МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры и защиты информации

Аннотация к дипломной работе

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ НАД КОНЕЧНЫМИ ПОЛЯМИ И ИХ ПРИМЕНЕНИЕ

Косач Максим Андреевич

Научный руководитель:
доктор физ.-мат. наук,
профессор В.В. Беняш-Кривец

2024

В дипломной работе 34 страницы, 2 иллюстрации (рисунка), 1 таблица, 7 источников.

КОНЕЧНЫЕ ПОЛЯ, ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ, КРИПТОГРАФИЯ, ШИФРОВАНИЕ, ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ, ПРОТОКОЛ ДИФФИ–ХЕЛЛМАНА

Объектом исследования в данной дипломной работе являются эллиптические кривые над конечными полями и их применение в различных областях, преимущественно в криптографии. Цель работы состоит в изучении математической теории эллиптических кривых, анализе их свойств и потенциальных применений в криптографии.

Полученные результаты включают:

1. теоретический анализ и систематизацию существующих знаний об эллиптических кривых над конечными полями,

2. оценку эффективности и безопасности криптографических алгоритмов, основанных на эллиптических кривых, с теоретической точки зрения.

Дипломная работа носит теоретический характер. Её результаты могут быть использованы в дальнейших исследованиях, а также частично включены в специальные курсы по криптографии.

Подтверждение достоверности материалов обеспечивается через математическое обоснование и анализ полученных результатов.

Работа выполнена самостоятельно, с привлечением актуальных исследований и достижений в области математики и криптографии.

У дыпломнай працы 34 старонкі, 2 ілюстрацыі (малюнка), 1 табліца, 7 крыніц.

КАНЧАТКОВЫЯ ПАЛІ, ЭЛІПТЫЧНЫЯ КРЫВЫЯ, КРЫПТАГРАФІЯ, ШЫФРАВАННЕ, ЭЛЕКТРОННЫ ЛІЧБАВЫ ПОДПІС, ПРАТАКОЛ ДЫФІ–ХЕЛМАНА.

Аб'ектам даследавання ў дадзенай дыпломнай працы з'яўляюцца эліптычныя крывыя над канчатковымі палямі і іх ужыванне ў розных галінах, пераважна ў крыптаграфіі. Мэта працы складаецца ў вывучэнні матэматычнай тэорыі эліптычных крывых, аналізе іх уласцівасцяў і патэнцыйных ужыванняў у крыптаграфіі.

Атрыманыя вынікі ўключаюць:

1. тэарэтычны аналіз і сістэматызацыю існуючых ведаў аб эліптычных крывых над канчатковымі палямі,

2. ацэнку эфектыўнасці і бяспекі крыптаграфічных алгарытмаў, заснаваных на эліптычных крывых, з тэарэтычнага пункту гледжання.

Дыпломная праца носіць тэарэтычны характар. Яе вынікі могуць быць выкарыстаны ў далейшых даследаваннях, а таксама часткова ўключаны ў спецыяльныя курсы па крыптаграфіі.

Пацвярджэнне дакладнасці матэрыялаў забяспечваецца праз матэматычнае абгрунтаванне і аналіз атрыманых вынікаў.

Праца выканана самастойна, з прыцягненнем актуальных даследаванняў і дасягненняў у галіне матэматыкі і крыптаграфіі.

Thesis project is presented in the form of an explanatory note of 34 pages, 2 figures, 1 table, 7 references.

FINITE FIELDS, ELLIPTIC CURVES, CRYPTOGRAPHY, ENCRYPTION, ELECTRONIC DIGITAL SIGNATURE, DIFFIE–HELLMAN PROTOCOL

The object of research in this diploma work is elliptic curves over finite fields and their application in various fields, mainly in cryptography. The purpose of the work is to study the mathematical theory of elliptic curves, analyze their properties and potential applications in cryptography.

Findings include:

1. theoretical analysis and systematization of existing knowledge about elliptic curves over finite fields,

2. assessment of the efficiency and security of cryptographic algorithms based on elliptic curves from a theoretical point of view.

The diploma work is theoretical in nature. Its results can be used in further research, and also partially included in special courses on cryptography.

Confirmation of the reliability of materials is provided through mathematical justification and analysis of the results obtained.

The work was carried out independently, with the involvement of current research and achievements in the field of mathematics and cryptography.