KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Nazwa przedmiotu	Kod ECTS
Quantum Cryptography	13.2.0416

Nazwa jednostki prowadzącej przedmiot

Instytut Fizyki Teoretycznej i Astrofizyki

Studia

wydział	kierunek		
Wydział Matematyki, Fizyki i Informatyki	Quantum Information Technology	poziom	wszystkie
		forma	wszystkie
		moduł specjalnościowy	wszystkie
		specjalizacja	wszystkie

Nazwisko osoby prowadzącej (osób prowadzących)

prof. UG, dr hab. Marcin Pawłowski

Formy zajęć, sposób ich realizacji i przypisana im liczba godzin

Formy zajęć

Wykład, Ćw. audytoryjne

Sposób realizacji zajęć

zajęcia on-line, zajęcia w sali dydaktycznej

Liczba godzin

Wykład: 30 godz., Ćw. audytoryjne: 30 godz.

Liczba punktów ECTS

5
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

Termin realizacji przedmiotu

2021/2022 letni

Status przedmiotu

obowiązkowy

Język wykładowy

angielski

Metody dydaktyczne

- Analiza zdarzeń krytycznych (przypadków)
- Dyskusja
- Rozwiązywanie zadań
- Wykład z prezentacją multimedialną

Forma i sposób zaliczenia oraz podstawowe kryteria oceny lub wymagania egzaminacyjne

Sposób zaliczenia

- Zaliczenie na ocenę
- Egzamin

Formy zaliczenia

- egzamin pisemny testowy
- kolokwium

Podstawowe kryteria oceny

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

Sposób weryfikacji założonych efektów uczenia się

Określenie przedmiotów wprowadzających wraz z wymogami wstępnymi

A. Wymagania formalne
none

B. Wymagania wstępne
Basic knowledge of mathematics at high school level is required.

Cele kształcenia

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.

Treści programowe

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

Wykaz literatury

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

Kierunkowe efekty uczenia się

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 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

Wiedza

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)

Umiejętności

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)

Kompetencje społeczne (postawy)

K01
The student understands the importance of data security in modern society and knows the impact of quantum technologies in that field. (K_K01

Kontakt

marcin.pawlowski@ug.edu.pl