INDIAN STATISTICAL INSTITUTE
M. Tech. (CrS) – II, Year: 2025–2026
Quantum Cryptology and Security
Mid-Semester Examination

**Date:** 08. 09. 2025 **Marks:** 30 **Time:** 1.5 Hours

**There are three questions. Each question is worth ten marks. Answer all parts of each question in the same place.**

1. (a) State and prove the no-cloning theorem.

   (b) A single-qubit state has Bloch-Sphere form $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$, with global phase suppressed. Suppose that you perform the following two experiments:
   - Standard-basis measurement gives $p_o = \frac{3}{4}$.
   - Hadamard-basis measurement gives $p_+ = \frac{1}{2}$.

   Determine $\theta$ and **all** possible values of $\phi$.

   (c) For any $\theta \in \mathbb{R}$, consider the matrix $\mathcal{R}(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$. Show that $\mathcal{R}(\theta)$ is unitary. Find the value of $\theta$ for which the following conditions hold.

$$\mathcal{R}(\theta)|0\rangle = |+\rangle$$
$$\mathcal{R}(\theta)|1\rangle = -|-\rangle$$

**[(1 + 2) + (1 + 2) + (2 + 2) = 10]**

2. (a) Let a cq-state be $\rho_{XQ} = \frac{1}{2}|0\rangle\langle 0|_X \otimes |+\rangle\langle +|_Q + \frac{1}{2}|1\rangle\langle 1|_X \otimes \frac{\mathbb{I}}{2}_Q$. Suppose that you measure $Q$ with the Hadamard-basis positive operator-valued measurements (POVM) $\{M_+, M_-\}$, where $M_+ = |+\rangle\langle +|$ and $M_- = |-\rangle\langle -|$. Compute the following two probabilities:
   - $\Pr[X = 0 \,|\, \text{outcome} = |+\rangle]$
   - $\Pr[X = 0 \,|\, \text{outcome} = |-\rangle]$

   with the help of Born's rule and the Bayes' theorem.

   (b) Consider the EPR pair $|EPR\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Compute the *reduced states* $\rho_A$ and $\rho_B$.

**[(3 + 3) + 4 = 10]**

3. (a) Show that strings of Pauli matrices $P^s = X^{s_1}Z^{s_2} \otimes X^{s_3}Z^{s_4} \otimes \cdots \otimes X^{s_{2n-1}}Z^{s_{2n}}$ with $s \in \{0,1\}^{2n}$ form an orthogonal basis for all linear operators $\mathcal{L}(\mathbb{C}^{2^n}, \mathbb{C}^{2^n})$, in which $n$-qubit density matrices $\rho$ can be described. That is, $\mathrm{tr}[(P^s)^\dagger P^{\hat{s}}] = 0$ for all $s \neq \hat{s}$, and that we can write a density matrix on $n$-qubit as

$$\rho = \frac{1}{2^n}\left(\mathbb{I}^{\otimes 2n} + \sum_{s\neq 0} \nu_s P^s\right).$$

   (b) Prove that the correlations in $\sigma_{AB} = |EPR\rangle\langle EPR|_{AB}$ are stronger than those in $\rho_{AB} = \frac{1}{2}|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B + \frac{1}{2}|1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B$.

**[5 + 5 = 10]**

*************************************