CS333 - Problem Set 2

1. In your own words, describe what it is about quantum states that makes it possible for Alice and Bob to share a secret key over a public channel (a public channel is a channel where eavesdropping is possible).

2. Read The Space-Based Quantum Cryptography Race and explain (1) why scientists are trying create a quantum cryptography satellite and (2) why is it important that the error rate is below some threshold. (Update if you are interested: the Chinese satellite has been launched and was used to hold a secure video conference. See Chinese satellite uses quantum cryptography.)

3. Decide whether each of the following vectors could represent a qubit state. If not, find the positive real number such that multiplying the vector by the number will create a valid quantum qubit state.

   (a) $\begin{pmatrix} e^{i\xi}\cos(\theta) \\ e^{-i\phi}\sin(\theta) \end{pmatrix}$

   (b) $\frac{1}{2}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$

4. Is the following a valid qubit measurement? Why or why not?

$$M = \left\{ \sqrt{\frac{1}{3}}|0\rangle + i\sqrt{\frac{2}{3}}|1\rangle, \sqrt{\frac{2}{3}}|0\rangle + i\sqrt{\frac{1}{3}}|1\rangle \right\} \tag{1}$$

5. Let $M = \{|\phi_0\rangle, |\phi_1\rangle\}$ be an orthonormal basis representing a qubit measurement, and let $|\psi\rangle$ be a vector representing a qubit quantum state. For this problem, you may want to refer to the Math Practice worksheet for properties of orthonormal bases.

   (a) Explain why there exist $\alpha_0, \alpha_1 \in \mathbb{C}$ such that $|\psi\rangle = \alpha_0|\phi_0\rangle + \alpha_1|\phi_1\rangle$. Show that $|\alpha_0|^2 + |\alpha_1|^2 = 1$. See final page for hint.

   (b) Suppose we measure $|\psi\rangle$ using M. Let p_0 be the probability of outcome $|\phi_0\rangle$ and let p_1 be the probability of outcome $|\phi_1\rangle$. Use part (a) to show that $p_0 + p_1 = 1$, that is, the sum of the outcome probabilities is 1.

   (c) What does this problem tell you about quantum measurements and quantum states?

6. Let $|\psi\rangle$ be a vector representing a qubit quantum state. Let $|\psi'\rangle = e^{i\phi}|\psi\rangle$ for $\phi \in \mathbb{R}$.

   (a) Show that $|\psi'\rangle$ also represents a qubit state.

   (b) Show that any measurements give exactly the same outcome statistics and states on $|\psi\rangle$ and $|\psi'\rangle$.

(c) Is it possible to tell the difference between $|\psi\rangle$ and $|\psi'\rangle$? What have you learned about quantum states and their mathematical representations from doing this problem?

7. Now that we have a mathematical description of quantum states and measurements, we can reinterpret our cryptographic scenarios using these mathematical descriptions (in particular using ket notation). Please use ket notation to describe the following scenarios. If applicable, calculate the probability of different possible outcomes:

   - Alice prepares a horizontally polarized photon and sends to Bob.
   - Eve intercepts the photon and has it pass through a vertically polarized filter before trying to detect the photon. If she detects a photon, she prepares a vertically polarized photon to send to Bob, and otherwise, she sends Bob a horizontally polarized photon. (Calculate the probability of each outcome occuring using our mathematical tools.)
   - Bob measures the photon he received from Eve by putting a right diagonally polarized filter in front of his photon detector. What outcomes does he get, and with what probability?

8. How long did you spend on this homework?

5a: try taking the inner product of $|\psi\rangle$ with itself. What value should this inner product take?