Recap

Jiageng Chen

2021.12

Symmetric Cryptography

- Blockcipher (PRF, PRP)
  - Operation mode: CBC, CTR,
- Stream cipher (PRG)
- From PRG to PRF (PRF to PRG)
- CPA encryption
  - Security model
  - Hybrid construction
- Cryptographic hash function
  - Birthday bound
- Message authentication code (MAC)
  - Application scenario
  - Security model
- Authenticated Encryption
  - AE model, CCA model
  - Construction

Math

- Group
- gcd to solve inversion
- Fermat’ s theorem
- Quadratic residue
  - Modula prime
  - Modula composite
  - Solution under p=3 mod 4
- Hard problems
  - DL, CDH, DDH, BDH
- Elliptic curve
  - Point addition, scalar multiplication(kP)
- Bilinear Pairing
  - Properties
  - Hard problems on pairing

Public key encryption

- Security Model
  - One-way trapdoor function
  - CPA, CCA
  - Random oracle model
- Schemes
  - RSA
    - Textbook version
    - Hybrid version
  - Elgamal
    - Traditional version
    - Modern view
  - Rabin encryption
    - Apply Chinese Remainder theorem to decrypt
  - ID-based encryption

Signature schemes

- Security model
  - Chosen message attack
- Schemes
  - RSA-FDH
  - BLS
- Security proofs