МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное
образовательное учреждение высшего образования
«Московский физико-технический институт (национальный исследовательский университет)»

Физтех-школа Радиотехники и Компьютерных Технологий

РЕФЕРАТ
по дисциплине
«Защита информации»

по теме:

ЗАДАЧИ, ЛЕЖАЩИЕ В ОСНОВЕ ПОСТКВАНТОВЫХ КЕМ

Студент:
Группа № Б01-108 *А.Л. Симанкович*

Долгопрудный 2024

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

1.1 Актуальность проблемы

Ассиметричное шифрование (шифрование с открытым ключом) лежит в основе множества ключевых сетевых протоколов (TLS, SSH, HTTPS). Однако устойчивость используемых в данный момент алгоритмов шифрования находится под угрозой квантовых компьютеров. При создании достаточно большого (в терминах количества кубитов – квантовых битов) компьютера, уже разработанные квантовые алгоритмы позволят получить доступ к огромному массиву информации, передающейся по сети. Под угрозой находятся переписки, банковские транзакции, личные данные, системы удаленного управления и т.п.

Для защиты от атак с помощью квантовых компьютеров разрабатываются специальные – постквантовые алгоритмы. Основным отличием от классических алгоритмов они отличаются требованием устойчивости как к классическим, так и квантовым атакам. При этом шифрование должно производится на классических компьютерах. Это позволит внедрить алгоритмы заранее и использовать повсеместно.

Стратегия ”Harvest now, decrypt later” заключается в сборе открытых ключей и зашифрованных данных сейчас, с расчетом на появление технологий, позволяющих расшифровать их в будущем. Это позволит злоумышленникам воспользоваться слабостью нынешнего шифрования. Взлом этих алгоритмов также позволит подменить подписи, использованные в прошлом, переписав историю транзакций (например, в блокчейне). Поэтому разработка и внедрение постквантовых алгоритмов должно производится задолго до того, как появятся квантовые компьютеры, представляющие угрозу (Y2Q или Q-day).

1.2 Механизмы шифрования ключа (KEM)

Задачи создания защищенного канала решаются наиболее быстро и удобно с помощью симметричного шифрования. В этом случае обе стороны используют общий секретный ключ. Недостаток этого подхода заключается в необходимости доставить секретный ключ, не раскрыв его злоумышленникам. В случае обеспечения такого доступа между агентами по сети этот недостаток становится критическим. Для его исправления используются KEM (Key Encapsulation Mechanism – механизм шифрования ключа).

KEM основаны на ассиметричном шифровании с открытым ключом. Агент A генерирует асимметричную пару ключей (s, p), открытый ключ p отправляет по сети агенту B. Агент B генерирует симметричный секретный ключ k, шифрует его с помощью открытого ключа p и отправляет шифр c. Агент A дешифрует c с помощью s, получая симметричный ключ k.

1.3 Классические алгоритмы

Все алгоритмы с открытым ключом опираются на сложность инвертирования некоторой односторонней функции. Такая функция должна иметь полиномиальную сложность при вычислении и экспоненциальную сложность при инвертировании. В прикладном смысле это означает, что шифрование с помощью открытого ключа должно быть быстрым, а дешифровка быстрой только с помощью секретного ключа.

На данный момент самые широкораспространенные алгоритмы используют факторизацию целых чисел (например, RSA), дискретный логарифм (EdDSA). Все эти задачи уязвимы к алгоритму Шора – квантовому алгоритму, который использует квантовое преобразование Фурье (QFT).

1.4 Постквантовые алгоритмы

Постквантовые алгоритмы основаны на задачах из различных областей математики, включая:

- Решетки (Lattice-based);
- Хэши (Hash-based);
- Коды ошибок (Code-based);
- Изогении (Isogeny-based).

Мы рассмотрим принципы работы нескольких из них.

2 АЛГОРИТМЫ НА РЕШЕТКАХ

В этой главе будут описаны задачи SVP/SIS и LWE, и основанные на них алгоритмы шифрования.

2.1 Решетки как математическая структура

Решетка – это периодическая “сетка” в пространстве Z^m. Для каждой решетки можно выбрать базис, причем он не единственный.

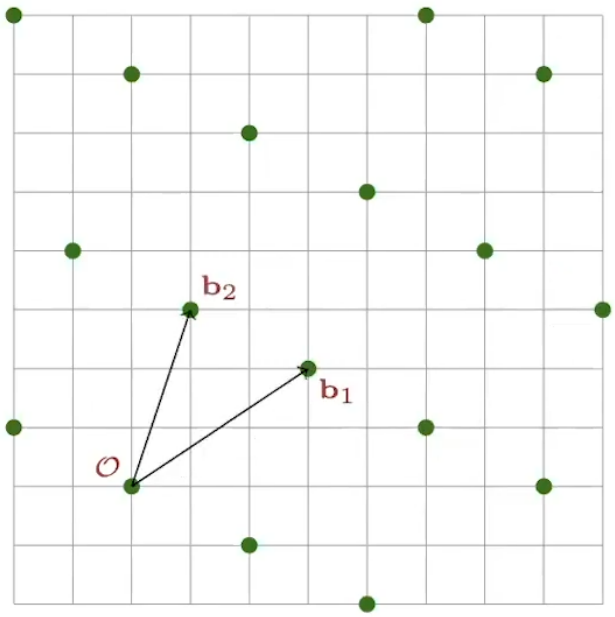

Рисунок 1 — Пример решетки и ее базиса при $m = 2$

Для них существует некоторый набор “стандартных”, хорошо изученных задач. Например, GapSVP, SIVP (Shortest Independent Vectors Problem). Эти задачи в сложных случаях (для сложных наборов параметров) не имеют полиномиальных алгоритмов решения.

2.2 SVP (Shortest Vector Problem)

Постановка задачи проста: найти самый короткий вектор $\boldsymbol{b_0}$ в решетке $\mathcal{L}$, заданной каким-то базисом.

Сложность задачи растет с размерностью решетки m. Обычно рассматриваются приближенные задачи – поиск вектора с длиной меньше $\gamma \boldsymbol{b_0}$. Имеющиеся алгоритмы (в том числе квантовые) требуют экспоненциальных памяти и времени для задачи с $\gamma = poly(m)$ [1].

Квантовые алгоритмы не исправляют ситуацию, поскольку не говорят ничего о геометрических свойствах. Например, алгоритм Шора хорошо справляется с поиском групповой структуры, но не позволяет находить кратчайшие вектора в геометрическом смысле.

2.3 SIS (Short Integer Solution)

Эта задача является алгебраической и на первый взгляд не имеет ничего общего с решетками.

Пусть $\mathbb{Z}_q^n$ – поле векторов размерности n по модулю q. Выберем равномерно случайную матрицу $A \in \mathbb{Z}_q^{n \times m}$. Задача – найти ненулевой $\boldsymbol{z} \in \mathbb{Z}^m$ такой, что $A\boldsymbol{z} = \mathbf{0} \in \mathbb{Z}_q^n$ при условии $\|\boldsymbol{z}\| < \beta \ll q$.

Если предположить, что SIS сложно решить, то, взяв $m > n \log_2 q$ определим хэш-функцию $f_A : \{0,1\}^m \to \mathbb{Z}_q^n$ как $f_A(\boldsymbol{x}) = A\boldsymbol{x}$. Такая функция будет устойчива к поиску коллизий, поскольку $A\boldsymbol{x} = A\boldsymbol{x'} \Rightarrow A(\boldsymbol{x} - \boldsymbol{x'}) = 0$, то есть $\boldsymbol{z} = \boldsymbol{x} - \boldsymbol{x'} \in \{0, \pm 1\}^m$ – решение SIS.

2.4 Связь SIS и SVP

Выясним, какое отношение SIS имеет к решеткам.

Матрица $A \in \mathbb{Z}_q^{n \times m}$ задает решетку $\mathcal{L}^{\perp}(A) = \{\boldsymbol{z} \in \mathbb{Z}^m : A\boldsymbol{z} = \mathbf{0}\}$. На Рисунке 2 изображена решетка для случая $m = 2$. Тогда нахождение $\boldsymbol{z}$ для SIS эквивалентно поиску “короткого” вектора в решетке $\mathcal{L}^{\perp}(A)$. То есть SIS эквивалентна SVP.

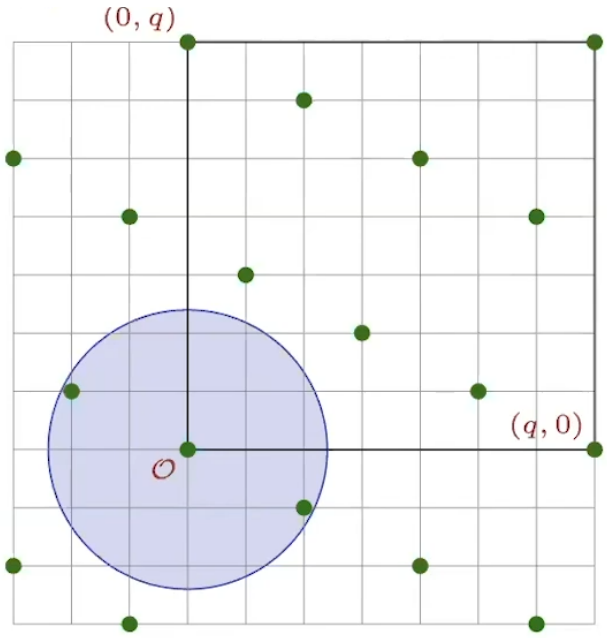

Рисунок 2 — Решетка и ограничение на длину вектора $\boldsymbol{z}$

Важным теоретическим результатом является сведение worst-case (нахождение решения на самых сложных вариантах) к average-case (нахождение решения для случайных

вариантов): Алгоритмом для нахождения “короткого” вектора для равномерно случайной A можно решить любую задачу GapSVP и SIVP [2]. Поскольку лучшие алгоритмы, которые были найдены, для сложных случаев GapSVP и SIVP – экспоненциальные, то считается, что полиномиального алгоритма для SIS не существует.

2.5 Применение SIS в криптографии

Предположим, что мы можем сгенерировать равномерно случайную матрицу A с “секретным ключом” T (trapdoor). Такой алгоритм существует, почти любая матрица может из равномерного распределения может быть создана в паре с ключом T [3]. Для подписи мы считаем хэш сообщения $H(\mu)$ и с помощью T находим достаточно короткий $\boldsymbol{z}$: $A\boldsymbol{z} = H(\mu) \in \mathbb{Z}_q^n$. В качестве $H(\mu)$ можно использовать любую достаточно надежную хэш-функцию (например, SHA). Для того, чтобы исключить “обучение” на выдаваемых $\boldsymbol{z}$ мы будем брать их из дискретного гауссова распределения. Иначе, T может быть восстановлен по набору $\boldsymbol{z}$ для различных $H(\mu)$ [4].

Для создания подписи на другое сообщение μ^* злоумышленнику требуется найти “достаточно короткий” $\boldsymbol{z}$ такой, что $A\boldsymbol{z}^* = H(\mu^*)$. Эта задача и есть SIS.

2.6 LWE (Learning With Errors)

Постановка задачи LWE: необходимо найти секретный $\boldsymbol{s} \in \mathbb{Z}_q^n$, зная $\boldsymbol{b}^T = \boldsymbol{s}^T A + \boldsymbol{e}^T$ – скалярные произведения случайных векторов с $\boldsymbol{s}$ с некоторой гауссовой ошибкой $\boldsymbol{e}$.

Матрица A вновь задает решетку, но уже иначе: $\mathcal{L}(A) = \{\boldsymbol{z}^T : \boldsymbol{z}^T = \boldsymbol{s}^T A \mod q\}$. Пример приведен на Рисунке 3. Таким образом, LWE сводится к задаче поиска узла решетки по точке в его окрестности.

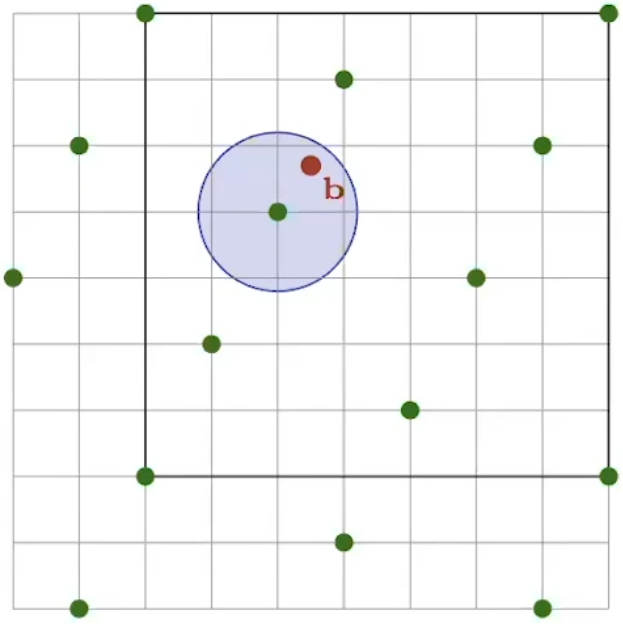

Рисунок 3 — Нахождение узла решетки по точке вблизи него (тут $\boldsymbol{e} \notin \mathbb{Z}_q^n$ для наглядности)

Теория говорит, что search-LWE – сложная задача. Есть сведение алгоритма для average-case LWE к worst-case задачам на решетках (GapSVP, SIVP) [5]. Эти задачи считаются не имеющими полиномиального решения даже квантовыми компьютерами, поэтому LWE считается квантово устойчивой.

Более того, можно показать, что если существует алгоритм, отличающий полностью случайные пары $(A, \boldsymbol{b})$ от тех, которые являются скалярным произведением с $\boldsymbol{s}$ (decision-LWE), то его можно свести к алгоритму для search-LWE [5].

2.7 Применение LWE в криптографии

Агенты А и Б выбирают равномерно случайную матрицу $A \in \mathbb{Z}_q^{n \times n}$. Эта матрица будет частью открытого ключа, общего для агентов. После чего агент А выбирает "короткий", равномерно случайный вектор $\boldsymbol{s} \in \mathbb{Z}_q^n$, Б – вектор $\boldsymbol{r}$ с такими же свойствами. Агент А вычисляет $\boldsymbol{u}^T \approx \boldsymbol{r}^T A \in \mathbb{Z}_q^n$, агент Б в свою очередь $\boldsymbol{v} \approx A\boldsymbol{s} \in \mathbb{Z}_q^n$. При вычислении $\boldsymbol{u}$ и $\boldsymbol{v}$ вносится ошибка из гауссова распределения, которое также является заранее выбранным и общеизвестным.

Заметим, что агент А может получить $\boldsymbol{r}^T\boldsymbol{v} \approx \boldsymbol{r}^T A\boldsymbol{s} \approx k$. В свою очередь агент Б получает $\boldsymbol{u}^T\boldsymbol{s} \approx \boldsymbol{r}^T A\boldsymbol{s} \approx k$. То есть А и Б получили два числа, очень близких к общему числу $k \in \mathbb{Z}_q$.

Тогда агент Б может закодировать бит как $c = k + \text{bit} \cdot \frac{q}{2}$.

При дешифровке агент А получает

$$c - k \approx \text{bit} \cdot \frac{q}{2} = \begin{cases} \text{число, близкое к нулю, bit = 0;} \\ \text{число, близкое к } \frac{q}{2}\text{, bit = 1.} \end{cases}$$

Для каждого нового бита нужно генерировать новую пару $\boldsymbol{s}$, $\boldsymbol{r}$, однако существуют способы ослабить это требование.

Рассмотрим задачу со стороны злоумышленника. Он имеет доступ к $\{A, \boldsymbol{u}, \boldsymbol{v}, c\}$. Его задача – распознать, $c = k$ или $c = k + \frac{q}{2}$. По сути это – задача decision-LWE. То есть она считается квантово устойчивой на сегодняшний день. Для злоумышленника набор $\{A, \boldsymbol{u}, \boldsymbol{v}, c\}$ неотличим от равномерно случайного.

Может показаться, что значения $\boldsymbol{r}$ и $\boldsymbol{s}$ можно получить обращением матрицы A. Однако, попытка применить A^{-1} к $\boldsymbol{u}$ или $\boldsymbol{v}$ дает

$$A^{-1}\boldsymbol{u} = A^{-1}A\boldsymbol{r} + A^{-1}\boldsymbol{e} = \boldsymbol{r} + A^{-1}\boldsymbol{e}.$$

При этом $A^{-1}\boldsymbol{e}$ вносит настолько сильный вклад, что выделить $\boldsymbol{r}$ становится невозможным.

2.8 Преимущества

Алгоритмы, основанные на решетках, обладают рядом преимуществ:

– задачи на решетках опираются на геометрические свойства, вычисление которых хорошо сопротивляются квантовым атакам;
– существуют теоремы, доказывающие, что из worst-case hardness задач следует их average-case hardness;
– обладают высокой степенью вычислительного параллелизма за счет линейной структуры.

Кроме того, их можно использовать для полностью гомоморфного шифрования (Fully Homomorphic Encryption) – шифрование, позволяющие совершать математические операции над данными не расшифровывая их.

3 АЛГОРИТМ НА ИЗОГЕНИЯХ

В этой главе будет рассмотрен принцип работы алгоритма SIDH (Supersingular Isogeny Diffie-Hellman).

3.1 Изогении как математическая структура

3.1.1 Эллиптические кривые

Изогении основаны на эллиптических кривых.

Нам понадобится сложение точек на эллиптических кривых (пример на Рисунке 4) и определение порядка точки: deg $P = n$, если $[n]P = \mathcal{O}$, где $[n]P$ – сложение P с самим собой n раз, $\mathcal{O}$ – нейтральный элемент .

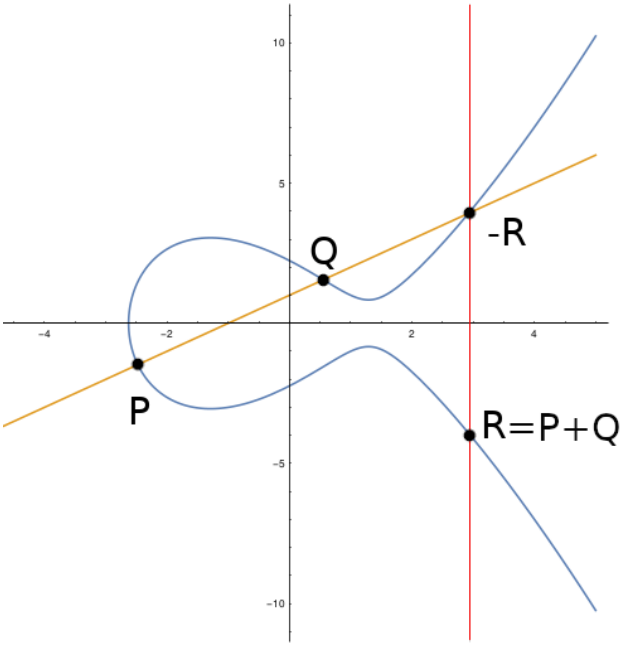

Рисунок 4 — Пример эллиптической кривой

Пусть дана $P \in E$, а точка S вычисляется как $S = [n]P \in E$. Классическая задача (используемая в EdDSA) – дискретный логарифм на эллиптических кривых, ставится так: найти n такое, что $S = [n]P$.

Эта задача сложная для классических компьютеров, но не для квантовых.

3.1.2 Изоморфизмы и j-инварианты

С этого момента будем работать в поле $\mathbb{F}_{q^2}$.

Для эллиптической кривой E_a можно ввести понятие j-инварианта – специальное число, описывающее данную кривую. Например, для кривой $E_a : y^2 = x^3 + ax^2 + x$ j-инвариант задается как $j(E_a) = \frac{256(a^3-3)^3}{a^2-4}$.

Кривые E и E' называются изоморфными ($E \cong E'$), если у них одинаковые j-инварианты. Между любыми изоморфными кривыми существует линейное преобразование ψ, переводящее одну кривую в другую. Соответственно, существует и обратное ему ψ^{-1}:

$$\begin{aligned} \psi \quad &: E \to E', \qquad (x, y) \to (\alpha x + \beta, \gamma y), \\ \psi^{-1} \quad &: E' \to E, \qquad (x, y) \to (\alpha' x + \beta', \gamma' y). \end{aligned}$$

Заметим, что у них отсутствуют особые точки, то есть $\ker \psi = \{\mathcal{O}_E\}$, $\ker \psi = \{\mathcal{O}'_E\}$, где $\mathcal{O}$ – нейтральный элемент группы.

3.1.3 Изогении

В случае, когда j-инварианты не равны, мы можем строить нелинейные отображения. Для некоторых пар E, E' у отображений появляются нули в знаменателе. У этих отображений $\ker \varphi$ нетривиален. Тогда E и E' называются изогенными друг другу, а отображение φ называется изогенией.

Для любого конечного подмножества G точек на E существует единственная изогения φ, для которой $\ker \varphi = G$. Формулы Велу (Vélu's formulas) по G вычисляют φ и E' [6].

Композиция изогений сохраняет групповые свойства:

$$\varphi(P + Q) = \varphi(P) + \varphi(Q).$$

Размер ядра φ будем называть его степенью: $\deg \varphi = \#(\ker \varphi)$. Для композиции изогений существует свойство:

$$\deg(\varphi_1 \circ \varphi_2) = \deg(\varphi_1) \cdot \deg(\varphi_2).$$

Таким образом, мы можем строить изогении очень высокого порядка как цепочку композиций изогений малого порядка.

3.1.4 Упрощаем начальные условия

1) Для всех изогений, полученных по формулам Велу выполняется свойство:

$$(x, y) \to (f(x), cyf'(x)), \quad c = \text{const}.$$

Поэтому мы можем опускать y в дальнейших выкладках.

2) Для алгоритма требуются изогении порядков $n = 2$ и $n = 3$.

3.2 Операции агентов

Операции агентов достаточно сложны и требуют выкладок в области теории групп. Общая идея заключается в разложении изогении высокого порядка на многократную композицию изогений малых порядков [7].

3.3 Граф j-инвариантов

Для любого простого числа p в поле $\mathbb{F}_{p^2}$ существует около $p/12$ особых эллиптических кривых (с точностью до гомоморфизма), которые позволяют ввести на них группу относительно умножения. Каждой из них соответствуют значение j-инварианта. На Рисунке 5 приведен пример для $p = 431$ [7].

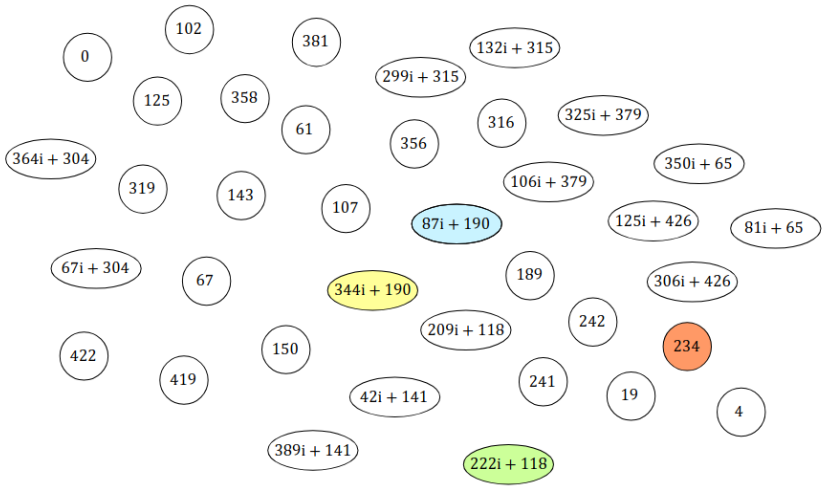

Рисунок 5 — Пример графа для $p = 431$

Операции каждого из агентов создают различный набор дуг, которые соединяют узлы графа j-инвариантов. Они изображены на Рисунках 6 и 7.

Важно отметить, что для любого p как бы мы не переставляли узлы, схема связей останется сложной. Это свойство отображает возможность добраться от одного узла до другого за малое число шагов.

Еще одним важным свойством является независимость полученных графов двух агентов.

Простое число p выбирается особым образом:

$$p = 2^k 3^m - 1.$$

При этом числа k и m задают количество изогений (шагов в графе), которые совершат агенты А и Б, соответственно.

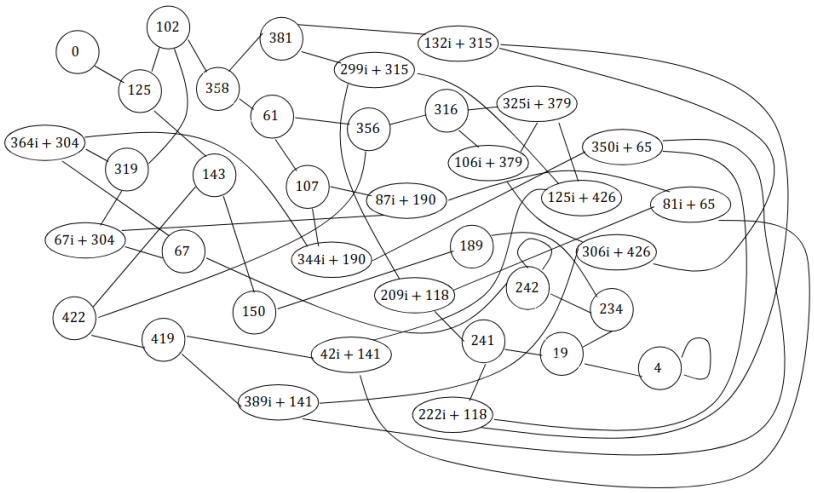

Рисунок 6 — Граф агента А, связанный изогениями второго порядка (по три ребра из каждой вершины)

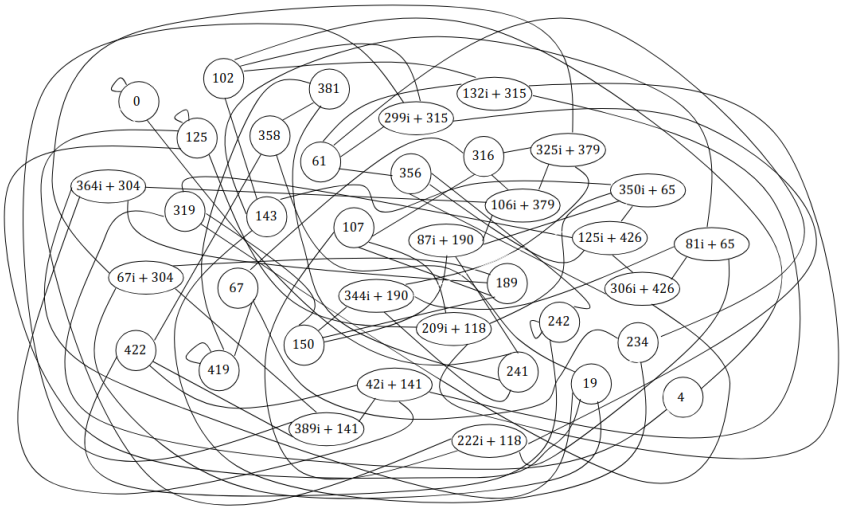

Рисунок 7 — Граф агента Б, связанный изогениями третьего порядка (по четыре ребра из каждой вершины)

3.4 Движение до открытого ключа

В качестве начальных условий выступает E_a – некоторая эллиптическая кривая, задающая начальный j-инвариант.

Рассмотрим движение агента А по графу. Он выбирает точку S порядка $\deg S = 2^4 = 16$.

На первом шаге он выполняет следующую последовательность операций:

$$S \to [2]S \to [4]S \to [8]S$$

$$\varphi_0 : \ker \varphi_0 = \{\mathcal{O}, [8]S\}.$$

Так он получает изогению φ_0 для перехода в другой узел.

Второй шаг:

$$S \to \varphi_0(S) \to [2]\varphi_0(S) \to [4]\varphi_0(S)$$

$$\varphi_0 : \ker \varphi_1 = \{\mathcal{O}, [4]\varphi_0(S)\}.$$

Так он получает следующую изогению φ_1 для перехода.

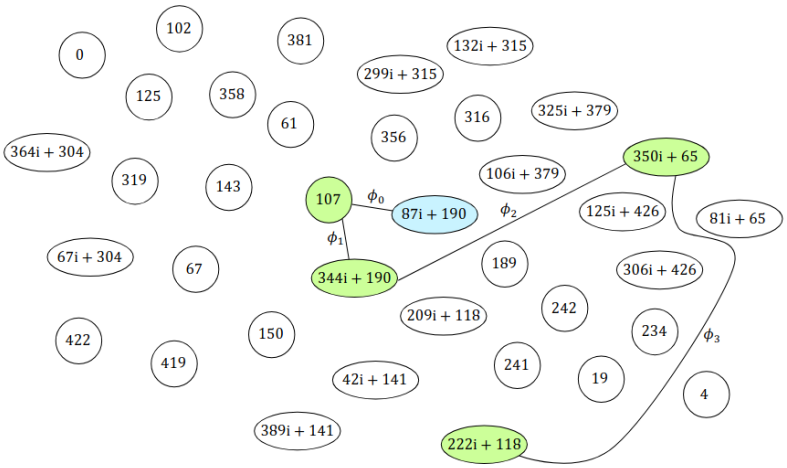

Рисунок 8 — Шаги агента А

Третий шаг:

$$S \to \varphi_0(S) \to \varphi_1(\varphi_0(S)) \to [2]\varphi_1(\varphi_0(S))$$

$$\varphi_2 : \ker \varphi_2 = \{\mathcal{O}, [2]\varphi_1(\varphi_0(S))\}.$$

Четвертый шаг:

$$S \to \varphi_0(S) \to \varphi_1(\varphi_0(S)) \to \varphi_2(\varphi_1(\varphi_0(S)))$$

$$\varphi_3 : \ker \varphi_3 = \{\mathcal{O}, \varphi_2(\varphi_1(\varphi_0(S)))\}.$$

Агент Б проводит аналогично 3 шага с $\deg S = 27$, $[3]$ и $deg\varphi_i = 3$.

По итогу каждый из агентов получает $\{S, \varphi_0, ...\varphi_m\}$ – закрытый ключ, а также итоговый узел E_n – открытый ключ.

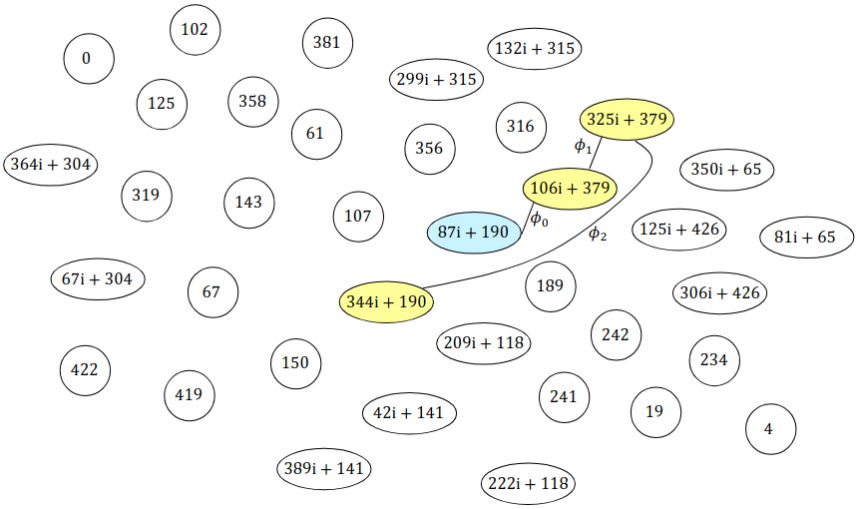

Рисунок 9 — Шаги агента Б

3.5 Движение до общего секретного ключа

Агенты А и Б передают друг другу их открытые ключи – новые начальные узлы в графе. Они проводят точно такое же движение по графу, но уже с новых узлов.

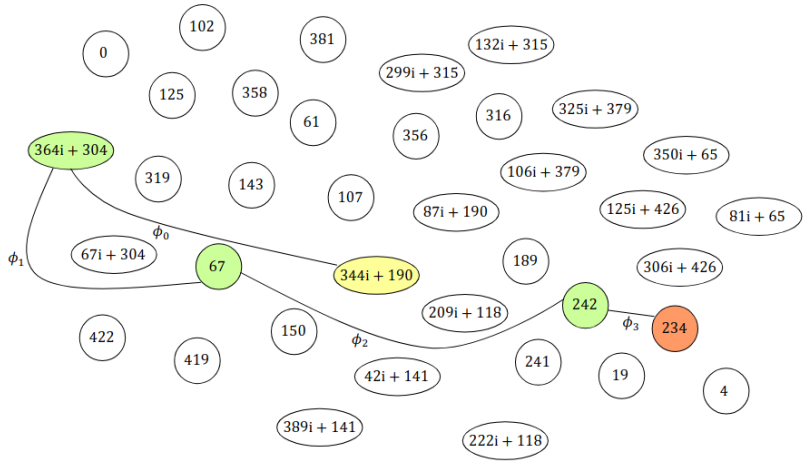

Рисунок 10 — Шаги агента А

Все эти построения приводят А и Б к общему узлу. При этом злоумышленник имеет лишь начальный узел и два открытых ключа. Изогении, приводящие к этому ключу, получены как композиция большого количества изогений малого порядка. Они имеют очень высокую степень, а сложность поиска обратного пути экспоненциально растет с порядком изогении [7].

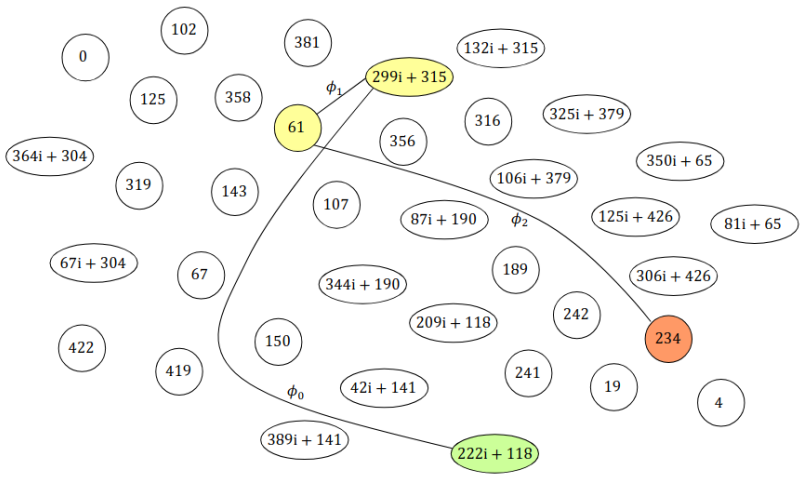

Рисунок 11 — Шаги агента Б

4 ЗАКЛЮЧЕНИЕ

Приход квантовых компьютеров угрожает большому количеству используемых алгоритмов, поэтому конфиденциальность информации фундаментально зависит от развития постквантового шифрования . Более того, оно стимулирует развитие криптографии в целом, повышая актуальность исследования как квантовых, так и неквантовых алгоритмов шифрования и взлома.

К счастью, этой области уделяется все больше внимания как со стороны государственных структур [8], так и частных компаний [9]. Например, NIST проводит отбор и стандартизацию алгоритмов постквантового шифрования. В процессе отбора были найдены важные уязвимости, в том числе в последнем раунде был взломан вышеописанный алгоритм SIDH, причем неквантовым алгоритмом [10]. Более тщательное изучение уже используемых алгоритмов (например, McEliece) повышает уверенность в том, что они действительно надежны в том числе против классических атак.

Задачи, лежащие в основе шифрования, опираются на новые, сложные абстракции. Использование этих задач в шифровании, поиск уязвимостей в алгоритмах приводит к более глубоким математическим исследованиям, развивая математическую область, на которую опирается шифрование.

Таким образом, потенциальное появление квантовых компьютеров повысило внимание, уделяемое безопасности информации, а оно, в свою очередь, дало толчок к развитию математических и криптографических направлений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Becker A.*, *Ducas L.*, *Gama N.*, *Laarhoven T.* New directions in nearest neighbor searching with applications to lattice sieving //. Vol. 1. — 01/2016. — P. 10–25.
2. *Ajtai M.* Generating hard instances of lattice problems (extended abstract) // Electron. Colloquium Comput. Complex. — 1996. — Vol. TR96. — URL: https://api.semanticscholar.org/CorpusID:6864824.
3. *Gentry C.*, *Peikert C.*, *Vaikuntanathan V.* How to Use a Short Basis: Trapdoors for Hard Lattices and New Cryptographic Constructions // Electronic Colloquium on Computational Complexity (ECCC). — 2008. — Sept. — Vol. 14.
4. *Ducas L.*, *Nguyen P.* Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures. — 2012. — Dec.
5. *Regev O.* On Lattices, Learning with Errors, Random Linear Codes, and Cryptography // Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing. — Baltimore, MD, USA : ACM, 2005. — P. 84–93. — (STOC '05). — URL: http://doi.acm.org/10.1145/1060590.1060603.
6. *Miret J.M.*, *Moreno Chiral R.*, *Rio A.* Generalization of Vélu's formulae for isogenies between elliptic curves // Publicacions Matematiques. — 2007. — June. — Vol. Proceed. I JTN. — P. 147–163.
7. *Costello C.* Supersingular Isogeny Key Exchange for Beginners //. — 01/2020. — P. 21–50.
8. Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now. — https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/.
9. Make It So: Software Speeds Journey to Post-Quantum Cryptography. — https://blogs.nvidia.com/blog/cupqc-quantum-cryptography.
10. SIKE Team: SIKE and SIDH is insecure. — 2022. — https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/sike-team-note-insecure.pdf.