Homework 2

Advanced Tools From Modern Cryptography
CS 758 : Spring 2022

Released: March 6 Sunday
Due: March 27 Sunday

Secure Multiparty Computation [Total 150 pts]

1. **Secure Switching of Linear Secret-Sharing.** [30 pts]

   Suppose Σ_1 and Σ_2 are two n-party linear secret-sharing schemes for messages in a set $\mathcal{M}$, with access structures $\mathcal{A}_1$ and $\mathcal{A}_2$ respectively.

   Consider the functionality $\mathcal{F}_{\Sigma_1 \to \Sigma_2}$ which interacts with parties $P_1, \ldots, P_n$ as follows: for each i, it accepts w_i from party P_i, where w_i is in the share-space of Σ_1. Then it computes $m := \Sigma_1.\mathsf{recon}(w_1, \ldots, w_n)$, and using fresh randomness, computes $(z_1, \ldots, z_n) \leftarrow \Sigma_2.\mathsf{share}(m)$. Finally, for each $i \in [n]$, it sends z_i to P_i.

   (Here recon denotes the deterministic reconstruction algorithm and share denotes the randomized sharing algorithm, for a secret-sharing scheme.)

   Recall the protocol from the lectures for share-switching: Each party P_i sets $(\sigma_{i,1}, \ldots, \sigma_{i,n}) \leftarrow \Sigma_2.\mathsf{share}(w_i)$, and sends $\sigma_{i,j}$ to P_j. Then, each party P_i computes and outputs $z_i = \Sigma_1.\mathsf{recon}(\sigma_{1,i}, \ldots, \sigma_{n,i})$.

   (a) In order to show that the above is a passive-secure protocol for $\mathcal{F}_{\Sigma_1 \to \Sigma_2}$ against an adversary who corrupts only a set $S \notin \mathcal{A}_2$, describe a simulator. (You need not prove that the simulation is good.)

   (b) Now consider an adversary who corrupts parties in a set $S \in \mathcal{A}_2$. In the above share-switching protocol, now the adversary can learn m. But in the ideal world also the adversary can learn m. Does that make the above protocol secure against passive corruption of parties in S? Justify your answer by either describing a simulator, or by arguing that there is no good simulator.

   Note. The Passive-BGW protocol from class can be formulated modularly as carrying out all interaction between the initial input sharing phase and the final output phase, only via the share-switching functionality.

2. **Semi-Honest to Semi-Malicious Security.** [15 pts]

   In the *semi-malicious* corruption model, the corrupt parties follow the protocol honestly, *except in the choice of randomness*, which may be arbitrary. Note that it has a stronger adversary than the semi-honest (or passive) corruption model.

   (a) Argue that in general a semi-honest secure protocol need not be semi-malicious. Specifically, assume that you are given a semi-honest secure protocol for (say) OT. Convert it into a protocol that remains semi-honest secure, but is *not semi-malicious secure*.

(b) Given a 2-party semi-honest secure protocol Π, show how it can be transformed into a semi-malicious secure protocol Π^* for the same functionality, using an extra round of interaction. You may assume that the parties are given access to an ideal commitment functionality.

Can you prove the semi-malicious security of Π^* by showing how to transform a simulator for Π (against semi-honest adversaries) into a simulator for Π^*? [Extra Credit]

3. **OT, OLE and Correlated Random Variables.** [30 pts]

Define Oblivious Transfer (OT) functionality over a field $\mathbb{F}$ (or, over a ring) as an SFE in which Alice inputs $(x_0, x_1) \in \mathbb{F}^2$ and Bob inputs $b \in \{0,1\}$; then Alice gets $\perp$ as output, but Bob gets x_b.

(a) Consider an inputless, randomized functionality RandOT, which outputs a random pair $(z_0, z_1) \in \mathbb{F}^2$ to Alice and (c, z_c) to Bob, where $c \in \{0,1\}$ is a random bit. Give a protocol π^{RandOT} that securely realizes OT, by accessing RandOT exactly once at the beginning of the protocol.

(b) Oblivious Linear-function Evaluation (OLE) functionality over a field $\mathbb{F}$ (or, over a ring) is a generalization of OT. It accepts $(a, b) \in \mathbb{F}^2$ from Alice and $x \in \mathbb{F}$ from Bob and sends $y = ax - b$ as output to Bob (and $\perp$ to Alice). Give a protocol ρ^{OLE} that passive-securely realizes OT (over the same field) by accessing OLE.

(c) Define an inputless, randomized version of OLE, called RandOLE, which outputs $(s_A, p_A) \in \mathbb{F}^2$ to Alice and $(s_B, p_B) \in \mathbb{F}^2$ to Bob, where (s_A, s_B, p_A, p_B) are uniformly random conditioned on the relation $s_A + s_B = p_A p_B$. (This distribution corresponds to picking p_A, p_B uniformly from the field, and setting s_A, s_B to be an additive sharing of p_A, p_B.)

For the case when $\mathbb{F} = GF(2)$ (the field of the two elements $\{0,1\}$), give a *deterministic, non-interactive* protocol σ^{RandOLE} that UC securely realizes RandOT, by accessing RandOLE exactly once.

Generalize Part (a) to OLE (for any field): i.e., give a protocol τ^{RandOLE} that securely realizes OLE, by accessing RandOLE exactly once at the beginning of the protocol. [Extra Credit]

4. $\binom{n}{r}$ **OT from** $\binom{2}{1}$ **OT.** [30 pts]

In this problem you shall construct protocols for r-out-of-n OT (which takes n bits $(x_1, \ldots, x_n)$ from Alice, a subset $S \subseteq \{1, \ldots, n\}$ such that $|S| = r$ from Bob and gives $\{(i, x_i) \mid i \in S\}$ to Bob), by accessing 1-out-of-2 OT.

(a) Describe a simple deterministic protocol for $\binom{n}{r}$ OT with information-theoretic security against passive adversaries, using n accesses to an ideal $\binom{2}{1}$ OT functionality. No proof of security is required.

Also state whether your protocol is secure against active corruption of (1) the sender, and (2) the receiver. Briefly justify each answer.

(b) Repeat the previous part for $r = n - 1$, but with the restriction that your protocol is allowed to make only $n - 1$ accesses to the ideal $\binom{2}{1}$ OT functionality.

Hint: Consider $n = 3$. Suppose Alice and Bob carry out two 1-out-of-2 OTs: the first with Alice's inputs being (x_1, x_2) and the second with (x_3, z). What should z be? What should Bob's input to the OTs be when the selection set $S = \{1,2\}$, $\{2,3\}$ and $\{3,1\}$?

Can you come up with an (active) adversarial strategy for Alice that cannot be simulated?

(c) Give a (randomized) protocol for $\binom{n}{1}$-OT using $n - 1$ accesses to that is secure against active corruption as well.

Hint: Consider $n = 3$. Suppose Alice and Bob carry out two 1-out-of-2 OTs: the first with Alice's inputs being (x_1, r) and the second with (y_2, y_3), where r is a random bit and $y_i = x_i \oplus r$. What should Bob's inputs in the two OTs be?

5. **OT from Smooth Projective Hash** [20 pts]

   Construct a UC secure $\binom{n}{n-1}$ OT protocol (in the common reference string model) from Smooth Projective Hash (SPH). You should describe the protocol (including the setup) in detail, using the syntax for SPH from class. Also, briefly sketch a proof of security.

6. **Commitment from OT** [25 points]

   In this problem we shall see two information-theoretic protocols for (UC-secure) commitment using an ideal functionality for some form of OT. Below Alice denotes the sender in the commitment protocol and Bob the receiver.

   (a) The following protocol can be used to commit to a single field element from an appropriate field $\mathbb{F}$. It uses a $\binom{k}{d}$ OT over $\mathbb{F}$ (where k is the statistical security parameter and d is an appropriate value to be determined), as follows:

   Commitment phase: Alice secret-shares her input $m \in \mathbb{F}$ using a (k, t) secret-sharing scheme (say, Shamir secret-sharing using degree $t - 1$ polynomials), where t is a parameter to be determined, and sends the k shares to the $\binom{k}{d}$ OT functionality. Bob picks up a random set of d shares from OT.

   Opening phase: Alice sends the k shares she used in the commitment phase. Bob checks if the d shares he had obtained during the commitment phase match the ones received now. If so, and if the k shares are a valid secret-sharing of $m \in \mathbb{F}$, then Bob outputs m as the opened value.

   This protocol is secure only if d, t are chosen appropriately, as explored below.

   i. For the scheme to be hiding, what constraint should you place on d, t?

   ii. Show that the scheme is not binding if $t = 2$ and $d = 1$. Specifically, give an adversarial strategy for Alice such that, *after the commitment phase*, for all $m' \in \mathbb{F}$, she can open the commitment successfully to m' with probability at least $1/\text{poly}(k)$.

   iii. Show that the scheme is not binding (as above) if $t = k$ and for any d that satisfies the condition for hiding, from (i). Here, for simplicity, you may assume that the (k, k)-secret-sharing scheme used is additive secret-sharing.

   iv. Suggest a setting of (t, d) such that the scheme is both hiding and binding. Briefly justify.

   (b) The next protocol is a bit-commitment protocol, and it uses a $\binom{2}{1}$ *string OT* functionality. Below, an outline of the protocol is given.

   Outline: During the commitment phase the parties invoke the string OT functionality just once, with Bob playing the role of the sender and Alice that of the receiver in the OT functionality. (Note the reversed roles.) During the opening phase, Alice sends a single message to Bob, who outputs a bit (the opened bit) or $\perp$ (indicating that he does not accept the opening). There is no other interaction in the protocol.

   Fill in the details of this protocol. (No proof of security needed.)