

**Karta przedmiotu**

Nazwa i kod przedmiotu	Quantum Cryptography, PG_00199109						
Kierunek studiów	Quantum Information Technology (O)						
Data rozpoczęcia studiów	październik 2026 r.	Rok akademicki realizacji przedmiotu			2026/2027		
Poziom kształcenia	II stopnia	Grupa zajęć			Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
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		90.0	150
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_W02] zna i rozumie w pogłębionym stopniu kluczowe oraz wybrane zaawansowane zagadnienia szczegółowe z zakresu technologii informacji kwantowej, w tym metody ich badania i rozwijania, oraz ich zastosowania w kontekście dynamicznych przemian technologicznych, w szczególności w obszarze przetwarzania informacji, kryptografii oraz rozwoju zaawansowanych systemów obliczeniowych		
	[QITL3_U02] potrafi wykorzystywać posiadaną wiedzę z zakresu technologii informacji kwantowej – formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach poprzez właściwy dobór źródeł i informacji z nich pochodzących, dokonywanie oceny, krytycznej analizy, syntezy, twórczej interpretacji i prezentacji tych informacji, a także poprzez dobór oraz stosowanie właściwych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych i przystosowanie istniejących lub opracowanie nowych metod i narzędzi		
	[QITL3_W01] zna i rozumie w pogłębionym stopniu wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające złożone zależności między nimi, stanowiące zaawansowaną wiedzę ogólną z zakresu technologii informacji kwantowej, a także metodologię badań naukowych właściwą dla tej dyscypliny oraz jej znaczenie w kontekście współczesnych kierunków rozwoju nauki i technologii		
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 ocena końcowej
	lecture part: exam	51.0%	50.0%
	tutorial part: test	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		