

Homework 10

Due: December 8, 2023

CS 1510: Intro. to Cryptography and Computer Security

1 Zero-Knowledge Proofs of Complex Statements

- a. Let (P_1, V_1) be an honest-verifier zero-knowledge proof system for language L_1 and (P_2, V_2) be an honest-verifier zero-knowledge proof system for language L_2 . Design an honest-verifier zero-knowledge proof system (P, V) for the language $L_1 \cap L_2$. ($x \in L_1 \cap L_2$ if and only if $x \in L_1$ and $x \in L_2$.) Remember to prove completeness, soundness, and zero-knowledge properties of your proof system.
- b. Give a zero-knowledge proof system (P, V) (with efficient prover) for the following language.

$$L = \{((G_0, G_1), (G'_0, G'_1)) \mid G_0 \simeq G_1 \vee G'_0 \simeq G'_1\}$$

Note: Make sure the verifier does not learn which of the two pairs of graphs is isomorphic.

2 PSI with Secret Sharing

We saw the PSI-CA scheme in class (Lecture 23, Slide 9). 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 (Gen, Enc, Dec) for a message space \mathbb{Z}_p with an additional rerandomization function. Semi-formally, this rerandomization function is defined $\text{Rerand} : \mathcal{C} \rightarrow \mathcal{C}$ over ciphertext space \mathcal{C} , such that for any message m , any ciphertext $c = \text{Enc}(m)$, and any rerandomized ciphertext $c' = \text{Rerand}(c)$, $\text{Dec}(c) = \text{Dec}(c') = m$. 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 1-out-of-n Oblivious Transfer

In Lecture 23 we saw 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 $H : \mathbb{G} \rightarrow \{0, 1\}^\ell$.
- b. Prove that if CDH is hard in \mathbb{G} and H is a random oracle, then your protocol is semi-honest secure.

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. You will be permitted to use this one-page resource (along with the other weeks' resources) on the midterm and final.

Changes to this document prior to the exams are permitted, but for each change, you will be asked to state what you changed and why. For example, if you dropped something and replaced it with something else, justify why the thing you dropped wasn't as important as the thing you inserted, why you think it might be more useful for the exam, etc.

Please note that the purpose of this question is to help you organize and synthesize the material for your own future use. It will be graded based on completion—we will not be checking it for correctness.