POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Elementy kwantowej kryptografii, PG_00045424		
Kierunek studiów	Fizyka Techniczna		
Data rozpoczęcia studiów	październik 2022 r.	Rok akademicki realizacji przedmiotu	2023/2024
Poziom kształcenia	I stopnia - inżynierskie	Grupa zajęć	Grupa zajęć fakultatywnych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki
Forma studiów	stacjonarne	Sposób realizacji	na uczelni
Rok studiów	2	Język wykładowy	polski
Semestr studiów	3	Liczba punktów ECTS	4.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Wydział Fizyki Technicznej i Matematyki Stosowanej -> Katedra Fizyki Teoretycznej i Informatyki Kwantowej		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	prof. dr hab. Paweł Horodecki	
	Prowadzący zajęcia z przedmiotu	dr inż. Marcin Nowakowski prof. dr hab. Paweł Horodecki	

Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	30.0	0.0	0.0	0.0	15.0	45
	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	45	0.0	0.0	45

Cel przedmiotu	Wprowadzenie do podstawowych idei i aspektów kwantowej kryptografii

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K6_K01] Rozumie potrzebę uczenia się przez całe życie oraz potrzebę podnoszenia kompetencji zawodowych i osobistych. Potrafi inspirować i organizować proces uczenia się innych osób.	Student rozumie otwarty charakter badań nowoczesnych dziedzin i potrafi wskazać problemy, które wciąż potrzebują rozwiązania bądź też jego optymalizacji. Potrafi w sposób twórczy dyskutować nad możliwymi rozwiązaniami.	[SK4] Ocena umiejętności komunikacji, w tym poprawności językowej [SK1] Ocena umiejętności pracy w grupie [SK2] Ocena postępów pracy
	[K6_U07] Potrafi w sposób popularny przedstawić podstawowe fakty z zakresu fizyki oraz pokrewnych dziedzin i dyscyplin nauki.	Student potrafi przedstawić w sposób popularny podstawowe idee kwantowej kryptografii w sposób przystępny dla niespecjalistów.	[SU2] Ocena umiejętności analizy informacji [SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu
	[K6_U08] Posiada umiejętność przygotowywania prac i opracowań pisemnych oraz wystąpień ustnych, w językach polskim i angielskim, dotyczących zagadnień szczegółowych z zakresu fizyki oraz pokrewnych dziedzin i dyscyplin nauki.	Student potrafi prawidłowo przygotować referat z zakresu kwantowej kryptografii i kompetentnie brać udział w seminaryjnej dyskusji na temat tej dziedziny.	[SU1] Ocena realizacji zadania [SU2] Ocena umiejętności analizy informacji [SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu [SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania
	[K6_W02] Posiada uporządkowaną wiedzę w zakresie podstaw fizyki, obejmującą mechanikę, termodynamikę, elektryczność i magnetyzm, optykę, fizykę atomu i cząsteczki, fizykę ciała stałego, fizykę jądra atomowego i cząstek elementarnych.	Student zna i rozumie podstawy matematyczne mechaniki kwantowej ze szczególnym uwzględnieniem kwantowej zmiennej dyskretnej. Zna i rozumie podstawowe idee i metody kryptografii kwantowej. Potrafi wyjaśnić protokoły kryptografii kwantowej z uwzględnieniem ich fizycznej specyfiki. Potrafi zaprezentować wybrane zagadnienia kryptografii kwantowej oraz rozwiązać proste zagadnienia w jej zakresie.	[SW1] Ocena wiedzy faktograficznej [SW2] Ocena wiedzy zawartej w prezentacji [SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym

Treści przedmiotu	Formalizm mechaniki kwantowej zmiennej dyskretnej. Koncepcja kwantowej teorii informacji a klasyczna teoria informacji: entropia klasyczna i kwantowa. Twierdzenie o niemożności klonowania. Twierdzenie Steinspringa. Pojęcie kanału kwantowego. Kanał kubitowy błąd bitu i błąd fazy Zakłócenia zewnętrzne jako możliwy przejaw ataku kryptograficznego Protokół BB84 Kwantowe układy złożone: iloczyn tensorowy i kwantowe splątanie Kwantowa tomografia i detekcja kwantowego splątania Izomorfizm Choi-Jamiołkowskiego Koncepcja kwantowej korekcji błędu perspektywa kryptograficzna Protokół E91 Paradygmat LOCC Destylacja kwantowego splątania a proces generacji klucza kryptograficznego Twierdzenie Shora-Preskilla Informacja koherentna. Funkcja Holevo i formuła Devetaka-Wintera Generacja klucza bez destylacji splątania - możliwości i ograniczenia Model ukrytych zmiennych i twierdzenie Bella. Wybrane nierówności Bella Koncepcja kryptografii niezależnej od urządzenia Lemat Jordana i jego zastosowanie Pojęcie zmiennej ciągłej w mechanice kwantowej Formalizm kwantowego oscylatora harmonicznego i stany koherentne.

<table>
<tr><td></td><td>Wariant protokołu BB84 dla zmiennej ciągłej

Problem kryptograficznie bezpiecznej losowości: kwantowa ekspansja i

i kwantowe wzmocnienie losowości.</td></tr>
<tr><td>Wymagania wstępne
i dodatkowe</td><td>Podstawy algebry i analizy matematycznej</td></tr>
<tr><td>Sposoby i kryteria
oceniania osiąganych
efektów uczenia się</td><td>
<table>
<tr><th>Sposób oceniania (składowe)</th><th>Próg zaliczeniowy</th><th>Składowa oceny końcowej</th></tr>
<tr><td>seminarium</td><td>60.0%</td><td>40.0%</td></tr>
<tr><td>egzamin</td><td>60.0%</td><td>60.0%</td></tr>
</table>
</td></tr>
<tr><td>Zalecana lista lektur</td><td>
<table>
<tr><td>Podstawowa lista lektur</td><td>Kwantowe obliczanie i kwantowa informacja (ang.) ,Isaac Chuang, Michael Nielsen, Cambridge University Press (2000)</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td>Kryptografia kwantowa (ang.) , Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Reviews of Modern

Physics, Vol. 74, (2002)</td></tr>
<tr><td>Adresy eZasobów</td><td>Adresy na platformie eNauczanie:</td></tr>
</table>
</td></tr>
<tr><td>Przykładowe zagadnienia/
przykładowe pytania/
realizowane zadania</td><td>Oblicz entropię von Neumanna dla zadanego mieszanego stanu kwantowego

Oszacuj pojemność krytoptograficzną danego kanału kwantowego

Udowodnij twierdzenie o niemożności klonowania (wariant z układem pomocniczym)</td></tr>
<tr><td>Praktyki zawodowe
w ramach przedmiotu</td><td>Nie dotyczy</td></tr>
</table>