COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 1 **due: 12:59PM, October 8th, 2019**

Ground rules:

Please format your solutions so that each problem begins on a new page, and so that your name appears at the top of each page.

You are encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of a dean. We will grade as many problems as possible, but sometimes one or two problems will not be graded. Your lowest homework grade of the semester will be dropped from your final grade.

Problems:

1. **Perfect secrecy.** Recall that an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is called *perfectly secure* if for any messages m_0, m_1 and any ciphertext c,

$$\Pr_{k \leftarrow \mathsf{Gen}}\left(\mathsf{Enc}_k(m_0) = c\right) = \Pr_{k \leftarrow \mathsf{Gen}}\left(\mathsf{Enc}_k(m_1) = c\right).$$

   Prove or disprove (giving the simplest counterexample you can find) the following statements about perfect secrecy for secret-key encryption.

   (a) Perfect secrecy is equivalent to the following definition: for any $m_0, m_1 \in \mathcal{M}$, and any function $\mathcal{A} : \mathcal{C} \to \{0,1\}$,

$$\Pr_{k \leftarrow \mathsf{Gen},\, b \leftarrow_U \{0,1\}}[\mathcal{A}(\mathsf{Enc}_k(m_b)) = b] = \frac{1}{2}.$$

   (b) There is a perfectly secret encryption scheme for which the ciphertext always reveals 99% of the bits of the key k to the adversary.

   (c) There is an encryption scheme that is not perfectly secret, yet the adversary cannot guess the key with probability greater than $1/|\mathcal{K}|$.

   (d) In a perfectly secret encryption scheme, the ciphertext is uniformly random. That is, for every $m \in \mathcal{M}$, the probability $\mathbf{Pr}_{k \leftarrow \mathsf{Gen}}(\mathsf{Enc}_k(m) = c)$ is the same for every ciphertext $c \in \mathcal{C}$.

   (e) Perfect secrecy is equivalent to the following definition, which says that the ciphertext and message are independent (as random variables). Formally, for any probability distribution $\mathcal{D}$ over the message space $\mathcal{M}$ and any $\bar{m} \in \mathcal{M}$ and $\bar{c} \in \mathcal{C}$,

$$\Pr_{m \leftarrow \mathcal{D},\, k \leftarrow \mathsf{Gen}}\left(m = \bar{m} \wedge \mathsf{Enc}_k(m) = \bar{c}\right) = \Pr_{m \leftarrow \mathcal{D}}(m = \bar{m}) \cdot \Pr_{m \leftarrow \mathcal{D},\, k \leftarrow \mathsf{Gen}}\left(\mathsf{Enc}_k(m) = \bar{c}\right).$$