INDIAN STATISTICAL INSTITUTE
M. Tech (CrS) II Year: 2021–2022
Quantum Cryptology and Security
End-Semester Examination

Date: 01. 02. 2022 Maximum Marks: 100 Time: 3 Hours

Answer any five questions. All the parts of a question should be answered at the same place.

1. (a) State and prove the **no-cloning theorem**.
   (b) Explain how quantum entanglement can be exploited in **teleportation**.
   (c) Consider a single qubit pure quantum state $|\psi\rangle$ with $|0\rangle$ and $|1\rangle$ having equal probability of being observed when measured in the standard computational basis. Separately consider a mixed state $|\phi\rangle$ where $|0\rangle$ and $|1\rangle$ are present in equal proportion. Provide the **density matrices** of $|\psi\rangle$ and $|\phi\rangle$. Briefly explain the **Bloch-sphere** representations of $|\psi\rangle$ and $|\phi\rangle$.

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

2. (a) Given a Boolean function $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3x_1$, provide a schematic diagram of the oracle U_f.
   (b) Draw the connection between the Walsh transform of a Boolean function g and the final amplitudes of different states before measurement when g is used as an oracle in the **Deutsch-Jozsa (DJ) algorithm**.
   (c) Consider a 3-input 1-output Boolean function $h(x_1, x_2, x_3) = x_1x_2x_3$. Using h as an oracle of the DJ algorithm, determine the state with highest probability after the measurement.

   [5+5+10=20]

3. (a) Consider an n-input 1-output Boolean function $f : \{0,1\}^n \to \{0,1\}$ with m many 1's in the output column such that $1 \leq m \leq 2^n$. Give a brief idea about the application of **Grover's search algorithm** on f depending upon the values of m. For example, $m = 1$ is the simplest case, where the Grover's iterate run for $O(\sqrt{2^n})$ times in order to identify the input where $f = 1$.
   (b) Explain step by step how Grover's algorithm can be exploited to mount a generic attack on any block cipher and finally specify the effective key size against quantum adversary.

   [10+(8+2)=20]

P.T.O.

4. (a) Write down the conditions $\mathcal{C}$ on $f : \{0,1\}^n \to \{0,1\}^n$ such that when f is used as an oracle, **Simon's algorithm** can deterministically find the nonzero hidden shift $s \in \{0,1\}^n$ where $f(x) = f(x \oplus s),\ \forall x \in \{0,1\}^n$.

   (b) Check whether the Boolean function $f(x_1, x_2, x_3) = x_3, (x_1 \oplus x_2), (x_1 \oplus x_1)$ satisfies the criteria $\mathcal{C}$. Provide a schematic diagram of the oracle U_f.

   (c) Give an example of a 4-input 4-output Boolean function g satisfying $\mathcal{C}$. Provide the truth table or the ANF.

   (d) Briefly explain the application of Simon's algorithm in cryptanalysis of symmetric-key ciphers.

[5+5+5+5=20]

5. (a) Write down the matrix representation of the gate that corresponds to quantum Fourier transform (QFT). Determine the output state when QFT is applied on an n-qubit state $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$.

   (b) Clearly state the problem statement of **Shor's factoring algorithm**.

   (c) Explain the impact of Shor's factoring algorithm in cryptanalysis of RSA public-key algorithm.

   (d) Provide a step by step description of Shor's algorithm in the context of factoring a product of two primes.

[(2+3)+2+3+10=20]

6. (a) Briefly outline the important quantum steps in **BB84** Quantum Key Distribution (QKD) protocol to obtain the raw key.

   (b) Explain the purpose of using two different orthogonal bases while generating the raw key bits.

   (c) What happens if Bob keeps all the received qubits unmeasured until they discuss about the choice of basis over a public channel?

   (d) Describe the process of obtaining the final key from the raw-key in the BB84 QKD protocol.

[4+4+6+6=20]

7. With necessary examples, briefly describe the ideas on the following, highlighting the security issues.

   (a) **Quantum Secret Sharing**,

   (b) **Quantum Multiparty Computation**.

[10+10=20]