

---

# Мелкозернистая параллельная реализация алгоритма Монтгомери

---

Руководитель: доктор физико-  
математических наук, профессор  
Соболевский П.И.

---

# Существующие направления в вычислительной математике

- Последовательные вычисления и алгоритмы
  - Параллельные вычисления и алгоритмы
-

---

# Алгоритм Монтгомери

- 1985 г.
- RSA 1977 г.

---

# Реализация алгоритма Монтгомери на FPGA.

Включает в себя следующие этапы:

---

---

# Оптимизация алгоритмов:

- Модулярное возведение в степень больших чисел
- Алгоритм умножения по методу Монтгомери



---

# Построение графовых моделей:

- Построение графовой модели для модулярного возведение в степень больших чисел
  - Построение графовой модели для алгоритма умножения по методу Монтгомери
-

- 
- Построение линейного систолического массива для модулярного возведения в степень
  - Логика реализации алгоритма возведения в степень по методу Монтгомери на FPGA
-

---

Особая важность результата -  
применение его  
при реализации криптографических  
алгоритмов

---



---

# Основные положения, выносимые на защиту:

- Изучение материала в предметной области



---

## Основные положения, выносимые на защиту:

- Проведение исследований в области больших чисел. Анализ уже существующих и уже реализовывающихся алгоритмов
-

---

## Основные положения, выносимые на защиту:

- Реализовать полученный алгоритм возведения в степень по методу Монтгомери на FPGA
-

---

## Основные положения, выносимые на защиту:

- Достижения минимального времени при реализации алгоритма Монтгомери
  - Достижение минимального использования ресурсов локальной памяти
-

---

## Диссертация должна содержать следующие структурные части

- титульный лист;
  - оглавление;
  - перечень условных обозначений (при необходимости);
  - введение;
  - общую характеристику работы;
-

---

## Диссертация должна содержать следующие структурные части

- основную часть, разбитую на главы, в которой приводят анализ научной литературы, описание использованных методов, оборудования и материалов, а также сущность и основные результаты исследования;
  - заключение;
  - библиографический список;
  - приложения (при необходимости).
-

---

Спасибо за внимание

---