COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 1 **due: 23:59PM, September 23rd, 2025**

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. If you use an AI tool to partially solve a question, or improve your write-up of a solution, then you should also mention it. All questions on the homework, including requests for clarifications or typos, should be directed to the Ed forum.

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of an academic committee.

Each of the four problem set counts for 20% of the total homework grade. (Each of the two readings will count for 10% of the final homework grade.)

The first problem discusses the notion of perfect secrecy. It does not have to do with quantum information, only the definition. The second and third problems are about quantum money. Both problems can be attempted as soon as the definition of quantum money has been given, which will be done on Tuesday 16th in class. The third problem is substantially longer than the first two and will require time, so do not start it at the last minute.

Problems:

1. (10 points) **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,

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

   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 $\bar{c} \in \mathcal{C}$,

$$\underset{m \leftarrow \mathcal{D},\, k \leftarrow \mathsf{Gen}}{\mathbf{Pr}} \big(m = \bar{m} \wedge \mathsf{Enc}_k(m) = \bar{c}\big) \;=\; \underset{m \leftarrow \mathcal{D}}{\mathbf{Pr}}(m = \bar{m}) \cdot \underset{m \leftarrow \mathcal{D},\, k \leftarrow \mathsf{Gen}}{\mathbf{Pr}} \big(\mathsf{Enc}_k(m) = \bar{c}\big) \;.$$

2. (4 points)**Measurement attacks**
Consider all cloning attacks that take the following form. The adversary decides on an arbitrary orthonormal basis $(|u_0\rangle, |u_1\rangle)$ for the single-qubit space $\mathbb{C}^2$. It then measures the challenger's state $|\psi_\$\rangle$ in the basis $(|u_0\rangle, |u_1\rangle)$ to obtain an outcome $b \in \{0,1\}$. Finally, the adversary returns the density matrix $\rho = |u_b\rangle\langle u_b| \otimes |u_b\rangle\langle u_b|$.

(a) Express the success probability of this attack as a function of the coefficients α, β of $|u_0\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. (Since $|u_1\rangle$ is orthogonal to $|u_0\rangle$, without loss of generality $|u_1\rangle = \beta\,|0\rangle - \alpha\,|1\rangle$.)

(b) Find the choice of α, β that maximizes the success probability (don't forget about complex numbers!).

(c) How does this attack compare to the ones seen in class?

3. (12 points) **Improving Wiesner's quantum money**
Consider the following six single-qubit states:

$$\Big\{\, |\psi_1\rangle = |0\rangle\,,\, |\psi_2\rangle = |1\rangle\,,\, |\psi_3\rangle = |+\rangle\,,\, |\psi_4\rangle = |-\rangle\,,\, |\psi_5\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}},\, |\psi_6\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}} \Big\}.$$

Suppose we create a money scheme in which each bit of a bill's serial number is encoded into one of these six states, chosen uniformly at random (with probability 1/6 each) by the bank.

(a) Consider the attack on this scheme which attempts to copy the bill in the standard basis, using the unitary $U : |0\rangle|0\rangle \mapsto |0\rangle|0\rangle$, $U : |1\rangle|0\rangle \mapsto |1\rangle|1\rangle$. What is its success probability? Recall that the success probability is defined as

$$\sum_{k=1}^{6} \frac{1}{6} \Big|\big(\,\langle\psi_k| \otimes \langle\psi_k|\,\big)\, U\big(\,|\psi_k\rangle \otimes |0\rangle\,\big)\Big|^2.$$

What if we choose U to copy in the Hadamard basis instead?

Consider the following map T from single-qubit quantum money states to two-qubit density matrices, where we write $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$:

$$\begin{aligned}
|0\rangle\langle 0| \mapsto \rho_0 &= \frac{2}{3}\,|00\rangle\,\langle 00| + \frac{1}{3}\,|\psi^+\rangle\langle\psi^+|\ ,\\
|1\rangle\langle 1| \mapsto \rho_1 &= \frac{2}{3}\,|11\rangle\langle 11| + \frac{1}{3}\,|\psi^+\rangle\langle\psi^+|\ ,\\
|+\rangle\langle +| \mapsto \rho_+ &= \frac{1}{12}\big(2\,|00\rangle + \sqrt{2}\,|\psi^+\rangle\big)\big(2\,\langle 00| + \sqrt{2}\,\langle\psi^+|\big)\\
&\quad + \frac{1}{12}\big(2\,|11\rangle + \sqrt{2}\,|\psi^+\rangle\big)\big(2\,\langle 11| + \sqrt{2}\,\langle\psi^+|\big)\ ,\\
|-\rangle\langle -| \mapsto \rho_- &= \frac{1}{12}\big(2\,|00\rangle - \sqrt{2}\,|\psi^+\rangle\big)\big(2\,\langle 00| - \sqrt{2}\,\langle\psi^+|\big)\\
&\quad + \frac{1}{12}\big(2\,|11\rangle - \sqrt{2}\,|\psi^+\rangle\big)\big(2\,\langle 11| - \sqrt{2}\,\langle\psi^+|\big)\ .
\end{aligned}$$

(b) Show that there exists a valid unitary operation V acting on the entire 3-qubit space $\mathbb{C}^8$ that satisfies

$$\begin{aligned}
|0\rangle_A\,|00\rangle_{BC} &\mapsto \frac{2}{\sqrt{6}}\,|00\rangle_{AB}\,|0\rangle_C + \frac{1}{\sqrt{3}}\,|\psi^+\rangle_{AB}\,|1\rangle_C\ ,\\
|1\rangle_A\,|00\rangle_{BC} &\mapsto \frac{1}{\sqrt{3}}\,|\psi^+\rangle_{AB}\,|0\rangle_C + \frac{2}{\sqrt{6}}\,|11\rangle_{AB}\,|1\rangle_C\ .
\end{aligned}$$

(c) Describe the map T as a sequence of three operations: (i) add some ancilla qubits to the single-qubit input of T; (ii) apply V; (iii) trace out a qubit. Specify what the ancilla qubits are and which qubit to trace out.

The previous questions justify that T is a valid quantum map, because it can be written as a sequence of three valid operations.

(d) Show that for any single-qubit quantum money scheme (including Wiesner's scheme seen in class, the six-state scheme described above, and any other scheme using even more states), there is a cloning attack that succeeds with probability at least $\frac{2}{3}$.

(e) (Bonus 3pts) As it turns out, the six-state scheme described above is optimal, in the sense that it is possible (but not easy) to show that the best cloning attack succeeds with probability *at most* $\frac{2}{3}$. Suggest a quantum money scheme which uses only four single-qubit states but is such that the optimal attack succeeds with probability exactly $\frac{2}{3}$ (and in particular is better than Wiesner's scheme). *[Hint: Think about the Bloch sphere — use all the available space! Partial credit given for any scheme that does better than Wiesner, together with credible evidence for it being better.]*