Zaproszenie do obliczeń i algorytmów kwantowych - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Zaproszenie do obliczeń i algorytmów kwantowych
Kod przedmiotu	11.0-WE-AEIT-ZOiAK
Wydział	Wydział Informatyki, Elektrotechniki i Automatyki
Kierunek	Automatyka i robotyka, Elektrotechnika, Informatyka
Profil	ogólnoakademicki
Rodzaj studiów	doktoranckie
Semestr rozpoczęcia	semestr zimowy 2018/2019

Informacje o przedmiocie

Semestr	3
Liczba punktów ECTS do zdobycia	2
Typ przedmiotu	obieralny
Język nauczania	polski
Sylabus opracował	• prof. dr hab. Roman Gielerak

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Wykład	15	1	-	-	Egzamin

Cel przedmiotu

- wprowadzenie do nowego modelu obliczeniowego opartego o paradygmat fizyki kwantowej

- prezentacja kwantowych modeli obliczeniowych

-wprowadzenie do algorytmiki kwantowej

- zastosowania technologii kwantowych do kryptografii

Wymagania wstępne

-podstawy fizyki kwantowej

-podstawy algebry liniowej i analizy matematycznej

Zakres tematyczny

Wstęp. Historia narodzin i perspektywy informatyki kwantowej. Algorytm Schora (info): zagrożenie dla kryptografii RSA.

Narodziny teorii kwantowej: historia wczesnej fazy. Dualizm korpuskularno-falowy mikroświata. Cząsteczki światła: fotony i ich podstawowe własności, polaryzacja.

Ogólna struktura mechaniki kwantowej: przestrzeń Hilberta, stany czyste, amplitudy prawdopodobieństwa. Reprezentacja położeń: funkcja falowa, równanie Schrodingera. Obserwable i wartości wlasne. Rozkłady spektralne. Operacje unitarne. Pomiary kwantowomechaniczne: wartości średnie, możliwe wartości pomiaru, zasada superpozycji. Zasada redukcji stanu (dekoherencja). Zasada nieoznaczoności Heisenberga. Układy złożone: opis za pomocą iloczynów tensorowych.

Stany splatane, miary splątania. Q-bity.

Model obwodowy Podstawowe bramki kwantowe; jedno, dwu- i trzy-kubitowe. Zagadnienie uniwersalności układu bramek. Dyskretyzacja. Obwody kwantowe. Problem Jotzsy-Deutcha jako przykład działania komputera kwantowego.

Wybrane algorytmy kwantowe i ich implementacje Kwantowy algorytm przeszukiwania: kwantowa maszyna Grovera. Algorytm Shora.Kryptografia RSA. Analiza teoretyczna algorytmu kwantowego.

Perspektywy: sprzętowa strona projektu. Fizyczne realizacje najprostszych bramek kwantowych.

Idee kwantowej kryptografii.Przeglad podstawowych protokołow kwantowej dystrybucji kluczy i ich implementacje

Metody kształcenia

wykład: wykład problemowy, wykład konwencjonalny

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
-zapoznanie z podstawami algorytmiki kwantowej	• K_W01 • K_U03	• egzamin - ustny, opisowy, testowy i inne	• Wykład

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
-zapoznanie z kwantowa kryptografia	• K_W01 • K_U01	• egzamin - ustny, opisowy, testowy i inne	• Wykład
-zapoznanie z podstawowymi modelami obliczeń kwantowych	• K_W01	• egzamin - ustny, opisowy, testowy i inne	• Wykład

Warunki zaliczenia

Egzamin ustny lub prezentacja referatu i jego wspolna dyskusja , referatu przydzielanego w trybie indywidualnym

Literatura podstawowa

1.M.A. Nielsen , I.L.Chuang , Quantum Computation and Quantum Information , Cambridge University Press, 2000

2. I. Bengtsson , K.Życzkowski ,Geometry of Quantum States. An Introduction to Quantum Entanglement. Cambridge University Press, 2006.

3. K. Giaro ,Elementy Kwantowego Modelu Obliczen i Algorytmiki Kwantowej , Wydawnictwo Naukowe OWSLiZ , Olsztyn 2013

4. Nicolas Gisin, Gre´goire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Quantum cryptography, REVIEWS OF MODERN PHYSICS, VOLUME 74, JANUARY 2002

Literatura uzupełniająca

Uwagi

Zmodyfikowane przez prof. dr hab. inż. Marcin Witczak (ostatnia modyfikacja: 27-03-2018 12:08)