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

Date: 21. 11. 2025 **Marks:** 100 **Time:** 3 Hours

Answer any five questions out of the seven. Each question is worth twenty marks. Answer all the parts of each question in the same place.

1. (a) Explain the principle of quantum entanglement and describe how it can be used in a two-party quantum secret sharing (QSS) protocol. Why is it that neither party can reconstruct the secret individually?
   (b) Compare the classical and quantum winning probabilities of the non-local game CHSH.

   [(5 + 5) + 10 = 20]

2. Describe three different quantum approaches that can be used to determine whether a device is a working bomb or a dud without triggering an explosion. Discuss how each approach works and the advantages of using quantum techniques over classical methods.

   [(5 + 5 + 5) + 5 = 20]

3. (a) Using a quantum circuit, explain how two classical bits of information can be transmitted from one place to another using a single qubit. Include a detailed description and a quantum circuit to support your explanation.
   (b) Explain the Bernstein-Vazirani algorithm using quantum circuits and determine its time complexity.

   [10 + 10 = 20]

4. (a) Define the bounded-error quantum polynomial (BQP) and the bounded-error probabilistic polynomial (BPP) time complexity classes.
   (b) Transform $|\psi\rangle = \frac{|0\rangle+|3\rangle}{\sqrt{2}}$ using standard quantum Fourier transform matrix QFT_4.
   (c) Let $\widehat{x}$ denotes the decimal representation of the binary string x. Given a periodic function $f : \{0,1\}^3 \to \{0,1\}^3$, design a quantum circuit to find the period r, such that $\widehat{f(x)} \equiv \widehat{x} \bmod 2$, $\forall\ x \in \{0,1\}^3$.

   [(2 + 2) + 6 + 10 = 20]

5. (a) Given an oracle for a Boolean function $f : \{0,1\}^N \to \{0,1\}$ such that there exists a unique element x^* with $f(x^*) = 1$ and $f(x) = 0$ for all $x \neq x^*$, describe a quantum algorithm, along with the corresponding circuit diagram based on Grover's search, that finds x^* using $O(\sqrt{N})$ oracle queries.

(b) Given a unitary matrix $U = -i|0\rangle\langle 0| + i|1\rangle\langle 1|$ and an eigenvector $|v\rangle = |0\rangle$. estimate the value of $\theta \in [0, 1)$ such that $U|v\rangle = e^{2\pi i\theta}|v\rangle$.

[10 + 10 = 20]

6. (a) Given a function $f : \{0,1\}^n \to \{0,1\}$, design a quantum circuit to determine whether f is constant or balanced. Provide a detailed explanation of the circuit and its components, and describe how the algorithm works to achieve the desired result.

   (b) Given a black-box function $f : \{0,1\}^n \to \{0,1\}$ and a promise that $f(x) = x \cdot s$. design a quantum circuit to find the secret message $s \in \{0,1\}^n$.

[10 + 10 = 20]

7. (a) Given a two-to-one function $f : \{0,1\}^n \to \{0,1\}^n$ such that $f(x) = f(x \oplus s)$. design a quantum circuit to find the secret message $s \in \{0,1\}^n$.

   (b) Describe all the steps of Shor's algorithm, including circuit diagrams and runtime order, to factor $N = 221$.

[10 + 10 = 20]

****