CS 276: Homework 4

Due Date: Sunday, Apr 19, 2026 at 8:59pm via Gradescope

Usage of LLMs/Generative AI tools is prohibited. Other online resources (textbooks/lecture notes) are permissible.

1. Recall that an IBE scheme $\mathcal{E}_{id} = (G, K, E, D)$ where:

   - $G(1^n)$: setup; outputs master public key mpk and master secret key msk.
   - $K(msk, id)$: keygen; outputs secret key sk_{id} for identity id.
   - $E(mpk, id, m)$: encrypts m under identity id, outputs ciphertext c.
   - $D(sk_{id}, c)$: decrypts; outputs m or $\perp$.

   and satisfies correctness and IBE-CPA security (as defined in the notes). Consider a weaker version IBE-CPA* without any key queries as follows:

   Game $\mathbf{Exp}^{\textbf{IBE-CPA*}}_{\Pi,\mathcal{A}}(n)$

   (a) $\mathcal{A}$ outputs challenge identity id^*.
   (b) Challenger runs $(mpk, msk) \leftarrow G(1^n)$, sends mpk to $\mathcal{A}$.
   (c) $\mathcal{A}$ outputs messages (m_0, m_1).
   (d) Challenger samples $b \leftarrow \{0,1\}$, computes $c^* \leftarrow E(mpk, id^*, m_b)$, sends c^* to $\mathcal{A}$.
   (e) $\mathcal{A}$ outputs b'; output 1 if $b' = b$, else 0.

   Given a IND-CPA secure public key encryption scheme, construct an IBE scheme that satisfies IBE-CPA* security but not IBE-CPA security.

2. Show that the following commitment scheme for bits satisfies both the hiding and binding properties.

   Let $G : \{0,1\}^n \to \{0,1\}^{3n}$ be a secure PRG. To commit to a bit $b \in \{0,1\}$, Alice and Bob engage in the following protocol:

   - **Commit**: Bob commits to bit $b \in \{0,1\}$ by doing the following:
     (a) Alice chooses a random $r \in \{0,1\}^{3n}$ and sends r to Bob.
     (b) Bob chooses a random $s \in \{0,1\}^n$ and computes:

     $$c = \text{com}(s, r, b) := \begin{cases} G(s) & \text{if } b = 0, \\ G(s) \oplus r & \text{if } b = 1. \end{cases}$$

     Bob outputs c as the commitment string and uses s as the opening string.
   - **Open**: Bob sends (b, s) to Alice. Alice accepts the opening if $c = \text{com}(s, r, b)$ and rejects otherwise.

3. Recall the ZK proof for graph isomorphism: the interaction is $\mathcal{P}(x, w) \leftrightarrow \mathcal{V}(x)$ where x represents graphs $G_0 = (V, E_0)$ and $G_1 = (V, E_1)$ and w represents a permutation on V such that $w(G_0) = G_1$.

   (a) $\mathcal{P}$ samples a random permutation $\sigma : V \to V$ and sends the graph $H = \sigma(G_1)$ to $\mathcal{V}$.

   (b) $\mathcal{V}$ samples a random bit b and sends it to $\mathcal{P}$.

   (c) If $b = 1$, then $\mathcal{P}$ defines a permutation τ to be σ. If $b = 0$, then instead $\tau = \sigma \circ w$. $\mathcal{P}$ then sends τ to $\mathcal{V}$.

   (d) $\mathcal{V}$ verifies that $\tau(G_b) = H$ and accepts if so.

   Given two instances of this problem (G_0, G_1) and (G_2, G_3) such that $G_0 \cong G_1$ and $G_2 \cong G_3$ but the prover only has access to a witness for one of the two instances, construct a ZK proof for the statement "$G_0 \cong G_1$ OR $G_2 \cong G_3$" and show that it satisfies completeness, soundness and zero-knowledge.
   Note that the proof must not leak which of the two instances the prover has a witness for. You cannot assume that all the graphs have the same vertex set (only that the two graphs in each instance have the same vertex set).