МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры и защиты информации

Юшкевич Сергей Владимирович

ВЫЧИСЛЕНИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Аннотация к дипломной работе

Научный руководитель:
кандидат физ.-мат. наук,
доцент С.В.Тихонов

Допущена к защите
«___» _____ 2023 г.
Зав. кафедрой высшей алгебры и защиты информации
доктор физ.-мат. наук, профессор В.В.Беняш-Кривец

Минск, 2023

РЕФЕРАТ

Дипломная работа содержит 33 с., 11 рис., 5 источников.

Ключевые слова: *эллиптическая кривая, обратная точка, поле, порядок точки, кратная точка, сложение точек эллиптической кривой, аффинное пространство, проективное пространство, Якобиевые координаты, криптосистемы, дзета-функция эллиптической кривой, порядок группы точек.*

Целью работы является изучение эллиптических кривых, их применении в криптосистемах, а также программная реализация сложения точек эллиптической кривой.

Первая глава посвящена теоретическим положениям.

В первом пункте даются основные определения и вывод формул сложения в аффинных координатах.

Во втором пункте рассматриваются формулы сложения в проективных координатах.

В третьем пункте приводятся формулы в Якобиевых координатах.

Вторая глава посвящена программной реализации нахождения кратной точки в различных координатах.

Третья глава посвящена анализу полученных результатов, а также сравнению скорости нахождения кратной точки в различных координатах.

Четвёртая глава посвящена вычислению порядка группы точек эллиптической кривой при помощи дзета-функции.

РЭФЕРАТ

Дыпломная праца змяшчае 33 с., 11 мал., 5 крыніцы.

Ключавыя словы: *эліптыная крывая, зваротная кропка, поле, парадак кропкі, кратная кропка, складанне кропак эліптычнай крывой, аффінная прастора, праектыўная прастора, Якобіевыя каардынаты, крыптасістэмы, дзэта-функцыя эліптычнай крывой, парадак групы кропак*.

Мэтай работы з’яўляецца вывучэнне эліптычных крывых, іх прымяненне ў крыптасістэмах, а таксама праграмная рэалізацыя складання кропак эліптычнай крывой.

Першы раздел прысвечаны тэарэтычным палажэнням.

У першым пункце даюцца асноўныя вызначэнні і вывядзенне формул складання ў аффінных каардынатах.

У другім пункце разглядаюцца формулы складання ў праектыўных каардынатах.

У трэцім пункце прыводзяцца формулы ў Якобіевых каардынатах.

Другі раздзел прысвечаны праграмнай рэалізацыі знаходжання кратнай кропкі ў розных каардынатах.

Трэці раздзел прысвечаны аналізу атрыманых вынікаў, а таксама параўнанні хуткасці знаходжання кратнай кропкі ў розных каардынатах.

Чацверты раздзел прысвечаны вылічэнню парадку групы кропак эліптычнай крывой пры дапамозе дзэта-функцыі.

ABSTRACT

The diploma work contains 33 pages, 11 figures, 5 sources.

Keywords*: elliptic curve, inverse point, field, order of a point, multiple point, addition of points of an elliptic curve, affine space, projective space, Jacobian coordinates, cryptosystems, elliptic curve zeta-function, point group order.*

The purpose of the work is to study elliptic curves, their application in cryptosystems, as well as the software implementation of the addition of elliptic curve points.

The first chapter is devoted to theoretical provisions.

In the first paragraph, the basic definitions and derivation of addition formulas in affine coordinates are given.

In the second paragraph, addition formulas in projective coordinates are considered.

The third paragraph contains formulas in Jacobian coordinates.

The second chapter is devoted to the software implementation of finding a multiple point in different coordinates.

The third chapter is devoted to the analysis of the results obtained, as well as the comparison of the speed of finding a multiple point in different coordinates.

The fourth chapter is devoted to calculating the order of a group of points of an elliptic curve using the zeta function.