University of Gdańsk

Subject card

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Subject name and code | Quantum Cryptography, PG_00199109 | | | | | | |
| Field of study | Quantum Information Technology | | | | | | |
| Date of commencement of studies | October 2026 | | Academic year of realisation of subject | | 2026/2027 | | |
| Education level | Master's studies | | Subject group | | Obligatory subject group in the field of study<br>Subject group related to scientific research in the field of study | | |
| Mode of study | full-time studies | | Mode of delivery | | at the university | | |
| Year of study | 1 | | Language of instruction | | English | | |
| Semester of study | 2 | | ECTS credits | | 6.0 | | |
| Learning profile | academic | | Assessment form | | exam | | |
| Conducting unit | | | | | | | |
| Name and surname of lecturer (lecturers) | Subject supervisor | | dr Akshata Shenoy | | | | |
| | Teachers | | | | | | |
| Lesson types | Lesson type | Lecture | Tutorial | Laboratory | Project | Seminar | SUM |
| | Number of study hours | 30.0 | 30.0 | 0.0 | 0.0 | 0.0 | 60 |
| | E-learning hours included: 0.0 | | | | | | |
| Learning activity and number of study hours | Learning activity | Participation in didactic classes included in study plan | | Participation in consultation hours | | Self-study | SUM |
| | Number of study hours | 60 | | 0.0 | | 90.0 | 150 |
| Subject objectives | Knowledge and understanding of standard methods and aims of quantum cryptography. The student should know basic quantum protocols for key distribution, randomness generation and cryptoanalysis. The student should also be able to sketch their security proofs and know their applications. | | | | | | |

**Learning outcomes**

| Course outcome | Subject outcome | Method of verification |
|---|---|---|
| [QITL3_W02] knows and understands on deepened level key and selected advanced detailed issues in the field of quantum information technology, including methods of their research and development, and their applications in the context of dynamic technological changes, in particular in the area of information processing, cryptography and the development of advanced computing systems | | |
| [QITL3_U02] is able to use their knowledge of quantum information technology – formulate and solve complex and unusual problems and innovatively perform tasks in unpredictable conditions by appropriately selecting sources and information derived from them, evaluating, critically analyzing, synthesizing, creatively interpreting, and presenting this information, as well as by selecting and applying appropriate methods and tools, including advanced information and communication techniques and adapting existing methods and tools or developing new ones | | |
| [QITL3_W01] knows and understands in depth selected facts, objects and phenomena, as well as the methods and theories related to them, explaining the complex relationships between them, constituting advanced general knowledge in the field of quantum information technology, as well as the scientific research methodology specific to this discipline and its importance in the context of contemporary directions of development of science and technology | | |

**Subject contents**

Basics of classical cryptography: symmetric and asymmetric protocols; security proofs; typical attacks; post-quantum cryptography.Quantum key distribution: BB84, E91 and BBM92 protocols and their security proofs.Quantum cryptoanalysis: Shors algorithm.Quantum random number generators: methods of generation; randomness amplification.Device independent cryptography: Bell inequality-based; semi-device independent protocols.Quantum hacking: photon number splitting, intercept-resend and detector blinding attacks.Other quantum cryptographic protocols: secret sharing; quantum fingerprinting; oblivious transfer; bit commitment.Elements of practical quantum cryptography: typical setups; known issues; current trends

**Prerequisites and co-requisites**

**Assessment methods and criteria**

| Subject passing criteria | Passing threshold | Percentage of the final grade |
|---|---|---|
| lecture part: exam | 51.0% | 50.0% |
| tutorial part: test | 51.0% | 50.0% |

**Recommended reading**

| | |
|---|---|
| Basic literature | Quantum Computation and Quantum Information, M.A. Nielsen, I.L. Chuang, Cambridge University Press |
| Supplementary literature | None. |
| eResources addresses | |

**Example issues/ example questions/ tasks being completed**

**Work placement**

Not applicable

Document generated electronically. Does not require a seal or signature.