БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к магистерской диссертации

Алгоритмы защиты информации на эллиптических кривых

ГОРБУНОВА Елена Владимировна

Научный руководитель:
доктор технических наук,
профессор В.А. Липницкий

Минск, 2015

Магистерская диссертация представлена в виде пояснительной записки объемом 55 страниц, 3 таблицы, 14 источников, 7 приложений объемом 16 листов.

КОНЕЧНЫЕ ПОЛЯ, ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ, ПРОТОКОЛ ДИФФИ-ХЕЛЛМАНА, КРИПТОСИСТЕМА ЭЛЬ-ГАМАЛЯ

Во введении рассматриваются современные системы защиты информации и их недостатки. Также предлагается решение упомянутых проблем в освоении новых криптографических систем на основе эллиптических кривых.

В главе 1 «Поля Галуа» рассмотрены основные определения и теоремы, связанные с теорией эллиптических кривых над конечными полями. Также реализован алгоритм построения всех элементов конечного поля определенного вида.

В главе 2 «Эллиптические кривые» рассмотрены основные определения и теоремы, связанные с теорией эллиптических кривых. Также, выделены три класса неизоморфных суперсингулярных эллиптических кривых и представлены их стандартные представители. Реализован алгоритм построения всех точек суперсингулярных эллиптических кривых над конечными полями определенного вида.

В главе 3 «Системы шифрования-дешифрования на эллиптических кривых» рассмотрены основные достоинства криптосистем на эллиптических кривы. Также на основе эллиптических кривых реализованы протокол распределения ключей Диффи-Хеллмана и криптосистема Эль-Гамаля. Предоставлен алгоритм шифрования текста точками эллиптических кривых.

The Master's Thesis is presented in the form of an explanatory note of 55 pages, 14 tables, 14 references, 7 applications volume of 16 sheets.

FINITE FIELDS, ELLIPTIC CURVES, DIFFI-HELLMAN KEY EXCHANGE, ELGAMAL ENCRYPTION

The introduction deals with modern information security systems and their shortcomings. It is also proposed to solve the above problems in the development of new cryptographic systems based on elliptic curves.

In chapter 1 "Galois field" the basic definitions and theorems relating to the theory of elliptic curves over finite fields are shown. Also, the algorithm for constructing all the elements of a finite field is presented.

In chapter 2 "Elliptic curves" the basic definitions and theorems relating to the theory of elliptic curves are shown. Also, the three classes of isomorphic supersingular elliptic curves are presented and their standard representatives are proposed. The algorithm for constructing all points supersingular elliptic curves over finite fields of a certain type is realized.

Chapter 3, "System encryption-decryption on elliptic curves" are considered the main advantages of elliptic curve cryptosystems. Also based on elliptic curves implemented protocol key distribution Diffie-Hellman, and El Gamal cryptosystem. The encryption algorithm of the text by elliptic points is realized.