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

Date: 03. 12. 2021 Maximum Marks: 50 Time: 3 Hours

Answer any part of any question. Maximum marks you can obtain is 50. The paper is of 55 marks.

Please answer all parts of a question at the same place.

1. (a) Briefly explain the idea of quantum entanglement.
   (b) Is the following n-qubit quantum state

$$\frac{1}{\sqrt{2}}\left(\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n}+\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)^{\otimes n}\right)$$

   entangled? Give explanation.

[2+3=5]

2. (a) Draw the circuit diagram for creating the maximally entangled Bell State, $|\psi\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$, starting from state $|00\rangle$.
   (b) Provide the complete 4×4 matrix representation for the above circuit.

[5+5=10]

3. Suppose A and B are two parties staying far apart, without any communication channel. Suppose A is given a random bit x and B is given another random bit y. Without communicating among themselves A outputs the bit a and B outputs another bit b. They win the game if $a \oplus b = x \cdot y$.
   (a) Classically what could be the best strategy for A and B to win this game?
   (b) Can they achieve a better strategy in quantum domain with an entanglement? If yes, explain.

[2+3=5]

4. (a) Clearly state the problem statement that the Deutsch-Jozsa algorithm solves.
   (b) Compare the query complexity of Deutsch-Jozsa algorithm with respect to the corresponding classical query complexity.
   (c) For the given 3-input 1-output Boolean function $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3$, write down the output state just before the measurement step in the Deutsch-Jozsa algorithm.

[2+3+5=10]

5. Characterize the quantum states $|\psi\rangle, \left|\psi^{\perp}\right\rangle$, such that Hadamard gate when applied on $|\psi\rangle$, outputs $\frac{1}{\sqrt{2}}\left(|\psi\rangle + \left|\psi^{\perp}\right\rangle\right)$ and when applied on $\left|\psi^{\perp}\right\rangle$ results $\frac{1}{\sqrt{2}}\left(|\psi\rangle - \left|\psi^{\perp}\right\rangle\right)$. Note that, $|\psi\rangle = |0\rangle$ and $\left|\psi^{\perp}\right\rangle = |1\rangle$ satisfy the conditions while $|\psi\rangle = |0\rangle$ and $\left|\psi^{\perp}\right\rangle = i\,|1\rangle$ does not satisfy the condition. [5]

6. (a) State the purpose of Grover's search algorithm in terms of the effective key length in the domain of symmetric key cryptography.

   (b) Given a 3-input 1-output Boolean function $f(x_1, x_2, x_3) = 1 \oplus x_2x_3 \oplus x_1x_2x_3$, how to determine the input point(s) where $f(x_1, x_2, x_3) = 0$, using the Grover's algorithm.

   [3+7=10]

7. (a) Clearly write down the problem statement of Simon's algorithm.

   (b) Consider the truth table of a 3-input 3-output Boolean function $f : \{0,1\}^3 \to \{0,1\}^3$ as given below. Find the hidden shift (if any) using the Simon's algorithm. Explain all the steps with relevant circuit diagram.

x	$f(x)$
000	110
001	101
010	000
011	011
100	101
101	110
110	011
111	000

Table 1: The truth table of the Boolean function $f : \{0,1\}^3 \to \{0,1\}^3$.

[2+(6+2)=10]