МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт искусственного интеллекта

Базовая кафедра информационной безопасности № 252

КУРСОВАЯ РАБОТА

по дисциплине

«Криптографические методы защиты информации»

Тема курсовой работы

«Постквантовая криптография и алгоритм NTRU»

Студентка группы ККСО-03-19: Никишина А.А. _____

Руководитель курсовой работы: Бондакова О.С. _____

Работа представлена к защите «____» _____ 2023 г.

Допущен к защите «____» _____ 2023 г.

Москва 2023

Содержание

1. Введение

1.1. Введение в криптографию и ее роль в современном информационном обществе

Криптография - это наука об обеспечении безопасности информации с помощью использования математических методов и алгоритмов. С ее помощью информация может быть зашифрована таким образом, что доступ к ней имеют только те, кому предоставлены соответствующие ключи. Криптография играет важную роль в современном информационном обществе, обеспечивая конфиденциальность, целостность и аутентичность данных.

Одной из основных целей криптографии является защита конфиденциальности данных. В цифровой эпохе большое количество информации передается и хранится в электронном виде. Криптография позволяет зашифровать данные таким образом, что они становятся непонятными для посторонних лиц. Только тот, кто имеет соответствующий ключ, сможет расшифровать данные и получить доступ к ним. Это особенно важно для передачи конфиденциальной информации, такой как банковские данные, медицинские записи, персональные сообщения и т.д.

Криптография также обеспечивает целостность данных. Она позволяет проверить, не были ли данные изменены или повреждены в процессе передачи или хранения. Для этого используются хэш-функции и цифровые подписи.

Аутентификация – еще один важный аспект криптографии. С ее помощью можно проверить, что информация или сущность, с которой ведется общение, является действительной. Это особенно важно в сети Интернет, где существует риск подделки или манипуляции данных. Криптографические протоколы аутентификации позволяют установить взаимное доверие между сторонами и обеспечить безопасность коммуникации.

В современном информационном обществе криптография имеет широкое применение. Она используется в системах малого бизнеса, банковских операциях, государственных системах безопасности, облачных сервисах и многих других областях. Без надежных криптографических методов и алгоритмов было

бы практически невозможно обеспечить безопасность и конфиденциальность информации, а также защититься от кибератак и хакерских атак.

Однако криптография не является статической областью. Она постоянно развивается и адаптируется к новым вызовам и угрозам. Криптографы постоянно работают над созданием новых алгоритмов и протоколов, а также анализируют существующие системы на уязвимости. Это важно, чтобы быть шаг впереди потенциальных злоумышленников и обеспечить безопасность информации в будущем.

Также, криптография играет неотъемлемую роль в современном информационном обществе. Она обеспечивает конфиденциальность, целостность и аутентичность данных, защищает от кибератак и гарантирует безопасность коммуникации. Понимание основных принципов и методов криптографии является важным для всех, кто работает с информацией и стремится обеспечить ее защиту в современном цифровом мире.

1.2. Концепция постквантовой криптографии и её необходимость

В последние несколько десятков лет, появилось новое направление в криптографии – постквантовая криптография. Это область, которая изучает методы и алгоритмы, способные справиться с угрозами, связанными с будущим развитием квантовых компьютеров. Для понимания необходимости постквантовой криптографии, важно ознакомиться с основами квантовых вычислений.

Квантовые компьютеры – это компьютеры, которые основаны на принципах квантовой механики и способны выполнять определенные вычисления гораздо быстрее, чем классические компьютеры. Они обладают свойством квантовой суперпозиции, которое позволяет им обрабатывать не только 0 и 1 (биты), как классические компьютеры, но и комбинации этих состояний - кубиты.

Однако возникает проблема: квантовые компьютеры могут быть способны взламывать некоторые существующие криптографические алгоритмы, основанные на сложности факторизации или решения дискретного логарифма. Например, алгоритм Шора, разработанный Питером Шором в 1994 году, поз-

воляет эффективно факторизовать большие числа на квантовом компьютере, что подрывает безопасность многих современных криптографических протоколов.

Здесь нам и становится необходимой постквантовая криптография. Она предлагает новые алгоритмы и протоколы, которые устойчивы к атакам, проводимым с использованием квантовых компьютеров. Основная идея заключается в использовании математических задач, которые сложно решить как на классическом, так и на квантовом компьютере.

Примером алгоритма постквантовой криптографии является криптосистема на основе решетки (Lattice-based cryptography). Она основана на сложности решения задач, связанных с математическими структурами, известными как решетки. Решетки представляют собой сетку точек в многомерном пространстве, и решение задач, связанных с решетками, требует значительных вычислительных ресурсов.

Другим примером является код Мак-Элиса (McEliece code-based cryptosystem), основанный на сложности декодирования полных линейных кодов. Этот алгоритм использует линейные коды для шифрования данных и сложную задачу декодирования, которая на классическом компьютере требует больших вычислительных затрат, а на квантовом компьютере остается вычислительно сложной.

Постквантовая криптография не только предлагает новые алгоритмы, но и требует разработки новых стандартов безопасности, которые учитывают потенциальные угрозы со стороны квантовых компьютеров. В этом процессе важно сотрудничество между криптографами, учеными и индустрией для разработки и внедрения новых стандартов.

Постквантовая криптография становится все более важной в современном информационном обществе. Хоть и на данный момент квантовые компьютеры не получили широкого распространения, их развитие создает потенциальную угрозу для существующих криптографических систем. Постквантовая криптография предлагает новые методы и алгоритмы, которые способны справиться с этими угрозами и обеспечить безопасность передачи и хранения информации в будущем.

1.3. Обзор алгоритма NTRU и его применимости в постквантовой криптографии

NTRU (Nth degree Truncated Polynomial Ring Unit) – это семейство алгоритмов, которые были разработаны в 1996 году Майклом Одом, Жаклином Шеном и Робертом Силверманом. NTRU относится к криптографическим системам на основе решеток и становится все более актуальным с развитием постквантовой криптографии.

Основная идея алгоритма NTRU состоит в использовании математических операций над полиномами для шифрования и расшифровки данных. Он основан на арифметике кольца многочленов, а именно на многочленах над модулем и их операциях сложения и умножения. Главным преимуществом NTRU является его относительная вычислительная эффективность и высокая скорость работы.

Алгоритм NTRU использует два основных ключа: открытый ключ и закрытый ключ. Открытый ключ используется для шифрования данных, а закрытый ключ - для их расшифровки. Одним из главных преимуществ NTRU является его устойчивость к квантовым атакам. Алгоритм основан на сложной задаче решетки, известной как задача SIS (Short Integer Solution), которая остается вычислительно сложной даже для квантовых компьютеров.

Задача SIS (Short Integer Solution) - это одна из ключевых задач, используемых в постквантовой криптографии. Она заключается в поиске короткого вектора целых чисел, удовлетворяющего определенным условиям. Более конкретно, задача SIS связана с поиском короткого вектора в решетке, который является решением линейных уравнений с ограниченной длиной вектора.

Сложность задачи SIS заключается в том, что поиск короткого вектора в решетке является NP-трудной задачей, то есть не существует эффективного алгоритма, способного решить ее за полиномиальное время. Это делает задачу SIS привлекательной для использования в криптографии, так как сложность ее решения создает трудности для потенциальных злоумышленников или атакующих.

Помимо своей устойчивости к квантовым атакам, NTRU обладает и дру-

гими преимуществами. Он имеет малый размер ключа, что делает его более эффективным для применения в ресурсоограниченных средах, таких как мобильные устройства и Интернет вещей. Кроме того, NTRU имеет высокую скорость работы и хорошую производительность при шифровании и расшифровке данных.

Применимость алгоритма NTRU в постквантовой криптографии связана с его способностью предоставить безопасность даже в условиях развития квантовых компьютеров. Поскольку алгоритм основан на решетках, которые сложно атаковать с использованием квантовых вычислений, NTRU может быть использован для обеспечения безопасной передачи и хранения информации в будущем.

Несмотря на свои преимущества, алгоритм NTRU имеет и некоторые ограничения. Он требует определенного выбора параметров для достижения оптимальной безопасности, и эти параметры должны быть выбраны с учетом текущих знаний о криптоанализе и вычислительных возможностях. Кроме того, NTRU не является широко распространенным алгоритмом в настоящее время, поэтому его реализации и поддержка могут быть ограничены.

Подытоживая вышесказанное, алгоритм NTRU представляет собой эффективное и устойчивое квантовым атакам решение в области постквантовой криптографии. Он основан на математических операциях над полиномами и предлагает высокую скорость работы и надежную защиту данных. Применение NTRU может быть ценным для обеспечения безопасности информации в условиях быстрого развития квантовых компьютеров.

2. Основная часть

2.1. Обзор постквантовой криптографии

2.1.1. Уязвимости классической криптографии перед квантовыми вычислениями

Одной из основных уязвимостей классической криптографии перед квантовыми вычислениями является факторизация больших чисел. Некоторые популярные алгоритмы шифрования, такие как RSA, основаны на сложности факторизации больших простых чисел. Однако с использованием квантовых алгоритмов, таких как алгоритм Шора, квантовый компьютер может эффективно факторизовать большие числа, что подрывает безопасность таких шифров.

Еще одной уязвимостью является дискретный логарифм. Многие криптографические протоколы, включая Diffie-Hellman и эллиптическую криптографию, основаны на сложности вычисления дискретного логарифма. Квантовые алгоритмы, такие как алгоритм Гровера, могут решать эту задачу значительно быстрее, чем классические алгоритмы, что может угрожать безопасности данных, защищенных такими протоколами.

Кроме того, некоторые криптосистемы, такие как системы на основе эллиптической криптографии, могут быть уязвимы к атакам Гилберта-Мэтьюса-Нидхема (GMN-атакам), которые используют квантовые вычисления для нахождения секретного ключа, используемого в криптосистеме.

Для структурирования этих проблем классической криптографии, составим таблицу.

Уязвимость	**Описание**	**Влияние квантовых вычислений**
Факторизация больших чисел	Некоторые алгоритмы шифрования, например RSA, основаны на сложности факторизации больших простых чисел.	Квантовые алгоритмы, включая алгоритм Шора, могут эффективно факторизовать большие числа, угрожая безопасности таких шифров.
Дискретный логарифм	Многие криптографические протоколы, такие как Diffie-Hellman и эллиптическая криптография, основаны на сложности вычисления дискретного логарифма.	Квантовые алгоритмы, например алгоритм Гровера, могут решать задачу дискретного логарифма значительно быстрее, чем классические алгоритмы, что создает угрозу для безопасности данных, защищенных такими протоколами.
GMN-атаки на системы на основе эллиптической криптографии	Некоторые криптосистемы на основе эллиптической криптографии могут быть уязвимы к атакам Гилберта-Мэтьюса-Нидхема (GMN-атаки), которые используют квантовые вычисления для нахождения секретного ключа.	Квантовые алгоритмы могут сократить время атаки GMN и подорвать безопасность систем на основе эллиптической криптографии.

Таблица 1: Уязвимости классической криптографии.

2.1.2. Постановка задачи разработки постквантовых криптосистем

Постановка задачи разработки постквантовых криптосистем включает следующие ключевые аспекты:

1) Алгоритмы устойчивые к квантовым атакам: Необходимо исследовать и разработать новые криптографические алгоритмы, которые будут устой-

чивы к атакам квантовыми вычислениями. Эти алгоритмы должны использовать математические задачи, которые квантовые компьютеры не могут решать существенно быстрее, чем классические компьютеры.

2) Аутентификация и цифровые подписи: Постквантовые криптосистемы должны обеспечивать надежную аутентификацию и возможность создания цифровых подписей. Это важно для подтверждения подлинности отправителя и целостности передаваемых данных.

3) Защита от атак с использованием квантовых алгоритмов: Постквантовые криптосистемы должны быть устойчивы к атакам с использованием квантовых алгоритмов, таких как алгоритм Шора или алгоритм Гровера. Защита от этих атак требует применения новых математических методов и алгоритмов.

4) Эффективность и вычислительная сложность: Разработанные постквантовые криптосистемы должны быть эффективными с точки зрения вычислительной сложности. Они должны работать на практических компьютерах с разумными ресурсами и обеспечивать приемлемую производительность.

5) Стандартизация и принятие: Для широкого принятия и использования постквантовых криптосистем необходимы стандарты и протоколы, которые будут поддерживаться различными платформами и системами. Это важно для обеспечения совместимости и взаимодействия между различными системами и устройствами.

2.1.3. Обзор основных подходов к постквантовой криптографии

1) Криптография на основе решеток:

   - *Описание:* Этот подход использует математические задачи на основе решеток для создания постквантовых криптосистем. Задача SIS (Short Integer Solution) и задача LWE (Learning With Errors) являются примерами таких задач.

Обучение с ошибками (Learning with errors, LWE) – задача нахождения многочлена с коэффициентами из определённого кольца вычетов, для которого дана система линейных уравнений, в которой есть ошибки (что делает простую вычислительную задачу сложной).

- *Преимущества:* Алгоритмы на основе решеток обеспечивают безопасность относительно квантовых атак, имеют эффективные математические основы и хорошо исследованы.
- *Недостатки:* Некоторые алгоритмы на основе решеток могут быть вычислительно сложными и требовать больших вычислительных ресурсов.

2) Криптография на основе кодов:

- *Описание:* В этом подходе используются коды, которые могут обеспечить защиту информации от квантовых атак. Примерами являются коды Мак-Элиса и коды Нидхема-Лутца.
- *Преимущества:* Алгоритмы на основе кодов обладают высокой степенью безопасности относительно квантовых вычислений, а также имеют низкую вычислительную сложность.
- *Недостатки:* Криптография на основе кодов может иметь ограниченную пропускную способность и требовать больших объемов хранилища.

3) Криптография на основе множеств:

- *Описание:* Этот подход использует задачи, связанные с множествами, для создания постквантовых криптосистем. Примером такой задачи является задача суммы подмножества.
- *Преимущества:* Криптография на основе множеств обеспечивает высокую степень безопасности относительно квантовых атак и имеет небольшую вычислительную сложность.

- *Недостатки:* Некоторые алгоритмы на основе множеств могут быть более сложными для реализации и требовать больше вычислительных ресурсов.

4) Криптография на основе графов:

   - *Описание:* В этом подходе используются задачи, связанные с графами, для создания постквантовых криптосистем. Примерами таких задач являются задача коммивояжера и задача кратчайшего пути.
   - *Преимущества:* Алгоритмы на основе графов обладают высокой безопасностью относительно квантовых вычислений и имеют простую структуру.
   - *Недостатки:* Некоторые алгоритмы на основе графов могут быть вычислительно сложными и требовать больших ресурсов.

2.2. Алгоритм NTRU

2.2.1. Общее описание алгоритма NTRU

NTRUEncrypt, изначально называвшийся NTRU, был изобретён в 1996 году и представлен миру на конференциях CRYPTO[en], Конференция RSA, Eurocrypt[en]. Причиной, послужившей началом разработки алгоритма в 1994 году, стала статья «Algorithms for quantum computation: discrete logarithms and factoring», в которой говорилось о лёгкости взлома существующих алгоритмов на квантовых компьютерах, которые, как показало время, не за горами. В этом же году, математики Jeffrey Hoffstein, Jill Pipher и Joseph H. Silverman, разработавшие систему вместе с основателем компании NTRU Cryptosystems, Inc. (позже переименованной в SecurityInnovation), Даниелем Лиеманом (Daniel Lieman) запатентовали своё изобретение.

Криптосистема NTRU (N-th degree truncated polynomial ring) основана на алгебраической структуре полиномиального кольца. Поиск кратчайшего вектора в заданной числовой решетке – трудноразрешимая задача. NTRU относят к быстрым криптосистемам – ее можно использовать в устройствах с

ограниченными ресурсами, поэтому она эффективна и возможно ее дальнейшее применение и развитие.

2.2.2. Разбор шагов алгоритма: основы криптосистемы, шифрование, дешифрование

Основы криптосистемы. Пусть R — полиномиальное кольцо с неприводимым многочленом $R = \frac{Z[x]}{(x^N - 1)}$. В таком кольце произведение (обозначается $*$) задается не как обычное произведение многочленов, а как «произведение свертки», то есть X^N заменяется на 1, X^{N+1} – на X и так далее. Такое кольцо R называют *кольцом усеченных многочленов*. Необходимые параметры криптосистемы – это N (размерность кольца R), p и q – два взаимно простых в R числа (обычно q – большое). Многочлены $f \in R$ и $g \in R$ выбираются пользователем Бобом так, чтобы многочлен f был обратим в R. Боб вычисляет f_q^{-1} и f_p^{-1} в кольцах $R = \frac{Z[x]}{(q, x^N - 1)}$ и $R = \frac{Z[x]}{(p, x^N - 1)}$ соответственно. Для генерации открытого ключа Боб вычисляет многочлен h: $h = f_q^{-1} * g \mod q$.

Шифрование. Для шифрования текста $m \in R$ Алиса (сторона, желающая отослать сообщение) использует открытый ключ Боба (сторона, принимающая сообщение) h, выбирает случайным образом многочлен $r \in R$ и вычисляет e (шифр-текст): $e \equiv r * h + m \mod q$.

Дешифрование. Используя свой секретный ключ, Боб вычисляет: $a \equiv f * e \mod q$. Коэффициенты для a Боб выбирает так, чтобы они лежали в интервале $(-0.5q, 0.5q)$. Затем он приводит многочлен a по модулю p и вычисляет $f_q^{-1} * a \mod p$. Полученное значение есть m.

Для более наглядной демонстрации работы алгоритма опишем основную цепочку сравнений.
Когда Боб вычисляет сравнение $a \equiv f * e \mod q$, в действительности:

$a \equiv f * e \mod q = f * (r * h + m) \mod q =$ [так как $e \equiv r * h + m \mod q$]
$= f * (r * p \cdot f_q * g + m) \mod q =$ [так как $h = p \cdot f_q^{-1} * g \mod q$]
$p \cdot r * g + f * m \mod q$ [так как $f * f_q = 1 \mod q$].
$b = f * m \mod p$; $f_p * b = f_p * f + m = m \mod p$.

2.2.3. Методы оптимизации алгоритма NTRU

Разберем некоторые методы оптимизации параметров NTRU.

1) Большую часть времени занимают вычисления произведений в кольце и нахождения обратных. Поэтому для уменьшения времени выполнения представим секретный ключ f в виде: $1 + p \cdot f_1 \cdot f_1 \in R$. Тогда $f_p^{-1} = 1$, и необходимость вычислять обратный по $\mod p$, и второе произведение при дешифровании исчезает.

2) Необязательно p быть целым, p может быть и многочленом, главное, чтобы p и q были взаимно просты в кольце R. При выборе $p = X + 2$ имеем все требования криптосистемы (взаимная простота эквивалентна тому, что элементы p, q и $X^N - 1$ образуют единичный идеал в $Z[X]$) и отображение бинарный многочлен m(x) $\to R/pR$ инъективно.

Открытый и секретный ключи криптосистемы – многочлены, их можно представить в виде векторов, а вектора, в свою очередь, – в виде векторов n-мерных числовых решеток. Рассмотрим основные шаги.
Секретные ключи Боба (f, g) представим в виде короткого вектора $(f, g) \in Z^{2n}$. Решетка этих секретных параметров будет q-ичной решеткой $\Delta_q((T \cdot f, T \cdot g)^T)$. При таких условиях открытый ключ будет выглядеть $H = \begin{bmatrix} I & 0 \\ T \cdot h & q \cdot I \end{bmatrix}$, где $h = (T \cdot f)^{-1} \cdot g \mod q$.
Зашифровка текста $m\{1, 0, -1\}^n$ с $d_f + 1$ положительных единиц и с d_f отрицательных производится с помощью наугад выбранного вектора $r \in \{1, 0, -1\}^n$ по схеме: $\begin{bmatrix} -r \\ m \end{bmatrix} \mod \begin{bmatrix} I & 0 \\ T \cdot h & q \cdot I \end{bmatrix} = \begin{bmatrix} 0 \\ (m + [T \cdot h] \cdot r) \mod q \end{bmatrix}$ (редукция вектора ошибок (-r, m) по базису H). Первые n координат всегда нулевые, а n-размерное векторное пространство $(m + [T \cdot h] \cdot r) \mod q = c$ и будет зашиф-

рованным сообщением.
Расшифровывается сообщение умножением шифр-текста c на матрицу $[T \cdot f] \mod q$.

Зашифровка текста длиной $(n-k) \cdot \log_2 p$ бит займет $O(n^2)$ арифметических операций, столько же расшифровка сообщения (длина шифр-текста $n \cdot \log_2 q$ бит). Тогда длины секретного и открытого ключей равны $2n \cdot \log_2 p$ бит и $n \cdot \log_2 q$ бит.

2.2.4. Анализ преимуществ и недостатков алгоритма NTRU

Воспользуемся сравнительной таблицей криптосистем NTRU, RSA, McEliece и GHH.

Параметры шифрования	NTRU	RSA	McEliece	GGH
Скорость шифрования	N^2	N^2	N^2	N^2
Скорость дешифрования	N^2	N^3	N^2	N^2
Длина открытого ключа	N	N	N^2	N^2
Длина секретного ключа	N	N	N^2	N^2

Таблица 2. Сравнительная таблица криптосистем (N — параметр безопасности)

По ней видно, что криптосистема NTRU выигрывает у последних двух за счет длины открытого и секретного ключей (длины ключей в McEliece и GHH равны N^2), а у RSA – за счет высокой скорости шифрования/дешифрования и создания ключей.

Наиболее очевидный способ взлома NTRU – атака перебором. Злоумышленник может искать:

1) секретный ключ f, подбирая его так, чтобы $f * h \mod q$ было небольшим;

2) многочлен g, подбирая его так, чтобы $g * h^{-1} \mod q$ было небольшим;

3) вектор ошибок r, проверяя $e - r * h \mod q$.

Пытаясь отыскать секретный ключ f (f представлен как $f = 1 + p \cdot F$), мы точно знаем, что первая координата этого многочлена равна 1. Тогда при полном

переборе векторов (а именно так удобнее представлять многочлен) останется проверить $\begin{bmatrix} 2 \\ N-1 \end{bmatrix}$ всевозможных вариантов для f (поворотов оставшихся $d_f - 1$ единиц), при этом проверяя произведение $f * h$ (это произведение есть многочлен g и оно состоит из 0 и 1). Такой многочлен появится d_f раз среди $\begin{bmatrix} 2 \\ N-1 \end{bmatrix}$, поскольку существует d_f поворотов многочлена f с единицей на первом месте. Злоумышленнику останется отыскать подходящий ключ из этих d_f многочленов.

Существуют и другие способы, которыми злоумышленник может «взломать» криптосистему. Один из них – атака «метод встречи посередине». Главный ее момент — представление $f : (f_1 + f_2) * h = g$. Для коэффициентов это уравнение перепишем так: $(f_1 * h)[i] = -(f_2 * h)[i] + 0$ или 1. Поэтому злоумышленник будет перебирать всевозможные значения f_1 и f_2 , замечая, что полученные коэффициенты вектора f_2 должны отличаться от коэффициентов f_1 не более чем на 1 (все вычисления проводятся по модулю q). Таких совпадений получится $d_f!$ (для «лидирующей» единицы существует $(d_f - 1)!$ положений $(d_f - 1)$ единиц). Злоумышленнику останется проверить их.

Также существует атака с подобранным шифротекстом. С практической точки зрения её можно считать самой опасной для данного алгоритма.

1) Атакующий создает шифротекст $C(x) = y * h(x) + y$ (где y целое число, а h(x) открытый ключ Алисы) и отправляет его Алисе.

2) При попытке расшифровать сообщение Алиса вычисляет $a = f(x) * C(x) \mod q = y * f(x) * h(x) + y * f(x) \mod q = y * g(x) + y * f(x) \mod q$ т.к. многочлены g(x) и f(x) имеют коэффициенты -1,0,1, то коэффициенты многочлена a принадлежат множеству 0,y,-y,2y,-2y. Получается, что если атакующий выбрал y, таким что y<q/2 и 2y>q/2, то при сведении a(x) по модулю q, изменяются только те элементы многочлена a(x) коэффициенты у которых равны $\pm 2y$.

3) Представим теперь, что i-й коэффициент $a_i = 2y$, тогда

$a(x) \mod q = y*g(x)+y*f(x)-q*x^i$ и значит окончательное сообщение после расшифровки приобретает вид:
$f_p(x) * a(x) = y * f_p(x) * g(x) + y * f(x) * f_p(x) - q * x^i * f_p(x) \mod p$.
Т.о. если атакующий выбирает у делящимся нацело на p, то в результате получается многочлен $z(x) = -q * x^i * f_p(x) \mod p$

4) Для вычисления секретного ключа Алисы, осталось всего-навсего вычислить $-q * z^{-1}(x) * x^i \mod p$

Применяя данную схему атаки, противник может восстановить секретный ключ с вероятностью P=0.13 или, грубо говоря, для восстановления секретного ключа атакующему потребуется отправить всего порядка 10 подобранных шифротекстов.

Существенным недостатком данного алгоритма является необходимость использования только рекомендованных параметров. Именно такое же требование вызывало всеобщее недовольство во время перехода на эллиптические кривые и способствовало всяческими подозрениям о наличии бэкдоров.

	N	p	q	*df*	*dg*	*dr*
NTRU167:3	167	3	128	61	20	18
NTRU251:3	251	3	128	50	24	16
NTRU503:3	503	3	256	216	72	55
NTRU167:2	167	2	127	45	35	18
NTRU251:2	251	2	127	35	35	22
NTRU503:2	503	2	253	155	100	65

Таблица 3. Таблица рекомендованных параметров для NTRU

2.3. Применение алгоритма NTRU в постквантовой криптографии

2.3.1. Рассмотрение решений, основанных на алгоритме NTRU, для защиты различных типов данных и коммуникаций

Алгоритм NTRU предлагает эффективные решения для защиты различных типов данных и коммуникаций в постквантовую эпоху. Вот несколько примеров применения алгоритма NTRU для защиты данных и коммуникаций:

1) Шифрование данных:
   Алгоритм NTRU может быть использован для шифрования конфиденциальных данных, таких как файлы, сообщения или базы данных. При использовании NTRU для шифрования данных, отправитель преобразует исходные данные в шифротекст с использованием открытого ключа получателя. Затем получатель может дешифровать шифротекст, используя свой закрытый ключ. Это обеспечивает конфиденциальность данных и защиту от квантовых атак.

2) Защита коммуникаций:
   Алгоритм NTRU может быть использован для защиты коммуникаций между двумя или более участниками. Он может быть применен для шифрования и расшифровки сообщений, передаваемых через сеть, обеспечивая конфиденциальность и целостность данных. Кроме того, алгоритм NTRU может использоваться для аутентификации сообщений, позволяя проверить, что сообщение было отправлено именно от ожидаемого отправителя.

3) Цифровые подписи:
   Алгоритм NTRU также может быть использован для создания и проверки цифровых подписей. Цифровая подпись, созданная с использованием закрытого ключа отправителя, позволяет получателю убедиться в подлинности отправителя и целостности данных. Алгоритм NTRU обеспечивает высокую степень безопасности при создании и проверке цифровых

подписей, что делает его привлекательным в постквантовую эпоху.

4) Защита инфраструктуры облачных вычислений:
   Алгоритм NTRU может быть использован для защиты инфраструктуры облачных вычислений, где данные и вычисления могут быть переданы между различными узлами. Использование NTRU для шифрования данных и аутентификации может обеспечить безопасность и конфиденциальность в облачных средах, где присутствует высокий уровень сетевой и информационной уязвимости.

Алгоритм NTRU предоставляет мощные инструменты для защиты различных типов данных и коммуникаций в постквантовую эпоху. Его эффективность, скорость и сопротивляемость квантовым вычислениям делают его привлекательным выбором для различных сценариев применения в области криптографии и информационной безопасности.

2.3.2. Обзор существующих примеров применения алгоритма NTRU в реальных системах

Обзор существующих примеров применения алгоритма NTRU в реальных системах демонстрирует его широкую применимость в различных областях. Вот несколько конкретных примеров использования алгоритма:

1) NTRU в области защиты данных и коммуникаций:
   - Фирма Security Innovation: Компания Security Innovation внедрила алгоритм NTRU в свою систему SecureMail, обеспечивая защиту конфиденциальности электронной почты. Это позволяет пользователям отправлять и получать шифрованные сообщения с использованием NTRU.
   - Проект PQCRYPTO: В рамках проекта PQCRYPTO, исследователи из разных университетов и организаций проводят исследования и разработки по различным постквантовым криптосистемам, включая алгоритм NTRU.

2) NTRU в области защиты IoT и мобильных устройств:

- Фирма Entrust: Компания Entrust использует алгоритм NTRU для защиты коммуникаций и данных в рамках своих решений для IoT-устройств. Это обеспечивает безопасность передачи данных и защиту от атак в контексте Интернета вещей.
- Проект PQShield: PQShield - стартап, который занимается разработкой постквантовых криптографических решений. Они проводят исследования и разработки, включая использование алгоритма NTRU для защиты мобильных устройств и IoT-устройств.

3) NTRU в области защиты сетевых протоколов:

- Проект Open Quantum Safe (OQS): OQS является проектом с открытым исходным кодом, который разрабатывает и предоставляет реализации постквантовых криптографических алгоритмов, включая NTRU. Их цель - предоставить безопасные альтернативы классическим криптографическим алгоритмам для защиты сетевых протоколов.
- Протокол New Hope: Протокол New Hope использует алгоритм NTRU для защиты протоколов обмена ключами в сетях. Он обеспечивает безопасную передачу данных в условиях уязвимости классической криптографии перед квантовыми вычислениями.

Это лишь несколько примеров использования алгоритма NTRU в реальных системах. Следует отметить, что применение алгоритма NTRU продолжает активно исследоваться и разрабатываться, и в будущем ожидаются новые примеры его использования в различных сферах информационной безопасности и криптографии.

3. Заключение

В ходе курсовой работы были рассмотрены основные аспекты постквантовой криптографии и алгоритма NTRU. Целью данного исследования было изучить концепцию постквантовой криптографии и рассмотреть применение алгоритма NTRU в данной области.

В рамках работы был проведен обзор постквантовой криптографии, включающий изучение основных уязвимостей классической криптографии перед квантовыми вычислениями. Были рассмотрены основные подходы к постквантовой криптографии, включая алгоритм NTRU.

Был проведен детальный анализ алгоритма NTRU, включая его общее описание, шаги генерации ключей, шифрования и дешифрования. Также были обсуждены преимущества и недостатки данного алгоритма. Подробно рассмотрены различные применения алгоритма NTRU в постквантовой криптографии, включая защиту данных и коммуникаций.

Исходя из проведенного исследования, можно сделать следующие выводы:

Во-первых, постквантовая криптография представляет собой актуальное направление в области информационной безопасности, которое становится все более важным с учетом возможных угроз со стороны квантовых вычислений. Она обеспечивает надежные методы шифрования и аутентификации, способные справиться с вычислительной мощностью квантовых компьютеров.

Во-вторых, алгоритм NTRU является одним из перспективных исследовательских направлений в постквантовой криптографии. Он обладает эффективностью и хорошей стойкостью к атакам, а также имеет широкий спектр применений в различных областях.

Однако, необходимо отметить, что постквантовая криптография и алгоритм NTRU все еще являются активными областями исследований. Существуют открытые вопросы и вызовы, требующие дальнейших исследований и разработок. Безопасность алгоритма NTRU должна быть тщательно исследована и проверена перед его широким применением в реальных системах.

В заключение хотелось бы сказать что, данная работа представляет важ-

ность постквантовой криптографии и алгоритма NTRU для обеспечения безопасности в условиях квантовых вычислений. Исследования и разработки в этой области продолжаются, и они имеют потенциал для создания эффективных методов защиты информации в будущем.

С учетом актуальности и перспективности постквантовой криптографии и алгоритма NTRU, можно придти к выводу, что дальнейшие исследования и разработки в этой области будут играть важную роль в обеспечении безопасности информации в постквантовой эпохе.

4. Список литературы

1) Научно-образовательный журнал для студентов и преподавателей «StudNet» №3/2021. «Криптосистема Мак-Элиса и проблемы её внедрения» – Баев Д.А.

2) «АНАЛИЗ СТРУКТУРЫ И СТОЙКОСТИ КРИПТОСИСТЕМЫ NTRU» – Киршанова Е.А.

3) «Постквантовая криптография: основные подходы и причины использования» – https://habr.com/ru/sandbox/163505/

4) «NTRUEncrypt криптосистема будущего?» – https://habr.com/ru/articles/127878/

5) «Low-cost Implementations of NTRU for pervasive security» – Ali Can Atıcı, Lejla Batina, Junfeng Fan, Ingrid Verbauwhede, S. Berna Ors Yalcın

6) «NTRU: A Ring Based Public Key Cryptosystem» – Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman.

7) «Lattice-based cryptography.» – Micciiancio D., Regev O..

8) «Optimization for NTRU» – Hoffstein J., Silverman J..

9) «NTRUEncrypt: самый быстрый асимметричный шифр» – https://habr.com/ru/articles/118458/