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

Криптография на эллиптических кривых

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента (ки) 4 курса 421 Группы
направление (специальность) 02.03.01 Математика и компьютерные науки

Механико-математического факультета

Магомедшерифова Бекера Гюлеметовича

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

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

Саратов 2017

ВВЕДЕНИЕ

Вместе с неограниченными возможностями компьютерные технологии приносят новые проблемы, главной из них стала проблема защиты информации. Одновременно с улучшениями систем защиты совершенствуются и алгоритмы взлома. А это в свою очередь требует немедленного усовершенствования и повышения надежности защиты персональных данных. Для этого был создан раздел науки под название криптология, чьим основным направлением является криптография.

Криптография в основном базируется на методах предлагаемых алгебраической геометрией, абстрактной алгеброй, теорией чисел.

Один из таких перспективных методов основан на теории эллиптических кривых над конечными полями, разработанной, независимо друг от друга, Нилом Коблицем и Виктором Миллером в конце прошлого столетия для применения в криптографии.

Большинство современных криптографических систем естественным образом можно перестроить на крипстосистемы на эллиптических кривых, основанные на задаче дискретного логарифмирования на эллиптической кривой над конечными полями. Основная идея заключается в том, что известный алгоритм, используемый для конкретных конечных групп, переписывается для использования рациональных точек эллиптических кривых.

В работе представлено три раздела. В первом собраны необходимые определения и теоремы из теории эллиптических кривых и рассмотрены особенности таких кривых, задаваемых над различными полями. Также представлены формулы для подсчета суммы двух точек эллиптической кривой. Во втором разделе дается оценка количества точек эллиптической кривой, описываются алгоритмы подсчета точек. В третьем рассмотрены основные криптосистемы на эллиптических кривых, такие как аналог ключевого обмена Диффи-Хеллмана, аналог системы Эль-Гамаля, аналог криптосистемы RSA.

1 Основное содержание работы

В **Разделе 1** собрана основная теория эллиптических кривых и рассмотрены особенности эллиптических кривых над различными полями.

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

$$y^2 = x^3 + ax + b, \qquad (1)$$

вместе с единственным элементом, обозначаемым O и называемым «точка в бесконечности».

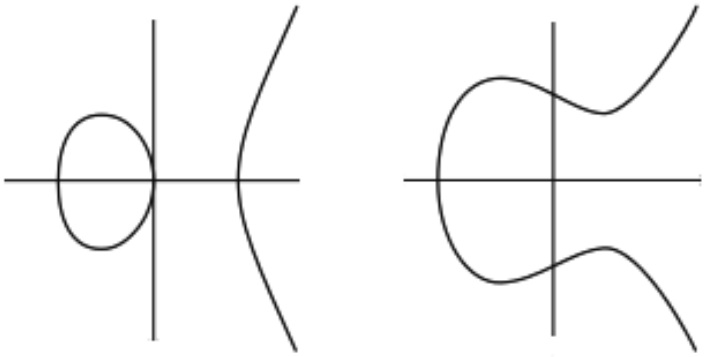

Рисунок 1

Если K - поле характеристики 2, то эллиптическая кривая над K - это множество точек, удовлетворяющих уравнению типа

$$y^2 + cy = x^3 + ax + b, \qquad (2')$$

либо типа

$$y^2 + xy = x^3 + ax^2 + b, \qquad (2'')$$

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

$$y^2 = x^3 + ax^2 + bx + c, \qquad (3)$$

Рассмотрели эллиптические кривые над *полем вещественных чисел*.

Поскольку характеристика поля вещественных чисел — 0, а не 2 или 3, то эллиптическая кривая — плоская кривая, определяемая уравнением вида $y^2 = x^3 + ax + b$, где a и b — вещественные числа.

Определение эллиптической кривой также требует, чтобы кривая не имела особых точек. Это значит, что график не должен иметь каспов и самопересечений. Достаточно проверить, что дискриминант $\Delta = -16(4a^3 + 27b^2)$ не равен 0.

Отметим, что множество точек эллиптической кривой образуют абелеву группу.

Определение 2. Пусть E -эллиптическая кривая над вещественными числами, и пусть P и Q - две точки на E. Определим точки $-P$ и $P + Q$ по следующим правилам.

1. Если P - точка в бесконечности O, то $-P = O$ и $P + Q = Q$, т. е. O - тождественный элемент по сложению («нулевой элемент») группы 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, а их y-координаты различаются только знаком, т. е. $-(x, y) = (x, -y)$.. Из пункта (1) сразу следует, что $(x, -y)$ - также точка на E.
3. Если P и Q имеют различные x-координаты, то прямая $l = PQ$ 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 в Q, и мы тогда полагаем $R = Q$). Определяем теперь $P + Q$ как точку $-R$, т.е. как отражение от оси x третьей точки пересечения. Геометрическое построение, дающее $P + Q$, приводится ниже в примере.

4. Если $Q = -P$ (т.е. x-координата Q та же, что и у P, а -координата отличается лишь знаком), то полагаем $P + Q = O$ (точке в бесконечности; это является следствием пункта (1)).
5. Остается возможность $P = Q$. Тогда считаем, что l - касательная к кривой в точке P. Пусть R - единственная другая точка пересечения l с E. Полагаем $P + Q = -R$ (в качестве R берем P, если касательная прямая в P имеет «двойное касание», т.е. если P есть точка перегиба кривой).

Над *полем рациональных чисел*.

Порядком точки P на кривой E называется наименьшее натуральное N такое, что $NP = O$.

Теорема Морделла. На эллиптической кривой E существует такое конечное множество рациональных точек бесконечного порядка $P_1, P_2, \ldots, P_n$, что любая точка на эллиптической кривой представляется в виде:

$$P = a_1P_1 + a_2P_2 + \ldots + a_nP_n + Q,$$

где $a_1, \ldots, a_n$ - целые числа, однозначно определенные для точки P, а Q - точка кручения, являющаяся точкой конечного порядка.

Над *конечными полями*. Оценку точек эллиптической кривой дает теорема Хассе.

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

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

В **Разделе 2** рассматриваются точки эллиптической кривой их количество, описываются алгоритмы подсчета точек.

Если N нечетно, то под нетривиальной точкой порядка N мы будем подразумевать точку $P \neq 0$, такую, что $NP = 0$. Если N четно, то под нетривиальной точкой порядка N мы будем подразумевать точку $P \neq 0$, такую, что $NP = 0$, но $2P \neq 0$.

Предложение 3. Пусть $y^2 = f(x)$ - эллиптическая кривая над любым полем K характеристики, не равной двум. Тогда имеется не более чем N^2 точек порядка N над любым расширением K' поля K.

Алгоритмы расчета точек:

Алгоритм 1.

Вход: Эллиптическая кривая $E(K) : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_5$.

Выход: Число N точек эллиптической кривой $E(K)$.

Метод.

1. Выбрать точку $Q \in E(K)$. Для этого выбрать случайную координату $x_0 \in K$ так, чтобы существовала y-координата $y_0 \in K$, удовлетворяющая уравнению кривой.
2. Найти целок число $k \leftarrow [\sqrt[4]{2q}]$.
3. Вычислить точки $Q, 2Q, 3Q, \ldots, kQ$ и отсортировать полученную базу данных по x координате (при этом оказываются известными точки $-Q, -2Q, \ldots, -kQ$).
4. Вычислить точки $P \leftarrow (2k+1)Q, R \leftarrow (q+1)Q$, после чего сравнить поочередно x-координаты точек $R, R \pm P, R \pm 2P, \ldots, R \pm kP$ с базой данных (равенство означает, что $R + dkQ = eQ$ для некоторых целых d, e). Отсюда найти предполагаемое число точек: $N \leftarrow q + 1 + dk - e$.
5. Результат N.

Алгоритм Чуфа для вычисления числа N точек эллиптической кривой E над полем K использует вычисления в полях функций $K[x, y]/(E(K), f_{l_i}(x))$, где $(E(K))$ – идеал, задающий кривую, $f_{l_i}(x)$ – полиномы деления, и содержит три шага:

1. вычисление набора попарно взаимно простых чисел $\{l_i\}$ и соответствующих полиномов деления в кольце $K[x]$;
2. нахождение вычетов числа $T = q + 1 - N$ по модулям малых взаимно простых чисел l_i

3. восстановление числа точек по китайской теореме об остатках.

В **Разделе 3** изложены вводная теория криптографии, основные криптосистемы на эллиптических кривых, основанные на задаче дискретного логарифмирования на эллиптической кривой над конечным полем.

По определению, криптосистема с открытым ключом обладает тем свойством, что знание шифрующего преобразования не позволяет по ключу шифрования найти ключ дешифрования, избежав чрезвычайно длинных вычислений. Другими словами, шифрующая функция $f : \mathcal{P} \to \mathcal{C}$ легко вычисляется, если ключ шифрования известен, но вычислять значения обратной функции $f^{-1} : \mathcal{C} \to \mathcal{P}$ очень сложно, если конечно не известна дополнительная информация (ключ дешифрования).

Определение 5. Дискретный логарифм на Е. Пусть E - эллиптическая кривая над F_q и B - точка на E. Задачей дискретного логарифмирования на E (с основанием B) называется задача нахождения для данной точки $P \in E$ такого целого числа $x \in Z$ (если оно существует), что $xB = P$.

Эллиптическая криптография относится к разряду асимметричной, то есть шифрование происходит с помощью *открытого ключа*. Это было обосновано тем, что дискретный логарифм на эллиптической кривой оказался сложнее классического дискретного логарифма на конечном поле. До сих пор не существует быстрых алгоритмов взлома сообщения, зашифрованного с помощью эллиптической кривой.

Представлены аналоги систем с открытым ключом в конечных полях, основанные на задаче дискретного логарифмирования на эллиптической кривой над полем F_q.

Аналог ключевого обмена Диффи-Хеллмана. Сначала открыто выбирают какое-либо конечное поле F_q и какую-либо эллиптическую кривую E над ним. Их ключ строится по случайно точке P на этой эллиптической кривой. Если у них есть случайная точка P , то, например, ее x-координата дает случайный элемент F_q, который можно затем преобразовать в r-разрядное целое

число в p-ичной системе счисления (где $q = p^r$), и это число может служить ключом в их классической криптосистеме. Они должны выбрать точку P так, чтобы все их сообщения друг другу были открытыми и все же никто, кроме них двоих, ничего бы не знал о P.

А и Б первым делом открыто выбирают точку $B \in E$ в качестве «основания». Мы не требуем, чтобы B была образующим элементом в группе точек кривой E. Эта группа может быть и не циклической. Нам хотелось бы, чтобы порожденная B подгруппа было большой, предпочтительно того же порядка величины, что и сама E. Предположим, что B - взятая открыто точка на E весьма большого порядка (равно N, либо большому делителю N).

Чтобы образовать ключ, А случайным образом выбирает целое число a, сравнимое по порядку величины с q (которое близко к N); это число она держит в секрете. Она вычисляет $aB \in E$ и передает это точку открыто. Б делает тоже самое: он выбирает случайно b и открыто передает $bB \in E$. Тогда используемый ими секретный ключ - это $P = abB \in E$. Оба пользователя могут вычислить этот ключ. Например, А знает bB (точка передана открыто) и свое собственной секретное a. Однако любая третья сторона знает лишь aB и bB. Кроме решения задачи дискретного логарифмирования - нахождения a по B и aB (или нахождения b по B и bB), - по видимому, нет способа найти abB, зная лишь aB и bB.

Аналог системы Мэсси-Омуры Это криптосистема с открытым ключом для передачи элементов сообщения m, которые мы теперь предположим представленными точками P_m фиксированной (и не скрываемой) эллиптической кривой E над F_q (q берется большим). Предполагается также, чтобы общее число N точек на E вычислено и не составляет секрета. Каждый пользователь системы секретно выбирает такое целое случайное число e между 1 и N, что НОД$(e, N) = 1$. Используя алгоритм Евклида он находит затем обратное $e^{(-1)}$ к числу e по модулю N, т.е. такое целое число d, что $de \equiv 1(modN)$.

Если А хочет послать Б сообщение P_m, то он сначала посылает ему

точку $e_A P_m$. Это ничего не говорит Б, который, не зная ни e_A, ни d_A, не может восстановить P_m. Однако, не придавая этому значения, он умножает ее на свое e_B и посылает обратно А $e_B e_A P_m$.

На третьем шаге А должен частично раскрыть свое сообщение, умножив $e_B e_A P_m$ на d_A. Так как $NP_m = 0$ и $d_A e_A \equiv 1(modN)$, при этом получается точка $e_B P_m$, которую А возвращает Б. Тот может теперь прочитать сообщение, умножив точку $e_B P_m$ на d_B.

Аналог системы Эль-Гамаля.Это - криптосистема с открытым ключом для передачи сообщений P_m. Мы исходим из данных не секретных:

1. конечного поля F_q
2. определенной над ним эллиптической кривой E
3. точки-«основания» B на ней.

(Знать общее число N точек на E нам не нужно). Каждый из пользователей выбирает случайное целое число a, которое держит в секрете, затем находит и делает общедоступной точку aB.

Чтобы послать Б сообщение P_m, А выбирает случайно целое число k и посылает пару точек $(kB, P_m + k(a_B B))$ (где $a_B B$ - открытый ключ Б). Чтобы прочитать сообщение, Б умножает первую точку из полученной пары на свое секретное число a_B и вычитает результат умножения из второй точки:

$$P_m + k(a_B B) - a_B(kB) = P_m$$

Таким образом, А посылает замаскированное P_m вместе с «подсказкой» kB, при помощи которой можно снять «маску» $ka_B B$, если знать секретное число a_B. Злоумышленник, который умеет решать задачу дискретного логарифмирования на E, может, конечно найти a_B, зная $a_B B$ и B.

Также в этом разделе представлены *способы выбора точки и кривой.*

Случайный выбор (E,B). Выбираем сначала случайным образом три элемента из F_q^* в качестве x, y, a. Далее полагаем $b = y^2 - (x^3 + ax)$. Убеждаемся в том, что кубический многочлен $x^3 + ax + b$ не имеет кратных корней,

что равносильно проверке условия $4a^3+27b^2 \neq 0$. (Если это условие не выполняется, берем другую случайную тройку x, y, a). Полагаем $B = (x, y)$. Тогда B - точка на эллиптической кривой $y^2 = x^3 + ax + b$.

Редукция глобальной пары (E,B) по модулю p. Выберем сначала «глобальную» эллиптическую кривую E и точку B бесконечного порядка на ней.

Далее мы выбираем большое простое число p (или, если наша кривая определена над расширением K поля Q, выбираем некоторый простой идеал в K) и рассматриваем редукцию E и B по модулю p. Точнее, для всех p, за исключением нескольких малых простых чисел, коэффициенты в уравнении для E имеют взаимно простые с p знаменатели и , следовательно, могут рассматриваться как коэффициенты в уравнении по модулю p. Если сделать замену переменных, приведя полученное уравнение над F_p к виду $y^2 = x^3 + ax + b$, то кубический многочлен в правой части не будет иметь кратных корней (за исключением нескольких малых простых p) и поэтому дает эллиптическую кривую над F_p (которую мы будем обозначать $E(modp)$). Координаты точки B, будучи также приведенными по модулю p, дают точку на эллиптической кривой $E(modp)$, которую мы будем обозначать $B(modp)$. При использовании этого способа мы раз и навсегда фиксируем E и B и за счет этого получаем много различных возможностей изменения простого p.

Еще в данном разделе было изложено как для представленных криптосистем надлежащим образом *выбрать точку* B.

Описанных криптосистемы могут быть надежными, даже если точка B не является порождающим элементом. Фактически нужно, чтобы в циклической группе, порождаемой B, задача дискретного логарифмирования не была эффективно разрешима. Это будет выполняться, если порядок B делится на очень большое простое число,например, имеющее порядок величины, близкий к N.

Один из способов гарантировать, что наш выбор B является надлежащим (т.е B порождает эллиптическую кривую) - это взять такую эллиптическую

кривую и такое конечное поле, чтобы число точек N было простым числом. Тогда всякая точка $B \neq 0)$ будет порождающим элементом.

Если использовать первый из описанных выше методов, то при фиксированном F_p можно продолжать выбор пар (E, B), пока не найдется такая, для которой число точек на E - простое число.

Если применять второй метод, то для фиксированной глобальной эллиптической кривой E над Q можно продолжать выбирать простые p, пока не найдем кривую $E(modp)$, число точек на которой - простое. Предполагается, что вероятность выбора p с требующимся свойством $O(\log p)$.

Замечание 2. Для того чтобы $E(modp)$ имела простой порядок N при большом p, надо выбирать E так, чтобы она имела тривиальное кручение, т.е. чтобы на ней не было точек конечного порядка, кроме O. В противном случае N будет делиться на порядок периодической подгруппы.

ЗАКЛЮЧЕНИЕ

В ходе данной работы были изложены основные моменты теории эллиптической криптографии. В частности, были рассмотрены аналоги систем с открытым ключом, основанные на задаче дискретного логарифмирования на эллиптической кривой, определенной над конечным полем; были показаны способы выбора эллиптической кривой и точки на ней с системах Эль-Гамаля и Диффи-Хеллмана; были изложены алгоритмы подсчета количества точек эллиптической кривой.

Подводя итог, следует отметить преимущества и недостатки эллиптической криптографии.

Плюсами являются:высокая стойкость к взлому, гораздо меньшая длина ключа по сравнению с классической асимметричной криптографией; скорость работы эллиптических алгоритмов гораздо выше, чем у классических; также из-за маленькой длины ключа и высокой скорости работы, алгоритмы криптографии на эллиптических кривых могут использоваться в устройствах с ограниченными вычислительными ресурсами.

Минусами являются то, что не всякая эллиптическая кривая подходит для построения криптосистемы; также то, что для переноса криптосистем на эллиптические кривые требуется серьезная теоретическая база. Массовый переход на эллиптические криптосистемы приведет к возникновению множества уязвимостей и ошибок, которые уже отработаны для привычных методов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Коблиц, Н. Введение в эллиптические кривые и модулярные формы. М.: Мир, 1988. С. 320.

2 Коблиц, Н. Курс теории чисел и криптографии. М.: ТВП, 2001. С. 254.

3 Ростовцев, А. Г., Маховенко, Е. Б.Теоретическая криптография. СПб.: Профессионал, 2005. С. 480.

4 Ленг, С. Эллиптические функции. М.: Наука, 1984. С. 312.

5 Кнэпп, Э. Эллиптические кривые. М.: Факториал, 2004. С. 488.

6 Ван дер Варден, Б. Л. Алгебра. М.: Наука, 1979. С. 623.

7 Вейль, А. Основы теории чисел. М.: Мир, 1972. С. 408.

8 Маховенко, Е. Б. Теоретико-числовые методы в криптографии. М.: Гелиос АРВ, 2006. С. 320.

9 Лидл, Р., Нидеррайтер, Х. Конечные поля. М.: Мир, 1988. С. 390.

10 Ростовцев, А. Г. Алгебраические основы криптографии. СПб.: Мир и Семья, 2000. С. 354.

11 Прасолов, В. В., Соловьев, Ю. П. Эллиптические кривые и алгебраические уравнения. СПб.: Факториал, 1997. С. 288.

12 Ростовцев, А.Г., Маховенко, Е.Б. Введение в криптографию с открытым ключом. СПб.: Мир и Семья, 2001. С. 336.

13 Нечаев, В.И. Элементы криптографии. Основы теории защиты информации. М.: Высшая школа, 1999. С. 109.

14 Мао, В. Современная криптография теория и практика. М.: Вильямс, 2005. С. 768.

15 Ященко, В.В. Введение в криптографию. М.: МЦНМО, 1999. С. 272.

16 Болотов, А.А., Гашков, С.Б., Фролов, А.Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006. С. 280.

17 Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2006. С. 335.

18 Смарт, Н. Криптография. М.: Техносфера, 2005. С. 528.

19 Баричев, С.Г., Серов, Р.Е. Основы современной криптографии.

20 Жельников, В. Криптография от папируса до компьютера. М.: ABF, 1996. С. 335.

21 Шнайер, Б. Прикладная криптография. М.: Диалектика, 2003. С. 610.