COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise Solution # 10

1. **A Weak Coin Flipping Protocol**

   (a) We see from the description of steps 3 and 4 that when Alice and Bob are honest, they always both return the same outcome $c = a \oplus b$. Since a and b are both chosen uniformly at random, c is also uniformly random. Therefore, the protocol is correct.

   (b) Bob's reduced density matrix after step 1 is

   $$\rho_a = \mathrm{Tr}_A(|\psi_a\rangle\langle\psi_a|) = \frac{1}{2}\mathrm{Tr}_A\big((|0\rangle|\psi_{a,0}\rangle + |1\rangle|\psi_{a,1}\rangle)(\langle 0|\langle\psi_{a,0}| + \langle 1|\langle\psi_{a,1}|)\big)$$
   $$= \frac{1}{2}(|\psi_{a,0}\rangle\langle\psi_{a,0}| + |\psi_{a,1}\rangle\langle\psi_{a,1}|)\ .$$

   Simplifying the latter gives

   $$\rho_a = \cos^2(\frac{\alpha}{2})\,|0\rangle\langle 0| + \sin^2(\frac{\alpha}{2})\,|a+1\rangle\langle a+1|\ .$$

   (c) Recalling the interpretation of the fidelity as the square root of the probability that Alice can convince Bob that a state is another. Hence the probability that Alice wins given that Bob sent b is precisely $F^2(\sigma_b, |\psi_b\rangle\langle\psi_b|)$, and this can be upper bounded (tracing out the qubit system) by $F^2(\sigma, \rho_b)$.

   (d)

   $$\mathbf{Pr}(\text{Alice wins}) = \frac{1}{2}\big(\mathbf{Pr}(\text{Alice wins}|b=0) + \mathbf{Pr}(\text{Alice wins}|b=1)\big)$$
   $$\leq \frac{1}{2}\big(F^2(\sigma,\rho_0) + F^2(\sigma,\rho_1)\big)\ .$$

   Using the fact from the hint we get

   $$\mathbf{Pr}\left(\text{Alice wins}\right) \leq \frac{1}{2}\big(1 + F(\rho_0,\rho_1)\big)\ .$$

   Finally, we can calculate $F(\rho_0,\rho_1) = \|\sqrt{\rho_0}\sqrt{\rho_1}\|_{tr} = \cos^2(\frac{\alpha}{2})$, which gives us the desired bound.

   (e) The state possessed by Alice after Bob has applied U and returned his qutrit to Alice is

   $$id \otimes U\,|\psi_a\rangle = id \otimes U\frac{1}{\sqrt{2}}(|0\rangle|\psi_{a,0}\rangle + |1\rangle|\psi_{a,1}\rangle)\ ,$$

   which is

   $$\frac{1}{\sqrt{2}}\Big(\,|0\rangle\left(\cos\frac{\alpha}{2}\,|\xi_{0,\bar{a}}\rangle + \sin\frac{\alpha}{2}\,|\xi_{a+1,\bar{a}}\rangle\right) + |1\rangle\left(\cos\frac{\alpha}{2}\,|\xi_{0,\bar{a}}\rangle - \sin\frac{\alpha}{2}\,|\xi_{a+1,\bar{a}}\rangle\right)\Big)\ .$$

The probability of Bob winning, given that Alice has picked a, is the modulus squared of the overlap between the honest state $|\psi_a\rangle$ expected by Alice and the state after Bob's unitary, that is

$$\begin{aligned}
\Big| \langle\psi_a| \otimes id \cdot \frac{1}{\sqrt{2}}\Big(|0\rangle \Big(\cos\frac{\alpha}{2} |\xi_{0,\bar{a}}\rangle + \sin\frac{\alpha}{2} |\xi_{a+1,\bar{a}}\rangle \Big) \\
+ |1\rangle \Big(\cos\frac{\alpha}{2} |\xi_{0,\bar{a}}\rangle - \sin\frac{\alpha}{2} |\xi_{a+1,\bar{a}}\rangle \Big)\Big)\Big|^2 \\
= \frac{1}{4}\Big| \langle\psi_{a,0}| \otimes I\Big(\cos\frac{\alpha}{2} |\xi_{0,\bar{a}}\rangle + \sin\frac{\alpha}{2} |\xi_{a+1,\bar{a}}\rangle \Big) \\
+ \langle\psi_{a,1}| \otimes I\Big(\cos\frac{\alpha}{2} |\xi_{0,\bar{a}}\rangle - \sin\frac{\alpha}{2} |\xi_{a+1,\bar{a}}\rangle \Big)\Big|^2 .
\end{aligned}$$

Substituting the definitions of $|\psi_{a,0}\rangle$ and $|\psi_{a,1}\rangle$ gives, after simplification,

$$\mathbf{Pr}(\text{Bob wins} \mid \text{Alice sent } a) = |\cos^2\frac{\alpha}{2} \langle 0| \otimes I\, |\xi_{0,\bar{a}}\rangle + \sin^2\frac{\alpha}{2} \langle a+1| \otimes I\, |\xi_{a+1,\bar{a}}\rangle\, |^2 .$$

(f) Yes, it should be!

(g) You are told that

$$\mathbf{Pr}(\text{Bob wins}|\text{Alice picked } a) \leq \Big(\cos^2(\frac{\alpha}{2}) \|\, |\xi_{0,\bar{a}}\rangle \,\| + \sin^2(\frac{\alpha}{2}) \Big)^2 .$$

You can bound $\mathbf{Pr}$(Bob wins) by averaging the latter bound over $a \in \{0,1\}$. This is maximized when $\|\, |\xi_{0,0}\rangle \,\| = \|\, |\xi_{0,1}\rangle \,\| = \frac{1}{\sqrt{2}}$ (recall that $\|\, |\xi_{0,0}\rangle \,\|^2 + \|\, |\xi_{0,1}\rangle \,\|^2 = 1$). Thus, $\mathbf{Pr}$(Bob wins) is bounded by $\Big(\frac{1}{\sqrt{2}}\cos^2(\frac{\alpha}{2}) + \sin^2(\frac{\alpha}{2})\Big)^2$.

(h) The bias is minimized by choosing α that makes Alice and Bob's probabilities of dishonestly winning equal. That is, from the tight bounds found earlier, α such that

$$\frac{1}{2}(1 + \cos^2\frac{\alpha}{2}) = \Big(\frac{1}{\sqrt{2}} \cos^2\frac{\alpha}{2} + \sin^2\frac{\alpha}{2} \Big)^2 .$$

Solving for α makes the two sides equal to 0.739, i.e. no player can win with probability greater than 0.739. Thus the bias is 0.239.

2. **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,

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

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.