KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIWERSYTET GDAŃSKI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt jest współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Course title **Quantum Cryptography**	**ECTS code** 13.2.0416

Name of unit administrating study
Department of Mathematics, Physics and Informatics

Studies

Faculty	**Field of study/ phd studies/doctoral school/postgraduate studies**	**Type**	**Form**
Quantum Information Technology	MSc studies	stationary	

Teaching staff
Dr hab. Marcin Pawłowski; Dr Nikolai Miklin

Forms of classes, the realization and number of hours	**ECTS credits**
A. Forms of classes, in accordance with the UG Rector's regulations **Lecture, auditory exercises**	**Total: 5 ECTS including:** **30 h of lecture – 1 ECTS point;** **30 h of exercises – 1 ECTS point;** **30 h of consultation – 1 ECTS point;** **60 h of student's own work - 2 ECTS points.**
B. The realization of activities **classes in the teaching room of the University of Gdańsk** **blended learning**	
C. Number of hours **Lecture: 30, exercises: 30**	

The academic cycle
According to study program

Type of course	**Language of instruction**
mandatory	**English**

Teaching methods
lecture with multimedia presentation

discussion
case analysis
problem solving

Form and method of assessment and basic criteria for evaluation or examination requirements

A. Final evaluation, in accordance with the UG study regulations
Exam
Credit with grade

B. Assessment methods
Exercises: tests
Lecture: written exam

C. The basic criteria for evaluation or exam requirements

Exercises: Averages score of two tests.
Lecture:
A positive assessment of the written examination assessed by percentage ("UG Study Regulations")

D. Method of verification of the established effects of education

established effect of education	exam	activity	tests
W01	+	+	+
W02	-	+	+
U01	-	+	+
U02	-	+	+
K01	-	+	-

Required courses and introductory requirements

A. Formal requirements

none

B. Prerequisites

Basic knowledge of mathematics at high school level is required.

Aims of education

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.

Course contents

The course contents includes presentation of the following concepts (lecture and exercises will be devoted to the same topics):

- **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: Shor's 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.**

Bibliography of literature

A. Literature required to pass the course

- **"Quantum Computation and Quantum Information", M.A. Nielsen, I.L. Chuang, Cambridge University Press.**
- **Collection of scientific papers supplied by the lecturer.**

The learning outcomes (for the field of study and specialization)	**Knowledge**
K_W02 *Student has in-depth knowledge of advanced mathematics, mathematical and computer methods necessary to solve physical problems of medium complexity and advanced in the area of quantum information and its technological aspects* *K_W03* *Student knows advanced experimental, observational and numerical techniques allowing to plan and perform a complex physical experiment or computer simulation* *K_U02* *Student can apply mathematical knowledge to*	W01: The student knows examples of several quantum cryptographic protocols, understands their scope of applications, advantages, common issues and vulnerabilities.(K_W02, K_W03) W02 The student knows basics of classical cryptography – especially problems which can be solved with its quantum counterpart and dangers due to quantum computers. (K_W02, K_W03) **Skills** U01 The student can analyze security of quantum key distribution protocols. (K_U02) U02 The student knows how to perform attacks on basic cryptographic systems and how to counteract them. (K_U02) U03 The student can establish key and randomness generation rates for given protocols. (K_U02) **Social competence** K01 The student understands the importance of data security in modern society and knows the impact of quantum technologies in that field. (K_K01)

formulating, analyzing and solving problems related to information theory *K_K06* *Student is aware of the dangers of obtaining information from unverified sources, including those from the Internet*	

Contact
marcin.pawlowski@ug.edu.pl