第一节 概述 略

第二节 认证技术概述

- 交互式证明系统 p3
  - NP问题
  - 图灵机
  - 验证者 证明者
    - 验证者忠诚性假设 根据交互式证明系统完备性得到
- 上帝也不能欺骗 交互式证明系统的可靠性 p11
  - 交互式证明系统定义 安全性证明
    - 可靠性
    - 完备性
  - 验证者能力可以很弱 证明者能力无限大
- 基于二次剩余问题的证明系统 p19
- 零知识证明 p23

第三节 数据完整性验证

- 完整性验证概述 p3
  - 完整性 消息没有被改变
  - 验证块和数据块关系
  - 消息认证函数是单向函数
  - 完整性认证的数学基础
    - hash函数
    - 单向置换
- 基于加密算法的消息认证 (被淘汰 反面教材) p9
  - 加密与认证的关系
- 基于hash函数的消息认证 p14
  - Hash函数 p14
    - hash函数概念
      - 是 压缩函数
      - 安全要求
        - 单向性
        - 弱碰撞
        - 强碰撞
  - hash函数构造 p22
  - MD5/SHA1 p26
  - 基于困难问题的hash构造 p36
    - SqHash
  - 长数据的hash处理 p42
    - 压缩函数
- 基于MAC的消息认证 p47
  - 定义 消息认证码 MAC
    - 带密钥的hash函数 HMAC
      - 信息头尾均用用密钥封锁

- 数据完整性的盲验证概述 p57
    - 本质是交互式证明系统

第四节 数字签名技术

- 概述 p3
    - 功能：消息来源认证
    - 单向陷门函数概念
- 数字签名方案 p13
    - RSA
    - ElGamal
    - DSA
    - DSS
- 基于身份的签名 p25
- 盲签名 p29
- 数据的盲认证 p38
- 代理签名 p46
    - ElGamal
    - K-P-W
    - 其他

第五节 身份认证技术

- 概述 p3
    - P向V证明身份的过程
    - 信任根
        - 不能直接传送 避免重放攻击
    - 采用时变参数
- 基于密钥中心的认证协议 p12
- 零知识证明技术 p21
- KERBEROS认证系统 p36
- OAUTH认证协议 p51

Important

- 加密 数据接收者身份认证
- 签名 数据来源认证
- 公钥密码体系
- 陷门函数
    - 无密钥时 单向函数
    - 有密钥时 容易求逆 非单向函数