Homework 4

Deadline: 11:59pm, Nov 19, 2017

1. (15 points) Given *any* 1-out-of-2 oblivious transfer (OT) protocol, construct a 1-out-of-4 OT protocol. (Note: It is not ok to show that a specific 1-out-of-2 protocol, e.g., the one we saw in class, implies 1-out-of-4 OT)

2. Let L be an NP language with witness relation R such that every statement $x \in L$ has at least two different witnesses. A non-interactive proof system (K, P, V) for language L is called **witness indistinguishable** if for any triplet (x, w_0, w_1) s.t. $R(x, w_0) = 1$ and $R(x, w_1) = 1$, the distributions $\{\sigma, P(\sigma, x, w_0)\}$ and $\{\sigma, P(\sigma, x, w_1)\}$ are computationally indistinguishable, where $\sigma \leftarrow K(1^n)$.

   (a) (5 points) Prove that any NIZK proof system is also a non-interactive witness indistinguishable (NIWI) proof system. (Hint: Earlier in the class, we proved that semantically secure encryption implies IND-CPA encryption. Use a similar idea here.)

   (b) (5 points) The definition of NIWI above only considers a single statement. Prove that witness indistinguishability property *composes*, i.e., if (K, P, V) satisfies the above definition, then it also satisfies the following: for any polynomial $q(\cdot)$ and triplets $\{(x_i, w_i^0, w_i^1)\}_{i \in q}$ s.t. $R(x_i, w_i^0) = 1$ and $R(x_i, w_i^1) = 1$, the distributions

   $$\left\{\sigma, \left\{P(\sigma, x_i, w_i^0)\right\}_{i \in q}\right\} \text{ and } \left\{\sigma, \left\{P(\sigma, x_i, w_i^1)\right\}_{i \in q}\right\}$$

   are computationally indistinguishable, where $\sigma \leftarrow K(1^n)$.

(c) (15 points) Recall that the NIZK proof system we constructed in class required a fresh common random string (CRS) for each statement proved. However, we want to reuse the same random string to prove *multiple* statements while still preserving the zero-knowledge property.

So we define a new NIZK proof system with stronger zero knowledge property called the multi-statement NIZK proof system as follows (this definition also captures adaptive zero-knowledge property).

A NIZK proof system (K, P, V) for a language L with corresponding relation R is a *multi-statement NIZK proof system* if there exists a PPT machine $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ such that for all PPT machines $\mathcal{A}_1$ and $\mathcal{A}_2$ we have that

$$\left| \Pr\left[\begin{array}{r} \sigma \leftarrow K(1^n) \\ (\{x_i, w_i\}_{i\in[q]}, \texttt{st}) \leftarrow \mathcal{A}_1(\sigma) \\ \text{s.t. } \forall i \in [q], R(x_i, w_i) = 1 \\ \forall i \in [q], \pi_i \leftarrow P(\sigma, x_i, w_i) \\ \mathcal{A}_2(\texttt{st}, \{\pi_i\}_{i\in[q]}) = 1 \end{array} \right] - \Pr\left[\begin{array}{r} (\sigma, \tau) \leftarrow \mathcal{S}_1(1^n) \\ (\{x_i, w_i\}_{i\in[q]}, \texttt{st}) \leftarrow \mathcal{A}_1(\sigma) \\ \text{s.t. } \forall i \in [q], R(x_i, w_i) = 1 \\ \forall i \in [q], \pi_i \leftarrow \mathcal{S}_2(\sigma, x_i, \tau) \\ \mathcal{A}_2(\texttt{st}, \{\pi_i\}_{i\in[q]}) = 1 \end{array} \right] \right| \leq \texttt{negl}(n)$$

Prove that given a single statement NIZK proof system (K, P, V) for NP, the following construction is a multi-statement NIZK proof system (K', P', V') for NP:

Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a length-doubling PRG:

- K', on input the security parameter, computes $\sigma \leftarrow K(1^n)$ along with a random string y of length $2n$ and outputs $\sigma' = (\sigma, y)$.
- P' on input (σ', x, w) proves (using P) that there exists a pair (w, s) such that $R(x, w) = 1 \vee y = G(s)$ where s is a seed for the PRG G.
- V', on input (σ', x, π) outputs $V(\sigma', x, \pi)$.