«Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского» (ННГУ)

Институт информационных технологий, математики и механики
Кафедра: Алгебры, геометрии и дискретной математики

Направление подготовки: «Фундаментальная информатика и информационные технологии»

Алгоритмы шифрования, основанные на задачах о кратчайшем и ближайшем векторах решетки.

Выполнил: студент группы 381806-2

Напылов Евгений Игоревич

Научный руководитель: Доцент, кандидат физико-математических наук Веселов Сергей Иванович

Нижний Новгород
2022

Актуальность

Наиболее популярные алгоритмы шифрования с открытым ключом:

1. Rivest-Shamir-Adleman (RSA) → Задача факторизации целых чисел

2. Эллиптические кривые (ECC)
3. Diffie-Hellman (DH)
4. El Gamal

Задача дискретного логарифмирования

Проблема: Данные математические задачи могут быть решены за полиномиальное время с помощью квантового алгоритма Шора.

Возможное решение: Использование задач решеток в качестве основы алгоритмов шифрования.

Цель и задачи работы

- Объект – шифрование текста.
- Предмет – шифрование с использованием решеток.
- Цель – изучение алгоритмов шифрования на основе решеток и математических задач, лежащих в их основе.
- Задачи:
  - Изучение задач о кратчайшем и ближайшем векторах решетки и методов их решения.
  - Изучение алгоритмов шифрования GGH и NTRU.
  - Анализ безопасности алгоритмов с учетом различных видах атак.
  - Реализация алгоритма NTRU на языке программирования высокого уровня.

Понятие решетки

Решетка – подмножество линейного пространства.

Базис решетки – линейно-независимая система векторов.

$$(\vec{b}_1, \ldots, \vec{b}_n) \in \mathbb{R}^n$$

Решетка – множество L, элементами которого являются линейные комбинации базисных векторов с целыми коэффициентами.

$$L = \{ \sum_{i=1}^{n} l_i \vec{b}_i \mid l_i \in \mathbb{Z} \}$$

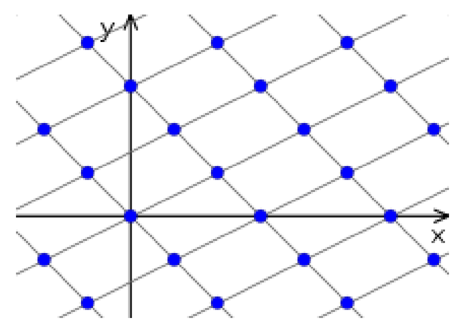

Рисунок 1. Двумерная решетка.

Задача о ближайшем векторе решетки

Дана решетка $L = \{ \sum_{i=1}^{n} l_i \vec{b}_i \mid l_i \in \mathbb{Z} \}$, $(\vec{b}_1, \ldots, \vec{b}_n) \in \mathbb{R}^n$

Задан вектор $\vec{w} \in \mathbb{R}^n$

Требуется найти вектор v из решетки L, для которого справедливо неравенство:

$$||\vec{v} - \vec{w}|| \leq ||\vec{x} - \vec{w}||, \ \forall \vec{x} \in L$$

Методы решения задачи о ближайшем векторе решетки

- Метод Бабая ближайшей плоскости

  Постепенное понижение размерности задачи

- Метод округления Бабая

  Разложение заданного вектора w по базису решетки с округлением коэффициентов до целых чисел.

$$\vec{w} = \sum_{i=1}^{n} \alpha_i \vec{b}_i \quad (\vec{b}_1, \ldots, \vec{b}_n)\vec{\alpha} = \vec{w} \quad \vec{v} = \sum_{i=1}^{n} \lfloor \alpha_i \rceil \vec{b}_i$$

- Метод вложения

  Сведение задачи ближайшего вектора v в решетке L к задаче кратчайшего вектора $[\vec{e}, M]$ в решетке с базисом $([\vec{b}_1, 0], \ldots [\vec{b}_n, 0], [\vec{w}, M])$

$$\vec{w} \approx \vec{v} = \sum_{i=1}^{n} l_i \vec{b}_i \quad \vec{e} = \vec{w} - \sum_{i=1}^{n} l_i \vec{b}_i \quad \vec{v} = \vec{w} - \vec{e}$$

Задача о кратчайшем векторе решетки

Дана решетка $L = \{ \sum_{i=1}^{n} l_i \vec{b}_i \mid l_i \in \mathbb{Z} \}, \ (\vec{b}_1, \ldots, \vec{b}_n) \in \mathbb{R}^n$

Требуется найти ненулевой вектор решетки, имеющий наименьшую длину.

$$\vec{v} \in L, \ ||\vec{v}|| = min||\vec{w}_i||, \forall \vec{w}_i \in L$$

Идея решения: Приведение базиса решетки к базису, который как можно ближе к ортогональному и как можно короче.

Методы решения задачи о кратчайшем векторе решетки

- Алгоритм Лагранжа-Гаусса редукции базиса (двумерный)

$$||\vec{b}_1|| \leq ||\vec{b}_2|| \leq ||\vec{b}_2 + q\vec{b}_1||, \forall q \in \mathbb{Z} \longrightarrow \vec{b}_1$$ - кратчайший вектор решетки

- Алгоритм Ленстры-Ленстры-Ловаса (LLL) редукции базиса

$$|\mu_{ij}| \leq \frac{1}{2} \ \forall i,j : 1 \leq j \leq i \leq n \quad \mu_{i,j} = \frac{(\vec{b}_i, \vec{b}_j^*)}{(\vec{b}_j^*, \vec{b}_j^*)} \qquad \longrightarrow ||\vec{b}_1|| \leq 2^{(n-1)/2}||\vec{v}||$$

$$(\vec{b}_i^*, \vec{b}_i^*) \geq (\sigma - \mu_{i,i-1}^2)(\vec{b}_{i-1}^*, \vec{b}_{i-1}^*) \ \forall i : 2 \leq i \leq n$$

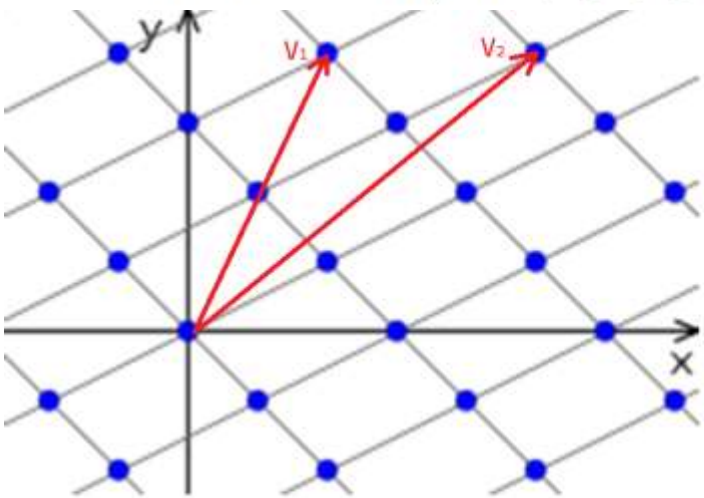

Рисунок 2. Исходный базис (“плохой”).

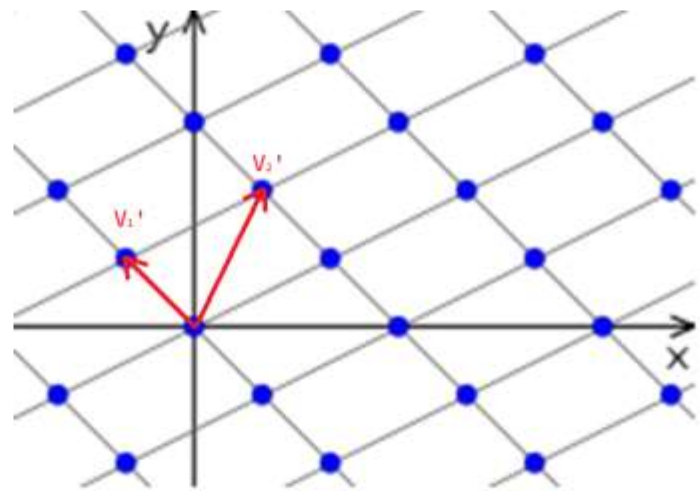

Рисунок 3. Редуцированный базис (“хороший”).

Схема шифрования GGH

- **Секретный ключ:** B - “хороший” базис решетки, унимодулярная матрица T
- **Публичный ключ:** B’ - “плохой” базис той же решетки, B’ = TB

- **Сообщение:** $\mathrm{m} \in Z^n$

- **Шифрование:** $c = mB' + e$, где
  $e = (\delta_1\sigma, \ldots, \delta_n\sigma)$, $\delta_i \in \{-1, 1\}$, σ - небольшое число

- **Дешифрование:**
  - $c' = cB^{-1} = mT + eB^{-1}$
  - Поиск ближайшего для с’ вектора решетки в базисе B с помощью метода округления Бабая.
  - Полученный ближайший вектор: mT
  - Для получения исходного сообщения: $m = mTT^{-1}$

Схема шифрования NTRU

Получатель

Секретные ключи
Случайные многочлены f и g, которые имеют обратные элементы по модулям p и q соответственно.

Публичный ключ
$$h = f_q * g \ (mod\ q)$$

Зашифрованное сообщение
e

Дешифрование
$$a = f * e \ (mod\ q)$$
$$\frac{-q}{2} \leq \alpha_i \leq \frac{q}{2}$$
$$m = f_p * a \ (mod\ p)$$

Исходное сообщение
m

Отправитель

Публичный ключ
$$h$$

Исходное сообщение
m

Случайный многочлен ϕ

Шифрование
$$e = p\phi * h + m \ (mod\ q)$$

Параметры NTRU:

- N – степень многочленов
- p << q – модули

Обозначение: f_p, f_q – обратные элементы по модулям

Атака на NTRU с помощью решетки

Условия: Известны параметры N, p, q, перехвачен публичный ключ h.

$$A = \begin{pmatrix} \alpha & 0 & \dots & 0 & h_0 & h_1 & \dots & h_{N-1} \\ 0 & \alpha & \dots & 0 & h_{N-1} & h_0 & \dots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \alpha & h_1 & h_2 & \dots & h_0 \\ 0 & 0 & \dots & 0 & q & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & q & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & q \end{pmatrix}$$

α – небольшое целое число

Строки матрицы образуют базис решетки L

Проблема: кратчайшим вектором решетки является $(\alpha f, g)$

Уровень безопасности	N	p	q
Минимальный	167	3	128
Стандартный	251	3	128
Высокий	347	3	128
Высочайший	503	3	256

Программная реализация NTRU. Схема приложения.

Библиотека NTL для работы с многочленами

Класс NTRU

- Генерация ключей
- Шифрование
- Дешифрование
- Конвертер строка ↔ многочлен
- Файловый ввод-вывод
- Прочие вспомогательные методы

Интерфейс командной строки

- Парсер аргументов
- Управление приложением

Графический интерфейс

- Файловые диалоги
- Предпросмотр файлов
- Управление приложением

Используемые технологии:

- C++
- NTL - многочлены
- OpenMP – производительность
- QT – графический интерфейс
- Python - автоматизация тестов

Программная реализация NTRU. Результаты.

В результате было создано 2 программных продукта:

1. Библиотека шифрования для C++
2. Полноценное приложение для шифрования файлов (с консольным и графическим интерфейсами)

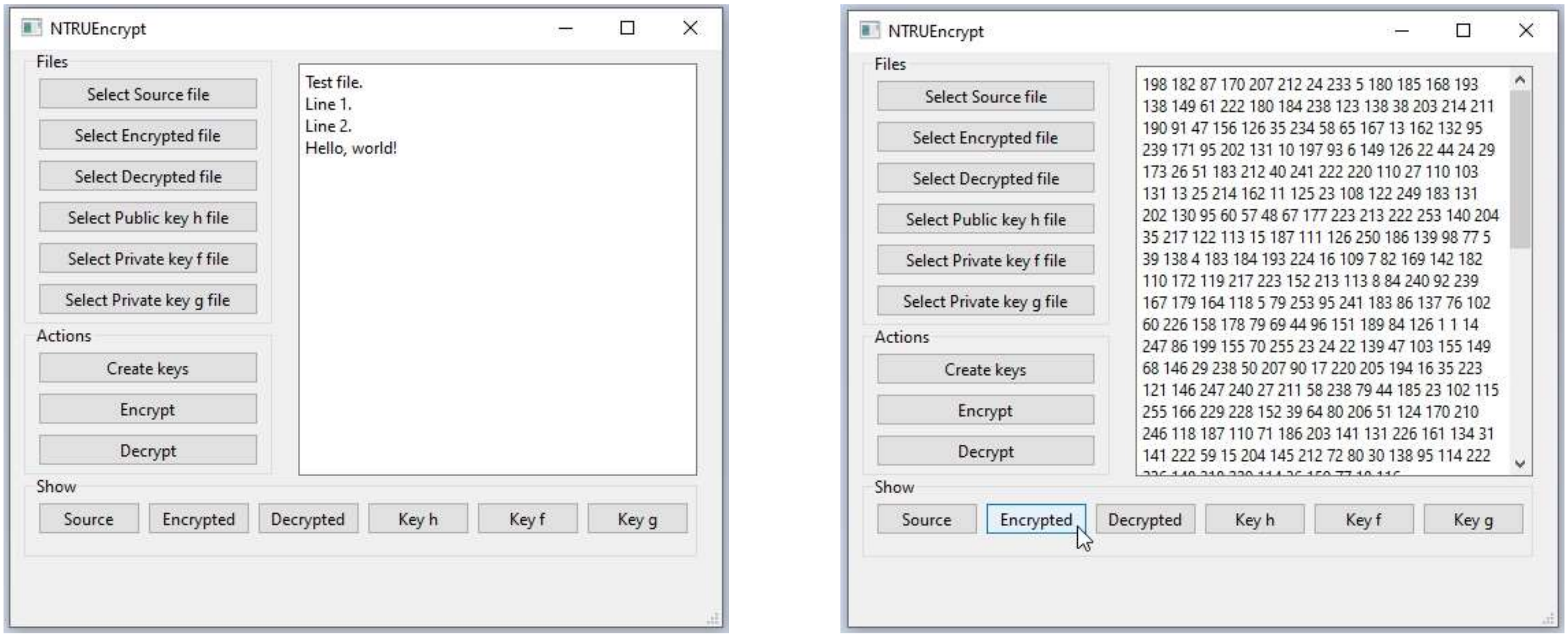

Рисунок 4. Демонстрация шифрования файла с помощью разработанной программы.

Программная реализация. Производительность.

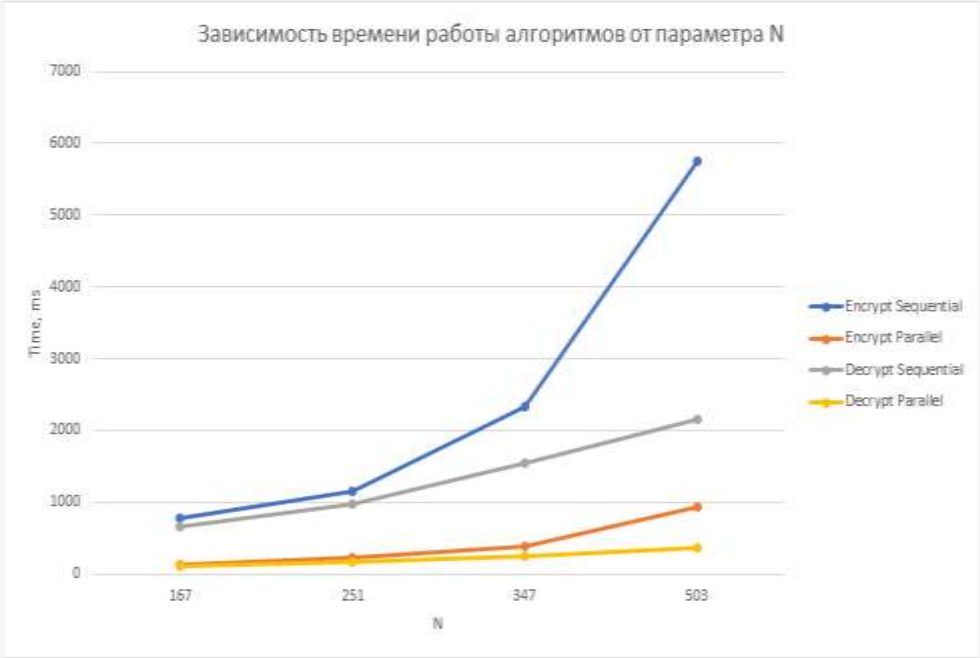

Рисунок 5. Зависимость производительности от параметра N.

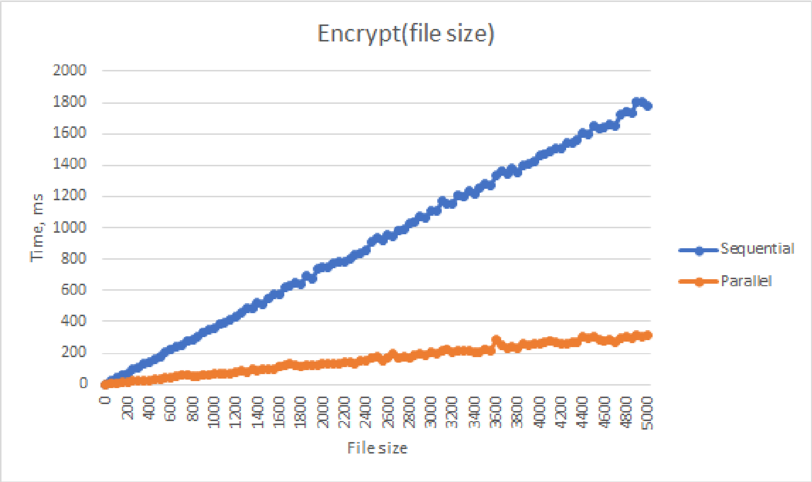

Рисунок 6. Зависимость производительности шифрования от числа символов в файле.

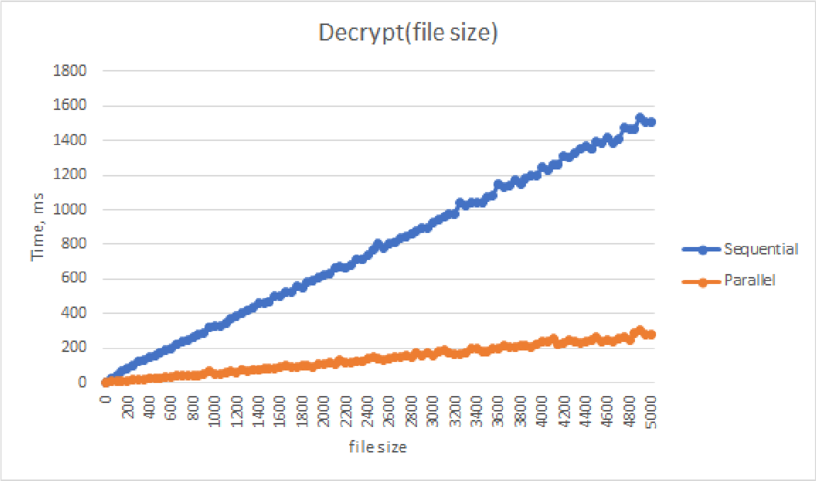

Рисунок 6. Зависимость производительности шифрования от числа символов в файле.

Зависимость от параметра N – полином 2-ой степени.

Зависимость от размера файла – линейная.

Заключение

- Были рассмотрены задачи о кратчайшем и ближайшем векторах решетки и алгоритмы решения.
- Рассмотрены алгоритмы шифрования GGH и NTRU, которые могут стать основными алгоритмами при переходе на квантовые компьютеры.
- Исследованы различные виды атак на данные криптосистемы.
- Разработана библиотека шифрования с помощью схемы NTRU для языка C++.
- Разработана конечная программа, позволяющая шифровать файлы с помощью схемы NTRU, обладающая графическим интерфейсом и интерфейсом командной строки для автоматизации действий с помощью командного интерпретатора ОС.

Список использованных источников и литературы

1. Шокуров А.В, Кузюрин Н.Н, Фомин С.А, Решетки, алгоритмы и современная криптография
2. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, NTRU: A Ring-Based Public Key Cryptosystem
3. Seong-Hun Paeng, Bae Eun Jung, and Kil-Chan Ha, A Lattice Based Public Key Cryptosystem Using Polynomial Representations
4. Joseph H. Silverman, NTRU and Lattice-Based Crypto: Past, Present, and Future
5. S. D. Galbraith, Mathematics of public key cryptography, Cambridge University Press, April 2012
6. Abderrahmane Nitaj, The Mathematics of the NTRU Public Key Cryptosystem
7. NTL: A Library for doing Number Theory (documentation) https://libntl.org/doc/tour.html
8. Xagawa D. K. Cryptography with lattices. – 2010
9. e Micheli G., Heninger N., Shani B. Characterizing overstretched NTRU attacks //Journal of Mathematical Cryptology. – 2020. – Т. 14. – No. 1. – С. 110-119
10. Комарова А. В. и др. Теоретические возможности комбинирования различных математических примитивов в схеме электронной цифровой подписи //Кибернетика и программирование. – 2017. – No. 3. – С. 80-92