Assignment
Quantum Cyber Security

Due: 12:00 Friday 21 March, 2025

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.

Note: Question 1 and Question 2 are worth 10 marks each, while Question 3 is worth 5 marks (see each subquestion for the exact breakdown).

1. Consider the six state QKD protocol given in the lectures, where Alice selects states from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+_y\rangle, |-_y\rangle\}$ uniformly at random and sends them to Bob. Here, $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $|\pm_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle)$.

   Suppose that, before Bob receives each state, a malicious party Eve applies an S operator with probability q. The corresponding quantum channel Φ_q that Eve applies acts on a density matrix ρ as

   $$\Phi_q(\rho) = (1-q)\rho + qS\rho S^\dagger,$$

   where S is the linear transformation defined by $S = |0\rangle\langle 0| + i\,|1\rangle\langle 1|$ (and make sure you take the complex conjugate of the operator when needed in applying the channel).

   (a) Show that the density matrices of the states Bob receives for each of the six possible states sent by Alice are given by:

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

   where $|\pm_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle)$ are the eigenvectors of the Pauli-Y operator. [3 marks]

(b) The raw key consists of rounds where Bob measures in the same basis Alice prepared her state in. Calculate the average error rates e_b, e_p, and e_y for the bases $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$, and $\{|+_y\rangle, |-_y\rangle\}$, respectively. [4 marks]

(c) Consider now a different scenario where we have a symmetric channel where all errors (e_b, e_p, e_y) are the same and equal to the average of your answers to question $1(b)$, $D = \frac{1}{3}(e_b + e_p + e_y) = e'_b = e'_p = e'_y$.
Determine the secret key rate $R_{\text{six-state}}$ for this symmetric channel, in the asymptotic limit (i.e. no 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. (a) Evaluate the binary entropy $h(p)$ for Bernoulli processes with $p = 1/8$ and $p = 1/16$. [2 marks]

(b) Consider the mixed state ρ for an ensemble in which, with probability 1/2 each, the state $|0\rangle$ 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 p and applies a gate B (defined below) with probability $1 - p$. This quantum channel is described by the Kraus operators

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

where B is defined by the matrix

$$B = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}. \tag{1}$$

Evaluate the action of the quantum channel with $p = 1/8$ on the state $\rho = |-\rangle\langle -|$, where $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. [3 marks]

(d) Charlie is given one of two possible states

$$\rho = |1\rangle\langle 1| \quad \text{or} \quad \sigma = |+_y\rangle\langle +_y|.$$

Evaluate the fidelity $F(\rho, \sigma)$ of the two states. Using the fidelity, what can we say about the maximum probability with which Charlie can correctly identify the state? [3 marks]

3. In the following question, the sum operation will be done modulo 2, i.e. $0 \oplus 1 = 1 \oplus 0 = 1$ and $1 \oplus 1 = 0 \oplus 0 = 0$.

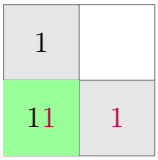
Alice and Bob play a non-local game, where they are *not* allowed to communicate during each round of the game (but are allowed to agree on a strategy before the game).

Alice and Bob are to independently fill in a 2×2 grid with zeroes and ones. In each round, Alice is assigned a row, and Bob is assigned a column. Suppose Alice is assigned row i, and Bob is assigned row j. They must follow the following rules:

- **Rule 1**. Each cell must be assigned a value from the set $\{0, 1\}$.
- **Rule 2**. The sum of Alice's entries must be $\alpha_i \in \{0, 1\}$ (modulo 2).
- **Rule 3**. The sum of Bob's entries must be $\beta_j \in \{0, 1\}$ (modulo 2).

They win if they both enter the same value into the cell shared by their row and column, and they lose otherwise (see Figure 1 below). Neither player has knowledge of which row or column the other player has been assigned.

(a) Show that if $\alpha_1 \oplus \alpha_2 \oplus \beta_1 \oplus \beta_2 = 0$, there exists a classical strategy that allows Alice and Bob to win the game with probability 1. [1 mark]



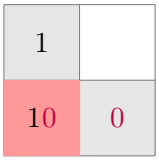


Figure 1: An example of the game, with $\beta_2 = 1, \alpha_1 = \alpha_2 = \beta_1 = 0$. In this round, Alice is assigned the second row, and Bob is assigned the first column. The values in red indicate the answer Alice puts down, and the values in black indicate the answer Bob puts down. In the left scenario, Alice and Bob win because they have put the same value on their shared cell, and in the right, they lose because they have put different values on their shared cell. You can also check that Rule 2 and Rule 3 are also satisfied.

(b) Suppose that $\alpha_1 \oplus \alpha_2 \oplus \beta_1 \oplus \beta_2 = 1$. Find the best classical strategy for Alice and Bob and the probability they win in that case. [2 marks]

(c) Suppose now that $\beta_2 = 1$ and $\alpha_1 = \alpha_1 = \beta_1 = 0$. Suppose Alice and Bob share the entangled state:

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}), \tag{2}$$

where the first qubit is in Alice's lab and the second in Bob's..

Let $A_0 = Z, A_1 = X, B_0 = \frac{1}{\sqrt{2}}(X+Z)$, and $B_1 = \frac{1}{\sqrt{2}}(X-Z)$. Alice and Bob measure these observables according to the following figure:

A_0	A_0
A_1	A_1

B_0	$-B_1$
B_0	B_1

Figure 2: The quantum strategy for Alice and Bob. Alice measures the operators depicted on the left grid; Bob measures the operators depicted on the right grid.

Alice and Bob write down 0 if the measurement outcome is $+1$ and they write down 1 if the measurement outcome is -1.

For example, if Alice is given row 2, and Bob is given column 1, Alice measures $\{A_1, A_1\}$, and Bob measures $\{B_0, B_0\}$. If upon measuring A_0, Alice obtains the outcome -1, and if Bob obtains the outcome -1 upon measuring B_0, then we are in the scenario depicted by the left-hand figure in Figure 1.

- Explain why the constraints concerning the modulo-2 sums of the rows and columns are always satisfied.
- Find the probability of them winning using this quantum strategy.

  Hint: You can use the fact that the win probability for this scenario is equal to $1/2 + S/8$ where S is the CHSH quantity given in the lectures (called β in the lecture).

[2 marks]