



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Projekt współfinansowany przez
Unię Europejską w ramach
Europejskiego Funduszu
Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Nazwa przedmiotu		Kod ECTS	
Podstawy Informatyki Kwantowej		11.3.1690	
Nazwa jednostki prowadzącej przedmiot			
Instytut Informatyki			
Studia			
wydział	kierunek	poziom	drugiego stopnia
Wydział Matematyki, Fizyki i Informatyki	Informatyka	forma	stacjonarne
		moduł	wszystkie
		specjalnościowy	wszystkie
		specjalizacja	wszystkie
Nazwisko osoby prowadzącej (osób prowadzących)			
prof. UG, dr hab. Karol Horodecki			
Formy zajęć, sposób ich realizacji i przypisana im liczba godzin		Liczba punktów ECTS	
Formy zajęć		7 Przedmiot fakultatywny w wymiarze 30h wykładu i 30h ćwiczeń/lab. + praca własna studenta.	
Wykład, Ćw. laboratoryjne			
Sposób realizacji zajęć			
zajęcia w sali dydaktycznej			
Liczba godzin			
Wykład: 30 godz., Ćw. laboratoryjne: 30 godz.			
Termin realizacji przedmiotu			
2021/2022 letni			
Status przedmiotu		Język wykładowy	
fakultatywny (do wyboru)		polski	
Metody dydaktyczne		Forma i sposób zaliczenia oraz podstawowe kryteria oceny lub wymagania egzaminacyjne	
<ul style="list-style-type: none"> - Rozwiązywanie zadań - Wykład z prezentacją multimedialną 		Sposób zaliczenia	
		<ul style="list-style-type: none"> - Zaliczenie na ocenę - Egzamin 	
		Formy zaliczenia	
		<ul style="list-style-type: none"> - ustalenie oceny zaliczeniowej na podstawie ocen cząstkowych otrzymywanych w trakcie trwania semestru - kolokwium - egzamin pisemny (dłuższa wypowiedź pisemna / rozwiązanie problemu) 	
		Podstawowe kryteria oceny	
		Aktywność na ćwiczeniach, wyniki dwóch kolokwium z umiejętności praktycznych przetwarzania kwantowej informacji, egzamin pisemny z teorii przedmiotu	
Sposób weryfikacji założonych efektów uczenia się			

zakładany efekt kształcenia	egzamin	kolokwium	projekt	sprawdzian	referat	raport	aktywność w dyskusji	obserwacja postawy
Wiedza								
K_W01	X	X					X	
K_W02	X							
K_W03	X	X						
K_W04	X							
K_W06	X	X						
P_W1	X	X						
P_W2	X	X						
P_W3	X	X						
Umiejętności								
K_U01								X
K_U03	X							
K_U05	X							
K_U08			X				X	
P_U1								X
P_U2								X
P_U3	X						X	
P_U4								X
Kompetencje								
K_K01							X	X
K_K04	X	X						
K_K05		X						
P_K1								X
P_K2							X	X

Określenie przedmiotów wprowadzających wraz z wymogami wstępnymi**A. Wymagania formalne**

brak

B. Wymagania wstępne

Podstawy algebry liniowej i rachunku prawdopodobieństwa, podstawowa wiedza na temat teorii złożoności obliczeniowej i bramek logicznych oraz umiejętność programowania w językach imperatywnych

Cele kształcenia

Zaprezentowanie nowoczesnych celów, możliwości i ograniczeń oraz metod przetwarzania informacji zapisanej na kwantowych nośnikach danych.

Treści programowe

W zakresie przedmiotu przewidziane jest przedstawienie podstawowych osiągnięć kwantowej informatyki, w tym:

- krótkie przedstawienie historycznych podstaw mechaniki kwantowej
- wprowadzenie formalizmu mechaniki kwantowej (MK), w tym aksjomatów MK, notacji Diraca oraz pojęcia przestrzeni Hilberta.
- szczegółowe omówienie podstawowych efektów kwantowej komunikacji, w tym kwantowej teleportacji, kwantowego gęstego kodowania, kwantowej kryptografii (protokoły E91, B92, BBM, BB84 i ich warianty) oraz zakaz kwantowego klonowania.
- w kontekście dowodu bezpieczeństwa protokołu BB84 zostaną wprowadzone podstawy kwantowych kodów korekcji błędów.
- w zakresie kwantowego obliczania zostaną omówione algorytm Deutscha-Jozsy, algorytm Simona, algorytm Grovera i algorytm Shora (ten ostatni jako podstawę do złamania szyfrowania RSA).
- zostanie wprowadzony jeden języków programowania kwantowego komputera, takich jak QASM.
- omówione zostanie obszernie zjawisko splątania (miary splątania, różne klasy mieszanych stanów splątanych, takich jak stany o związanym splątaniu i stany bezpieczne),
- omówione zostanie zjawisko nielokalnych korelacji (nierówności Bella i wykorzystanie ich do kryptografii niezależnej od urządzenia).
- wprowadzone zostaną elementy teorii informacji Shannona, w tym pojęcie entropii Shannona oraz pojęcie wzajemnej informacji, jak również ich kwantowych odpowiedników wraz z wykorzystaniem w kontekście Kwantowego Internetu.

Wykaz literatury

- „Quantum computation and Quantum information” M. A. Nielsen and I. L. Chuang Cambridge University Press, Cambridge (2000)
- "Wprowadzenie do algorytmów kwantowych", K. Giaro, M. Kamiński, Exit 2003
- „Quantum entanglement” R. Horodecki, M. Horodecki, P. Horodecki, K. Horodecki Rev. Mod. Phys. (2009)
- "Bell nonlocality" N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner. Rev. Mod. Phys., 86:839, (2014).
- „Introduction to Quantum Computation and Information” H.-K. Lo, S. Popescu T. Spiller, World Scientific (1998)
- „Elements of Information Theory” T. M. Cover and J. A. Thomas Wiley Series in Telecommunications (1991)
- publikacje dotyczące tematyki wykładu zawarte w bazie www.arxiv.org/quant-ph

Kierunkowe efekty uczenia się

K_W01: ma pogłębioną wiedzę z działów matematyki niezbędnych do studiowania informatyki; dobrze rozumie rolę i znaczenie konstrukcji rozumowań matematycznych

K_W02: ma pogłębioną wiedzę w zakresie języków formalnych, modeli obliczeń oraz zagadnień złożoności obliczeniowej; zna aparat formalny pozwalający na formułowanie i badanie własności obiektów informatycznych

K_W03: ma pogłębioną wiedzę na temat paradygmatów programowania oraz zaawansowanych konstrukcji programistycznych; zna aktualne trendy w językach programowania

K_W04: zna złożone struktury danych oraz zaawansowane metody algorytmicznego rozwiązywania problemów obliczeniowo trudnych (algorytmy wykładnicze, aproksymacja, heurystyki)

K_W06: zna dobrze zasady bezpieczeństwa i higieny pracy w zawodzie informatyka

K_U01: potrafi zastosować wiedzę matematyczną do formułowania, analizowania i rozwiązywania zadań związanych z informatyką

K_U03: projektuje, analizuje pod kątem poprawności i złożoności obliczeniowej oraz buduje algorytmy z wykorzystaniem zaawansowanych technik programistycznych i struktur danych

K_U05: potrafi zastosować znane algorytmy w konkretnych sytuacjach, potrafi efektywnie dobrać rodzaj algorytmu w zależności od postawionego problemu

K_U08: potrafi pozyskiwać informacje z literatury fachowej, baz danych, Internetu oraz innych źródeł, integrować je, oceniać ich wiarygodność, dokonywać interpretacji oraz wyciągać wnioski i formułować opinie

K_K01: zna ograniczenia własnej wiedzy i rozumie potrzebę dalszego uczenia się

K_K04: rozumie i docenia znaczenie uczciwości intelektualnej w działaniach własnych i innych osób; postępuje etycznie

K_K05: potrafi myśleć i działać w sposób przedsiębiorczy z zachowaniem zasad etyki zawodowej

Wiedza

Student, który uzyska zaliczenie zna

- fundamentalne koncepcje informatyki kwantowej,
- cele, możliwości i ograniczenia przetwarzania informacji z wykorzystaniem praw mechaniki kwantowej

Efekty przedmiotowe

P_W1: zna i potrafi stosować formalizm mechaniki kwantowej do formułowania podstawowych faktów z zakresu informatyki kwantowej (K_W01)

P_W2: zna ataki na standardową kryptografię z użyciem kwantowego komputera oraz na kwantową kryptografię zależną i niezależną od urządzenia, ma także ogólną wiedzę o aktualnych kierunkach rozwoju i nowoczesnych wariantach omawianych kierunków wiedzy (K_W06, K_W01)

P_W3: zna wybrane algorytmy w zakresie obliczeń kwantowych (K_W02), w tym algorytm Grovera (K_W04), oraz jeden z języków programowania kwantowego komputera (K_W03)

Umiejętności

Student, który uzyska zaliczenie:

- potrafi zorientować się w dziedzinie i umiejscowić nowe osiągnięcia na tle już dokonanych odkryć.
- wykorzystuje poznaną wiedzę aby sformułować własne pomysły dotyczące przetwarzania danych zapisanych na kwantowych nośnikach.
- potrafi zastosować właściwy algorytm kwantowy w zależności od celu przetworzenia danych zapisanych na kwantowych nośnikach.

Efekty przedmiotowe

P_U1: potrafi zastosować znane algorytmy kwantowe w konkretnych sytuacjach wymagających przetwarzania informacji zapisanej na kwantowych nośnikach, potrafi efektywnie dobrać rodzaj i sposób wykonania algorytmu w zależności od postawionego problemu (K_U05)

P_U2: potrafi zastosować wiedzę matematyczną do formułowania, analizowania i rozwiązywania problemów dotyczących przetwarzania informacji w szybki i/lub bezpieczny sposób, związanych z informatyką kwantową (K_U01)

P_U3: zna i rozumie dowody złożoności obliczeniowej wybranych algorytmów kwantowych (K_U03)

P_U4: umie znajdować niezbędne informacje w literaturze fachowej, bazach danych m.in. pod adresem www.arxiv.org i innych źródłach, zna podstawowe czasopisma i konferencje naukowe w swojej specjalności oraz umiejscowić nowe osiągnięcia na tle już dokonanych odkryć (K_U08)

Kompetencje społeczne (postawy)

Student, który uzyska zaliczenie

- jest bardziej otwarty na niestandardowe podejście do wykorzystania znanych obszarów wiedzy, jak ma to miejsce w wielu obszarach informatyki kwantowej
- rozumie konieczność dalszego kształcenia się

Efekty przedmiotowe

P_K1 potrafi myśleć i działać w sposób etyczny i przedsiębiorczy, dzięki temu, że staje się bardziej otwarty na oparte o etykę niestandardowe podejście do wykorzystania znanych już obszarów wiedzy takich jak kwantowa kryptografia (K_K04, K_K05)

P_K2 Zna możliwe kierunki dalszego rozwoju pozwalające na pogłębienie wiedzy na temat bezpieczeństwa zapewnianego na sposób kwantowy (takich jak

	bezpieczeństwo losowości oraz tematyki obliczeń kwantowych takich jak odporne na błędy obliczanie kwantowe) (K_K01)
--	---

Kontakt

khorodec@inf.ug.edu.pl
--