МИНОБРНАУКИ РОССИИ

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 ВЫПУСКНОЙ КВАЛИФИФКАЦИОННОЙ РАБОТЫ

студента 4 курса 421 группы

направление 02.03.01 — Математика и компьютерные науки

механико-математического факультета

Немоляева Ильи Владиславовича

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. Криптография позволяет ограничить круг получателей ресурсов, используя алгоритмы шифрования и криптосистемы. Данный раздел формировался с давних времён, а сейчас является неотъемлемой частью сетевого общения.

Тем не менее, несмотря на изобретательность сущетсвующих протоколов, на ряду со способами защиты и сокрытия информации, развиваются методы вскрытия криптосистем.

Метод создания криптосистем на основе эллиптических кривых над конечными полями, разработанный, независимо друг от друга, Нилом Коблицем и Виктором Миллером в конце прошлого столетия, является одним из перспективных.

Большинство современных криптографических систем можно перестроить на криптосистемы на эллиптических кривых, основанные на задаче дискретного логарифмирования на эллиптической кривой. Уже используемый для конкретных конечных групп, алгоритм переписывается для использования рациональных точек эллиптической кривой.

Основное содержание работы. Пусть[1] 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 мнножество точек (x, y), $x, y \in K$, удовлетворяющих уравнению

$$y^2 = x^3 + ax + b \tag{1.1}$$

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

Замечание 1.1 Общая формула уравнения эллиптической кривой, которая применима при любом поле имеет вид $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$.

Теорема 1.1 Для любой неособой кубической кривой имеется проективная замена координат, приводящая её в форму Вейерштрасса. Если коэффициенты уравнения исходной кривой рациональны и на кривой имеется хотя бы одна рациональная точка, то существует возможность найти проективную

[1]Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц — М.: Научное издательство ТВП, 2001. — 260 с.

замену с рациональны[2] $\alpha_i, \beta_i, \gamma_i \quad (i = 1, 2, 3)$, которая сможет преобразить исходную кривую в кривую в форме Вейерштрасса с рациональными a и b.

Замечание 1.2 Если $F(x, y) = 0$ — неявное уравнение, выражающее y как функцию x в (1.1), то есть $F(x, y) = y^2 - x^3 - ax - b$, то точка (x, y) этой кривой называется неособенной или гладкой точкой, если по крайней мере, одна из частных производных $\partial F/\partial x$, $\partial F/\partial y$ в этой точке не равна нулю.

Предложение 1.1 Эллиптическая кривая, заданная уравнением (1.1), является особой тогда и только тогда, когда её дискриминант равен 0. $\triangle = 4a^3 + 27b^2$

Эллиптические кривые над $\mathbb{R}$. 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 $P + Q = O$, то есть O — тождественный элемент по сложению или «нулевой элемент» группы точек.

2. Точки $P = (x, y)$ и $-P$ имеют одинаковые x-координаты, а их y-координаты различаются только знаком, то есть $-(x, y) = (x, -y)$.

3. Если P и Q имеют различные x-координаты, то прямая $l = \overline{PQ}$ имеет с E ещё в точности одну точку пересечения R. За исключением, когда l — касательная в одной из точек. В таком случае, если l касательная в точке P, то $R = P$. Определяем теперь $P + Q$ как точку $-R$, то есть как отражение от оси x третьей точки пересечения.

4. Если $Q = -P$, то полагаем $P + Q = O$.

5. Если $P = Q$, то 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 берём P, если касательная l в P имеет «двойное касание», то есть если P — точка перегиба кивой.

В соответствии с рисунком 1.1, чтобы найти $P + Q$ на эллиптичсекой кривой $y^2 = x^3 - x$ в плоскости xy, проводим прямую $\overline{PQ}$ и в качестве $P + Q$ берём точку, симметричную относительно оси x третьей точке, определяемой пересечением $\overline{PQ}$ и кривой. Если P совпадёт с Q, то есть требуется найти

[2]Острик, В.В. Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые / В.В. Острик, М.А. Цфасман — М.: МЦНМО, 2011. — 48 с.

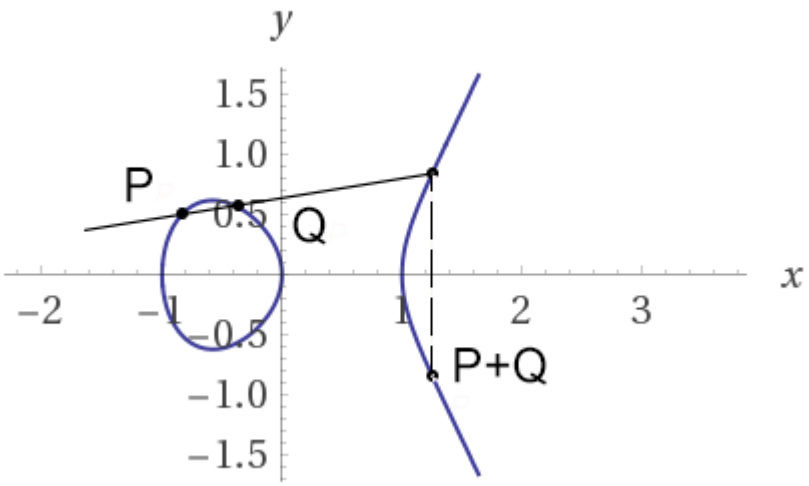

Рисунок 1.1

$2P$, тогда используется касательная в точке P. В таком случае точка $2P$ симметрична третьей точке, в которой эта касательная пересекает кривую.

В соответствии с рисунком 1.2, представлен результат работы программы для вычисления суммы точек эллиптической кривой, заданной в форме Вейерштрасса, в случае, когда эллиптическая кривая задана с коэффициентами $a = 1$ и $b = 1$.

```
E: y^2 = x^3+1.0*x+1.0
Point P = (1.0,1.7320508075688772)
Point Q = (1.5,2.4238399287081647)
P + Q = (-0.585711247493329,0.46190477299930954)

Process finished with exit code 0
```

Рисунок 1.2

Эллиптические кривые над $\mathbb{C}$. Если задана эллиптическая криая (1.1) над комплексными числами, то существует решётка L и функция комплексного переменного, называемая функцией Вейерштрассе, со следующими свойствами:

1. $\wp(z)$ аналитична всюду, кроме точек L, в каждой из которых имеет полюс второго порядка;

2. $\wp(z)$ удовлетворяет дифференциальному уравнению

$$(\wp'(z))^2 = \wp^3 + a\wp + b$$

и, следовательно, при любом $z \notin L$ точка $(\wp(z), \wp'(z))$ лежит на эллиптической кривой E;

3. два комплесных числа z_1 и z_2 дают одну и ту же точку $(\wp(z), \wp'(z))$ на E тогда и только тогда, когда $z_1 - z_2 \in L$;

4. отображение, которое люой точке $z \notin L$ ставит в соответствие точку $(\wp(z), \wp'(z))$ на E, а любой точке $z \in L$ — точку в бесконенчости O, даёт взаимно однозначное соответсвие между E и факторгруппой C/L комплексной плоскости по подгруппе L;

5. это взаимно однозначное соответствие есть изоморфизм абелевых групп, иными словами, если z_1 соответсвует точке $P \in E$, а z_2 — точке $Q \in E$, то $z_1 + z_2$ соотвествует точке $P + Q$.

Эллиптические кривые над $\mathbb{F}_q$. Обозначим[3] $\#E(\mathbb{F}_q)$ конечное число рациональных точек на эллиптической кривой E. Ожидаемое число точек кривой близко к $q + 1$ и можноположить

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

где «дефект» t называется следом отображения Фробениуса в q.

Теорема 1.2(Теорема Хассе) След отображения Фробениуса удовлетворяет неравенству $|t| \leqslant 2\sqrt{q}$.

Эндоморфизм Фробениуса φ — эндомофризм группы E над алгебраическим замыканием $\overline{\mathbb{F}_q}$.

Существует два частных случая криптографически непригодных эллиптических кривых:

а) Кривая $E(\mathbb{F}_q)$ называется аномальной, если её след Фробениуса равен 1, то есть $\#E(\mathbb{F}_q) = q$. Эта кривая особенно неудобна, когда q — простое число.

б) Кривая $E(\mathbb{F}_q)$ называется суперсингулярной, если характеристика p поля $\mathbb{F}_q$ делит след Фробениуса t. Такиз кривых также стараются избегать в криптографии. При $q = p$ суперсингулярная кривая насчитывает $p+1$ точку, поскольку $t = 0$ в этом случае. Если же $q = p^r$, то t у суперсингулярных кривых может принимать значения. При нечётном r: $t = 0$,

[3]Смарт, Н. Криптография / Н. Смарт — М.: Техносфера, 2005. — 528 с.

$t^2 = 2q$ и $t^2 = 3q$. При чётном r: $t^2 = 4q$, $t^2 = q$, если $p = 1 \pmod 3$, и $t = 0$, если $p \neq 1 \pmod 4$.

Инвариантами кривой называются такие выражения, составленные из коэффициентов её уравнения, которые не меняются при переходе от одной прямоугольной декартовой системы координат к другой такой же системе.

j-инвариантом[4] на эллиптической кривой называется значение, которое вычисляется по формуле $j = c_4^3/\triangle$ где c_4 число, зависящее от коэффициентов уравнения эллиптической кривой, а $\triangle$ дескриминант.

Порядок точки. Фиксируем положительное число N. Пусть

$$f(x) = ax^3 + bx^2 + cx + d = a(x - e_1)(x - e_2)(x - e_3)$$

— кубический полином с коэффициентами в поле K характеристики, не равной 2. Предположим, что корни этого полинома различны. Опишем координаты точек порядка N на эллиптической кривой $y^2 = f(x)$. При $N = 2$ точки порядка N — это бесконечная точка и точки $(e_i, 0)$, $i = 1, 2, 3$. Предположим, что $N > 2$. Если N нечётно, то под нетривальной точкой порядка N подразумевается точка $P \neq 0$, такая, что $NP = 0$. Если N чётно, то под нетривиальной точкой порядка N подразумевают точку $P \neq 0$, такую, что $NP = 0$, но $2P \neq 0$.

Предложение 2.1 Пусть K' — любое расширение поля K. Пусть $\sigma : K' \to \sigma K$ — любой изоморфизм полей, оставляющий точки поля K на месте. Пусть $P \in \mathbb{P}^2_{K'}$ — точка на эллиптической кривой $y^2 = f(x)$, точный порядок которой равен N. Тогда точка σP имеет точный порядок N, где для $P = (x, y, z) \in \mathbb{P}^2_{K'}$ обозначаем $\sigma P = (\sigma x, \sigma y, \sigma z) \in \mathbb{P}^2_{\sigma K'}$

Теорема 2.1(Теорема Вейля) Дзета-функция есть рациональная функция от T вида

$$Z(T; E/\mathbb{F}_q) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}, \tag{2.1}$$

где от эллиптической кривой E зависит лишь целое число a. Значение a связано с числом $N = N_1$ соотношением $N = q + 1 - a$. Кроме того, дискриминант квадратного трёхчлена в числителе отрицателен, $a^2 < 4q$, таким

[4]Кнэпп, Э. Эллиптические кривые / Э. Кнэпп — М.: Факториал Пресс, 2004. — 488 с.

образом, этот трёхчлен имеет два комплексно сопряжённых корня α и β, оба по модулю равные $\sqrt{q}$.

Замечание 2.1 Если записать числитель (2.1) в виде $(1-\alpha T)(1-\beta T)$ и затем взять производную от логарифмов обеих частей, можно убедится, что формула (2.1) эквивалентна последовательности соотношений

$$N_r = q^r + 1 - \alpha^r - \beta^r, \quad r = 1, 2, ...$$

Так как α и β, также как и a, определяются значением $N = N_1$, то число точек над $\mathbb{F}_q$ однозначно определяет число точек над любым его расширением. Таким образом, теорему Вейля можно использовать для нахождения числа точек над расширениями высокой степени.

Метод нахождения числа точек в общем случае. Дана эллиптическая кривая $E(K)$, заданная общим уравнением $y^2 + a_1xY + a_3y = x^3 + a_2x^2 + a_4x + a_5$. Пусть N — число точек эллиптической кривой $E(K)$.

1. Выберем точку $P \in E(K)$. Для этого выбираем случайную x-координату $x_0 \in K$ так, чтобы существовала y-координата $y_0 \in K$, удовлетворяющая уравнению кривой.

2. Находим целое число $k \leftarrow [\sqrt[4]{2q}]$.

3. Вычисляем точки P, $2P$, $3P$, ..., kP и отсортировываем полученную базу данных по x-координате (при этом оказываются известными и точки $-P$, $-2P$, $-3P$, ..., $-kP$).

4. Вычисляем точки $Q \leftarrow (2k+1)P$, $R \leftarrow (q+1)P$, после чего сравниваем поочерёдно x-координаты точек R, $R \pm Q$, $R \pm 2Q$,...,$R \pm kQ$ с базой данных (равенство означает, что $R + dkP = eP$ для некоторых целых d, e). Отсюда находим предполагаемое число точек: $N \leftarrow q + 1 + dk - e$

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, $f_{l_i}(x)$ — полином деления, и содержит три шага:

1. вычисление набора попарно взаимно простых чисел $\{l_i\}$ и соответсвующих полиномов деления в кольце $K[x]$;

2. нахождение вычетов числа $T = q + t - N$ по модулям малых взаимно простых чисел l_i;

3. восстановление числа точек по китайской теореме об остатках.

Криптосистеы с открытым ключом. Пусть P и C множества всех возможноых элементов открытого текста и шифртекста. И пусть функции f, f^{-1} имеют вид:

$$C \equiv P + b \pmod{\mathrm{N}}$$

$$P \equiv C - b \pmod{\mathrm{N}}$$

где P и C элементы из соответствующих множест, b сдвиг, по которому осуществляется преобразование, N основание системы счисления.

По определению, криптосистема с открытым ключом обладает свойством, что знание шфирующего преобразования не позволяет по ключу шифрования найти ключ дешифрования, избежав очень длинных вычислений. То есть $f : P \to C$ легко вычисляется, если ключ K_E известен, но вычислять значения обратной функции $f^{-1} : C \to P$ очень сложно. Иными словами, с точки зрения вычисляемости, функция f является необратимой без ключа K_D. Такая функция называется функцией с замком.

Однонаправленной[5] называется такая функция f, для которой легко определить значение функции $y = f(x)$, но практически невозможно отыскать для заданного y такое x, что $y = f(x)$.

Смысл названия «открытый ключ» состоит в том, что информация, используемая при отправке шифрованных сообщений — ключ шифрования K_E — может быть раскрыта без риска, что кто-либо получит возможность прочесть открытый текст. Пусть имеется группа пользователей криптосистемы, каждый из которых хочет иметь возможность принимать и дешифровать конфиденциальные сообщения от любого другого без участия третьих лиц.

Заметим, что система с открытым ключом позволяет двум участникам начать секретный обмен данными без предворительного контакта, без взаимной проверки и без предворительного обмена какой-либо информацией. Вся необходимая информация для посылки шифрованного сообщения является общедоступной.

[5]Шаньгин, В.Ф. Информационная безопасность / В.Ф. Шаньгин — М.: ДМК Пресс, 2014. — 702 с.

Криптосистема[6] RSA, предложенная в 1977 году Р.Ривестом, Э.Шамиром и Л.Адлеманом и названная по первым буквам фамилий авторов, широко используется для шифрования с открытым ключом и цифровой подписи.

Безопасность криптосистемы[7] RSA основана на том, что по заданным целым числам найти их произведение не составляет больших трудов, а разложить длинное целое число на простые множетили гораздо сложнее.

Каждому пользователю системы RSA соответствует пара открытый и закрытый ключ. Для выработки ключей нужно сгенерировать большие простые числа p и q, $p \neq q$, вычислить их произведение $n = pq$ и функцию Эйлера

$$\varphi(n) = (p-1)(q-1).$$

Функция Эйлера[8] $\varphi(a)$ определяется для всех a и представляет собою число чисел ряда $0, 1, ..., a-1$, взаимно простых с a.

Далее необходимо выбрать целое число e, $1 < e < \varphi(n) - 1$, взаимно простое с $\varphi(n)$, и вычислить d — мультипликативно обратное к e по модулю

$$\varphi(n) : d \equiv e^1 \pmod{\varphi(n)},$$

то есть $ed \equiv 1 \pmod{\varphi(n)}$. Числа e и d называются открытым и закрытым показателями соотвественно. Пара (n, e) является открытым ключом, число d является секретным ключом. Множетили p и q должны храниться в секрете или могут быть уничтожены после выработки ключей.

Пусть (n, e) — открытй ключ пользователя A. Чтобы передать пользователю A зашифрованнное сообщение m, $1 < m < n$, пользователь B вычисляет шифртекст $c \equiv m^e \pmod{n}$. Для расшифрования шифртекста c пользователь A возводит его в степень d: $m \equiv c^d \pmod{n}$.

Лемма 3.1 Задача разложения на множетели числа $n = pq$ и задача вычисления функции Эйлера $\varphi(n)$ полиномиально эквивалентны.

---

[6]Гатченко, Н.А. Криптографическая защита информации / Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев — СПб.: НИУ ИТМО, 2012. — 142 с.

[7]Маховенко, Е.Б. Теоретико-числовые методы в криптографии: Учебное пособие / Е.Б. Маховенко — М.: Гелиос АРВ, 2006. — 320 с.

[8]Иванов, Б.Н. Дискретная математика. Алгоритмы и программы: Учеб. пособие. / Б.Н. Иванов — М.: Лаборатория Базовых Знаний, 2001. — 288 с.

Теорема 3.1 Задача вычисления закрытого показателя d сводится с полиномиальной сложностью к задаче вычисления функции $\varphi(n)$.

В общем случае задача дешифрования системы RSA эквивалентна задаче извлечения корня степени e по модулю n.

Алгоритм разложения на множители по известным показателям RSA.

Вход. Число n, показатели e, d, где $ed \equiv 1 \pmod{\varphi(n)}$.

Выход. Такие числа p и q, что $n = pq$.

1. Представить число $N = ed - 1$ в виде $N = 2^f s$, где число s нечётное.

2. Выбрать случайное число a, $2 \leqslant a \leqslant n-2$, и вычислить $u \leftarrow a^s \pmod{n}$, $v \leftarrow u^2 \pmod{n}$.

3. Пока $v \neq 1$, полагать $u \leftarrow v, \quad v \leftarrow u^2 \pmod{n}$.

4. При $u = -1$ вернуться на шаг 2. В противном случае вычислить $p \leftarrow \text{НОД}(u-1, n), \quad q \leftarrow \text{НОД}(u+1, n)$.

5. Результат: p, q.

Пусть p — нечётное простое число. Рассмотрим мультипликативную группу кольца $\mathbb{Z}/p\mathbb{Z}$. Она циклична, то есть существуют такие числа a, что сравнение

$$a^x \equiv b \pmod{p} \tag{3.1}$$

разрешимо относительно x при любом $b \in \mathbb{Z}$, не делящемся на p. Числа a с этим свойством называются первообразными корнями, и количество их равна $\varphi(p-1)$, где φ — функция Эйлера. Целое x, удовлетворяющее сравнению (3.1), называется индексом или дискретным логарифмом числа b.

По заданному числу x достаточно быстро можно вычислить $a^x \bmod p$. Однако, выполнение обратной операции, вычисление по заданному b его дискретного логарифма является очень сложной в вычислительном отношении задачей.

Криптосистемы на эллиптических кривых. Для эллиптических кривых аналогом умножения двух элементов группы $\mathbb{F}_q^*$ служит сложение двух точек эллиптической кривой E, определённой над $\mathbb{F}_q$. Таким образом, аналог возведения в степень k элемента из $\mathbb{F}_q^*$ — это умножение точки $P \in E$ на целое число k. Возведение в k-ю степень в $\mathbb{F}_q^*$ методом повторного возведения в квадрат можно осуществить за $O(\log k \log^3 q)$ двоичных операций.

Предложение 4.1 Пусть эллиптическая кривая E определена уравнением Вейерштрасса $y^2 = x^3 + ax + b$ над конечным полем $\mathbb{F}_q$. Если задана точка P на E, то координаты kP можно вычислить за $O(\log k \log^3 q)$ двоичных операций.

Замечание 4.1 Оценки времени работы в приведённом выше предложении являются наилучшими, особенно для конечных полей характеристики $p = 2$.

Замечание 4.2 Если известно число N точек на эллиптическоей кривой E и если $k > N$, то в силу равенства $NP = 0$, можно заменить k его наименьшим неотрицательным вычетом по модулю N. В таком случае оценка заменяется на $O(\log^4 q)$.

Пусть E — эллиптическая кривая над $\mathbb{F}_q$ и B — точка на E. Задачей дискретного логарифмирования с основанием B на E называется задача нахождения для данной точи $P \in E$ такого числа $x \in \mathbb{Z}$, если оно существует, что $xB = P$.

Основные преимущества криптосистем на эллиптических кривых заключается в том, что не известны субэкспоненциальные алгоритмы вскрытия этих систем, если в них не используются суперсингулярные кривые, а также кривые, порядки которых делятся на большое простое число.

Аналог ключевого обмена Диффи-Хеллмана. Пользователи C и D для начала открыто выбирают точку $B \in E$ в качестве основания. B играет ту же роль, что и образующий g в системе Диффи-Хеллмана для конечных полей. Однако, не требуется, чтобы точка B была образующим элементом в греппе точек кривой E. Эта группа может и не быть цилической. Даже если она циклическая, нет необходимости тратить время на проверку того, что B это образующий элемент. Предположим, что B — взятая открыто точка на E весьма большого порядка, который равен либо N, либо большому делителю N, где N — число точек кривой E.

Чтобы образовать ключ, пользователь C случайным образом выбирает целое число a, сравнимое по порядку величины с q, которое близко к N. Это число пользователь C держит в секрете. Пользователь C вычисляет $aB \in E$ и передаёт эту точку открыто. Пользователь D делает то же самое: он выбирает

случайно b и открыто передаёт $bB \in E$. Тогда используемый ими серкетный ключ — это $P = abB \in E$. Оба пользователя могут вычислить этот ключ.

Аналог системы Мэсси-Омуры. Это криптосистема[9] с открытым ключом для передачи элементов сообщения m, которые по предположению представлены точками P_m открытой фиксированной эллиптической кривой E над $\mathbb{F}_q$, q берётся большим. Предполагается также, что общее число N точек на E вычислено и не скрыто. 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, то есть такое целое d, что $de \equiv 1 \pmod{N}$. Если один пользователь хочет прислать другому сообщение P_m, то он сначала посылает ему точку $e_A P_m$ (индекс A указывает на первого пользователя). Это ничего не говорит другому пользователю, который не зная ни e_A, ни d_A, не может восстановить P_m. Однако, не придавая этому значения, он умножает её на своё e_B и посылает обратно первому пользователю $e_B e_A P_m$. На третьем шаге первый пользователь должен частично раскрыть своё сообщение, умножив $e_B e_A P_m$ на d_A. Так как $NP_m = O$ и $d_A e_A \equiv 1 \pmod{N}$, при этом получается точка $e_B P_m$, которую первый пользователь возвращает второму. Тот теперь может прочитать сообщение, умножив точку $e_B P_m$ на d_B.

Аналог системы Эль-Гамаля. Это — другая система с открытым ключом для передачи сообщений P_m. Как и в системе Мэсси-Омуры, поле $\mathbb{F}_q$, определённая над ним эллиптическая кривая E, точка на данной кривой B — известны. Каждый из пользователей выбирает случайное целое число a, которое держит в секрете, затем находит и делает общедоступной точку aB.

Чтобы послать сообщение P_m, пользователь выбирает случайно целое число k и посылает пару точек $(kB, P_m + k(a_B B))$, где $a_B B$ — открытый ключ другого пользователя, которому отправляется сообщение. Чтобы прочитать сообщение, получатель умножает первую точку из пары на своё серктеное число a_B и вычитает результат умножения из второй точки: $P_m + k(a_B B) - a_B(kB) = P_m$.

[9]Онацкий, А.В. Ассиметричные методы шифрования. Модуль 2. Криптографические методы защиты информации в телекоммуникационных системах и сетях / А.В. Оницкий, Л.Г. Йона — Одесса: ОНАС им. А.С. Попова, 2010. — 148 с.

Заключение. В результате данной работы были рассмотрены особенности использования эллиптических кривых и их характеристик в создании криптосистем. Данный метод позволяет на стороне пользователя производить более быстрые операции по созданию ключей и преобразовании информации, подготовке её к передаче. При этом сохраняется надёжность системы, а отстуствие точных алгоритмов решения задачи дискретного логарифмирования на эллиптических кривых даёт перспективы использвание их в дальнейшем.

Одним из достоинств эллиптических кривых также является то, что они доставляют большое число возможных групп. Можно изменить как основное поле, так и коэффициенты уравнения кривой.

Многие используемые криптосистемы ранее в создании своих ключей могут использовать алгоритмы, базирующиеся на свойствах эллиптических кривых. Тем не менее для реализации данной задачи потребуется правильно выбрать вид кривой, так как не каждая кривая подойдёт для реализации криптосистемы.