**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ**

**Кафедра математической кибернетики**

САХНЕНКО Дмитрий Игоревич

**РЕАЛИЗАЦИЯ УМНОЖЕНИЯ ПО МЕТОДУ МОНТГОМЕРИ НА ОСНОВАНИИ МОДУЛЯРНОЙ АРИФМЕТИКИ**

Дипломная работа

Научный руководитель: кандидат технических наук, доцент Д. А. Городецкий

Допущен к защите «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2019 г. Зав. кафедрой математической кибернетики доктор физико-математических наук, профессор А. Л. Гладков

Минск, 2019

# РЕФЕРАТ

Дипломная работа содержит:

* 48 страниц,
* 17 иллюстраций (скриншотов),
* 3 таблицы,
* 3 приложения,
* 6 использованных источников.

Ключевые слова: МОДУЛЯРНАЯ АРИФМЕТИКА, СИСТЕМА ОСТАТОЧНЫХ КЛАССОВ, МОДУЛЯРНОЕ УМНОЖЕНИЕ, АЛГОРИТМ МОНТГОМЕРИ, УМНОЖЕНИЕ МОНТГОМЕРИ.

В дипломной работе рассматриваются вопросы проектирования устройств для модулярного умножения на основе алгоритма Монтгомери.

Целью дипломной работы является разработка генератора аппаратного алгоритма умножения по методу Монтгомери на основании использования модулярной арифметики на языке Verilog и проведение сравнительного анализа полученного алгоритма со стандартным модулярным умножением.

В дипломной работе получены следующие результаты:

1. Разработана программа, генерирующая Verilog-описание умножения двух операндов с задаваемым значением модуля.
2. Проведен сравнительный анализ разработанной программы со стандартным модулярным умножением.

# ABSTRACT OF THE THESIS

Thesis contains:

* 48 pages,
* 17 illustrations,
* 3 tables,
* 3 appendices,
* 6 used sources.

Tags: MODULAR ARITHMETICS, RESIDUE NUMBER SYSTEM, MODULAR MULTIPLICATION, MONTGOMERI ALGORITHM, MONTGOMERI MULTIPLICATION.

The thesis deals with the design of devices for modular multiplication based on the Montgomery algorithm.

The aim of the thesis is to develop a generator of a hardware multiplication algorithm according to the Montgomery method based on the use of modular arithmetic in the Verilog language and to conduct a comparative analysis of the obtained algorithm with standard modular multiplication.

In the thesis work obtained the following results:

1. A program has been developed that generates a Verilog-description of multiplying two operands with a given module value.
2. A comparative analysis of the developed program with standard modular multiplication was carried out.

# РЭФЕРАТ

Дыпломная работа змяшчае:

* 48 старонак,
* 17 iлюстрацый,
* 3 таблiцы,
* 3 дадатку,
* 6 выкарыстаных крынiц.

Ключавыя словы: МАДУЛЯРНАЯ АРЫФМЕТЫКА, СIСТЭМА РЭШТКАВЫХ КЛАССАЎ, МАДУЛЯРНАЕ МНОЖАННЕ, АЛГАРЫТМ МАНТГОМЕРЫ, МНОЖАННЕ МАНТГОМЕРЫ.

У дыпломнай працы разглядаюцца пытанні праектавання прылад для мадулярнага множання на аснове алгарытму Мантгомеры.

Мэтай дыпломнай працы з'яўляецца распрацоўка генератара апаратнага алгарытму множання па метадзе Мантгомеры на падставе выкарыстання мадулярнай арыфметыкі на мове Verilog і правядзенне параўнальнага аналізу атрыманага алгарытму са стандартным мадулярным памнажэннем.

У дыпломнай працы атрыманы наступныя вынікі:

1. Распрацавана праграма, якая генеруе Verilog-апісанне множання двух аперанд з задаваямым значэннем модуля.
2. Праведзены параўнальны аналіз распрацаванай праграмы са стандартным мадулярным памнажэннем.