

## Subject card

|                                             |                                                                                                                                                                                                                                                                                               |                                                          |                                         |                                     |                                                |            |     |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|-----------------------------------------|-------------------------------------|------------------------------------------------|------------|-----|
| Subject name and code                       | Quantum Cryptography, PG_00158046                                                                                                                                                                                                                                                             |                                                          |                                         |                                     |                                                |            |     |
| Field of study                              | Quantum Information Technology                                                                                                                                                                                                                                                                |                                                          |                                         |                                     |                                                |            |     |
| Date of commencement of studies             | October 2024                                                                                                                                                                                                                                                                                  |                                                          | Academic year of realisation of subject |                                     | 2024/2025                                      |            |     |
| Education level                             | Master's studies                                                                                                                                                                                                                                                                              |                                                          | Subject group                           |                                     | Obligatory subject group 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                         |                                     |                                                |            |     |
| Conducting unit                             |                                                                                                                                                                                                                                                                                               |                                                          |                                         |                                     |                                                |            |     |
| Name and surname of lecturer (lecturers)    | Subject supervisor                                                                                                                                                                                                                                                                            |                                                          | dr Akshata Shenoy                       |                                     |                                                |            |     |
|                                             | Teachers                                                                                                                                                                                                                                                                                      |                                                          | dr Akshata Shenoy<br><br>Shahana Aziz   |                                     |                                                |            |     |
| 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                                 |                                                | 30.0       | 90  |
| 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 cryptanalysis. 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_U01] is able to apply the scientific method in solving physical problems and reasoning in the field of quantum information theory                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | The student can analyze security of quantum key distribution protocols.<br>The student knows how to perform attacks on basic cryptographic systems and how to counteract them.                                                                                                                                                       | [SU4] test/exam - oral or written |
|                                                                | [QITL3_W01] has extended knowledge in the field of general physics and advanced knowledge in the area of quantum information theory; knows the history of the development of quantum information theory and its importance for the progress of science, knowledge of the world and social development                                                                                                                                                                                                                                                                                                                                                                                                                                              | The student knows examples of several quantum cryptographic protocols, understands their scope of applications, advantages, common issues and vulnerabilities.<br><br>The student knows basics of classical cryptography – especially problems which can be solved with its quantum counterpart and dangers due to quantum computers | [SW4] test/exam - oral or written |
|                                                                | [QITL3_U02] has the skills to plan and conduct basic and advanced research and calculations in the area of quantum information theory or its applications                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | The student can establish key and randomness generation rates for given protocols                                                                                                                                                                                                                                                    | [SU4] test/exam - oral or written |
| 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Adresy na platformie eNauczanie:                                                                                                                                                                                                                                                                                                     |                                   |
| Example issues/<br>example questions/<br>tasks being completed |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                      |                                   |
| Work placement                                                 | Not applicable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                      |                                   |

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