COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise # 10

This exercise sheet is designed to help you review the concepts discussed in the lecture and explore some additional interesting results that were not covered in the lecture. Exercises marked with * will have solutions provided after the exercise session, while those marked with ⧫ will be the main focus during the exercise session. You are encouraged to discuss with other students, and ask for help if you get stuck for too long.

1. **A Weak Coin Flipping Protocol** In class we studied a strong quantum coin flipping protocol with bias 1/4. In this problem you'll see how a variation of that same protocol allows to construct a weak coin flipping protocol with bias smaller than 1/4.
   Recall that in a weak coin flipping protocol, if the outcome is c then we define Alice's cheating probability as $P_A^* = Pr[c = 0]$, maximized over Alice's (cheating) strategies, and similarly $P_B^* = Pr[c = 1]$ for Bob. We say that the cheating probability of the protocol is $\max\{P_A^*, P_B^*\}$. The protocol in this problem is parametrised by $\alpha \in [0, \pi]$, over which you'll optimise later on.
   For $a, x \in \{0, 1\}$, define the qutrit state $|\psi_{a,x}\rangle$ in the space $\mathcal{H}_t = \mathbb{C}^3$ as

   $$|\psi_{a,x}\rangle = \cos(\frac{\alpha}{2})\,|0\rangle + \sin(\frac{\alpha}{2})(-1)^x\,|a+1\rangle \tag{1}$$

   and $|\psi_a\rangle \in \mathcal{H}_s \otimes \mathcal{H}_t = \mathbb{C}^2 \otimes \mathbb{C}^3$ as

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

   The protocol is as follows.

   - Alice picks $a \in_R \{0, 1\}$, prepares the state $|\psi_a\rangle \in \mathcal{H}_s \otimes \mathcal{H}_t$ (i.e. a state of one qubit and one qutrit) and sends to Bob the right half of the state (the qutrit).
   - Bob picks $b \in_R \{0, 1\}$ and sends it to Alice.
   - Alice reveals the bit a to Bob. Let $c = a \oplus b$. If $c = 0$, then Alice sets $c_A = 0$ and sends to Bob the other part of the state $|\psi_a\rangle$ (the qubit). Bob checks that the qutrit-qubit pair he received is indeed in the state $|\psi_a\rangle$ (by making a measurement with respect to any orthogonal basis of $\mathcal{H}_s \otimes \mathcal{H}_t$ containing $|\psi_a\rangle$). If the test is passed, Bob sets $c_b = 0$, and so Alice wins the game. Else Bob concludes that Alice has deviated from the protocol, and aborts.
   - If, on the other hand, $c = a \oplus b = 1$, then Bob sets $c_B = 1$, and returns the qutrit he received in round 1. Alice checks that her qubit-qutrit pair is in state $|\psi_a\rangle$. If the test is passed, she sets $c_A = 1$, so Bob wins the game. Else Alice concludes that Bob has tampered with her qutrit to bias the game, and aborts.

(a) Verify that this protocol satisfies correctness.

(b) What is Bob's reduced density matrix ρ_a after step 1, in the case that Alice has prepared the honest state $|\psi_a\rangle$? (Note that the subscript a refers to the classical bit and not the system of Alice or Bob!)

Now, suppose Bob is honest while Alice may cheat. We aim to obtain a (tight) upper bound on Alice's winning probability. The most general strategy is for Alice to prepare a pure state $|\phi\rangle \in \mathcal{H} \otimes \mathcal{H}_s \otimes \mathcal{H}_t$, where $\mathcal{H}$ is an ancillary space (one can always purify the state via $\mathcal{H}$). Then she sends the qutrit part in $\mathcal{H}_t$ to Bob, and keeps the part of the state in $\mathcal{H} \otimes \mathcal{H}_s$.

We can assume without loss of generality that in step 3 of the protocol Alice always replies with $a = b$ (so that $c = 0$), and consequently tries to pass Bob's check. For this, she performs an arbitrary unitary U_b on her part of $|\phi\rangle$, so that she gets $|\phi_b\rangle = (U_b \otimes I)|\phi\rangle$, and then sends the qubit in $\mathcal{H}_s$ to Bob. The final joint state can then be written as $|\phi_b\rangle = \sum_i \sqrt{p_i}\,|i\rangle\,|\phi_{i,b}\rangle$ for some $\{p_i\}$ and Schmidt bases $\{|i\rangle\}$ of $\mathcal{H}$ and $\{|\phi_{i,b}\rangle\}$ of $\mathcal{H}_s \otimes \mathcal{H}_t$.

Let σ_b be the density matrix of Bob's qubit-qutrit pair at the end of the protocol. And let σ be Bob's reduced density matrix after the first step of the protocol (i.e. just the qutrit).

(c) Show that the probability that Alice wins given that Bob sent b is at most $F^2(\sigma, \rho_b)$, with $F(\cdot,\cdot)$ the fidelity (here ρ_b is defined as in (b)). *[Hint: express it first in terms of the fidelity of two density matrices and then use the fact that fidelity is non-decreasing under taking partial trace.]*

(a) Use the above to bound the probability that Alice wins. *[Hint: You might find useful the fact that for any three density matrices σ, ρ_0, ρ_1, it holds that $F^2(\sigma, \rho_0) + F^2(\sigma, \rho_1) \leq 1 + F(\rho_0, \rho_1)$.]*

Now we turn to Bob's winning probability when he is potentially cheating and Alice is honest. He will be trying to infer as much as he can about the value of the bit a, so that he can send back a bit b such that $a \oplus b = 1$, at the same trying to cause as little disturbance as possible to the joint state $|\psi_a\rangle$, so as to pass Alice's final check. The most general strategy that he can employ is to perform a unitary U on the space $\mathcal{H}_t \otimes \mathcal{H} \otimes \mathbb{C}^2$ of the qutrit he received from Alice, some ancillary qubits and a qubit reserved for his reply. And then measure the last qubit and send the outcome as b to Alice.

Suppose without loss of generality that the unitary is such that

$$U : |i\rangle\,|\bar{0}\rangle\,|0\rangle \mapsto |\xi_{i,0}\rangle\,|0\rangle + |\xi_{i,1}\rangle\,|1\rangle \tag{3}$$

where $|\bar{0}\rangle$ is the initial state of the ancilla qubits, and for some states $|\xi_{i,0}\rangle, |\xi_{i,1}\rangle$, not necessarily orthogonal, such that $\|\xi_{i,0}\|^2 + \|\xi_{i,1}\|^2 = 1$.

(a) Calculate the probability that Bob wins given that Alice sent a. Simplify the expression you find using the definitons of $|\psi_{a,0}\rangle$ and $|\psi_{a,1}\rangle$.

(b) Verify that the expression found in the previous question is upper bounded by

$$\Big(\cos^2(\frac{\alpha}{2})\|\xi_{0,\bar{a}}\| + \sin^2(\frac{\alpha}{2})\Big)^2 .$$

(c) Use the above mentioned bound to calculate an upper bound for the probability that Bob wins, and maximise it over the choice of $|\xi_{0,0}\rangle$ and $|\xi_{0,1}\rangle$.

(d) Determine the value of the parameter α that minimizes the overall bias of the protocol. What is the bias?

2. **A Simple Quantum Bit Commitment Protocol**
As you know, perfectly secure quantum bit commitment is impossible. Nonetheless, it is possible to construct protocols in which Alice and Bob can cheat to some extent, but not completely.
For a cheating Alice and honest Bob, we define Alice's cheating probability as

$$P_A^* = \frac{1}{2}\big(\,\mathbf{Pr}[\text{Alice opens } b = 0 \text{ successfully}] + \mathbf{Pr}[\text{Alice opens } b = 1 \text{ successfully}]\big) ,$$

maximized over Alice's (cheating) strategies. For a cheating Bob and an honest Alice, instead, we let Bob's cheating probability be

$$P_B^* = \mathbf{Pr}[\text{Bob guesses b after the commit phase}] ,$$

maximized over Bob's (cheating) strategies. The cheating probability of the protocol as a whole is then defined as $\max\{P_A^*, P_B^*\}$. In this question, we introduce a simple example of such a protocol:

- *Commit phase*: Alice commits to bit b by preparing the state

$$|\psi_b\rangle = \sqrt{\alpha}\,|bb\rangle + \sqrt{1-\alpha}\,|22\rangle$$

and Alice sends the second qutrit to Bob. Here, $0 \leq \alpha \leq 1$ is a parameter that we will optimize over at the end.

- *Open phase*: Alice reveals the classical bit b and sends the first qutrit over to Bob, who checks that the pure state is the correct one by making a measurement with respect to any orthogonal basis containing $|\psi_b\rangle$.

(a) What is the density matrix ρ_b that Bob has after the *commit phase* if Alice has committed to bit b and honestly prepared state $|\psi_b\rangle$?

(b) Compute Bob's cheating probability P_B^* by recalling the operational interpretation of the trace distance.

Next, let's calculate Alice's cheating probability. Let the underlying Hilbert space be $\mathcal{H} \otimes \mathcal{H}_s \otimes \mathcal{H}_t$, where $\mathcal{H}_t$ corresponds to the qutrit that is sent to Bob in the commit phase, $\mathcal{H}_s$ to the qutrit that is sent during the opening phase, and $\mathcal{H}$ is any auxiliary system that Alice might use. For the most general strategy, we can assume that she prepares the pure state $|\phi\rangle$, as it can always be purified on $\mathcal{H}$.
We can write $|\phi\rangle = \sum_i \sqrt{p_i} |i\rangle |\tilde{\psi_{i,b}}\rangle$ where $\{|i\rangle\}$ and $\{|\tilde{\psi_{i,b}}\rangle\}$ are vectors obtained from the Schmidt decomposition across $\mathcal{H}$ and $\mathcal{H}_s \otimes \mathcal{H}_t$ respectively. So, the reduced density matrix on $\mathcal{H}_s \otimes \mathcal{H}_t$ is $\sigma_b = \sum_i p_i |\tilde{\psi_{i,b}}\rangle \langle\tilde{\psi_{i,b}}|$. Moreover, let σ be Bob's reduced density matrix after the commit phase, i.e. just a qutrit.

(c) Compute the probability of dishonest Alice successfully opening bit b in terms of the fidelity of two density matrices, and hence give an upper bound on Alice's cheating probability. *[Hint: use the fact that the fidelity is non-decreasing under taking partial trace, in particular tracing out system $\mathcal{H}_s$.]*

(d) Give an upper bound to Alice's cheating probability in terms of α. *[Hint: You might find useful the inequality $F^2(\rho_1, \rho_2) + F^2(\rho_1, \rho_3) \leq 1 + F(\rho_2, \rho_3)$ for arbitrary density matrices ρ_1, ρ_2, ρ_3.]*

Note that the bound on Bob's cheating probability that you obtained in (b) is tight, since it is the best possible probability of distinguishing between two known states, and he knows what the two states are when Alice is honest.
Importantly, the bound on Alice's cheating probability that we obtained in (d) is also tight. There is a simple cheating strategy that allows Alice to achieve this bound, without even making use of the ancillary system $\mathcal{H}$.

(e) Which of the following states of two qutrits can Alice prepare?

   i. $|\psi_0\rangle + |\psi_1\rangle$, normalized.

   ii. $|\psi_0\rangle - |\psi_1\rangle$, normalized.

   iii. $|\psi_0\rangle + \frac{\sqrt{3}}{2} |\psi_1\rangle$, normalized.

(f) By combining the calculations so far on Alice and Bob's cheating probabilities, determine the α that minimizes the overall cheating probability $\max\{P_A^*, P_B^*\}$ of the protocol.