Assignment
Quantum Cyber Security

Due: 12:00 Thursday 28 March, 2024

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. 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 $p = 1/2$.

   [3 marks]

   (b) Alice sends Bob a quantum state ρ_j with probability p_j, where $j \in \{1, \ldots, n\}$, so that Bob has the mixed state $\rho = \sum_{j=1}^{n} p_j \rho_j$. Use the Holevo bound to show that the maximum amount of information transmitted by N qubits is N bits. How much information can be transmitted if the states are instead composed of N qu*trits*, where the state space of a qutrit is defined as a three-dimensional complex Hilbert space?

   [3 marks]

   (c) The phase-flip channel, which does nothing with probability p and flips the phase of $|1\rangle$ to $-|1\rangle$ with probability $1-p$, has Kraus operators

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

   where Z is the Pauli operator defined by $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. Evaluate the action of the phase-flip 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

   $$\rho = |0\rangle\langle 0| \quad \text{or} \quad \sigma = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 1|).$$

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?

[2 marks]

2. **Quantum Coin Flipping:**
Recall the quantum coin flipping protocol of Ambainis mentioned in the lecture notes where the following four qutrit states have been used:

$$|\phi_{a,x}\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), & a = 0, x = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), & a = 0, x = 1 \\ \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle), & a = 1, x = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle), & a = 1, x = 1 \end{cases}$$

where $|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $|2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

(a) We want to first look at Bob's cheating strategy. Compute the mixed states ρ_0 and ρ_1 corresponding to the mixture of states Bob receives from Alice for the choice of random bit a being 0 and 1 respectively.

[3 marks]

(b) Write down the matrix form of $\rho_0 - \rho_1$. Then calculate the trace norm of $\| \rho_0 - \rho_1 \|_{tr}$.
Note: The trace distance is related to the trace norm in this way:
$T(\rho_0, \rho_1) = \frac{1}{2}\|\rho_0 - \rho_1\|_{tr}$.

[2 marks]

(c) Now use the Holevo-Helstrom bound for maximal probability of distinguishing two mixed states, i.e. the following equation:

$$P_{opt}^{dist} = \frac{1}{2} + \frac{1}{4} \| \rho_0 - \rho_1 \|_{tr},$$

to obtain the maximum cheating probability of Bob for this protocol and hence determine the minimum bias for a dishonest Bob.

[1 mark]

(d) In this part, we will look at a weak coin-flipping protocol. Let's assume that outcome 0 means that Bob wins, and outcome 1 is a win for Alice. The protocol is as follows:

- Step 1: Alice prepares a pair of systems in an entangled state $|\psi_{AB}\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$, being $|\psi_{AB}\rangle = \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|11\rangle$ and sends subsystem B to Bob.
- Step 2: Bob performs a 2-outcome POVM measurement $\{E_0, E_1\}$ on the qubit he received (System B), and sends a classical bit b that is the outcome bit to Alice. Let $E_0 = \frac{2}{3}|0\rangle\langle 0|$. (You can find what's E_1 using properties of POVMs.)
- Step 3: If $b = 0$ then Bob sends his system (B) back to Alice, if $b = 1$ then Alice sends her system (A) to Bob. The party that receives the system then performs the projective measurements $\{|\psi_b\rangle\langle\psi_b|, I - |\psi_b\rangle\langle\psi_b|\}$, where the $|\psi_b\rangle$ is defined as follows:

$$|\psi_b\rangle = \frac{I \otimes \sqrt{E_b}\,|\psi_{AB}\rangle}{\sqrt{\langle\psi_{AB}|\, I \otimes E_b\,|\psi_{AB}\rangle}}$$

I) Write down the reduced density matrix $\rho_B = Tr_A[|\psi_{AB}\rangle \langle\psi_{AB}|]$ that is being sent from Alice to Bob. Also, write down the state $|\psi_b\rangle$ for both cases where $b = 0$ and $b = 1$.

II) Following all the steps of the protocol, explain why this protocol is correct (achieves weak coin flipping) if both Alice and Bob are honest and they follow the protocol.

III) You may have noticed that in the above protocol, there is an extra measurement that allows Alice and Bob to catch each other cheating! Explain how they can detect each other's cheating by describing the four possible outcomes of the protocol. (You can explain your answer by trying to give an attack where either Alice or Bob are trying to cheat.)

[6 marks]

Note: Each of the above subquestions counts for 2 marks.

3. Consider the following two functions:

$$A(x,i,j) = (-1)^{x\oplus i}(-1)^{x\cdot j} \text{ and } B(y,i,j) = (-1)^{y\oplus i}(-1)^{y\cdot j}\,.$$

All inputs x, y, i, j are single (classical) bits. Assume that these deterministic functions, correspond to the outcomes of Alice (the $A(x,i,j)$) and Bob (the $B(y,i,j)$) at some QKD protocol. The i, j occur with same probability, and are unknown to Alice and Bob.

(a) Show that the expectation values and the correlations that they obtain are the same as for the BBM92 QKD protocol. Recall that in that protocol, the expectation value of each observable A, B was zero (equal probability for each outcome), the expectation value of the correlator when measuring in the same basis was one (perfect correlation), while the expectation value of the correlator when measuring in a different basis is zero (completely uncorrelated).
Note: to compute the expectation value of an observable you need to sum over the hidden variables i, j, while to compute the correlator you need to multiply the two observables and then sum over the hidden variables i, j.

[2 marks]

(b) Explain why the result of the previous question means that the BBM92 protocol is not device independent.

[1 mark]