INDIAN STATISTICAL INSTITUTE
Semester Examination
M. Tech. (CS) II year (1st Sem): 2015–2016
Quantum Information Processing and Quantum Computation

Date: 07. 12. 2015 Maximum Marks : 40 Time : 2.5 Hours

Please try to write all the part answers of a question at the same place.

1. (a) What is measure-and-resend attack on BB84 protocol?
   (b) Derive an expression of success probability of determining the correct key by a measure-and-resend attacker.

   [4 + 6]

2. (a) What is the non-identity square-root of a one-qubit identity gate?
   (b) What is the difference between CNOT and CCNOT gates?
   (c) Design a swap gate using only CNOT gates.

   [3 + 4 + 3]

3. (a) Show that $\forall \mathbf{x} \in \{0,1\}^n$,

$$H^{\otimes n} |\mathbf{x}\rangle = \frac{1}{2^n} \sum_{\mathbf{y} \in \{0,1\}^n} (-1)^{\mathbf{x}\cdot\mathbf{y}} |\mathbf{y}\rangle .$$

   (b) What are the interpretations of different measurement outputs in Deutsch-Jozsa algorithm?

   [6 + 4]

4. (a) How is Grover's search problem different from the satisfiability problem?
   (b) Can the solution of one of the above two problems be used to solve the other?
   (c) What is the geometric interpretation of Grover's algorithm?

   [2 + 3 + 5]

5. (a) Show that factoring can be reduced to order-finding.
   (b) What are the implications of Shor's algorithm in the domain of cryptography and security against a quantum adversary?

   [6 + 4]