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

студента 4 курса 421 группы

направления 02.03.01 «Математика и компьютерные науки»

механико-математического факультета

Петрова Данилы Витальевича

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

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

Саратов 2023

Введение. Исторически сложилось так, что криптография в основном имела дело с методами конфиденциальной передачи информации таким образом, чтобы третья сторона (называемая злоумышленником) не могла прочитать информацию, даже если передача осуществляется по небезопасному каналу, такому как телефонная линия общего пользования. Для обеспечения безопасной передачи можно использовать самый старый и, безусловно, самый быстрый тип криптографии - криптографию с секретным ключом, также называемую криптографией с симметричным ключом. В таком подходе возникает проблема о безопасной передаче закрытого ключа по открытому каналу. В 1976 году Уитфилд Диффи и Мартина Хеллман опубликовали работу «Новые направления в современной криптографии» содержащая первые асимметричные шифры, решающие задачу о передачи закрытого ключа по небезопасному каналу, но не без недостатков, связанные с медлительностью шифрования-дешифрования. А годом позже появилось первое их практическое применение реализованное алгоритмом Рон Ривест, Ади Шамир и Леонард Адлеман сокращенно RSA, преимущество которого заключается в экспоненциальной сложности разложения большого полупростого числа на два простых. Однако, с ростом вычислительной мощности современных компьютеров, возникают сомнения в безопасности этого метода.

С развитием алгебраической геометрии и теории чисел вырастает отдельная теория эллиптических кривых над конечными полями, которая находит себя в приложениях криптографии. Использование эллиптических кривых в шифровании предложили Нил Коблиц и Виктор С.Миллер независимо друг от друга в 1985 году. Криптография на эллиптических кривых (ECC) представила новую степень безопасности для криптосистем с открытым ключом, которые предоставляют комбинированные услуги шифрования и цифровой подписи. Обладает преимуществами в сравнении с RSA такими как меньше времени на шифровку, экономия пропускной способности.

Основное содержание работы. Рассмотрим важные определения.

Определение 0.0.16. Алгебраической кривой порядка n над полем F называется множество точек $(x, y), x, y \in F$, удовлетворяющих уравнению вида $F(X, Y) = 0$, где $F(X, Y)$ полином степени n с коэффициентами из F.

Определение 2.1.1. Эллиптической кривой E над полем F называется гладкая кривая, задаваемая уравнением вида:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \quad a_i \in F. \tag{2.1}$$

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

Если характеристика поля не равна 2, 3, то после упрощения (2.1), линейной заменой переменной (а именно, $X = X - \frac{1}{3}a_2$) можно также удалить член X^2 и без потери общности полагать, что кривая задана уравнением вида

$$Y^2 = X^3 + aX + b, \quad a, b \in F, \quad charF \neq 2, 3. \tag{2.3}$$

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 (2.3) эллиптической кривой E можно связать дискриминант

$$\triangle(E) = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 = \frac{4a^3 + 27b^2}{108} \tag{2.4}$$

полинома $x^3 + ax + b$ и не изменяющийся при линейных преобразованиях j-вариант

$$j(E) = \frac{1278(4a^3)}{\triangle(E)} \tag{2.5}$$

Определение 0.0.19. Кривую $F(X, Y) = 0$ назовем гладкой, если не существует такой точки $(x_0, y_0) \in F^2$ лежащей на этой кривой, для которой выполнялось следующее условие

$$\frac{\partial F(x_0, y_0)}{\partial x} = 0, \quad \frac{\partial F(x_0, y_0)}{\partial y} = 0.$$

Если $\triangle = 0$, то указанный полином обладает кратным корнем и в точке (x, 0), где нарушается условие гладкости кривой. Вообще справедлива следующая теорема.

Теорема 2.1.2. Кривая E гладкая тогда и только тогда, когда ее дискриминант ненулевой.

Она предоставляет критерий гладкости без поиска производных для каждой такой кривой, достаточно посчитать дискриминант и подтвердить, что он отличный от нуля.

Пусть поле $F = R$. Ньютон доказал, что над полем действительных чисел любую эллиптическую кривую можно преобразовать к форме Вейерштрасса $Y^2 = X^3 + aX + b$. Введем правила сложение точек на этой кривой. А именно:

1) элементами некоторого множества являются точки эллиптической кривой;

2) нейтральный элемент это бесконечная удаленная точка;

3) обратный элементу P есть точка симметричная оси X и имеет обозначение $-P$;

4) на этом множестве задано сложение по следующему правилу: сумма трех точек лежащих на одной прямой будет равно бесконечно удаленной точке $(P + Q + R = O)$.

Для этого множества выполняется закон ассоциативности и закон коммутативности о чем говорит следующая теорема Анри Пуанкаре:

Теорема 2.2.1. Множество $E(F)$ с операцией сложения, описанной выше, образует абелеву группу.

Свойства описанные выше работают и для эллиптических кривых над конечными полями. Они полезны с точки зрения их использования в криптосистемах, а именно на этой группе будет тяжело подобрать или вычислить обратную функцию дешифрования к фукнции шифрования, когда дело дойдет до дискретного логарифмирования на эллиптических кривых.

Эллиптические кривые над конечными полями имеют конечные группы точек. Порядок этой группы назовем порядком эллиптической кривой. Порядок точки P эллиптической кривой называется наименьшее число k такое, что $kP = O$. По теореме Лагранжа порядок точки делит порядок эллиптической кривой.

Теорема 2.5.1 Пусть группа G конечна, и H — её подгруппа. Тогда порядок G равен порядку H, умноженному на количество её левых или правых классов смежности (индекс подгруппы).

Порядки кривых при изоморфизме сохраняются, а также остается неизменным порядок группы.

Для небольших полей вычисление группы точек данной кривой и ее порядка не составляет труда.

Пользуясь символом Лежандра, легко указать на формулу для числа точек на кривой $Y^2 = f(X)$ над полем F_p, $p > 2$. Действительно, сравнение по модулю $Y^2 \equiv f(x)\ mod\ p$ относительно Y при фиксированном x содержит (при $p > 2$) $1 + \left(\frac{f(x)}{p}\right)$ решений. Учитывая бесконечно удаленную точку, получаем формулу для порядка кривой над полем F_q, $p > 2$ в виде

$$p + 1 + \sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right). \tag{2.6}$$

При малых простых p, пользуясь этой формулой и теорией квадратичных вычетов порядок кривой над полем F_q находить довольно легко.

Оказывается вычисление порядка эллиптической кривой не всегда просто или даже возможно. В действительности общая формула для вычисления порядка группы произвольной кривой неизвестна. Также остается неизвестным, можно ли за полиномиальное время найти кривую данного порядка. Имеются продвижения в результатах, где показывают вычисление порядка группы эллиптической кривой над кольцом вычетов по модулю n полиномиально эквивалентна задаче разложения числа n на множители. Однако, известны способы выбора эллиптической кривой для которой найти порядок относительно не сложно. Эти способы важны в своей значимости, потому что в криптографии очень полезно, чтобы порядок имел большие простые множители, иначе проблема дискретного логарифмирования может быть решена.

Есть приближенно точная формула для порядка эллиптической кривой над конечным полем о ней свидетельствует теорема Хассе.

Теорема 2.5.2 Порядок N эллиптической кривой над полем F_q удовлетворяет неравенству

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

В случае полей малой характеристики порядок группы эллиптической кривой легко найти по формуле (2.6).

Преимущество эллиптических кривых над конечными полями заключается в том, что имеется большое многообразие групп с разными порядками для одного и того же поля F_q. Даже доказано, что для любого простого p порядки групп кривых над полем F_p почти равномерно распределены на отрезке $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$. Появляется возможность подобрать кривую, порядок которой имеет только один большой делитель.

Поставим задачу дискретного логарифмирования

Определение 3.2.4. Дана конечная циклическая группа G с групповой операцией $\circ$ и мощностью n. Рассматриваем образующий элемент $a \in G$ и другой элемент $b \in G$. Задача дискретного логарифмирования заключается в нахождении целого x, где $1 \leq x \leq n$, такого, что:

$$b = a \cdot a \cdot ... \cdot a = a^x$$

Если рассматривать частный случай задачи дискретного логарифмирования для циклической группы Z_p^* порядка $p-1$ и образующий элемент $a \in Z_p^*$ и другой элемент $b \in Z_p^*$, то имеем задачу определения целого числа $1 \leq x \leq p-1$ такого, что:

$$a^x \equiv b \ mod \ p.$$

Такой элемент x существует, поскольку элемент a образующий, и каждый элемент группы может быть выражен как степень любого образующего элемента. Элемент x называется дискретным логарифмом b по основанию a, и обозначается он так:

$$x = log_a b \ mod \ p.$$

Вычисление дискретных логарифмов по модулю простого числа является очень сложной задачей, если параметры достаточно велики. Поскольку возведение в степень $a^x \equiv b \ mod \ p$ прост в вычислении, это образует одностороннюю функцию.

Поставим задачу дискретного логарифмирования на группе точек эллиптических кривых.

Определение 4.1.3. 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 $1 \leq d \leq \#E$.

$$P + P + ... + P = dP = T. \tag{4.2}$$

В криптосистемах d - это закрытый ключ, который является целым числом, в то время как открытый ключ T - точка на кривой с координатами $T = (x_T, y_T)$. Напротив, в случае задачи дискретного логарифмирования в Z_n^*, оба ключа были целыми числами. Операция в уравнении называется точечным умножением, поскольку можно формально записать $T = dP$.

Точечное умножение является аналогом возведения в степень в мультипликативных группах. Вот алгоритм для эффективного подсчета точечного умножения.

Задача 1. Пусть Алиса и Боб хотят безопасно на основе своих закрытых ключей сформировать общий секретный ключ, который есть только у них. Допускается, что существует третье лицо желающее перехватить их сообщение.

Эту задачу разрешает протокол Диффи-Хеллмана.

Протокол Диффи-Хеллмана это криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.

Согласуем параметры кривой.

1) Выберем простое число p и эллиптическую кривую $E(F_p)$

$$y^2 \equiv x^3 + ax + b \; mod \; p \tag{4.3}$$

2) Выберем образующий элемент $P = (x_P, y_P)$

Простое число p, кривая, заданная ее коэффициентами a, b, и образующий элемент P являются параметрами предметной области.

Кривые должны обладать определенными свойствами, чтобы быть надежными. Фактический обмен ключами должен происходить следующим образом.

Пусть Алиса выбирает приватный ключ $k_{prA} = a \in \{2, 3, ..., \#E - 1\}$ и вычисляет открытый $k_{pubA} = aP = A = (x_A, y_A)$, а Боб соответственно $k_{prB} = b \in \{2, 3, ..., \#E - 1\}$ и $k_{pubB} = bP = B = (x_B, y_B)$. Они обмениваются открытыми ключами между собой и применяют на полученные ключи свои закрытые ключи $T_{AB} = aB = bA$. Получаем, что Алиса и Боб теперь хранят совместный секрет T_{AB}.

Как видно из протокола говоря неформальным языком, Алиса и Боб выбирают закрытые ключи a и b соответственно, которые представляют собой два больших целых числа. С помощью закрытых ключей оба генерируют свои соответствующие открытые ключи A и B, которые являются точками на кривой. Открытые ключи вычисляются путем умножения на точки. Обе стороны обмениваются этими общедоступными параметрами друг с другом. Затем T_{AB} вычисляется как Алисой, так и Бобом путем выполнения умножения на вторую точку с использованием открытого ключа, который они получили, и их собственного секретного параметра. Совместный секретный T_{AB} может быть использован для получения сессионного ключа, например, в качестве входных данных для алгоритма AES.

Одна из координат совместного секретного центра T_{AB} теперь можно использовать в качестве сессионного ключа. На практике часто координата x хэшируется и затем используется в качестве симметричного ключа. Обычно требуются не все биты. Например, в 160-битной схеме ECC хэширование x-координата с SHA-1 приводит к 160-битному выводу, из которых только 128 будут использоваться в качестве ключа AES.

Причина, по которой стоит использовать эллиптические кривые, заключается в том, что ECDLP обладает очень хорошими односторонними характеристиками. Если злоумышленник хочет взломать ECDH, у него есть следующая информация: E, p, P, A и B. Он хочет вычислить совместный секрет между Алисой и Бобом $T_{AB} = a \cdot b$. Это называется задачей Диффи–Хеллмана об эллиптической кривой (ECDHP).

Если эллиптическая кривая выбрана с осторожностью, то наиболее известные атаки на ECDLP значительно слабее лучших алгоритмов для решения задачи DL по модулю p и лучших алгоритмов факторинга, которые используются для RSA-атак. В частности, алгоритмы индексного исчисления,

которые являются мощными атаками на DLP по модулю p неприменимы к эллиптическим кривым. Для тщательно отобранного эллиптические кривые, единственными оставшимися атаками являются универсальные алгоритмы DL, то есть метод маленьких- гигантских шагов Шенкса и метод rho Полларда. На практике обычно используются разряды эллиптической кривой длиной до 256 бит, которые обеспечивают уровень безопасности до 128 бит.

Такая безопасность достигается выбором особых надежных кривых. Существует несколько семейств кривых, которые обладают криптографическими недостатками. Однако их относительно легко обнаружить. На практике часто используются стандартизированные кривые, такие как кривые, предложенные Национальным институтом стандартов и технологий (NIST).

Основные плюсы криптографии на эллиптических кривых:

1) высокий уровень безопасности при меньшей длине ключа по сравнению с другими асимметричными криптосистемами;

2) меньшие затраты на хранение и передачу информации, а также на вычисления в криптографических протоколах;

3) большое разнообразие эллиптических кривых, которые можно использовать для разных целей и потребностей.

Основные минусы криптографии на эллиптических кривых:

1) сложность выбора подходящих эллиптических кривых, которые не подвержены известным атакам и обладают хорошими свойствами;

2) необходимость использования специальных алгоритмов для работы с точками на эллиптических кривых, которые могут быть менее эффективными или сложными в реализации, чем стандартные арифметические операции;

3) уязвимость перед квантовыми компьютерами, которые могут решать задачу дискретного логарифмирования за полиномиальное время.

Заключение. В этой работе рассмотрено основные понятия и различные виды криптосистем и методов шифрования, основанных на эллиптических кривых над конечными полями. Однако в работе не был затронут вопрос о протоколах на гиперэллиптических кривых, поскольку он выходит за ее рамки.

Эллиптическая криптография является одним из современных и перспективных направлений в криптографии, которое обладает рядом преимуществ

перед другими асимметричными криптосистемами, такими как RSA, такие как меньше времени на шифровку, экономия пропускной способности и высокий уровень безопасности при меньшей длине ключа. Также обозначены некоторые недостатки эллиптической криптографии, связанные с трудностями выбора подходящих эллиптических кривых, необходимостью использования специальных алгоритмов для работы с точками на кривых и уязвимостью перед квантовыми компьютерами.

Реализован алгоритм Диффи-Хеллмана на эллиптических кривых, который позволяет двум сторонам, имеющим пары открытый/закрытый ключ на эллиптических кривых, получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Этот секретный ключ может быть использован как для шифрования дальнейшего обмена, так и для формирования нового ключа, который затем может использоваться для последующего обмена информацией с помощью алгоритмов симметричного шифрования. Этот алгоритм является вариацией протокола Диффи-Хеллмана с использованием эллиптической криптографии.

Эллиптическая криптография помогает защищать информацию от несанкционированного доступа, изменения или подделки, а также подтверждать подлинность авторства или иных свойств объекта.