Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal

2A21S015

## Mid-Semester Examination (February 2025)

**Course Name:** Quantum Cryptography
**Semester:** II
**Duration:** 1 Hour 30 Minutes

**Course Code:** CS826
**Course:** M.Tech. (CSE-IS)
**Marks:** 40

**Note:** Answer all the questions.

**Q1. (a)** Consider the complex number z=1+2i. **[08]**

**(i)** Find the real component *z* of $\Re(z)$.

**(ii)** Find the imaginary component z of $\Im(z)$.

**(iii)** Write z in the polar form $re^{i\theta}$.

**(iv)** Find the conjugate z*.

**(b)** A qubit is in the state **[04]**

$$\frac{1+i\sqrt{3}}{3}|0\rangle+\frac{2-i}{3}|1\rangle.$$

If you measure the qubit, what is the probability of getting
(a) $|0\rangle$?
(b) $|1\rangle$?

**Q2. (a)** A qubit is in the state

$$A\left(2e^{i\pi/6}|0\rangle-3|1\rangle\right).$$

(i) Normalized the state (i.e., find A.). **[04]**

(ii) If you measure the qubit, what is the probability that you get $|0\rangle$? **[04]**

**Q3.** Consider a map *U* that transforms the Z-basis states as follows.

$$U|0\rangle=\frac{\sqrt{3}}{2}|0\rangle+\frac{\sqrt{3}+i}{4}|1\rangle,$$
$$U|1\rangle=\frac{\sqrt{3}+i}{4}|0\rangle-\frac{\sqrt{3}+3i}{4}|1\rangle.$$

Say $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ is a normalized quantum state, i.e., $|\alpha|^2+|\beta|^2=1$.

(i) Calculate $U|\psi\rangle$. **[05]**

(ii) From your answer to (i), is *U* a valid gate? Explain your reasoning. **[05]**

**Q4.** (a) The Hadamard gate turns $|0\rangle$ into $|+\rangle$, and $|1\rangle$ into $|-\rangle$.

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle,$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle.$$

From the definition of Hadamard gate, prove that H|+> = |0>, H|-> = [illegible]|1> and H|i> = [illegible]|-i>. [02+02+02]

(b) Consider each logical classic gate with inputs A and B, outputs C and D, and the truth table below. Is each gate a valid quantum gate? Why? [02+02]

(a)

| A | B |
|---|---|
| 0 | 0 |
| i | 1 |

↓ C

CD

(b)

| A | B |
|---|---|
| 0 | 1 |
| 1 | 1 |

↓ D

CD

H|i> = |-i>

0 0
0 1
00
11

---

|00> + |11>

|01> + |11

Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal

## End-Semester Examination (May 2025)

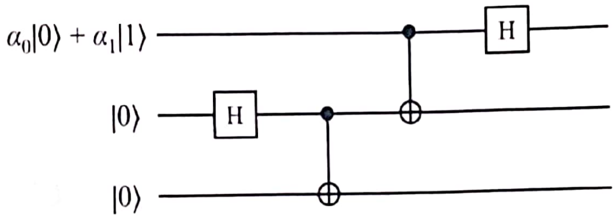
| | |
|---|---|
| **Course Name:** Quantum Cryptography | **Course Code:** CS826 |
| **Semester:** II | **Course:** M.Tech. (CSE-IS) |
| **Duration:** 03 Hours | **Marks:** 80 |

**Note:** Answer all the questions.

**Q1. (a)** Explain Shor's Algorithm and describe through a suitable example how it can pose a threat to RSA. **[6]**

**(b)** A SWAP gate takes two inputs $x_1$ and $x_2$ and outputs $x_2$ and $x_1$; i.e., it swaps the values of two registers. Show how to build a SWAP gate using only CNOT gates. **[6]**

**Q2.** Consider the following quantum circuit:



An equivalent description of the circuit (calling the registers $x_1, x_2, x_3$) is:

1. Initialize $x_1$ to $\alpha_0\,|0\rangle + \alpha_1\,|1\rangle$
2. Initialize $x_2$ to $|0\rangle$
3. Initialize $x_3$ to $|0\rangle$
4. Hadamard($x_2$)
5. CNOT($x_2$, $x_3$)
6. CNOT($x_1$, $x_2$)
7. Hadamard($x_1$)

**a)** Determine with proof the state of the three qubits at the end of the circuit's operation. **[05]**

**b)** If we then measure the three qubits, give the outcomes and their probabilities that arise. **[05]**

**Q3.** Calculate the following inner products. **[03+03+03]**

**a)** $\langle 10|11\rangle$.

**b)** $\langle +-|01\rangle$.

**c)** $\langle 1+0|1-0\rangle$.

Q4. (a) If you measure the left qubit, what outcomes can you get, what are the corresponding probabilities of those outcomes, and what does the state collapse to for each outcome? Is this state a product state, partially entangled state, or maximally entangled state? [03+03+03]

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle).$$

(b) Alice and Bob share an EPR-pair,

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Suppose they each measure their qubit with an X-observable (which corresponds to a particular projective measurement with possible outcomes +1, −1). Find the following. [10]

(a) $P_{00}$.

(b) $P_{01}$.

(c) $P_{10}$.

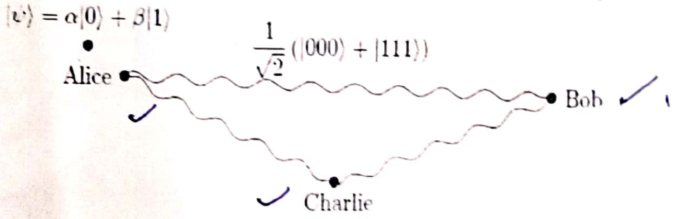
(d) $P_{11}$.

(e) $E(A',B') = P00 - P01 - P10 + P11$.

Q5. Alice wants to teleport a qubit in an unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Charlie, and Bob is helping her. They share three entangled qubits in the GHZ state:

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

The left qubit is Alice's, the middle qubit is Bob's, and the right qubit is Charlie's.


$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$
Alice
Bob
Charlie

Altogether, the initial state of the system is

$$|\psi\rangle|\mathrm{GHZ}\rangle = (\alpha|0\rangle - \beta|1\rangle)\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$$

$$= \frac{1}{\sqrt{2}}(\alpha|0000\rangle - \alpha|0111\rangle - \beta|1000\rangle - \beta|1111\rangle)$$

So, the left two qubits are Alice's, the second-to-right qubit is Bob's, and the right qubit is Charlie's.

**(a)** Show that if Alice applies CNOT to her qubits (so the far left qubit is the control and the second-to-left qubit is the target) and then the Hadamard gate to her left qubit, the state of the system becomes **[5]**

$$\frac{1}{2}\big[|00\rangle(\alpha|00\rangle+\beta|11\rangle)+|01\rangle(\beta|00\rangle+\alpha|11\rangle)$$
$$+|10\rangle(\alpha|00\rangle-\beta|11\rangle)+|11\rangle(-\beta|00\rangle+\alpha|11\rangle)\big].$$

**(b)** Next, Alice measures her two qubits and makes the results known. What values can she get, with what probabilities, and what does the state collapse to in each case? **[5]**

**Q6. (a)** Explain the Crystal-Kyber public encryption algorithm. **[6]**

**(b)** Show that the following gates are reversible or irreversible. **[4]**

(i) OR. (ii) XOR. (iii) NAND. (iv) NOR

**Q7. (a)** Let's assume:

Alice's key:

A = 1 0 1 1 0 1 1 0

Bob's key:

B = 1 0 1 1 1 1 1 0

The above Alice and Bob raw keys contain discrepancies. Demonstrate how the Cascade protocol can be used to detect and correct errors. **[5]**

**(b)** Explain the BB84 Quantum Key Distribution protocol with the help of a suitable example. **[5]**

---