Assignment
Quantum Cyber Security

Due: 12:00 Friday 20 March, 2026

This assignment counts for **25% of the course** and you must answer **all three** questions. The weights of each question and sub-question are given (number of marks), but note that this is **not** indicative of how difficult the corresponding sub-question is. Note also that notation is set individually in each problem, and the same letters may have different meanings in each problem.

Important message:

Please remember the good scholarly practice requirements of the University regarding work for credit. You can find guidance at the School page https://web.inf.ed.ac.uk/infweb/admin/policies/academic-misconduct. This page also has links to the relevant University pages.

1. Consider the scenario of the BB84 quantum key distribution protocol. Alice selects states from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ uniformly at random and sends them to Bob. Suppose that, before Bob receives each state, a malicious party Eve applies a T operator with probability q. The corresponding quantum channel Φ_q that Eve applies acts on a density matrix ρ as

$$\Phi_q(\rho) = (1-q)\rho + qT\rho T^\dagger,$$

where T is the linear transformation defined by $T = |0\rangle\langle 0| + e^{\frac{i\pi}{4}} |1\rangle\langle 1|$. Also, for studying the transformation of BB84 states under this channel, it is useful to define a family of states, known as planar states, as:

$$|+_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta} |1\rangle),$$

and $|-_\theta\rangle := |+_{\pi+\theta}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\theta} |1\rangle)$. These are the states on the equator of the Bloch sphere.

(a) Show that the (mixed) states Bob receives for each of the four possible states sent by Alice have density matrices of the form:

$$\begin{aligned}
|0\rangle &\mapsto |0\rangle\langle 0|, \\
|1\rangle &\mapsto |1\rangle\langle 1|, \\
|+\rangle &\mapsto (1-q)\,|+\rangle\langle +| + q\,|+_\alpha\rangle\langle +_\alpha|, \\
|-\rangle &\mapsto (1-q)\,|-\rangle\langle -| + q\,|-_\alpha\rangle\langle -_\alpha|
\end{aligned}$$

Determine the value of α. [3 marks]

(b) The raw key is generated from positions where Bob measured in the basis to which the state sent by Alice belongs. Calculate the average error rates e_b and e_p for the bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ respectively. [3 marks]

(c) Evaluate the secret key rate R_{BB84} in the asymptotic limit of finite-size effects with perfect detection and ideal classical post-processing. For which values of q is it possible to distil a secret key? [3 marks]

2. In your submission please include the steps that lead to your answers.

(a) Evaluate the binary entropy $h(p)$ for Bernoulli processes with $p = 1/4$ and $p = 1/32$. [2 marks]

(b) Consider the mixed state ρ for an ensemble in which, with probability 1/2 each, the state $|1\rangle$ or the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ occurs. Calculate the von Neumann entropy. [2 marks]

(c) Consider a quantum channel that does nothing with probability $1 - p$ and applies a Hadamard transformation with probability p. This quantum channel is described by the Kraus operators

$$E_0 = \sqrt{1-p}I, \quad E_1 = \sqrt{p}H,$$

where H is the Hadamard operator defined by $H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$. Evaluate the action of the quantum channel with $p = 1/2$ on the state $\rho = |+\rangle\langle +|$, where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. [2 marks]

(d) Charlie is given one of two possible states

$$\rho = |1\rangle\langle 1| \quad \text{or} \quad \sigma = |-\rangle\langle -|$$

Where $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Evaluate the fidelity $F(\rho, \sigma)$ of the two states. What can we say about the maximum probability with which Charlie can correctly identify the state? [3 marks]

3. Recall the definition of planar states from 1:

$$|+_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle),$$

Bob is given one state from the set $\{|0\rangle, |+_{\pi/4}\rangle\}$ and is asked to do unambiguous state discrimination, meaning that he only tells which state he is given in the cases that he is sure about the correctness of his answer. Obviously, his success probability depends on the way he chooses to measure the given state.

(a) Suppose that Bob measures the given state in the computational basis, $\{|0\rangle, |1\rangle\}$. What is his success probability? (as a hint, you can first think about this question: In the case of which outcome he can be sure about the given state?) [3 marks]

(b) Suppose that Bob tries to follow an alternative strategy: he chooses a POVM with three operators $\{E_1, E_2, E_3\}$, which two of them are:

$$E_1 = a|1\rangle\langle 1| \qquad E_2 = b|-_{\pi/4}\rangle\langle -_{\pi/4}|$$

Justify why these two operators are good choices for unambiguous prediction. Find the third operator E_3 and the success probability following this strategy in terms of a, b. [2 marks]

(c) Maximize the success probability obtained from part (b) and compare that to the value obtained from part (a). Which strategy is a more clever choice? [2 marks]