CS355: Topics in cryptography **Fall 2002**

Assignment #2

Due: Wednesday, Dec. 4th, 2002.

Problem 1: (SFE) We are given a generic protocol $\mathcal{P}$ for 2-party Secure Function Evaluation in the honest-but-curious model. For any fixed n, use $\mathcal{P}$ to construct a generic n-party, $(n-1)$-private, Secure Function Evaluation protocol in the honest-but-curious model. Show that your protocol is $(n-1)$-private.
Hint: use recursion.

Problem 2: (ZK) In class we saw Zero-Knowledge protocols for proving that a number is a quadratic residue modulo N and for proving that equality of discrete logarithms. Your goal is to give Zero-Knowledge protocols for the complement languages. Remember to prove soundness, completeness, and zero-knowledge.

- **a.** Give a Zero-Knowledge protocol for the language containing all pairs (N, x) where $x \in \mathbb{Z}_N$ and x is *not* a quadratic residue in $\mathbb{Z}_N$.
- **b.** Let G be a group of prime order q. Give a Zero-Knowledge protocol for the language containing all tuples (g, g^a, h, h^b) where $g, h \in G$ and $a \neq b \bmod q$.

Problem 3: (Protocols) Let p be a prime. Suppose user A has an $x \in \mathbb{Z}_p$ and user B has a $y \in \mathbb{Z}_p$. They wish to compute the following function: $f(x, y) = 0$ when $x = y$ and $f(x, y) = 1$ when $x \neq y$, without revealing any other information about x or y. Your goal is to give an efficient and practical solution to this problem in the honest-but-curious settings.

- **a.** Suppose there is a third party who is willing to help. Give an efficient 3-party protocol for computing $f(x, y)$ so that nothing else is revealed to any single party (1-private). Prove 1-privacy by showing a simulator for each party's view of the protocol (the simulator is given $f(x, y)$ and that party's input).
  Hint: Try using a random hash function from $\mathcal{H} = \{ax + b \mid a \in \mathbb{Z}_p^*,\ b \in \mathbb{Z}_p\}$.
- **b.** What is the most efficient protocol you can give without the third party?

Problem 4: (WUF) You are given a family of WUFs $h_k \colon \{0,1\}^{2n} \mapsto \{0,1\}^n$.

- **a.** Show that the family of functions $\tilde{h}_k \colon \{0,1\}^{2n} \times \{0,1\}^n \mapsto \{0,1\}^n$ defined as

$$\tilde{h}_k(x_0, x_1) = h_k(h_k(x_0), x_1)$$

  need not be a WUF. (Recall that if h_k is a family of collision-resistant functions, then $\tilde{h}_k$ is guaranteed to be collision-resistant. This is an observation, not a hint.)
- **b.** Prove that $H_{k,m}(x_0, x_1) = h_k(h_k(x_0) \oplus m, x_1)$, where $|m| = n$, is a family of WUFs.