2022-2023学年秋季学期

课程名称: 信息安全数学基础

英文名称: Mathematical Foundations for Information Security

授课团队：胡磊、许军、王丽萍

助　　教：郭一

信息安全数学基础

Mathematical Foundations for Information Security

[第 8 次课] 算法和具体概念小结

授课教师：许军

授课时间：2021年11月2日

概 要

- 信息安全中的有限代数集合及其四则运算、方幂运算和开平方的快速运算原理与算法
- 从无限代数集合到有限代数集合的数学基本概念和具体实例
- 有限代数集合带来的数据处理优劣性质和密码计算困难问题特性

加减法

- 与乘除法等其他运算相比，加减法的计算复杂度低得多，其成本被忽略不计。无加减法的快速算法。

乘法：Karatsuba快速乘法

- 适用于信息安全中的大整数的快速乘法、高次多项式的快速乘法
- 原理：“二分法”：

$$(a_0 + a_1 \cdot x^t)(b_0 + b_1 \cdot x^t)$$

$$= a_0b_0 + [(a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1]\, x^t + a_1b_1 \cdot x^{2t}$$

模逆：欧几里德算法（整数、域上多项式）

- 辗转相除：求最大公因子（最大公因式）

- 除法：等于被除式和除式逆的乘法
- 扩展欧几里德除法——求(s,t)，使得sa+tb=(a,b)。求(s(x),t(x))，使得sf+tg=(f,g)
- 可以只求一个系数：
  - ✓ 求a模素数p的逆。求f(x)模不可约多项式p(x)的逆
  - ✓ 秦九韶的大衍求一术
- 扩展欧几里德除法的复杂度：迭代步数、s和t的规模
- BCH纠错码译码中的关键方程求解

幂运算g^k

- 重复平方——相乘法（组合算法）
  - ✓ 适用于整数模p的幂运算、多项式模p(x)的幂运算
  - ✓ 从低位到高位、或从高位到低位
  - ✓ 秦九韶算法之多项式赋值
  - ✓ 乘法更少的重复平方——相乘法
- **Shamir's trick**——交换群中两个元素的幂运算$g^k h^l$
  - ✓ **DSA**签名验证
- 模幂运算的快速方法：**Montgomery**算法
  - ✓ 适用于整数模p的幂运算、多项式模p(x)的幂运算

开平方

- 整数模素数开平方
- 能否开平方的判定：基于二次互反律和辗转相除的计算雅可比符号的方法
- 开平方算法
  - ✓ 椭圆曲线的点嵌入
  - ✓ 模4余3的素数

约减模数：从大模数到小模数

- 中国剩余定理
  - ✓ **RSA—CRT**
- 模素数幂p^n的同余式的解法
  - ✓ 幂级数思想
  - ✓ 基于**Taylor**展开（只展开到一级导数）

素数来自何方

- 素性判定（**Fermat**、**Solovay-Stassen**、**Miller-Rabin**）

概念：整除

- 带余除法、整除概念及其相关性质
  - ✓ 离散对数问题的至多平方根复杂度
- 素数、不可约多项式
- 最大公因子最小公倍数及其相关性质

概念：同余与剩余类

- 整数同余的概念及其性质
- 剩余类（群的陪集、环的理想概念的具体例子）
- 完全剩余系：从无限集合到有限集合
  - ✓ 这个环有无零因子——是否模素数
  - ✓ **p**元有限域：四则运算和幂运算
  - ✓ **p**元域上多项式环模一个**n**次不可约多项式——$\mathbf{p^n}$元有限域：四则运算和幂运算
- 简化剩余系（环的乘法群的具体例子）
  - ✓ 何时是循环群

概念：互素模数的同余式组

- 同余式的中国剩余定理思想
  - ✓ 光滑阶群上的离散对数的脆弱性
- 模素数幂p^n的同余式求解的幂级数思想

概念：模意义下的平方元

- 平方剩余的概念
- 勒让德符号的概念（它是一种特殊的雅可比符号，雅可比符号是它的推广）

概念：阶与原根（循环群生成元）

- 群中阶的概念及相关性质
- 指数、指标的概念及相关性质
- 原根存在（简化剩余系是循环群）的条件

判定问题

- 素数判定的思想
- 判定的出发点、判定结论的对错、通过多次判定提升判定正确率的迭代次数