COMS W6261: Advanced Cryptography: Minimalist Cryptography
Instructor: Tal Malkin

Readings for Secure Computation (last updated 4/2/16)

Secure computation has been an active area of research since the 80s, and still is going strong, with many new ideas, techniques, and applications (as well as models, definitions, and proofs). We have only touched on the topic (see the class webpage for a summary for what we covered). Here I give some pointers for reading related to what we have already covered, and a small sample of papers in other directions beyond what we covered.

Note: most papers are linked via a hyperlink below.

General reading corresponding to class

- Goldreich's volume II chapter 7 (general cryptographic protocols). The presentation is a bit different from ours (e.g., different order), and certainly much more rigorous, including proofs.
- shelat-Pass on-line textbook chapter 6 includes some coverage of secret sharing, Yao's garbled circuit evaluation, and oblivious transfer.
- Lindell and Pinkas "A Proof of Security of Yao's Protocol for Two-Party Computation" (available here).
- Belalre, Hoang, Rogaway, "Foundations of Garbled Circuits" (available here). In upcoming classes we will see a different formalization of this primitive via randomized encodings.
- Cramer-Damgard-Nielsen have a recent textbook focusing on secret sharing and secure computation in the information-theoretic setting

Examples for further reading The following are selected based on things that were mentioned in class in passing (sometimes in response to student questions). They are not meant to be exhaustive in any way (I made an effort to keep the number of such papers small - let me know if you want more reading references!)

- Some Oblivious Transfer papers:
  - Peikert, Vaikuntanathan, Waters 08. Proved in the UC model; the instantiation based on DDH is one of the most efficient malicious-secure OT, that is used in some implementations.
  - Choi, Dachman-Soled, Malkin, Wee 08. malicious OT from semi-honest OT in a black box way, in the adaptive setting (also UC).
  - Oblivious Transfer is complete: in the static model, see the classic paper (STOC 88) by Kilian Founding Cryptography on Oblivious Transfer. Twenty years later (Crypto 08), Ishai, Prabhakaran and Sahai showed this for the adaptive model (along with other results).

- Some other approaches to achieving malicious security:
  - Cut-and-choose for malicious security with Yao's garbled circuits: See Lindell-Pinkas 11 and Lindell 13.
  - Ishai, Prabhakaran, Sahai 08 combine information-theoretic solutions for honest-majority case together with semi-honest but no honest-majority protocols to obtain malicious and no honest majority solutions.

There are also various survey talks on secure computation (e.g., Simons's crypto semeseter and BIU winter schools, linked from the class webpage under reading and on the projects page). In particular, for the 2015 winter school on secure computation with a practical focus, see `http://crypto.biu.ac.il/5th-biu-winter-school`.