Cryptography

Lecture 14 – Exam Review

Arkady Yerukhimovich

October 14, 2024

Outline

1. General Concepts

2. Perfect Encryption

3. Private-Key Crypto
   - Building Blocks
   - Encryption
   - Authentication

Security Definitions

- Game-based security definitions
  - How they capture adversary capabilities
  - What it means for $\mathcal{A}$ to win
  - The use of oracles in the definitions
  - Be able to write a definition given an adversary description

Security Definitions

- Game-based security definitions
    - How they capture adversary capabilities
    - What it means for $\mathcal{A}$ to win
    - The use of oracles in the definitions
    - Be able to write a definition given an adversary description
- Understand difference between “indistinguishability” and “unforgeability” style definitions

Security Definitions

- Game-based security definitions
  - How they capture adversary capabilities
  - What it means for $\mathcal{A}$ to win
  - The use of oracles in the definitions
  - Be able to write a definition given an adversary description
- Understand difference between “indistinguishability” and “unforgeability” style definitions
- Relationships between definitions (e.g., CCA is strengthening of CPA)

Proofs by Reduction

- Understand proof structure and what it implies
  - Assume existence of adversary $\mathcal{A}_c$ vs. construction
  - Show this implies existence of adversary $\mathcal{A}_r$ vs. assumption
    - Step 1: Build such an $\mathcal{A}_r$
    - Step 2: Show that $\mathcal{A}_r$ wins his security game

Proofs by Reduction

- Understand proof structure and what it implies
  - Assume existence of adversary $\mathcal{A}_c$ vs. construction
  - Show this implies existence of adversary $\mathcal{A}_r$ vs. assumption
    - Step 1: Build such an $\mathcal{A}_r$
    - Step 2: Show that $\mathcal{A}_r$ wins his security game
- Be able to give proof for simple examples

Proofs by Reduction

- Understand proof structure and what it implies
  - Assume existence of adversary $\mathcal{A}_c$ vs. construction
  - Show this implies existence of adversary $\mathcal{A}_r$ vs. assumption
    - Step 1: Build such an $\mathcal{A}_r$
    - Step 2: Show that $\mathcal{A}_r$ wins his security game
- Be able to give proof for simple examples
- Remember common techniques
  - $\mathcal{A}_r$ simulates the challenger for $\mathcal{A}_c$
  - Replace output of PRG with random string
  - Replace PRF with random function

Proofs by Reduction

- Understand proof structure and what it implies
    - Assume existence of adversary $\mathcal{A}_c$ vs. construction
    - Show this implies existence of adversary $\mathcal{A}_r$ vs. assumption
        - Step 1: Build such an $\mathcal{A}_r$
        - Step 2: Show that $\mathcal{A}_r$ wins his security game
- Be able to give proof for simple examples
- Remember common techniques
    - $\mathcal{A}_r$ simulates the challenger for $\mathcal{A}_c$
    - Replace output of PRG with random string
    - Replace PRF with random function
- Note: Not enough to just draw picture of reduction, have to explain why it works.

Outline

1. General Concepts
2. Perfect Encryption
3. Private-Key Crypto
   - Building Blocks
   - Encryption
   - Authentication

One-Time Pad

- Construction
- Security definition
- Limitations
  - One-time use
  - Key as long as message
  - Be able to argue why these are inherent

Outline

1 General Concepts

2 Perfect Encryption

3 Private-Key Crypto

- Building Blocks
- Encryption
- Authentication

PRGs

- Security definition
  - Length extension
  - Pseudorandomness – as a game
- Be able to argue whether simple constructions are or aren't necessarily PRGs

PRFs

- Security definition
  - Recall what we mean by random function – what is the distribution
  - Indistinguishability from a random function – as a game
  - Oracle notation
- Syntax – distinguish between key and input

Private-Key Encryption

- Definitions
  - Security vs. eavesdropper
  - CPA
  - CCA
  - Authenticated encryption

Private-Key Encryption

- Definitions
  - Security vs. eavesdropper
  - CPA
  - CCA
  - Authenticated encryption
- Constructions
  - PRG + OTP – what this achieves and limitations
  - PRF + OTP – what this achieves and limitations
- Proofs of security – remember basic proof structure

Private-Key Encryption

- Definitions
  - Security vs. eavesdropper
  - CPA
  - CCA
  - Authenticated encryption
- Constructions
  - PRG + OTP – what this achieves and limitations
  - PRF + OTP – what this achieves and limitations
- Proofs of security – remember basic proof structure
- Modes of operations
  - Why we need modes of operations
  - Constructions and key properties (CBC, CTR)
  - Padding oracle attack – why this breaks CCA security

MACs

- Goals and why this is important
- Security definition
- Construction based on PRF

MACs

- Goals and why this is important
- Security definition
- Construction based on PRF
- Domain extension
    - General using only MAC
    - Hash-and-MAC

MACs

- Goals and why this is important
- Security definition
- Construction based on PRF
- Domain extension
  - General using only MAC
  - Hash-and-MAC
- Using MACs to build authenticated encryption
  - Encrypt and authenticate
  - Authenticate then encrypt
  - Encrypt then authenticate

Hash Functions

- What is a CRHF, how it differs from a PRF
- Security definition

Hash Functions

- What is a CRHF, how it differs from a PRF
- Security definition
- Applications
  - Passwords
  - Identifiers
  - Hash-and-MAC

Hash Functions

- What is a CRHF, how it differs from a PRF
- Security definition
- Applications
    - Passwords
    - Identifiers
    - Hash-and-MAC
- Domain extension

Exam Procedures

- Exam on Wed., Oct. 16, 12:45-2:00 PM in the classroom
- You may bring 2 pieces of 8.5 x 11 inch paper (back and front) with notes
- No computers, phones, or calculators during exam – bring pens or pencils

Exam format

The exam will contain the following:

1. 10 True/False questions – no partial credit
2. 2-3 long answer questions – definitions, reductions, PRG/PRF, Encryption, MACs, Hash functions
3. 1 challenge problem
4. Questions may have multiple parts, complete as much as you can.