Quantum communications course 2022: oral part of the exam

In the oral exam, no aids are allowed. You will randomly get one of these topics.

C1

History of cryptography and the place of quantum key distribution in it.

C2

One-time pad. Quantum key distribution networks.

C3

Weak coherent source and its photon number statistics. Photon number splitting attack on QKD.

C4

Heralded single-photon source. Passive state preparation. Why the heralded source is used in the ground-to-satellite teleportation experiment [J.-G. Ren *et al.*, Nature **549**, 70 (2017)].

C5

Properties of optical fiber, free-space atmospheric and satellite channels for quantum communication. Advantages, disadvantages, and challenges of each type of channel for QKD.

C6

Optical beamsplitters, attenuators, polarization controllers, phase and intensity modulators, isolators and circulators.

C7

Types of optical power meters. Types of single-photon detectors. How a single-photon detector based on an avalanche photodiode works.

D1

Qubits: Dual- and single-rail qubits. How to encode states of light to make qubits.

D2

Bloch sphere. Phase coding of single photon.

D3

Measurement: What is measurement in quantum mechanics. How to measure qubit. Measurement of non-orthogonal states.

D4

How to make annihilation operator with measurement. Quantum random number generator. Interaction-free object detection (“bomb detector”).

C8

BB84 quantum key distribution protocol and post-processing.

C9

Intercept-resend attack on BB84.

C10

Decoy-state protocol.

C11

How can one use entanglement for experimental QKD?

C12

Quantum key generation rates in experiments. What limits QKD distance?

D5

Quantum superposition. Pure and mixed states. Transition from pure states to mixed states and vice versa.

D6

Double-slit interference and quantum erasure. Quantum ensembles and density matrix.

D7

Quantum measurements. Measurement-induced transformations. Quantum Zeno paradox. Projective measurements.

D8

Generalized measurements and POVM. Examples of optical schemes for generalized quantum measurements. Accessible information. Holevo bound.

D9

Entangled states. Bell basis. Correlations of entangled states. Remote state preparation.

D10

Entangled photons. Heralded sources of single photons. Superluminal communication and the “no-cloning” theorem.

D11

Security of BB84 protocol. Equivalence of prepare-and-measure and entanglement-based QKD.

D12

Detection of eavesdropping attempts in QKD. Intercept-resend attack. Optimal attack.

D13

Bell inequality. Examples of Bell's inequality violation.

D14

Bell measurement with linear optics. Quantum teleportation.

C13

Security and threat model of QKD. The use of quantum random number generator in QKD. The need to trust the manufacturer. Processing double-clicks.

C14

Optical Trojan-horse attack and countermeasures to it.

C15

Detector control attack and countermeasures to it.

C16

Twin-field QKD protocol [M. Lucamarini *et al.*, Nature **557**, 400 (2018)].

C17

Types of countermeasures against imperfections. Distinguishability of source states. Certification of cryptographic tools.