Quantum communications course 2019: exam

Questions at the oral exam will cover everything discussed on the lectures and journal paper seminars, as well as your overall understanding of the course. They may include problems to solve.

At the exam you will get three written initial questions, one from each third of the course, picked at random from a large pool of questions. You may then spend up to 1 h preparing your solutions (which you may write down), before proceeding to orally present and defend them to the lecturers. You may be asked extra questions orally. All aids including internet access are allowed while you prepare the solutions to the three initial questions, however you must work alone and refrain from discussions and communication with other persons.

*Topics covered in **Yury Kurochkin's** lectures:*

Qubits. Dual- and single-rail qubits. How to encode states of light to make qubits. Discrete variables vs. continuous variables. Bloch sphere. Phase coding of single photon.

Measurement in quantum mechanics. How to measure qubit. Measurement of non-orthogonal states. How to make annihilation operator with measurement. Interaction-free detection.

QKD: Basic quantum cryptography protocols (BB84, decoy-state, differential-phase-shift, coherent-one-way). Intercept-resend attack. How to realise QKD protocols on physical level. How qubits are prepared and measured in experiment. Free-space and fiber realisations. Using entanglement in experimental QKD.

Main applications of QKD and how they work. Quantum key generation rate in experiments. Limits on QKD distance. Quantum networks. Trusted repeaters. Satellite QKD and its challenges.

*Topics covered in **Denis Sych's** lectures:*

Quantum superposition. Pure and mixed states. Transition from pure states to mixed states and vice versa. Double-slit interference and quantum erasure. Quantum ensembles and density matrix.

Quantum measurements. Measurement-induced transformations. Quantum Zeno paradox. Projective measurements. Generalized measurements and POVM. Examples of optical schemes for generalized quantum measurements. Accessible information. Holevo bound.

Entangled states. Bell basis. Correlations of entangled states. Remote state preparation. Entangled photons. Heralded sources of single photons. "Ghost" imaging and "ghost" interference. Superluminal communication and the "no-cloning" theorem.

BB84 protocol. Equivalence of prepare-and-measure and entanglement-based QKD. Decoy state QKD. Detection of eavesdropping attempts. Intercept-resend attack. Optimal attack. Bell inequality. Examples of Bell's inequality violation.

Bell measurement with linear optics.

*Topics covered in **Vadim Makarov's** lectures:*

History of cryptography. Present vs. future threats. Quantum cryptography. Basic QKD protocol. Trusted-node QKD networks.

Security and threat model of QKD. The use of quantum random number generator in QKD. The need to trust the manufacturer. Processing double-clicks. Optical Trojan-horse attack and countermeasures to it. Plug-and-play QKD scheme.

Detector control attack. Measurement-device-independent QKD. Electronic scheme of APD-based single-photon detector.

Optical implementation of quantum teleportation.

Twin-field QKD protocol.

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