Обзор и классификация алгоритмов деления и приведения по модулю больших целых чисел для криптографических приложений

Мария Ковтун
Ковтун Владислав
Компания «Сайфер»

Содержание

- Введение
- Актуальность
- Классификация алгоритмов
- Выводы

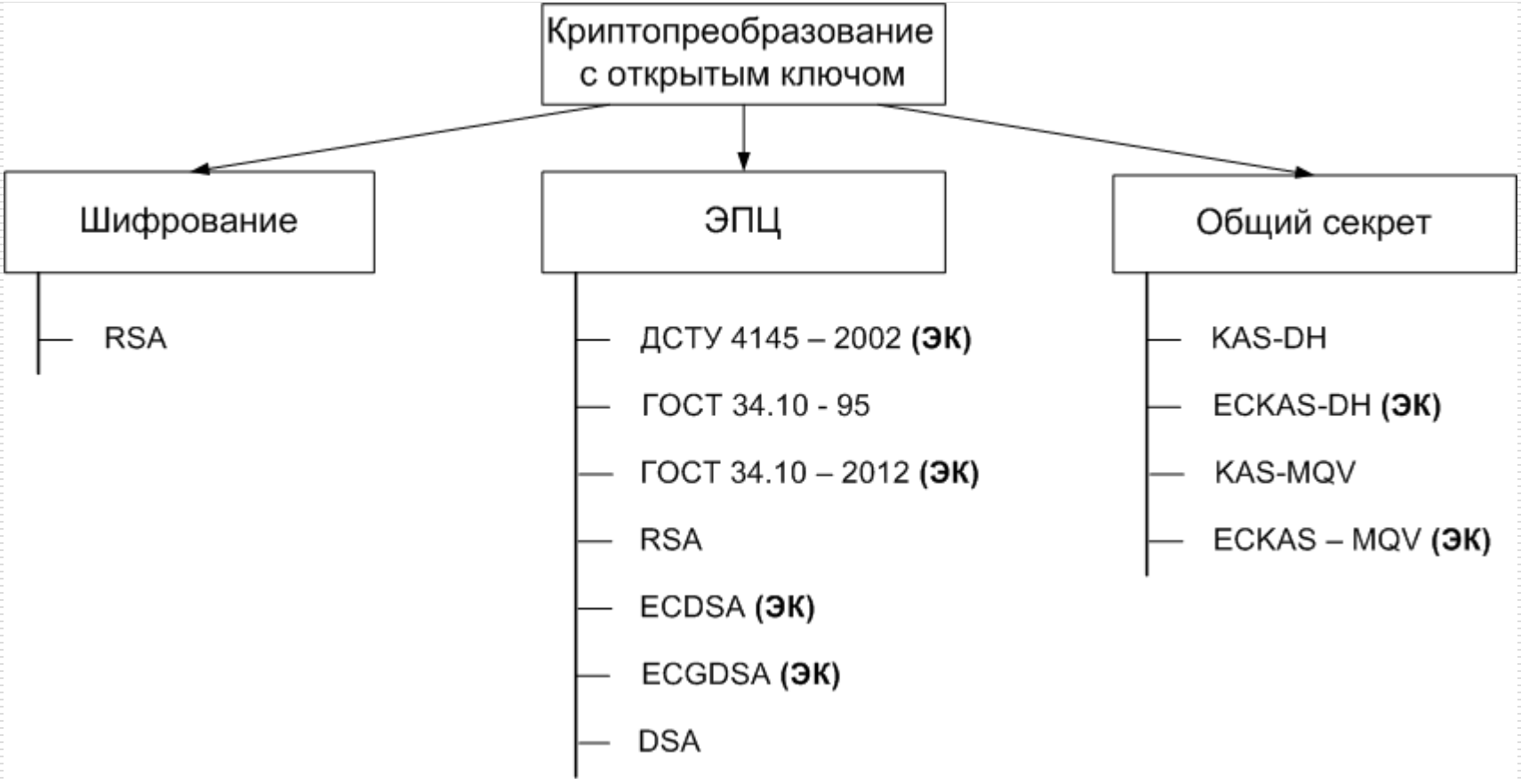
Введение

Цель: классификации алгоритмов деления и приведения по модулю больших целых чисел для заданных условий

Объект: операция деления и приведения по модулю больших целых чисел

Предмет: алгоритмы деления и приведения по модулю больших целых чисел

Актуальность



Актуальность

<table>
<tr><td>Криптопреобразования</td><td colspan="3">Зашифровывание/ расшифровывание</td><td colspan="3">Формирование и проверка цифровой подписи</td><td colspan="3">Обмен ключами</td></tr>
<tr><td rowspan="2">Арифметика в группе точек эллептической кривой</td><td colspan="6">Скалярное умножение точек эллиптической кривой</td><td colspan="3" rowspan="2">Генерация случайной точки</td></tr>
<tr><td colspan="4">Сложение точек</td><td colspan="2">Удвоение точки</td></tr>
<tr><td>Арифметика в поле FG(p)</td><td>Умножение</td><td>Сложение</td><td>Деление</td><td>Возведение в квадрат</td><td>Приведение по модулю</td><td>Инвертирование</td><td>Извлечения квадратного корня</td></tr>
<tr><td>Операции над массивами</td><td colspan="2">Сдвиг</td><td colspan="2">Сравнение</td><td colspan="2">Сложение</td><td>Вычитание</td><td>Умножение</td></tr>
<tr><td>Команды CPU</td><td colspan="9">mov, mul, shr, shl, add, sub</td></tr>
</table>

КАК ПРАВИЛЬНО ВЫБРАТЬ АЛГОРИТМ?

Выбор алгоритма (общие)

- Условия
  - Тип реализации (SW/HW)
  - Переносимость
  - Максимальное быстродействие
  - Минимальный размер оперативной памяти
  - Минимальный размер кода
  - Пониженное энергопотребление
  - Реальный масштаб времени

Выбор алгоритма (общие)

- Условия
  - Минимальная (но продолжительная) загрузка процессора
  - Минимизация ошибок – самопроверка
  - Защита от атак на реализацию
    - Время отклика
    - Потребляемая мощность
  - Стоимость
    - Разработки/Владения
    - Сопровождения

Выбор алгоритма (SW)

- Характеристики процессора
  - Набор инструкций
    - Стандартный
    - Расширенный
  - Количество потоков
  - Разрядность (8, 16, 32, 64)
  - Энергопотребление|Тепловыделение
  - Специфические возможности (Intel TurboBoost)

Выбор алгоритма (SW)

- Операционная система
- Компилятор C++
  - GCC
  - Intel
  - Microsoft
  - NVidia CUDA
  - Open CL
  - AMD Stream OpenCL APP
  - И т.д.

Выбор алгоритма (SW)

- Доступный объем оперативной памяти
  - Данные
  - Код
- Доступный объем постоянной памяти
  - Данные
  - Код

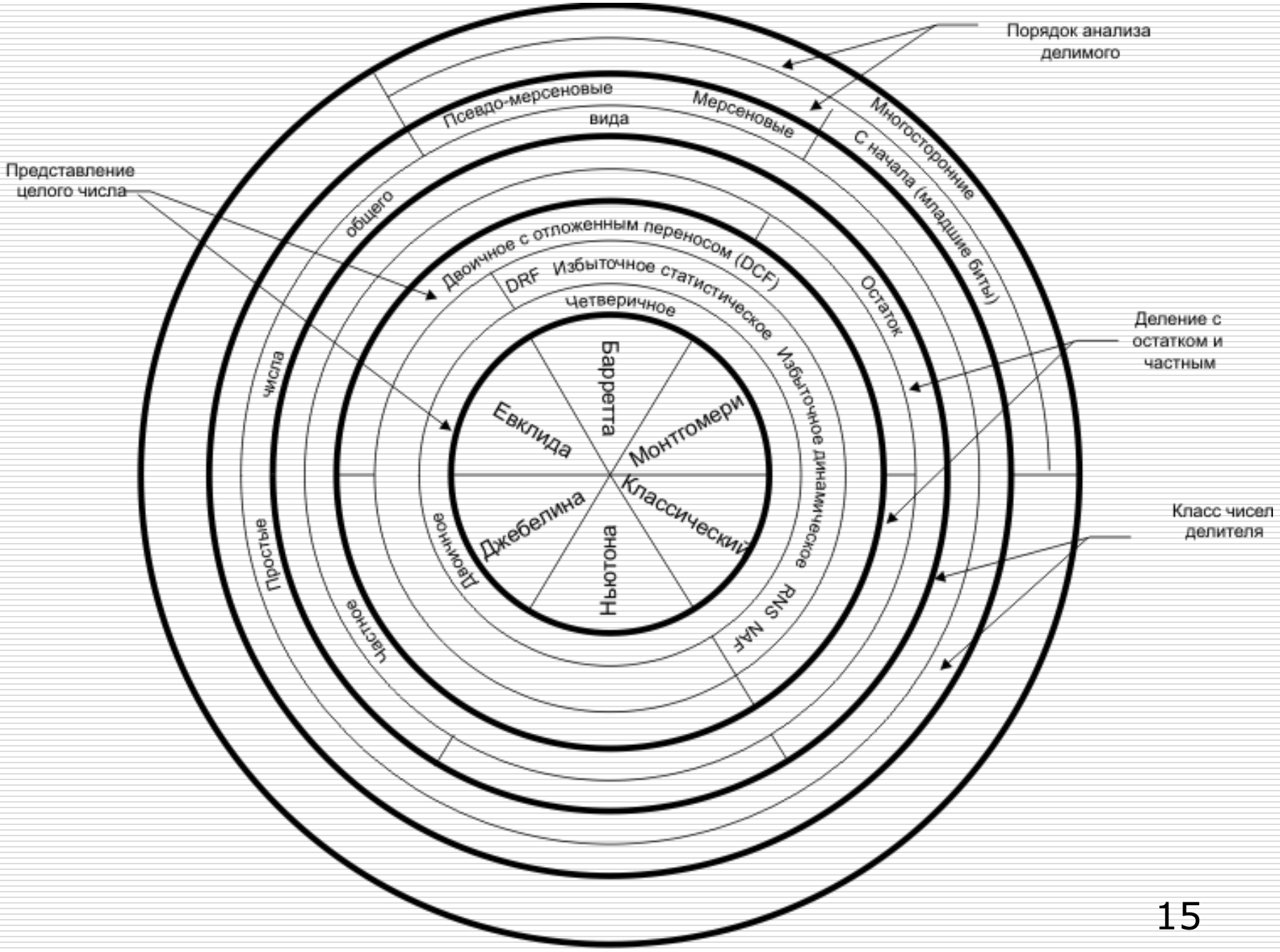
Выбор алгоритма (HW)

- Технология
  - ASIC
  - FPGA
- Частота
- Разрядность
- Энергопотребление
- Количество элементов
- И т.д.

КЛАССИФИКАЦИЯ АЛГОРИТМОВ ДЕЛЕНИЯ И ПРИВЕДЕНИЯ ПО МОДУЛЮ

Представление целого числа (делимого и делителя)

- Двоичное (**обычное**)
- Четверичное
- Двоичное сокращенное (двоичное DRF)
- Избыточное статическое
- Избыточное динамическое
- Несмежное (NAF)
- Остаточных классов (RNS)
- Двоичное, с отложенным переносом (**DCF**)
- Смешанные
- ZOT = представление

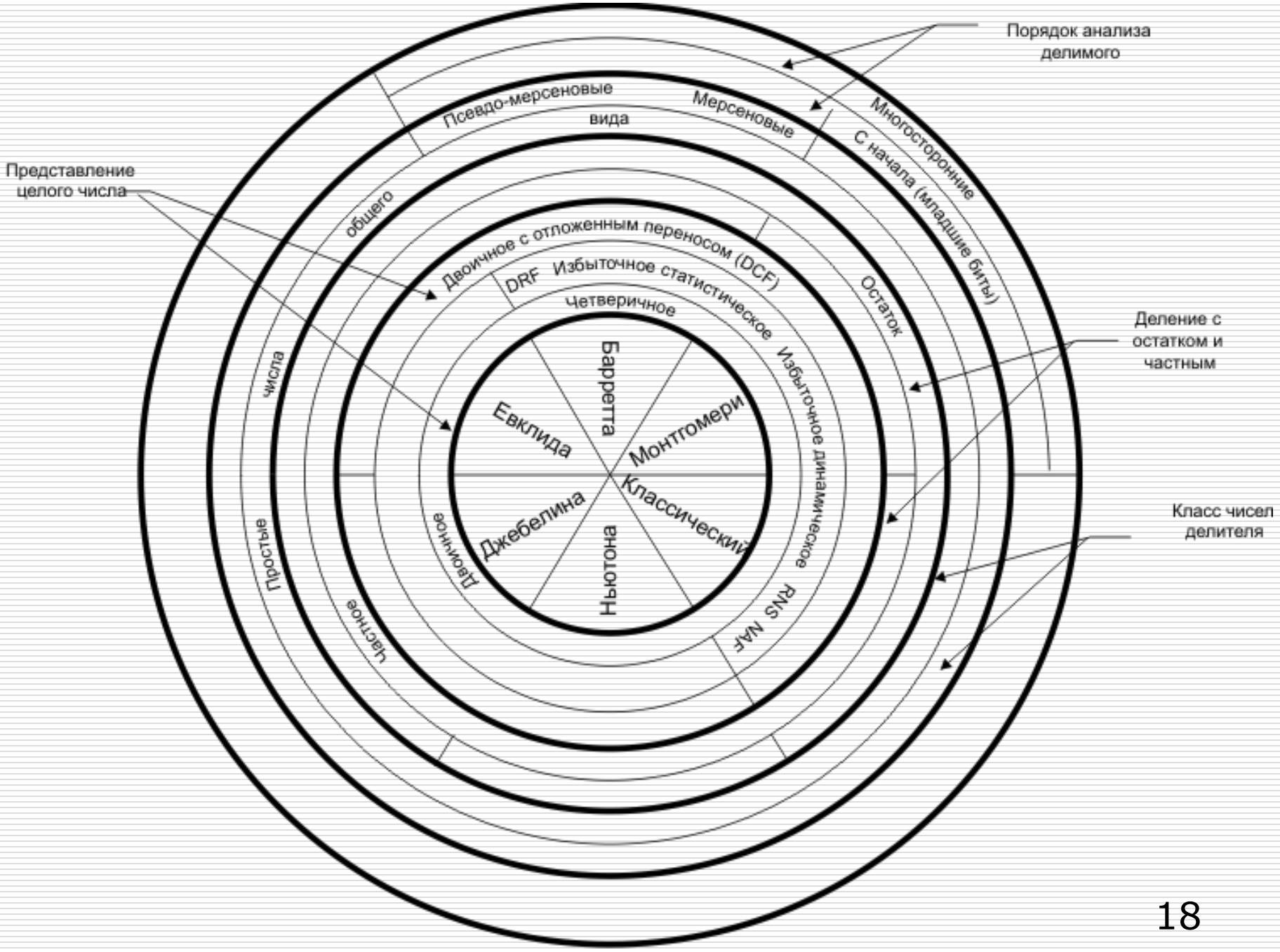

Порядок анализа делимого
Представление целого числа
Деление с остатком и частным
Класс чисел делителя
Псевдо-мерсеновые
Мерсеновые
вида
общего
числа
Простые
Частное
Двоичное
Многосторонние
С начала (младшие биты)
Остаток
Двоичное с отложенным переносом (DCF)
DRF
Избыточное статистическое
Четверичное
Избыточное динамическое
RNS NAF
Барретта
Монтгомери
Евклида
Классический
Джебелина
Ньютона

Делитель - произвольные числа, не обязательно простые

- Алгоритм деления «в столбик»
- Алгоритм деления Барретта
- Алгоритм деления Монтгомери
- Расширенный алгоритм Эвклида

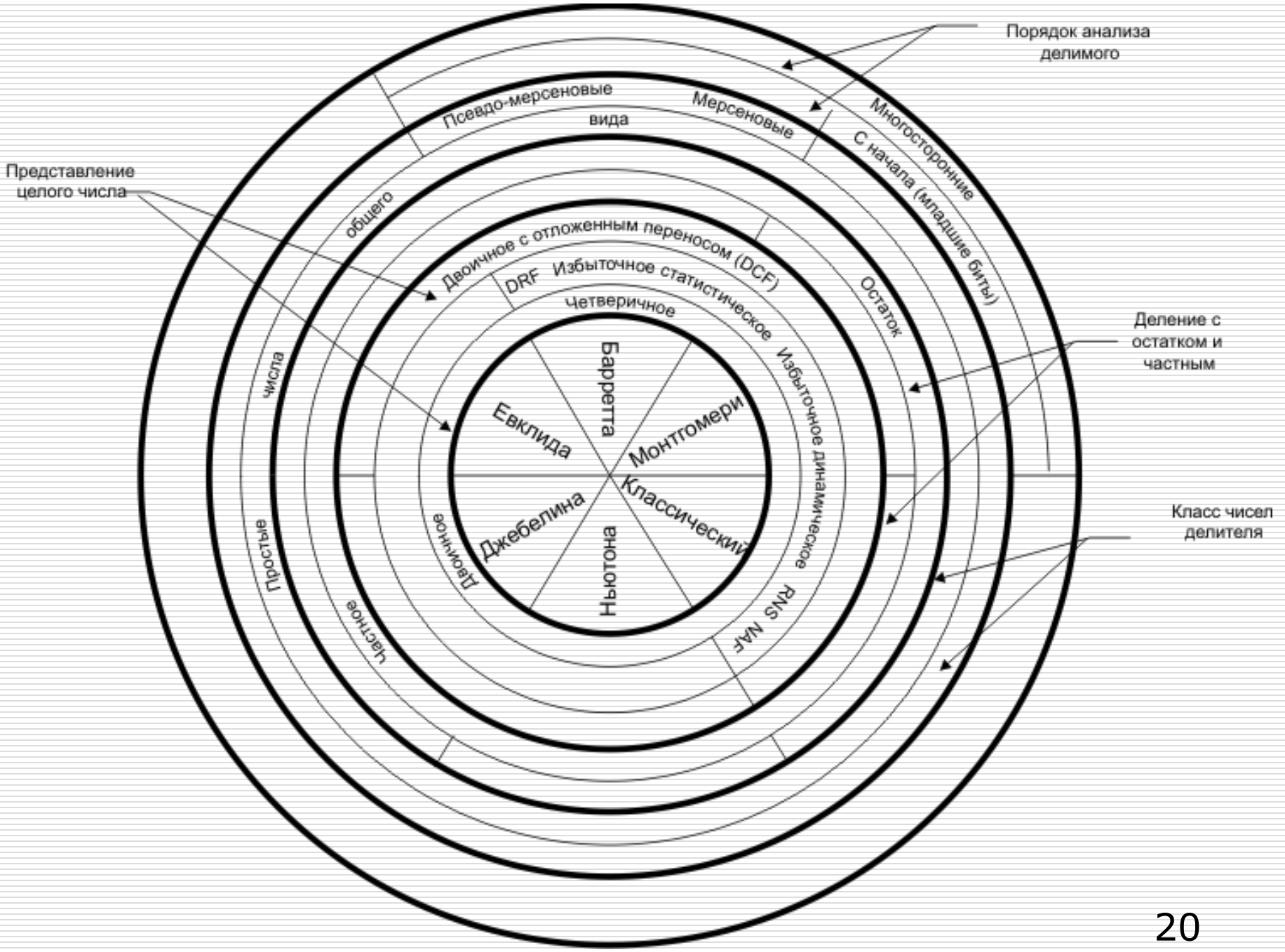
Полученный результат

- Для получения только частного
- Для получения только остатка – приведение по модулю
- Для получения, как частного, так и остатка


Порядок анализа делимого
Представление целого числа
Деление с остатком и частным
Класс чисел делителя
Псевдо-мерсеновые вида
Мерсеновые
Многосторонние
С начала (младшие биты)
общего
числа
Простые
Частное
Двоичное
Остаток
Двоичное с отложенным переносом (DCF)
DRF
Избыточное статистическое
Четверичное
Избыточное динамическое
RNS NAF
Барретта
Евклида
Монтгомери
Джебелина
Классический
Ньютона

Тип делителя (класс чисел)

- Составные числа (не простые)
- Простые числа общего вида
- Простые числа, являющиеся обобщенными простыми Мерсенна и псевдо-Мерсенна


Порядок анализа делимого
Представление целого числа
Деление с остатком и частным
Класс чисел делителя
Псевдо-мерсеновые
Мерсеновые
вида
Многосторонние
С начала (младшие биты)
общего
Двоичное с отложенным переносом (DCF)
DRF
Избыточное статистическое
Четверичное
Остаток
числа
Барретта
Евклида
Монтгомери
Джебелина
Классический
Ньютона
Простые
Частное
Двоичное
Избыточное динамическое
RNS NAF

Направление анализа делимого

- С начала (с младших бит) в алгоритме Монтгомери
- С конца (с старших бит) в алгоритме Барретта
- Двусторонние и многосторонние, как для алгоритма Барретта, так и для Монтгомери

Базовый алгоритм

- Классический
- Монтгомери и его модификации
- Барретта и их модификации
- Универсальный и жестко запрограммированный специальный делитель (модуль)
- Расширенный алгоритм Евклида
- Алгоритм итераций Ньютона
- Алгоритм деления Джебелина

Точность получения результата

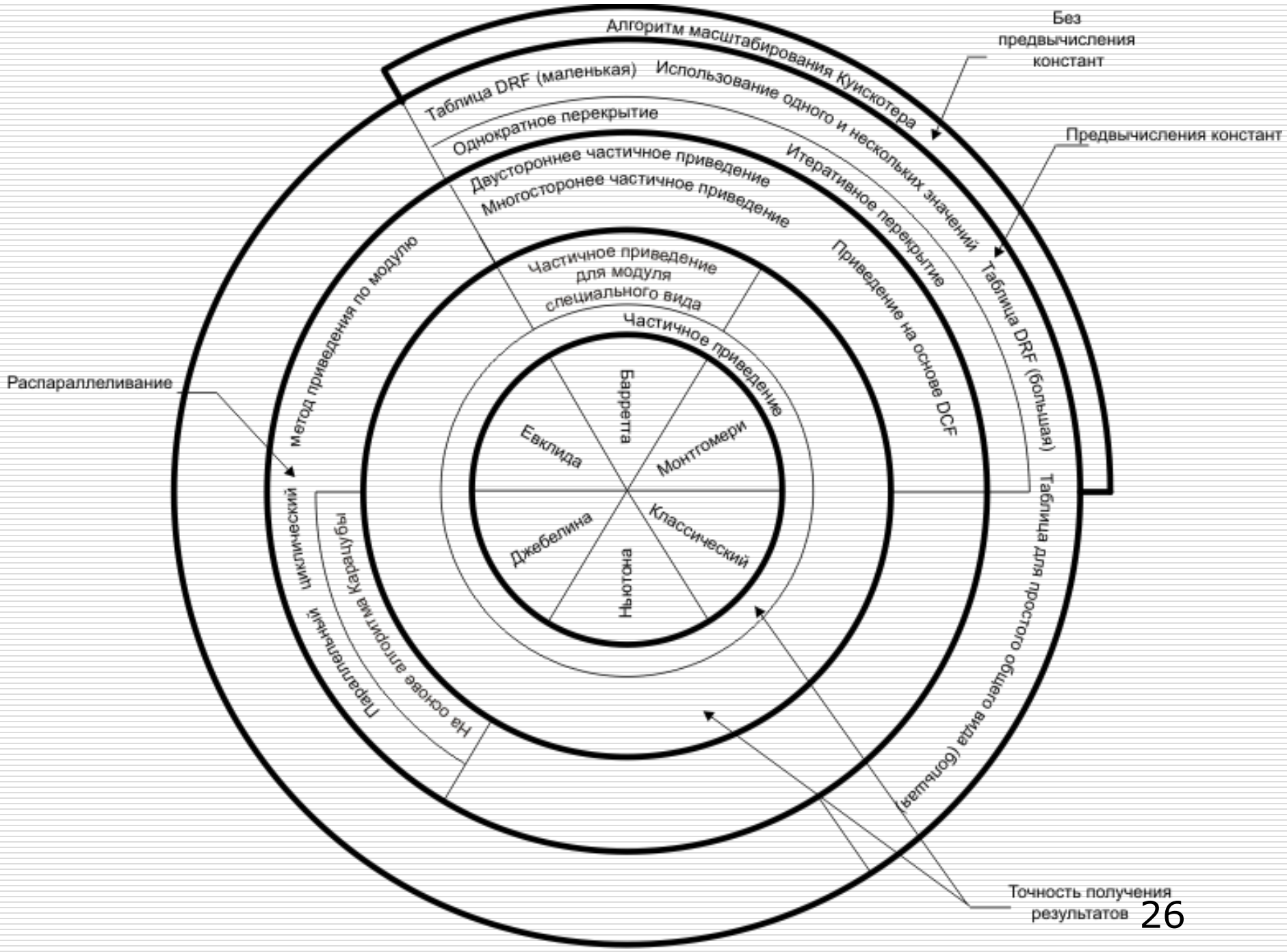
- Частичное деление/приведение для алгоритма Монтгомери
- Частичное деление/приведение для алгоритма Барретта
- Частичное деление/приведение для алгоритма «в столбик»
- Частичное приведение для модуля специального вида

Распараллеливание

- Двустороннее частичное деление/приведение для алгоритма Монтгомери
- Многостороннее частичное деление/приведение для алгоритма Монтгомери
- Двустороннее и многостороннее частичное деление/приведение для алгоритма Барретта

Распараллеливание

- Деление/приведение для алгоритма Барретта на основе DCF
- Деление с использованием параллельного алгоритма Карацубы, предложенное Джебелином
- Алгоритм распараллеливания представления многократной точности через одинарную точность целого числа


Алгоритм масштабирования Куискотера
Без предвычисления констант
Предвычисления констант
Таблица DRF (маленькая)
Использование одного и нескольких значений
Однократное перекрытие
Итеративное перекрытие
Двустороннее частичное приведение
Многосторонее частичное приведение
Приведение на основе DCF
Таблица DRF (большая)
Частичное приведение для модуля специального вида
Частичное приведение
Таблица для простого общего вида (большая)
Распараллеливание
Метод приведения по модулю
Барретта
Евклида
Монтгомери
Джебелина
Классический
Ньютона
Циклический
Параллельный
На основе алгоритма Карацубы
Точность получения результатов

Предвычисления

- Однократное и итеративное перекрытие алгоритма Барретта
- Использование одного или нескольких предвычисленных значений (алгоритм Барретта, Монтгомери, Классический)
- Таблица предвычислений для простого общего вида (большая) (алгоритм Барретта, Монтгомери, Классический)

Предвычисления

- Таблица предвычислений для простого специального вида DRF (большая) (алгоритм Барретта, Монтгомери, Классический)
- Таблица предвычислений для модуля специального вида DRF (маленькая) (алгоритм Барретта, Монтгомери, Классический)

Без предвычисленых констант

- Без вычислений констант для алгоритма Монтгомери (алгоритм масштабирования Куискотера)
- Без вычислений констант для алгоритма Барретта (алгоритм масштабирования Куискотера)

Алгоритм умножения

- Без умножения (на основе расширенного алгоритма Эвклида)
- Алгоритм Комба
- Алгоритм Карацубы
- Алгоритм Фюрера
- Быстрое преобразование Фурье (FFT)
- Алгоритм Toom-Cook

Вспомогательные алгоритмы

- Без вспомогательных алгоритмов
- С вспомогательными алгоритмами
  - Инвертирование
  - Извлечение квадратного корня
  - И т.д.

ВЫВОДЫ

Выводы

- Сформулированы основные условия разработки криптосистем
- Проведен обзор известных алгоритмов деления и приведения по модулю целых чисел **для криптографических приложений**

Выводы

- Проведено исследование известных алгоритмов деления
- Предложена классификация по различным критериям

Вопросы?

Спасибо за внимание!

Компания «Сайфер»

Мария Ковтун

email: mg.kovtun@gmail.com