Cryptography - HW #3
Due: Wednesday 10/29/14

1. **Multi-statement NIZK:** The NIZK proof system we constructed in class required a fresh common random string (CRS) for each statement proved. In various settings we would like to reuse the same random string to prove multiple theorem statements while still preserving the zero-knowledge property.

A multi-statement NIZK proof system \((K,P,V)\) for a language \(L\) with corresponding relation \(R\) is a NIZK proof system for \(L\) with a stronger zero-knowledge property, defined as follows: 

\[\exists \text{ a PPT machine } S = (S_1,S_2) \text{ such that } \forall \text{ PPT machines } A_1 \text{ and } A_2 \text{ we have that:} \]

\[
\begin{align*}
\Pr & \left[ \sigma \leftarrow K(1^\kappa), \right. \\
& \left. \{\{x_i, w_i\}_{i \in [q]}, \text{state} \} \leftarrow A_1(\sigma), \right. \\
& \text{such that } \forall i \in [q], (x_i, w_i) \in R \right] - \Pr \left[ \sigma \leftarrow S_1(1^\kappa), \right. \\
& \left. \{\{x_i, w_i\}_{i \in [q]}, \text{state} \} \leftarrow A_1(\sigma), \right. \\
& \text{such that } \forall i \in [q], (x_i, w_i) \in R \right] \\
\leq & \text{negl}(\kappa) .
\end{align*}
\]

Assuming that a single statement NIZK proof system \((K,P,V)\) for NP exists, construct a multi-statement NIZK proof system \((K',P',V')\) for NP.

**Hint:** Let \(g : \{0,1\}^{\kappa} \rightarrow \{0,1\}^{2\kappa}\) be a length doubling PRG. Let \(K'\) output the output of \(K\) along with \(y\), a random \(2\kappa\) bit string. To prove \(x \in L\) the prover \(P'\) proves that \(\exists (w,s)\) such that either \((x,w) \in R\) or \(y = g(s)\).

2. Prove that a selectively secure identity based encryption scheme implies a digital signature scheme for which no attacker can generate universal forgery under a chosen message attack.