Министерство образования и науки Российской Федерации

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 МАГИСТЕРСКОЙ РАБОТЫ

студента 2 курса 227 группы

направления 02.04.01 «Математика и компьютерные науки»

механико-математического факультета

Россинского Родиона Вячеславовича

Научный руководитель
доцент, к.ф.-м.н. Е.В. Сецинская

Зав. кафедрой:
к.ф.-м.н., доцент А.М. Водолазов

Саратов 2017 г.

Введение

Криптография - наука о методах обеспечения конфиденциальности, секретности передаваемой информации, её целостности, аутентификации сообщающихся сторон - авторство должно устанавливаться однозначно. Целостность подразумевает невозможность незаметного изменения данных посторонним. Криптография берёт своё начало с первых методов шифрования информации с целью её защиты от посторонних.

Преобразование исходного текста при помощи специального алгоритма и *ключа*, зная которые возможно обратное преобразование в исходный текст, называется *шифрованием*. Участвующий в шифровании ключ называется криптографическим ключом, процесс же шифрования и расшифрования(дешифрования) информации таким способом - симметричным, поскольку используется один и тот же ключ. Способ сокрытия данных от посторонних таким образом называется симметричной криптосистемой. Существуют различные алгоритмы для симметричных криптосистем: потоковые и блочные шифры. Потоковые позволяют шифровать информацию последовательно, побитово, а блочные алгоритмы шифрования преобразуют целый сегмент данных как единое целое. Размер шифруемого блока порядка 64-128 бит. Для реализации шифрования при помощи симметричных криптосистем криптографический ключ (или же алгоритм шифрования в целом) должен быть известен обеим сторонам до начала передачи сообщений. В качестве исторического примера такой криптосистемы может быть назван широко известный шифр Цезаря, в котором буквы исходного текста сдвигаются на определенное известное число позиций. Существуют и более современные реализации симметричных криптосистем в рамках различных алгоритмов шифрования, таких как: AES(Advanced Encryption Standard), Blowfish, RC5(Rivest's Cipher 5/Ron's Code 5), RC4(Rivest cipher 4) и т.д.

Использование двух ключей - открытого и закрытого, означает применение асимметричной криптосистемой. Ключи выбраны такими, что нельзя получить значение другого ключа, даже имея свою часть закрытого ключа. Открытый ключ передаётся через незащищённый канал. Криптографические системы с открытым ключом нашли своё применение в ряде сетевых протоколов: SSL(Secure Sockets Layer), TLS(Transport Layer Security) в SSH(Secure

Shell). Второй протокол является логическим продолжением первого, он же лёг в основу протокола HTTPS (HyperText Transfer Protocol Secure), пришедшего на смену нешифрованному протоколу HTTP.

Цель работы заключается в изучении эллиптических кривых, начиная от теоретических основ и до их практического применения в современной криптографии.

Актуальность работы обусловлена тем, что шифрование в современном мире является неотъемлемой частью передачи информации. Необходимо оно для подтверждения подлинности, для сохранения конфиденциальности информации. Эллиптические кривые являются одним из вариантов, который, возможно, придёт на смену RSA.

Структура выпускной квалификационной работы(ВКР) представляет собой следующие три главы (приводится информация только по основной части ВКР):

1. *Основные понятия и определения.* В данной главе рассматриваются теоретические основы, начиная с задачи о конгруэнтных числах и до эллиптических кривых. Рассматриваются эллиптические кривые над различными полями, описываются операции над точками эллиптической кривой . Рассматривается понятие порядка точки на кривой.
2. *Задачи криптографии, решаемые с помощью эллиптических кривых.* Излагается материал о применении эллиптических кривых при решении таких задач криптографии, как факторизация и проверка на простоту .
3. *Основные эллиптические криптосистемы.* Представлена информация о существующих методиках расчёта дискретного логарифма при помощи эллиптических кривых, последовательно излагается алгоритм расчёта числа точек эллиптической кривой методом Чуфа. Даётся описание и принцип работы протоколов, использующих эллиптические кривые, таких как протокол Диффи-Хеллмана; алгоритма электронной подписи (ECDSA).

Конгруэнтные числа - рациональные положительные числа $r \in \mathbb{Q}$, если они являются площадью прямоугольного треугольника с рациональными длинами сторон. Если $X, Y, Z \in \mathbb{Q}$ - длины сторон треугольника, а число r

конгруэнтно, то для любого r можно найти такое число $s \in \mathbb{Q}$, что $s^2 r$ будет являться числом, свободным от квадратов.

Прямоугольнику со сторонами X, Y, Z и площадью n можно поставить в соответствие точку на плоскости xy, которая располагается на кривой из уравнения $y^2 = x^3 - n^2 x$. Не любая точка на кривой происходит из прямоугольного треугольника, так как полученная таким способом точка (1) должна лежать в $(Q^+)^2, x = \dfrac{Z}{2}^2 = u^2$, а (2) знаменатель первой координаты такой точки должен делиться на 2:

Теорема 1. Пусть точка (x, y) принадлежит кривой, заданной уравнением $y^2 = x^3 - n^2 x$. Если x удовлетворяет следующим условиям:

1) x - квадрат некоторого рационального числа.
2) x имеет четный знаменатель.
3) числитель x является взаимно простым с n

то число x происходит из прямоугольного треугольника с рациональными длинами сторон и площадью n и может быть получено при помощи соотношений из теоремы 2.

Теорема 2. Если n - целое положительное число, свободное от квадратов, то для тройки чисел X, Y, Z выполняется следующее условие: $X < Y < Z$, то можно установить однозначное и взаимное соответствие между прямоугольными треугольниками со сторонами X, Y, Z и площадью n и числами x, для которых верно утверждение, что x, $x - n$ и $x + n$ являются квадратами рациональных чисел. Соответствие может быть выражено через следующие формулы $\left(X, Y, Z \to \left(\dfrac{Z}{2}\right)^2\right)$:

$$\begin{aligned} x \to X &= \sqrt{x+n} - \sqrt{x-n} \\ Y &= \sqrt{x+n} + \sqrt{x-n} \\ Z &= 2\sqrt{x} \end{aligned}$$

Число n является конгруэнтным тогда и только тогда, когда некоторое число x, а также числа $x - n$ и $x + n$ являются квадратами рациональных чисел.

Эллиптической кривой над полем K называют множество точек, удовлетворяющих уравнению::

$$y^2 = x^3 + ax + b \tag{1.4}$$

а также дополнительный элемент - точка O, которая носит название «точка в бесконечности». Поле K - это поле характеристики, отличной от 2 и 3. В формуле 1.4 a, b входят в K, а сам многочлен не имеет кратных корней.

Если поле K является полем характеристики 2, то под эллиптической кривой над K подразумевается множество точек, являющихся решением уравнения одного из двух типов:

$$y^2 + cy = x^3 + ax + b \tag{1.5}$$

или

$$y^2 + xy = x^3 + ax^2 + b \tag{1.6}$$

Для поля характеристики 2 допустимо, что кубическое уравнение из 1.5 и 1.6 может иметь кратные корни.

Если K - поле характеристики 3, то решения должны удовлетворять следующему уравнению:

$$y^2 = x^3 + ax^2 + bx + c \tag{1.7}$$

Кубический многочлен в правой части уравнения 1.7 не имеет кратных корней.

Помимо всех точек, удовлетворяющих вышеприведенным уравнениям, к эллиптическим кривым дополнительно относится «точка в бесконечности» O.

Существует общая форма записи уравнения эллиптической кривой, применимая при любом поле K:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.8}$$

Пусть E - эллиптическая кривая над полем вещественных чисел, точки P и Q принадлежат этой кривой. Определим точки $-P$ и $P+Q$ по следующим правилам:

1. Если P - «точка в бесконечности» O, то $P+Q=Q$, а $-P=O$. Точка O - нулевой элемент.
2. Точки $-P$ и P отличаются только знаком перед координатой y при одинаковой координате x - обе точки: $P(x,y)$ и $-P(x,-y)$ принадлежат кривой E.
3. Если точки P и Q различаются по координате x, то прямая l, проходящая через эти две точки, пересекает кривую E в одной единственной точке R во всех случаях, кроме:
   - l является касательной в точке P. В этом случае считаем $R=P$.
   - l является касательной в точке Q. Тогда полагаем $R=Q$.

   Результатом сложения точек P и Q во всех остальных случаях будем считать точку $-R$, которую можно получить отражением относительно оси x третьей точки пересечения кривой E и прямой l. Таким образом, $P+Q=-R$. Такое правило сложения коммутативно.
4. Если $Q=-P \to P+Q=O$.
5. Если же $Q=P$, то будем считать прямую l касательной в точке P. Тогда R будет второй точкой пересечения прямой l и кривой E. Если же точка P является точкой перегиба, то в качестве R также берём точку P.

Наибольшую популярность в криптографии имеют эллиптические кривые над конечными полями. Способ **проверки на простоту** числа при помощи эллиптических кривых является аналогом критерия простоты Поклингтона:

Теорема 3. Рассмотрим натуральное n. Обозначим E множество всех точек, удовлетворяющих уравнению $y^2 = x^3 + ax + b$ по модулю n ($u\text{НОД}\left(4a^3+27b^2, n\right) = 1$). Пусть m - некоторое целое число, у которого есть простой делитель $q > \left(n^{1/4}+1\right)^2$, то если $\exists$ точка P такая, что верны следующие утверждения:

1. $mP = O$
2. $(m/q)P$ определена и $(m/q)P \neq O$

то число n - простое.

Разложение на простые множители, известное также как факторизация, предположительно является вычислительно весьма сложной задачей для больших чисел. Этот факт положен в основу множества используемых алгоритмов, протоколов шифрования.

Существует алгоритм, который позволяет находить нетривиальные делители числа n при помощи эллиптических кривых - метод Ленстры. Алгоритм работает быстрее любого экспоненциального метода, но медленнее алгоритмов с полиномиальной сложностью - является субэкспоненциальным. Ход действий алгоритма следующий:

1. Выбираем некоторую кривую E и точку P на ней.
2. Проверка того, что E не имеет кратных по модулю p корней.
3. Выбираем числа B, C такие, что B является наибольшим значением делителя целого числа k, которое возникает в процессе поиска точки kP. Чем больше выбранное число B, тем с большей вероятностью выполняется равенство $kP(\mod p) = O(\mod p)$ для выбранной кривой, точки на ней и некоторого p. И тем больше времени необходимо на расчёт $kP(\mod p)$. B должно быть выбрано из критерий оптимальности работы алгоритма. C - максимальное значение для делителя p, для которого должно выполниться условие $kP(\mod p) = O(\mod p)$. Затем число k представляется в виде произведения:

$$k = \prod_{l \leq B} l^{\alpha_l}, \tag{2.3}$$

где каждое простое число $\leq B$, а его степень $\leq C$. Согласно теореме Хассе [], в случае $p + 1 + 2\sqrt{p} < C$ и отсутствия делителя больше числа B для порядка кривой E по модулю p, число k будет являться кратным этому порядку и, соответственно, $kP(\mod p) = O(\mod p)$.

Задача **дискретного логарифмирования** заключается в обращении некоторой функции g^x в конечной группе G. В рамках применения эллиптических кривых для её решения, задачу рассматривают отдельно для группы точек эллиптической кривой над конечным полем.

Задача дискретного логарифмирования для эллиптической кривой сводится к нахождению такого показателя l, что $P = lQ$, точка P - известна, а

Q - порождающий элемент группы $\rightarrow P \in \langle Q \rangle$.

Задача может решаться различными методами. Например, методом Гельфонда, также известным как метод Силвера-Полига-Хеллмана, «встречи посередине», методом больших и малых шагов (метод Гельфонда-Шенкса), встречи на случайной дереве и методом Полларда. Согласно методу Гельфонда, задача сводится полиномиально к задаче логарифмирования в подгруппе, имеющий максимальный простой порядок, поэтому число r часто выбирается простым.

Алгоритм Полларда. Известна эллиптическая кривая $E(\mathbb{F}_q)$ над конечным полем $\mathbb{F}_q$, точка на этой кривой $P \in E(\mathbb{F}_q)$, порождающий элемент Q. Группа, порожденная элементом Q, имеет простой порядок r.

Необходимо найти l такое, что $P = lQ$.

Решение проходит через ряд последовательных шагов:

1. Выбрать подходящее отображение $\tau(R)$, обладающее необходимыми свойствами.
2. Использовать произвольные показатели a, b, c, d и положить $R = aQ + bP$, а $S = cQ + dP$.
3. С помощью отображения τ получить новые значения для $R, S \rightarrow R = \tau(R), S = \tau(\tau(S))$, вычисляя в ходе этих преобразований логарифмы точек R и S в кольце $\mathbb{F}_r(l)$ до тех пор, пока не выполнится условие $R = \pm S$
4. Приравниваются логарифмы для R, S, решением уравнения вычисляется l. Если решения нет, то необходимо выбрать другое отображение, вернувшись к первому шагу.

Алгоритм Гельфонда. Задана кривая E над конечным полем $\mathbb{F}_q$, Q - порождающий элемент группы (образующая точка, генератор), известна точка P на кривой E, разложение порядка группы в следующем виде: $\#E(\mathbb{F}_q) = \prod_{j=1}^{n} p_j^{a_j} = N$.

Необходимо на найти логарифм l такой, что $P = lQ$.

Алгоритм выполняется n-итераций.

1. $q = p_i, a = a_i$.
2. $S = O, k_{-1} = 0$

3. Вычисляется $Q' = \frac{N}{q}Q$
4. В течение $a-1$ итераций выполняются следующие действия (i - текущий шаг):
   4.1. $S = S + k_{i-1}q^{i-1}Q$
   4.2. $P' = \frac{N}{q^{i+1}}(P - S)$
   4.3. Вычислить логарифм $k_i = log_{Q'}P'$. Для этого можно воспользоваться методом Полларда.
5. $l_i = k_0 + k_1 q + k_2 q^2 + ...k_{a-1}q^{a-1}(\mod q^a)$

Из l_i необходимо восстановить l - для этого можно применить китайскую теорему об остатках []. Полученный l и будет искомым результатом.

Алгоритм Чуфа позволяет найти число точек эллиптической кривой над некоторым конечным полем $\mathbb{K}$, используя полиномы деления.

Алгоритм Чуфа. Обозначим N искомое число точек кривой E над конечным полем $\mathbb{K}$ через вычисления в полях функций $K[x,y]/(E(\mathbb{K}), f_{l_i}(x)$, где $E(\mathbb{K})$ - задающий кривую идеал, $f_l(x)$ - $l-$ый полином деления. Ход алгоритма может быть записан через следующие три шага:

1. Вычисление всех попарно и взаимно простых чисел l_i, а также соответствующих полиномов деления в кольце $K[x]$;
2. Нахождение $T = q + 1 - N$ - вычетов по модулям простых чисел l_i, являющихся взаимно простыми.
3. Число точек восстанавливается по китайской теореме об остатках [].

Наиболее сложным в алгоритме является второй шаг - для различных характеристик поля $\mathbb{K}$ будут существовать различные условия существования точки P.

Для некоторых эллиптических кривых число точек может быть определено проще, чем алгоритмом Чуфа. Это возможно по крайней мере в двух случаях: если эллиптическая кривая $E(K)$ с известным числом точек над рассматривается над конечным расширением $_1$ поля и если рассматриваются эллиптические кривые над простыми полями, обладающие комплексным умножением над полем .

Протоколы на эллиптических кривых. *ECDSA* - **e**lliptic **c**urve **d**igital **s**ignature **a**lgorithm - протокол электронной подписи, основанный на задаче

дискретного логарифмирования. Его предшественник - DSA, основывался на дискретном логарифмировании над полем целых чисел. В ECDSA эта же задача решается в группе точек эллиптической кривой.

Алгоритм вычисления цифровой подписи. Для сообщения уже подсчитано некоторое значение хэш-функции $H : h$. После этого необходимо проделать следующие действия:

1. Случайным образом выбрать некоторое целое число k из промежутка $[1, q-1]$, где q - порядок некоторой циклической подгруппы для группы точек эллиптической кривой.
2. Посчитать кратную P точку: $kP = (x_1, y_1)$. Отсюда вычислить число $r = x_1(\mod q)$. Если $r = 0$, то необходимо выбрать другое k.
3. Рассчитать $k^{-1}(\mod q)$ и найти $s = k^{-1}(h + x \cdot r) \mod q$. В случае, если $x = 0$, то нужно выбрать другое k на первом шаге.

Протокол Диффи-Хеллмана, ECDH - **e**lliptic **c**urve **D**iffie-**H**ellman - протокол выработки общего секретного ключа путём применения эллиптических кривых для данной задачи. Предполагается, что перед началом процедуры стороны владеют открытым и закрытым ключами. Подразумевается, что канал связи может быть прослушан. Полученный общий секретный ключ может использоваться при шифровании дальнейших сообщений, для создания нового ключа, который будет использоваться обеими сторонами в случае симметричного шифрования.

Набор параметров, которые должны быть согласованными перед началом сообщения: p, a, b, G, n, h для общего случая и $m, f(x), a, b, G, n, h)$ для поля характеристики 2. Дополнительно каждая сторона в передачи информации должна иметь пару ключей: закрытый ключ d (d - выбранное случайным образом число из промежутка $[1, n-1]$ и открытого ключа Q, где $Q = d \cdot G$. Перед началом абоненты обмениваются своими открытыми ключами: (d_A, Q_A) и (d_B, Q_B). Первый абонент вычисляет $(x_k, y_k) = d_A \cdot Q_B$, второй - $(x_k, y_k) = d_B \cdot Q_A$. Общим секретом будет являться координата получившейся точки x_k.

Криптосистема Мэсси-Омура изначально позиционировалась как улучшения протокола Шамира. Протокол реализован в двух различных вариантах: классическом(дискретное логарифмирование) и основанном на эллип-

тических кривых. Полученное при помощи протокола сообщение зачастую используется в качестве ключа других криптосистем.

Криптосистема Эль-Гамаля основана также на сложности вычисления дискретного логарифма в конечном поле. Существует её вариация, в которой используется множество точек эллиптической кривой.

Генерация в открытого и закрытого ключа в схеме Эль-Гамаля на эллиптических кривых происходит следующим образом:

1. Выбирается некоторая эллиптическая кривая E и точка $P(x, y)$ на ней.
2. Находится точка $Q = d \cdot P$, где d - некоторое случайно выбранное целое число.
3. Совокупность выбранной E, P и посчитанной точки Q определяются как открытый ключ. Выбранное число d становится секретным ключом.

Заключение

В ходе работы были изучены теоретические основы применения эллиптических кривых: рассмотрена задача о конгруэнтных числах, осуществлен плавный переход к понятию эллиптических кривых. ЭК были рассмотрены над различными полями: вещественными, рациональными, комплексными, конечными. Были даны основные определения и рассмотрены базовые операции над точками кривых. По ходу рассуждения приведены необходимые теоремы и их доказательства. Изучены основные задачи, существующие в криптографии: факторизации и проверки на простоту, и способы применения эллиптических кривых для их решения. Рассмотрена задача дискретного логарифмирования и методики её решения, в которых применяются эллиптические кривые. Рассмотрены протоколы и алгоритмы, базирующиеся на свойствах эллиптических кривых в рамках их применения для решения задач криптографии.

Применение эллиптических кривых в криптографии обладает как преимуществами, так и недостатками. К преимуществам относятся:

1. Меньшая длина ключа, чем в RSA. 160-битный ключ обеспечивает аналогичный уровень безопасности, что и 1024-битный для RSA. Из этого факта вытекают остальные преимущества использования эллиптических кривых

2. Большая скорость работы алгоритма. Ускорение может быть более чем десятикратным по сравнению с RSA.
3. Меньшие требования к производительности устройств и объёму установленной на них памяти.

Недостатки же связаны со сложностью теоретической базы, необходимой для понимания функционирования криптосистем на эллиптических кривых и вытекающей из этого сложности реализации соответствующих алгоритмов, что обусловливает большее число ошибок. Плюсом RSA является тот факт, что за долгое время его применения, подход стал хорошо отлажен, а теория, лежащая в его основе, относительно проста для понимания.