CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 7

Deadline: November 18, 2019; 11:59 AM

1. **(15 points)** Let $\mathcal{E} = (\mathcal{E}.\mathsf{Gen}, \mathcal{E}.\mathsf{Enc}, \mathcal{E}.\mathsf{Dec})$ be an **IND-CPA** secure secret key encryption scheme and $\mathcal{M} = (\mathcal{M}.\mathsf{Gen}, \mathcal{M}.\mathsf{Tag}, \mathcal{M}.\mathsf{Ver})$ be a **UF-CMA** secure MAC scheme. Consider the following encryption scheme $(\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$:

   - $\mathsf{KeyGen}(1^\lambda)$: Generate $k_{\mathcal{E}} \leftarrow \mathcal{E}.\mathsf{Gen}(1^\lambda)$ and $k_{\mathcal{M}} \leftarrow \mathcal{M}.\mathsf{Gen}(1^\lambda)$. Output $k = (k_{\mathcal{E}}, k_{\mathcal{M}})$
   - $\mathsf{Encrypt}(k, m)$: Parse $k = (k_{\mathcal{E}}, k_{\mathcal{M}})$. Compute $c' \leftarrow \mathcal{E}.\mathsf{Enc}(k_{\mathcal{E}}, m)$, $\sigma \leftarrow \mathcal{M}.\mathsf{Tag}(k_{\mathcal{M}}, c')$. Output $c = (c', \sigma)$.
   - $\mathsf{Decrypt}(k, c)$: Parse $k = (k_{\mathcal{E}}, k_{\mathcal{M}})$ and $c = (c', \sigma)$. If $\mathcal{M}.\mathsf{Ver}(k_{\mathcal{M}}, c', \sigma) \neq 1$, output $\perp$. Else, output $m \leftarrow \mathcal{E}.\mathsf{Dec}(k_{\mathcal{E}}, c')$.

   Prove that this scheme is **IND-CCA2** secure.

2. **(10 points)** We want to design a sealed-bid auction scheme. Assume that the seller is honest and that there are two potential buyers – Alice and Bob. First Alice submits her bid and then Bob submits his bid. A natural security requirement from a sealed-bid auction scheme is that Bob (who makes his bid after Alice) should not be able to choose his bid based on the bid made by Alice, since otherwise the former can always outbid the latter.

   Now consider the following proposal to perform a sealed-bid auction between Alice and Bob: The seller publishes a public key pk for the **ElGamal encryption scheme**. Both Alice and Bob send an ElGamal encryption $\mathsf{Enc}(\mathsf{pk}, x)$ of their bid x over a public channel (i.e. everyone can observe the encrypted bids), and then the seller decrypts both the bids and awards the product to the highest bidder.

   Explain why this proposal does not satisfy the security requirement of sealed bid auction by designing a cheating Bob, who wins the auction by making sure that his bid is two-times that of Alice's bid.

3. **(10 points)** Let $(\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ be an **IND-CCA2** secure public-key bit-encryption scheme. Consider the following encryption scheme $(\mathsf{KeyGen}', \mathsf{Encrypt}', \mathsf{Decrypt}')$ for two-bit messages.

   - $\mathsf{KeyGen}'(1^\lambda)$: Generate $(\mathsf{sk}_1, \mathsf{pk}_1) \leftarrow \mathsf{KeyGen}(1^\lambda)$ and $(\mathsf{sk}_2, \mathsf{pk}_2) \leftarrow \mathsf{KeyGen}(1^\lambda)$. Output $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$ and $\mathsf{sk} = (\mathsf{sk}_1, \mathsf{sk}_2)$.
   - $\mathsf{Encrypt}'(\mathsf{pk}, m)$: Parse $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$ and parse $m = m_1 \| m_2$. Compute $c_1 \leftarrow \mathsf{Enc}(\mathsf{pk}_1, m_1)$ and $c_2 \leftarrow \mathsf{Enc}(\mathsf{pk}_2, m_2)$. Output $c = (c_1, c_2)$.
   - $\mathsf{Decrypt}'(\mathsf{sk}, c)$: Parse $\mathsf{sk} = (\mathsf{sk}_1, \mathsf{sk}_2)$ and parse $c = (c_1, c_2)$. Compute $m_1 = \mathsf{Dec}(\mathsf{sk}_1, c_1)$ and $m_2 = \mathsf{Dec}(\mathsf{sk}_2, c_2)$. Output $m = m_1 \| m_2$.

   Show that this scheme is not **IND-CCA2** secure.

4. **(15 points)** Suppose that Alice and Bob hold correlated inputs of the following form: Alice has (r_0, r_1), where each $r_i \xleftarrow{\$} \{0,1\}$ and Bob has (c, r_c), where $c \xleftarrow{\$} \{0,1\}$.

Further suppose that at a later point, Alice and Bob wish to securely compute 1-out-of-2 OT with inputs (x_0, x_1) and b respectively. Show how Alice and Bob can use their correlated inputs for performing this task without using any cryptographic assumptions. That is, design a protocol for 1-out-of-2 OT that achieves *unconditional* security against semi-honest adversaries. Argue correctness and security of your protocol. (You don't need to give a full formal proof.)

(**Hint:** Recall that one-time pads do not require any cryptographic assumptions.)