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 $\{(x_i, w^0_i, w^1_i)\}_{i \in q}$ s.t. $R(x_i, w^0_i) = 1$ and $R(x_i, w^1_i) = 1$, the distributions $\{\sigma, \{P(\sigma, x_i, w^0_i)\}_{i \in q}\}$ and $\{\sigma, \{P(\sigma, x_i, w^1_i)\}_{i \in q}\}$ are computationally indistinguishable, where $\sigma \leftarrow K(1^n)$. 

1
(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 $S = (S_1, S_2)$ such that for all PPT machines $A_1$ and $A_2$ we have that

$$\Pr\left[\begin{array}{l}
\sigma \leftarrow K(1^n) \\
\{x_i, w_i\}_{i \in [q]}, \text{st} \leftarrow A_1(\sigma) \\
s.t. \forall i \in [q], R(x_i, w_i) = 1 \\
\forall i \in [q], \pi_i \leftarrow P(\sigma, x_i, w_i) \\
A_2(\text{st}, \{\pi_i\}_{i \in [q]}) = 1
\end{array}\right] - \Pr\left[\begin{array}{l}
(\sigma, \tau) \leftarrow S_1(1^n) \\
\{x_i, w_i\}_{i \in [q]}, \text{st} \leftarrow A_1(\sigma) \\
s.t. \forall i \in [q], R(x_i, w_i) = 1 \\
\forall i \in [q], \pi_i \leftarrow S_2(\sigma, x_i, \tau) \\
A_2(\text{st}, \{\pi_i\}_{i \in [q]}) = 1
\end{array}\right] \leq \text{negl}(n)$$

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 $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ 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 $(\sigma', x, w)$ proves (using $P$) that there exists a pair $(w, s)$ such that $R(x, w) = 1 \lor y = G(s)$ where $s$ is a seed for the PRG $G$.
- $V'$, on input $(\sigma', x, \pi)$ outputs $V(\sigma', x, \pi)$. 