CS65500: Advanced Cryptography Instructor: Aarushi Goel

Homework 2

Due: February 13; 2025 (11:59 PM)

Consider the following definition of a 1-out-of-2 oblivious transfer protocol. Then answer the questions below:

Definition 1 (Two-Message Semi-Honest OT) *A two-message 1-out-of-2 oblivious transfer between a receiver R and a sender S is defined by a tuple of 3 PPT algorithms $(\mathsf{OT}_R, \mathsf{OT}_S, \mathsf{OT}_{\mathsf{out}})$. The OT protocol works as follows (let λ be the security parameter):*

1. ***Receiver:*** *The receiver computes $(\mathsf{msg}_R, \rho) \leftarrow \mathsf{OT}_R(1^\lambda, b)$, where $b \in \{0,1\}$ is the receiver's input. It sends msg_R to the sender.*
2. ***Sender:*** *The sender computes $\mathsf{msg}_S \leftarrow \mathsf{OT}_S(1^\lambda, \mathsf{msg}_R, (m_0, m_1))$, where $m_0, m_1 \in \{0,1\}^*$ are the sender's input. The sender sends msg_S to the receiver.*
3. ***Receiver's Output:*** *The receiver computes $m_b \leftarrow \mathsf{OT}_{\mathsf{out}}(\rho, \mathsf{msg}_S)$.*

This protocol satisfies the following properties:

- ***Correctness***: *For each $m_0, m_1 \in \{0,1\}^*$, $b \in \{0,1\}$, it holds that*

$$\Pr\left[\begin{array}{r}(\rho, \mathsf{msg}_R) \leftarrow \mathsf{OT}_R\left(1^\lambda, b\right) \\ \mathsf{msg}_S \leftarrow OT_S\left(1^\lambda, \mathsf{msg}_R, (m_0, m_1)\right)\end{array} \middle| \; \mathsf{OT}_{\mathsf{out}}\left(\rho, \mathsf{msg}_R, \mathsf{msg}_S\right) = m_b\right] = 1,$$

- ***Security against Semi-Honest Sender***: *It holds that,*

$$\left\{(\mathsf{msg}_R^0, \rho^0) \leftarrow \mathsf{OT}_R\left(1^\lambda, 0\right) \;\middle|\; \mathsf{msg}_R^0\right\} \approx_c \left\{(\mathsf{msg}_R^1, \rho^1) \leftarrow \mathsf{OT}_R\left(1^\lambda, 1\right) \mid \mathsf{msg}_R^1\right\}$$

- ***Security against Semi-Honest Receiver***: *It holds that for each $b \in \{0,1\}$, $m_0, m_1, m_0', m_1' \in \{0,1\}^*$, and $m_b = m_b'$,*

$$\left\{\mathsf{OT}_S\left(1^\lambda, \mathsf{msg}_R, (m_0, m_1)\right)\right\} \approx_c \left\{\mathsf{OT}_S\left(1^\lambda, \mathsf{msg}_R, (m_0', m_1')\right)\right\}$$

  where $(\mathsf{msg}_R, \rho) \leftarrow OT_R(1^\lambda, b)$.

1 On the Equivalence of Definitions

Prove that an oblivious transfer protocol $\pi = (\mathsf{OT}_R, \mathsf{OT}_S, \mathsf{OT}_{\mathsf{out}})$ that satisfies Definition 1 also meets the simulator-based definition of semi-honest secure 1-out-of-2 OT discussed in class.

2 1-out-of-4 Oblivious Transfer

Let $(\mathsf{OT}_R, \mathsf{OT}_S, \mathsf{OT}_{\mathsf{out}})$ be a semi-honest secure, two message, 1-out-of-2 oblivious transfer protocol that satisfies Definition 1. Now consider the following $(\mathsf{OT}^*_R, \mathsf{OT}^*_S, \mathsf{OT}^*_{\mathsf{out}})$ construction of a 1-out-of-4 oblivious transfer protocol:

1. $(\mathsf{msg}^*_R, \rho^*) \leftarrow \mathsf{OT}^*_R(1^\lambda, b)$**:** Let $b \in [4]$ be the receiver's input. For each $i \in [4]$, the receiver computes the following:
$$\text{if } b = i,\ (\mathsf{msg}^i_R, \rho^i) \leftarrow \mathsf{OT}_R(1^\lambda, 1); \text{ else, } (\mathsf{msg}^i_R, \rho^i) \leftarrow \mathsf{OT}_R(1^\lambda, 0).$$
Finally, the receiver sets $\mathsf{msg}^*_R = \left(\{\mathsf{msg}^i_R\}_{i\in[4]}\right)$, $\rho^* = \left(\{\rho^i\}_{i\in[4]}\right)$ and sends msg^*_R to the sender.

2. $\mathsf{msg}^*_S \leftarrow \mathsf{OT}^*_S(1^\lambda, \mathsf{msg}^*_R, (m_1, m_2, m_3, m_4))$**:** Let $m_1, m_2, m_3, m_4 \in \{0,1\}^*$ be the sender's inputs. The sender parses $\mathsf{msg}^*_R = \left(\{\mathsf{msg}^i_R\}_{i\in[4]}\right)$. For each $i \in [4]$, the sender computes the following:
$$\mathsf{msg}^i_S \leftarrow \mathsf{OT}_S(1^\lambda, \mathsf{msg}^i_R, (0, m_i)).$$
Finally, the sender sets $\mathsf{msg}^*_S = \left(\{\mathsf{msg}^i_S\}_{i\in[4]}\right)$ and sends msg^*_S to the receiver.

3. $m_b \leftarrow \mathsf{OT}^*_{\mathsf{out}}(\rho^*, \mathsf{msg}^*_S)$**:** The receiver parses $\rho^* = \left(\{\rho^i\}_{i\in[4]}\right)$ and $\mathsf{msg}^*_S = \left(\{\mathsf{msg}^i_S\}_{i\in[4]}\right)$. Finally, it computes and outputs $m_b \leftarrow \mathsf{OT}_{\mathsf{out}}(\rho^b, \mathsf{msg}^b_S)$.

Prove that the above construction $(\mathsf{OT}^*_R, \mathsf{OT}^*_S, \mathsf{OT}^*_{\mathsf{out}})$ **is that of a semi-honest secure 1-out-of-4 oblivious transfer protocol.** (Note that you need to argue correctness and security against a semi-honest sender and receiver.)

3 OT Combiner

Let $(\mathsf{OT}^1_R, \mathsf{OT}^1_S, \mathsf{OT}^1_{\mathsf{out}})$ and $(\mathsf{OT}^2_R, \mathsf{OT}^2_S, \mathsf{OT}^2_{\mathsf{out}})$ be two message, 1-out-of-2 oblivious transfer (OT) protocols, both satisfying correctness and security against a semi-honest sender. However, **only one of them is guaranteed to be secure against a semi-honest receiver.** Now, consider the following new construction $(\mathsf{OT}^*_R, \mathsf{OT}^*_S, \mathsf{OT}^*_{\mathsf{out}})$ of a two-message oblivious transfer protocol:

- $(\mathsf{msg}^*_R, \rho^*) \leftarrow \mathsf{OT}^*_R(1^\lambda, b)$: Let $b \in \{0,1\}$ be the receiver's input. The receiver computes $(\mathsf{msg}^1_R, \rho^1) \leftarrow \mathsf{OT}^1_R(1^\lambda, b)$ and $(\mathsf{msg}^2_R, \rho^2) \leftarrow \mathsf{OT}^2_R(1^\lambda, b)$. Finally, the receiver sets $\mathsf{msg}^*_R = (\mathsf{msg}^1_r, \mathsf{msg}^2_r)$, $\rho^* = (\rho^1, \rho^2)$ and sends msg^*_R to the sender.

- $\mathsf{msg}^*_S \leftarrow \mathsf{OT}^*_S(1^\lambda, \mathsf{msg}^*_R, (m_0, m_1))$: Let $m_0, m_1 \in \{0,1\}^*$ be the sender's inputs. The sender parses $\mathsf{msg}^*_R = (\mathsf{msg}^1_R, \mathsf{msg}^2_R)$ and randomly samples $m^1_0, m^2_0, m^1_1, m^2_1 \in \{0,1\}^*$, such that $m^1_0 \oplus m^2_0 = m_0$ and $m^1_1 \oplus m^2_1 = m_1$. The sender then computes $\mathsf{msg}^1_S \leftarrow \mathsf{OT}^1_S(1^\lambda, \mathsf{msg}^1_R, (m^1_0, m^1_1))$ and $\mathsf{msg}^2_S \leftarrow \mathsf{OT}^2_S(1^\lambda, \mathsf{msg}^2_R, (m^2_0, m^2_1))$. Finally, the sender sets $\mathsf{msg}^*_S = (\mathsf{msg}^1_S, \mathsf{msg}^2_S)$ and sends msg^*_S to the receiver.

- $m_b \leftarrow \mathsf{OT}^*_{\mathsf{out}}(\rho^*, \mathsf{msg}^*_S)$: The receiver parses $\rho^* = (\rho^1, \rho^2)$ and $\mathsf{msg}^*_S = (\mathsf{msg}^1_S, \mathsf{msg}^2_S)$. The receiver then computes $m^1_b \leftarrow \mathsf{OT}^1_{\mathsf{out}}(\rho^1, \mathsf{msg}^1_S)$ and $m^2_b \leftarrow \mathsf{OT}^2_{\mathsf{out}}(\rho^2, \mathsf{msg}^2_S)$. Finally, the receiver outputs $m_b = m^1_b \oplus m^2_b$.

Prove that the above construction $(\mathsf{OT}^*_R, \mathsf{OT}^*_S, \mathsf{OT}^*_{\mathsf{out}})$ **is a 1-out-of-2 oblivious transfer that is secure against a semi-honest receiver.** (Note that you **DO NOT** need to show that this protocol is also secure against a semi-honest sender.)

4 Public-Key Encryption

Recall the following definition of a public-key encryption:

Definition 2 (IND-CPA Secure Public-Key Encryption) *For all $\lambda \in \mathbb{N}$, a CPA-secure public-key encryption comprises of a tuple of PPT algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *defined as follows:*

- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$*: The key generation algorithm takes the security parameter 1^λ as input and outputs a public-key* pk *and a secret-key* sk*.*
- $ct \leftarrow \mathsf{Enc}(\mathsf{pk}, m; r)$*: The encryption algorithm takes as input, the public-key* pk*, a message $m \in \{0,1\}^*$ and a random string $r \in \{0,1\}^\lambda$, and outputs a ciphertext ct.*
- $m \leftarrow \mathsf{Dec}(\mathsf{sk}, ct)$*: The decryption algorithm takes as input the secret-key* sk *and a ciphertext ct, and outputs a message m.*

These algorithms satisfy the following:

1. ***Correctness:*** *Let $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$, then $\forall m \in \{0,1\}^*$ and uniformly sampled $r \leftarrow\!\!\$ \{0,1\}^\lambda$, it holds that:*
$$\Pr\left[m \leftarrow \mathsf{Dec}\left(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, m; r)\right)\right] = 1$$
2. ***IND-CPA Security:*** *Let $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$, then $\forall m_0, m_1 \in \{0,1\}^*$, the following two distributions are computationally indistinguishable:*
$$\left\{\mathsf{Enc}(\mathsf{pk}, m_0; r); r \leftarrow\!\!\$ \{0,1\}^\lambda\right\} \quad \textit{and} \quad \left\{\mathsf{Enc}(\mathsf{pk}, m_1; r); r \leftarrow\!\!\$ \{0,1\}^\lambda\right\}$$

Let $(\mathsf{OT}_R, \mathsf{OT}_S, \mathsf{OT}_{\mathsf{out}})$ be a semi-honest secure two message 1-out-of-2 oblivious transfer protocol that satisfies Definition 1. Now consider the following construction of a public-key encryption:

- $\mathsf{KeyGen}(1^\lambda)$: Compute $(\mathsf{msg}_R, \rho) \leftarrow \mathsf{OT}_R(1^\lambda, 0)$. Set $\mathsf{pk} = \mathsf{msg}_R$ and $\mathsf{sk} = \rho$. Output $(\mathsf{pk}, \mathsf{sk})$.
- $\mathsf{Enc}(\mathsf{pk}, m)$: Compute $\mathsf{msg}_S \leftarrow \mathsf{OT}_S(1^\lambda, \mathsf{pk}, (m, m))$ and set $ct = \mathsf{msg}_S$. Output ciphertext ct.
- $\mathsf{Dec}(\mathsf{sk}, ct)$: Compute and output $m \leftarrow \mathsf{OT}_{\mathsf{out}}(\mathsf{sk}, ct)$.

Prove that the above is an IND-CPA secure public-key encryption scheme, i.e., it satisfies Definition 2.