МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры и защиты информации

Аннотация к дипломной работе

АЛГОРИТМЫ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Данильчик Инна Дмитриевна

Научный руководитель:
кандидат физ.-мат. наук,
доцент Д.В. Васильев

Минск, 2015

РЕФЕРАТ

Дипломная работа содержит:

– 34 страницы;
– 2 иллюстрации (рисунка), 3 таблицы;
– 23 использованных источника.

Объект исследования: Эллиптические кривые над конечным полем.

Цель работы: Выяснить какие формы эллиптических кривых эффективнее всего использовать в алгоритмах вычисления кратной точки.

Ключевые слова: ЭЛЛИПТИЧЕСКАЯ КРИВАЯ, КРАТНАЯ ТОЧКА, КРИВАЯ ВЕЙЕРШТРАССА, КРИВАЯ МОНТГОМЕРИ, СКРУЧЕННАЯ КРИВАЯ ЭДВАРДСА, КРИВАЯ ЭДВАРДСА

В дипломной работе производится сравнительный анализ сложности операции вычисления кратных точек на эллиптических кривых, представленных в различных формах, показывается выигрыш использования скрученной кривой Эдвардса по сравнению с другими видами кривых, строится эффективный алгоритм вычисления кратных точек.

ABSTRACT

Thesis work contains:

− 34 pages;
− 2 pictures, 3 tables;
− 23 sources used.

Research object: Elliptic curves over finite fields.

Objective: To find out what forms of elliptic curves used in the most effective algorithm for calculating multiple points.

Keywords: ELLIPTIC C URVES, M ULTIPLE P OINT, WEIERSTRASS CURVES, MONTGOMERY C URVES, TWISTED EDWARDS CURVES, EDWARDS CURVES

This paper introduces comparative analysis of the complexity mathematical operations for computation multiple points on elliptic curves, which presented in various forms, shows the win of representation Twisted Edwards Curves compared to the other curve forms, constructed an efficient algorithm to calculate multiple points.