Homework 10

Due: December 9, 2024

CS 1510: Intro. to Cryptography and Computer Security

1 1-out-of-n Oblivious Transfer

In Lecture 23, we saw (will see) a construction and proof of security for 1-out-of-2 OT, where the sender has two messages and the receiver asks for one.

a. Extend this scheme to 1-out-of-n OT, where the sender has n messages and the receiver asks for one. The desired security goals for 1-out-of-n OT follow from the 1-out-of-2 case: the sender should not learn which message the receiver wants, and the receiver should not learn the decryption of any other message besides the one it has requested. You may assume the same setting as 1-out-of-2 OT: a cyclic group $\mathbb{G}$ of order q with generator g, and a random oracle $H : \mathbb{G} \to \{0,1\}^\ell$. You may not reduce to 1-out-of-2 OT.

b. Prove that if CDH is hard in $\mathbb{G}$ and H is a random oracle, then your protocol is semi-honest secure.

2 PSI with Secret Sharing

We saw the PSI-CA scheme in class (Lecture 22, Slide 12). Let's say that Alice and Bob also want to secret share each of the x_i values that are in the intersection of their two sets while still not learning which values are shared. That is, Alice and Bob want to compute a function $f(X, Y)$ such that Alice and Bob both receive output $|X \cap Y|$, Alice receives $\{r_{A,i}\}_{i \in [|X \cap Y|]}$, and Bob receives $\{r_{B,i}\}_{i \in [|X \cap Y|]}$. Each $r_{A,i}$ and $r_{B,i}$ should be distributed uniformly at random (in $\mathbb{Z}_p$, as defined below) and $\{r_{A,i} + r_{B,i}\}_{i \in [|X \cap Y|]} = X \cap Y$. You may assume all the elements in X and Y are from $\mathbb{Z}_p$.

You may assume an additively homomorphic encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ for a message space $\mathbb{Z}_p$ with an additional rerandomization function. Semi-formally, this rerandomization function is defined $\mathsf{Rerand} : \mathcal{C} \to \mathcal{C}$ over ciphertext space $\mathcal{C}$, such that for any message m, any ciphertext $c = \mathsf{Enc}(m)$, and any rerandomized ciphertext $c' = \mathsf{Rerand}(c)$, $\mathsf{Dec}(c) = \mathsf{Dec}(c') = m$. Additionally, for any PPT adversary $\mathcal{A}$, the rerandomized ciphertext c' is computationally indistinguishable from a fresh encryption of m even when the secret key of the encryption scheme is known to $\mathcal{A}$. Since you will not be completing the security proof (but may need this concept as an intuition to motivate your protocol and simulator

constructions), you may use the Rerand function as-is (that is, you need not formalize it further).

a. Give a construction that satisfies the above functionality f.

b. Argue why it is correct.

c. Start the proof of security by providing constructions of the simulator for both Alice and Bob (you do not need to finish the proof).

Useful Fact: A secret can be shared in an additively homomorphic way if Bob holds r_i and Alice holds $x_i - r_i$.

3 Three-Party Computation

Given a (semi-honest) secure two-party computation protocol that can compute any function $f(x, y)$, construct a (semi-honest) secure three-party computation protocol that can compute any function $g(x, y, z)$. You *don't* have to formally prove its security.

Hint: For three parties Alice, Bob, Charlie, think of Alice as one party and {Bob, Charlie} as another party in a secure two-party computation protocol.

4 SWHE and FHE Discussion

The following are reflection questions that you may answer informally, with your understanding and intuition rather than mathematical arguments and proofs.

a. What is one potential real-world use-case of somewhat or fully homomorphic encryption? Precisely describe the participants and purpose in the SWHE or FHE application: who owns the data and who is computing on the data? Why is this setup useful?

b. When it comes to practical applications of computing privately over large datasets, it is often desirable to aggregate data from multiple sources or data owners, each with their own secret key. Consider the GSW scheme from class. Is it feasible to instantiate this cryptosystem such that two different key holders can homomorphically compute over their ciphertexts? Why or why not?

5 Summary Question

Summarize the most important insights from this week's material, including from the lectures, notes, textbooks, homework problems, and other resources you find helpful, into a one-page resource. We expect that these summary pages will help you with the take-home midterm and final. Please note this question is graded based on completion—we will not be checking it for correctness. However, we will be checking it for relevance to the week's content and length.