INFR111872022-3SS1SEM2 QCS assignment

Jure Sternad

TOTAL POINTS

23 / 25

QUESTION 1

9 pts

1.1 **3 / 3**

✓ **- 0 pts** *Correct*

- 3 pts Wrong/missing

- 2 pts Some steps fine, but details and explanation why missing

- 1.5 pts Explanation for the hard cases (+/- states) missing and expression not following from previous step.

1.2 **3 / 3**

✓ **- 0 pts** *Correct*

- 1.5 pts computed one of e_p,e_b correctly

- 0.5 pts More details on how you got the results are needed

- 2 pts Few steps/thought right, but overall answer wrong

- 3 pts wrong or no answer

1.3 **3 / 3**

✓ **- 0 pts** *Correct*

- 0.5 pts did not mention that at q=1 the rate vanishes so no key can be distilled

- 1 pts Not getting the final condition correctly

- 1.5 pts not specifying result/not giving sufficient details

- 3 pts wrong or missing

- 1.5 pts some steps are correct but wrong result

QUESTION 2

9 pts

2.1 **2 / 2**

✓ **- 0 pts** *Correct*

- 1 pts one binary entropy wrong

- 1 pts some steps ok, but not giving final numerical answer (or wrong answer)

- 2 pts wrong or missing

2.2 **1.5 / 2**

- 0 pts Correct

- 2 pts wrong or missing

✓ **- 0.5 pts** *steps correct but numerical error leads to wrong final answer*

- 1 pts wrong but some correct steps.

2.3 **2 / 2**

✓ **- 0 pts** *Correct*

- 0.5 pts wrong final answer but correct steps

- 1 pts some steps correct but others and the final answer, wrong

- 1.5 pts mostly wrong but some steps correct

2.4 **3 / 3**

✓ **- 0 pts** *Correct*

- 1.5 pts wrong/missing the bound on distinguishing given the fidelity

- 0.5 pts small error (numerical or in definition)

- 2.5 pts mostly wrong but some steps fine

- 3 pts wrong or missing

QUESTION 3

7 pts

3.1 **3 / 3**

✓ **- 0 pts** *Correct*

- 2 pts wrong but some thoughts/method is correct

- 3 pts missing or wrong

3.2 **2 / 2**

✓ **- 0 pts** *Correct*

- 1 pts explanation for valid strategy correct, but probability of success wrong or missing

- 0.5 pts numerical error/miscalculation

- 2 pts missing or wrong

- 1 pts steps correct for both parts, but also mistakes leading to wrong conclusion

3.3 **0.5 / 2**

- 0 pts Correct

- 0.5 pts some details are missing

- 2 pts missing or wrong

- 1 pts good ideas but wrong in the details

✓ **- 1.5 pts** *mostly wrong but some ideas fine*

1 you don't use the non-local game in your QKD protocol

Question 1

(a)

- $|0\rangle \rightarrow \Phi_q(|0\rangle\langle 0|) = (1-q)|0\rangle\langle 0| + q\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\0 & -i\end{bmatrix} = (1-q)|0\rangle\langle 0| + q\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} = |0\rangle\langle 0|$
- $|1\rangle \rightarrow \Phi_q(|1\rangle\langle 1|) = (1-q)|1\rangle\langle 1| + q\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\0 & -i\end{bmatrix} = (1-q)|1\rangle\langle 1| + q\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix} = |1\rangle\langle 1|$
- $|+\rangle \rightarrow \Phi_q(|+\rangle\langle +|) = (1-q)|+\rangle\langle +| + \frac{q}{2}\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\0 & -i\end{bmatrix} = (1-q)|+\rangle\langle +| + \frac{q}{2}\begin{bmatrix}1 & 1\\i & i\end{bmatrix}\begin{bmatrix}1 & 0\\0 & -i\end{bmatrix} =$ $(1-q)|+\rangle\langle +| + \frac{q}{2}\begin{bmatrix}1 & -i\\i & -1\end{bmatrix} = |+\rangle\langle +|(1-q) + q|+_y\rangle\langle +_y|$,
  since $|+_y\rangle\langle +_y| = \begin{bmatrix}1 & -i\\i & -1\end{bmatrix}$
- $|-\rangle \rightarrow \Phi_q(|-\rangle\langle -|) = (1-q)|-\rangle\langle -| + \frac{q}{2}\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}\begin{bmatrix}1 & -1\\-1 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\0 & -i\end{bmatrix} = (1-q)|-\rangle\langle -| +$ $\frac{q}{2}\begin{bmatrix}1 & -1\\-i & i\end{bmatrix}\begin{bmatrix}1 & 0\\0 & -i\end{bmatrix} = (1-q)|-\rangle\langle -| + \frac{q}{2}\begin{bmatrix}1 & i\\-i & -1\end{bmatrix} = |-\rangle\langle -|(1-q) + q|-_y\rangle\langle -_y|$,
  since $|-_y\rangle\langle -_y| = \begin{bmatrix}1 & i\\-i & 1\end{bmatrix}$

(b)

- Probability that Alice sent the state $|0\rangle$ and that Bob measured $|1\rangle$:

$$Tr(\Phi_q(|0\rangle\langle 0|)|1\rangle\langle 1|) = \langle 1|\Phi_q(|0\rangle\langle 0|)|1\rangle = \langle 1|0\rangle\langle 0|1\rangle = 0$$

- Probability that Alice sent the state $|1\rangle$ and that Bob measured $|0\rangle$:

$$Tr(\Phi_q(|1\rangle\langle 1|)|0\rangle\langle 0|) = \langle 0|\Phi_q(|1\rangle\langle 1|)|0\rangle = \langle 0|1\rangle\langle 1|0\rangle = 0$$

- Probability that Alice sent the state $|+\rangle$ and that Bob measured $|-\rangle$:

$$Tr(\Phi_q(|+\rangle\langle +|)|-\rangle\langle -|) = \ldots = \frac{q}{2}$$

- Probability that Alice sent the state $|-\rangle$ and that Bob measured $|+\rangle$:

$$Tr(\Phi_q(|-\rangle\langle -|)|+\rangle\langle +|) = \ldots = \frac{q}{2}$$

$\implies e_b = 0$ and $e_p = \frac{\frac{q}{2}+\frac{q}{2}}{2} = \frac{q}{2}$

1.1 **3 / 3**

✓ **- 0 pts** *Correct*

- 3 pts Wrong/missing

- 2 pts Some steps fine, but details and explanation why missing

- 1.5 pts Explanation for the hard cases (+/- states) missing and expression not following from previous step.

Question 1

(a)

- $|0\rangle \to \Phi_q(|0\rangle\langle 0|) = (1-q)|0\rangle\langle 0| + q\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix} = (1-q)|0\rangle\langle 0| + q\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix} = |0\rangle\langle 0|$
- $|1\rangle \to \Phi_q(|1\rangle\langle 1|) = (1-q)|1\rangle\langle 1| + q\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix} = (1-q)|1\rangle\langle 1| + q\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix} = |1\rangle\langle 1|$
- $|+\rangle \to \Phi_q(|+\rangle\langle +|) = (1-q)|+\rangle\langle +| + \frac{q}{2}\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix} = (1-q)|+\rangle\langle +| + \frac{q}{2}\begin{bmatrix}1 & 1\\ i & i\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix} =$
  $(1-q)|+\rangle\langle +| + \frac{q}{2}\begin{bmatrix}1 & -i\\ i & -1\end{bmatrix} = |+\rangle\langle +|(1-q) + q|+_y\rangle\langle +_y|$,
  since $|+_y\rangle\langle +_y| = \begin{bmatrix}1 & -i\\ i & -1\end{bmatrix}$
- $|-\rangle \to \Phi_q(|-\rangle\langle -|) = (1-q)|-\rangle\langle -| + \frac{q}{2}\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{bmatrix}1 & -1\\ -1 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix} = (1-q)|-\rangle\langle -| +$
  $\frac{q}{2}\begin{bmatrix}1 & -1\\ -i & i\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix} = (1-q)|-\rangle\langle -| + \frac{q}{2}\begin{bmatrix}1 & i\\ -i & -1\end{bmatrix} = |-\rangle\langle -|(1-q) + q|-_y\rangle\langle -_y|$,
  since $|-_y\rangle\langle -_y| = \begin{bmatrix}1 & i\\ -i & 1\end{bmatrix}$

(b)

- Probability that Alice sent the state $|0\rangle$ and that Bob measured $|1\rangle$:
  $$Tr(\Phi_q(|0\rangle\langle 0|)|1\rangle\langle 1|) = \langle 1|\Phi_q(|0\rangle\langle 0|)|1\rangle = \langle 1|0\rangle\langle 0|1\rangle = 0$$
- Probability that Alice sent the state $|1\rangle$ and that Bob measured $|0\rangle$:
  $$Tr(\Phi_q(|1\rangle\langle 1|)|0\rangle\langle 0|) = \langle 0|\Phi_q(|1\rangle\langle 1|)|0\rangle = \langle 0|1\rangle\langle 1|0\rangle = 0$$
- Probability that Alice sent the state $|+\rangle$ and that Bob measured $|-\rangle$:
  $$Tr(\Phi_q(|+\rangle\langle +|)|-\rangle\langle -|) = \ldots = \frac{q}{2}$$
- Probability that Alice sent the state $|-\rangle$ and that Bob measured $|+\rangle$:
  $$Tr(\Phi_q(|-\rangle\langle -|)|+\rangle\langle +|) = \ldots = \frac{q}{2}$$

$\implies e_b = 0$ and $e_p = \frac{\frac{q}{2}+\frac{q}{2}}{2} = \frac{q}{2}$

1.2 **3 / 3**

✓ **- 0 pts** *Correct*

- **- 1.5 pts** computed one of e_p,e_b correctly
- **- 0.5 pts** More details on how you got the results are needed
- **- 2 pts** Few steps/thought right, but overall answer wrong
- **- 3 pts** wrong or no answer

(c)

$Q = 1, \xi = 1, \triangle(n, \epsilon) = 0$

$$\implies R_{BB84} = \frac{1}{2}(1 - h(e_b) - h(e_p)) = \frac{1}{2}(1 + \frac{q}{2}\log\frac{q}{2} + (1 - \frac{q}{2})\log(1 - \frac{q}{2})),$$

since

$$e_b = 0 \implies h(e_b) = 0$$

$$e_p = \frac{1}{2} \implies h(e_p) = -\frac{q}{2}\log\frac{q}{2} - (1 - \frac{q}{2})\log(1 - \frac{q}{2})$$

Secret key is possible to distil when $\frac{1}{2}(1 + \frac{q}{2}\log\frac{q}{2} + (1 - \frac{q}{2})\log(1 - \frac{q}{2})) > 0$, or when $q = 0$. This holds $\iff q \in (0, 1) \cap (1, 2)$. Since q is a probability, it holds that it is possible to distil the secret key for any $q \in [0, 1)$.

Question 2

(a)

- $h(\frac{1}{8}) = -\frac{1}{8}\log\frac{1}{8} - \frac{7}{8}\log\frac{7}{8} = -\frac{1}{8}(-3) - \frac{7}{8}\log\frac{7}{8} = \frac{3}{8} - \approx 0.544$
- $h(\frac{1}{16}) = -\frac{1}{16}\log\frac{1}{16} - \frac{15}{16}\log\frac{15}{16} = -\frac{1}{16}(-4) - \frac{15}{16}\log\frac{15}{16} = \frac{1}{4} - \frac{15}{16}\log\frac{15}{16} \approx 0.337$

(b)

We first calculate the density matrix for ρ:

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

To find the eigenvalues, we first calculate the determinant of $\begin{bmatrix} \frac{3}{4} - \lambda & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} - \lambda \end{bmatrix}$:

$$(\frac{3}{4} - \lambda)(\frac{1}{4} - \lambda) - \frac{1}{16} = \frac{3}{16} - \lambda + \lambda^2 - \frac{1}{16} = \lambda^2 - \lambda + \frac{1}{8}$$

Then we see that $\lambda^2 - \lambda + \frac{1}{8} = 0 \iff \lambda = \frac{2 \pm \sqrt{2}}{4}$
Finally, we calculate the von Neumann entropy as follows:

$$H(\rho) = \frac{2 - \sqrt{2}}{4}\log(\frac{2 - \sqrt{2}}{4}) - \frac{2 + \sqrt{2}}{4}\log(\frac{2 + \sqrt{2}}{4}) \approx 0.122 + 0.059 = 0.181$$

(c)

$$\Phi(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger =$$

$$= \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \sqrt{1-p}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \sqrt{1-p}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{4}(\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}) = \frac{1}{4}\begin{bmatrix} 1 & -1 \\ -1 & 3 \end{bmatrix}$$

1.3 **3 / 3**

✓ **- 0 pts** *Correct*

- 0.5 pts did not mention that at q=1 the rate vanishes so no key can be distilled

- 1 pts Not getting the final condition correctly

- 1.5 pts not specifying result/not giving sufficient details

- 3 pts wrong or missing

- 1.5 pts some steps are correct but wrong result

(c)

$Q = 1, \xi = 1, \triangle(n, \epsilon) = 0$

$$\implies R_{BB84} = \frac{1}{2}(1 - h(e_b) - h(e_p)) = \frac{1}{2}(1 + \frac{q}{2}\log\frac{q}{2} + (1 - \frac{q}{2})\log(1 - \frac{q}{2})),$$

since

$$e_b = 0 \implies h(e_b) = 0$$

$$e_p = \frac{1}{2} \implies h(e_p) = -\frac{q}{2}\log\frac{q}{2} - (1 - \frac{q}{2})\log(1 - \frac{q}{2})$$

Secret key is possible to distil when $\frac{1}{2}(1 + \frac{q}{2}\log\frac{q}{2} + (1 - \frac{q}{2})\log(1 - \frac{q}{2})) > 0$, or when $q = 0$. This holds $\iff q \in (0, 1) \cap (1, 2)$. Since q is a probability, it holds that it is possible to distil the secret key for any $q \in [0, 1)$.

Question 2

(a)

- $h(\frac{1}{8}) = -\frac{1}{8}\log\frac{1}{8} - \frac{7}{8}\log\frac{7}{8} = -\frac{1}{8}(-3) - \frac{7}{8}\log\frac{7}{8} = \frac{3}{8} - \approx 0.544$
- $h(\frac{1}{16}) = -\frac{1}{16}\log\frac{1}{16} - \frac{15}{16}\log\frac{15}{16} = -\frac{1}{16}(-4) - \frac{15}{16}\log\frac{15}{16} = \frac{1}{4} - \frac{15}{16}\log\frac{15}{16} \approx 0.337$

(b)

We first calculate the density matrix for ρ:

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

To find the eigenvalues, we first calculate the determinant of $\begin{bmatrix} \frac{3}{4} - \lambda & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} - \lambda \end{bmatrix}$:

$$(\frac{3}{4} - \lambda)(\frac{1}{4} - \lambda) - \frac{1}{16} = \frac{3}{16} - \lambda + \lambda^2 - \frac{1}{16} = \lambda^2 - \lambda + \frac{1}{8}$$

Then we see that $\lambda^2 - \lambda + \frac{1}{8} = 0 \iff \lambda = \frac{2 \pm \sqrt{2}}{4}$
Finally, we calculate the von Neumann entropy as follows:

$$H(\rho) = \frac{2 - \sqrt{2}}{4}\log(\frac{2 - \sqrt{2}}{4}) - \frac{2 + \sqrt{2}}{4}\log(\frac{2 + \sqrt{2}}{4}) \approx 0.122 + 0.059 = 0.181$$

(c)

$$\Phi(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger =$$

$$= \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \sqrt{1-p}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\sqrt{1-p}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{4}(\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}) = \frac{1}{4}\begin{bmatrix} 1 & -1 \\ -1 & 3 \end{bmatrix}$$

2.1 **2 / 2**

✓ **- 0 pts** *Correct*

- 1 pts one binary entropy wrong

- 1 pts some steps ok, but not giving final numerical answer (or wrong answer)

- 2 pts wrong or missing

(c)

$Q = 1, \xi = 1, \triangle(n, \epsilon) = 0$

$$\implies R_{BB84} = \frac{1}{2}(1 - h(e_b) - h(e_p)) = \frac{1}{2}(1 + \frac{q}{2}\log\frac{q}{2} + (1 - \frac{q}{2})\log(1 - \frac{q}{2})),$$

since

$$e_b = 0 \implies h(e_b) = 0$$

$$e_p = \frac{1}{2} \implies h(e_p) = -\frac{q}{2}\log\frac{q}{2} - (1 - \frac{q}{2})\log(1 - \frac{q}{2})$$

Secret key is possible to distil when $\frac{1}{2}(1 + \frac{q}{2}\log\frac{q}{2} + (1 - \frac{q}{2})\log(1 - \frac{q}{2})) > 0$, or when $q = 0$. This holds $\iff q \in (0, 1) \cap (1, 2)$. Since q is a probability, it holds that it is possible to distil the secret key for any $q \in [0, 1)$.

Question 2

(a)

- $h(\frac{1}{8}) = -\frac{1}{8}\log\frac{1}{8} - \frac{7}{8}\log\frac{7}{8} = -\frac{1}{8}(-3) - \frac{7}{8}\log\frac{7}{8} = \frac{3}{8} - \approx 0.544$
- $h(\frac{1}{16}) = -\frac{1}{16}\log\frac{1}{16} - \frac{15}{16}\log\frac{15}{16} = -\frac{1}{16}(-4) - \frac{15}{16}\log\frac{15}{16} = \frac{1}{4} - \frac{15}{16}\log\frac{15}{16} \approx 0.337$

(b)

We first calculate the density matrix for ρ:

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

To find the eigenvalues, we first calculate the determinant of $\begin{bmatrix} \frac{3}{4} - \lambda & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} - \lambda \end{bmatrix}$:

$$(\frac{3}{4} - \lambda)(\frac{1}{4} - \lambda) - \frac{1}{16} = \frac{3}{16} - \lambda + \lambda^2 - \frac{1}{16} = \lambda^2 - \lambda + \frac{1}{8}$$

Then we see that $\lambda^2 - \lambda + \frac{1}{8} = 0 \iff \lambda = \frac{2 \pm \sqrt{2}}{4}$

Finally, we calculate the von Neumann entropy as follows:

$$H(\rho) = \frac{2 - \sqrt{2}}{4}\log(\frac{2 - \sqrt{2}}{4}) - \frac{2 + \sqrt{2}}{4}\log(\frac{2 + \sqrt{2}}{4}) \approx 0.122 + 0.059 = 0.181$$

(c)

$$\Phi(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger =$$

$$= \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \sqrt{1-p}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \sqrt{1-p}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{4}(\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}) = \frac{1}{4}\begin{bmatrix} 1 & -1 \\ -1 & 3 \end{bmatrix}$$

2.2 **1.5 / 2**

- **- 0 pts** Correct
- **- 2 pts** wrong or missing
- ✓ **- 0.5 pts** *steps correct but numerical error leads to wrong final answer*
- **- 1 pts** wrong but some correct steps.

(c)

$Q = 1, \xi = 1, \triangle(n, \epsilon) = 0$

$$\implies R_{BB84} = \frac{1}{2}(1 - h(e_b) - h(e_p)) = \frac{1}{2}(1 + \frac{q}{2}\log\frac{q}{2} + (1 - \frac{q}{2})\log(1 - \frac{q}{2})),$$

since

$$e_b = 0 \implies h(e_b) = 0$$

$$e_p = \frac{1}{2} \implies h(e_p) = -\frac{q}{2}\log\frac{q}{2} - (1 - \frac{q}{2})\log(1 - \frac{q}{2})$$

Secret key is possible to distil when $\frac{1}{2}(1 + \frac{q}{2}\log\frac{q}{2} + (1 - \frac{q}{2})\log(1 - \frac{q}{2})) > 0$, or when $q = 0$. This holds $\iff q \in (0, 1) \cap (1, 2)$. Since q is a probability, it holds that it is possible to distil the secret key for any $q \in [0, 1)$.

Question 2

(a)

- $h(\frac{1}{8}) = -\frac{1}{8}\log\frac{1}{8} - \frac{7}{8}\log\frac{7}{8} = -\frac{1}{8}(-3) - \frac{7}{8}\log\frac{7}{8} = \frac{3}{8} - \approx 0.544$
- $h(\frac{1}{16}) = -\frac{1}{16}\log\frac{1}{16} - \frac{15}{16}\log\frac{15}{16} = -\frac{1}{16}(-4) - \frac{15}{16}\log\frac{15}{16} = \frac{1}{4} - \frac{15}{16}\log\frac{15}{16} \approx 0.337$

(b)

We first calculate the density matrix for ρ:

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

To find the eigenvalues, we first calculate the determinant of $\begin{bmatrix} \frac{3}{4} - \lambda & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} - \lambda \end{bmatrix}$:

$$(\frac{3}{4} - \lambda)(\frac{1}{4} - \lambda) - \frac{1}{16} = \frac{3}{16} - \lambda + \lambda^2 - \frac{1}{16} = \lambda^2 - \lambda + \frac{1}{8}$$

Then we see that $\lambda^2 - \lambda + \frac{1}{8} = 0 \iff \lambda = \frac{2 \pm \sqrt{2}}{4}$

Finally, we calculate the von Neumann entropy as follows:

$$H(\rho) = \frac{2 - \sqrt{2}}{4}\log(\frac{2 - \sqrt{2}}{4}) - \frac{2 + \sqrt{2}}{4}\log(\frac{2 + \sqrt{2}}{4}) \approx 0.122 + 0.059 = 0.181$$

(c)

$$\Phi(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger =$$

$$= \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \sqrt{1-p}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \sqrt{1-p}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} =$$

$$= \frac{1}{4}(\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}) = \frac{1}{4}\begin{bmatrix} 1 & -1 \\ -1 & 3 \end{bmatrix}$$

2.3 **2 / 2**

✓ **- 0 pts** *Correct*

- 0.5 pts wrong final answer but correct steps

- 1 pts some steps correct but others and the final answer, wrong

- 1.5 pts mostly wrong but some steps correct

(d)

$$F(\rho,\sigma) = Tr(\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}) = Tr(\sqrt{\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\\frac{1}{2} & \frac{1}{2}\end{bmatrix}\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}}) = Tr(\sqrt{\begin{bmatrix}0 & 0\\0 & \frac{1}{2}\end{bmatrix}}) = \frac{1}{\sqrt{2}}$$

$$D(\rho,\sigma) = \frac{1}{2}Tr(|\rho-\sigma|) = \frac{1}{2}Tr(|\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix} - \begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\\frac{1}{2} & \frac{1}{2}\end{bmatrix}|) = \frac{1}{2}Tr(|\frac{1}{2}\begin{bmatrix}-1 & -1\\-1 & 1\end{bmatrix}|) =$$

$$= \frac{1}{2}Tr(\sqrt{\frac{1}{4}\begin{bmatrix}-1 & -1\\-1 & 1\end{bmatrix}\begin{bmatrix}-1 & -1\\-1 & 1\end{bmatrix}} = \frac{1}{2}Tr(\sqrt{\begin{bmatrix}\frac{1}{2} & 0\\0 & \frac{1}{2}\end{bmatrix}}) = \frac{1}{2}Tr(\begin{bmatrix}\sqrt{\frac{1}{2}} & 0\\0 & \sqrt{\frac{1}{2}}\end{bmatrix}) = \frac{1}{\sqrt{2}}$$

The maximum probability that Charlie can correctly identify the state is $\frac{1}{2}(1+D(\rho,\sigma)) = \frac{1}{2}(1+\frac{1}{\sqrt{2}}) \approx 0.854$.

Question 3

(a)

The following is an example of the Mermin-Peres magic square game. It is known that the best classical strategy can ensure the win probability of $\frac{8}{9}$. In order to satisfy the rules, the players can choose the following sets of values:

- Alice can either fill the row with the numbers 1,-1,-1 or 1,1,1.
- Bob can either fill the column with the numbers: 1,1,-1 or -1,-1,-1

In order to maximize the probability of winning, they must pick a set of numbers where most of the match is. There are two equivalent solutions:

- Alice picks 1,-1,-1 and Bob picks -1,-1,-1
- Alice picks 1,1,1 and Bob picks 1,1,-1

In both cases, there are five equal values and one different. Let us assume that Alice and Bob decide: Alice picks 1,-1,-1 and Bob picks -1,-1,-1. Since they always share one cell, the probability of winning is the same for any of the nine scenarios. Let us observe the scenario where Alice gets the first row, and Bob gets the first column. As we can see, the only scenario where they lose the game is:

1,-1	-1	-1
1		
1		

There are nine possible outcomes (since we need to distinguish between all the values), and the probability of them losing is $\frac{1}{9}$. Since that is the case for any row and column Alice and Bob get, the final probability of them winning the game is $\frac{8}{9}$.

2.4 **3 / 3**

✓ **- 0 pts** *Correct*

- 1.5 pts wrong/missing the bound on distinguishing given the fidelity

- 0.5 pts small error (numerical or in definition)

- 2.5 pts mostly wrong but some steps fine

- 3 pts wrong or missing

(d)

$$F(\rho,\sigma) = Tr(\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}) = Tr(\sqrt{\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\\frac{1}{2} & \frac{1}{2}\end{bmatrix}\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}}) = Tr(\sqrt{\begin{bmatrix}0 & 0\\0 & \frac{1}{2}\end{bmatrix}}) = \frac{1}{\sqrt{2}}$$

$$D(\rho,\sigma) = \frac{1}{2}Tr(|\rho-\sigma|) = \frac{1}{2}Tr(|\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix} - \begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\\frac{1}{2} & \frac{1}{2}\end{bmatrix}|) = \frac{1}{2}Tr(|\frac{1}{2}\begin{bmatrix}-1 & -1\\-1 & 1\end{bmatrix}|) =$$

$$= \frac{1}{2}Tr(\sqrt{\frac{1}{4}\begin{bmatrix}-1 & -1\\-1 & 1\end{bmatrix}\begin{bmatrix}-1 & -1\\-1 & 1\end{bmatrix}} = \frac{1}{2}Tr(\sqrt{\begin{bmatrix}\frac{1}{2} & 0\\0 & \frac{1}{2}\end{bmatrix}}) = \frac{1}{2}Tr(\begin{bmatrix}\sqrt{\frac{1}{2}} & 0\\0 & \sqrt{\frac{1}{2}}\end{bmatrix}) = \frac{1}{\sqrt{2}}$$

The maximum probability that Charlie can correctly identify the state is $\frac{1}{2}(1 + D(\rho,\sigma)) = \frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \approx 0.854$.

Question 3

(a)

The following is an example of the Mermin-Peres magic square game. It is known that the best classical strategy can ensure the win probability of $\frac{8}{9}$. In order to satisfy the rules, the players can choose the following sets of values:

- Alice can either fill the row with the numbers 1,-1,-1 or 1,1,1.
- Bob can either fill the column with the numbers: 1,1,-1 or -1,-1,-1

In order to maximize the probability of winning, they must pick a set of numbers where most of the match is. There are two equivalent solutions:

- Alice picks 1,-1,-1 and Bob picks -1,-1,-1
- Alice picks 1,1,1 and Bob picks 1,1,-1

In both cases, there are five equal values and one different. Let us assume that Alice and Bob decide: Alice picks 1,-1,-1 and Bob picks -1,-1,-1. Since they always share one cell, the probability of winning is the same for any of the nine scenarios. Let us observe the scenario where Alice gets the first row, and Bob gets the first column. As we can see, the only scenario where they lose the game is:

1,-1	-1	-1
1		
1		

There are nine possible outcomes (since we need to distinguish between all the values), and the probability of them losing is $\frac{1}{9}$. Since that is the case for any row and column Alice and Bob get, the final probability of them winning the game is $\frac{8}{9}$.

3.1 **3 / 3**

✓ **- 0 pts** *Correct*

- 2 pts wrong but some thoughts/method is correct

- 3 pts missing or wrong

(b)

As it was shown in many papers, if the players are allowed to share an entangled quantum state, it is possible for them to win the magic square game with certainty. In order to see why this strategy is valid (the products of row and colum values are correct), let us consider the following:

- The three matrices in any one row, or in any one column, of this grid all commute with each other. That is, we can multiply any two or three of them together in any order, and the result will not be affected by the order.
- If we multiply all three matrices in any row, we always get the identity matrix.
- If we multiply all three matrices in any column, we always get the opposite of the identity matrix.
- For each of the nine matrices, all of their eigenvectors have eigenvalues of 1 or –1.

As a result, each cell within the specified context is filled with either a 1 or a 0, where the product of the row cells is equivalent to 1 and the product of the column cells is equivalent to -1.

Since all the matrices commute with one another, it is possible to identify four orthogonal vectors in the 4-dimensional space that serve as simultaneous eigenvectors of all three matrices at once. For instance, considering the third row, the standard basis vectors:

$$\{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$$

can serve as eigenvectors for all three matrices, and the four corresponding eigenvalues can be obtained from the diagonals of each of the three matrices consecutively:

$$\{1,-1,1,-1\}$$

$$\{1,-1,-1,1\}$$

$$\{1,1,-1,-1\}$$

Therefore, we can construct a single measurement on the quantum system that tells us all three quantities measured by the three matrices in the row or column.

In order to understand how the answers of Alice and Bob are correlated, they must share maximally entangled states. A maximally entangled state possesses a specific type of symmetry such that if Ψ is maximally entangled and U is any unitary operation, then $U \otimes U^{\dagger} |\Psi\rangle = |\Psi\rangle$.Therefore, if Bob measures in the same basis as Alice, their outcomes will be fully correlated. Therefore even if Alice and Bob use different measurement choices, their outcomes at the intersections will agree.

Assuming that A represents any observable applicable to Alice's system, and B corresponds to the corresponding observable for Bob's system, the correlation value of $\langle\Psi| AB |\Psi\rangle = 1$ ensures that the players win the game every time.

3.2 **2 / 2**

✓ **- 0 pts** *Correct*

- **- 1 pts** explanation for valid strategy correct, but probability of success wrong or missing
- **- 0.5 pts** numerical error/miscalculation
- **- 2 pts** missing or wrong
- **- 1 pts** steps correct for both parts, but also mistakes leading to wrong conclusion

(c)

The protocol can work as follows:

1. Any trusted or untrusted party distributes to Alice and Bob n copies of the state Ψ
2. Alice measures chooses a random row from the grid and measures in all of the three observables $x^{(i)} = (x_1^{(i)}, x_2^{(i)}, x_3^{(i)})$. She obtains triplets of results $a^{(i)} = (a_1^{(i)}, a_2^{(i)}, a_3^{(i)})$. It holds that $a_j^{(i)} \in \{-1, 1\}$ for any j. She stores pairs of $(a^{(i)}, x^{(i)})_n$
3. Bob measures chooses a random row from the grid and measures in all of the three observables $y^{(i)} = (y_1^{(i)}, y_2^{(i)}, y_3^{(i)})$. He obtains triplets of results $b^{(i)} = (b_1^{(i)}, b_2^{(i)}, b_3^{(i)})$. It holds that $b_j^{(i)} \in \{-1, 1\}$ for any j. He stores pairs of $(b^{(i)}, y^{(i)})_n$
4. Alice and Bob announce the bases $x^{(i)}, y^{(i)}$ and they keep positions where they used the same basis
5. If there was no eavesdropping then $a^{(i)} = b^{(i)}$ $\forall i$ of the raw key

Intuition: If non-locality exists, then it is impossible for Eve to have a perfect correlation with Alice's string. This is due to the monogamy of entanglement, which is valid for maximum violation and applies to any violation because the presence of local hidden variables would be implied by perfect correlation.

3.3 **0.5 / 2**

- **- 0 pts** Correct
- **- 0.5 pts** some details are missing
- **- 2 pts** missing or wrong
- **- 1 pts** good ideas but wrong in the details

✓ **- 1.5 pts** *mostly wrong but some ideas fine*

1 you don't use the non-local game in your QKD protocol

gradescope

School of Informatics

Quantum Cyber Security
Coursework

B232245
April 2023