Правительство Российской Федерации

Федеральное государственное автономное образовательное   
учреждение высшего образования

Национальный исследовательский университет

«Высшая школа экономики»

Московский институт электроники и математики

Факультет прикладной математики и кибернетики

Кафедра «Компьютерная безопасность»

**КУРСОВАЯ РАБОТА**

по дисциплине «Программирование алгоритмов защиты информации»

Программная реализация алгоритма возведения в степень точки

на эллиптической кривой в форме квадрики Якоби

с использованием библиотеки gmp

**Выполнил(а):** студент группы СКБ172 Попов Ю.Л.

**Проверил:** доцент Нестеренко А. Ю.

**МОСКВА – 2020**

**Оглавление**

[Введение 2](#_Toc54972437)

[Теоретическая часть 4](#_Toc54972438)

[Работа с библиотекой gmp 7](#_Toc54972439)

[Исходные данные 8](#_Toc54972440)

[Структура программы 10](#_Toc54972441)

[Пример вывода программы 11](#_Toc54972442)

[Список использованной литературы 12](#_Toc54972443)

# Введение

Предметом изучения данной курсовой работы является программная реализация эллиптической кривой в форме квадрики Якоби.

Курсовая работа состоит из двух частей: первая – изучение эллиптической кривой и основных математических алгоритмов, вторая – написание программы на языке С с использованием библиотеки gmp. Параметры для проверки правильности работы программы были определены данными, предложенными в документе «Рекомендации по стандартизации. Задание параметров скрученных эллиптических кривых Эдвардса в соответствии с ГОСТ Р 34.10-2012».

Эллиптическая криптография – раздел криптографии, который изучает асимметричные криптосистемы, основанные на эллиптических кривых над конечными полями, где образующая точка **P** используется в качестве открытого ключа, а значение степени **k**, в которую возводится точка, используется как секретный ключ. Основное преимущество эллиптической криптографии заключается в том, что на сегодняшний день не известно существование субэкспоненциальных алгоритмов решения задачи дискретного логарифмирования 𝑘 = log𝑃𝑄.

# Теоретическая часть

Исследуемая в данной курсовой работе эллиптическая кривая имеет следующий вид:

*Y2 = eX4 – 2dX2Z2 + Z4*,

где **e** и **d** – некоторые коэффициенты, *(X : Y : Z)* – точка на данной кривой, заданная в проективных координатах, *e, d, X, Y, Z* *Zp*, **p** – простое. Все точки данной кривой принадлежат некоторой аддитивной абелевой группе, то есть все операции будут выполняться по некоторому модулю **p**.

*Нейтрального элемент* – это такая точка **O**, что выполняются следующие свойства:

1. *O + O = O;*
2. *O + (X : Y : Z) = (X : Y : Z) + O = (X : Y : Z).*

Для эллиптических кривых в форме квадрики Якоби нейтральный элемент равен *(0 : 1 : 1).*

Обратным элементом к точке *(X : Y : Z)*  является *(–X : Y : Z)*.

*Порядком точки* ***P*** называется такое минимальное число **k**, что *kP = O*.

Можно определить две операции для элементов, принадлежащих аддитивной абелевой группе: сложение двух различных точек и удвоение одной точки. Для кривых в форме квадрики Якоби удвоение является просто операцией сложения точки с самой собой, что позволяет обойтись только одной операцией.

Формулы сложения двух точек *(X1 : Y1 : Z1)* и *(X2 : Y2 : Z2)* представлены в следующем виде:

*X3 = X1Z1Y2 + Y1X2Z2*

*Y3 = (Z12Z22 + eX12X22)(Y1Y2 – 2dX1X2Z1Z2) + 2eX1X2Z1Z2(X12Z22 + Z12X22)*

*Z3 = Z12Z22 – eX12X22*.

Алгоритм сложения двух точек *(X1 : Y1 : Z1)* и *(X2 : Y2 : Z2)* представлен в следующем виде [2]:

*T1 = X1*

*T2 = Y1*

*T3 = Z1*

*T4 = X2*

*T5 = Y2*

*T6 = Z2*

*T7 = T1T3*

*T7 = T2 + T7*

*T8 = T4T6*

*T8 = T5 + T8*

*T2 = T2T5*

*T7 = T7T8*

*T7 = T7 – T2*

*T5 = T1T4*

*T1 = T1 + T3*

*T8 = T3T6*

*T4 = T4 + T6*

*T6 = T5T8*

*T7 = T7 – T6*

*T1 = T1T4*

*T1 = T1 – T5*

*T1 = T1 – T8*

*T3 = T12*

*T6 = T6 + T6*

*T3 = T3 – T6*

*T4 = eT6*

*T3 = T3T4*

*T4 = dT6*

*T2 = T2 – T4*

*T4 = T82*

*T8 = T52*

*T8 = eT52*

*T5 = T4+T8*

*T2 = T2T5*

*T2 = T2+T3*

*T5 = T4 – T8*

*(= X1Z1)*

*(= X1Z1 + Y1)*

*(= X2Z2)*

*(= X2Z2 + Y2)*

*(= Y1Y2)*

*(= X3 + Y1Y2 + X1X2Z1Z2)*

*(= X3 + X1X2Z1Z2)*

*(= X1X2)*

*(= X1 + Z1)*

*(= Z1Z2)*

*(= X2 + Z2)*

*(= X1X2Z1Z2)*

*(= X3)*

*(= X1Z2 + X2Z1 + X1X2 + Z1Z2)*

*(= X1Z2 + X2Z1 + Z1Z2)*

*(= X1Z2 + X2Z1)*

*(= X12Z22 + X22Z12 + 2X1X2Z1Z2)*

*(= 2X1X2Z1Z2)*

*(= X12Z22 + X22Z12)*

*(= 2eX1X2Z1Z2)*

*(= 2eX1X2Z1Z2(X12Z22 + X22Z12) )*

*(= 2dX1X2Z1Z2)*

*(= Y1Y2 – 2dX1X2Z1Z2)*

*(= Z12Z22)*

*(= X12X22)*

*(= eX12X22)*

*(= Z12Z22 + eX12X22)*

*(= (Z12Z22 + eX12X22)(Y1Y2 – (= 2dX1X2Z1Z2) )*

*(= Y3)*

*(= Z3)*

*X3 = T7*

*Y3 = T2*

*Z3 = T5*

Преобразование в аффинные координаты из проективных:

*x = X / Z*

*y = Y / Z2*

Если **P** – точка на кривой и *k* *Z*, то *Q = Q + Q + … + Q [k раз] = kP* – *кратная точка*.

В криптографии точка **P** является открытым ключом, а значение **k** используется как секретный ключ.

**k** называется дискретным логарифмом точки **Q** по снованию **P**. Эффективное вычисление *kP* осуществляется повторением операций удвоения и сложения точек (алгоритм «Лесенка Монтгомери»): при запуске программы можно наглядно увидеть разницу в скорости вычисления кратной точки с помощью алгоритма и цикла со сложением.

Aлгоритм «Лесенка Монтгомери»:

Пусть *Q = O, R = P, P = (X1 : Y1 : Z1)*.

Идем по каждому биту из двоичного представления числа **k**, при этом точка

*Q* → *nP = (Xn : Yn : Zn)*, а *R → (n + 1)P = (Xn+1 : Yn+1 : Zn+1)*.

На каждом шаге:

По окончании работы алгоритма *Q* – искомая точка.

# Установка библиотеки gmp на Ubuntu:

1. Скачиваем архив с официального сайта: <https://gmplib.org/#DOWNLOAD>. Например,  [gmp-6.2.0.tar.xz](https://gmplib.org/download/gmp/gmp-6.2.0.tar.xz)
2. Разархивируем папку и переходим в неё.
3. Выполняем следующие команды:

./configure

make

make check

make install

Подключение библиотеки к проекту в CMakeLists.txt:



Подключение библиотеки в программе:

#include <gmp.h>

# Исходные данные

Параметры для проверки правильности работы программы были определены данными, предложенными в документе «Рекомендации по стандартизации. Задание параметров скрученных эллиптических кривых Эдвардса в соответствии с ГОСТ Р 34.10-2012».

Для проверки был взят набор параметров id-tc26-gost-3410-2012-256-paramSetA:

* **p** – характеристика простого поля, над которым определятся эллиптическая кривая: 11579208923731619542357098500868790785326998466564056403945758400791312963931910;
* **q** – порядок подгруппы простого порядка группы точек эллиптической кривой: 2894802230932904885589274625217197696333856029809225344251215340878553035888710;
* **a** – параметр a эллиптической кривой в форме Вейерштрасса: 8778976548588580879336975129440684117161458992519345690985596216650501812715710;
* **x** – координата x точки P, являющейся порождающим элементом: 6598735018258456079030864061958683471210554512626975936540676896245329832605610;
* **y** – координата y точки P, являющейся порождающим элементом: 2285518920298496287042140250411039929315223538290810574174998740572132043529210.

На основе данных параметров с помощью программы Wolfram Mathematica также была вычислена координата x точки (θ, 0) – точки второго порядка в форме Вейерштрасса:

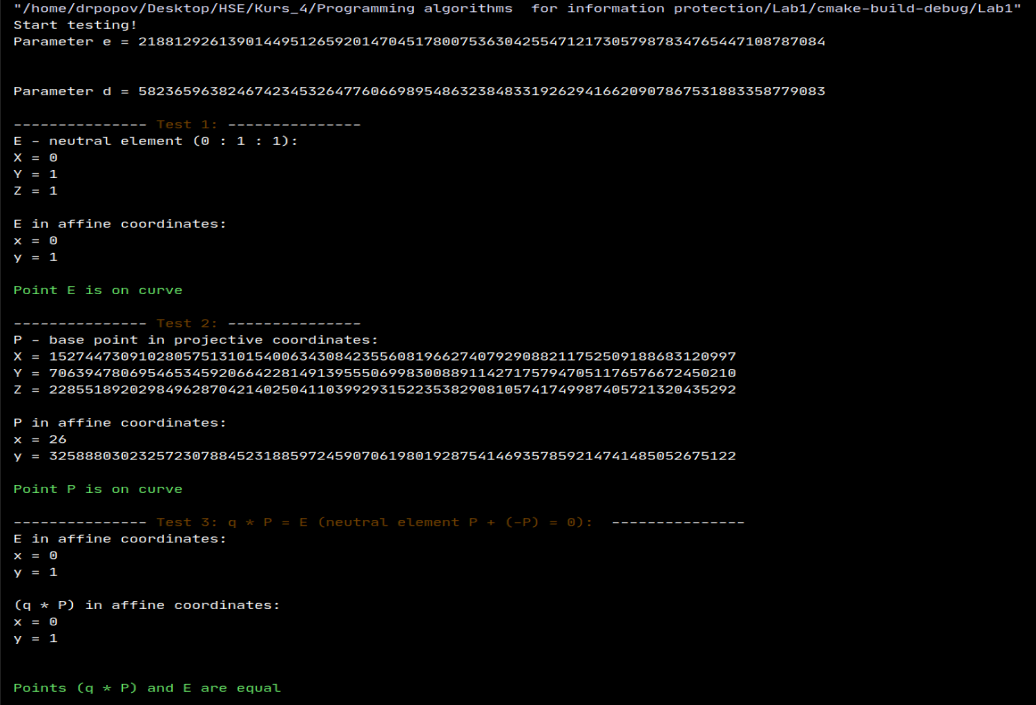
45406901841243432197237808352745960766645447974551280157210070390239194589810

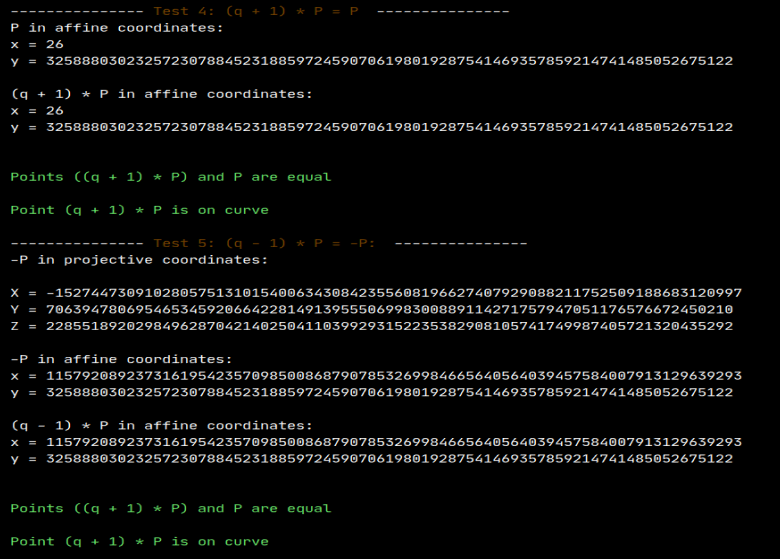
# Структура программы

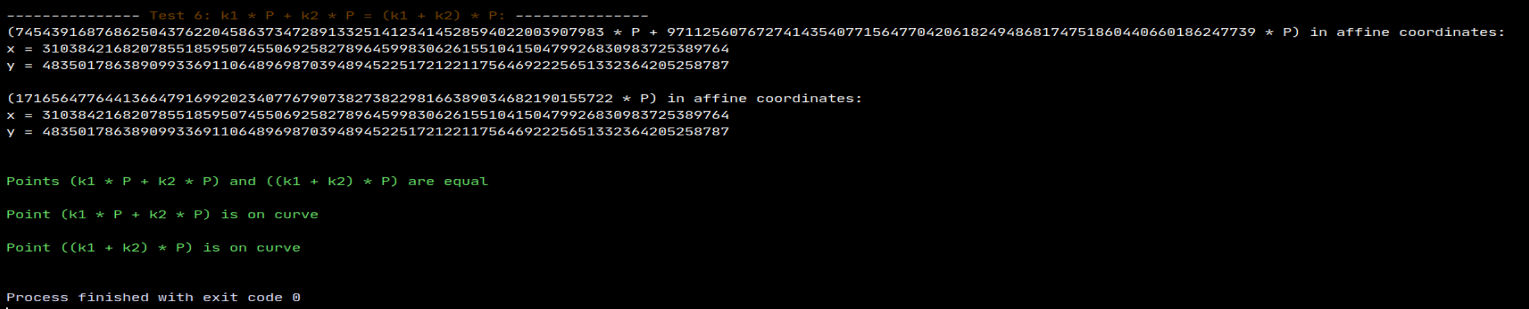
Программа состоит из четырех файлов:

1. **main.c** – содержит вычисления, тесты и вывод;
2. **parameters.h** – содержит параметры
3. **сurve.h** – содержит описания структур, описывающих точки и кривую, а также описания всех необходимых функций;
4. **сurve.c** – содержит определения функций, описанных в одноименном заголовочном файле.

# Вывод программы







# Список использованной литературы

1. Нестеренко А. Ю. – Курс лекций «Методы программной реализации СКЗИ»;
2. O. Billet, M. Joye. The Jacobi model of an elliptic curve and side-channel analysis, proceedings of AAECC-15, Lecture Notes in Computer Science;
3. «Рекомендации по стандартизации. Задание параметров скрученных эллиптических кривых Эдвардса в соответствии с ГОСТ Р 34.10-2012».