МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра алгебры и защиты информации

СТАСКЕВИЧ
Алексей Анатольевич

ИДЕНТИФИКАЦИОННЫЕ КРИПТОСИСТЕМЫ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Дипломная работа

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

Допущена к защите

«___» _____ 2019 г.

Зав. кафедрой алгебры и защиты информации
доктор физико-математических наук, профессор В.В. Беняш-Кривец

Минск, 2019

Стаскевич А. А. Идентификационные криптосистемы на эллиптических кривых (дипломная работа). - Минск: БГУ, 2019. – 23 с.

Дипломная работа содержит

- 23 страницы
- 1 приложение
- 4 использованных источника

Ключевые слова: ЭЛЛИПТИЧЕСКАЯ КРИВАЯ, ФУНКЦИЯ ВЕЙЕРШТРАССА, СХЕМА БОНЕ-ФРАНКЛИНА, СПАРИВАНИЕ ВЕЙЛЯ, ПРОЕКТИВНАЯ ПЛОСКОСТЬ, КОНЕЧНОЕ ПОЛЕ, ДИВИЗОР

В дипломной работе изучаются эллиптические кривые и их свойства, их отображение на комплексную плоскость. Рассматривается реализация идентификационной системы Боне-Франклина.

Целью работы является изучение идентификационных криптосистем на эллиптических кривых.

Для достижения данной цели использовались:

- теория конечных полей,
- спаривание Вейля,
- дивизоры,
- язык программирования Python.

В дипломной работе получены следующие результаты:

1. изучена теоретическая база по билинейным спариваниям на эллиптических кривых,
2. рассмотрена схема Боне-Франклина и ее реализация,
3. реализованы некоторые методы для работы с эллиптическими кривыми

Новизна результатов заключается в разработке компьютерной модели методов для языка программирования Python.

Дипломная работа носит теоретический (практический) характер. Ее результаты могут быть использованы в дальнейших исследованиях белорусской школы криптографии.

Все результаты дипломной работы строго доказаны в соответствии с принятыми в математике правилами. Обоснованность и достоверность полученных результатов обусловлена строгими математическими доказательствами сформулированных в работе лемм и теорем и согласованностью с результатами.

Дипломная работа выполнена автором самостоятельно.

Staskevich A.A. Identity-based cryptosystems on elliptic curves (diplom paper). - Minsk: BSU, 2019. - 23 p.

- Diplom paper contains
  - 23 pages
  - 1 application
  - 4 used sources

Key words: ELLIPTIC CURVE, WEIRSTRASS FUNCTION, BONE-FRANKLIN SCHEME, WEIL PAIRING, PROJECTIVE PLANE, FINITE FIELD, DIVISOR

In the thesis work are studied elliptic curves and their properties, their mapping to the complex plane. The implementation of the Boneh-Franklin identity-based scheme is considered.

The aim of the work is to study identity-based cryptosystems on elliptic curves.

To achieve this goal were used:
- theory of finite fields,
- Weil pairing,
- divisors,
- Python programming language.

In the thesis work obtained the following results:
1. studied the theoretical basis for bilinear pairings on elliptic curves,
2. considered the Boneh-Franklin scheme and its implementation,
3. implemented some methods for working with elliptic curves

The novelty of the results lies in the development of a computer model of methods for the Python programming language.

Thesis is theoretical (practical) character. Its results can be used in further research of the Belarusian school of cryptography.

All the results of the thesis are rigorously proved in accordance with the rules adopted in mathematics. The validity and reliability of the results obtained is due to rigorous mathematical proofs of the lemmas and theorems formulated in the paper and consistency with the results.

Thesis was done by the author himself.

Стаскевич А. А. Ідэнтыфікацыйныя крыптасістэмы на эліптычных крывых (дыпломная праца). - Мінск: БДУ, 2019. - 23 с.

Дыпломная праца ўтрымлівае

- 23 старонкі
- 1 прыкладанне
- 4 выкарыстаных крыніцы

Ключавыя словы: ЭЛІПТЫЧНАЯ КРЫВАЯ, ФУНКЦЫЯ ВЕЙЕРШТРАСА, СХЕМА БАНЕ-ФРАНКЛІНА, СПАРВАННЕ ВЕЙЛЯ, ПРАЕКТЫЎНАЯ ПЛОСКАСЦЬ, КАНЕЧНАЕ ПОЛЕ, ДІВІЗОР

У дыпломнай працы вывучаюцца эліптычныя крывыя і іх ўласцівасці, іх адлюстраванне на камплексную плоскасць. Разглядаецца рэалізацыя ідэнтыфікацыйнай сістэмы Боне-Франкліна.

Мэтай працы з'яўляецца вывучэнне ідэнтыфікацыйных крыптасістэм на эліптычных крывых.

Для дасягнення дадзенай мэты выкарыстоўваліся:

- тэорыя канчатковых палёў,
- спарванне Вейля,
- дівізоры,
- мова праграмавання Python

У дыпломнай працы атрыманы наступныя вынікі:

1. вывучана тэарэтычная база па білінейны спарвання на эліптычных крывых,
2. разгледжана схема Боне-Франкліна і яе рэалізацыя,
3. рэалізаваны некаторыя метады для працы з эліптычнымі крывымі

Навізна вынікаў заключаецца ў распрацоўцы камп’ютарнай мадэлі метадаў для мовы праграмавання Python.

Дыпломная праца носіць тэарэтычны (практычны) характар. Яе вынікі могуць быць выкарыстаны ў далейшых даследаваннях беларускай школы крыптаграфіі.

Усе вынікі дыпломнай працы строга даказаныя ў адпаведнасці з прынятымі ў матэматыцы правіламі. Абгрунтаванасць і дакладнасць атрыманых вынікаў абумоўлена строгімі матэматычнымі доказамі сфармуляваных у працы лемм і тэарэм і узгодненасцю з вынікамі.

Дыпломная праца выканана аўтарам самастойна.