GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Elements of quantum cryptography , PG_00045424		
Field of study	Technical Physics		
Date of commencement of studies	October 2020	Academic year of realisation of subject	2021/2022
Education level	first-cycle studies	Subject group	Optional subject group 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	2	Language of instruction	Polish
Semester of study	3	ECTS credits	4.0
Learning profile	general academic profile	Assessment form	assessment
Conducting unit	Department of Theoretical Physics and Quantum Information -> Faculty of Applied Physics and Mathematics		
Name and surname of lecturer (lecturers)	Subject supervisor	prof. dr hab. Paweł Horodecki	
	Teachers	prof. dr hab. Paweł Horodecki dr inż. Marcin Nowakowski	

Lesson types and methods of instruction	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	30.0	0.0	0.0	0.0	15.0	45
	E-learning hours included: 0.0						
	Adresy na platformie eNauczanie:						

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	45	0.0	0.0	45

Subject objectives	Introduction to fundamental ideas and aspects of quantum cryptography

Learning outcomes	Course outcome	Subject outcome	Method of verification
	K6_W02	The student knows and understands the mathematical foundations of quantum mechanics with particular emphasis on quantum discrete variable. He knows and understands the basic ideas and methods of quantum cryptography. He can explain quantum cryptography protocols taking into account their physical character. He can present selected topics of quantum cryptography and solve simple problems within its scope.	[SW1] Assessment of factual knowledge [SW2] Assessment of knowledge contained in presentation [SW3] Assessment of knowledge contained in written work and projects
	K6_U07	The student is able to present in a popular way the basic ideas of quantum cryptography in a way that is accessible to non-specialists	[SU2] Assessment of ability to analyse information [SU3] Assessment of ability to use knowledge gained from the subject
	K6_U08	The student is able to properly prepare a lecture in the field of quantum cryptography and competently participate in a seminar discussion on this field.	[SU1] Assessment of task fulfilment [SU2] Assessment of ability to analyse information [SU3] Assessment of ability to use knowledge gained from the subject [SU5] Assessment of ability to present the results of task
	K6_K01	The student is able to assimilate the fundamental of achievements in the field of modern knowledge and can identify issues that still need a solution or an optimization. He is able to discuss in a creative way on their possible solutions.	[SK4] Assessment of communication skills, including language correctness [SK1] Assessment of group work skills [SK2] Assessment of progress of work

Subject contents	Quantum mechanics - discrete variable formalism The idea of quantum information and classical information theory: quantum and classical entropy No-cloning theorem Steinspring theorem The concept of quantum channel Qubit channel - bit-flip error and phase error External noise as potential result of cryptographic attack BB84 protocol Quantum composite systems: tensor product and quantum entanglement Quantum fomography and quantum entanglement detection Choi-Jamiołkowski isomorphism The idea of quantum error correction cryptographic perspective E91 protocol Shora-Preskill theorem LOCC paradigm Quantum entanglement distillation and generation of cryptographic key Coherent information Holevo function and i Devetaka-Wintera formula Cryptographic key generation without entanglement distillation - possibilities and limitations Local hidden variables model and Bell theorem Selected Bell inequalities The idea of device independent quantum cryptography Jordan lemma and its application The continuous variable concept in quantum mechanics Formalism of quantum oscillator and coherent states

<table>
<tr><td></td><td>Continuous variables variant of BB84

The problem of cryptographically secure rendomness: quantum expansion and quantum amplification of randomness</td></tr>
<tr><td>Prerequisites and co-requisites</td><td>Basic algebra and mathematical analysis</td></tr>
<tr><td>Assessment methods and criteria</td><td>
<table>
<tr><th>Subject passing criteria</th><th>Passing threshold</th><th>Percentage of the final grade</th></tr>
<tr><td>exam</td><td>60.0%</td><td>60.0%</td></tr>
<tr><td>seminar</td><td>60.0%</td><td>40.0%</td></tr>
</table>
</td></tr>
<tr><td>Recommended reading</td><td>
<table>
<tr><td>Basic literature</td><td>Quantum Computation and Quantum Information, Isaac Chuang, Michael Nielsen, Cambridge University Press (2000)</td></tr>
<tr><td>Supplementary literature</td><td>Quantum cryptography (ang.) , Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Reviews of Modern

Physics, Vol. 74, (2002)</td></tr>
<tr><td>eResources addresses</td><td></td></tr>
</table>
</td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td>Calculate von Neumann entropy for a given mixed state

Estimate secret key capacity of a given channel

Prove the no-cloning theorem (varaint with ancilla)</td></tr>
<tr><td>Work placement</td><td>Not applicable</td></tr>
</table>