CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 6

Deadline: December 7; 2022, 1:30 PM EST

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)** 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 n-bit messages.

   - $\mathsf{KeyGen}'(1^\lambda)$: For $i \in \{1, ..., n\}$, generate $(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow \mathsf{KeyGen}(1^\lambda)$. Output $\mathsf{pk} = (\mathsf{pk}_1, ..., \mathsf{pk}_n)$ and $\mathsf{sk} = (\mathsf{sk}_1, ..., \mathsf{sk}_n)$
   - $\mathsf{Encrypt}'(\mathsf{pk}, m)$: Parse $\mathsf{pk} = (\mathsf{pk}_1, ..., \mathsf{pk}_n)$ and parse $m = m_1 \| ... \| m_n$. For $i \in \{1, ..., n\}$, compute $c_i \leftarrow \mathsf{Enc}(\mathsf{pk}_i, m_i)$. Output $c = (c_1, ..., c_n)$.
   - $\mathsf{Decrypt}'(\mathsf{sk}, c)$: Parse $\mathsf{sk} = (\mathsf{sk}_1, ..., \mathsf{sk}_n)$ and parse $c = (c_1, ..., c_n)$. For $i \in \{0, ..., n\}$, compute $m_i = \mathsf{Dec}(\mathsf{sk}_i, c_i)$. Output $m = m_1 \| ... \| m_n$.

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

3. **(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.)

4. **(10 points)** Let Alice and Bob be two parties with inputs $a \in \mathbb{Z}_q$ and $b \in \mathbb{Z}_q$, respectively. They wish to check if their inputs are equal, i.e., whether $a = b$. They want to do this while making sure that they do not learn any other information about the other party's input. In other words, if $a \neq b$, then Alice should not learn b and Bob should not learn a.

   Let $\mathbb{G}$ be a cyclic group of prime order q with generator g. They run the following protocol:

- Alice samples a random value $r \xleftarrow{\$} \mathbb{Z}_q$. It then computes $X = g^r$ and $Y = g^{ar}$. It sends (X, Y) to Bob.
- Bob computes X^b. It outputs 1 if $X^b = Y$, and 0 otherwise.

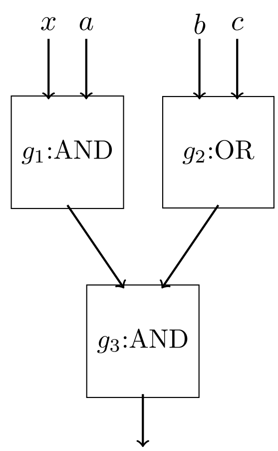
Explain why this protocol is not secure against semi-honest Bob.

5. **(15 points)** Let Alice and Bob have inputs a and b, respectively. They want to securely send $(a + b)$ to a third-party Carol. Devise a protocol where Alice and Bob are only allowed to send **at most one message to each other** and **at most one message each to Carol**. Your protocol should satisfy all of the following security properties:

   - *Security against Semi-honest Alice:* Alice should not learn b.
   - *Security against Semi-honest Bob:* Bob should not learn a.
   - *Security against Semi-honest Carol:* Carol should not learn a and b.

   Argue that your protocol indeed satisfies all three security conditions, and gives the correct output to Carol. (You don't need to give a formal proof).

6. **(15 points)** Let C be a Boolean circuit as shown in the following figure.



   Let $(\mathsf{Garble}, \mathsf{Eval})$ be the garbling scheme discussed in class. Recall that the $\mathsf{Garble}()$ function, when given this Boolean circuit C as input, outputs the following:

$$(\hat{G} = \{\hat{g}_1, \hat{g}_2, \hat{g}_3\}, \hat{\mathsf{In}} = \{K_0^1, K_1^1, K_0^2, K_1^2, K_0^3, K_1^3, K_0^4, K_1^4\}) \leftarrow \mathsf{Garble}(C),$$

   where $\hat{G}$ is the set of 3 garbled gates and $\hat{\mathsf{In}}$ is the set of wire keys for the 4 input wires in this circuit. In this question, we will see that the privacy of inputs in a garbled circuit does not hold if the adversary has both the keys for a wire.

   Consider an adversary who knows the description of C, garbled gates $\hat{G}$ and input wire keys $\{K_0^1, K_1^1, K_a^2, K_b^3, K_c^4\}$. Note that the adversary gets both the input wire keys for the first input wire, and only one key for each of the remaining 3 input wires. Also note that the values a, b, c are not known to the adversary.

   Show how this adversary can use this information to learn at least one out of a, b or c.

   (**Hint: Use the truth table of the gates to derive information.**)