МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и теории чисел

Криптосистема на эллиптических и гиперэллиптических кривых

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 2 курса 227 группы

направление 02.04.01 — Математика и компьютерные науки

механико-математического факультета

Яковлевой Анастасии Александровны

Научный руководитель
доцент, к.ф.-м.н., доцент _____ В.В. Кривобок
подпись, дата

Зав. кафедрой
зав. каф., к.ф.-м.н., доцент _____ А.М. Водолазов
подпись, дата

Саратов 2025

Введение. Тема данной магистерской работы - «Криптосистема на эллиптических и гиперэллиптических кривых».

Актуальность темы исследования. В современном мире, где данные играют все большую роль, защита конфиденциальности, целостности и доступности становится критически важной задачей. Криптография - это наука, которая занимается защитой данных от несанкционированного доступа, и представляет собой одну из основных технологий в области информационной безопасности.

Актуальность выбранной темы связана с необходимостью изучения современных методов и алгоритмов криптографической защиты информации, а также поиска эффективных решений для построения надежных защитных систем на основе эллиптических и гиперэллиптических кривых.

Цели и задачи. Основная цель работы заключается в исследовании фундаментальных математических и алгоритмических принципов криптосистем, построенных на эллиптических и гиперэллиптических кривых, а также в проведении сравнительного анализа эффективности вычислений в таких системах по сравнению с традиционным алгоритмом RSA. Для достижения данной цели были поставлены следующие задачи:

- Изучение основных математических принципов криптографии и алгоритмов шифрования.
- Исследование наиболее распространенных методов криптозащиты данных.
- Проведение сравнительной оценки эффективности операций с использованием криптографии на эллиптических кривых (ECC) и алгоритма RSA.

Содержание работы. Работа состоит из пяти разделов, каждый из которых посвящен отдельному аспекту построения и анализа криптосистем на эллиптических и гиперэллиптических кривых.

В первом разделе рассматриваются основные положения теории эллиптических кривых, а также подробно изучаются свойства эллиптических кривых над различными полями: действительных, комплексных и рациональных чисел.

Второй раздел посвящён изучению конечных полей, включая их характеристику, способы разложения многочленов, а также особенности эллиптических кривых, определённых над конечными полями.

Третий раздел включает анализ количества точек на эллиптических кривых и рассмотрение важных теорем Хассе и Хассе-Вейля, определяющих эти свойства.

Четвертый раздел посвящён открытым криптографическим протоколам. В нём рассматривается задача дискретного логарифмирования, в том числе основополагающие алгоритмы и алгоритм Полига-Хеллмана, а также представлено описание алгоритма RSA.

В пятом разделе приводится обзор и анализ протоколов, основанных на эллиптических кривых: построение задачи дискретного логарифмирования, обмен ключами Диффи–Хеллмана, схема электронной подписи Эль-Гамаля. Также в разделе проводится исследование криптографической стойкости ECC и проводится сравнение её с RSA.

Апробация. Доклад по теме исследования был представлен на кафедре компьютерной алгебры и теории чисел.

Основное содержание работы. Для начала необходимо ознакомиться с основными понятиями криптографии и изучить методы решения задачи дискретного логарифмирования, а также обратить внимание на современные направления, такие как использование эллиптических и гиперэллиптических кривых в криптографии.

Криптография — это область науки, которая занимается методами защиты информации от несанкционированного доступа. В её основе лежат такие понятия, как криптосистемы, шифрование, расшифровка, ключи, алгоритмы, аутентификация и другие. Криптография обеспечивает конфиденциальность передачи данных, их целостность и защищает от подделки или изменения информации со стороны неавторизованных лиц, используя методы сокрытия информации и специальные математические алгоритмы.

Ключи шифрования — это специальные символьные последовательности, предназначенные для защиты информации при её передаче. Ключ шифрования может быть открытым или секретным, в зависимости от типа используемой криптосистемы. В асимметричных системах для шифрования исполь-

зуется открытый ключ, а для расшифровки — секретный. В симметричных системах один и тот же секректный ключ применяется для обоих процессов.

Алгоритмы шифрования задают правила трансформации данных в защищённую форму и обратно. Они делятся на симметричные (требуют одинаковых ключей для шифрования и дешифрования) и асимметричные (используют пару ключей: открытый и секретный) 1.

Современные криптографические методы используют широкий спектр математических инструментов, таких как абстрактная алгебра, теория чисел, линейная алгебра, теория поля, комбинаторика, теория вероятностей, а также квантовые алгоритмы. Вся эта база относится к дискретной математике 2.

Важную роль в криптографии играют такие математические понятия, как множества, функции, простые числа, операции по поиску НОД и НОК, а также различные факторы и алгоритмы работы с многочленами и матрицами. Среди алгебраических структур в криптографии часто используются группоиды, моноиды, полугруппы, группы, кольца и поля.

Основной криптографической задачей долгое время оставалась проблема разложения больших целых чисел на множители. Однако сегодня всё большее значение приобретают задачи, связанные с дискретным логарифмом на эллиптических и гиперэллиптических кривых.

Эллиптические и гиперэллиптические кривые — это специальные алгебраические структуры, которые находят широкое применение в современных криптосистемах. Криптография на эллиптических кривых (ECC) предлагает высокий уровень защиты при меньших длинах ключей по сравнению с традиционными алгоритмами, а криптосистемы на гиперэллиптических кривых являются перспективным направлением для дальнейшего повышения безопасности и эффективности. Криптосистемы на основе этих кривых основываются на сложности задачи дискретного логарифмирования в группе точек кривой, что существенно усложняет криптоанализ.

Таким образом, криптосистемы на эллиптических и гиперэллиптических кривых являются современным и важным направлением исследований в криптографии, обладающим преимуществами по безопасности и производительности по сравнению с классическими системами.

Фундаментальное свойство эллиптических кривых раскрывается следующей теоремой:

Теорема 1 (О циклических подгруппах)**.** Точки эллиптической кривой вместе с бесконечно удаленной точкой O образуют:

- Циклические подгруппы
- В специальных случаях - полную циклическую группу

Этот результат имеет непосредственное практическое значение, что будет показано далее.

На основе теоретической базы вводится центральное для криптографии понятие:

Определение 2 (ECDLP)**.** Для эллиптической кривой E с образующей P и произвольной точкой T задача состоит в нахождении целого $d \in [1, \#E]$, удовлетворяющего соотношению:

$$\underbrace{P + P + \cdots + P}_{d \text{ раз}} = dP = T \tag{1}$$

В отличие от классических систем:

	Приватный ключ	Публичный ключ
Классическая схема	Целое число	Целое число
ECC	Целое число d	Точка кривой $T = (x_T, y_T)$

Протокол Диффи-Хеллмана

Алгоритм включает следующие этапы:

1. Инициализация параметров:
   - Выбор простого p и кривой $E(F_p) : y^2 \equiv x^3 + ax + b \mod p$
   - Фиксация образующей точки $P = (x_P, y_P)$
2. Генерация ключей:
   - Участник A: $k^A_{priv} = a$, $k^A_{pub} = aP = A$
   - Участник B: $k^B_{priv} = b$, $k^B_{pub} = bP = B$

3. Обмен и вычисление:

$$T_{AB} = aB = bA$$

Для обеспечения безопасности криптосистемы должны удовлетворять:
- Условию гладкости кривой ($\Delta \neq 0$)
- Достаточному порядку группы точек
- Защите от известных атак (MOV, Weil descent)

Замечание 3. Полная спецификация параметров для стандартных кривых (например, NIST P-256) приведена в Приложении А.

Схема Эль-Гамаля и эллиптические кривые

- Основана на сложности DLP в $\mathbb{F}_p$:

$$y \equiv g^x \mod p$$

- Подпись: (a, b), где:

$$a \equiv g^k \mod p, \quad b \equiv (h(M) - xa)k^{-1} \mod (p-1)$$

- Проверка:

$$y^a a^b \equiv g^{h(M)} \mod p$$

Адаптация для ECC

- Замена мультипликативной группы на группу точек эллиптической кривой
- Публичный ключ: $B = xA$ (скалярное умножение)
- Стойкость обеспечивается ECDLP

Криптографические параметры

Исследование криптостойкости ECC и сравнение с RSA

Криптография на эллиптических кривых (ECC) — одна из ключевых современных технологий открытых ключей, активно внедряемая в криптогра-

Параметр	**Требования**
Кривая	Неособая ($\Delta \neq 0$)
Порядок группы	Простое число
Безопасность	Защита от MOV/Weil

фических протоколах. ECC обеспечивает сопоставимую стойкость с алгоритмами RSA и дискретного логарифмирования при существенно меньших размерах ключей (160–256 бит против 1024–3072 бит для RSA/DL), что особо важно для устройств с ограниченными ресурсами. В основе ECC лежит обобщённая задача дискретного логарифмирования, позволяющая реализовывать такие протоколы, как Диффи–Хеллман, в пространстве точек эллиптических кривых.

На практике ECC отличается высокой эффективностью и меньшими требованиями к пропускной способности, однако операции с открытыми ключами у RSA могут быть быстрее при некоторых параметрах. Реализация ECC требует глубоких математических знаний, в частности, из алгебры, геометрии и теории чисел. Рост популярности ECC обусловлен необходимостью высокого уровня безопасности при малых издержках, что особенно актуально для мобильных и IoT-устройств. Многие современные стандарты (например, FIPS 186-4 и рекомендации NIST) уже содержат параметры и методы применения эллиптических кривых.

Криптостойкость ECC

Криптографическая стойкость ECC базируется на сложности задачи вычисления дискретного логарифма на эллиптических кривых (ECDLP). Эта задача формулируется следующим образом:

Пусть дана эллиптическая кривая над конечным полем и две точки P и Q, где $Q = kP$ для некоторого неизвестного целого k. Требуется найти k по P и Q.

На сегодняшний день не существует известных полиномиальных алгоритмов решения ECDLP для общих эллиптических кривых. Наиболее эффективные методы атаки (например, метод пола и потолка или алгоритм Гельмана-

Мейдера-Штрассена) имеют экспоненциальную сложность $O(\sqrt{n})$, где n — порядок группы точек.

Криптостойкость RSA

Криптостойкость алгоритма RSA основана на задаче факторизации больших целых чисел. Для нахождения закрытого ключа злоумышленнику необходимо разложить большое составное число $N = pq$ (произведение двух больших простых чисел) на множители.

Наиболее эффективным известным алгоритмом для взлома RSA является метод решета числового поля (Number Field Sieve, NFS) со сложностью $O(\exp((\log N)^{1/3}(\log\log N)^{2/3}))$, что на практике позволяет использовать вполне реализуемые атаки при недостаточной длине ключа.

Экспериментальное сравнение производительности ECC и RSA

Сравнительная оценка операций на эллиптических кривых (ECC) и RSA проводилась на Python 3.10 с библиотекой `cryptography`. Методика включала:

- Генерацию ключевых пар (ECDSA на `secp256k1` и RSA-2048)
- Операции подписи/проверки и обмена ключами (ECDH)
- Статистическую обработку (100 итераций)

Таблица 1 — Среднее время операций (мс)

Операция	Время, мс
RSA-2048 подпись	77.97
ECC-256 подпись	3.46
ECDH обмен ключами	2.41

Преимущества ECC:

- 256-битный ключ ECC эквивалентен 3072-битному RSA при меньших вычислительных затратах
- Компактность ключей и высокая скорость (ECDSA в 3 раза быстрее RSA)

- Гибкость выбора кривых под требования системы

Ограничения:

- Сложность выбора кривых и реализации арифметики
- Уязвимость к квантовым атакам (как и RSA)
- Требует тщательного проектирования параметров

ECC оптимальна для ресурсоограниченных систем, но требует учёта долгосрочных угроз и переосмысления архитектуры криптосистем.

Заключение. В ходе данной работы была рассмотрена эволюция криптографических методов — от классических симметричных шифров до современных асимметричных систем на основе эллиптических кривых. Особое внимание уделялось математическим основам ECC: алгебраической структуре, поведению на различных полях, а также ключевым теоретическим результатам, определяющим количество точек на кривой. Проведён анализ криптографической стойкости ECC и продемонстрировано её преимущество перед устаревающими схемами, такими как RSA, с точки зрения безопасности и эффективности.

В работе реализован алгоритм Диффи-Хеллмана для обмена ключами на эллиптических кривых (приведён в соответствии с приложением А), а также проведён сравнительный анализ производительности ECC и RSA (результаты тестирования и программный код приведены в соответствии с приложением Б). Полученные данные подтверждают, что использование ECC обеспечивает не только высокий уровень безопасности, но и значительную экономию вычислительных ресурсов по сравнению с традиционными системами с открытым ключом.

Проделанное исследование демонстрирует, что криптография на эллиптических кривых представляет интерес как с теоретической, так и с практической точки зрения — особенно для применения в современных условиях, включая среды с ограниченными вычислительными возможностями. Актуальность данной области будет только возрастать в связи с появлением новых угроз, прежде всего связанных с развитием квантовых вычислений. Изучение методов, таких как изогении и другие постквантовые подходы на базе эллиптических кривых, открывает перспективы дальнейших исследований и разработки защищённых протоколов будущего.

Систематизация математических основ и криптографических применений эллиптических кривых, представленная в работе, способствует устойчивому развитию как теории, так и практики информационной безопасности.