CS 276: Homework 3

Due Date: Sunday, Mar 15, 2026 at 8:59pm via Gradescope

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

Definition 0.1 (Trapdoor Permutation (TDP)) *A* trapdoor permutation *is a trapdoor function* $(\mathsf{TDP.Gen}, f, f^{-1})$ *where for every* $(s,t) \leftarrow \mathsf{TDP.Gen}(1^n)$*, the function* $f(s,\cdot) : \mathcal{D}(s) \to \mathcal{D}(s)$ *is a* permutation *on its domain* $\mathcal{D}(s)$*.*

Notation. To avoid confusion between the public-key and secret-key schemes, we write the secret-key encryption scheme as $\mathsf{SKE} = (\mathsf{G}, \mathsf{E}, \mathsf{D})$, where G generates a key, E encrypts, and D decrypts.

1. **(IND-CCA Security from Trapdoor Permutations.)**

   Let $(\mathsf{TDP.Gen}, f, f^{-1})$ be a trapdoor permutation and let H be a random oracle $H : \{0,1\}^* \to \{0,1\}^n$. Let $\mathsf{SKE} = (\mathsf{G}, \mathsf{E}, \mathsf{D})$ be an IND-CCA-secure secret-key encryption scheme. Consider the following public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:

   - $\mathsf{Gen}(1^n)$: Run $\mathsf{TDP.Gen}(1^n)$ to obtain (s,t). Set $\mathsf{pk} = s$ and $\mathsf{sk} = t$.
   - $\mathsf{Enc}(\mathsf{pk}, m)$: Sample $x \xleftarrow{\$} \mathcal{D}(s)$ and compute $y \leftarrow f(s,x)$. Encrypt m using the secret-key scheme with key $H(x)$: compute $z \leftarrow \mathsf{E}(H(x), m)$. Output $c = (y,z)$.
   - $\mathsf{Dec}(\mathsf{sk}, c)$: Parse $c = (y,z)$ and compute $x \leftarrow f^{-1}(t,y)$. Decrypt using the secret-key scheme: compute $m \leftarrow \mathsf{D}(H(x), z)$. Output m.

   Prove that Π is IND-CCA-secure in the random oracle model.

   Hint: We have shown that this is IND-CPA-secure (Theorem 6.1)