Handout 16: Problem Set 9

Instructor: Anna Lysyanskaya *Teaching Assistant: Moses Liskov*

This problem set is due on Wednesday, December 12. THERE WILL BE NO EXTENSIONS.

Problem 1

(33 points) Recall that in a commitment scheme there are two ITMs, C and R (for committer and receiver), which operate in two stages (they are given an auxillary input, either 'c' or 'r', to indicate which stage they are in at the time). Recall the definition:

Correctness:
$\forall b \in \{0,1\}\ \forall k$
$\Pr[u \leftarrow C(b, 1^k, `c') \leftrightarrow R(1^k, `c') \rightarrow v;$
$\quad C(u, `r') \leftrightarrow R(v, `r') \rightarrow b' : b' = b] = 1$

Hiding:
$\forall \{R'_k\} PPTF\ \exists \nu \in negl\ \forall k$
$\Pr[b \leftarrow \{0,1\}; u \leftarrow C(b, 1^k, `c') \leftrightarrow R'_k(1^k, `c') \rightarrow b' :$
$\quad b = b'] < 1/2 + \nu(k)$

Binding:
$\forall \{C'_k\} PPTF\ \exists \nu \in negl\ \forall k$
$\Pr[u \leftarrow C'_k(1^k, `c') \leftrightarrow R(1^k, `c') \rightarrow v; C'_k(u, 0, `r') \leftrightarrow R(v, `r') \rightarrow b_0;$
$\quad C'_k(u, 1, `r') \leftrightarrow R(v, `r') \rightarrow b_1 : b_0 \neq b_1] < \nu(k)$

Prove that if a commitment scheme exists, then a one-way function exists. Hint: Be careful to remember that in a commitment scheme, the commit stage may take multiple messages.

Problem 2

Consider the following commitment scheme. Suppose there are public parameters p (a prime), and g and h, two generators modulo p, and that these are chosen at random at the start and made available to both parties.

To commit to a bit b, the committer chooses a random r and computes $g^r h^b$, which is sent to the verifier. To open the commitment, the committer reveals r and b.

(a) (11 points) Prove that this is a secure commitment scheme. More precisely, prove that this scheme is correct, that it is hiding unconditionally, and that it is binding if the discrete log problem is hard.

(b) (11 points) If instead the committer generates p, g, and h, is the scheme secure? Prove your answer. If no, is there a way to fix it easily?

(c) (11 points) If instead the receiver generates p, g, and h, is the scheme secure? Prove your answer. If no, is there a way to fix it easily?

Problem 3

Consider the following zero-knowledge protocol for proving that a value a is a quadratic residue modulo n, in which

Input: n and a. Let $\alpha^2 \equiv a \bmod n$ be the square root of a.

1. P chooses a random prime $p = 2q+1$ where q is a random k-bit prime, and a random g or order q, and randomly chooses β and sets $h = g^\beta \bmod p$. P sends p, q, g, h to V.
2. V computes a random string c of length k and a random r, and sends $x = g^r h^c$ to P.
3. P chooses k random values $r_1, \ldots, r_k$ and computes $s_i = r_i^2$ and sends $s_1, \ldots, s_k$ to V.
4. V sends r and c to P.
5. P checks that $x = g^r h^c$. If so, P sends to V, for each i, the value $t_i = r_i \alpha^{c_i}$, where $c = c_1 \circ \ldots \circ c_k$. P also sends β to V
6. V checks that $t_i^2 \equiv s_i a^{c_i}$ for each i, and that $h = g^\beta$. If so, V accepts, otherwise V rejects.

This defines a P, V which you will prove is a zero-knowledge proof system. It should be clear that P, V has completeness 1. The idea of this construction is to simply parallelize the ZKP we presented in class for quadratic residuosity. In order to prove zero-knowledgeness we need to add the commitment x into the protocol, as you will see when proving this.

(a) (17 points) Prove that P, V has negligible soundness (ie, V can only be convinced with negligible probability if a is a quadratic non-residue modulo n).

(b) (17 points) Prove that if the discrete logarithm problem is hard, then P, V is zero-knowledge.