CSE208: Advanced Cryptography (FHE)

Daniele Micciancio

UCSD

Fall 2023

Section 1

Introduction

CSE208: (Graduate) Advanced Cryptography

- Instructor: Daniele Micciancio
- TA: Yizhao Zhang
- Prerequisites:
  - CSE207 or equivalent (modern cryptography):
    - security definitions (e.g., IND-CPA)
    - security proofs by reduction, "hybrid arguments", etc.
    - algorithms, probability, etc.
  - Some programming (C/C++)
  - Not required: CSE206A (Lattice Algorithms)
- Reading:
  - no textbook, only research papers
  - slides/notes on course webpage
  - blackboard / your own notes

Topic: Cryptography + Computation

- Past topics: Zero Knowledge, Functional Encryption, Secure Computation, etc.
- This quarter: **Fully Homomorphic Encryption (FHE)**
  - Encryption schemes that supports the evaluation of arbitrary programs on encrypted inputs
- Applications:
  - secure outsourced computing
  - building block for MPC and more
- See Eurocrypt 2019 invited talk "FHE from the ground up" slides 1-10

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

- OpenFHE
- IBM HElib (Halevi & Shoup)
- Microsoft SEAL
- 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)
- . . . many more

Press releases, magazine articles, interviews, etc.

- Microsoft SEAL open source homomorphic encryption library gets even better for .NET developers!
- Fully Homomorphic Encryption on IBM Cloud Hyper Protect Virtual Servers
- The next step in homomorphic encryption for Linux on IBM Z and LinuxONE
- Unlocking the Potential of Fully Homomorphic Encryption
- Is Fully Homomorphic Encryption now a reality?
- Fully homomorphic encryption revolutionises healthcare data privacy and innovation
- Just search for it

Homework and Evaluation

- Homework assignments:
  - ∼5 assignments, due within one week from assignment date
  - Cover theoretical/mathematical topics, definitions, notation
  - submitted on gradescope
  - HW1 will go out by Tuesday Oct 3 (due Oct 10)

Homework and Evaluation

- Homework assignments:
  - ~5 assignments, due within one week from assignment date
  - Cover theoretical/mathematical topics, definitions, notation
  - submitted on gradescope
  - HW1 will go out by Tuesday Oct 3 (due Oct 10)
- Project:
  - Goal: get your hands dirty using one of the many available HE libraries
  - Minimal requirement: not much coding, but enough to demonstrate ability to make use of the library
  - Open ended: do something you like / find interesting
  - Evaluated primarily based on written report

Administrivia:

- Course webpage: http://cseweb.ucsd.edu/classes/fa23/
  - probably not there yet, will post before next class
  - general course information, office hour, etc.
  - pointers to papers and other reading material
  - homework assignments
- Teamwork:
  - You can work in groups of size up to three both for HW and Project
  - Goal is to learn from each other, not to split the work
  - Working in teams is encouraged

Course Schedule

This is very tentative and subject to change

Week 1: Introduction and Definition

- FHE Definition
- Gentry's Boostrapping theorem

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

Week 5: Algebraic Number Theory

- I really hope you like math!

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 ...