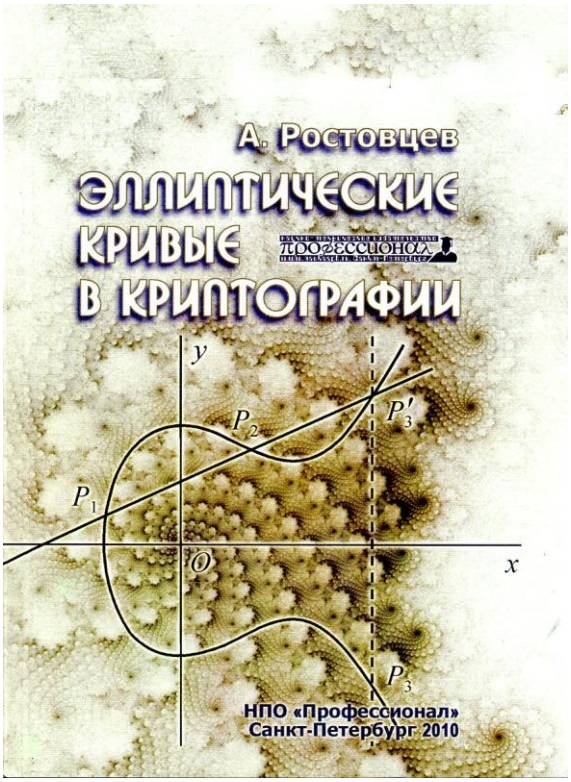
Эллиптические кривые в криптографии. Теория и вычислительные алгоритмы



Содержание

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 j

2.5.6. Модулярный полином и модулярная кривая

2.5.7. Поле классов мнимого квадратичного порядка

2.6. Дискриминант и j-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