

# 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. Optimal qubit strategies in the CHSH game.**

*This problem is a little harder. It will be graded, but it is ok if you are not able to complete it. You should still read it, as the result of the problem is used in the following problem.*

The goal of this problem is to evaluate the maximum success probability that can be achieved in the CHSH game by players sharing a two-qubit entangled state of the form

$$|\psi_\theta\rangle_{AB} = \cos(\theta) |0\rangle_A |0\rangle_A + \sin(\theta) |1\rangle_A |1\rangle_B, \quad (1)$$

where  $\theta \in [0, \pi/4]$  (other values of  $\theta$  can be reduced to this case by simple change of basis or phase flip). Having fixed the state, what are the optimal measurements for the players, and what is their success probability?

We will assume the players each makes a basis measurement on their qubit. Recall that an observable  $O$  is a  $2 \times 2$  matrix with complex entries such that  $O$  is Hermitian ( $O^\dagger = O$ ) and squares to identity ( $O^2 = \mathbb{I}$ ). For any single-qubit basis measurement  $\{|u_0\rangle, |u_1\rangle\}$ , there is an associated observable  $O = |u_0\rangle\langle u_0| - |u_1\rangle\langle u_1|$ . Conversely, any observable that is not  $\pm\mathbb{I}$  has two non-degenerate eigenvalues  $+1$  and  $-1$ , so we can uniquely identify it with a basis.

To reduce the number of cases to consider we first make a few symmetry observations.

- (a) Let  $O$  be a single-qubit observable such that  $O$  is non-degenerate ( $O \neq \pm\mathbb{I}$ ). Show that there exists real numbers  $\alpha, \beta, \gamma$  such that  $\alpha^2 + \beta^2 + \gamma^2 = 1$  and  $O = \alpha X + \beta Y + \gamma Z$ , with  $X, Y, Z$  the standard Pauli matrices.
- (b) Let  $\mathcal{B} = A_0 \otimes B_0 + A_1 \otimes B_0 + A_0 \otimes B_1 - A_1 \otimes B_1$ . Show that the success probability of the strategy in the CHSH game is  $p_s = \frac{1}{2} + \frac{1}{4} \langle \psi_\theta | \mathcal{B} | \psi_\theta \rangle$ .

- (c) Argue that for the purposes of computing the maximum success probability in the CHSH game of players using state  $|\psi_\theta\rangle_{AB}$  as in (1) we may without loss of generality restrict our attention to observables of the form  $A_x = \cos(\alpha_x)X + \sin(\alpha_x)Y$  and  $B_y = \cos(\beta_y)X + \sin(\beta_y)Y$  for some angles  $\alpha_x, \beta_y \in [0, 2\pi)$ . [Hint: do a rotation on the Bloch sphere.]

Based on the symmetry argument from the previous questions we have reduced our problem to understanding the maximum value that  $\langle\psi_\theta|\mathcal{B}|\psi_\theta\rangle$  can take, when  $|\psi_\theta\rangle$  is as in (1) and  $\mathcal{B}$  is defined from observables  $A_x, B_y$  as in (b). To understand this maximum value we compute the spectral decomposition of  $\mathcal{B}$ .

- (d) Show that  $(Z \otimes \mathbb{I})\mathcal{B}(Z \otimes \mathbb{I}) = (\mathbb{I} \otimes Z)\mathcal{B}(\mathbb{I} \otimes Z) = -\mathcal{B}$ . [Hint: use the special form of  $A_x$  and  $B_y$  you obtained from question (b).]
- (e) Show that  $\mathcal{B}$  has a basis of eigenvectors of the form  $|\phi_{ab}\rangle = e^{i\theta_{ab}}|ab\rangle + |\bar{a}\bar{b}\rangle$ , where  $a, b \in \{0, 1\}$  and  $\bar{a} = 1 - a$ ,  $\bar{b} = 1 - b$ . Note that up to local rotations this is the Bell basis.
- (f) Write  $\mathcal{B}^2$  as a  $4 \times 4$  matrix depending on the angles  $\alpha_x, \beta_y$ , and show that  $\text{Tr}(\mathcal{B}^2) \leq 16$ .
- (g) Show that the largest success probability achievable in the CHSH game using  $|\psi_\theta\rangle_{AB}$  is at most  $\frac{1}{2} + \frac{1}{4}\sqrt{1 + \sin(2\theta)}$ . [Hint: Decompose  $|\psi_\theta\rangle$  in the eigenbasis of  $\mathcal{B}$ . Use (f) and the symmetries from (d) to bound the bound the success probability via the expression found in (b).]
- (h) Give a strategy for the players which achieves this value, i.e. specify the players' observables.

## 2. Trading success probability for randomness in the CHSH game.

The goal of this problem is to show that, if players succeed with higher and higher probability in the CHSH game then Alice's outputs in the game must contain more and more randomness.

- (a) Suppose that Alice and Bob play the CHSH game using a two-qubit entangled state  $|\psi_\theta\rangle_{AB}$  as in (1). Let  $p_\theta(a|x)$  be the probability that, in this strategy, Alice returns answer  $a \in \{0, 1\}$  to question  $x \in \{0, 1\}$ . Show that  $\max_{a,x} p_\theta(a|x) \leq \cos(2\theta)$ .
- (b) Let  $p_s = \frac{1}{2} + \frac{1}{4}I$  be the players' success probability in CHSH, where  $I \in [-2, 2]$ . Using (g) from the previous problem, deduce from (a) that

$$\forall a, x \in \{0, 1\}, \quad p_\theta(a|x) \leq \frac{1}{2} \left( 1 + \sqrt{2 - \frac{I^2}{4}} \right).$$

- (c) Suppose now the players use any single-qubit strategy (not necessarily using  $|\psi_\theta\rangle$ ). Prove a lower bound on the conditional min-entropy  $H_{\min}(A|X = x)$ , for any  $x \in \{0, 1\}$ , that is generated in Alice's outputs, as a function of the players' success probability in the CHSH game.

- (d) Show that the bound from (b) is tight: for any  $\theta \in [0, \pi/4]$  find a strategy for the players using  $|\psi_\theta\rangle$  such that  $\max_{a,x} p_\theta(a|x) = \frac{1}{2}(1 + \sqrt{2 - I^2/4})$ .

### 3. 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

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

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

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

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  $\rho_b$  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  $\sigma$  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  $\alpha$ . *[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  $\rho_1, \rho_2, \rho_3$ .]*

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  $\alpha$  that minimizes the overall cheating probability  $\max\{P_A^*, P_B^*\}$  of the protocol.