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

Трофименко Таисии Сергеевны

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

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

Саратов 2022

Введение. В последнее время все больше и больше внедряются в нашу повседневную жизнь информационные технологии, пытаясь захватить в ней все: от важнейших государственных проектов до решения обычных бытовых проблем. Одной из них является проблема защиты информации от несанкционированного посягательства теми, кто доступа к этой информации иметь не должен. В связи с этим почти одновременно с развитием информационных и компьютерных технологий начали развиваться и технологии защиты информации, развитие которых с некоторой точки зрения гораздо более критично, чем развитие непосредственно информационных технологий. Ведь с совершенствованием систем защиты, совершенствуются и методы взлома, обхода этих защит, что требует постоянного пересмотра и увеличения надежности защиты информации.

В последние два десятилетия все большее применение в криптографии находит одна из областей теории чисел и алгебраической геометрии – теория эллиптических кривых над конечными полями. Основная причина этого состоит в том, что эллиптические кривые над конечными полями доставляют неисчерпаемый источник конечных абелевых групп, которые (даже если они велики) удобны для вычислений и обладают богатой структурой. Шифрование данных методом эллиптических кривых преследует цели выработать метод быстрого и эффективного шифрования на базе эллиптической криптографии и в то же время повысить устойчивость шифрования (стойкость шифра) и целостность передаваемой информации в процессе протоколе обмена данными.

Роль основной криптографической операции выполняет операция скалярного умножения точки на эллиптической кривой на данное целое число, определяемое через операции сложения и удвоения точек эллиптической кривой. Последние, в свою очередь, выполняются на основе операции сложения, умножения и инвертирования в конечном поле, над которыми рассматривается кривая. Особый интерес к криптографии эллиптических кривых обусловлен теми преимуществами, которые дают её применение в беспроводных коммуникациях - высокое быстродействие и небольшая длина ключа.

Основное содержание работы. Рассмотрим важные определения.

Определение 1. Эллиптической кривой E над полем K называется множе-

ство точек (x, y), координаты которых принадлежат полю и удовлетворяют кубическому уравнению:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in K \tag{1}$$

Если K характеристика поля $p \neq 2$ и $p \neq 3$, то эллиптическая кривая над K - это множество точек, удовлетворяющих уравнению

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

Уравнением вида (2) называется формой Вейерштрасса[1].

Примеры эллиптических кривых представлены в соответствии с рисунком 1.

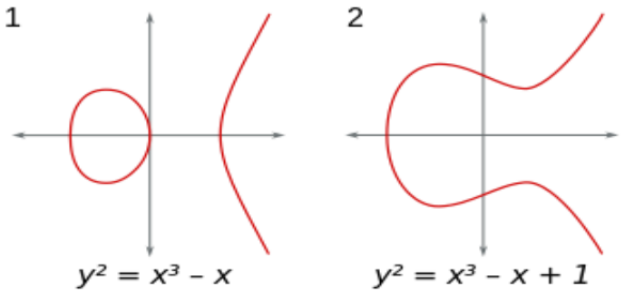

Рисунок 1 — Эллиптические кривые

Над полем действительных чисел эллиптическая кривая задается уравнением

$$y^2 = x^3 + ax + b.$$

Так как

$$y = \pm\sqrt{x^3 + ax + b},$$

то график кривой симметричен относительно оси абсцисс. Точки его пересечения с этой осью – корни кубического уравнения

$$x^3 + ax + b$$

[1]Коблиц, Н. Введение в эллиптические кривые и модулярные формы / Н. Коблиц. М.: Мир, 1988. - 320 с.

Здесь можно использовать формулу Кардано. Дискриминант вычисляется по формуле (3)

$$D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 \tag{3}$$

При этом: 1. если $D < 0$, то уравнение имеет три разных действительных корня α, β и γ; 2. если $D = 0$, то уравнение имеет действительные корни α, β, β , два из которых одинаковы; 3. если $D > 0$, то уравнение имеет один действительный корень α и два комплексных.

Определение 2. Эллиптическую кривую E называют сингулярной , если на кривой существует хотя бы одна особая точка $(x; y)$, в которой одновременно

$$\frac{\partial F}{\partial x} = 0 \text{ и } \frac{\partial F}{\partial y} = 0,$$

где $F(x, y) = y^2 + a_1xy + a_3y - x^3 + a_2x^2 + a_4x + a_6 = 0$.

Замечание 1. Если характеристика поля $p \neq 2$ и $p \neq 3$, то кривая $y^2 = x^3 + ax + b \ (mod\ p)$ будет несингулярной при условии, что ее дискриминант $D \neq 0$, а это, в свою очередь, эквивалентно условию $4a^3 + 27b^2 \neq 0(mod\ p)$ [2].

Отметим чрезвычайно важное свойство точек эллиптической кривой: они образуют абелеву группу относительно операции сложения точек. А именно:

1) элементы группы являются точками эллиптической кривой;

2) единичный элемент — это бесконечно удалённая точка 0;

3) обратная величина точки P — это точка,симметричная относительно оси x;

4) сложение задаётся следующим правилом: сумма трёх ненулевых точек P, Q и R, лежащих на одной прямой, будет равна $P + Q + R = 0$.

Стоит учесть, что в последнем правиле нам требуются только три точки на одной прямой, и порядок расположения этих трёх точек не важен. Это значит, что если три точки P, Q и R лежат на одной прямой, то $P+(Q+R) = Q+(P+R) = R+(P+Q) = \cdots = 0$. Таким образом интуитивно доказали, что наш оператор $+$ обладает свойствами ассоциативности и коммутативности: находимся в абелевой группе.

[2]Лекция 4 (2 семестр) БСит [Электронный ресурс]: [сайт]. - URL: https://bit.nmu.org.ua/ua/student/metod/cryptology/(дата обращения: 06.03.2022). - Загл. с экрана. - Яз.рус.

Далее рассмотрим эллиптические кривые над конечными полями и важную теорему Хассе - Вейля.

Эллиптические кривые над конечными полями имеют, естественно, конечные группы точек. Порядок этой группы будем называть порядком эллиптической кривой. Порядком точки P эллиптической кривой называется наименьшее число k такое, что $kP = O$. В соответствии с теоремой Лагранжа порядок точки делит порядок эллиптической кривой. При определении порядка кривой ее можно заменить на удобную изоморфную ей кривую, так как у изоморфных кривых порядки одинаковы.

Пользуясь символом Лежандра, легко указать формулу для числа точек на кривой $Y^2 = f(X)$ над полем $GF(p),\ p > 2$. Действительно, сравнение $Y^2 \equiv f(x)(mod\ p)$ относительно Y при фиксированном x имеет (при $p > 2$) $1+\frac{f(x)}{p}$ решений (это верно и при $f(x) = 0$). Учитывая бесконечно удаленную точку, получаем формулу для порядка кривой над полем $GF(p),\ p > 2$ в виде

$$p + 1 + \sum_{x=0}^{p-1} \frac{f(x)}{p} \tag{4}$$

При небольших простых p, используя эту формулу и теорию квадратичных вычетов, порядок кривой над полем $GF(p)$ находить довольно легко.

Расчет порядка эллиптической кривой не всегда прост или да же не возможен. Общая формула для вычисления порядка произвольной кривой неизвестна. Однако известны способы выбора эллиптических кривых над конечными полями, допускающих простое определение порядка. Эти способы очень важны, потому что в криптографическом отношении полезными являются эллиптические кривые, порядок которых содержит большие простые множители.

Известна асимптотически точная формула для порядка эллиптической кривой над конечным полем. Она была найдена в тридцатые годы немецким математиком Хельмутом Хассе.

Теорема 1. В соответствии с теоремой Хассе порядком N эллиптической кривой над полем $GF(q)$ удовлетворяет неравенству

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

Это эквивалентно системе неравенств

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

Теорема Хассе в случае простого конечного поля кажется интуитивно очевидной, так как квадратичные вычеты и невычеты по простому модулю распределены в определенном смысле равномерно и в сумме

$$\sum_{x=0}^{p-1} \frac{f(x)}{p}$$

слагаемые ± 1 ведут себя подобно случайному блужданию по прямой.

Справедлива и более общая теорема Хассе-Вейля:

Теорема 2. Пусть E - эллиптическая кривая над полем $GF(q)$ и N - порядок ее группы. Тогда для порядка $N(n)$ группы эллиптической кривой $E(GF(q^n))$ над полем $GF(q^n)$ справедливой формулы

$$N(n) = q^n + 1 - \alpha^n - \beta^n,$$

где α и β корни квадратного уравнения $x^2 - tx + q = 0$, в котором коэффициент $t = q + 1 - N$. Всегда выполняется неравенство $t^2 \leq 4q$ и в случае строгого неравенства корни квадратного уравнения α и β будут комплексно сопряженными [3].

В случае полей малой характеристики порядок группы эллиптической кривой легко найти по формуле (4).

Не более важную роль играет задача дискретного логарифмирования.

Задача 1. "Дискретный логарифм"

Даны примитивный элемент $g, b \neq 0$, простое число p. Найти x такое, что

$$g^x \equiv b \ (mod\ p).$$

[3] Жданов, О.Н. Эллиптические кривые. Основы теории и криптографические приложения / О.Н. Жданов, В. А. Чалкин. М.: Эдиториал УРСС, 2013. - 200 с.

Опишем сейчас применение дискретного логарифма для задачи формирования общего секретного ключа двумя пользователями (задача 2), связанными открытым (для противника) каналом связи.

Задача 2. "Формирование секретного ключа"

Абоненты A и B взаимодействуют по открытому каналу связи. Могут ли они, не имея вначале никакой секретной информации, организовать обмен так, чтобы в конце у них появлялся общий секретный ключ. Предполагается, что пассивный противник может перехватить все сообщения, которыми они обмениваются.

Диффи и Хеллман предложили решать эту задачу с помощью дискретного логарифма (алгоритм 1).

Алгоритм 1. Протокол выработки общего секретного ключа

1) A и B независимо друг от друга выбирают по одному натуральному числу X_A и X_B. Эти элементы они держат в секрете.

2) Каждый из них вычисляет новый элемент

$$Y_A \equiv a^{X_A} \ (mod\ p), \qquad Y_B \equiv a^{X_B} \ (mod\ p),$$

причем числа p и a считаются общедоступными. Потом они обмениваются этими элементами по каналу связи.

3) A получив Y_B и зная свой секретный элемент X_A вычисляет новый элемент

$$Y_B^{X_A} = (a^{X_B})^{X_A} \mod p.$$

Аналогично поступает B:

$$Y_a^{X_B} = (a^{X_A})^{X_B} \mod p.$$

После этого у A и B появился общий элемент $a^{X_a X_B} \mod p$, который и объявляется общим ключом.

Задача A Противник знает $p,\ a,\ a^{X_A}, a^{X_B}$, но не знает X_A и X_B и хочет узнать $a^{X_A X_B}$.

По гипотезе Диффи-Хеллмана такая задача — вычислительно трудна[4].

Определение 3. Пусть E - эллиптическая кривая над F_q и $P \in E(F_q)$ - фиксированная точка на ней. Задача дискретного логарифмирования на E - это задача нахождения такого целого числа $x \in Z$, что $xP = Q$, где Q - произвольная точка. Обозначим $x = \log_P Q$.

Задача дискретного логарифма на эллиптической кривой является более трудной для решения, чем задача дискретного логарифмирования в конечных полях. Она является простой лишь, например, если B как элемент группы G выбран малого порядка. Если группа G циклическая, то в качестве B нужно выбирать порождающий элемент, тогда для $0 \leq x \leq N-1$ логарифм $x = \log_P Q$ определяется однозначно, в противном случае логарифм может не существовать. На эллиптической кривой наиболее быстрые методы решения дискретного логарифма имеют сложность $O\sqrt{q}$, где q - количество точек эллиптической кривой.

Основные преимущества криптосистем на эллиптических кривых заключаются в том, что не известны алгоритмы дискретного логарифмирования для вскрытия этих систем, если в них не используются суперсингулярные кривые и кривые, порядки которых делятся на большое простое число[5].

Теперь, опишем аналог н систем с открытым ключом, основанные на задаче дискретного логарифмирования на эллиптической кривой, определенной над конечным полем F_q.

Протокол Диффи-Хеллмана. Предположим, что абоненты А и Б хотят договориться о ключе, которым будут впоследствии пользоваться в некоторой классической криптосистеме. Прежде всего, они открыто выбирают какое-либо конечное поле F_q и какую-либо эллиптическую кривую E над ним. Их ключ строится по случайной 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 (здесь пользуем словом «случайный»

[4]Шокуров, А.В Решетки, алгоритмы и современная криптография / А.В. Шокуров, Н.Н. Кузюрин, Фомин С.А. М.:[б. и.], 2008. - 125 с.

[5]Ростовцев, А.Г. Теоретичекая криптография / А.Г. Ростовцев, Е.Б. Маховенко. - Санкт - Петербург: НПО "Профессионал 2014. - 478 с.

в неточном смысле; лишь хотим сказать, что выбор из некоторого большого множества допустимых ключей произволен и непредсказуем). 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.

Рассмотрим алгоритм ключевого обмена Диффа-Хеллмана на эллиптических кривых.

Шаг 1. Абоненты (пользователи) А и Б первым делом открыто выбирают точку $b \in E$ в качестве «основания»; B играет ту же роль, что образующий q в системе Диффи-Хеллмана для конечных полей. Однако, не требуется, чтобы B была образующим элементом в группе точек кривой E. Эта группа может и не быть циклической. Даже если она циклическая, мы не хотим тратить время на проверку того, что B – образующий элемент (или даже на нахождение общего числа N точек, которое нам не понадобится в последующем). Нам хотелось бы, чтобы порожденная B подгруппа была большой, предпочтительно того же порядка величины, что и сама E. Пока что предположим, что B – взятая открыто точка на E весьма большого порядка (равного либо N, либо большому делителю N).

Шаг 2. Для того чтобы образовать ключ, А вначале случайным образом выбирает целое число a, сравнимое по порядку величины с q (которое близко к N); это число он держит в секрете. Он вычисляет $aB \in E$ и передает эту точку открыто.

Шаг 3. Абонент Б делает то же самое: он выбирает случайно b и открыто передает $bB \in E$.

Шаг 4. Тогда используемый ими секретный ключ – это $P = ab \in E$. Оба пользователя могут вычислить этот ключ. Например, А знает bB (точка была передана открыто) и свое собственное 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 .

В настоящее время для целей криптографии обычно используются эллиптические кривые над простым полем и над полем характеристики 2. В системах Диффи – Хеллмана и Эль-Гамаля существует два подхода к выбору эллиптической кривой и базовой точки на ней.

1. Случайный выбор.

Выбираем какое-либо большое конечное поле $GF(q)$ с характеристикой $p > 3$, в котором кривую можно будет задать уравнением $y^2 = x^3 + ax + b$. Произвольно задав тройку чисел $x, y, a \in GF(q)$, вычисляем $b = y^2 - (x^3 + + ax)$ и проверяем условие $4a^3 + 27b^2 \neq 0(mod\ p)$. Если оно выполнено, то кривая подобрана, а если нет, то выбираем другую случайную тройку x, y, a и повторяем процесс. Когда кривая подобрана, то точка $P(x, y)$ лежит на кривой. Если условие $4a^3 + 27b^2 \neq 0(mod\ p)$ не выполнено, то выбираем другую тройку x, y, a и т.д.

2. Редукция глобальной пары кривая – точка по $mod\ p$ (редукция данных – это сведение данных со сложной структурой к более простой форме).

Пусть E – эллиптическая кривая над полем рациональных чисел (назовем ее «глобальной») и $P(x, y)$ – точка бесконечного порядка на кривой. Например, точка $P(0; 0)$ является точкой бесконечного порядка на кривой $y^2 + y = x^3 - x^2$ и порождает всю группу рациональных точек на кривой. Далее выбираем большое простое число p и выполняем редукцию: для всех больших p коэффициенты в уравнении кривой E будут иметь обратные элементы по $mod\ p$ и могу рассматриваться как коэффициенты в уравнении кривой по $mod\ p$. Можно с помощью специальной замены переменных свести уравнение кривой к виду $y^2 = x^3 + ax + b$, где кубический многочлен не будет иметь кратных корней и дает поэтому эллиптическую кривую над полем $GF(p)$. Если координаты точки $P(x, y)$ также привести по модулю, то это даст искомую точку на эллиптической кривой. При использовании второго способа раз и навсегда фиксируем кривую E и точку $P(x, y)$, а меняя значения p , получаем много разных кривых над полем $GF(p)$.

Одна из гарантий, того что выбранная базовая точка $P(x, y)$ будет генератором группы, – это выбор таких кривой и поля, для которых количество точек кривой N_E – простое число (тогда любая точка будет генератором)[6].

Заключение. В данной работе были изложены основные понятия, связанные с теорией эллиптических кривых, рассмотрены особенности их использования в криптографии. Были рассмотрены способы, с помощью которых

[6]Жданов, О.Н. Эллиптические кривые. Основы теории и криптографические приложения / О.Н. Жданов, В. А. Чалкин. М.: Эдиториал УРСС, 2013. - 200 с.

может быть выбрана эллиптическая кривая и точки на ней, а также алгоритмы для вычисления суммы и удвоения точек.

Достоинствами такой криптографии является её надежность, поскольку нет точных алгоритмов для решения задачи дискретного логарифмирования на эллиптических кривых. Так же скорость работы эллиптических алгоритмов значительно выше, чем у алгоритмов классической криптографии. Преимущество эллиптических кривых над конечными полями заключается в том, что имеется большое многообразие групп с разными порядками для одного и того же поля $GF(q)$. Доказано, что для любого простого p порядки групп кривых над полем $GF(p)$ почти равномерно распределены на отрезке $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$. Это часто дает возможность подобрать кривую, порядок которой имеет только один большой простой делитель.

Однако есть и минусы, связанные с эллиптической криптографией, в частности то, что требуется правильный подбор эллиптической кривой, так как не всякая кривая подходит для построения криптосистемы.