ALPTEKİN KÜPÇÜ

Assistant Professor of Computer Science and Engineering

KOÇ
UNIVERSITY

Two Main Types of Cloud

- Outsource a job to a more powerful entity
  - Outsourcing computation to Amazon EC2
  - Outsourcing storage to Google Drive
  - Outsourcing file distribution to Rapidshare

- Outsource a job to multiple entities
  - Outsourcing computation to regular users as in SETI@Home
  - Outsourcing storage to peers as in P2P storage system Wuala
  - Outsourcing music distribution to peers as in P2P file sharing system Napster

- In both cases:
  - No service/security guarantees
  - Resources not under your control
  - Untrusted setting

Outsourced Computation

- Amazon EC2
  - Homomorphic Encryption
    - Slow, active research funding for faster versions
- Amazon and Microsoft and Google
  - Secure Multi-Party Computation
  - Secret Sharing
  - (Zero-Knowledge) Proofs
- SETI@Home
  - Crypto, Game Theory and Mechanism Design
    - Very fast (about 0.1% overhead)
    - Security guarantee (i.e. high correctness and low waste)

Authentication

- Password-based Authentication
  - Secure against Dictionary Attacks
  - Minimal change on client/server
  - Usability consideration
  - Privacy-friendly
- Electronic IDs and Passports
  - Anonymous Credentials
  - Zero-Knowledge Proofs
  - Privacy-friendly e-cash for transportation
  - Privacy-preserving surveillance

Collaboration Areas

- **Outsourced Databases**
  - Privacy of data and query
  - (Anonymous) access control
  - Integrity
- **Electronic Health**
  - Privacy-preserving Information Sharing
  - Biometric Encryption
- **Peer-to-Peer Systems**
  - Streaming
  - Economics
- **Theoretical Limits**
  - Distributing Trust
  - Efficiency vs. Privacy

ALPTEKİN KÜPÇÜ

Assistant Professor of Computer Science and Engineering

http://crypto.ku.edu.tr

KOÇ UNIVERSITY