CSE 5852: Problem Set 10

Due: December 9, 2016

You have two options for this assignment. The first involves summarizing a talk the second involves summarizing a paper. Clearly indicate which option you are using on your submission.

1 Talk Option

Ran Canetti is giving the CSE colloquium at 12:15 on December 2 in ITE 336. Do the following:

1. Attend his talk.
2. Ask a technical question during his presentation.
3. Write a one-page summary of the talk. Be clear what you understood and what you don't understand.

2 Paper Option

Read Boaz Barak's recent paper "Hopes, fears, and software obfuscation." The paper is available at: http://www.boazbarak.org/Papers/obfuscation-preprint.pdf. Provide a one-page summary of the paper in your own words. Feel free to skip some of the underlying mathematics, instead focus on the properties of the different cryptographic objects. Include answers to the following questions:

1. What is cryptographic obfuscation?
2. What was proved in 2001?
3. What was the recent breakthrough in 2013?
4. What is fully-homomorphic encryption? How does it differ than obfuscation?