CSE208: Advanced Cryptography

Daniele Micciancio

UCSD

Fall 2020

Section 1

Introduction

CSE208: Advanced Cryptography

- Graduate Level Advanced Cryptography
- Prerequisites:
  - CSE207 or equivalent
  - Solid theoretical background, cryptographic definitions, etc.
  - Some programming

CSE208: Advanced Cryptography

- Graduate Level Advanced Cryptography
- Prerequisites:
  - CSE207 or equivalent
  - Solid theoretical background, cryptographic definitions, etc.
  - Some programming
- Past topics: Zero Knowledge, Functional Encryption, Secure Computation, etc.
- Not required: CSE206A (Lattice Algorithms)

CSE208: Advanced Cryptography

- Graduate Level Advanced Cryptography
- Prerequisites:
  - CSE207 or equivalent
  - Solid theoretical background, cryptographic definitions, etc.
  - Some programming
- Past topics: Zero Knowledge, Functional Encryption, Secure Computation, etc.
- Not required: CSE206A (Lattice Algorithms)
- Reading:
  - no textbook
  - mostly research papers
  - see course webpage, canvas, etc.

Fall 2020 Topic

- Fully Homomorphic Encryption:
  - Encryption schemes that supports the evaluation of arbitrary programs on encrypted inputs
- Applications:
  - secure outsourced computing
  - building block for MPC and more

Brief History of Homomorphic Encryption

- 1978: Rivest, Adleman & Dertouzos posed the problem
- 2009: Gentry 2009 proposed the first candidate solution
- 2010-2020: Work towards more efficient solutions based on standard complexity assumptions (Brakerski, Vaikuntanathan, Gentry, Halevi, Smart, ...)

Software libraries

- IBM HElib (Halevi & Shoup)
- Microsoft SEAL
- NJIT/Duality PALISADE (Rohloff, Cousins & Polyakov)
- Functional Lattice Cryptography LoL (Crockett & Peikert)
- Fastest FHE of the West FHEW (Ducas & Micciancio)
- FHE over the Torus TFHE (Chillotti, Gama, Georgieva & Izabachene)
- Approximate FHE HEAAN (Cheon, Kim, Kim & Song)

Software libraries

- IBM HElib (Halevi & Shoup)
- Microsoft SEAL
- NJIT/Duality PALISADE (Rohloff, Cousins & Polyakov)
- Functional Lattice Cryptography LoL (Crockett & Peikert)
- Fastest FHE of the West FHEW (Ducas & Micciancio)
- FHE over the Torus TFHE (Chillotti, Gama, Georgieva & Izabachene)
- Approximate FHE HEAAN (Cheon, Kim, Kim & Song)

- In the News:
  - February 21, 2019: Microsoft SEAL open source homomorphic encryption library gets even better for .NET developers!
  - June 4, 2020: IBM releases FHE toolkit for MacOS and iOS; Linux and Android Coming Soon

Homework and Evaluation

- Homework assignments:
  - 3 assignments, due within one week from assignment date
  - Cover theoretical/mathematical topics

Homework and Evaluation

- Homework assignments:
  - 3 assignments, due within one week from assignment date
  - Cover theoretical/mathematical topics
- Small Project:
  - Goal: Try to use one of the many HE libraries
  - Not much coding, but you will have to write and compile a few lines of code
  - Evaluated primarily based on written report

Administrivia:

- Course webpage: http://cseweb.ucsd.edu/classes/fa20/
  - general course information
  - pointers to papers and other reading material
- Canvas:
  - recording of lectures
  - homework distribution/collection
  - grades
  - discussion board

Course Schedule (Tentative)

Week 1: Introduction and Definition

- FHE Definition
- Gentry's Boostrapping theorem
- Homework 1 out

Week 2-4: Fundamental techniques based on general lattices

- LWE encryption
- Linear Homomorphic computations
- Key Switching and Proxy re-encryption
- Nested encryption and homomorphic multiplication
- Ciphertext Tensoring and homomorphic multiplication
- Homomorphic Decryption and Bootstrapping algorithms
- Homework 2 out

Week 5: Algebraic Number Theory

- I really hope you like math!
- Homework 3 out

Week 6-10: Efficient FHE from Ring LWE

- Message packing techniques
- Linear transformations on structured matrices
- Other FHE schemes: GHS, BFV,FHEW, AP13, TFHE, CKKS ...