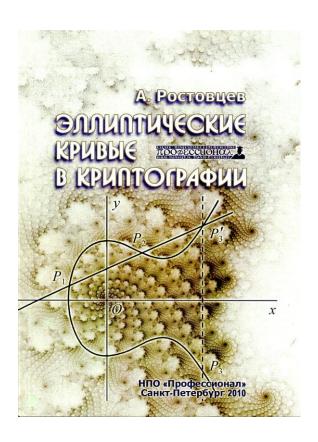
## Эллиптические кривые в криптографии. Теория и вычислительные алгоритмы



## Содержание

## Введение

Глава 1. Сведения из алгебры

- 1.1. Множества и алгоритмы
- 1.2. Группы
- 1.3. Коммутативные кольца
- 1.4. Поля
- 1.5. Мнимые квадратичные порядки

Глава 2. Эллиптические кривые

- 2.1. Алгебраические кривые
- 2.1.1. Аффинная и проективная плоскости

- 2.1.2. Сложение точек на кубике
- 2.1.3. Пересечение кубики и прямой. Особые точки
- 2.2. Функции и отображения алгебраических кривых
- 2.2.1. Регулярные функции и регулярные отображения
- 2.2.2. Рациональные функции и рациональные отображения
- 2.3. Дивизоры на алгебраических кривых
- 2.4. Нормальные формы эллиптической кривой
- 2.5. Эллиптические кривые над полем комплексных чисел
- 2.5.1. Эллиптические функции
- 2.5.2. Параметризация эллиптической кривой эллиптическими функциями
- 2.5.4. Изоморфизмы и эндоморфизмы эллиптических кривых
- 2.5.5. Модулярная функция і
- 2.5.6. Модулярный полином и модулярная кривая
- 2.5.7. Поле классов мнимого квадратичного порядка
- 2.6. Дискриминант и ј-инвариант
- 2.7. Закон сложения точек эллиптической кривой
- 2.8. Эллиптические кривые над числовыми полями
- 2.9. Отображения эллиптических кривых
- 2.9.1. Функции на эллиптических кривых
- 2.9.2. Отображение Фробениуса
- 2.9.3. Формальная группа
- 2.9.4. Изоморфизмы эллиптических кривых
- 2.9.5. Эндоморфизмы эллиптических кривых
- 2.9.6. Изогении эллиптических кривых
- 2.10. Спаривание Вейля
- 2.11. Эллиптические кривые над конечными полями и кольцами

- 2.11.1. Число точек
- 2.11.2. Изогении
- 2.11.3. Эллиптические кривые над кольцами /n
- Глава 3. Криптосистемы на эллиптических кривых
- 3.1. Установление сеансового ключа
- 3.2. Цифровая подпись
- 3.2.1. Стандарт подписи ECDSA
- 3.2.2. Стандарт подписи РФ ГОСТ Р 34.10-2001
- 3.2.3. Стандарт подписи Германии
- 3.2.4. Короткая подпись на билинейных отображениях
- 3.3. Шифрование с открытым ключом
- 3.3.1. Шифрование по Эль-Гамалю
- 3.3.2. Гомоморфное шифрование с открытым ключом
- 3.4. Генераторы случайной последовательности
- 3.5. Безопасность криптосистем на эллиптических кривых
- 3.6. Криптосистемы на изогениях эллиптических кривых
- Глава 4. Вычислительные алгоритмы
- 4.1. Алгоритмы умножения чисел и полиномов
- 4.1.1. Модульное умножение
- 4.1.2. Умножение в конечных полях характеристики 2, 3
- 4.2. Деление
- 4.2.1. Деление в кольце
- 4.2.2. Деление в евклидовых кольцах целых алгебраических чисел
- 4.3. Обращение и вычисление наибольшего общего делителя
- 4.4. Решение алгебраических уравнений в конечных полях
- 4.4.1. Извлечение квадратных и кубических корней

- 4.4.2. Решение алгебраических уравнений
- 4.5. Вычисление символа Якоби
- 4.6. Проверка чисел и полиномов над конечным полем на простоту
- 4.7. Разложение простого числа в мнимом квадратичном порядке
- 4.8. Сложение и комплексное умножение точек эллиптической кривой
- 4.9. Умножение точки на число
- 4.9.1. Двоичное окно
- 4.9.2. Окно размером несколько бит
- 4.10. Вычисление билинейных отображений на эллиптической кривой
- 4.11. Арифметика группы классов мнимых квадратичных порядков
- 4.12. Вычисление числа классов и группы классов мнимого квадратичного порядка
- 4.13. Вычисление полинома, задающего поле классов мнимого квадратичного порядка
- 4.14. Генерация эллиптической кривой над конечным полем с вычислимым числом точек
- 4.15. Разложение составного числа
- 4.16. Генерация эллиптической кривой с вычислимой степенью расширения для спаривания Вейля
- 4.17. Эллиптическая кривая с заданным числом изогений
- 4.18. Вычисление числа точек эллиптической кривой над конечным полем
- 4.18.1. Алгоритм Чуфа
- 4.18.2. Алгоритм SEA
- 4.19. Вычисление изогений

Литература

Приложение 1. Алгебраические и численные вычисления в пакетах MATHEMATICA, MAPLE

Приложение 2. Программа генерации эллиптической кривой в пакете MATHEMATICA

Приложение 3. Гиперэллиптические кривые рода 2

Указатель