COM-440, Introduction to Quantum Cryptography, Fall 2025

Final   **date: January 13th, 2026**

Please format your solutions so that each problem begins on a new page, and so that your SCIPER appears at the top of each page.

The final has 13 short questions, to be handed in on this sheet of paper (total: 6.5pts) and 3 problems to be handed in on your own paper (total: 16pts), for a total of 8 single-sided sheets of paper. Your total out of 22.5 points will be scaled down to a grade out of 20 which will constitute your final grade.

1 Short questions

Circle the correct answer directly on this sheet of paper, and turn it in with your SCIPER number clearly marked at the top. *(1/2pt per question)*

1. Alice encodes a single qubit in state $|\psi\rangle$ using the quantum one-time pad. An adversary Eve has no information at all about Alice's two key bits k_1 and k_2. What is the state of the encoded qubit from the point of view of Eve?

   (a) $\rho = \frac{1}{2}\left(|\psi\rangle\langle\psi| + XZ\,|\psi\rangle\langle\psi|\,ZX\right)$

   (b) $\rho = \frac{\mathbb{I}}{2}$

   (c) $\rho = X^{k_1} Z^{k_2}\,|\psi\rangle\langle\psi|\,Z^{k_2} X^{k_1}$

2. In the same setup, what is the state of the encoded qubit as seen by a third party Bob, who does know the key bits k_1 and k_2?

   (a) $\rho = \frac{1}{2}\left(|\psi\rangle\langle\psi| + XZ\,|\psi\rangle\langle\psi|\,ZX\right),$

   (b) $\rho = \frac{\mathbb{I}}{2},$

   (c) $\rho = X^{k_1} Z^{k_2}\,|\psi\rangle\langle\psi|\,Z^{k_2} X^{k_1}$

3. True or false: Any scheme for sharing a *classical* secret among n parties in such a way that no single party can recover the secret alone requires at least $n/2$ shares to recover the secret.

   (a) True

   (b) False

4. Charlie wants to share a 4-bit classical secret between Alice and Bob in such a way that neither can recover it alone. What is the minimum number of qubits either Alice or Bob must hold?

(a) 1

(b) 2

(c) 3

(d) 4

5. Consider the cq-state

$$\rho_{XE} = \frac{1}{4}|0\rangle\langle0|_X \otimes |+\rangle\langle+|_E + \frac{3}{4}|1\rangle\langle1|_X \otimes |-\rangle\langle-|_E. \tag{1}$$

What is the conditional min-entropy $H_{\min}(X|E)$ of this state?

(a) $H_{\min}(X|E) = 0$

(b) $H_{\min}(X|E) = 2 - \log 3$

(c) $H_{\min}(X|E) = 2 - \frac{3}{4}\log 3$

(d) $H_{\min}(X|E) = 1$

6. Recall that in the tripartite guessing game Eve prepares a state ρ_{AEB} such that Alice and Bob each get a single qubit A and B respectively, while Eve keeps an arbitrary state. Alice chooses a random basis $\theta \in \{0, 1\}$, measures her qubit to obtain a bit x_A, and publicly announces θ. Bob measures in the same basis as Alice to obtain a bit x_B. Eve's goal is to produce a bit x_E such that the probability that $x_A = x_B = x_E$ is maximized.

   Suppose that Eve prepares the initial state $\rho_{AEB} = |\psi\rangle\langle\psi|_{AE} \otimes |0\rangle\langle0|_B$, where $|\psi\rangle_{AE} = \frac{1}{\sqrt{2}}(|00\rangle_{AE} + |11\rangle_{AE})$ is a maximally entangled state. What is the optimal probability that Eve guesses Alice's outcome?

   (a) $\frac{1}{2}$

   (b) $\frac{3}{4}$

   (c) $\frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \approx 0.85$

   (d) 1

7. In the same setup, what is the optimal probability that Bob guesses Alice's outcome?

   (a) $\frac{1}{2}$

   (b) $\frac{3}{4}$

   (c) $\frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \approx 0.85$

   (d) 1

8. Consider again the same guessing game, except that now the inital state is the GHZ state $|GHZ\rangle_{ABE} = \frac{1}{\sqrt{2}}(|000\rangle_{ABE} + |111\rangle_{ABE})$. Can both Eve and Bob guess Alice's measurement outcome in the standard basis with full certainty?

(a) Yes

(b) No

9. Suppose Ext : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a (k, ε) strong extractor. For which of the following random variables X and Y is it true that $\|\rho_{Ext(X,Y)YE} - I \otimes \rho_{YE}\|_{tr} \leq \varepsilon$? Mark all that apply.

   (a) X is uniform and independent of Y and E, and Y is such that $H(Y|E) \geq k$.

   (b) X is a such that $H(X|E) = k - 1$, and Y is uniform and independent of X and E.

   (c) X is such that $H(X|E) \geq k$, and Y is uniform and independent of X and E.

   (d) X is such that $H(X|E) \geq k$, and Y is uniform with $H(Y|X) < d$.

10. Alice and Bob communicate over a special classical channel such that Bob correctly receives all the bits from Alice. However, Eve receives a bit b_E that is equal to Alice's bit with probability $q = \frac{1}{2}$ and with probability $1 - q = \frac{1}{2}$ equal to Alice's bit flipped. Is it necessary for Alice and Bob to perform randomness extraction on their strings to reduce Eve's knowledge about the key?

   (a) Yes, Alice and Bob need to perform randomness extraction, since there is a non-zero probability that Eve received Alice's key bit.

   (b) No, randomness extraction is not required, because Eve holds no information about the key.

11. Now the channel between Alice and Bob has been modified such that Bob still receives all the bits from Alice, but Eve always receives Alice's bit flipped. Is it now necessary for Alice and Bob to perform randomness extraction on their bit strings to reduce Eve's knowledge about the key?

   (a) Yes, Alice and Bob need to perform randomness extraction, to reduce Eve's knowledge about the key.

   (b) No, randomness extraction is not required, because Eve never receives the key bit, so she holds no information about the key.

   (c) Alice and Bob cannot obtain the key in this scenario, because Eve has as much information about the key as Bob has.

12. In the device-independent setting, attacks by Eve can be modeled by specifying what kinds of devices she gives to Alice and Bob. Which of the following attacks do we hope our device-independent protocol to protect against? Circle all that apply.

   (a) Alice's devices communicate with Bob's devices during the protocol.

   (b) Eve gets to examine Alice and Bob's devices at the end of the protocol.

   (c) Alice's devices send information to Eve during the protocol.

3

(d) Eve's laboratory is arbitrarily entangled with Alice and Bob's laboratory at the beginning of the protocol.

13. Consider the following protocol for bit commitment: Alice prepares $|\psi_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ if she commits to $x = 0$, or she prepares $|\psi_{01}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ if she commits to $x = 1$. Then she sends the register B to Bob. Finally, in the open phase, Alice sends Bob her register A, so that Bob can perform a measurement in the Bell basis on the two qubits in registers A and B to learn Alice's bit. Is this protocol correct and secure?

(a) Yes

(b) No

2 Problems

1. *(4 points)* **A Guessing Game.**
   Imagine that Alice and Eve play a guessing game where they share a two-qubit state ρ_{AE}. First, Alice produces a random bit $\theta \in \{0, 1\}$, and she measures her qubit in the standard basis if $\theta = 0$ and in the Hadamard basis if $\theta = 1$. In both cases she obtains a bit $x \in \{0, 1\}$ as measurement outcome. She then announces θ to Eve. Eve's goal is to guess the bit x. Imagine that $\rho_{AE} = |\text{EPR}\rangle\langle\text{EPR}|$, where as usual $|\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, so Alice and Eve share a maximally entangled pair of qubits. In this scenario we know that if Eve measures in the same basis as Alice she will get the same outcome and thus be able to guess x perfectly.

   (a) Suppose now that Alice wants to foil Eve so, before measuring, she first applies some unitary U_A to her qubit, and then measures. Of course Eve, being really smart, gets wind of this so she will know what unitary Alice has used before measuring. So they share the state

   $$|\Phi_U\rangle = (U_A \otimes \mathbf{1}_E)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

   and Eve knows θ and U_A. In this scenario, what is Eve's optimal guessing probability, and what is a strategy that achieves it?

   (b) Consider now a scenario in which Alice's strategy consists in choosing one out of three possible unitaries, according to a distribution that may depend on her choice of θ. The three unitaries are the same whether $\theta = 0$ or $\theta = 1$, and Eve knows what they are as well as the distribution used by Alice, but she does not learn which unitary Alice eventually selected. Provide a set of three unitaries that makes Eve's guessing probability the lowest possible. (You do not need to prove that your strategy is optimal.)

   (c) Suppose we restrict Alice's set of possible unitaries to contain only two. Can she still make Eve's guessing probability as low as in part (b)?

2. *(4 points)* **Thinking adversarially**.
   In this problem you are asked to play the role of the eavesdropper Eve in a QKD protocol. Eve observes two parties, Alice and Bob, trying to implement a certain protocol. Because QKD is hard, Alice and Bob might try to cut corners in the implementation of their protocol. Here are two suggested protocols that Alice and Bob might want to implement. For each of them, either argue (in broad lines) security or provide an explicit attack for Eve. (If arguing security, you will be arguing that for some "reasonable" choice of the unspecified parameters, such as for privacy amplification, Alice and Bob can obtain a secure key based on the template provided.)

   Protocol 1:
   Alice and Bob can communicate through a classical authenticated channel, and a quantum (non-authenticated) channel.

(a) Alice generates bit strings $x, \theta \in \{0, 1\}^n$ uniformly at random.

(b) Alice prepares qubits $|x_i\rangle_{\theta_i}$ for $i = 1, \ldots, n$ where as usual $|x\rangle_\theta = H^\theta |x\rangle$, and sends them to Bob.

(c) Alice announces the basis string θ.

(d) Bob measures the qubits he received according to the bases specified by the string θ and obtains a string x'.

(e) Alice randomly selects a subset $T \subseteq \{1, \ldots, n\}$ of size $|T| = n/2$ and announces it to Bob. Alice, Bob exchange x_T and x'_T and abort if $x_T \neq x'_T$.

(f) Alice and Bob perform information reconciliation and privacy amplification, on the strings x_S and x'_S respectively, where $S = \{1, \ldots, n\}\backslash T$, with adequate parameters to obtain a shared key.

Protocol 2:

(a) Alice creates n EPR pairs and sends one half of each to Bob.

(b) She generates a string $\theta \in \{0, 1\}^n$ uniformly at random and measures her half of each pair according to the corresponding bit of θ (standard basis for 0, Hadamard for 1)

(c) Bob generates a random string θ', and similarly measures his half of the EPR pairs. Then Bob announces over an authenticated channel that he received and measured his qubits.

(d) Alice and Bob announce θ and θ' over an authenticated channel.

(e) Alice randomly selects a subset $T \subseteq \{i : \theta_i = \theta'_i\}$ of size $|T| = n/4$ and announces it to Bob. Alice, Bob exchange x_T and x'_T and abort if $x_T \neq x'_T$.

(f) Alice and Bob perform information reconciliation and privacy amplification, on the strings x_S and x'_S respectively, where $S = \{i : \theta_i = \theta'_i\}\backslash T$, with adequate parameters to obtain a shared key.

3. *(8 points)* **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, $0 \le \alpha \le 1$ 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 $F^2(\rho_1, \rho_2) + F^2(\rho_1, \rho_3) \le 1 + F(\rho_2, \rho_3)$ 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 to achieve the bound in (d)?

    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.

4. *(8 points)* **Cloning attacks NEED TO EDIT BASED ON PDF**
In this problem we study the effectiveness of a simple cloning attack for the eavesdropper in the BB84 key distribution protocol. Recall that in the protocol Alice prepares N single-qubit states $|x_j\rangle_{\theta_j}$, for $j \in \{1, \ldots, N\}$ and random $x_j, \theta_j \in \{0, 1\}$, and sends each of these states to Bob.

Now suppose the eavesdropper Eve intercepts each of the states sent by Alice, and does the following:

(i) With probability $1 - p$, she applies the cloning map T_1 from Problem 6(a) in HW2. She keeps the second qubit and forwards the first qubit to Bob.

(ii) With probability p, she applies the cloning map T_2 from Problem 6(b) in HW2. She keeps the second qubit, traces out (i.e. ignores) the third qubit, and forwards the first to Bob.

For simplicity, first assume $N = 1$. Based on the results of HW2 Problem 6 (you may consult the solution available online), evaluate the following:

(a) Suppose both Alice and Bob measure their qubit in the correct basis $\theta = \theta_1$. If $p = 0$, what is the probability that they get the same outcome (recall $\theta \in \{0, 1\}$ is chosen uniformly at random). Same question if $p = 1$. Same question for a general $0 < p < 1$.

(b) Answer the same questions, where now Alice and Eve measure their qubit. What is the probability that they get the same outcome?

(c) What is the probability that all of Alice, Bob and Eve all obtain the same outcome, if they each measure their respective qubit in basis θ? (Answer for a general p.)

Let's continue with the BB84 protocol. We now consider a number of rounds $N = 4n$. Suppose that in $2n$ of the rounds (exactly), Alice and Bob happen to make the same basis choice; call these the agreement rounds, $R \subseteq \{1, \ldots, N\}$. They select exactly n of these rounds for testing; call these rounds the testing rounds, $T \subseteq R$. You may assume all rounds behave the same.

(d) What is the expected number of errors (non-agreement of their measurement outcomes) that Alice and Bob will notice in the testing rounds T, as a function of p?

(e) Invert the previous bound: as a function of the fraction δ of errors detected in the testing rounds, what is a reasonable estimate $\hat{p}$ for p that Alice and Bob could come up with?

(f) Suppose Alice and Bob make a guess $\hat{p}$ for p based on the method from the previous question. Using question (b), deduce a bound on the min-entropy $H_{\min}(A|E)$ per round that they could estimate for the rounds in $K = R \backslash T$.

(g) Conclude: how many bits of key, as a function of p and N, can Alice and Bob reasonably hope to generate from the protocol? *[Hint: This is a subtle calculation. Alice and Bob will have to perform both information reconciliation and privacy amplification on the rounds in K. First, estimate the number of bits they will need to exchange to perform information reconciliation. Second, deduce a bound on the min-entropy of the resulting agreed-on string. Third, use the best privacy amplification method you know of to maximize the length of extracted key]*