0368-4499: Seminar in cryptographic protocols

Spring 2015

Instructor: Ran Canetti. Office Hours: please coordinate. Email: canetti@tau.ac.il

Official time: Thursdays 11:00am - 1pm. However, the time seems to be inconvenient for several of the students so we will try to find a more convenient time at the first meeting. If you want to take the course but cannot make it to the first meeting, please contact Ran by email ahead of time.

Prerequisites: The graduate cryptography course (0368-4162) or equivalent knowledge in theoretical cryptography (primitives, constructions, and proof methods).

Syllabus: The seminar will cover basic works in cryptographic protocols, functional encryption and program obfuscation. The goal is to entice the students' curiosity to go deeper, and prepare them to do research in cryptography.

Requirements: Students will be required to prepare and give a presentation on a paper of choice (either from the list below or by agreement with instructor). Preparing a presentation involves presenting it to instructor ahead of time and working together to polish it. In addition problem sets may be given.

Lecture Topics: Below is a list of lecture topics for students to pick from. The lectures to be given and their order will be decided in the first two meetings, based on the makeup of the class and the preferences of the students. The order will mostly be the one shown. (Obviously only a subset of the topics will be covered in class.)

In much of the list below only the original papers are mentioned. Often the covered material has better or alternative descriptions in later papers. There may also be presentation materials available online. You are encouraged to use all of these to improve your understanding and your

presentation – please consult with Instructor.

Composition and round complexity of Zero-Knowledge protocols

- On the Composition of Zero-Knowledge Proof Systems
  Oded Goldreich, Hugo Krawczyk, SIAM Journal on Computing

- How to Construct Constant-Round Zero-Knowledge Proof Systems for NP
  O. Goldreich and A. Kahan,
  A note on constant-round zero-knowledge proofs for NP
  Alon Rosen, TCC 2004

- How to Go Beyond the Black-Box Simulation Barrier
  Boaz Barak
  FOCS 2001 106-115

- Concurrent Zero-Knowledge. Rosen, Alon, plus overview of later results.

Non-Interactive Zero Knowledge and CCA-secure encryption

- Multiple Non-Interactive Zero Knowledge Proofs Under General Assumptions.
  Uriel Feige, Dror Lapidot, Adi Shamir
  SIAM J. Comput. 29(1): 1-28 (1999)IZK: FLS
- Y. Lindell. A Simpler Construction of CCA2-Secure Public-Key Encryption Under General Assumptions. In the Journal of Cryptology, 19(3):359-377, 2006.

Non-malleable commitments

- Danny Dolev, Cynthia Dwork, Moni Naor:
  Nonmalleable Cryptography. SIAM J. Comput. 30(2): 391-437 (2000)

Multi-party computation and Universally Composable security

- A Proof of Yao's Protocol for Secure Two-Party Computation. Yehuda Lindell, Benny Pinkas: IACR Cryptology ePrint Archive 2004: 175 (2004)
- Universally Composable Security: A New Paradigm for Cryptographic Protocols
  Ran Canetti
  Cryptology ePrint Archive: Report 2000/067
- Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation
  Michael Ben-Or Shafi Goldwasser Avi Wigderson
  STOC 1988
- Universally Composable Commitments.
  R. Canetti and M. Fischlin. Crypto, 2001. Long version at eprint.iacr.org/2001/055.
- Universally composable two-party and multi-party secure computation.
  R. Canetti, Y. Lindell, R. Ostrovsky, A. Sahai.
  34th STOC, 2002. Longer version at eprint.iacr.org/2002/140.

Program Obfuscation

- On the (Im)possibility of Obfuscating Programs
  Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan and Ke Yang
  Crypto 2001
  http://www.math.ias.edu/~boaz/Papers/obfuscate.ps

- Towards realizing random oracles: Hash functions that hide all partial information.
  R. Canetti. Crypto, 1997. Longer version available at eprint.iacr.org/1997/007 .
  (look in MAyank Varia's PhD thesis and Nir Bitansky's MSc thesis)

- Boaz Barak, Sanjam Garg, Yael Tauman Kalai, Omer Paneth, Amit Sahai:
  Protecting Obfuscation against Algebraic Attacks. EUROCRYPT 2014: 221-238

- Candidate Multilinear Maps from Ideal Lattices
  Sanjam Garg and Craig Gentry and Shai Halevi
  http://eprint.iacr.org/2012/610

- Obfuscating Circuits via Composite-Order Graded Encoding
  Benny Applebaum and Zvika Brakerski

- How to Use Indistinguishability Obfuscation: Deniable Encryption, and More
  Amit Sahai and Brent Waters
  http://eprint.iacr.org/2013/454