31. Data Privacy

- 为什么需要data privacy(P2)
- **the target of data privacy system:** Allow data **to be used**, and **protect it from being stolen**
- **Common Attacks(P5)**

Basic data privacy method

ZERO-KNOWLEDGE PROOF

- background(P9-10)
- **Interactive Zero-Knowledge Proof framework (P12)**
- **Scenario: Graph Isomorphism(P13-15)**

PIR: Private Information Retrieval

- background(P17)
- overview(P18)
- Information-Theoretic PIR(P19)
  - example: **2-Server PIR(P24)**
- Computational PIR

OT: Oblivious Transfer

- background(P27)
- overview(P28)
- example: **1-out-of-2 OT(P29-30)**

DP: Differential privacy

- background(P35)

- overview(P36)
- **Properties of Differential privacy(P37)** 不是很清楚
- **How to Implement a DP Algorithm（P38）**

SECRET SHARING

- Key Idea（P41）
- **Creation and Reconstruction(P42-44)**
- **Pros and Cons(P45)**

SECURE MPC: Multi-Party Computing

- background(P47)
- example: **Millionaire Problem(P48)**
- notice（P49）
  - **Garbled Circuits（P50）**
  - **Different sMPC Protocols（P52）**

HOMOMORPHIC ENCRYPTION

- background(P55)
- overview(P56)
- **SWHE and FHE(P57)**

HARDWARE ENCLAVE