Uniwersytet Gdański

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 cryptoanalysis. 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	The student has an advanced understanding of the principles, security, and methods for the analysis and implementation of quantum cryptographic protocols, as well as their significance for secure information processing and the development of modern quantum communication technologies.	[SW4] test/egzamin - ustny lub pisemny
[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	The student is able to analyze, design, and evaluate quantum cryptographic protocols by selecting appropriate security models, analytical methods, and computational tools, and to critically assess their properties, limitations, and applications in secure quantum communication.	[SU5] realizacja zadania problemowego
[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	The student has an advanced understanding of the fundamental phenomena, models, and protocols of quantum cryptography, their theoretical foundations, and their significance for secure communication, quantum information technologies, and contemporary scientific research.	[SW4] 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 osiąganych 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. Michael A. Nielsen & Isaac L. Chuang (2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press. ISBN: 978-1-107-00217-3.
Uzupełniająca lista lektur	None.
Adresy eZasobów	

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	1. Explain how the fundamental principles of quantum mechanics guarantee the security of quantum key distribution protocols. Discuss the roles of the no-cloning theorem and quantum measurement. 2. Describe the operation and security analysis of a selected QKD protocol (e.g., BB84 or E91), including eavesdropping detection, error correction, and privacy amplification. 3. Discuss the principal attack models against quantum cryptographic systems and the methods used to ensure security, including device-independent and measurement-device-independent QKD. 4. Describe the physical implementation of quantum cryptographic systems and discuss the main technological challenges involved in practical quantum communication. 5. Discuss advanced applications of quantum cryptography, including quantum authentication, quantum secret sharing, quantum digital signatures, and their role in future quantum communication networks.
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.