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 $S(\rho_B) = \log_2(3) - \frac{2}{3}$.*

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.*

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 $\sigma_0 = \frac{1}{2}|\Phi_+\rangle\langle\Phi_+| + \frac{1}{2}|\Phi_-\rangle\langle\Phi_-|$ $\sigma_1 = \frac{1}{2}|\Phi_+\rangle\langle\Phi_+| + \frac{1}{2}|\Psi_+\rangle\langle\Psi_+|$)*