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]

Solution: Bob receives each state after Eve has applied the bit flip channel with probability q. Therefore,

$$\begin{aligned}
&|0\rangle \mapsto \Phi_q(|0\rangle\langle 0|) = (1-q)\,|0\rangle\langle 0| + q\,|0\rangle\langle 0| = |0\rangle\langle 0|\,,\\
&|1\rangle \mapsto \Phi_q(|1\rangle\langle 1|) = (1-q)\,|1\rangle\langle 1| + q(|0\rangle\langle 0| + i\,|1\rangle\langle 1|)\,|1\rangle\langle 1|\,(|0\rangle\langle 0| - i\,|1\rangle\langle 1|) = |1\rangle\langle 1|\,,\\
&\quad .
\end{aligned}$$

For the remainder, let's perform a few preliminary calculations:

$$\begin{aligned}
S\,|+\rangle\langle +|\,S^\dagger &= \tfrac{1}{2}\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -i\end{pmatrix}\\
&= \tfrac{1}{2}\begin{pmatrix}1 & -i\\ i & 1\end{pmatrix} = \begin{pmatrix}1\\ i\end{pmatrix}\cdot\begin{pmatrix}1\\ i\end{pmatrix}^\dagger\\
&= |+_y\rangle\langle +_y|\,.\\
S\,|-\rangle\langle -|\,S^\dagger &= \tfrac{1}{2}\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -i\end{pmatrix}\\
&= \tfrac{1}{2}\begin{pmatrix}1 & i\\ -i & 1\end{pmatrix} = \begin{pmatrix}1\\ -i\end{pmatrix}\cdot\begin{pmatrix}1\\ -i\end{pmatrix}^\dagger\\
&= |-_y\rangle\langle -_y|\,.\\
S\,|+_y\rangle\langle +_y|\,S^\dagger &= \tfrac{1}{2}\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\begin{pmatrix}1 & -i\\ i & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -i\end{pmatrix}\\
&= \tfrac{1}{2}\begin{pmatrix}1 & i\\ -i & 1\end{pmatrix} = \begin{pmatrix}1\\ -i\end{pmatrix}\begin{pmatrix}1 & -i\end{pmatrix}\\
&= |-\rangle\langle -|\,,\\
S\,|-_y\rangle\langle -_y|\,S^\dagger &= \tfrac{1}{2}\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\begin{pmatrix}1 & i\\ -i & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -i\end{pmatrix}\\
&= \tfrac{1}{2}\begin{pmatrix}1 & -i\\ i & 1\end{pmatrix} = \begin{pmatrix}1\\ i\end{pmatrix}\begin{pmatrix}1 & i\end{pmatrix}\\
&= |+\rangle\langle +|\,.
\end{aligned}$$

The results immediately follow these calculations.

(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]

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

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

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

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

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

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

(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]

Solution:

If the errors in different bases are equal and equal to the QBER: $(e_b = e_p = e_y = D)$, we have:

$$R_{\text{SSP}} = \frac{1}{3}\left(1 + \frac{3D}{2}\log_2\frac{D}{2} + \left(1 - \frac{3D}{2}\right)\log_2\left(1 - \frac{3D}{2}\right)\right).$$

Since $D = q/3$, we get:

$$R_{\text{SSP}} = \frac{1}{3}\left(1 + \frac{q}{2}\log_2\left(\frac{q}{6}\right) + \left(1 - \frac{q}{2}\right)\log_2\left(1 - \frac{q}{2}\right)\right). \tag{1}$$

To get the values of q for which it is possible to distil the secret key, we solve for the roots of this expression:

$$1 + \frac{q}{2}\log_2\left(\frac{q}{6}\right) + \left(1 - \frac{q}{2}\right)\log_2\left(1 - \frac{q}{2}\right) = 0,$$

which has approximate solution $q \approx 0.379$. Since this function goes to 1 as $q \to 0^+$, this is positive for values smaller than this, so it is possible to distil it $q < 0.379$.

2. (a) Evaluate the binary entropy $h(p)$ for Bernoulli processes with $p = 1/8$ and $p = 1/16$. [2 marks]

Solution:

The binary entropy is given by

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

For $p = 1/8$, we have

$$h(1/8) = -\frac{1}{8}\log_2\frac{1}{8} - \frac{7}{8}\log_2\frac{7}{8} \approx 0.5436.$$

For $p = 1/16$, we have

$$h(1/16) = -\frac{1}{16}\log_2\frac{1}{16} - \frac{15}{16}\log_2\frac{15}{16} \approx 0.3373.$$

(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 von Neumann entropy of the mixed state ρ is given by

$$S(\rho) = -\operatorname{tr}(\rho\log_2\rho).$$

The density matrix for the mixed state is

$$\rho = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1}{4}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} = \begin{pmatrix}3/4 & 1/4\\ 1/4 & 1/4\end{pmatrix}$$

The eigenvalues are $1/2 \pm \sqrt{2}/4$, and the larger of the two is ≈ 0.8535. We onbtain our result by noting that the von Neumann entropy is equal the binary entropy of the eigenvalue(s) of the density matrix $S(\rho) = h(\lambda)$ and that the binary entropy $h(0.8535)$ is approximately 0.6.

The von Neumann entropy is

$$S(\rho) = -\operatorname{tr}\left(\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\log_2\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\right) = -\log_2\frac{1}{2} = 1.$$

(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

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

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]

Solution: We have

$$\begin{aligned}
\mathcal{E}(\rho) &= E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger \\
&= p\rho + (1-p) B\rho B^\dagger \\
&= \frac{1}{8} |-\rangle\langle -| + \frac{7}{8} B |-\rangle\langle -| B^\dagger \\
&= \frac{1}{8} |-\rangle\langle -| + \frac{7}{16} \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \frac{\sqrt{3}}{2} & \frac{1}{2} \\ \frac{-1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} \\
&= \frac{1}{16} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} + \frac{7}{32} \begin{pmatrix} 2+\sqrt{3} & -1 \\ -1 & 2-\sqrt{3} \end{pmatrix} \\
&= \frac{1}{32} \begin{pmatrix} 16+7\sqrt{3} & -9 \\ -9 & 16-7\sqrt{3} \end{pmatrix}
\end{aligned}$$

(d) Charlie is given one of two possible states

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

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]

Solution: The fidelity between the two pure states $|1\rangle$ and $|+_y\rangle$ is given by

$$\begin{aligned}
F(\rho, \sigma) &= |\langle 1|+_y\rangle|^2 \\
&= |\langle 1| \frac{1}{\sqrt{2}} (|0\rangle + i\,|1\rangle)\rangle|^2 \\
&= \left| \frac{1}{\sqrt{2}} (\langle 1|0\rangle + i\langle 1|1\rangle) \right|^2 \\
&= \left| \frac{1}{\sqrt{2}} (0 + i \cdot 1) \right|^2 \\
&= \left| \frac{i}{\sqrt{2}} \right|^2 \\
&= \frac{1}{2}.
\end{aligned}$$

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

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

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

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

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. 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.

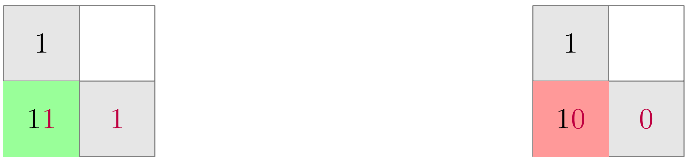

Figure 1: An example of the game, with $\beta_2 = 1, \alpha_1 = \alpha_2 = \beta_1 = 0$. In this round, Alice is assigned the second row, and Bob is assigned the first column. The values in red indicate the answer Alice puts down, and the values in black indicate the answer Bob puts down. In the left 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.

(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]

Solution: The first observation is that one can fill a (unique) grid of entries, that is compatible with the conditions 2 and 3 (i.e. the requirements of both Alice and Bob). We will do this by construction, but first we can see that the sum of all entries is $\alpha_1 + \alpha_2$ which is the sum of the two rows, but it should also be equal to $\beta_1 + \beta_2$ which is the sum of the two columns, and thus these two are equal. The condition that $\alpha_1 \oplus \alpha_2 \oplus \beta_1 \oplus \beta_2 = 0$ is compatible with this.

Let a_{ij} denote the entry in row i and column j of the grid. The rules Alice and Bob must satisfy are given by:

$$a_{11} \oplus a_{12} = \alpha_1 \tag{3}$$
$$a_{21} \oplus a_{22} = \alpha_2 \tag{4}$$
$$a_{11} \oplus a_{21} = \beta_1 \tag{5}$$
$$a_{12} \oplus a_{22} = \beta_2 \tag{6}$$

Assume $\alpha_1 \oplus \alpha_2 \oplus \beta_1 \oplus \beta_2 = 0$. We show that the system of linear equations is consistent, meaning it is possible to fill the four by four grid with zeroes and ones in a way that satisfies the eqs. (3) to (6).

Let $a_{11} = t \in \{0, 1\}$. Then the choices

$$a_{12} = \alpha_1 \oplus t, \tag{7}$$

$$a_{21} = \beta_1 \oplus t, \tag{8}$$

$$a_{22} = \alpha_2 \oplus \beta_1 \oplus t, \tag{9}$$

satisfy eqs. (3) to (6). Indeed:

$$t \oplus (\alpha_1 \oplus t) = \alpha_1,$$

and

$$\begin{aligned}
&a_{21} \oplus a_{22} \\
&= (\beta_1 \oplus t) \oplus (\alpha_2 \oplus \beta_1 \oplus t), \\
&= \alpha_2 \oplus (2t) \oplus (2\beta_1), \\
&= \alpha_2.
\end{aligned}$$

For eq. (5), we have

$$\begin{aligned}
&a_{11} \oplus a_{21} \\
&= t \oplus \beta_1 \oplus t \\
&= \beta_1.
\end{aligned}$$

Finally,

$$\begin{aligned}
&a_{12} \oplus a_{22} \\
&= (\alpha_1 \oplus t) \oplus (\alpha_2 \oplus \beta_1 \oplus t), \\
&= \alpha_1 \oplus \alpha_2 \oplus \beta_1, \\
&= \beta_1 \oplus \beta_2 \oplus \beta_1, \\
&= \beta_2.
\end{aligned}$$

Where we used that $\alpha_1 \oplus \alpha_2 = \beta_1 \oplus \beta_2$, which follows from the first observation we made (that the sum of the columns should be equal to the sum of the rows if Alice and Bob use the same matrix/grid).

(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]

Solution:

This question has two parts. First we need to show that there is no classical strategy that wins with certainty. Then one needs to give a classical deterministic strategy that can win with the maximum probability of 3/4 and explain that this is optimal classically.

Any classical deterministic strategy relies on a pre-agreed set of questions/answers. This corresponds to a 2 × 2 matrix for each player. To win always, they need to use the same grid/matrix (so that the common square always gets the same answer). We note that the sum of the elements of the agreed matrix is equal to the sum of the two rows: $\sum_{i,j} a_{ij} = \alpha_1 \oplus \alpha_2$. But we also note that the sum of the elements of the agreed matrix is equal to the sum of the two columns: $\sum_{i,j} a_{ij} = \beta_1 \oplus \beta_2$. However, by the assumption of this sub-question $\alpha_1 \oplus \alpha_2 \neq \beta_1 \oplus \beta_2$, thus a perfect deterministic strategy does not exist.

The next best that they can have is that Alice and Bob have a strategy that agrees in 3 of the 4 inputs, i.e. they use the same matrix for 3 squares of the grid, while they disagree in the fourth one. If such strategy exists (which we show below), this wins with probability of success 3/4. Note, that the same bound applies for non-deterministic strategies (that may not have fixed set of answers per player), but is harder to prove and required in this question.

Now we show a way to saturate this bound:

For example, let $a_{11} = 0$, then $a_{12} = \alpha_1$, and $a_{21} = \beta_1$. Then, the last square cannot be filled consistently. Alice needs to have sum of row 2 being α_2, thus she needs $a_{22} = \alpha_2 \oplus \beta_1$. Bob needs to have sum of column 2 being β_2 thus needs $b_{22} = \beta_2 \oplus \alpha_1$. But $a_{22} \neq b_{22}$, since $a_{22} \oplus b_{22} = \alpha_2 \oplus \beta_1 \oplus \beta_2 \oplus \alpha_1 = 1$ (according to the constraint of this subquestion).

In other words following the below strategy (where Alice replies the first matrix and Bob replies the second matrix) wins with probability 3/4 (i.e. wins unless the challenger asks Alice's second row and Bob's second column, in which case they lose) and is optimal.

$$\begin{pmatrix} 0 & \alpha_1 \\ \beta_1 & \alpha_2 \oplus \beta_1 \end{pmatrix} \quad ; \quad \begin{pmatrix} 0 & \alpha_1 \\ \beta_1 & \beta_2 \oplus \alpha_1 \end{pmatrix}$$

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

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}), \tag{10}$$

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]

Solution:

After measuring A_i, for $i \in \{0, 1\}$, Alice will obtain outcome ± 1. Let $a = 0$ if she obtains $+1$ and $a = 1$ if she obtains -1. Similarly, after measuring B_j, for $j \in \{0, 1\}$, Bob will obtain outcome ± 1. Let $b = 0$ if he obtains $+1$, and $b = 1$ if he obtains -1.

There are two cases. Suppose Alice is assigned row i and Bob is assigned column j, and $(i, j) \neq (2, 1)$. Then, the sum of the entries in Alice's row is $a \oplus a = 0$, and the sum of the entries in Bob's column is $b \oplus b = 0$.

Suppose Alice is assigned row 2 and Bob is assigned column 1. Then, the sum of the entries in Alice's row is $a \oplus a = 0$, and the sum of the entries in Bob's column is $b \oplus (1 - b) = 1$. These satisfy the constraints.

Now, let's consider the winning condition: Alice and Bob win if their shared cell has the same value. Let $x \equiv i - 1$, $y \equiv j \mod 2$. If $(x, y) \neq (1, 1)$, then Alice and Bob win if and only $a \equiv b \mod 2$. If $(x, y) = (1, 1)$, then Alice and Bob win if and only if $a \equiv b + 1 \mod 2$. This is precisely the winning condition of the CHSH game. and the maximum winning probability is given by $\frac{2 + \sqrt{2}}{4} \approxeq 0.85$.

Note that since the probability of winning given this strategy is larger than the optimal classical strategy, quantumly we can achieve higher probabilities of winning.