

Karta przedmiotu

Nazwa i kod przedmiotu	Quantum Cryptography, PG_00158046						
Kierunek studiów	Quantum Information Technology (O)						
Data rozpoczęcia studiów	październik 2025 r.		Rok akademicki realizacji przedmiotu		2025/2026		
Poziom kształcenia	II stopnia		Grupa zajęć		Grupa zajęć obowiązkowych z zakresu kierunku studiów		
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	1		Język wykładowy		angielski		
Semestr studiów	2		Liczba punktów ECTS		6.0		
Profil kształcenia	ogólnoakademicki		Forma zaliczenia		egzamin		
Jednostka prowadząca							
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr Akshata Shenoy				
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	30.0	30.0	0.0	0.0	0.0	60
	W tym liczba godzin zajęć na odległość: 0.0						
Aktywność studenta i liczba godzin pracy	Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów		Udział w konsultacjach		Praca własna studenta	RAZEM
	Liczba godzin pracy studenta	60		0.0		30.0	90
Cel przedmiotu	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.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[QITL3_U02] posiada umiejętności planowania i przeprowadzenia podstawowych oraz zaawansowanych badań i obliczeń w obszarze teorii informacji kwantowej lub jej zastosowań	The student can establish key and randomness generation rates for given protocols	[SU4] test/egzamin - ustny lub pisemny
	[QITL3_W01] ma rozszerzoną wiedzę w zakresie fizyki ogólnej oraz zaawansowaną z obszaru teorii informacji kwantowej; zna historię rozwoju teorii informacji kwantowej i jej znaczenie dla postępu nauk ścisłych i przyrodniczych, poznania świata i rozwoju społecznego	The student knows examples of several quantum cryptographic protocols, understands their scope of applications, advantages, common issues and vulnerabilities. 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/egzamin - ustny lub pisemny
	[QITL3_U01] potrafi zastosować metodę naukową w rozwiązywaniu problemów fizycznych i wnioskowaniu w zakresie teorii informacji kwantowej	The student can analyze security of quantum key distribution protocols. The student knows how to perform attacks on basic cryptographic systems and how to counteract them.	[SU4] test/egzamin - ustny lub pisemny
Treści przedmiotu	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		
Wymagania wstępne i dodatkowe			
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	tutorial part: test	51.0%	50.0%
	lecture part: exam	51.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	Quantum Computation and Quantum Information, M.A. Nielsen, I.L. Chuang, Cambridge University Press	
	Uzupełniająca lista lektur	None.	
	Adresy eZasobów		
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania			
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.