МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

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

Кафедра компьютерной алгебры и теории чисел

Криптосистемы на эллиптических кривых

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 4 курса 421 группы

направление 02.03.01 - Математика и компьютерные науки

механико-математического факультета

Галишниковой Екатерины Александровны

Научный руководитель
доцент, к.ф.-м.н., доцент ____________ В.В. Кривобок

Зав. кафедрой
зав. каф., д.ф.-м.н., доцент ____________ А.М. Водолазов

Саратов 2025

Введение. В современном мире обеспечение безопасности и конфиденциальности информации становится критически важным. С ростом числа кибератак и утечек данных криптография играет ключевую роль в защите данных в различных сферах. Одной из наиболее перспективных областей криптографии являются криптосистемы на эллиптических кривых (ECC), которые предлагают высокий уровень безопасности при относительно небольших размерах ключей. Эллиптические кривые были предложены для криптографии в 1985 году Нилом Коблитцем и Виктором Миллером. Они привлекают внимание благодаря своим уникальным свойствам и вычислительной эффективности. В отличие от традиционных систем, таких как RSA, ECC используют сложность дискретного логарифмирования на эллиптических кривых, что позволяет обеспечивать высокий уровень безопасности с меньшими ключами, уменьшая вычислительные и коммуникационные нагрузки. Актуальность ECC обусловлена несколькими факторами: уязвимостью традиционных систем к атакам, растущими требованиями к безопасности данных и практическим применением ECC в стандартах и протоколах, таких как TLS и цифровые подписи. В данной бакалаврской работе рассматриваются основные аспекты криптосистем на эллиптических кривых, включая их математические свойства, алгоритмы шифрования, цифровых подписей и обмена ключами, а также вопросы безопасности и устойчивости. Цель работы — дать всестороннее представление о преимуществах и возможностях ECC и продемонстрировать их практическое применение.

Основное содержание работы. Начнем с определения эллиптической кривой.

Определение 21 Эллиптической кривой E над полем F называется гладкая кривая, задаваемая уравнением вида:

$$Y^2 + a_1XY + a_3Y = x^3 + a_2X^2 + a_4X + a_6. \tag{1}$$

Обозначим $E(F)$ множество точек, которые удовлетворяют этому уравнению и кроме того, содержит бесконечную точку, которую обозначим O.

В зависимости от характеристики поля F общее уравнение эллиптической кривой может быть упрощено. Если поле F не является полем характеристики 2, то без потери общности можно полагать, что $a_1 = a_3 = 0$, т.е. вместо уравнения (1) рассматривать уравнение

$$Y^2 = X^3 + a_2X^2 + a_4X + a_6, a_i \in F. \tag{2}$$

Если характеристика поля не равна 2, 3, то после упрощения левой части (2), линейной заменой переменной (а именно, $X = X - \frac{1}{3}a_3$) можно также удалить член X^2 и без потери общности полагать, что кривая задана уравнением вида

$$Y^2 = X^3 + aX + b, a, b \in F, charF \neq 2, 3. \tag{3}$$

В частности, в таком виде представимы эллиптические кривые над полем нулевой характеристики, например, эллиптические кривые над полем R действительных чисел. Последние имеют хорошую интерпретацию кривой и наглядное демонстрирование ее свойств.

С уравнением 3 эллиптической кривой E можно связать дискриминант

$$\Delta(E) = (\frac{a}{3})^3 + (\frac{b}{2})^2 = \frac{4a^3 + 27b^2}{108} \tag{4}$$

многочлена $x^3 + ax + b$ и не изменяющийся при линейных преобразованиях j-инвариант

$$j(E) = \frac{1278(4a^3)}{\Delta(E)}. \tag{5}$$

Если $\Delta = 0$, то указанный многочлен имеет кратные корни и в точке $(x, 0)$ нарушается условие гладкости кривой. Справедлива следующая теорема.

Теорема 22 Кривая E гладкая тогда и только тогда, когда ее дискриминант ненулевой.

Пусть поле $F = R$. Тогда обозначим

Определение 25 Эллиптические кривые над полем действительных чисел можно записать в форме Вейерштрасса:

$$Y^2 = X^3 + aX + b, \tag{6}$$

Перед следующим определением необходимо отметить чрезвычайно важное свойство точек эллиптической кривой: они образуют абелеву группу относительно операции сложения точек.

Определение 26 Пусть E - эллиптическая кривая над полем вещественных чисел и пусть P и Q - две точки на E. Определим точки $-P$ и $P+Q$ по следующим правилам:

1. Точка O - является нейтральным элементом по сложению (или «нулевым элементом») в группе точек. В следующих пунктах предполагается, что ни P, ни Q не являются точками в бесконечности.
2. Точки $P = (x, y)$ и $-P$ имеют одинаковые x-координаты, но их y-координаты различаются только знаком, то есть $-(x, y) = (x, -y)$. Из 1 пункта следует, что $(x, -y)$ - также точка E.
3. Если точки P и Q имеют различные x-координаты, то прямая $l = \overline{PQ}$ имеет с E еще в точности одну точку пересечения R (за исключением двух случаев: когда она оказывается касательной в P, и мы тогда полагаем $R = P$, или касательной Q, и мы тогда полагаем $R = Q$). Определяем теперь $P+Q$ как точку $-R$, то есть как отражение оси x третьей точки пересечения. Геометрическое постороение, дающее $P+Q$, приводится на рисунках (3.1) и (3.2).
4. Если $Q = -P$ (то есть x-координата Q та же, что и у P, а y-координата отличается лишь знаком), то полагаем $P+Q = O$ (равняется «точке в бесконечности»; это является следствием 1 пункта).
5. Остается рассмотреть случай, когда $P = Q$. Тогда считаем, что l - касательная к кривой в точке P. Пусть R - единственная другая точка пересечения l с E. В этом случае полагаем, что $P+Q = R$ (в качестве R берем P, если касательная прямая в P имеет «двойное касание», то есть если P есть точка перегиба кривой).

Определение 27 Пусть E - эллиптическая кривая, опреленная над полем C компексных чисел, то есть E - это множество пар (x, y) комплексных чисел, удовлетворяющих уравнению (2), вместе с точкой в бесконечности O. С точки зрения обычных геометрических представлений E двумерна, то есть представляет собой поверхность в четырехмерном вещественном пространстве, координатами в котором являются действительные и мнимые части точек x и y.

Пусть L – это решетка на комплексной плоскости. Это означает, что L представляет собой абелеву группу, состоящую из всех целочисленных линейных комбинаций двух комплексных чисел ω_1 и ω_2, где ω_1 и ω_2 не коллинеарны: $L = Z\omega_1 + Z\omega_2$ здесь Z – множество целых чисел. Например, если $\omega_1 = 1$, $\omega_2 = i$, то L – множество всех гауссовых целых чисел, то есть квадратная сетка из всех комплексных чисел с целыми действительной и мнимой частями. Если задана эллиптическая кривая $y^2 = x^3 + ax + b$ над полем компексных чисел, то как оказывается, существуют решетка L и функция компексного переменного, называемая «p-функцией Вейерштрасса» и обозначаемая $p_L(z)$, со следующими свойствами:

1. Функция $p(z)$ аналитична всюду, кроме точек L, в каждой из которых имеется полюс второго порядка.
2. Функция $p(z)$ удовлетворяет дифференциальному уравнению $p'^2 = p^3 + + ap + b$ и, следовательно, при любом $z \notin L$ точка $(p(z), p(z))$ лежит на эллиптической кривой E.
3. Два комплексных числа z_1 и z_2 дают одну и ту же точку $(p(z), p'(z))$ на E тогда и только тогда, когда $z_1 - z_2 \in L$.
4. Отображение, которое любой точке $z \notin L$ ставит в соответсвие точку $(p(z), p(z))$ на E, а любой точке $z \in L$ - точку в бесконечности O, дает взаимно однозначное соответсвие между E и фактор группой C/L комплексной плоскости по подгруппе L.
5. Это взаимно однозначное соответствие есть изоморфизм абелевых групп, иными словами, если z_1 соответсвует точке $P \in E$, а z_2 - точке $Q \in E$, то $z_1 + z_2$ соответствие точке $P + Q$.

Таким образом, можно представить абелеву группу E как комплексную плоскость разделённую на ячейки некоторой решёткой. Чтобы наглядно изобразить эту группу, заметим, что каждый класс эквивалентности. $z+L$ существует один и только один представитель в «фундоментальном параллелограмме», состоящем из комплексных чисел вида $a\omega_1 + b\omega_2$, где $0 \leq a, b \leq 1$ (если

L - гауссовы числа, то фундаментальный параллелограмм - это единичный квадрат).

Определение 28 Если в уравнении $y^2 = x^3 + ax + b$, a и b - рациональные числа, то естественно рассматривать рациональные решения (x, y), то есть эллиптическую кривую над полем Q рациональных чисел.

Теорема 29 На эллиптической кривой E, заданной уравнением с целыми коэффициентами, группа $E(Q)$ рациональных точек является конечнопорожденной абелевой группой.

Определение 30 Предположим, что K - конечное поле F_q, с $q = p^r$ элементами, где p — простое число, а r — положительное целое число. Пусть E — эллиптическая кривая, определенная над F_q. Если K - поле характеристики 2, то эллиптическая кривая над K - это множество точек, удовлетворяющих уравнению либо типа

$$y^2 + cy = x^3 + ax + b, \tag{7}$$

либо типа

$$y^2 + xy = x^3 + ax + b, \tag{8}$$

где кубические многочлены в правых частях могут иметь кратные корни. Эти уравнения дополняются «точкой в бесконечности» O.

Если K - поле характеристики 3, то эллиптическая кривая над K - это множество точек, удовлетворяющих уравнению либо типа

$$y^2 = x^3 + ax^2 + bx + c, \tag{9}$$

где кубический многочлен в правой части не имеет кратных корней. Это уравнение также дополняется «точкой в бесконечности» O.

Любая эллиптическая кривая над полем K характеристики, отличной от 2 и 3, изоморфна кривой вида

$$y^2 = x^3 + ax^2 + b, \tag{10}$$

Особый интерес для криптографии представляет объект, называемый эллиптической группой по модулю p, где p является простым числом. Такая группа определяется следующим образом: выбираются два неотрицательных числа

a и b, которые меньше p и удовлетворяют условию

$$4a^3 + 27b^2 \pmod p \neq 0. \tag{11}$$

Тогда $E_p(a, b)$ обозначает эллиптическую группу по модулю p, элементами которой (x, y) являются пары неотрицательных чисел, меньших p и удовлетворяющих условию

$$y^2 = x^3 + ax^2 + b \pmod p \tag{12}$$

вместе с «точкой в бесконечности» O. В дальнейшем, говоря об эллиптической кривой, если не оговорено противное, будем иметь в виду эллиптическую группу по модулю p.

Пример 31 Рассмотрим следующую эллиптическую кривую $y^2 = x^3 + x + 1$ над полем с простым числом $p = 23$. В этом случае коэффициентые a и b равны 1, и условие для эллиптической группы по модулю 23 выполняется:

Результат решения этого примера известен как теорема Хассе.

Известно, что асимптотическая формула для порядка эллиптической кривой над конечным полем была найдена немецким математиком Хельмутом Хассе.

Теорема 32 Пусть N - число F_q - точек на эллиптической кривой, определенной над F_q. Тогда

$$|N - q - 1| \leq 2\sqrt{q}. \tag{13}$$

Это эквивалентно системе неравенств

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}. \tag{14}$$

Справедлива и более общая теорема Хассе-Вейля:

Теорема 33 Пусть E - эллиптическая кривая над полем $GF(q)$ и $N-$ порядок ее группы. Тогда для порядка $N(n)$ группы эллиптическй кривой $E(GF(q^n))$ над полем $(GF(q^n)$ справедлива формула

$$N(n) = q^n + 1 - \alpha^n - \beta^n, \tag{15}$$

где α β - корни квадратного уравнения $x^2 - tx + q = 0$, в котором коэффицент $t = q + 1 - N$. При этом всегда выполняется неравенство $t^2 \leq 4q$ и если оно строгое, то корни α и β будут комплексно сопряжёнными.

Задача открытого ключа : найти такую функцию $f(x)$, которая отвечает следующим требованиям:

1. Легко вычисляется: для любого значения x легко найти $y = f(x)$.
2. Обратная операция — нахождение x по заданному y (то есть вычисление $f^{-1}(y)$ — должна быть чрезвычайно трудной или практически невозможной без специальных данных (например, без секретного ключа).

Задача дискретного логарифмирования заключается в вычислении $x = log_b y$

Определение 34 Пусть G — конечная группа, b — элемент группы G и y — элемент группы G, являющийся степенью b. Любое целое число x, для которого $b^x = y$, называется дискретным логарифмом y по основанию b.

Алгоритм Полига-Хеллмана использует следующую стратегию:

1. Факторизация порядка группы: Предположим, что порядок группы n (то есть $p - 1$ для поля Z_p) имеет гладкую факторизацию:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k},$$

где p_i — простые числа, а e_i — их степени.

2. Решение подзадач: Для каждого простого делителя p_i алгоритм решает подзадачу вычисления дискретного логарифма по модулю $p_i^{e_i}$. Это позволяет разложить исходную задачу на более простые подзадачи.

3. Применение китайской теоремы об остатках: После решения всех подзадач результаты объединяются с помощью китайской теоремы об остатках, чтобы получить окончательное значение дискретного логарифма.

Рассмотрим алгоритм RSA. Пусть p и q — два различных случайно выбранных больших простых числа. Обозначим $n = pq$ и $\varphi(n) = (p-1)(q-1)$, где φ — функция Эйлера. Далее выбираем случайное число $d > 1$, которое взаимно простое с $\varphi(n)$, то есть $(d, \varphi(n)) = 1$, и находим e, которое удовлетворяет условию $1 < e < \varphi(n)$, и выполняет сравнение $ed \equiv 1 \mod \varphi(n)$.

Числа n, e и d называются соответственно модулем, экспонентой шифрования и экспонентой расшифрования. Пара чисел n и e образует открытый ключ шифрования, а оставшиеся числа p, q, $\varphi(n)$ и d составляют секретный ключ. Очевидно, что секретный ключ состоит из взаимозависимых величин, и, например, зная p, можно вычислить остальные параметры.

Для шифрования исходный текст возводится в степень e по модулю n. Для расшифровки криптографический текст возводится в степень d по модулю n.

Теорема 40 Точки на эллиптической кривой, включая бесконечно удалённую точку O, могут образовывать циклические подгруппы. В некоторых случаях все точки на эллиптической кривой вместе с точкой O образуют одну большую циклическую группу.

Определение 42 Дана эллиптическая кривая E. Рассмотрим образующий элемент P и другой элемент T. Задача дискретного логарифмирования на группе точек эллиптических кривых (ECDLP) заключается в нахождении целого числа d, где $1 \leq d \leq \#E$.

$$P + P + \ldots + P = dP = T. \tag{16}$$

В криптосистемах d — это закрытый ключ, представляющий собой целое число, тогда как открытый ключ T — это точка на эллиптической кривой с координатами $T = (x_T, y_T)$. В отличие от задачи дискретного логарифмирования в группе Z_n^*, где оба ключа были целыми числами, здесь открытый ключ — это точка на кривой. Операция в уравнении $T = dP$ называется точечным умножением, так как формально можно записать T как результат умножения точки P на скаляр d.

Ввод: эллиптическая кривая E вместе с точкой эллиптической кривой P скаляр $d = \sum_{i=0}^{t} d_i 2^i$ при $d_i \in \{0, 1\}$, и $d_t = 1$.

Выход: $T = dP$.

Инициализация: $T = P$.

Алгоритм:

1. Для $i = t - 1$ вплоть до 0

(a) $T = T + T \mod n$

(b) Если $d_i = 1$, то $T = T + P \mod n$

2. Возвращаем T

Рассмотрим протокол Диффи-Хеллмана Допустим, два пользователя (Аня и Боб) хотят согласовать ключ — случайный элемент из F_q^* — с помощью открытого обмена информацией через незащищенный канал связи. Аня выбирает случайное число a в диапазоне от 1 до $q-1$, которое держит в секрете, и вычисляет $g^a \in F_q$, которое объявляет открыто. Боб делает то же самое: он случайно выбирает b и объявляет g^b. В качестве секретного ключа используется g^{ab}. Оба пользователя могут вычислить этот ключ. Например, Аня знает g^b (это открытая информация) и свой собственный секретный ключ a. Она может вычислить значение g^{ab} и g^a. Если для мультипликативной группы F_q^* выполнено определенное условие, то построение ключа не позволит его определить.

Гипотеза Диффи–Хеллмана. Вычисление g^{ab} по g^a и g^b является крайне сложным.

Гипотеза Диффи–Хеллмана изначально не связана с задачей нахождения дискретного логарифма в конечной группе. Если бы существовал быстрый метод для вычисления дискретных логарифмов, то гипотеза Диффи–Хеллмана была бы опровергнута. Некоторые ученые считают, что обратное также верно, однако этот вопрос остается открытым. Другими словами, пока никто не предложил метод для получения g^{ab} из g^a и g^b без использования a и b. Тем не менее, возможно, что такой метод существует.

Далее рассмотрим следующий протокол шифрования.

В общем смысле при проверке цифровой подписи она корректна в том случае, когда выполняется запись

$$y^a a^b \equiv g^h \mod p. \tag{17}$$

Формальный алгоритм проверки цифровой подписи Эль-Гамаля включает следующие шаги.

Входные данные: сообщение M, открытый ключ (p, g, y), подпись (a, b)

Выходные данные: $True$ или $False$

Таким образом, рассмотрим алгоритм электронной подписи схемы Эль-Гамаля:

1. Проверить, входят ли элементы подписи a и b в диапазоны $0 < a < p$ и $0 < b < p - 1$, если проходят проверку, то $False$
2. Вычислить $w = b^{-1} \mod p$ и $h = h(M)$, где h — хеш-функция.
3. Вычислить $u_1 = w \cdot h \mod p$ и $u_2 = w \cdot a \mod p$.
4. Вычислить $v = g^{u_1} y^{u_2} \mod p$.
5. Сравнить v и a. Если $v = a$, то вернуть $True$, иначе $False$.

Заключение. В данной бакалаврской работе рассмотрены ключевые аспекты криптографии на эллиптических кривых (ЭК), включая их математические основы, криптографические системы и протоколы, а также вопросы безопасности и эффективности. В первой главе были изложены основные понятия эллиптических кривых, включая их определение, структуру и свойства. Особое внимание уделено эллиптическим кривым над различными полями, такими как поля рациональных чисел, конечные поля и поля комплексных чисел. Также рассмотрены алгоритмы вычисления точек на эллиптических кривых и их применение в криптографии. Во второй главе проанализированы криптографические системы, основанные на эллиптических кривых. Рассмотрены такие алгоритмы, как криптография с открытым ключом, дискретное логарифмирование, алгоритм Диффи-Хеллмана и криптосистема RSA. Особое внимание уделено сравнению этих алгоритмов с традиционными криптографическими методами, что позволило выявить преимущества и недостатки каждого из них. В третьей главе исследовались основные протоколы шифрования на эллиптических кривых. Рассмотрены протоколы, такие как постквантовое дискретное логарифмирование, обмен ключами Диффи-Хеллмана и схема электронной подписи Эль-Гамаля. Особое внимание уделено вопросам безопасности этих протоколов и их устойчивости к различным атакам. В заключение можно отметить, что криптография на эллиптических кривых представляет собой мощный и перспективный инструмент для обеспечения безопасности информации. Она обладает рядом преимуществ, таких как высокая эффективность, малые размеры ключей и устойчивость к известным атакам. Однако, несмотря на свои достоинства, криптография на эллиптических кривых требует дальнейших исследований и разработок для устранения существующих недостатков и повышения уровня безопасности.