Part 2: Quantum cryptography and quantum information theory (10 points)

Notations. $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. For two quantum mixed states ρ, σ, their trace distance is defined as $\Delta(\rho,\sigma) = \frac{1}{2}tr(\sqrt{(\rho-\sigma)(\rho-\sigma)^\dagger})$.

Question 3: Encoding of a bit b in two different ways (2 points)

Alice has a random bit $b \in \{0,1\}$ unknown to Bob. Consider the two following states

$$|\psi_0\rangle = \sqrt{\frac{2}{3}}|00\rangle_{XY} + \sqrt{\frac{1}{3}}|11\rangle_{XY}$$
$$|\psi_1\rangle = \sqrt{\frac{1}{3}}|0+\rangle_{XY} + \sqrt{\frac{1}{3}}|1-\rangle_{XY} + \sqrt{\frac{1}{3}}|20\rangle_{XY}$$

1. Assume Alice sends $\rho_b = Tr_X(|\psi_b\rangle\langle\psi_b|)$ to Bob. Show that this doesn't give him any information about b.
2. Assume Alice sends $|\psi_b\rangle$ to Bob. What is Bob's optimal probability of guessing b?

Question 4: Quantum Key Distribution with different states (6 points)

Fix any $\theta \in [0, \pi/2]$, we consider the unitary operation $U_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$. For $i \in \{0,1\}$, we define $|e_i\rangle = U_\theta|i\rangle$. We consider the two basis $B_0 = \{|0\rangle, |1\rangle\}$ and $B_1 = \{|e_0\rangle, |e_1\rangle\}$; Finally, let $|\psi_k^b\rangle = U_\theta^b|k\rangle$. We consider the variant of the BB-84 protocol where Alice wants to encode a bit k using basis b meaning she sends $|\psi_k^b\rangle$ to Bob.

1. Write $|e_0\rangle, |e_1\rangle$ as a function of θ.
2. To what value of θ does the standard BB-84 encoding seen in class correspond to?
3. Let ρ_b be the state received for a fixed basis b. This means we can write $\rho_b = \frac{1}{2}\left(|\psi_0^b\rangle\langle\psi_0^b| + |\psi_1^b\rangle\langle\psi_1^b|\right)$. Show that for any $\theta \in [0, \pi/2]$, one can guess b from ρ_b with probability at most $\frac{1}{2}$.
4. Let σ_k be the state received for a fixed bit k. This means we can write $\sigma_k = \frac{1}{2}\left(|\psi_k^0\rangle\langle\psi_k^0| + |\psi_k^1\rangle\langle\psi_k^1|\right)$. Our goal is to compute the probability of guessing k from σ_k.
   (a) For any two 1 qubit mixed states σ_0, σ_1 such that $\sigma_0 - \sigma_1 = \begin{pmatrix} A & B \\ B & -A \end{pmatrix}$ with $A, B \in \mathbb{R}$, show that $\Delta(\sigma_0, \sigma_1) = \sqrt{A^2 + B^2}$.
   (b) Show that in our case, $\Delta(\sigma_0, \sigma_1) = \cos(\theta)$ and conclude. *(Hint: One can use in the calculations* $(1 + \cos^2(\theta) + \sin^2(\theta))^2 = 4$ *and derive a simpler value for* $(1 + \cos^2(\theta) - \sin^2(\theta))^2$*)*
5. The above shows that for $\theta = \pi/2$, the receiver gets no information about k as well. Can you see a problem in using $\theta = \pi/2$ in the BB-84 key distribution protocol? How can the eavesdropper perfectly cheat in this setting?

Question 5: The Billion Dollar Company (1 point for an informal argument + 1 point for formal proof of failure)

The company SuperQuantum3000 offers a new storing device that can store $n \geq 2$ bits in a single qubit. Consider the string $\mathbf{b} = (b_1, \ldots, b_n) \in \{0,1\}^n$. Let also $\omega = e^{\frac{2i\pi}{2^n}}$. The idea of the company is to store $\mathbf{b}$ in the qubit

$$|\psi_{\mathbf{b}}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \omega^{\mathbf{b}}|1\rangle\right) \quad \text{where we interpret } \mathbf{b} \text{ as a number in } [0, 2^n - 1].$$

From $|\psi_{\mathbf{b}}\rangle$, one can easily recover $\mathbf{b}$ from the amplitude $\omega^{\mathbf{b}}$ of $|\psi_{\mathbf{b}}\rangle$. What is wrong with this approach? Show the limitations of this encoding.