Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет

"Высшая школа экономики»

Московский институт электроники и математики им. А.Н. Тихонова

Образовательная программа “Компьютерная безопасность”

Проект по программированию алгоритмов защиты информации

«Реализация вычисления кратной точки на кривой Эдвардса»

Выполнили работу:

Зеленецкая Дарина Николаевна СКБ192,

Добрин Даниил Андреевич СКБ191

Проверил работу:

Нестеренко А. Ю.

Вклад авторов проекта:
Зеленецкая Дарина - перевод материалов из источников, написание текста, оформление формул
Добрин Даниил - поиск источников, реализация алгоритма на языке python.

Эллиптические кривые Эдвардса в оригинальном виде

В 2007 году профессором университета Нью-Йорка Гарольдом Эдвардсом были рассмотрены свойства эллиптической кривой в форме[1]:

$$x^2 + y^2 = e^2(1 + x^2y^2) \quad (1)$$

форма является близкой к той, которая встречалась почти два века назад в работах Эйлера и Гаусса. Данный факт не сложно увидеть при $e = 1$ и замене знака “+” на “-” в правой части. Однако два века назад ученые не подозревали о том, что в будущем такое уравнение будет называться эллиптической кривой, так как данное понятие сформировалось почти век спустя после введения закона сложения точек кривой с образованием структуры абелевой группы.

Гарольду Эдвардсу впервые удалось доказать, что уравнение вида (1) описывает кривую, изоморфную кривой в форме Вейерштрасса, и получить закон сложения её точек:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2+x_2y_1}{e(1 + x_1x_2y_1y_2)}, \frac{y_1y_2+x_1x_2}{e(1 - x_1x_2y_1y_2)}\right) \quad (2)$$

Кривые в форме (2) называют оригинальной формой Эдвардса. Стоит также отметить, что нейтральным элементов здесь является точка $O = (0, e)$, а обратная точка определена как:

$$-(x_1, y_1) = (-x_1, y_1) \quad (3)$$

Из (2) несложно увидеть, что:

$$(x_1, y_1) + (0, e) = (x_1, y_1) \text{ и } (x_1, y_1) + (-x_1, y_1) = (0, e) \quad (4)$$

Кривые вида (1) существуют над всеми полями с нулевой характеристикой и над конечными полями F_p^m характеристики $p \neq 2$. Для них всегда существует точка 2-го порядка такая, что $2D_0 = O$. При совпадении слагаемых точек в (2) получаем в частном случае закон удвоения вида:

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{e(1 + x_1^2y_1^2)}, \frac{y_1^2 - x_1^2}{e(1 - x_1^2y_1^2)}\right) \quad (5)$$

Для проверки подставим в правую часть точку $O = (0, e)$, и получим решение для точки второго порядка $D_0 = (0, -e)$.

Стоит уточнить, что для задач криптографии могут вызвать больший интерес кривые вида (1) над полем F_q конечного порядка $q = p^m$. Очевидно, заменой $x \rightarrow \frac{x}{e}$ кривая (1) записывается в изоморфной форме:

$$x^2 + y^2 = 1 + e^4x^2y^2 \Rightarrow y^2 = \frac{1-x^2}{1-e^4x^2},\ e^4 \neq 1 \text{ (6)}$$

Модификация Бернстейна-Ланге

Вскоре после завершения исследований Гарольдом Эдвардсом в том же году выходит работа двух специалистов по криптографии Даниэля Бернстейна и Тани Ланге, в которой они предлагают свою модификацию эллиптической кривой (1) с введением параметра d над конечным полем F_p^m характеристики $p \neq 2.$

$$E:\ x^2 + y^2 = e^2(1 + dx^2y^2),\ d(1 - de^4) \neq 0,\ (\frac{d}{p}) =- 1 \text{ (7)}$$

Где $(\frac{d}{p})$ - символ Лежандра, параметр d - квадратичный невычет.

Универсальный закон сложения для точек эллиптической кривой с модификацией выглядит следующим образом:

$$(x_1, y_1) + (x_2, y_2) = (\frac{x_1y_2 + x_2y_1}{e(1+dx_1x_2y_1y_2)}, \frac{1_1y_2 - x_1x_2}{e(1-dx_1x_2y_1y_2)}) \text{ (8)}$$

Закон удвоения для точек эллиптической кривой с модификацией выглядит следующим образом:

$$2(x_1, y_1) = (\frac{2x_1y_1}{e(1+dx_1^2y_1^2)}, \frac{y_1^2-x_1^2}{e(1-dx_1^2y_1^2)}) \text{ (9)}$$

Принципиальными отличиями эллиптической кривой (7) от (1) являются циклическая структура группы точек (в отношении интересующих нас точек второго порядка) и, главное, отсутствие особых точек, при вычислении которых в в знаменатели появляется 0. Последнее свойство определены Бернстейном и Ланге как полнота закона сложения.

Как и для кривой (1) обратная точка определена как:

$$- (x_1, y_1) = (- x_1, y_1) \text{ (3)}$$

Нулем группы точек здесь является точка $O = (0, e)$, однако существуют лишь единственная точка второго порядка $D = (0, -e)$ и ровно две точки четвертого порядка $\pm F = (\pm e, 0)$.

Самым важным свойством является доказанная в работе Бернстейна и Ланге теорема о полноте закона сложения. Данная теорема звучит так:
“Для любых пар точек кривой знаменатели закона сложения не обращаются в ноль, что означает $dx_1x_2y_1y_2 \neq \pm 1$”. Доказательство теоремы не приведено в данной работе, однако вы можете сами ознакомиться с ней в оригинальной статье Даниэля Бернстейна и Тани Ланге [2].
В связи со свойством полноты закона сложения для кривых (7), их начали называть полные кривые Эдвардса. [3]

Реализация алгоритма вычисления кратных точек в форме Эдвардса

Так как в задание не было четкого указания какую модификацию кривых в форме Эдвардса выбирать, было принято решение выбрать полные кривые Эдвардса с модификациями Бернстейна-Ланге, так как реализация алгоритма вычисления кратных точек рассматривается в рамках программирования алгоритмов защиты информации. А как уже было сказано ранее, полнота закона сложения предоставляет возможность вычисления кратности для любых точек, в силу ограничения на параметры e и d.
Алгоритм реализован на языке python и находится в разделе приложение.

Приложение

```
e=int(0)
d=int(0)
while(e*d*(1-e*e*e*e*d)==0):
   print("Помните, что существуют ограничения на e и d:
e*d*(1-e^4*d)!=0")
   e = int(input("Введите параметр e: "))
   d = int(input("Введите параметр d: "))
   print("Параметры кривой Эдварса: "+ "e=" + str(e) + ", " + "d=" +
str(d))
x=1
y=0
print("Введите координаты точки, которую вы хотите удвоить")
x=float(input("x="))
y=float(input("y="))
print("Искомая кратная точка на кривой Эдвардса с параметрами "+"e=" +
str(e) + ", d="+ str(d) + ":")
print("P2" +"(" + str(float(2*x*y/(e+e*d*x*x*y*y))) +  "," +
str(float((y*y-x*x)/(e-e*d*x*x*y*y))) + ")")
```

Тестирование с параметрами e = 1, d = 2 для точки P(1,0)

```
e=int(0)
d=int(0)
while(e*d*(1-e*e*e*e*d)==0):
    print("Помните, что существуют ограничения на e и d: e*d*(1-e^4*d)!=0")
    e = int(input("Введите параметр e: "))
    d = int(input("Введите параметр d: "))
    print("Параметры кривой Эдварса: "+ "e=" + str(e) + ", " + "d=" + str(d))
x=1
y=0
print("Введите координаты точки, которую вы хотите удвоить")
x=float(input("x="))
y=float(input("y="))
print("Искомая кратная точка на кривой Эдвардса с параметрами "+"e=" + str(e) + ", d="+ str(d) + ":")
print("P2" +"(" + str(float(2*x*y/(e+e*d*x*x*y*y))) +  "," + str(float((y*y-x*x)/(e-e*d*x*x*y*y))) + ")")
```

```
Помните, что существуют ограничения на e и d: e*d*(1-e^4*d)!=0
Введите параметр e: 1
Введите параметр d: 2
Параметры кривой Эдварса: e=1, d=2
Введите координаты точки, которую вы хотите удвоить
x=1
y=0
Искомая кратная точка на кривой Эдвардса с параметрами e=1, d=2:
P2(0.0,-1.0)
```

Несложно проверить ручным вычислением, что алгоритм работает корректно.

Литература

[1] Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, PP. 393-422.

[2] Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advancesin Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. On the Theory and Applicationof Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. PP. 29–50.

[3] Bernstein Daniel J., Birkner Peter, Joye Marc, Lange Tanja, Peters Christiane. Twisted Edwards Curves. //IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17.