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

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

which is

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

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 conditioned on that Bob sends back $\bar{a}$, that is

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

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

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

(f) Yes, it should be!

$$\begin{aligned}
&|\cos^2\frac{\alpha}{2}\langle 0|\otimes\mathbb{I}\,|\xi_{0,\bar{a}}\rangle + \sin^2\frac{\alpha}{2}\langle a+1|\otimes\mathbb{I}\,|\xi_{a+1,\bar{a}}\rangle|^2 \\
&\le \left(\cos^2\frac{\alpha}{2}|\langle 0|\otimes\mathbb{I}\,|\xi_{0,\bar{a}}\rangle| + \sin^2\frac{\alpha}{2}|\langle a+1|\otimes\mathbb{I}\,|\xi_{a+1,\bar{a}}\rangle|\right)^2 \\
&\le \left(\cos^2\frac{\alpha}{2}\|\,|\xi_{0,\bar{a}}\rangle\,\| + \sin^2\frac{\alpha}{2}\right)^2 .
\end{aligned}$$

(g) You are told that

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

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

(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

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

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.