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 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	The student has an advanced understanding of the principles, security, and methods for the analysis and implementation of quantum cryptographic protocols, as well as their significance for secure information processing and the development of modern quantum communication technologies.	[SW4] test/exam - oral or written
[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	The student is able to analyze, design, and evaluate quantum cryptographic protocols by selecting appropriate security models, analytical methods, and computational tools, and to critically assess their properties, limitations, and applications in secure quantum communication.	[SU5] implementation of a problem task
[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	The student has an advanced understanding of the fundamental phenomena, models, and protocols of quantum cryptography, their theoretical foundations, and their significance for secure communication, quantum information technologies, and contemporary scientific research.	[SW4] 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
tutorial part: test	51.0%	50.0%
lecture part: exam	51.0%	50.0%

Recommended reading

Basic literature	Quantum Computation and Quantum Information. Michael A. Nielsen & Isaac L. Chuang (2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press. ISBN: 978-1-107-00217-3.
Supplementary literature	None.
eResources addresses	

Example issues/ example questions/ tasks being completed	1. Explain how the fundamental principles of quantum mechanics guarantee the security of quantum key distribution protocols. Discuss the roles of the no-cloning theorem and quantum measurement. 2. Describe the operation and security analysis of a selected QKD protocol (e.g., BB84 or E91), including eavesdropping detection, error correction, and privacy amplification. 3. Discuss the principal attack models against quantum cryptographic systems and the methods used to ensure security, including device-independent and measurement-device-independent QKD. 4. Describe the physical implementation of quantum cryptographic systems and discuss the main technological challenges involved in practical quantum communication. 5. Discuss advanced applications of quantum cryptography, including quantum authentication, quantum secret sharing, quantum digital signatures, and their role in future quantum communication networks.
Work placement	Not applicable

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