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. **Classical one time pad**

2. **Density matrices**

3. **Classical-quantum states**

4. **Quantum one-time pad**

   (a) Recall that a correct encryption scheme constitutes a well defined encryption function which takes a single quantum bit to a single quantum bit, E, and a well defined decryption function, D, which should operate as the inverse of E. Observe that E is well defined in the problem since $E = H^k$ and k is fixed with respect to E (we are only concerned with encrypting a single qubit). We wish to similarly define an inverse operation D. Since H is a valid quantum map over pure states, it must be a unitary transformation. Consequently, $H^{-1} = H^\dagger$. Now, notice that setting $D = (H^\dagger)^k$ will be an inverse of E,

   $$D(E(|\psi\rangle)) = (H^\dagger)^k (H)^k |\psi\rangle = (H^\dagger H)^k |\psi\rangle = \mathbb{I}^k |\psi\rangle = |\psi\rangle$$

   Thus, this encryption scheme is correct.

(b) Unfortunately for Alice, this encryption scheme is not correct. We will give an attack, described by the adversial game framework described in class. We first recollect this framework. An adversary gives Alice two qubits $\{|\psi_1\rangle, |\psi_2\rangle\}$. Alice then chooses any one of these $|\psi_i\rangle$ and a value for k, then returns to the adversary the qubit $E(|\psi_i\rangle)$. Given this qubit, the adversary final responds with which qubit was encrypted, namely responding with a $j \in \{1, 2\}$. The adversary wins if $\mathbf{Pr}[j = i] > 1/2$, otherwise Alice wins and her scheme is secure.

We describe such a winning strategy for the adversary. Recall that Alice has fixed H defining her scheme. Furthermore, we recall that the eigenvectors of H must be orthogonal since it is a unitary transformation. Denote these eigenvectors $|v_1\rangle$ and $|v_2\rangle$. Furthermore, considering their normalization makes them a set of two qubits. Now, suppose the adversary sends Alice these two qubits: $\{|v_1\rangle, |v_2\rangle\}$. Alice then chooses some k and i, and responds with $H^k |v_i\rangle$. The adversary then measures this qubit in the $\{|v_1\rangle, |v_2\rangle\}$ basis. Following this, if the adversary observes $|v_1\rangle$ he responds with $j = 1$, otherwise he must have observed $|v_2\rangle$ and in that case he responds with $j = 2$. Analyzing this scheme, observe that if $i = 1$, then $p_1 = |\langle v_1| H^k |v_1\rangle|^2 = |\langle v_1\rangle v_1|^2 = 1$ and $j = 1$ with probability 1, regardless of the value of k. Similarly, if $i = 2$ then $p_2 = |\langle v_2| H^k |v_2\rangle|^2 = |\langle v_2\rangle v_2|^2 = 1$ and $j = 2$ with probability 1. Thus we get,

$$\mathbf{Pr}[i = j] = \mathbf{Pr}[i = j \mid i = 1] \cdot \mathbf{Pr}[i = 1] + \mathbf{Pr}[i = j \mid i = 2] \cdot \mathbf{Pr}[i = 2] = \mathbf{Pr}[i = 1] + \mathbf{Pr}[i = 2] = 1 >$$

Hence, this scheme cannot be secure.

5. **State discrimination.**

6. **Unambiguous state discrimination**