МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНО ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра Компьютерной алгебры и теории чисел

# Криптосистемы на эллиптических кривых

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 2 курса 227 группы

направления 02.04.01 – математика и компьютерные науки

механико-математического факультета

Жадаевой Екатерины Михайловны

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

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

Саратов 2020

**Введение.** Теория эллиптических кривых является одним из важнейших разделов алгебраической геометрии, точнее ее раздела, изучающего плоские алгебраические кривые. Она тесно связана также с комплексным анализом и с теорией чисел, до сих пор интенсивно развивается и чрезвычайно обширна и сложна. В ее создании принимали участие многие крупнейшие математики прошлого, а начинается она с последнего из великих древнегреческих математиков — Диофанта. Структуру группы на эллиптических кривых определил знаменитый французский математик Анри Пуанкаре. Долгое время теория эллиптических кривых являлась чистейшей областью математики, не имеющей за ее пределами никаких приложений.

В криптографии с открытым ключом эллиптические кривые являются основой ряда алгоритмов ECC — криптографии на эллиптических кривых. Независимо друг от друга, идею создания эллиптической криптографии в своих работах выдвинули В. Миллер и Н. Коблиц. Эллиптические кривые вызывают такой интерес в криптографии из-за того, что с одной стороны они являются богатым источником конечных абелевых групп, обладающих полезными структурными свойствами, а с другой, на их основе обеспечиваются те же криптографические свойства, которыми обладают числовые или полиномиальные криптосистемы, но при существенно меньшем размере ключа.

Целью данной работы является изучение и анализ некоторых вопросов связанных с эллиптическими кривыми и основными криптосистемами на эллиптических кривых.

Для достижения поставленной цели были сформулированы и решены следующие задачи:

1. Дать основные определения и теоремы, связанные с теорией эллиптических кривых.

2. Привести описание некоторых методов, используемых для решения задачи дискретного логарифмирования.

3. Рассмотреть основные криптосистемы на эллиптических кривых, в частности аналог ключевого обмена Диффи-Хеллмана, и разработать его программную реализацию.

Работа состоит из введения, пяти разделов, заключения, списка использованных источников, включающего двадцать одно наименование, и приложения. Первые два раздела содержат в себе основные понятия об эллиптических кривых и конечных полях, особенности эллиптических кривых и их поведение в зависимости от того над какими полями заданы эти кривые. В третьем разделе описаны некоторые методы решения задачи дискретного логарифмировния, такие как $\rho$-метод Полларда, метод Гельфонда и Сильвера-Полига-Хеллмана и метод встречи посередине. Четвёртый раздел содержит описание необходимых понятий в криптографии и основные криптосистемы на эллиптических кривых, одними из которых являются аналог ключевого обмена Диффи-Хеллмана и аналог системы Мэсси-Омуры. В последнем, пятом, разделе находится описание реализации аналога ключевого обмена Диффи-Хеллмана для конкретной эллиптической кривой. Код этой реализации представлен в приложении.

Научная значимость работы заключается в систематизации сведений об использовании эллиптической криптографии для передачи информации.

**Основное содержание работы.** Основная часть состоит из пяти разделов.

Первый раздел представляет собой описание вспомогательных утверждений и теорем, связанных с алгебраическими и эллиптическими кривыми, таких как

**Определение 1.** Алгебраической кривой порядка $n$ над полем $F$ называется множество точек $(x, y), x, y \in F$, удовлетворяющих уравнению

$$F(X, Y) = 0,$$

где $F(X, Y)$ многочлен степени $n$ с коэффициентами из $F$ [1].

**Определение 2.** Эллиптической кривой $E$ над полем $F$ называется множество точек $(x, y)$ [2], координаты которых принадлежат полю и удовлетворяют уравнению

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

где $a_i \in F$.

**Определение 3.** Пусть $E$ — эллиптическая кривая над вещественными числами, и пусть $P$ и $Q$ — две точки на данной эллиптической кривой. Тогда 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. Долее будем полагать, что $P$ и $Q$ отличные от точек в бесконечности.
2. Точки $P = (x, y)$ и $-P$ имеют одинаковые $x$-координаты, в то время как их $y$-координаты различаются только знаком, т. е. $-(x, y) = (x, -y)$. Из пункта (1) следует, что $(x, -y)$ — также точка на кривой $E$.
3. Если $P$ и $Q$ имеют различные $x$-координаты, то прямая $I = PQ$ имеет с $E$ еще в точности одну точку пересечения $R$ (за исключением двух случаев: когда она оказывается касательной в $P$, и тогда полагаем $R = P$, или касательной в $Q$, и тогда полагаем $R = Q$). Определяем теперь $P + Q$ как точку $-R$, т. е. как отражение относительно оси $x$ третьей точки пересечения. Геометрическое построение, дающее $P + Q$.
4. Если $Q = -P$ (т.е. $x$-координата $Q$ та же, что и у $P$, а $y$-координата отличается лишь знаком), то полагаем $P + Q = O$ (точке в бесконечности; это является следствием пункта 1).
5. В случае, когда $P = Q$ считаем, что $I$ — касательная к кривой в точке $P$. Пусть $R$ — единственная другая точка пересечения $I$ 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) [3].

Второй раздел включает в себя некоторые вопросы, связанные с конечными полями и эллиптическими кривыми над ними.

Эллиптические кривые над конечными полями имеют 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.

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 порядок $N$ эллиптической кривой над полем $GF(q)$ удовлетворяет неравенству

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

Это эквивалентно системе неравенств

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

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 $GF(q^n)$ справедлива формула

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

где $\alpha$ и $\beta$ — 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 $\alpha$ и $\beta$ будут комплексно сопряженными.

В третьем разделе представлены основные методы решения задачи дискретного логарифмирования .

Задача дискретного логарифмирования, так же как и задача разложения на множители, используется во многих алгоритмах криптографии с открытым ключом. Данная задача послужила основой для создания протоколов шифрования и цифровой подписи, доказательств с нулевым разглашением и других криптографических протоколов [4].

**$\rho$-Метод Полларда.**

Рассмотрим алгоритм данного метода:

**Вход:**

Простое число $p$, число $a$ порядка $r$ по модулю $p$, целое число $b, 1 < b < p$; отображение $f$ обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.

**Выход:**

Показатель $x$, для которого $a^x \equiv b \pmod{p}$, если такой показатель существует.

**Алгоритм:**

1. Выберем произвольные целые числа $u, v$ и положим $c \leftarrow a^u b^v \pmod{p}$, $d \leftarrow c$.

2. Выполним $c \leftarrow f(c) \pmod{p}, d \leftarrow f(f(d)) \pmod{p}$, вычисляя при этом логарифмы для $c$ и $d$ как линейные функции от $x$ по модулю $r$, до получения равенства $c \equiv d \pmod{p}$.

3. Приравнивая логарифмы для $c$ и $d$, вычислим логарифм $x$ решением сравнения по модулю $r$.

**Результат:** $x$ или «Решений нет».

**Метод Гельфонда и Сильвера-Полига-Хеллмана.**

Алгоритм данного метода:

**Вход:**

Простое число $p$, число $a$ порядка $r$ по модулю $p$, где $r = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, целое число $b, 1 < b < p$.

**Выход:**

Показатель $x$, для которого $a^x = b \pmod{p}$, если такой показатель существует.

**Алгоритм:**

1. Для $i = 1, 2, \dots, n$ выполним следующие действия:

1.1. Положим $q \leftarrow p_i, \beta \leftarrow \alpha_i$.

1.2. Положим $c \leftarrow 1, y_{-1} \leftarrow 0$.

1.3. Вычислим $a' \leftarrow a^{\frac{r}{q}} \pmod{p}$.

1.4. Для $k = 0, 1, \dots, \beta - 1$ выполним следующие действия:

1.4.1. Положим

$$c \leftarrow c \cdot a^{y_{k-1} q^{k-1}} \pmod{p}, b' \leftarrow (bc^{-1})^{r/(q^{k+1})} \pmod{p}.$$

1.4.2. Вычислим логарифм $y_i \leftarrow \log_{a'} b'$ любым алгоритмом (например, p-методом Полларда).

1.5. Положим $x_i \leftarrow y_0 + y_1 q + \ldots + y_{\beta-1} q^{\beta-1} \pmod{q^\beta}$.

2. Восстановим логарифм $x$ из $x_1, x_2, \ldots, x_n$ по китайской теореме об остатках.

**Результат:** $x$.

**Метод встречи посередине.**

Метод встречи посередине представляет собой вероятностный вариант алгоритма Гельфонда и предполагает создание базы данных объема $O(\sqrt{r})$ из пар вида $(a^{x_j} \pmod p, x_j)$ для случайных чисел $x_j$ и ее сортировку по первой «координате». Для случайных чисел $y_i$ вычисляются значения $b^{y_i}$ и сравниваются с базой данных. Сравнение $b^{y_i} \equiv a^{x_j} \pmod p$ означает, что $xy_i \equiv$ $\equiv x_j \pmod r$, откуда $x \equiv x_j y_i^{-1} \pmod r$.

**Метод базы разложения.**

Рассмотрим алгоритм логарифмирования данным методом

**Вход:**

Простое число $p$, число $a$ порядка $r$ по модулю $p$, целое число $b, 1 < b < p$.

**Выход:** Показатель $x$, для которого $a^x \equiv b \pmod p$, если такой показатель существует.

**Алгоритм:**

1. Строим базу разложения $B \equiv \{-1, p_1, p_2, \ldots, p_h\}$ из первых простых чисел $p_j$, где $p_h \approx O(exp(c\sqrt{\ln p \ln\ln p})), c \approx 1$.

2. Случайным выбором показателей $u_i$ находим множество из $O(m)$ $B$-гладких чисел $l_i \leftarrow a^{u_i} \pmod p$ (при этом $B$-гладким может быть не $b_i$, а $p - b_i$, в этом случае в разложении участвует элемент -1 базы разложения):

$$b_i \equiv \prod_{j=0}^{h} p_j^{\alpha_{ij}} \pmod p. \qquad (1)$$

3. Подбором находим такой показатель $v$, что число $bv \pmod p$ является $B$-гладким:

$$b^v \equiv \prod_{j=0}^{h} p_j^{\beta_j} \pmod{p}. \tag{2}$$

4. Логарифмируя соотношения (1) и (2) по основанию $a$, запишем систему линейных сравнений:

$$u_i \equiv \sum_{j=0}^{h} \alpha_{ij} \log_a p_j \pmod{r}, xv \equiv \sum_{j=0}^{h} \beta_j \log_a p_j \pmod{r}.$$

5. Методом гауссова исключения выражаем $xv$ в виде линейной комбинации чисел $u_i$:

$$xv \equiv \sum_{i} d_i u_i \pmod{r}. \tag{3}$$

6. Если сравнение (3) имеет решение $x$, то

**Результат:** $x$. Иначе: «Решений нет».

Четвёртый раздел содержит основыные понятия криптографии и описание некоторых криптографий на эллиптических кривых, таких как аналог ключевого обмена Диффи-Хеллмана, аналог системы Мэсси-Омуры и аналог системы Эль-Гамаля, а так же способы выбора кривой и точки [5 — 6].

**Аналог ключевого обмена Диффи-Хеллмана.**

Рассмотрим алгоритм ключевого обмена Диффи-Хеллмана на эллиптических кривых.

**Шаг первый:** Пользователи А и Б первым делом открыто выбирают точку $B \in E$ в качестве «основания». В данном случае $B$ играет ту же роль, что образующий $g$ в системе Диффи-Хеллмана для конечных полей. Однако, не требуем, чтобы $B$ была образующим элементом в группе точек кривой $E$. Эта группа может и не быть циклической. Даже если она циклическая, не нужно тратить время на проверку того, что $B$ — образующий элемент (или даже на нахождение общего числа $N$ точек, которое не понадобится в последующем). 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 второй:** Для того чтобы образовать ключ, пользователь А вначале случайным образом выбирает целое число $a$, сравнимое по порядку величины с $q$ (которое близко к $N$), и держит его в секрете. Пользователь А вычисляет $aB \in E$ и передает эту точку открыто.

**Шаг третий:** Пользователь Б проделывает то же самое: он выбирает случайно $b$ и открыто передает $bB \in E$.

**Шаг четвертый:** Каждый из участников знает своё секретное число и значение, которое прислал ему другой пользователь. Тогда они оба могут получить секретный ключ, вычислив его с помощью своего секретного числа и открытого значения другого пользователя, как $P = abB \in E$. 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 $bB$.

**Аналог системы Мэсси-Омуры.**

Представляет собой криптосистему с открытым ключом. Рассмотрим алгоритм Месси-Омуры на эллиптических кривых.

Всем абонентам известна общедоступная информация, состоящая из кривой $E$, определенной в конечном поле $F_p$, ранга кривой $N$ и характеристикой поля $p$. Пусть вид кривой задается уравнением:

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

при этом

$$4a^3 + 27b^2 \neq 0, a, b \in F_p.$$

**Шаг первый:** Каждый из абонентов генерирует свою пару секретных чисел $e$ и $d$, являющиеся мультипликативно обратными по модулю ранга $N$:

$$ed \equiv 1 \pmod{N}.$$

Для этого необходимо выбрать такое число $e$, что

$$0 < e < N, \text{ НОД}(e, N) = 1.$$

В таком случае число $d$ можно легко вычислить, например, с помощью расширенного алгоритма Евклида из уравнения:

$$ed + Ny = 1.$$

Абонент А генерирует пару чисел $(e_a, d_a)$.

Абонент Б - пару чисел $(e_b, d_b)$.

**Шаг второй:** Абонент А хочет переслать абоненту Б секретное сообщение $M$, которому соответствует на кривой $E$ некоторая точка $P_m$.

Для этого он вычисляет значение точки $Q_1 = e_a P_m$. Отправляет значение $Q_1$ абоненту Б.

**Шаг третий:** Абонент Б вычисляет значение точки $Q_2 = e_b Q_1$. Отправляет значение $Q_2$ абоненту А.

**Шаг четвертый:** Абонент А вычисляет значение точки $Q_3 = d_a Q_2$. Отправляет значение $Q_3$ абоненту Б.

**Шаг пятый:** Абонент Б вычисляет значение точки $Q_4 = d_b Q_3$. Значение $Q_4$ равно точке $P_m$, соответствующей секретному сообщение $M$.

**Аналог системы Эль-Гамаля.**

Также является криптосистемой с открытым ключом для передачи сообщений $P_m$. Исходим из несекретных данных:

1) конечного поля $F_q$;

2) определенной над ним эллиптической кривой $E$;

3) точки-«основания» $B$ на эллиптической кривой (знать общее число $N$ точек на $E$ не нужно).

Каждый из участников 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, A посылает замаскированное $P_m$ вместе с «подсказкой» $kB$, при помощи которой можно снять «маску» $ka_BB$, если знать секретное число $a_B$. Злоумышленник, который умеет решать задачу дискретного логарифмирования на $E$, может, конечно, найти $a_B$, зная $a_BB$ и $B$.

Пятый раздел представляет собой описание реализации, на языке программирования java, аналога ключевого обмена Диффи-Хеллмана для конкретно заданной эллиптической кривой [7 — 8].

**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 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 $\left[p+1-2\sqrt{p}, p+1+2\sqrt{p}\right]$. 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.