COM-440, Introduction to Quantum Cryptography, Fall 2025

Final **due: October 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.

The total points value of the problems is 25 points. Your midterm grade will be the *minimum* of your total points number and *20*. This means that we do not expect you to solve all problems. Instead, we encourage you to spend the first 5-10 minutes looking at all problems and deciding which ones to attempt. Your goal is to collect as close to 20 points as possible in total, not necessarily to solve all questions.

Problems:

1. **A Simple Quantum Bit Commitment Protocol**

   (a) $\rho_b = \mathrm{Tr}_1(|\psi_b\rangle\langle\psi_b|) = \alpha\,|b\rangle\langle b| + (1-\alpha)\,|2\rangle\langle 2|$.

   (b) Recall that the optimal probability with which Bob can distinguish between two states ρ and σ is $\frac{1}{2} + \frac{1}{4}\|\rho - \sigma\|_{tr}$. In our protocol, Bob's cheating probability is the optimal probability with which he can distinguish between Alice commiting to 0 or to 1, i.e. between ρ_0 and ρ_1. So

$$P_B^* = \frac{1}{2} + \frac{1}{4}\|\rho_0 - \rho_1\| = \frac{1}{2} + \frac{\alpha}{4}\|\,|0\rangle\langle 0| - |1\rangle\langle 1|\,\|_{tr} = \frac{1}{2} + \frac{\alpha}{2}\,.$$

   (c) The probability that Alice successfully opens bit b equals the probability that she passes Bob's check for b at the end of the protocol, i.e. that Bob measures his part of the joint state and gets the honest $|\psi_b\rangle$ as the outcome:

$$\begin{aligned}\mathbf{Pr}(\text{Alice successfully opens } b) &= \sum_i p_i |\langle\psi_b|\tilde{\psi_{i,b}}\rangle|^2 \\ &= F^2(\sigma_b, |\psi_b\rangle\langle\psi_b|)\,.\end{aligned}$$

   Now, tracing out the system $\mathcal{H}_s$, and using the fact that the fidelity is non-decreasing under taking partial trace, we have

$$\begin{aligned}\mathbf{Pr}(\text{Alice successfully opens } b) &\leq F^2\Big(Tr_{\mathcal{H}_s}(\sigma_b), \mathrm{Tr}_{\mathcal{H}_s}(|\psi_b\rangle\langle\psi_b|)\Big) \\ &= F^2(\sigma, \rho_b)\,.\end{aligned}$$

   Hence

$$P_A^* \leq \frac{1}{2}\big(F^2(\sigma,\rho_0) + F^2(\sigma,\rho_1)\big)\,.$$

(d) From the previous problem we have that $P_A^* \leq \frac{1}{2}\Big(F^2(\sigma,\rho_0) + F^2(\sigma,\rho_1)\Big)$.
Applying the bound in the hint, we have $P_A^* \leq \frac{1}{2}\Big(1 + F(\rho_0,\rho_1)\Big)$.
Now, one can compute $F(\rho_0,\rho_1) = 1-\alpha$. So, substituting gives $P_A^* \leq 1 - \frac{\alpha}{2}$.

(e) When solving question 3, you found that

$$\mathbf{Pr}(\text{Alice successfully opens b}) = F^2(\sigma_b, |\psi_b\rangle\langle\psi_b|) \ .$$

Now, when Alice dishonestly prepares the state $|\psi_0\rangle + |\psi_1\rangle$ normalized, the fidelity is between two pure states. Thus,

$$\mathbf{Pr}(\text{Alice successfully opens b}) = \Big|\left(\langle\psi_0| + \langle\psi_1|\right)|\psi_b\rangle\Big|^2 / \Big\| \, |\psi_0\rangle + |\psi_1\rangle \, \Big\|^2 \ .$$

Now, one can easily compute $\| \, |\psi_0\rangle + |\psi_1\rangle \, \|^2 = 2(2-\alpha)$, and $|\, \langle\psi_0| + \langle\psi_1| \, |\psi_b\rangle \, |^2 = (2-\alpha)^2$. Clearly, by symmetry

$$\mathbf{Pr}(\text{Alice successfully opens 0}) = \mathbf{Pr}(\text{Alice successfully opens 1}) \ .$$

Hence,

$$P_A^* = \frac{(2-\alpha)^2}{2(2-\alpha)} = 1 - \frac{\alpha}{2} \ , \tag{1}$$

which achieves the upper bound. With similar calculations, one can check that options II and III do not achieve the upper bound.

(f) To minimize the cheating probability, one just needs to pick α such that $P_A^* = P_B^*$, i.e. $\frac{1}{2}(1+\alpha) = 1 - \frac{\alpha}{2}$.
Solving for α gives $\alpha = \frac{1}{2}$, which implies $P_A^* = P_B^* = \frac{3}{4}$. And the latter is the cheating probability.