МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

КАРПОВИЧ

Станислав Владимирович

КРИПТОСИСТЕМА XTR

Дипломная работа

Научный руководитель:
старший преподаватель,
А. В. Кушнеров

Допущен к защите

«___» _____ 2020 г.

Зав. кафедрой дифференциальных уравнений и системного анализа

доктор физ.-мат. наук, профессор В. И. Громак

Минск, 2020

В дипломной работе 39 страниц, 2 рисунка 1 таблица, 10 источников, одно приложение.

XTR-КРИПТОГРАФИЯ, ПОЛЯ ГАЛУА, КОНЕЧНЫЕ ПОЛЯ, КРИПТОСИСТЕМА ЭЛЬ-ГАМАЛЯ, СЛЕДЫ В КОНЕЧНОМ ПОЛЕ, РАСШИРЕНИЯ КОНЕЧНОГО ПОЛЯ, БАШНЯ РАСШИРЕНИЙ ПОЛЕЙ, WOLFRAM MATHEMATICA

Рассматриваются и изучаются конечные поля, расширения конечных полей и следы в конечных полях, XTR-криптография.

Были реализованы учебные криптосистемы Эль-Гамаля и XTR вариант XTR криптосистемы Эль-Гамаля. Проведено сравнение XTR варианта криптосистемы Эль-Гамаля с криптосистемами RSA и традиционной криптосистемой Эль-Гамаля.

В рамках работы были выявлены следующие преимущества XTR криптосистемы:

- Быстрая генерация параметров криптосистемы
- Небольшой размер ключей для получения той же криптостойкости
- Скорость шифрования и дешифрования

Дипломная работа выполнена автором самостоятельно.

The research has 39 pages, 2 pictures, 1 table, 10 references, one application.

XTR-CRYPTOGRAPHY, GALOIS FIELDS, FINAL FIELDS, EL GAMAL CRYPTOSYSTEM, FINAL FIELD TRACKS, FINAL FIELD EXTENSIONS, TOWER OF FIELD EXTENSIONS, WOLFRAM MATHEMATICA

Finite fields, extensions of finite fields and traces in finite fields, XTR-cryptography are examined and studied.

El-Gamal training cryptosystems and XTR version of the El-Gamal cryptosystem were implemented. An XTR comparison of the El Gamal cryptosystem with RSA cryptosystems and the traditional El Gamal cryptosystem is compared.

Where identified following advantages of the XTR cryptosystem:

- Fast generation of cryptosystem parameters
- Small key size for the same cryptographic strength
- Speed of Encryption and Decryption

The research was done solely by the author.