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

Homework 3

1. **(Required:)** Read the following paper (available here): A Proof of Security of Yao's Protocol for Two-Party Computation. Yehuda Lindell and Benny Pinkas. Journal of Cryptology, 2009.
2. **(Recommended:)** Read Oded Goldreich's Foundations of Cryptography Volume II: section 7.4 (Forcing two-party semi-honest behavior).
3. For optional further reading, check out some suggestions here.

Due date:

- by Tue 4/5 (before class): Read at least the introduction of the Lindell-Pinkas paper.
- by Tue 4/12: complete the reading.