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]

Solution: Bob receives each state after Eve has applied the Φ_q channel with probability q. We must first calculate what is the action of the S operator on each corresponding

state. We have:

$$\begin{aligned} S|0\rangle &= |0\rangle \\ S|1\rangle &= i|1\rangle \\ S|+\rangle &= \frac{1}{\sqrt{2}}(S|0\rangle + S|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) = |+_y\rangle \\ S|-\rangle &= \frac{1}{\sqrt{2}}(S|0\rangle - S|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) = |-_y\rangle \end{aligned}$$

Therefore,

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

(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]

Solution: The projectors for a measurement in the computational basis are $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$. The probability that Bob measures the state to be $|1\rangle$ but Alice sent $|0\rangle$ is

$$\begin{aligned} \mathrm{tr}[\Phi_q(|0\rangle\langle 0|)\,|1\rangle\langle 1|] &= \langle 1|\,\Phi_q(|0\rangle\langle 0|)\,|1\rangle \\ &= \langle 1|\,|0\rangle\langle 0|\,|1\rangle \\ &= 0 \end{aligned}$$

Similarly, the probability that Bob measures the state to be $|0\rangle$ but Alice sent $|1\rangle$ is

$$\begin{aligned} \mathrm{tr}[\Phi_q(|1\rangle\langle 1|)\,|0\rangle\langle 0|] &= \langle 0|\,\Phi_q(|1\rangle\langle 1|)\,|0\rangle \\ &= \langle 0|\,|1\rangle\langle 1|\,|0\rangle \\ &= 0 \end{aligned}$$

Therefore, $e_b = 0$.

The projectors for a measurement in the basis $\{|+\rangle, |-\rangle\}$ are $P_+ = |+\rangle\langle +|$ and $P_- = |-\rangle\langle -|$. The probability that Bob measures the state to be $|-\rangle$ but Alice sent $|+\rangle$ is

$$\begin{aligned} \mathrm{tr}[\Phi_q(|+\rangle\langle +|)\,|-\rangle\langle -|] &= \langle -|\,\Phi_q(|+\rangle\langle +|)\,|-\rangle \\ &= \langle -|\,[(1-q)\,|+\rangle\langle +| + q\,|+_y\rangle\langle +_y|]\,|-\rangle \\ &= q\,\langle -|\,|+_y\rangle\langle +_y|\,|-\rangle \\ &= \frac{q}{2} \end{aligned}$$

Similarly, the probability that Bob measures the state to be $|+\rangle$ but Alice sent $|-\rangle$ is

$$\begin{aligned} \mathrm{tr}[\Phi_q(|-\rangle\langle -|)\,|+\rangle\langle +|] &= \langle +|\,\Phi_q(|-\rangle\langle -|)\,|+\rangle \\ &= \langle +|\,[(1-q)\,|-\rangle\langle -| + q\,|-_y\rangle\langle -_y|]\,|+\rangle \\ &= \langle +|\,|-_y\rangle\langle -_y|\,|+\rangle \\ &= \frac{q}{2} \end{aligned}$$

Therefore, $e_p = \frac{q/2+q/2}{2} = \frac{q}{2}$.

(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]

Solution: The binary entropy of the error in the computational basis is

$$h(e_b) = 0$$

The binary entropy of the error in the basis $\{|+\rangle, |-\rangle\}$ is

$$h(e_p) = h\left(\frac{q}{2}\right) = -\frac{q}{2}\log_2\frac{q}{2} - \left(1-\frac{q}{2}\right)\log_2\left(1-\frac{q}{2}\right).$$

In the ideal case, the key rate is given by

$$\begin{aligned} R_{\text{BB84}} &= \frac{1}{2}(1 - h(e_b) - h(e_p)) \\ &= \frac{1}{2}\left(1 - h\left(\frac{q}{2}\right)\right) \\ &= \frac{1}{2}\left(1 + \frac{q}{2}\log_2\frac{q}{2} + \left(1-\frac{q}{2}\right)\log_2\left(1-\frac{q}{2}\right)\right) \end{aligned}$$

The above quantity is zero only when $q = 1$. This is a feasible value for q since q corresponds to the probability of performing an S operator (and thus $q \in [0, 1]$). Since $R_{\text{BB84}} > 0$ for all values of $q \in [0, 1)$ then it is always possible to distil a secret key except for $q = 1$.

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]

Solution: The binary entropy function is defined as

$$h(p) = -p\log_2 p - (1-p)\log_2(1-p).$$

Therefore, $h(1/8) = -\frac{1}{8}\log_2\frac{1}{8} - \frac{7}{8}\log_2\frac{7}{8} \approx 0.543$ and $h(1/16) \approx 0.337$.

(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]

Solution: The mixed state ρ can be written as:

$$\begin{aligned} \rho &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +| \\ &= \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|0\rangle\langle 1| + \frac{1}{4}|1\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| \end{aligned}$$

or in matrix notation:

$$\rho = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix}$$

In order to calculate the Von Neumann entropy we have to calculate the eigenvalues of ρ. The eigenvalues are the roots of the characteristic polynomial $\det(\rho - \lambda\mathbf{1}) = 0$. In our case, the two eigenvalues are $\lambda_1 = \frac{\sqrt{2}+1}{2\sqrt{2}} \approx 0.854$ and $\lambda_2 = \frac{\sqrt{2}-1}{2\sqrt{2}} \approx 0.146$. The Von Neumann entropy can thus be calculated as:

$$S(\rho) = -\lambda_1\log_2\lambda_1 - \lambda_2\log_2\lambda_2 \approx 0.6$$

(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]

Solution: The action of a channel with Kraus operators $\{E_j\}$ on a state ρ is

$$\rho \mapsto \sum_j E_j \rho E_j^\dagger.$$

In our case, $E_0^\dagger = E_0$ and $E_1^\dagger = E_1$, $p = 1/2$, and $\rho = |-\rangle\langle -|$. Thus, by noting $H|-\rangle = |1\rangle$, applying the quantum channel gives

$$\begin{aligned}\rho \mapsto p\rho + (1-p)H\rho H &= \frac{1}{2}(|-\rangle\langle -| + H|-\rangle\langle -|H) \\ &= \frac{1}{2}(|-\rangle\langle -| + |1\rangle\langle 1|) \\ &= \frac{1}{4}|0\rangle\langle 0| - \frac{1}{4}|0\rangle\langle 1| - \frac{1}{4}|1\rangle\langle 0| + \frac{3}{4}|1\rangle\langle 1|\end{aligned}$$

(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]

Solution: Let us first recognise that there are two alternative definitions of fidelity which may be used to obtain the correct solution, provided the choice of definition is consistent. The first of these (here denoted by F') is defined by

$$F'(\rho, \sigma) = \left(\operatorname{tr}\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}\right)^2,$$

and the second is simply $F(\rho, \sigma) = \sqrt{F'(\rho, \sigma)}$. Here, we will choose to adopt the latter definition, as is done in the lecture slides.

Since ρ is the density matrix for the pure state $|1\rangle$, the fidelity can be expressed in the simplified form

$$F(\rho, \sigma) = \sqrt{\langle 1|\sigma|1\rangle} = \frac{1}{\sqrt{2}}.$$

The maximum probability with which Charlie can identify the correct state is given by

$$p_{\text{guess}}^{\max} = \frac{1}{2}(1 + D(\rho, \sigma)),$$

where $D(\rho, \sigma)$ is the trace distance between ρ and σ. The trace distance is bounded above in terms of the fidelity as

$$D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2} = \sqrt{1 - \frac{1}{2}} = \frac{1}{\sqrt{2}},$$

and so $p_{\text{guess}}^{\max} \leq (2 + \sqrt{2})/4 \approx 0.854$. In fact, since $\sigma = |+\rangle\langle +|$ is also a pure state, the upper bound on the trace distance is in fact an equality, leading to $p_{\text{guess}}^{\max} = (2 + \sqrt{2})/4$.

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]

Solution: Alice and Bob must agree before the start of the game to a certain pre-determined configuration. By doing so, Alice and Bob can agree in all but one cell values. So the probability that their row and column intersect in that cell is $1/9$. As a result, agreeing on a pre-determined configuration will give them a winning probability of $P_{\text{win}} = 8/9$.

(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]

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

Figure 2: Quantum Strategy for Alice and Bob.

Solution: In this scenario, note that each row is formed of mutually commuting observables whose product is $-\mathbf{1}$. For example in row 1:

$$(X \otimes \mathbf{1})(X \otimes X)(\mathbf{1} \otimes X) = \mathbf{1} \otimes \mathbf{1}$$

Now we note that for any quantum state $|\psi\rangle$ it holds that $\langle\psi| \mathbf{1} \otimes \mathbf{1} |\psi\rangle = 1$ that gives expectation of the product as requested $+1$.
Similarly, each column is formed of mutually commuting observables whose product is $-\mathbf{1}$. For example in column 1:

$$(X \otimes \mathbf{1})(-X \otimes Z)(\mathbf{1} \otimes Z) = -\mathbf{1} \otimes \mathbf{1}$$

Now we note that for any quantum state $|\psi\rangle$ it holds that $\langle\psi| (-\mathbf{1} \otimes \mathbf{1}) |\psi\rangle = -1$ that gives expectation of the product as requested -1.
Moreover, the eigenvalues of each observable are $+1$ and -1 and so all the game rules are satisfied. Thus, sharing the state the entangled state $|\Psi\rangle$ and measuring observables in Figure 2 is indeed a valid strategy.

We will now show that if they follow this quantum strategy, then the winning probability is $P_{\text{win}} = 1$. If O_A is any of the given observables for Alice's system and O_B is the corresponding observable for Bob's system, the correlation $\langle\Psi| O_A O_B |\Psi\rangle = 1$ guarantees that the players always win. To see this, consider the observable $-Z \otimes X$ located on the second row and third column. Alice will measure the operator $O_A = -Z_1 \otimes X_3$ while Bob will measure the operator $O_B = -Z_2 \otimes X_4$. We first calculate the action of the the product $O_A O_B$ on the state $|\Psi\rangle = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$ to find:

$$(Z_1 \otimes Z_2 \otimes X_3 \otimes X_4) |\Psi\rangle = 2(|0011\rangle + |0000\rangle + |1111\rangle + |1100\rangle) = |\Psi\rangle \qquad (1)$$

and so the correlation is $\langle\Psi| O_A O_B |\Psi\rangle = 1$.

(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]

Solution: Suppose Alice and Bob share a large number of pairs $|\Psi\rangle = |\Phi^+\rangle_{1,2} \otimes |\Phi+\rangle_{3,4}$ where Alice has in possession qubits 1 and 3 while Bob has in possession qubits 2 and 4. Alice and Bob mark each of these pairs with an index i.

Alice and Bob choose respectively a column and a row uniformly at random and measure the corresponding observables as seen in Figure 2. After the measurements, they save the corresponding results. They both confirm that the results they got are "allowed" i.e. follow the rules of the game. Once they complete their measurements they communicate over a classical channel what rows and columns they randomly measured. As a next step, they randomly select a subset of indices $[j] \subset [i]$, announce the outcomes that they measured, and check whether their outcome is common on the same cell. This is the analogous step of parameter estimation (PE). If they agree, then the protocol is secure and so they can use the indices that they did not check as their secret key. In general they will find that they agree at a fraction that corresponds to the QBER. If this rate is above 8/9, they know that there was no classical strategy achieving this and thus it is possible with further classical postprocessing (IR and PA) as usual to distil a secret key.

.