Assignment
Quantum Cyber Security

Due: 12:00 Thursday 30 March, 2023

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 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 $S = |0\rangle\langle 0| + i\,|1\rangle\langle 1|$.

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

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

respectively 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 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 $p = 1/8$ 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 Hadamard transformation with probability $1-p$. This quantum channel is described by the Kraus operators

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

   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

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

   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. Consider the following non-local game, played by Alice and Bob, where both players are *not* allowed to communicate during each round of the game. Each round consists of Alice and Bob respectively being assigned a row and a column of an empty 3×3 grid which they must fill according to the following rules.

   - **Rule 1**. Each filled cell must have a value from the set $\{-1, +1\}$
   - **Rule 2**. Rows must contain an even number of negative entries (i.e. the product of Alice's entries to any assigned row must be $+1$).
   - **Rule 3**. Columns must contain an odd number of negative entries (i.e. the product of Bob's entries to any assigned column must be -1).

   Neither player has knowledge of which row or column the other has been assigned. The game is won if both players enter the same value into the cell shared by their row and column and it is lost otherwise (see Figure below).

Figure 1: In the left scenario Alice and Bob win the game, while in the right scenario, they lose. Alice assigns a number in each cell of a given row (numbers with black colour) so that the product of her entries is $+1$. On the other hand, Bob assigns numbers on a given column (numbers with purple colour) so that the product of his entries is -1.

   (a) Alice and Bob can agree to follow a deterministic strategy in which both of them know what values each player will assign in advance. Explain what is the best classical strategy that they can follow and then calculate what is the probability that they will win the game. [3 marks]

$X \otimes I$	$X \otimes X$	$I \otimes X$
$-X \otimes Z$	$Y \otimes Y$	$-Z \otimes X$
$I \otimes Z$	$Z \otimes Z$	$Z \otimes I$

Figure 2: Quantum Strategy for Alice and Bob.

(b) Suppose now that Alice and Bob are allowed to share an entangled state:

$$|\Psi\rangle = \left|\Phi^+\right\rangle_{1,2} \otimes \left|\Phi^+\right\rangle_{3,4}$$

which is the product of two maximally entangled two-qubit Bell states:

$$\left|\Phi^+\right\rangle_{a,b} = \frac{1}{\sqrt{2}}(|0\rangle_a \otimes |0\rangle_b + |1\rangle_a \otimes |1\rangle_b)$$

In this scenario, Alice has in possession qubits 1 and 3 while Bob has qubits 2 and 4. Depending on which row and column are assigned, the players make measurements on their respective quantum systems according to the observables given in Figure 2. The outcomes of the observables will determine the values which Alice and Bob will enter into their respective row and column. Note that each of these observables has eigenvalues $\{+1, -1\}$. Explain why this is a valid strategy (product of each row is $+1$, product of each column is -1) and analytically compute what is the success probability if they follow this strategy. [2 marks]

(c) Use this non-local game to construct a device-independent QKD protocol between Alice and Bob. Give the protocol and the intuition but there is no need to prove formally its security. [2 marks]