может успешно пройти опознавание, не зная ключа. Однако для этого он должен выполнить вычисления достаточно быстро — в реальном масштабе времени (недопустимую длительность вычислений легко заблокировать таймером). ■

Отметим, что квантовые компьютеры обладают низкой эффективной тактовой частотой [9, 10], поэтому даже если задача логарифмирования на эллиптической кривой может быть решена с полиномиальной сложностью, вычислить логарифм в реальном масштабе времени, по-видимому, невозможно.

Модификация протокола 1 позволяет реализовать диалоговую цифровую подпись. Открытый и секретный ключи те же, что и в протоколе 1. Кроме того, претендент и верификатор договариваются о вычисляемой в одну сторону хэш-функции h , свободной от коллизий.

Протокол 2. Диалоговая цифровая подпись.

Вход претендента. Секретный ключ, хэш-функция h .

Вход верификатора. Открытый ключ, хэш-функция h .

Результат. Цифровая подпись для сообщения m .

Метод.

1. Верификатор генерирует случайный показатель k , вычисляет точку $P_1 = kQ_1$ и посылает претенденту.
2. Претендент вычисляет $h(m)$ и проверяет, что $h(m) \neq 0$. Если это условие выполняется, он генерирует вычисляет точку $R_1 = h(m)P_1$ и вычисляет для нее изогению, получая подпись — точку $R_2 \in E_2$, и отправляет пару (m, R_2) верификатору.
3. Верификатор вычисляет $h(m)$ и проверяет, что $h(m) \neq 0$. Затем он вычисляет логарифм $kh(m)$ и проверяет, что выполняется равенство $R_2 = kh(m)Q_2$. В случае выполнения равенства подпись считается ложной. ■

Граф изогений будет иметь большой размер, если он образован хотя бы парой изогений, например, степеней 2 и 3; при этом число точек должно делиться на 2^2 и на 3^2 . Представляется целесообразным, чтобы оставшийся делитель был простым. Это позволит исключить существование других образующих для графа изогений. Однако приведет ли наличие других изогений малой степени к снижению сложности вычисления результирующей изогении, неясно.

Генерация ключа для опознавания осуществляется по методика [16]. Для этого нужно выбрать случайным образом дискриминант D , задающий мнимое квадратичное поле с числом классов 1, и такие два целых числа d и e , что число $p = d^2 + De^2$ является простым и хотя бы одно из чисел $p + 1 + 2d$, $p + 1 - 2d$ является простым числом, умноженным на 36. Затем нужно вычислить j -инвариант полученной кривой и найти j -инвариант очередной кривой решением случайно выбранного одного из двух модулярных уравнений и вычислить изогению между выбранными двумя кривыми. Этот процесс повторяется $O(\log p)$ раз. Начальная и конечная кривая являются открытым ключом, а цепочка j -инвариантов и изогений — секретным ключом.

Оценим число вершин графа изогений. Анализ изоморфизмов кривых [12] показывает, что число неизоморфных эллиптических кривых над полем \mathbf{F}_p равно $O(p)$. Изогенные кривые должны быть неизоморфными и иметь одинаковые числа точек. В соответствии с теоремой Хассе [12] количество вариантов для числа точек на кривой равно $O(\sqrt{p})$. Поэтому число изогенных кривых можно оценить частным от деления числа неизоморфных кривых на количество вариантов для числа точек, что составляет $O(\sqrt{p})$. Соответственно сложность нахождения цепочки изогений методом встречи посередине составит $O(\sqrt[4]{p})$.

Задача вычисления изогении, образованной цепочками изогений степеней 2 и 3, на квантовом компьютере представляется сложной. Действительно, для достаточно длинной цепочки изогений степень результирующей

щей изогении оказывается экспоненциальной, и задание соответствующего модулярного уравнения и уравнения для изогении потребует экспоненциально большого объема работы. Это не позволяет составить программу для квантового компьютера. Оперирование с изогениями малых степеней приводит к случайному блужданию на графе изогений и к многократному повторению одной и той же процедуры с переменными параметрами. По-видимому, для задачи о нахождении пути на графе квантовый компьютер будет менее эффективен, чем традиционный.

Литература

1. Boneh D., Lipton R. Quantum computation of hidden linear functions. // *Advances in Cryptology — Proceedings of CRYPTO '95 (LNCS 963)*, p. 424–437.
2. Buchmann J., Müller V. Algorithms for factoring integers. // Internet publication.
3. Chor B., Rivest J. A knapsack-type public key cryptosystem based on arithmetic in finite fields. // *Advances in Cryptology — Proceedings of CRYPTO '84 (LNCS 196)*, p. 54–65.
4. Couveignes J-M., Dewaghe L., Morain F. Isogeny cycles and the Schoof-Elkies-Atkin algorithm. Technical report LIX/RR/96/03.
5. ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. // *Advances in Cryptology — Proceedings of CRYPTO '84 (LNCS 196)*, p. 10–18.
6. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems // *Advances in Cryptology — CRYPTO '86, LNCS, v. 263, Springer-Verlag, 1987, pp. 186–194.*
7. FIPS Publication 186, Digital Signature Standard, Federal Information Processing Standards Publication 186, U.S. Department of Commerce / N.I.S.T., National Technical Information Service, Springfield, Virginia, May 1994.
8. Fouquet M., Morain F. Isogeny volcanoes and the SEA algorithm. — Technical report LIX/RR/00/05, 2000.
9. Hahn T., Meyer A., Nies S., Pfahler T. Implementing cryptographic protocols based on algebraic number fields. Technical report TI-99-24 nf, 1999 (Internet publication).
10. Hughes et al. The Los Alamos trapped ion quantum computer experiment. Technical report LA-UR-97-3301, 1997.
11. Hughes R. J. Quantum computation. Technical report LA-UR-98-288, 1998.
12. Husemöller D. Elliptic curves. — Springer-Verlag, 1987.
13. Lercier R., Morain F. Algorithms for computing isogenies between elliptic curves (preliminary version). // Internet publication.
14. Ленг С. Алгебра. — М.: Мир, 1968.

15. Ростовцев А. Г., Маховенко Е. Б. Изогении степени 2 и быстрая арифметика эллиптических кривых. // Проблемы информационной безопасности. Компьютерные системы. № 4, 2000.
16. Ростовцев А. Г., Маховенко Е. Б.. Введение в криптографию с открытым ключом. — СПб., Мир и Семья, Интерлайн, 2001.