0368.4162 Foundations of Cryptography January 2, 2019

Problem Set 5

Due: January 16

Instructions:

- Type your solution and email it to "focf19hw@gmail.com", with subject "HW#, ID#, Name".
- You're encouraged to use latex. You can find on the webpage the assignment's tex file to help you.
- You can cooperate. However, you should write the solution by yourself, and list all collaborators for each question. Same goes for any external sources that you may use.
- Do not discuss solutions over the course's forum. You are more than welcome though to ask for clarifications regarding the questions themselves.

1. Consider the GMW zero-knowledge proof system for 3COL when repeated sequentially $t = n \cdot |E|$ times. Let $G = (U, E)$ be a graph and let P^* be a (w.l.o.g deterministic) prover that manages the convince the verifier V of accepting with probability $n^{-O(1)}$.

   We will prove that we can efficiently extract a legal 3-coloring of G given oracle access to P^*. Here oracle access means that we can *rewind* P^*. Formally, we are given access to *the next message function of* P^* that given a transcript of all prover-verifier messages up to some point, generates the next prover message. In particular, any partial interaction in the first $i-1$ rounds, can be continued in different ways, by having the extractor choose different verifier messages as the $i+1$st message.

   Consider the random process of running t interactions with the prover (where at each one the verifier sends a random message). For $i \in [t]$, let p_i be a random variable that is the probability, over V's coins, that V accepts in the ith interaction, conditioned on the first $i-1$ interactions (this random variable becomes fixed once we fix the first $i-1$ interactions). Let G_i be the event that $p_i > 1 - \frac{1}{|E|}$.

   (a) (15 pts) Prove that the probability that in t interactions the prover convinces the verifier of accepting, but non of the events $G_1, \ldots, G_t$ occurred is bounded by $2^{-\Omega(n)}$.

   (b) (10 pts) Deduce that in t interactions the probability that for some i, the event G_i occurs is $n^{-O(1)}$.

   (c) (15 pts) Prove the existence of the required extractor.

2. Consider an auction with a seller party S and three participants A, B, C with inputs $a, b, c \in [2^n]$ representing they're bids. They run an MPC protocol (against malicious parties) for the function that gives S the identity and the bid of the highest bidder. Assume that b and c are chosen at random.

   (a) (15 pts) Prove that the probability that a corrupted A^* outputs b is negligible.

   (b) (15 pts) Prove that the probability that a corrupted A^* wins with bid $1 + \max\{b, c\}$ is negligible.

3. In the following question, addition and multiplication are done modulo 2.

   (a) (15 pts) Consider the following m-party randomized function mapping m pairs of bits to m bits:

   $$(a_1, b_1), \ldots, (a_m, b_m) \longmapsto c_1, \ldots, c_m \ ,$$

   where $c_1, \ldots, c_m$ are uniform in $\{0,1\}^m$ subject to $\sum_{i\in[m]} c_i = \left(\sum_{i\in[m]} a_i\right) \times \left(\sum_{i\in[m]} b_i\right)$. Describe a semi-honest protocol for computing the above function, assuming a semi-honest protocol for any two-party function.

   (b) (15 pts) Use the fact that $\{+, \times\}$ is a universal set of Boolean gates to describe a semi-honest protocol for any deterministic m-party function.

4. (**Bonus** 10 pts) Show that any two-message $(1, 2)$-OT (that is semi-honestly secure) implies public-key encryption.