Written exam MPRI 2-34-2
Quantum Information and Cryptography

March 7th, 2023. 12h45 –15h45 (3 hours)

The grading scale (points per question) is indicative only and is subject to change.

Notations

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{2}(|0\rangle - |1\rangle)$. $S(\rho) = -\rho \log_2(\rho)$. We also define $|0\rangle^+ = |0\rangle, |1\rangle^+ = |1\rangle, |0\rangle^\times = |+\rangle, |1\rangle^\times = |-\rangle$. We also define the Bell basis $\{|\Phi_+\rangle, |\Phi_-\rangle, |\Psi_+\rangle, |\Psi_-\rangle\}$ with

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \quad ; \quad |\Phi_-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$$
$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \quad ; \quad |\Psi_-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

Part 1: Quantum information and cryptography (10 points)

Question 1 (4 points)**.** *Let $|\psi_{AB}\rangle$ be any quantum pure state on 2 qubits. Each register A and B contains one of the qubits. Let $\rho_A = tr_B(|\psi_{AB}\rangle\langle\psi_{AB}|)$ and $\rho_B = tr_A(|\psi_{AB}\rangle\langle\psi_{AB}|)$. For each of the following assertions, say whether they are true or false, justify your answers.*

1. *If $\rho_A = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$ then necessarily $\rho_B = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$.*
2. *If $\rho_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ then necessarily $\rho_B = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$.*
3. *There exists a unitary U acting on 1 qubit st. $U\rho_A U^\dagger = \rho_B$.*
4. *If $\rho_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$, then $S(\rho_A) = 1$.*
5. *If $\rho_A = \frac{1}{3}|+\rangle\langle +| + \frac{2}{3}|-\rangle\langle -|$, then $S(\rho_B) = \log_2(3) - \frac{2}{3}$.*

Solution:

1. False: take for example $|\psi_{AB}\rangle = \sqrt{\frac{2}{3}}|0+\rangle + \sqrt{\frac{1}{3}}|1-\rangle$. We have $\rho_B = \frac{2}{3}|+\rangle\langle +| + \frac{1}{3}|-\rangle\langle -| \neq \rho_A$.
2. True: We can write the Schmidt decomposition $|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}|0\rangle|e_0\rangle + \frac{1}{\sqrt{2}}|1\rangle|e_1\rangle$. This gives $\rho_B = \frac{1}{2}|e_0\rangle\langle e_0| + \frac{1}{2}|e_1\rangle\langle e_1|$ where the $|e_i\rangle$ are pairwise orthogonal, which means $\rho_B = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} = \rho_A$.
3. True: Again from the Schmidt decomposition $|\psi_{AB}\rangle = \sum_i \alpha_i |e_i\rangle|f_i\rangle$, we have $\rho_A = \sum_i \lambda_i |e_i\rangle\langle e_i|$ and $\rho_B = \sum_i \lambda_i |e_i\rangle\langle e_i|$. Take the unitary $U : |e_i\rangle \to |f_i\rangle$ and we have indeed $U\rho_A U^\dagger = \rho_B$.
4. False: $\rho_A = \cos^2(\pi/8)|v\rangle\langle v| + \sin^2(\pi/8)|v^\perp\rangle\langle v^\perp|$ with $|v\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ and $|v^\perp\rangle$ is orthogonal to $|v\rangle$.
5. True: we have the spectral decomposition of ρ_A so $S(\rho_A) = -1/3\log_2(1/3) - 2/3\log_2(2/3) = \log_2(3) - \frac{2}{3}$.

□

Question 2 (2 points)**.** *Let* $|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle$*. Compute* $\rho_A = Tr_B|\psi_{AB}\rangle\langle\psi_{AB}|$ *and* $\rho_B = Tr_A|\psi_{AB}\rangle\langle\psi_{AB}|$*. Write the result in matrix form.*

Solution:

$$|\psi_{AB}\rangle = \frac{\sqrt{3}}{2}\left(\sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle\right)|0\rangle + \frac{1}{2}|01\rangle$$

so $\rho_A = \frac{3}{4}|\psi_1\rangle\langle\psi_1| + \frac{1}{4}|1\rangle\langle 1|$ with $|\psi_1\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$. This gives

$$\rho_A = \frac{3}{4}\begin{pmatrix} 2/3 & \sqrt{2}/9 \\ \sqrt{2}/9 & 1/3 \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1/2 & \sqrt{2}/12 \\ \sqrt{2}/12 & 1/2 \end{pmatrix}.$$

Notice that $|\psi_{AB}\rangle$ is symmetric with respect to swapping the A and B registers so $\rho_A = \rho_B$. □

Question 3 (4 points)**.** *Alice wants to perform a BB84 protocol with Bob. Recall that Alice uses the following BB84 encoding: for each bit k of the raw key (which is a uniformly random bit) and for a random of basis $b \in \{+, \times\}$ Alice sends $|k\rangle^b$ to Bob.*

1. *Assume Alice's source creates perfect qubits. Show that this encoding doesn't reveal any information about the basis b to Bob.*

2. *In practice, Alice can use an attenuated photonic source that is faulty and sometimes doubles the created state. This means that instead of creating $|k\rangle^b$, she sometimes creates $|\psi_k^b\rangle = |k\rangle^b \otimes |k\rangle^b$. When this happens, show that from the sent state $|\psi_k^b\rangle$, an eavesdropper can recover some information about b. What is the maximal probability of guessing b from $|\psi_k^b\rangle$ and what is the optimal measurement to achieve this optimal guessing probability? (Hint: Let σ_b be the state that Bob has when the photon doubles and when Alice has b. Show that $\sigma_0 = \frac{1}{2}|\Phi_+\rangle\langle\Phi_+| + \frac{1}{2}|\Phi_-\rangle\langle\Phi_-|$ $\sigma_1 = \frac{1}{2}|\Phi_+\rangle\langle\Phi_+| + \frac{1}{2}|\Psi_+\rangle\langle\Psi_+|$)*

Solution:

1. Let ρ_b be the state that Bob has depending on Alice's basis b. We have $\rho_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \mathbb{I}$. Similarly, $\rho_1 = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \mathbb{I} = \rho_0$ so Bob has no information about b.

2. Let σ_b be the state that Bob has when the photon doubles. We have $\sigma_0 = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$ and $\sigma_1 = \frac{1}{2}|++\rangle\langle ++| + \frac{1}{2}|--\rangle\langle --|$. We now write

$$\sigma_0 = \begin{pmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 \end{pmatrix}$$

$$\sigma_1 = \frac{1}{8}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} + \frac{1}{8}\begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Moreover,

$$\frac{1}{2}|\Phi_+\rangle\langle\Phi_+| + \frac{1}{2}|\Phi_-\rangle\langle\Phi_-| = \frac{1}{4}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix} + \frac{1}{4}\begin{pmatrix}1&0&0&-1\\0&0&0&0\\0&0&0&0\\-1&0&0&1\end{pmatrix} = \sigma_0$$

$$\frac{1}{2}|\Phi_+\rangle\langle\Phi_+| + \frac{1}{2}|\Psi_+\rangle\langle\Psi_+| = \frac{1}{4}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix} + \frac{1}{4}\begin{pmatrix}0&0&0&0\\0&1&1&0\\0&1&1&0\\0&0&0&0\end{pmatrix} = \sigma_1$$

This means σ_0, σ_1 are diagonalizable in the Bell basis. From there, we have $\Delta(\sigma_0, \sigma_1) = \frac{1}{2}$ and the probability that Bob guesses b is $\frac{1}{2} + \Delta(\rho_0, \rho_1)/2 = \frac{3}{4}$. Since the 2 states are diagonalizable in the Bell basis, the optimal distinguishing measurement is the measurement in the Bell basis.

□