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

Некоторые вопросы эллиптической криптографии

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 2 курса 227 группы

направления 02.04.01 «Математика и компьютерные науки»

механико-математического факультета

Россинской Лины Андреевны

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

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

Саратов 2017 г.

Введение

Криптографией называется очень древняя наука, занимающаяся формированием алгоритмов шифрования различных сообщений и документов, ориентированных на безопасность засекреченной информации и ее основные принципы – конфиденциальность, целостность, доступность только легальным пользователям. Для шифрования сообщений, реализации алгоритма цифровой подписи, алгоритма факторизации больших чисел и других важных явлений и методов криптографии в настоящее время широко используются группы точек эллиптической кривой - точки алгебраической кривой, редуцированной (вычисления проводятся по модулю характеристики N) и заданной над конечными структурами.

Применение эллиптической кривой в криптографии было открыто в 1985 году Н. Коблицем и В. Миллером. Это положило начало новому этапу развития криптографии, что соответственно сопровождалось ростом научных трудов, раскрывающих данную тему.

Эллиптическая криптография изучает ассимитритричные криптосистемы – системы шифрования, в которых задействована пара ключей - открытый ключ находится в общем доступе, а к закрытому имеет доступ только одна сторона, получатель зашифрованного сообщения, который используя открытый и закрытый ключ и выполняя с ними некоторые вычисления, сможет расшифровать сообщение.

Основное преимущество использования эллиптической кривой в криптографии – сложность вычисления дискретного логарифма на эллиптической кривой и, как следствие, отсутствие быстрых алгоритмов взлома криптосистем, основанных на задаче дискретного логарифмирования на эллиптических кривых, все это при меньшем размере ключа. В данной работе систематизируется информация, касающаяся некоторых вопросов эллиптической криптографии, что обосновывает ее актуальность и значимость.

Целью данной работы является изучение и анализ некоторых вопросов эллиптической криптографии. Новизной данной работы является понимание и реализация алгоритма сложения с помощью эллиптической кривой и алгоритма разложения на множители с помощью эллиптической кривой. Главными задачами является определение эллиптической кривой, рассмотрение ее свойств и особенностей, которые имеют приложение в криптографии, рассмотрение основных криптосистем на эллиптической кривой - протокол распределения ключей Диффи-Хеллмана, криптосистема Эль-Гамаля и Мэсси-Амура, а также алгоритм электронной цифровой подписи на эллиптичской кривой, алгоритма вычисления порядка группы точек на эллиптической кривой (алгоритм Шуфа), исследование важных приложений эллиптической кривой в криптографии – в частности критерия простоты (алгоритм Голдвассер-Килиана) и метода факторизации больших чисел с использованием эллиптической кривой (метод Ленстры).

Основное содержание работы

Определение 1. Пусть K – поле характеристики, отличной от 2, 3, и $x^3 + ax + b$ (где $a, b \in K$) – кубический многочлен без кратных корней. Эллиптическая кривая над K – это множество точек (x, y), $x, y \in K$, удовлетворяющих уравнению

$$y^2 = x^3 + ax + b \tag{1}$$

вместе с O – единственным бесконечно удаленным элементом.

Если $F(x, y) = 0$ - неявное уравнение, выражающее y как функцию x в 1, то есть $F(x, y) = y^2 - x^3 - ax - b$ (или $F(x, y) = y^2 + cy + x^3 + ax + b, y^2 + xy + x^3 + ax + b, y^2 - x^3 - ax^2 - bx - c$), то точка (x, y) этой кривой называется неособенной (или гладкой), если, по крайней мере, одна из частных производных $\frac{\partial F}{\partial x}$, $\frac{\partial F}{\partial y}$ в этой точке не равна нулю. Условие отсутвия кратных корней эквивалентно требованию, чтобы все точки были неособенными. Дискриминант этого уравнения $\Delta = 4a^3 + 27b^2 \neq 0$.

Пусть $K = R$ - поле вещественных чисел. Определим операцию сложения точек на эллиптической кривой.

Определение 2. Пусть P и Q - две точки на эллиптической кривой E над вещественными числами. Определим точки $-P$ и $P + Q$ по следующим правилам:

1. Если P – точка в бесконечности O, то она выступает в роли нулевого элемента $-P = O$ и $P + Q = Q$.

2. Если точки $P = (x, y)$ и $-P$ имеют одинаковые x-координаты, а их y-координаты различаются только знаком, т.е. $-(x, y) = (x, -y)$, точка $(x, -y)$ – также точка на E.
3. Если P и Q имеют различные x-координаты, то прямая $\overline{PQ}$ имеет с E еще одну точку пересечения R (за исключением случая, когда она является касательной в P, $R = P$ или касательной в Q, $R = Q$). Тогда $P + Q$ определяется как $-R$.
4. Если точки симметричны, т.е. $Q = -P$, то $P+Q = O$ (следствие пункта 1).
5. Если $P = Q$, l – касательная к кривой в точке P, R – единственная другая точка пересечения l с E, то $P + Q = -R$.

Операции сложения и удвоения точек имеют аналитические выражения. Приведем формулы для нахождения координат третьей точки $P + Q$. Пусть (x_1, y_1), (x_2, y_2), (x_3, y_3) - координаты точек P, Q, $P + Q$ соответственно. Координаты точки $P + Q$ можно представить следующим образом:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \quad y_3 = -y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3). \tag{2}$$

Для координат удвоенной точки верно:

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1, \quad y_3 = -y_1 + \frac{3x_1^2 + a}{2y_1}(x_1 - x_3). \tag{3}$$

Реализация алгоритма сложения точек на кривой приведена в Приложении магистерской работы на языке Python.

Множество точек эллиптической кривой с введенной на нем операцией сложения является аддитивной циклической (абелевой) группой.

Сложение точек эллиптической кривой над конечным полем F_q с $q = p$ или $q = p^r$ элементами выполняется по формулам 2. Все операции в этом случае производятся по $\mod p$. Группой точек эллиптической кривой E над полем F_q называется множество

$$E(K) = \{(x, y) \in F_q \times F_q : y^2 \equiv x^3 + ax + b \pmod p\} \cap \{O\}$$

Важным понятием эллиптической криптографии является порядок эллиптической кривой, который показывает количество точек кривой над конечным полем. Рассмотрим теорему Хассе, дающую оценку количеству точек эллиптической кривой.

Теорема 3. *Теорема Хассе* Пусть p – простое число, $p > 3$, $E_{a,b}$ – эллиптическая кривая, определенная над конечным полем $\mathbb{Z}/p\mathbb{Z}$. Тогда

$$||E_{a,b}(\mathbb{Z}/p\mathbb{Z})| - (p+1)| < 2\sqrt{p}.$$

Определение 4. Пусть E - эллиптическая кривая над F_q и $P, Q \in E(F_q)$. Задача дискретного логарифмирования на E - это задача нахождения для данных точек такого целого числа $x \in Z$, что $xP = Q$. Обозначим $x = \log_P Q$.

Задача дискретного логарифма на эллиптической кривой является более трудной для решения, чем задача дискретного логарифмирования в конечных полях.

Протокол распределения ключей Диффи-Хеллмана на эллиптической кривой

Сначала выбирается простое число $p \approx 2^{180}$ и параметры a и b для уравнения эллиптической кривой $E_p(a,b)$. Потом в $E_p(a,b)$ выбирается генерирующая точка $G = (x_1, y_1)$, при выборе которой важно, чтобы наименьшее значение n, при котором $nG = 0$, оказалось очень большим простым числом. Параметры $E_p(a,b)$ и G криптосистемы являются открытыми параметрами.

Обмен ключами между пользователями A и B производится по следующей схеме:

1. Участник A выбирает целое число n_A, меньшее n. Это число является закрытым ключом участника A. Затем участник A вычисляет открытый ключ $P_A = n_A \cdot G$, который представляет собой некоторую точку на $E_p(a,b)$.
2. Участник B выбирает закрытый ключ n_B и вычисляет открытый ключ P_B.
3. Участники обмениваются открытыми ключами, после чего вычисляют общий секретный ключ K.

Участник A: $K = n_A \cdot P_B$, участник B: $K = n_B \cdot P_A$.

Таким образом, оба пользователя получат общее секретное значение (координаты точки $n_A n_B P$), которое они могут использовать для получения ключа шифрования. Злоумышленнику для восстановления ключа потребуется решить сложную с вычислительной точки зрения задачу определения n_A и n_B по известным E, P, $n_A P$ и $n_B P$. Равенство ключей обеспечивается соотношением $K_{A,B} = n_A \cdot P_B = n_A \cdot (n_B \cdot G) = n_B \cdot (n_A \cdot G)$. Так как точка на эллиптической кривой имеет две координаты, то можно в качестве ключа брать либо только координату x, либо только координату y, либо их сумму $x + y$.

Схема Эль-Гамаля на эллиптической кривой

Необходимо зашифровать сообщение , которое может быть представлено в виде точки на эллиптической кривой $P_m(x, y)$.

Как и в случае обмена ключом, в системе шифрования/дешифрования в качестве параметров рассматривается эллиптическая кривая $E_p(a, b)$ и точка G на ней. Пользователь B выбирает закрытый ключ n_B и вычисляет открытый ключ $P_B = n_B \cdot G$. Для шифрования сообщения P_m используется открытый ключ P_B получателя B. Пользователь A выбирает случайное целое число k и вычисляет зашифрованное сообщение C_m, точку на эллиптической кривой.

$$C_m = \{k \cdot G, P_m + k \cdot P_B\}$$

Чтобы дешифровать сообщение, B умножает первую координату точки на свой закрытый ключ и вычитает результат из второй координаты:

$P_m + k \cdot P_B - n_B \cdot (k \cdot G) = P_m + k \cdot (n_B \cdot G) - n_B \cdot (k \cdot G) = P_m$

Пользователь A зашифровал сообщение P_m добавлением к нему $k \cdot P_B$. Никто не знает значения k, поэтому, хотя P_B и является открытым ключом, никто не знает $k \cdot P_B$. Противнику для восстановления сообщения придется вычислить k, зная G и $k \cdot G$, что является достаточно трудной задачей.

Получатель также не знает k, но ему в качестве подсказки посылается $k \cdot G$. Умножив $k \cdot G$ на свой закрытый ключ, получатель получит значение, которое было добавлено отправителем к незашифрованному сообщению. Таким образом, получатель, не зная k, но имея свой закрытый ключ, может восстановить незашифрованное сообщение.

Криптосистема Мэсси-Омура на эллиптической кривой Элементы m - сообщения, которое нам необходимо передать, представлены точками P_m эллиптической кривой E над F_q (q- большое). Общее число точек N на кривой вычислено и не секретно. Каждый пользователь системы выбирает такое целое случайное число e между 1 и N, что НОД $(e, N) = 1$. Используя алгоритм Евклида, находится обратное e^{-1} к числу e по модулю N, то есть целое число d, такое, что $de \equiv 1 \pmod N$. Если пользователь A хочет послать пользователю B сообщение P_m, он сначала посылает точку $e_A P_m$. Пользователь B, не зная e_A и d_A, умножает на свое e_B и отсылает обратно пользователю A $e_B e_A P_m$. Далее пользователь A должен умножить $e_B e_A P_m$ на d_A. $NP_m = O$ и $d_A e_a \equiv 1 \pmod N$, получается в результате умножения точка $e_B P_m$. Пользователь A возвращает ее пользователю B, который, умножив точку $e_B P_m$ на d_B может прочитать сообщение. Злоумышленник может знать $e_A P_m$, $e_B e_A P_m$, $e_B P_m$.

Алгоритм электронной цифровой подписи на эллиптической кривой

Создание ключей:

Выбирается эллиптическая кривая $E_p(a, b)$. Число точек на ней должно делиться на большое целое n. Выбирается точка $P \in E_p(a, b)$. Выбирается случайное число $d \in [1, n-1]$. Вычисляется $Q = d \cdot P$. Закрытым ключом является d, (E, P, n, Q) - открытый ключ.

Создание подписи:

1. Выбирается случайное число $k \in [1, n-1]$.
2. Вычисляется $k \cdot P = (x_1, y_1)$ и $r = x_1(\mod n)$, r не должно быть равно нулю, иначе подпись не будет зависеть от закрытого ключа. Если $r = 0$, выбирается другое случайное число k.
3. Вычисляется $k^{-1} \mod n$.
4. Вычисляется $s = k^{-1}(H(M) + dr)(\mod n)$. Проверяется, чтобы s не было равно нулю, иначе необходимого для проверки подписи числа $s^{-1} \mod n$ не существует. Если $s = 0$, выбирается другое случайное число k.

5. Подписью для сообщения является пара чисел (r, s).

Проверка подписи:

1. Проверить, что целые числа r и s принадлежат диапазону чисел $[0, n-1]$. В противном случае результат проверки отрицательный, и подпись отвергается.
2. Вычислить $w = s^{-1} (\mod n)$ и $H(M)$.
3. Вычислить $u_1 = H(M)w(\mod n)$, $u_2 = rw(\mod n)$.
4. Вычислить $u_1P + u_2Q = (x_0, y_0)$, $v = x_0(\mod n)$.
5. Подпись верна в том и только том случае, когда $v = r$.

Критерий простоты. Алгоритм Голдвассер-Килиана.

Существует вероятностный алгоритм доказательства простоты натуральных чисел с помощью эллиптических кривых, алгоритм Голдвассера и Килиана. При этом для любого натурального числа k доля k-значных простых чисел, для которых среднее время работы алгоритма полиномиально, будет не меньше, чем

$$1 - O(2^{-k^{c/\log\log k}}).$$

Данный алгоритм случайным образом выбирает эллиптическую кривую и проверяет выполнение некоторых условий. Выдает либо верный ответ, является ли данное число простым или составным, либо делает следующий случайный выбор. Работает до тех пор, пока проверка простоты не будет проведена.

1 шаг. Пусть $p_0 = n$, $i = 0$. Выбирают $k \in \mathbb{N}$ такое, что $2^{k-1} < p_0 < 2^k$.

2 шаг. Случайно выбирают $A, B \in C$ и проверяют условие $D = (4A^3 + 27B^2, p_i) = 1$. Если $i = 0$ и данный наибольший общий делитель лежит в интервале $(1; p_0)$, то $p_0 = n$ – составное, и алгоритм заканчивает работу. Если $i > 0$ $1 < D < p_i$, нужно возвратиться на 1 шаг. Если $i > 0$ и $D = p_i$, то возвращаются на 2 шаг (выбирают другие A, B).

3 шаг. В предположении, что p_i – простое число, для редуцированной кривой $y^2 = x^3 + ax + b \pmod{p_i}$ ищут величину $|E_{p_i}(\mathbb{Z}/p_i\mathbb{Z})|$ (например, с помощью алгоритма Шуфа, приведенного в магистерской работе). Если найденное значение $|E_{p_i}(\mathbb{Z}/p_i\mathbb{Z})|$ нечетно, то возвращаемся на 2 шаг. В противном случае полагают

$$q = |E_{p_i}(\mathbb{Z}/p_i\mathbb{Z})|/2$$

и проверяется выполнение теоремы Хассе

$$|2q - p_i - 1| < 2\sqrt{p_i}.$$

Если это последнее неравенство не выполняется для $i > 0$, то возвращаются на 1 шаг. Если оно не выполняется при $i = 0$, то $n = p_0$ – составное.

4 шаг. Делают l проходов вероятностного теста Соловея-Штрассена (или Миллера-Рабина) для проверки простоты q. Если q – составное, то возвращаются на 2 шаг. Значение l выбирается так, чтобы выполнялось неравенство $\left(\frac{1}{2}\right)^l \leqslant 1/p^3$.

5 шаг. Выбирают случайную точку $P = (x, y)$, $P \in E_{p_i}(\mathbb{Z}/p_i\mathbb{Z})$, что означает, что $x \in \mathbb{Z}/p_i\mathbb{Z}$ выбирается случайно и при $\left(\dfrac{x^3 + ax + b}{p}\right) = 1$ находится $y \equiv (x^3 + ax + b)^{1/2} \pmod{p}$, затем полагают $P = (x, y)$; иначе делается следующий выбор x.

6 шаг. Находится $P = (x, y) \in E_{p_i}(\mathbb{Z}/p_i\mathbb{Z})$, проверяется выполнение равенства $2qP = O$ на $E_{p_i}(\mathbb{Z}/p_i\mathbb{Z})$. Если это равенство не выполняется и $i > 0$, то возвращаются на 1 шаг. Если оно не выполняется и $i = 0$, то n – составное. Если оно выполнено, то полагают $p_{i+1} = q$.

7 шаг. Проверяетя выполнение неравенства

$$q \leqslant 2^{k^{c/\log\log k}}.$$

Здесь постоянная c взята из оценки сложности

$$O((\log n)^{c \log\log\log n})$$

алгоритма проверки простоты чисел Адлемана-Померанса-Румели или алгоритма Ленстры. Если неравенство не выполняется, то полагают: $i := i + 1$ и возвращаются на 1 шаг. Иначе алгоритм заканчивает работу и выдает ответ, что n – простое.

Конец алгоритма.

Корректность работы алгоритма основана на следующем утверждении.

Пусть $n \in \mathbb{N}$, $n > 1$, $(n, b) = 1$, E_n – эллиптическая кривая над $\mathbb{Z}/n\mathbb{Z}$, $P = (x, y) \in E_n(\mathbb{Z}/n\mathbb{Z})$, $P \neq O$. Пусть q – простое число, $q > n^{1/2} + 2n^{1/4} + 1$, $qP = 0$. Тогда n – простое число.

В алгоритме Голдвассер—Килиана в случае успеха будет построена цепочка

$$n = p_0 > p_1 > \ldots > p_l,$$

и из простоты p_l будет следовать простота n, согласно доказанному утверждению.

Разложение на множители с помощью эллиптической кривой

Разложение в произведение простых сомножителей или факторизация согласно основной теореме арифметики всегда существует и является единственным (с точностью до порядка следования множителей). Методы факторизации используются для выявления небольших простых делителей числа, что находит свое применение в криптографии – многие криптосистемы (например, знаменитая криптосистема RSA) основаны на вычислительно сложной задаче разложения на множители, поэтому продвижения ученых в этой области имеют большую значимость.

Существует модифицированный метод Полларда, найденный Ленстрой , в котором вместо группы $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)$ используется группа точек эллиптической кривой $E \pmod p$.

Пусть E - эллиптическая кривая с уравнением $y^2 = x^3 + ax + b$, $Z_n = \{0, 1, 2, \ldots, n-1\}$ – основное множество для координат точек на ней. Z_n не является полем, на нем не всегда может выполняться операция нахождения обратного элемента, а значит и суммы точек кривой. В случае невозможности вычисления суммы точек $P(x_1, y_1)$ и $Q(x_2, y_2)$, разность первых координат $x_2 - x_1$ должна быть равной 0 по модулю одного из делителей n, тогда, чтобы найти искомый делитель, нужно вычислить $\gcd(n, x_2 - x_1)$. Идея алгоритма Ленстры состоит в выборе на E базовой точки P_0 и домножении ее на всевозможные простые числа и их степени, пока не получится

$$kP_0 = \infty \pmod{p}, \tag{4}$$

где p – один из делителей n.

Заранее ни один делитель нам не известен, поэтому условие 4 невозможно проверить. Признаком успешного выполнения алгоритма является выполнение условия $\gcd(n, C) = d > 1$ при вычисления λ в операции сложения и удвоения точек при вычислении очередного кратного C точки P_0.

Работа алгоритма состоит из двух этапов. На первом этапе главную роль играет параметр B_1 – ограничитель первого этапа. Алгоритм Ленстры аналогичен $p-1$-методу Полларда, где операция возведения возведения в степень простого числа p заменяется операцией домножения точки эллиптической кривой на множитель p.

Первая стадия алгоритма Ленстры

1. Выбрать B_1.
2. Выбрать случайным образом, используя любой детерменистический метод, числа $x, y, a \in [0, n-1]$
3. Вычислить $b = y^2 - x^3 - ax \pmod{n}$ и $g = \gcd(n, 4a^3 + 27b^2)$. Если $g = n$, возвратиться к пункту 2. Если $1 < g < n$, прекратить вычисление – делитель найден. Иначе, определить кривую E: $y^2 = x^3 + ax + b$ и базовую точку-генератор $P_0(x, y)$.
4. Присвоить изменяемому параметру $P(x, y)$ начальное значение P_0.

Вычисление:

1. Для каждого простого числа $p < B_1$ найти наибольшую степень r, чтобы $p^r < B_1$. Выполнить умножение $p \cdot P$ r раз, каждое умножение выполняя с помощью алгоритма нахождения кратной точки.
2. Продолжать вычисление до тех пор, пока не будут пройдены все простые числа, меньшие B_1 или не найдется шаг, на котором выполнится $\gcd(n, P) = d > 1$.

Если выполнится последнее условие, то искомый делитель n найден, иначе, необходимо увеличить B_1 и повторить все заново или перейти ко второй стадии алгоритма.

Вторая стадия алгоритма Ленстры

Пусть число точек на эллиптической кривой имеет лишь один делитель $q > B_1$.

1. Выбрать новую границу B_2, выписать все простые числа из интервала $[B_1; B_2]$:$\{q_1, q_2, \ldots, q_m\}$.
2. Вычислять последовательно точки $q_1 \cdot P$, $q_2 \cdot P$, $q_3 \cdot P$ и т.д., пока не достигнем B_2 или не выполнится 4.

Реализация алгоритма Ленстры и вывод рабты программы на языке Python приведены в Приложении магистерской работы. Как можно увидеть, программа выводит один из делителей заданного числа и время работы.

Заключение В магистерской работе изложены математические понятия, связанные с эллиптическими кривыми, приведено описание операции сложения, использующейся в эллиптической криптографии. Рассмотрены основные варианты криптосистем с использованием эллиптических кривых - аналог обмена ключами Диффи-Хеллмана, схемы Эль-Гамаля, криптосистемы Мэсси-Омура, алгоритм электронной цифровой подписи с использованием эллиптических кривых. Также в работе были проанализированы и выявлены преимущества и недостатки использования эллиптической криптографии. Описан алгоритм вычисления порядка группы точек эллиптической кривой над конечным полем (алгоритм Шуфа), а также рассмотрены некоторые приложения эллиптической кривой – критерий простоты (критерий Голдвассер-Килиана) и разложение на множители с помощью эллиптической кривой (метод Ленстры). Были реализованы некоторые алгоритмы, описанные в данной работе, на языке Python, а именно – сложение точек эллиптической кривой и алгоритм факторизации с помощью эллиптических кривых (метод Ленстры).

Эллиптическая криптография - относительно новое направление, широко распространенное в настоящее время. Данная работа позволит систематизировать представление об эллиптических кривых и их применении в криптографии, что, в свою очередь, может привести к новым решениям в этой области. Вдобавок, необходимо сказать, что дальнейший прорыв в криптографии можно совершить, используя свойства гиперэллиптических кривых.