



Karta przedmiotu

Nazwa i kod przedmiotu	Elementy kwantowej kryptografii, PG_00045424						
Kierunek studiów	Fizyka Techniczna						
Data rozpoczęcia studiów	październik 2020 r.	Rok akademicki realizacji przedmiotu			2021/2022		
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	prof. dr hab. Paweł Horodecki dr inż. Marcin Nowakowski					
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						
	Adresy na platformie eNauczanie:						
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_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
	[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_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

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

	<p>Wariant protokołu BB84 dla zmiennej ciągłej</p> <p>Problem kryptograficznie bezpiecznej losowości: kwantowa ekspansja i</p> <p>i kwantowe wzmocnienie losowości.</p>		
Wymagania wstępne i dodatkowe	Podstawy algebry i analizy matematycznej		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	egzamin	60.0%	60.0%
	seminarium	60.0%	40.0%
Zalecana lista lektur	Podstawowa lista lektur	Kwantowe obliczanie i kwantowa informacja (ang.) , Isaac Chuang, Michael Nielsen, Cambridge University Press (2000)	
	Uzupełniająca lista lektur	Kryptografia kwantowa (ang.) , Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Reviews of Modern Physics, Vol. 74, (2002)	
	Adresy eZasobów		
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	<p>Oblicz entropię von Neumanna dla zadanego mieszanego stanu kwantowego</p> <p>Oszacuj pojemność kryptograficzną danego kanału kwantowego</p> <p>Udowodnij twierdzenie o niemożności klonowania (wariant z układem pomocniczym)</p>		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		