

# 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  $P_A^* = \mathbf{Pr}[c = 0]$ , maximized over Alice's (cheating) strategies, and similarly  $P_B^* = \mathbf{Pr}[c = 1]$  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

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

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

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

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  $\rho_a$  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  $\sigma_b$  be the density matrix of Bob's qubit-qutrit pair at the end of the protocol. And let  $\sigma$  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  $\rho_b$  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.]*
- (d) Use the above to bound the probability that Alice wins. *[Hint: You might find useful the fact that for any three density matrices  $\sigma, \rho_0, \rho_1$ , 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

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

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

- (e) Calculate the probability that Bob wins given that Alice sent  $a$ . Simplify the expression you find using the definitions of  $|\psi_{a,0}\rangle$  and  $|\psi_{a,1}\rangle$ .
- (f) Verify that the expression found in the previous question is upper bounded by

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

- (g) 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  $|\xi_{0,1}\rangle$ .
- (h) Determine the value of the parameter  $\alpha$  that minimizes the overall bias of the protocol. What is the bias?