Quantum Secure Communication Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

As the field of quantum communication continues to evolve and advance, there is a growing need for professionals with the knowledge and skills to tackle the complex challenges and opportunities it presents.

The course covers the fundamental concepts of quantum communication, including the properties of qubits and quantum registers, the manipulation of quantum states through quantum gates, and the principles and implementations of quantum key distribution.

Additionally, the course delves into various quantum communication protocols and their respective approaches, and the security challenges in quantum communication, such as attacks against quantum key distribution protocols, and the potential applications and future developments of a quantum internet.

Topics covered in the course;

- Introduction to quantum communication
- Qubit and quantum register
- Quantum gates
- Quantum key distribution
- Quantum communication protocols
- Quantum key distribution approaches
- Attacks against QKD protocols
- Quantum internet

Prerequisites

Fundamental knowledge of quantum computing.

What You Will Learn

You will;

- Be able to apply their knowledge of quantum key distribution
- Be equipped to utilise key distribution protocols
- Be able to comply with existing quantum communication standards and secure quantum networking
- Be able to explain active & passive quantum security attacks
- Be able to explain physical attacks on quantum key distribution protocols

Outline

Quantum Secure Communication Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Day 1

What is quantum communication about?

Qubit and quantum register

- Four postulates

IBM Quantum

How to prepare a superposition?

- Preparing an arbitrary quantum state

No cloning theorem

- No Cloning Theorem - Proof

Entanglement

- Decomposition exercise
- Entangled states
- Difference between product and entangled states
- What does entanglement mean?
- Famous entanglement pairs
- How to produce entangled pairs?
- Changing the bases of an entangled pair
- CNOT gate
- Bell state generator
- Generalized quantum entangler
- How to create entangled qubits physically? - An example

Implementation examples for qubits

- Physical qubits
- Di Vincenzo criteria
- Superconducting qubits
- Trapped ions
- Photonic qubits

Day 2

Quantum key distribution over optical fiber

- From theory to the real world
- Protocol stack of QKD

Two important quantum communication protocols

- Quantum Communication – the players
- Superdense coding
- Teleportation
- Superdense coding and Teleportation

Quantum Secure Communication Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Quantum Medium Access Control

- Medium Access Control in distributed environment - quantum WIFI
- Quantum WIFI - MAC
- Quantum MAC - JOIN
- Quantum MAC - LEAVE
- Quantum MAC - TRANSFER
- Quantum MAC - generalization
- Rebalacing
- Quantum periodic table

Density matrix and its application in quantum communications

- Decomposition exercise
- Introduction to density matrix formalism
- Calculation of density matrices
- Mixed states
- Geometrical representation
- Are density matrices unique?
- Partial trace
- Postulates with density matrices
- Teleportation
- State vs. density matrix formalisms

Why do we need quantum key distribution?

- Problem formulation
- Symmetric Keys
- Symmetric Keys – problems and solutions
- Asymmetric Key System
- Problem formulation
- Problem formulation – Quantum Key Distribution

Quantum key distribution approaches

- Two types of QKD
- In real life, quantum channel is not ideal
- BB84, the first QKD protocol
- SARG04 protocols
- B92 protocol
- Entanglement based QKD
- E91 protocol

Passive and active attacks

- Passive attack
- Active attack
- Attack types
- Denial of service attack
- Man-in-the-middle attack

Day 3

Non idealistic channels

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Why realistic quantum channels are important?
- General model of communication
- AWGN
- Channel capacity
- A suprising example
- Various quantum capacities
- Basic quantum channel models
- Effects in real fibers

Interesting QKD approaches

- Chicago Quantum Exchange
- Chinese Quantum Network: More than 4600 kilometers
- UK Quantum Communications Hub
- EuroQCI
- Companies: ID Quantique
- Companies: MagiQ
- Companies: Quintessence Labs

Technical study: implementing BB84

- High level overview
- Physical realization

Quantum key distribution via free-space

- Why to use free-space instead of fiber-based solution?

Errors in free-space quantum channels

- Quantum signals on free-space channels
- There are equations behind everything
- But this is what is important

Prepare-and-measure QKD vs entanglement-based QKD

- Prepare-and-measure QKD -advantages
- Prepare-and-measure QKD -disadvantages
- Entanglement-based QKD -advantages
- Entanglement-based QKD -disadvantages

Physical attacks on quantum key distribution protocols

- Intercept and resend
- Faked states attack
- Photon number splitting attack
- Trojan Horse Attack (Light Injection Attack)
- Using a beam splitter

Interesting free-space QKD approaches

- Scenarios for satellite based quantum communicatoins
- How to use an entanglement-based satellite system?
- Quantum Experiments at Space Scale (QUESS)

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Singapore’s mission in 2019
- SpooQy 1
- European answer: SAGA
- A draft concept of the European SAGA system
- Timeline for the SpaceQCI (from European Comission)
- Timeline for the SAGA mission (from ESA)
- Security threats to a satellite QKD system

Quantum Secure Network, Quantum Information Network

- Stages to achieve a global quantum internet

Ingredients of future's quantum internet

- Challenges
- Entanglement swapping
- Entanglement swapping - remarks
- Routing

Overview of standardization

- Working on standards
- Working on quantum communications standards
- ETSI Quantum-Safe Cryptography (QSC) working group
- ETSI - Quantum-Safe Cryptography (QSC)
- ETSI Industry Specification Group (ISG)
- ETSI QKD
- ETSI Standards – An example
- IETF QIRG – Standards for quantum internet
- IETF QIRG – Two dradts

Quantum communication: implementation challenges

- Technical study: implementing CV-QKD system

A Hungarian CV-QKD system

- Technical study: implementing quantum random number generator (QRNG)

The simplest QRNG

- A Hungarian QRNG system

Summary and outlook

- Future's satellite system
- QKD and autonomous vehicles
- QKD and 5G