CS 601.442/642 – Modern Cryptography Instructors: Aditya Hegde and Harry Eldridge

Homework 4

Deadline: February 26; 2026, 11:59pm ET

Instructions

- The solutions must be submitted via Canvas.
- You must typeset your solutions. We suggest using LaTeX or Typst.
- This homework includes a bonus question for practice. It will not be graded, even if submitted.

Problems

1. (10 points) Prove unconditionally[1] the existence of a PRF family $\{F_k\}_{k\in\{0,1\}^\lambda}$, where for each $k \in \{0,1\}^\lambda$, $F_k : \{0,1\}^{\lceil \log \lambda \rceil} \to \{0,1\}$.
2. (30 points) Let $\left\{F_k : \{0,1\}^\lambda \to \{0,1\}^\lambda\right\}_{k\in\{0,1\}^\lambda}$ be a family of PRFs. Discuss whether each $F'_k : \{0,1\}^{\lambda-1} \to \{0,1\}^{2\lambda}$ defined below is a PRF. If F' is a PRF, prove it via reduction. When F' is not a PRF, describe an efficient adversary that successfully attacks the PRF.
   (a) $F'_k(x) \coloneqq F_k(0\|x)\|F_k(1\|x)$.
   (b) $F'_k(x) \coloneqq F_k(0\|x)\|F_k(x\|1)$.
3. (30 points) Assuming the existence of PRFs, construct an encryption scheme that is multi-message secure but not CPA-secure.

   You may design an encryption scheme specifically to fail under CPA attacks; it does not need to be "natural."

   Hint: Compared to the multi-message security game, in the CPA game the adversary can obtain encryptions of messages of its choice even *after* seeing the challenge ciphertext. Can you embed extra information in the ciphertext that becomes useful only when the adversary has this additional power?
4. (30 points) Let λ be the security parameter and let $\ell \coloneqq \ell(\lambda)$ be a polynomially bounded integer. Let $\Pi_1 = (\mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\Pi_2 = (\mathsf{Enc}_2, \mathsf{Dec}_2)$ be two encryption schemes with message space $\{0,1\}^\ell$. It is known that at least one among Π_1 and Π_2 is CPA-secure, but we don't know which one. Show how to construct an encryption scheme Π with message space $\{0,1\}^\ell$ such that is guaranteed to be CPA-secure as long as at least one of Π_1 or Π_2 is CPA-secure. Provide a full proof of your solution.

Bonus Question: Let $\Pi = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme with key space $\{\mathcal{K}_\lambda\}_\lambda$ and message space $\{\mathcal{M}_\lambda\}_\lambda$.[2] Assume that for each $\lambda \in \mathbb{N}$, there exist at least two messages in $\mathcal{M}_\lambda$ and that there exists an efficient algorithm to sample messages uniformly at random from $\mathcal{M}_\lambda$. In this question, you will show that if Π is CPA-secure then it is computationally infeasible for an adversary to make an encryptor generate the same ciphertext twice.

Let $\mathcal{K} \coloneqq \mathcal{K}_\lambda$ and $\mathcal{M} \coloneqq \mathcal{M}_\lambda$ for brevity. We define the following game: The challenger samples $k \leftarrow\!\!\$\ \mathcal{K}$ uniformly at random and the adversary makes a series of queries; the i-th query is a message m_i, to which the challenger responds with $c_i \leftarrow \mathsf{Enc}(k, m_i)$. The adversary wins the game if any two c_i's are the same.

Show that if Π is CPA-secure then every non-uniform PPT adversary wins this game with at most negligible probability.

[1] Your proof should *not* rely on any computational assumptions like the existence of a PRG or PRF.

[2] $\{\mathcal{K}_\lambda\}_\lambda$ and $\{\mathcal{M}_\lambda\}_\lambda$ denote a sequence of sets such that when Π is used with a particular value of $\lambda = \lambda'$, the key space is $\mathcal{K}_{\lambda'}$ and the message space is $\mathcal{M}_{\lambda'}$.