Южно-Уральский государственный университет
Кафедра системного программирования

Выпускная квалификационная работа
на соискание академической степени
бакалавра информационных технологий
по направлению 010400.62 “Информационные технологии”

Адаптация алгоритма блочного симметричного шифрования AES для вычислительных систем на базе процессоров Cell

К.С. Пан

Рецензент:
кандидат техн. наук
П.Л. Цытович

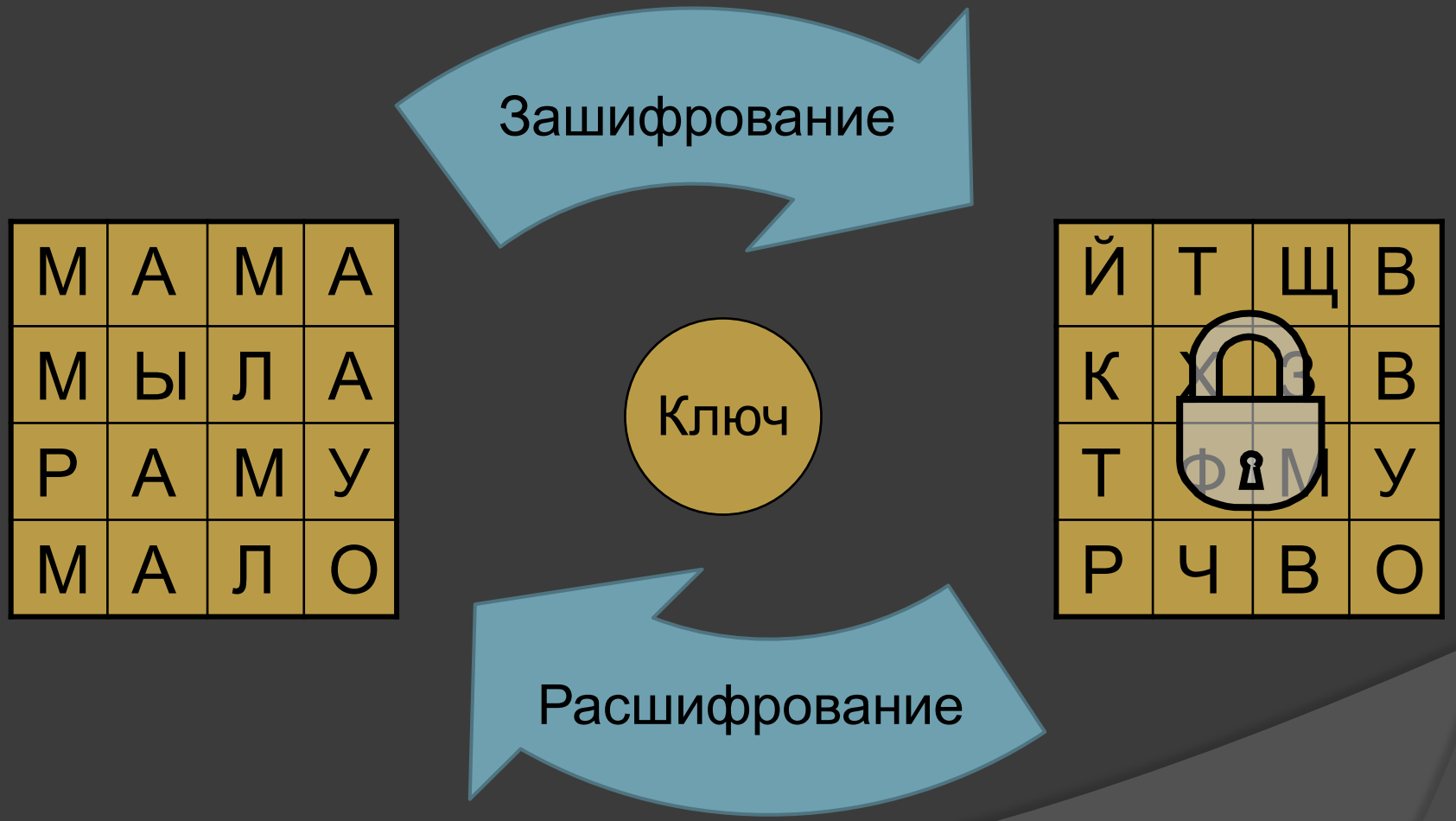
Научный руководитель:
кандидат физ.-мат. наук, доцент
М.Л. Цымблер

Челябинск-2009

Цель и задачи исследования

- Цель: разработка параллельной версии алгоритма шифрования по стандарту AES на процессорах Cell
- Задачи
  - Изучение архитектуры Cell и последовательного алгоритма AES
  - Разработка параллельного алгоритма, адаптированного для процессоров Cell
  - Проведение экспериментов по исследованию эффективности разработанного алгоритма

Advanced Encryption Standard (AES)



Шифрование данных произвольной длины

ДАННЫЕПРОИЗВОЛЬНОЙДЛИНЫРАЗБИВАЮТСЯНАБЛОКИ

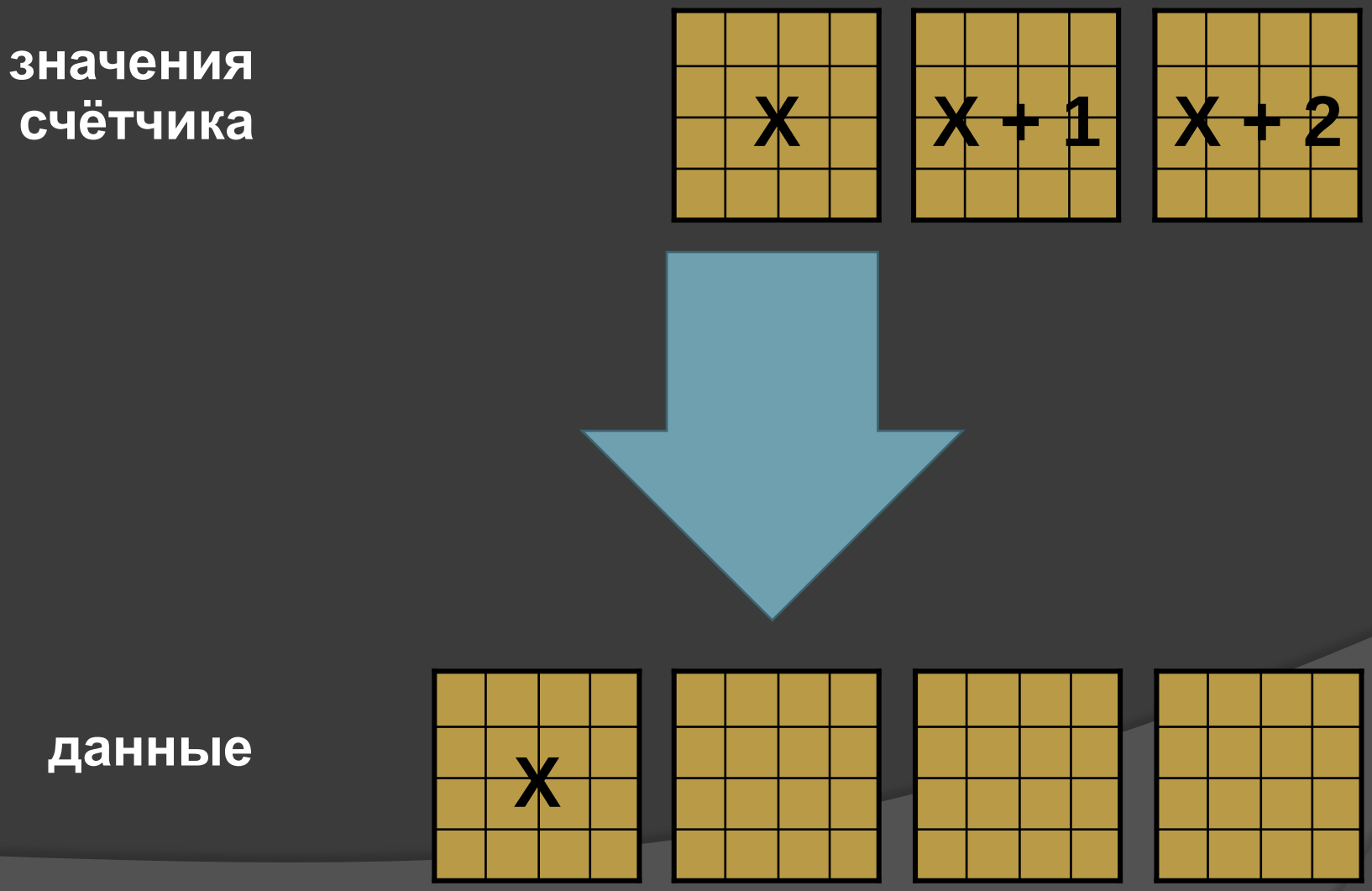
ДАННЫЕПРОИЗВОЛЬН	ОЙДЛИНЫРАЗБИВАЮТ	СЯНАБЛОКИ

Д	А	Н	Н
Ы	Е	П	Р
О	И	З	В
О	Л	Ь	Н

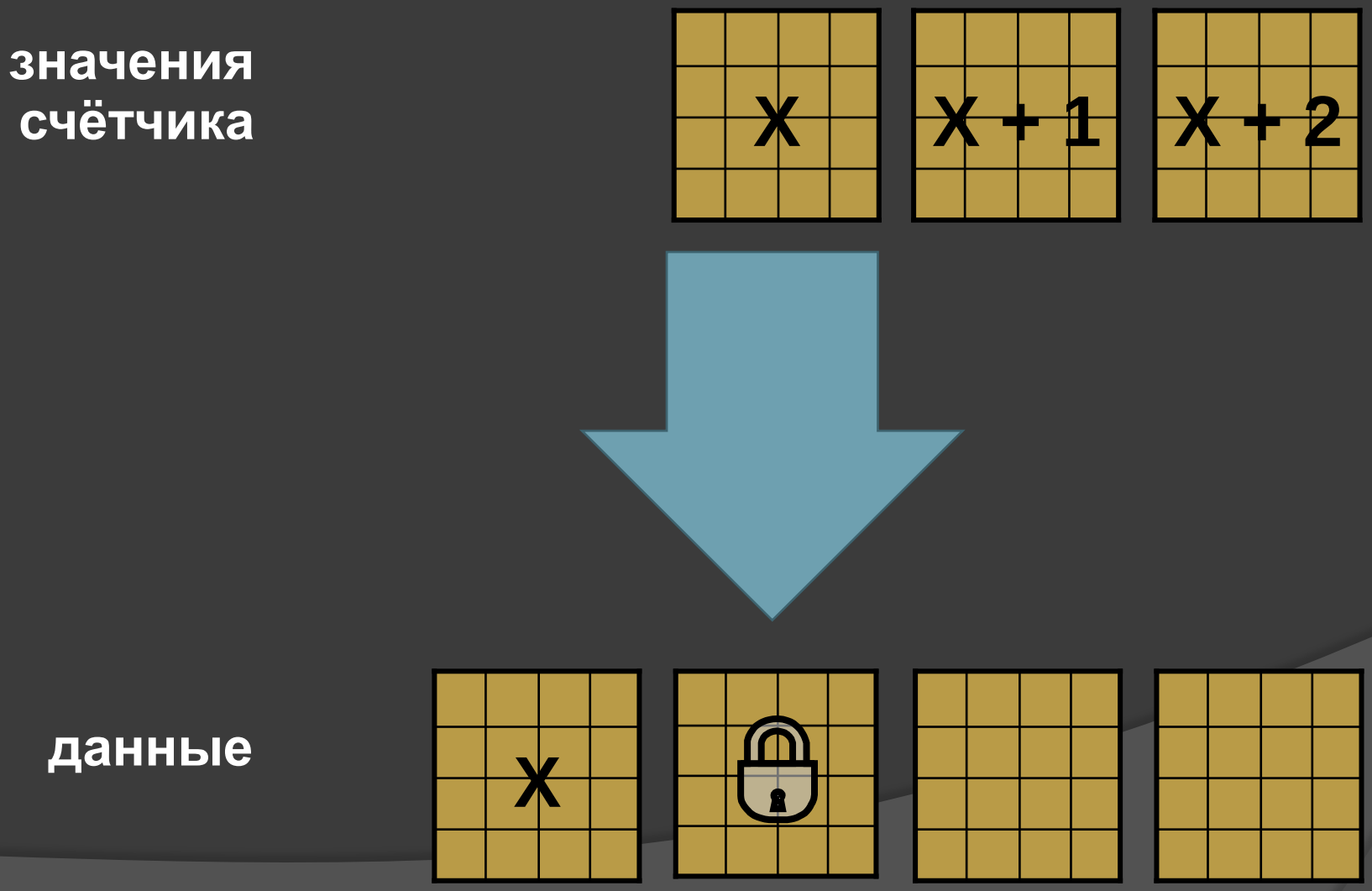
О	Й	Д	Л
И	Н	Ы	Р
А	З	Б	И
В	А	Ю	Т

С	Я	Н	А
Б	Л	О	К
И			

Шифрование в режиме счётчика

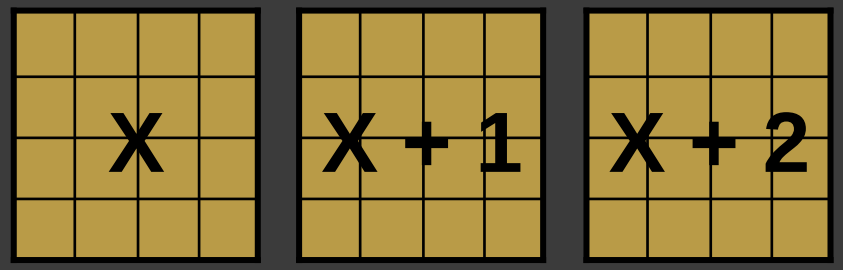


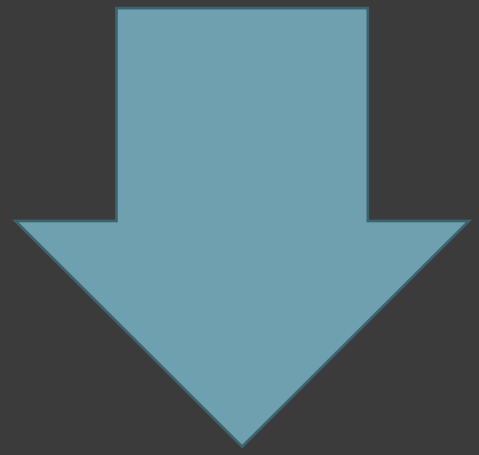
Шифрование в режиме счётчика



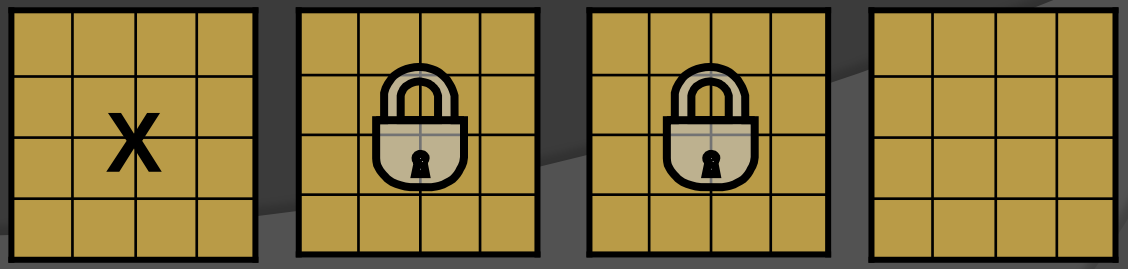
Шифрование в режиме счётчика

значения счётчика



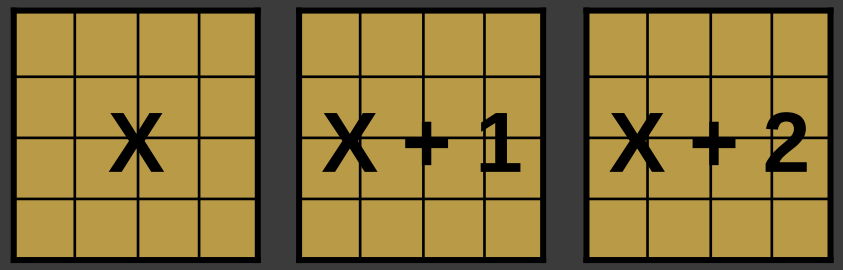


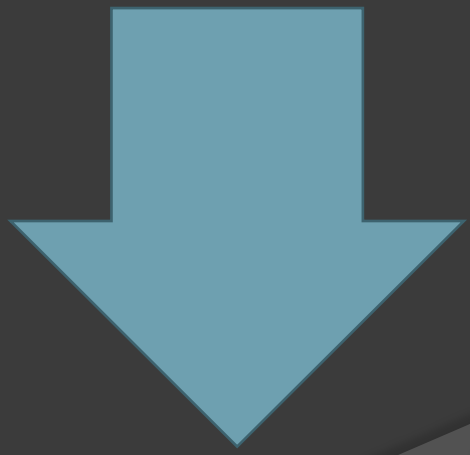
данные



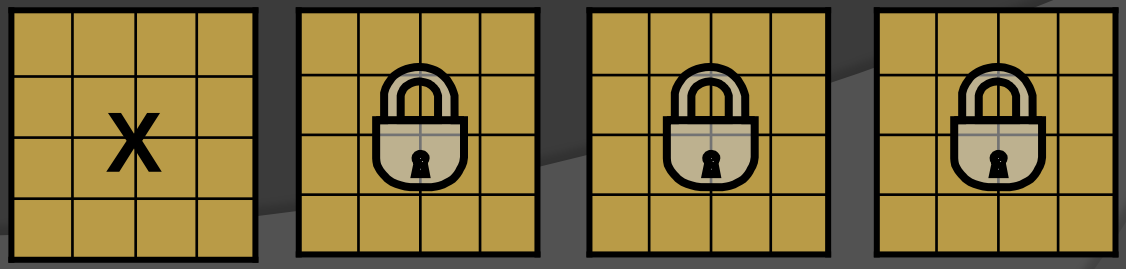
Шифрование в режиме счётчика

значения счётчика



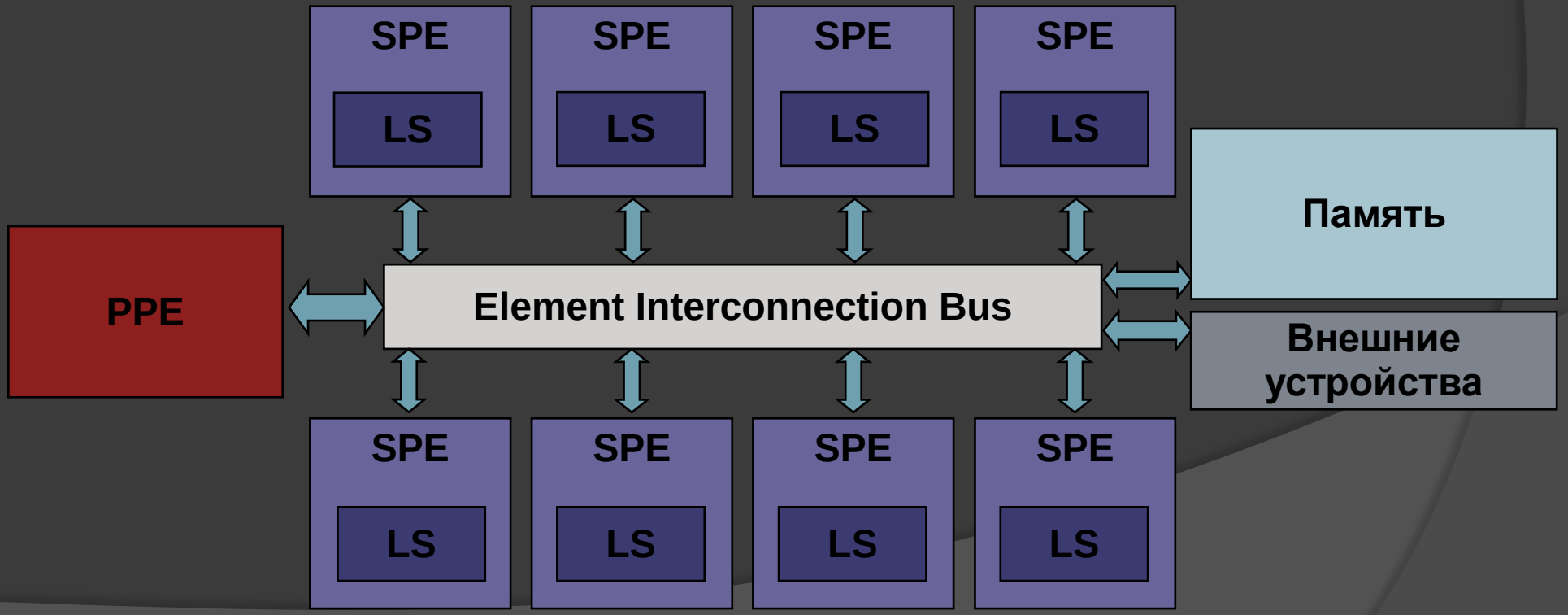


данные

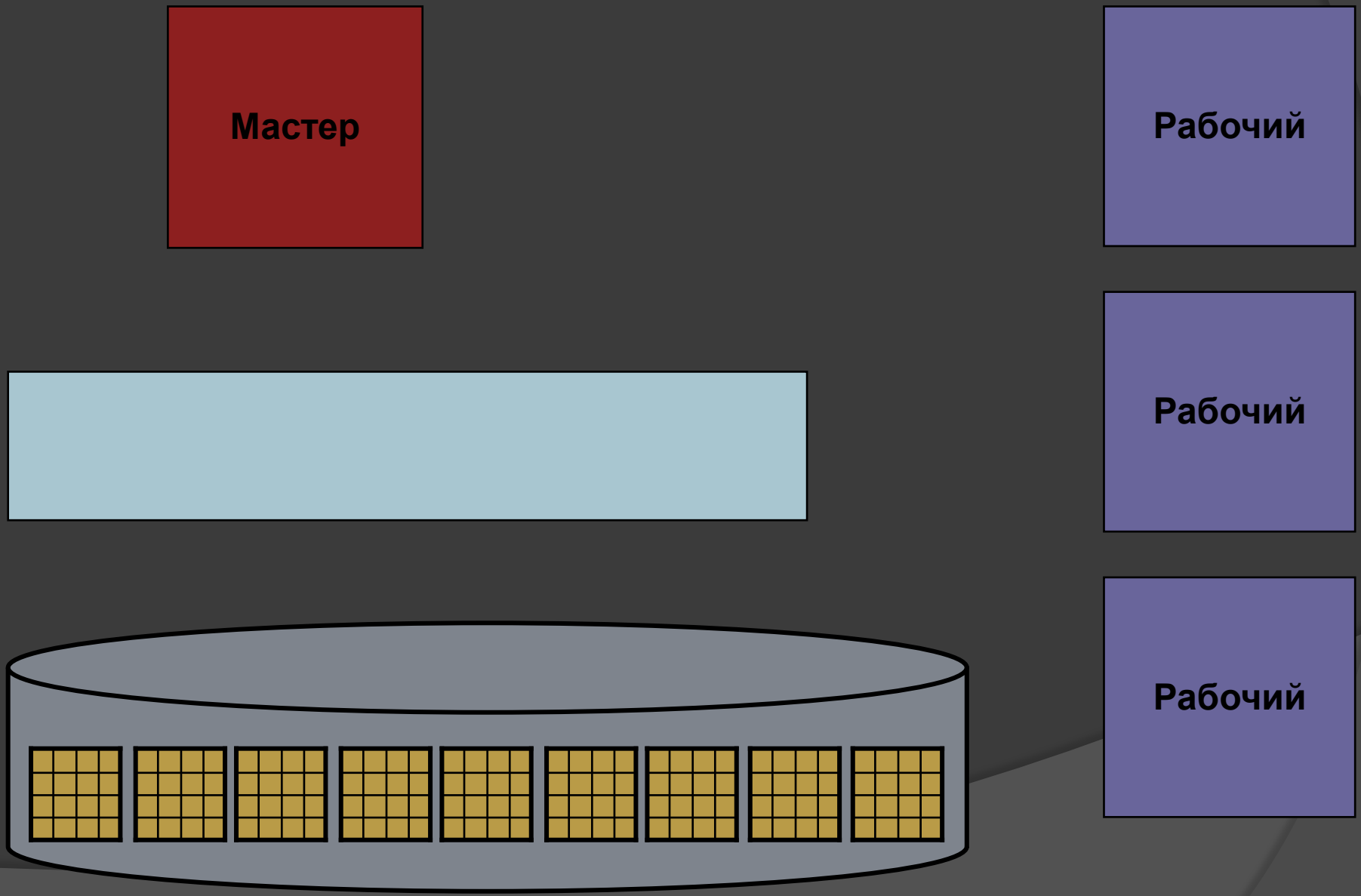


Процессор Cell

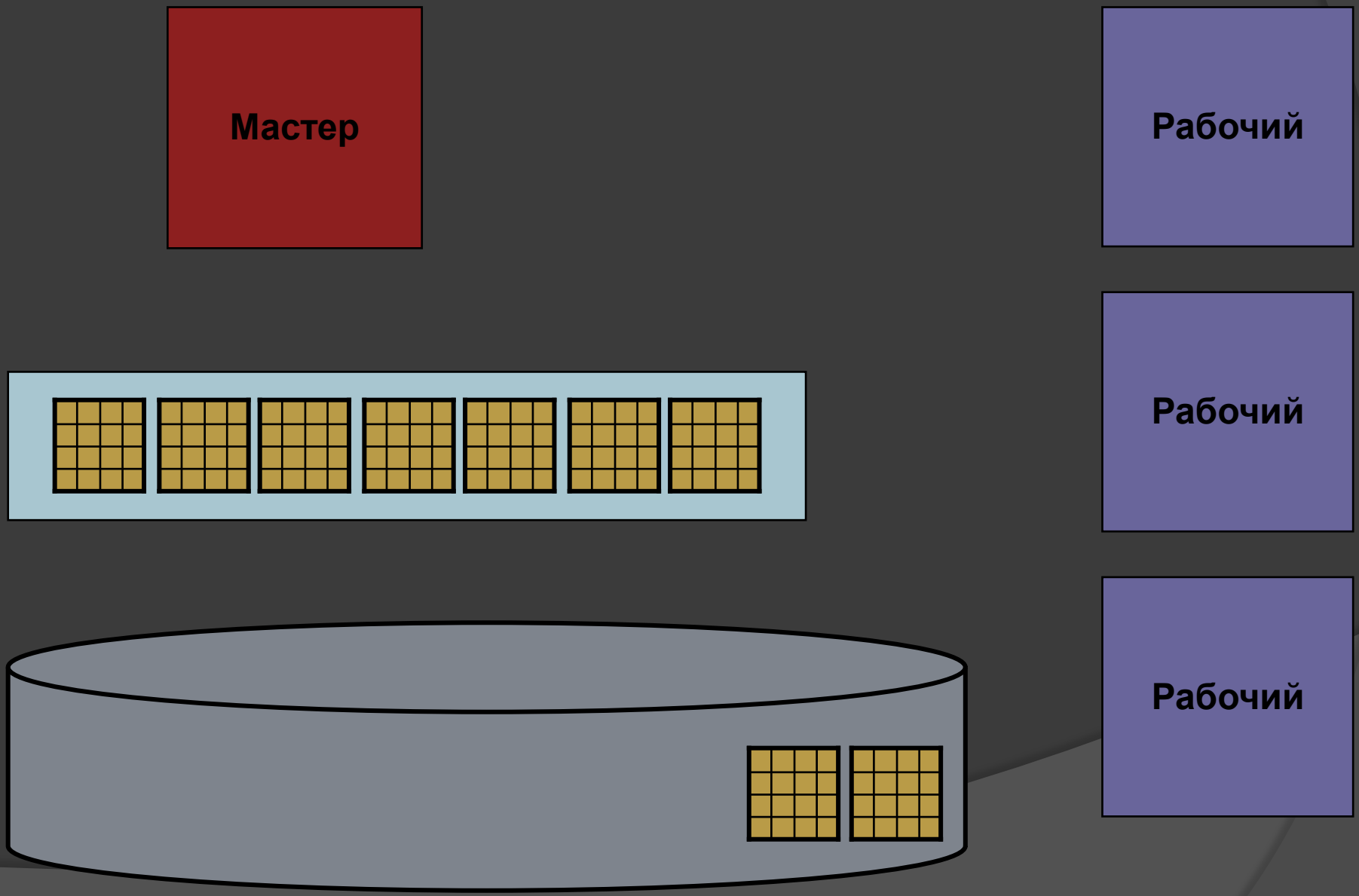
- Асимметричная архитектура
- Высокопроизводительные векторные вычисления
- Используется в самом производительном суперкомпьютере в мире (IBM Roadrunner)



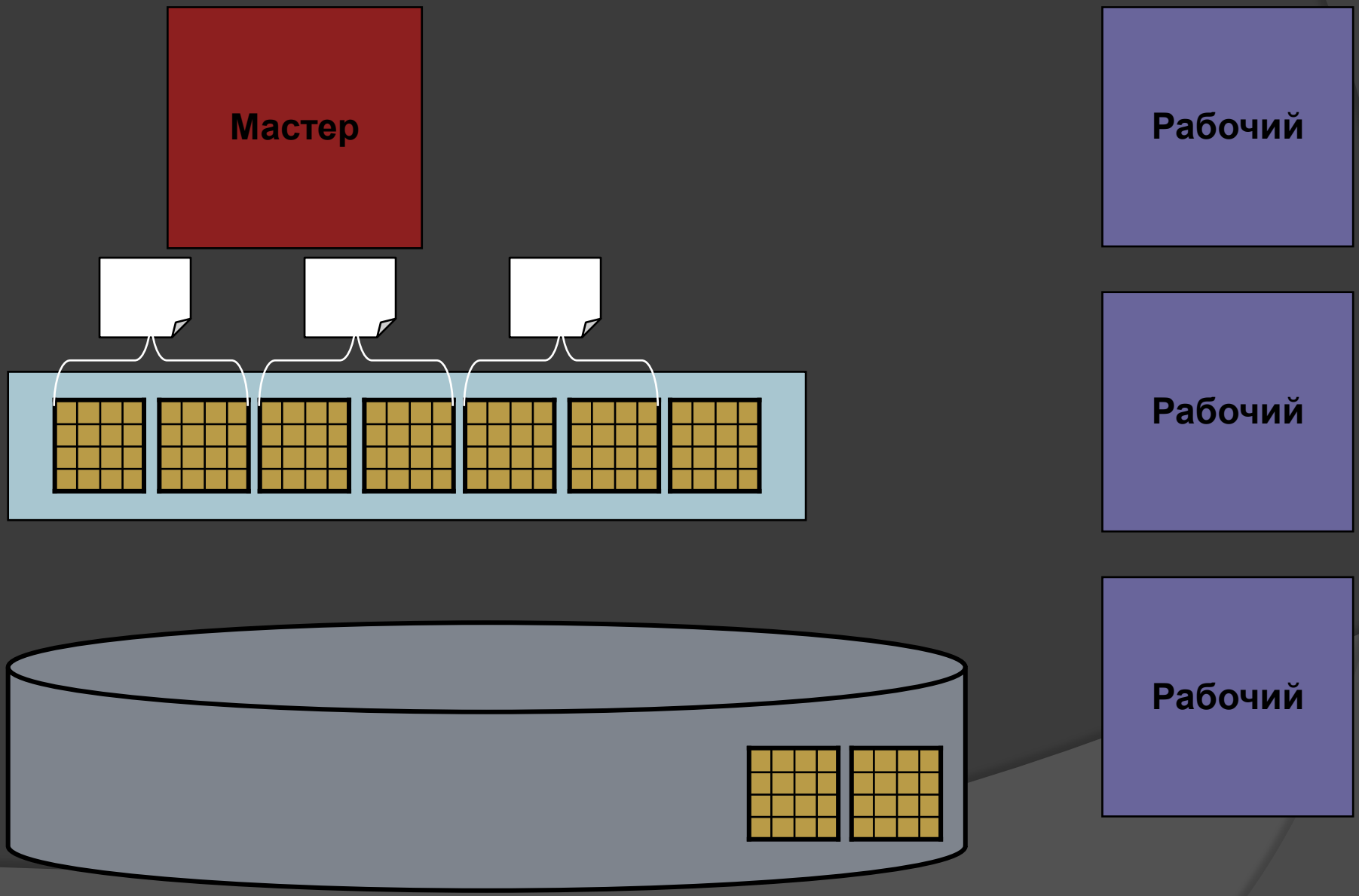
Загрузка данных в память



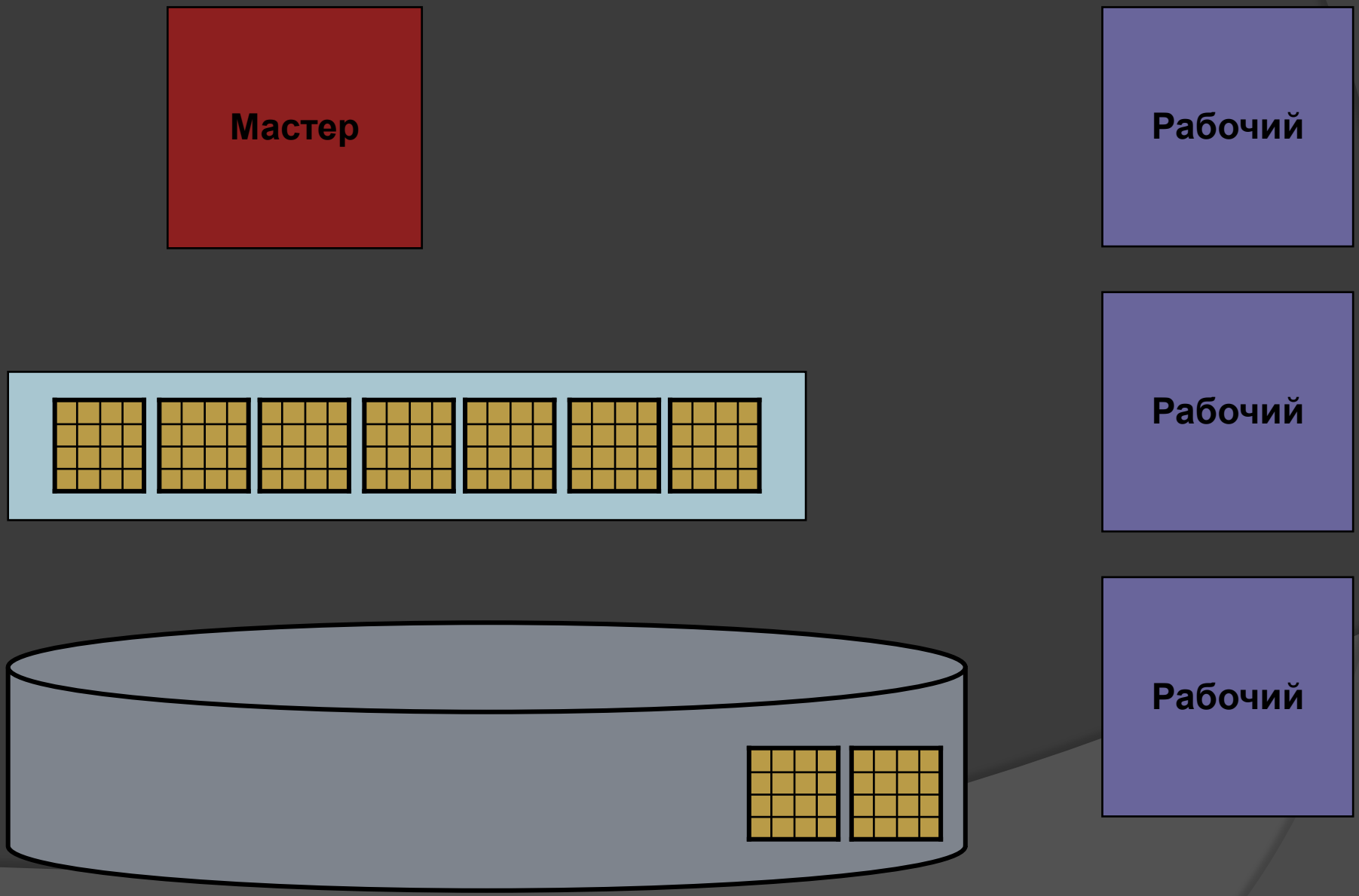
Формирование заданий



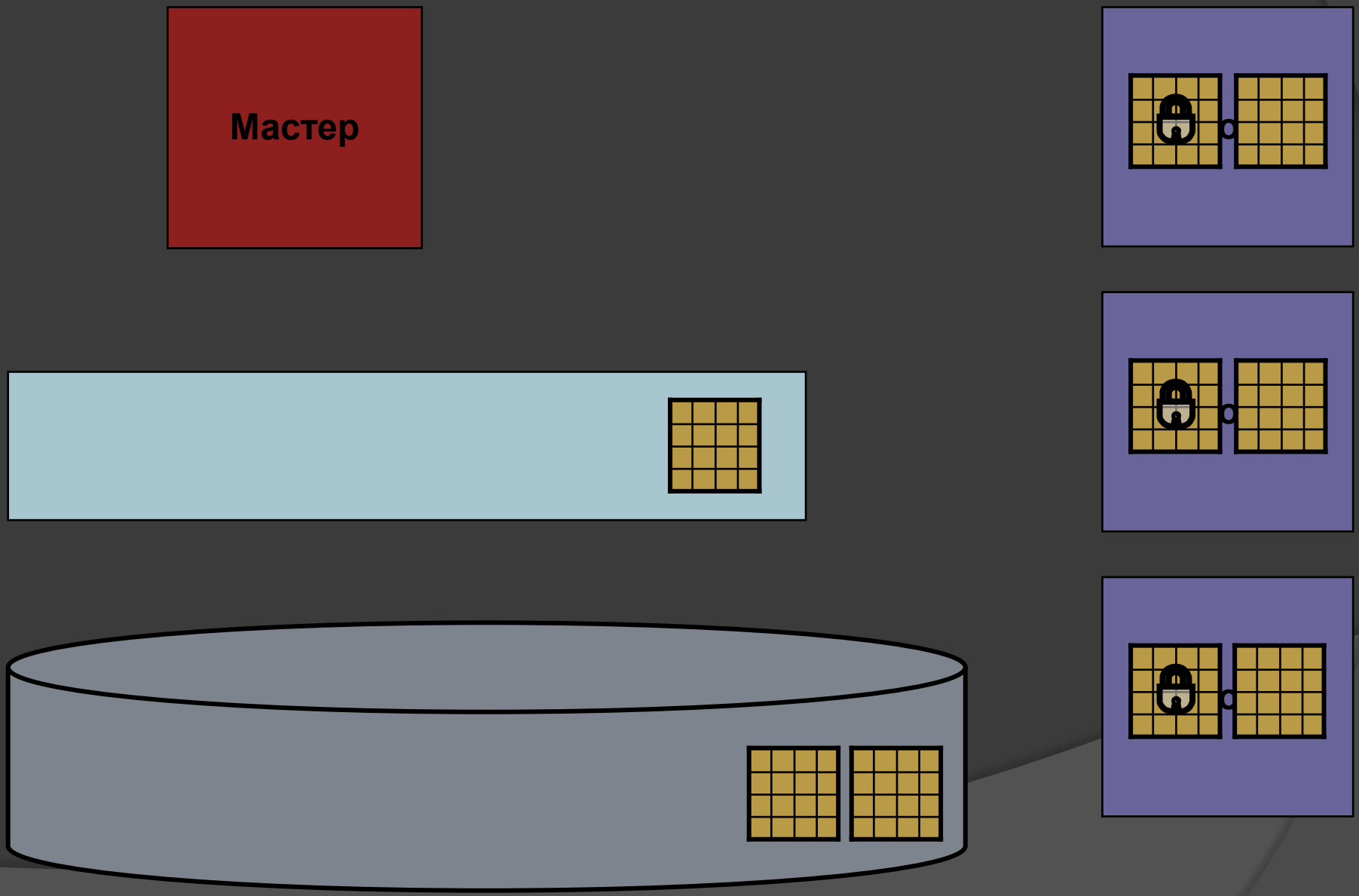
Отправка заданий



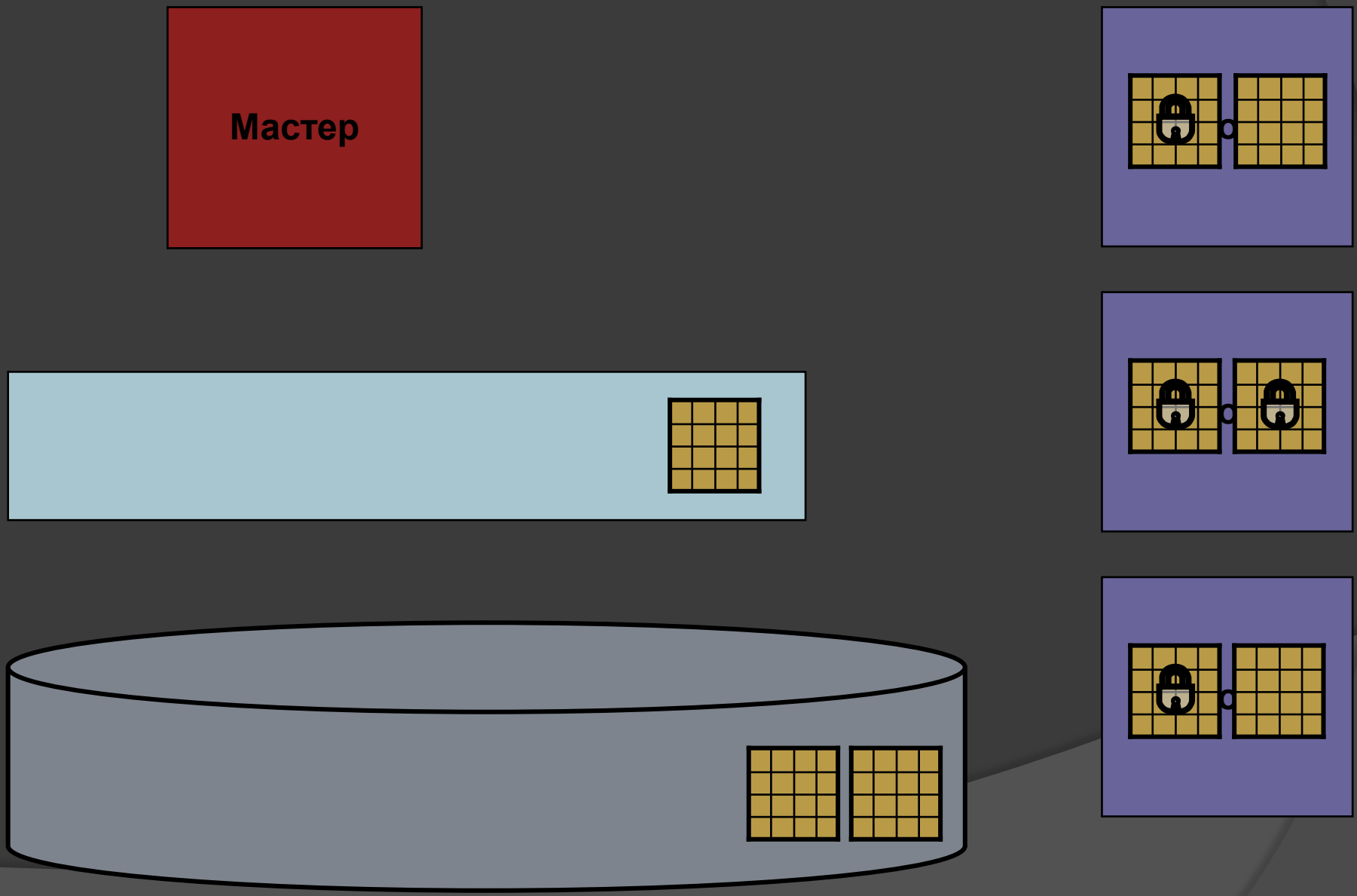
Загрузка данных в локальную память SPE



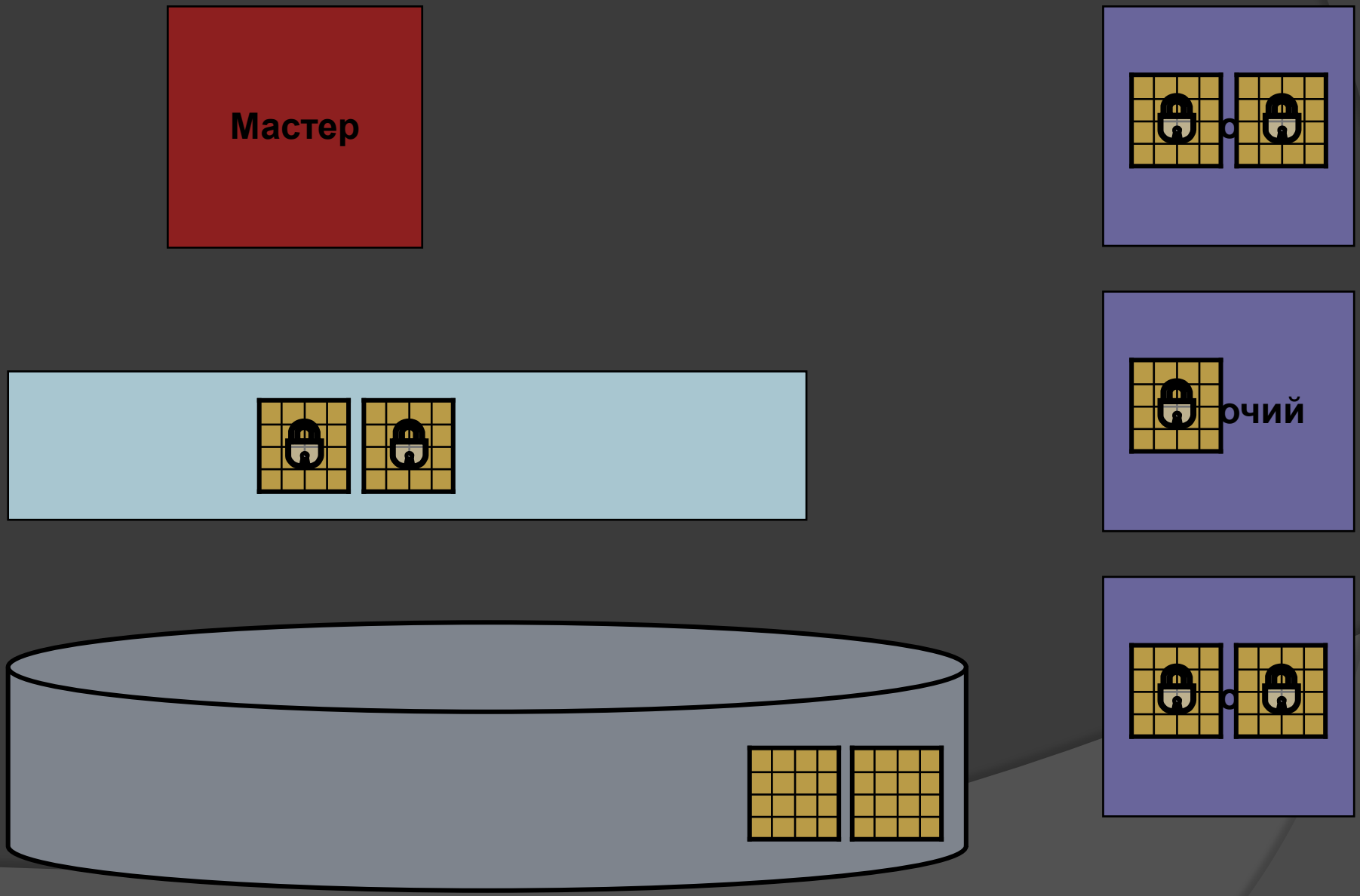
Шифрование блоков



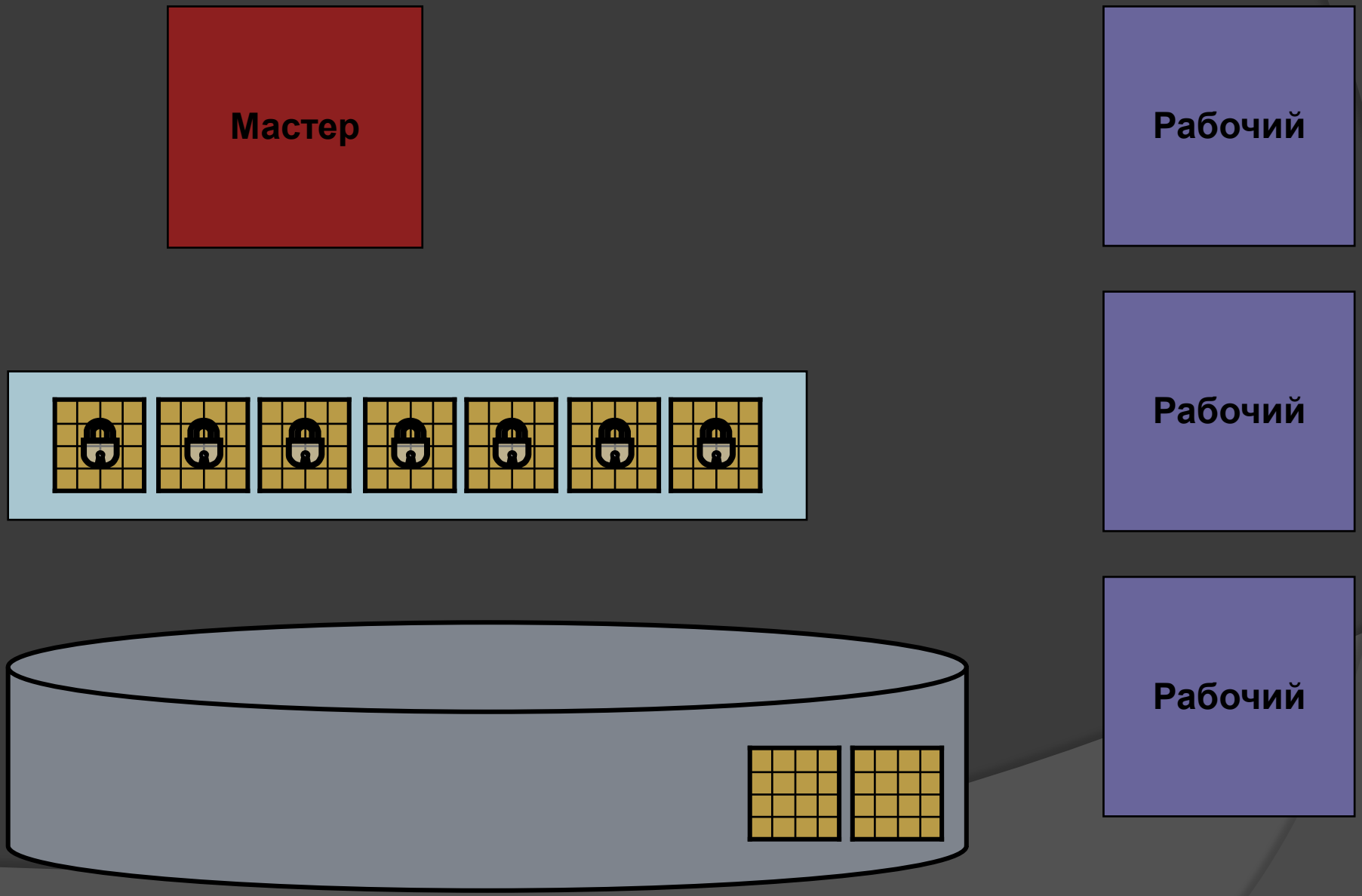
Шифрование блоков



Загрузка результатов в основную память



Запись результатов на диск



Реализация

- Название: PAES-CTR
- Язык: C++
- Инструментальные средства
  - IBM SDK for Multicore Acceleration
- Объем исходного кода: 938 строк
- Исходные тексты: http://pcs.susu.ru/projects/3/3.PAES-CTR.shtml

Оптимизация

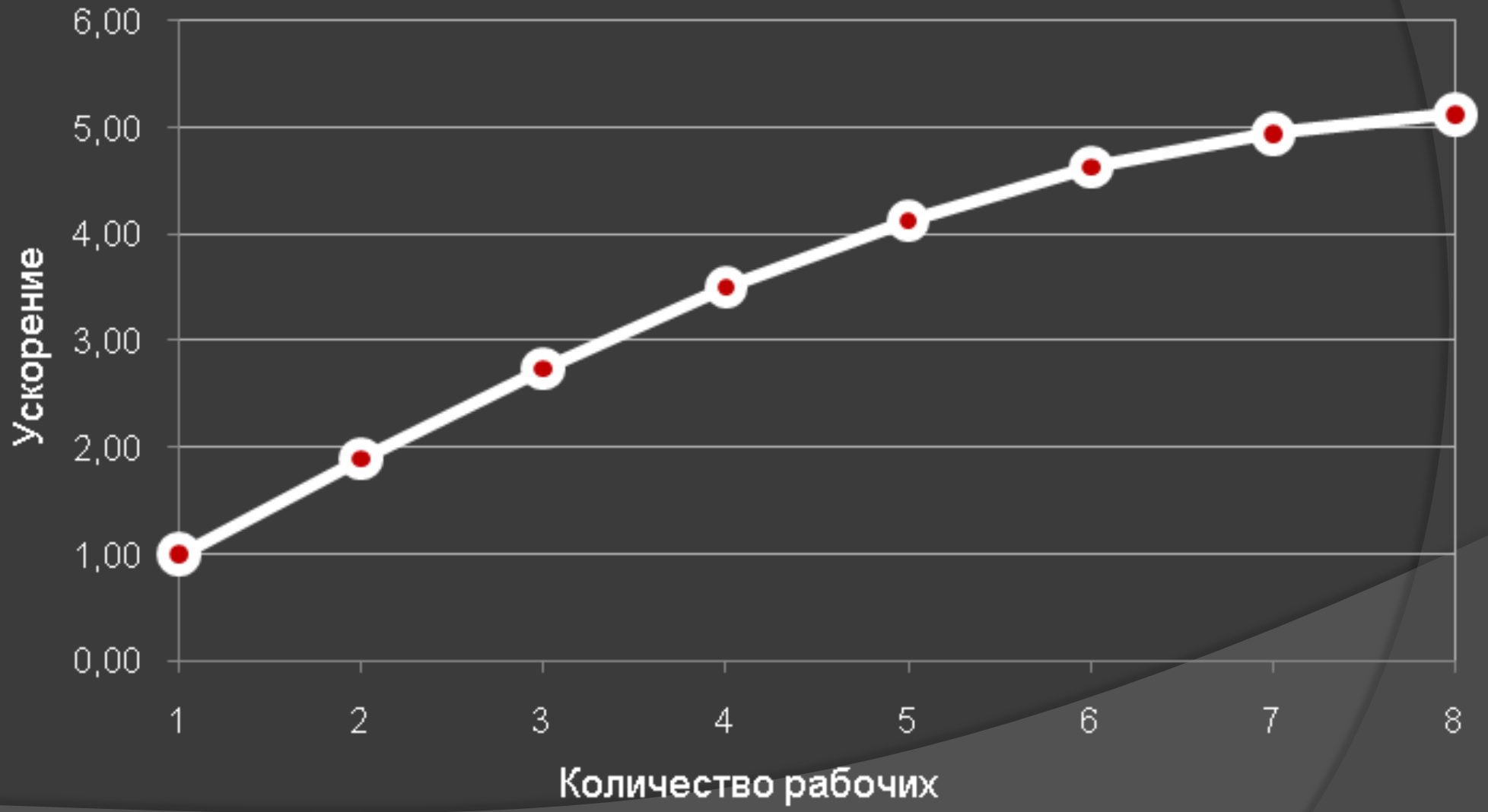
- Опережающая загрузка данных
- Векторная реализация шифрующих преобразований

Вычислительные эксперименты

- Цели экспериментов
  - Вычислить ускорение
  - Сравнить с другими реализациями
- Целевая система: Cellus в ЮУрГУ
  - 2 процессора PowerXCell 8i
  - Тактовая частота: 3.2 ГГц
  - Пропускная способность шины EIB: 200ГБ/с

Ускорение

Размер задачи: 1ГБ
Длина ключа: 128 бит



Сравнение

Размер задачи: 1ГБ
Длина ключа: 128 бит

Апробации

- Всероссийская научно-практическая конференция «Разработки Российской Федерации по приоритетным направлениям развития науки, технологии и техники» (11-13 мая 2009 г., ЮУрГУ)

Основные результаты

- Разработан алгоритм шифрования по стандарту AES в режиме счетчика, оптимизированный для вычислительных систем на базе процессоров Cell.
- Проведены вычислительные эксперименты, подтверждающие эффективность разработанного алгоритма.

Дополнительно: Эффективность

Размер задачи: 1ГБ
Длина ключа: 128 бит

Дополнительно: Стоимость

Размер задачи: 1ГБ
Длина ключа: 128 бит