Federal State Autonomous Educational Institution of Higher Education "Moscow Institute of Physics and Technology (National Research University)"

APPROVED
и.о. директора физтех-школы физики и исследований им. Ландау
A.A. Voronov

Work program of the course (training module)

course: Quantum Communications/Квантовая связь
major: Photonics and Optical Informatics
specialization: Photonics, Quantum Technologies & 2D Materials/Фотоника, квантовые технологии и двумерные материалы
Landau Phystech-School of Physics & Research
Chair of the Russian Quantum Centre
term: 1
qualification: Master

Semester, form of interim assessment: 1 (fall) - Exam

Academic hours: 30 AH in total, including:
lectures: 30 AH.
seminars: 0 AH.
laboratory practical: 0 AH.

Independent work: 30 AH.

Exam preparation: 30 AH.

In total: 90 AH, credits in total: 2

Authors of the program:

Y.V. Kurochkin, candidate of physics and mathematical sciences
D.V. Sych, candidate of physics and mathematical sciences
V.V. Makarov, phd (candidate of physics and mathematical sciences)

The program was discussed at the Chair of the Russian Quantum Centre 30.03.2020

Annotation

The course introduces theory and practice of quantum communications. It covers qubit encoding, superposition, entanglement, quantum measurements, practical aspects of fiber-optic and atmospheric communication channels. It introduces protocols for random number generation, interaction-free detection, ghost imaging, quantum teleportation.

A special attention is devoted to quantum key distribution, for which several protocols and implementations and approaches to building networks are detailed, along with an introduction into its security proofs and practical security aspects.

1. Study objective

Purpose of the course

to provide insights into modern applications of quantum mechanics to long-distance communication.

Tasks of the course

to give the students proper background for work and research in the field of photonic quantum technologies, especially of long-distance communication.

2. List of the planned results of the course (training module), correlated with the planned results of the mastering the educational program

Mastering the discipline is aimed at the formation of the following competencies:

Code and the name of the competence	Competency indicators
Gen.Pro.C-1 Gain fundamental scientific knowledge in the field of physical and mathematical sciences	Gen.Pro.C-1.1 Apply fundamental scientific knowledge in the field of physical and mathematical sciences
	Gen.Pro.C-1.3 Understands the interdisciplinary links in mathematics and physics and is able to apply them to problems in photonics and opto-informatics
Gen.Pro.C-2 Acquire an understanding of current scientific and technological challenges in professional settings, and scientifically formulate professional objectives	Gen.Pro.C-2.2 Assess the relevance and practical importance of research in professional settings
	Gen.Pro.C-2.3 Understand professional terminology used in modern scientific and technical literature and present scientific results in oral and written form within professional communication
Gen.Pro.C-3 Select and/or develop approaches to professional problem-solving with consideration to the limitations and specifics of different solution methods	Gen.Pro.C-3.1 Analyze problems, plan research strategy to achieve solution(s), propose, and combine solution approaches
Gen.Pro.C-4 Successfully perform a task, analyze the results and present conclusions, apply knowledge and skills in the field of physical and mathematical sciences and ICTs	Gen.Pro.C-4.2 Apply knowledge in the field of physical and mathematical sciences to solve problems, make conclusions, and evaluate the obtained results
Pro.C-1 Assign, formalize, and solve tasks, develop and research mathematical models of the studied phenomena and processes, systematically analyze scientific problems and obtain new scientific results	Pro.C-1.1 Locate, analyze, and summarize information on current research findings within a selected subject field
	Pro.C-1.2 Make hypotheses, build mathematical models of the studied phenomena and processes, evaluate the quality of the developed model

3. List of the planned results of the course (training module)

As a result of studying the course the student should:

know:

theoretical basis of quantum communications and its common applications to date.

be able to:

understand recent advances in quantum communications and cryptography.

master:

basic ideas and techniques of analysis of quantum communication systems.

4. Content of the course (training module), structured by topics (sections), indicating the number of allocated academic hours and types of training sessions

4.1. The sections of the course (training module) and the complexity of the types of training sessions

№	Topic (section) of the course	Types of training sessions, including independent work			
		Lectures	Seminars	Laboratory practical	Independent work
1	Introduction	2			2
2	Components of quantum- optical systems	2			2
3	Basics of quantum optics	2			2
4	Measurement in quantum mechanics	2			2
5	Quantum key distribution (QKD)	2			2
6	Applications of QKD	2			2
7	Quantum superposition	2			2
8	Quantum measurements	2			2
9	Entangled states	2			2
10	Security of BB84 protocol	2			2
11	Bell measurement with linear optics	2			2
12	Security and threat model of QKD	2			2
13	Paper seminar on quantum teleportation; Detector control attack	2			2
14	Paper seminar on twin-field QKD; Countermeasures against imperfections and certification	2			2
15	Discussion and question-and-answer session	2			2
AH in total		30			30
Exam preparation		30 AH.			
Total complexity		90 AH., credits in total 2			

4.2. Content of the course (training module), structured by topics (sections)

Semester: 1 (Fall)

1. Introduction

History of cryptography. Quantum cryptography. Demonstration that measurement changes a quantum state. Key distribution networks. Course overview. Sources of photons and coherent states. (Vadim)

2. Components of quantum- optical systems

Transmission of light in free space and optical fiber. Beamsplitters, polarizers, attenuators, wavelength filters, isolators and circulators. Modulators of polarization, phase, and intensity. Interferometers in single-photon regime. Photodetectors and power meters. Single-photon detectors. Integrated optics. (Vadim)

3. Basics of quantum optics

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. (Yury)

4. Measurement in quantum mechanics

How to measure qubit. Measurement of non-orthogonal states. How to make annihilation operator with measurement. Application examples: quantum random number generator, interaction-free detection. (Yury)

5. Quantum key distribution (QKD)

BB84 protocol and post-processing. 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. Decoy-state protocol. Differential-phase-coding protocol. (Yury)

6. Applications of 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. (Yury)

7. 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. (Denis)

8. 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. (Denis)

9. 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. (Denis)

10. Security of 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. (Denis)

11. Bell measurement with linear optics

Bell measurement with linear optics. Quantum teleportation. (Denis)

12. 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. (Vadim)

13. Paper seminar on quantum teleportation; Detector control attack

J.-G. Ren et al., “Ground-to-satellite quantum teleportation,” Nature 549, 70 (2017). Detector control attack and countermeasures to it. (Vadim)

14. Paper seminar on twin-field QKD; Countermeasures against imperfections and certification

M. Lucamarini et al., “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” Nature 557, 400 (2018). Types of countermeasures against imperfections. Distinguishability of source states. Certification of cryptographic tools. (Vadim)

15. Discussion and question-and-answer session

Discussion and question-and-answer session. (all lecturers)

5. Description of the material and technical facilities that are necessary for the implementation of the educational process of the course (training module)

A classroom equipped with multimedia-projector and projection screen.

6. List of the main and additional literature, that is necessary for the course (training module) mastering

Main literature

1. The Physics of Quantum Information, ed. by Bouwmeester, Ekert, Zeilinger; Springer, Berlin, Heidelberg (2000).
2. Nielsen and Chuang, Quantum Computation and Quantum Information, Cambridge University press (2010).

Additional literature

1. N. Gisin et al., Rev. Mod. Phys. 74, 145 (2002)
2. V. Scarani et al., Rev. Mod. Phys. 81, 1301 (2009)
3. F. Xu et al., arXiv:1903.09051

7. List of web resources that are necessary for the course (training module) mastering

https://arxiv.org/

8. List of information technologies used for implementation of the educational process, including a list of software and information reference systems (if necessary)

Multimedia technologies can be employed during lectures, including presentations.

9. Guidelines for students to master the course

Students should learn the basic concepts of quantum communications and cryptography, as well as how to apply their theoretical knowledge in practice.

For the successful assimilation of the course, in addition to attending classes, students are required to perform homework whose amount in hours should be not less than the number of hours specified in the curricula of the faculties. Studying at home includes:

- reading the recomended literature and making notes;
- processing and analysis of lecture materials (using notes, textbooks and scientific articles), answering questions, proving some statements;
- solving problems given on lectures and seminars for self-study;
- preparing for the tests and exams.

SUPPLEMENT

Assessment funds for course (training module)

major:	Photonics and Optical Informatics
specialization:	Photonics, Quantum Technologies & 2D Materials/Фотоника, квантовые технологии и двумерные материалы Landau Phystech-School of Physics & Research Chair of the Russian Quantum Centre
term:	1
qualification:	Master

Semester, form of interim assessment: 1 (fall) - Exam

Authors:

Y.V. Kurochkin, candidate of physics and mathematical sciences
D.V. Sych, candidate of physics and mathematical sciences
V.V. Makarov, phd (candidate of physics and mathematical sciences)

1. Competencies formed during the process of studying the course

Code and the name of the competence	Competency indicators
Gen.Pro.C-1 Gain fundamental scientific knowledge in the field of physical and mathematical sciences	Gen.Pro.C-1.1 Apply fundamental scientific knowledge in the field of physical and mathematical sciences
	Gen.Pro.C-1.3 Understands the interdisciplinary links in mathematics and physics and is able to apply them to problems in photonics and opto-informatics
Gen.Pro.C-2 Acquire an understanding of current scientific and technological challenges in professional settings, and scientifically formulate professional objectives	Gen.Pro.C-2.2 Assess the relevance and practical importance of research in professional settings
	Gen.Pro.C-2.3 Understand professional terminology used in modern scientific and technical literature and present scientific results in oral and written form within professional communication
Gen.Pro.C-3 Select and/or develop approaches to professional problem-solving with consideration to the limitations and specifics of different solution methods	Gen.Pro.C-3.1 Analyze problems, plan research strategy to achieve solution(s), propose, and combine solution approaches
Gen.Pro.C-4 Successfully perform a task, analyze the results and present conclusions, apply knowledge and skills in the field of physical and mathematical sciences and ICTs	Gen.Pro.C-4.2 Apply knowledge in the field of physical and mathematical sciences to solve problems, make conclusions, and evaluate the obtained results
Pro.C-1 Assign, formalize, and solve tasks, develop and research mathematical models of the studied phenomena and processes, systematically analyze scientific problems and obtain new scientific results	Pro.C-1.1 Locate, analyze, and summarize information on current research findings within a selected subject field
	Pro.C-1.2 Make hypotheses, build mathematical models of the studied phenomena and processes, evaluate the quality of the developed model

2. Competency assessment indicators

As a result of studying the course the student should:

know:

theoretical basis of quantum communications and its common applications to date.

be able to:

understand recent advances in quantum communications and cryptography.

master:

basic ideas and techniques of analysis of quantum communication systems.

3. List of typical control tasks used to evaluate knowledge and skills

Not provideed.

4. Evaluation criteria

Examples of checking tasks:

1. Prove the No-cloning theorem.
2. Scetch the scheme of blinding attack on the detector and give the explanation of its work.

Checking questions:

1. What are the pros and cons of quantum cryptography compared to classic cryptography?
2. Ways of coding of optical quantum states and for which applications each method suits the best.
3. Existing types of photon sources and differences between them.
4. Phenomena that cause losses in optical channel in atmosphere.
5. Properties of hash functions.

6. Best ways to handle vulnerabilities of quantum communication devices.

Examination cards:

Card 1.

1. Bell inequality. Examples of Bell's inequality violation.

2. What are the pros and cons of quantum cryptography compared to classic cryptography?

Card 2.

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

2. List all the QKD schemes and protocols that you have learned from the course. Evaluate and justify whether each of them is vulnerable to a Trojan horse attack, and if it is, how difficult it would be to protect it.

Card 3.

1. Quantum key propagation: the main protocols of quantum cryptography (describe how the three protocols discussed in the lectures work).

2. Properties of hash functions.

Card 4.

1. Measurement in quantum mechanics. How to measure qubit. Measurement of non-orthogonal states.

2. Prove the No-cloning theorem.

Билет 5.

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

2. Scetch the scheme of blinding attack on the detector and give the explanation of its work.

Assessment "excellent (10)" is given to a student who has displayed comprehensive, systematic and deep knowledge of the educational program material, has independently performed all the tasks stipulated by the program, has deeply studied the basic and additional literature recommended by the program, has been actively working in the classroom, and understands the basic scientific concepts on studied discipline, who showed creativity and scientific approach in understanding and presenting educational program material, whose answer is characterized by using rich and adequate terms, and by the consistent and logical presentation of the material;

Assessment "excellent (9)" is given to a student who has displayed comprehensive, systematic knowledge of the educational program material, has independently performed all the tasks provided by the program, has deeply mastered the basic literature and is familiar with the additional literature recommended by the program, has been actively working in the classroom, has shown the systematic nature of knowledge on discipline sufficient for further study, as well as the ability to amplify it on one's own, whose answer is distinguished by the accuracy of the terms used, and the presentation of the material in it is consistent and logical;

Assessment "excellent (8)" is given to a student who has displayed complete knowledge of the educational program material, does not allow significant inaccuracies in his answer, has independently performed all the tasks stipulated by the program, studied the basic literature recommended by the program, worked actively in the classroom, showed systematic character of his knowledge of the discipline, which is sufficient for further study, as well as the ability to amplify it on his own;

Assessment "good (7)" is given to a student who has displayed a sufficiently complete knowledge of the educational program material, does not allow significant inaccuracies in the answer, has independently performed all the tasks provided by the program, studied the basic literature recommended by the program, worked actively in the classroom, showed systematic character of his knowledge of the discipline, which is sufficient for further study, as well as the ability to amplify it on his own;

Assessment "good (6)" is given to a student who has displayed a sufficiently complete knowledge of the educational program material, does not allow significant inaccuracies in his answer, has independently carried out the main tasks stipulated by the program, studied the basic literature recommended by the program, showed systematic character of his knowledge of the discipline, which is sufficient for further study;

Assessment “good (5)” is given to a student who has displayed knowledge of the basic educational program material in the amount necessary for further study and future work in the profession, who while not being sufficiently active in the classroom, has nevertheless independently carried out the main tasks stipulated by the program, mastered the basic literature recommended by the program, made some errors in their implementation and in his answer during the test, but has the necessary knowledge for correcting these errors by himself;

Assessment “satisfactory (4)” is given to a student who has discovered knowledge of the basic educational program material in the amount necessary for further study and future work in the profession, who while not being sufficiently active in the classroom, has nevertheless independently carried out the main tasks stipulated by the program, learned the main literature but allowed some errors in their implementation and in his answer during the test, but has the necessary knowledge for correcting these errors under the guidance of a teacher;

Assessment “satisfactory (3)” is given to a student who has displayed knowledge of the basic educational program material in the amount necessary for further study and future work in the profession, not showed activity in the classroom, independently fulfilled the main tasks envisaged by the program, but allowed errors in their implementation and in the answer during the test, but possessing necessary knowledge for elimination under the guidance of the teacher of the most essential errors;

Assessment “unsatisfactory (2)” is given to a student who showed gaps in knowledge or lack of knowledge on a significant part of the basic educational program material, who has not performed independently the main tasks demanded by the program, made fundamental errors in the fulfillment of the tasks stipulated by the program, who is not able to continue his studies or start professional activities without additional training in the discipline in question;

Assessment “unsatisfactory (1)” is given to a student when there is no answer (refusal to answer), or when the submitted answer does not correspond at all to the essence of the questions contained in the task.

5. Methodological materials defining the procedures for the assessment of knowledge, skills, abilities and/or experience

The course is graded at an oral exam. The exam starts with a random task assigned to each student and time given for completion of the task. No aids are allowed. The student then proceeds to a chat with the examiner, at which he/she presents his/her solution to the assigned task. The examiner then asks the student several questions that evenly cover the course content. A final grade is assigned based on the quality of answers and demonstrated level of understanding.