CSE 5359

Fully Homomorphic Encryption

Ten H. Lai

Autumn 2013

- Instructor: Steve Lai
  - Office: DL 581
  - Office hours: TR 3:30-4:30 p.m.
  - Email: lai@cse.ohio-state.edu
  - Home page: www.cse.ohio-state.edu/~lai

- Prerequisite: CSE 5351/723 or any introductory encryption course; or CSE 5473/651 (network security).

Topics

- Graig Gentry, “Fully Homomorphic Encryption Using Ideal Lattices,” STOC 2009. PDF
- Brakerski and Vaikuntanathan, “Efficient Fully Homomorphic Encryption from (Standard) LWE,” FOCS 2011.
- Gentry, Sahai,Waters, “Homomorphic Encryption from Learning with Errors,” CRYPTO 2013.
- Other related papers.

Grading plan (tentative)

- Class attendance (30%)
  - Please be in class on time!
- Midterm exam (30%)
- Slides and presentation or final exam (40%)

- You may choose to not count attendance.
- You may also choose to do a project and/or write a term paper instead of taking exams.