(pieczęć wydziału)

KARTA PRZEDMIOTU

1. Nazwa przedmiotu: KRYPTOGRAFIA KWANTOWA **2. Kod przedmiotu: QCR**

3. Karta przedmiotu ważna od roku akademickiego: 2018/2019

4. Forma kształcenia: studia trzeciego stopnia

5. Forma studiów: studia stacjonarne

6. Studia: CyPhiS - Interdyscyplinarne studia doktoranckie w dziedzinie systemów cyber-fizycznych

7. Profil studiów:

8. Specjalność:

9. Rok: 2

10. Jednostka prowadząca przedmiot: Instytut Elektroniki, RAu3

11. Prowadzący przedmiot: dr hab. Piotr Zawadzki

12. Przynależność do grupy przedmiotów:

13. Status przedmiotu: obowiązkowy

14. Język prowadzenia zajęć: polski

15. Przedmioty wprowadzające oraz wymagania wstępne:

Zakłada się, że student zna w zakresie podstawowym elementy rachunku prawdopodobieństwa, właściwości przestrzeni wektorowych oraz pojęcia klasycznej teorii informacji.

16. Cel przedmiotu:

Celem przedmiotu jest zapoznanie studentów z metodami kwantowego przetwarzania informacji oraz wykorzystaniem tych technik do konstrukcji protokołów kryptograficznych. Omawiane zagadnienia dotyczą wykorzystania specyfiki systemów kwantowych do konstrukcji systemów teleinformatycznych o właściwościach niemożliwych do uzyskania metodami klasycznymi. Jako przykłady takich konstrukcji szczegółowo omawiany jest algorytm Shor'a oraz protokoły kwantowej dystrybucji klucza (QKD), protokoły bezpośredniej bezpiecznej komunikacji kwantowej (QDC) oraz komunikacja kontrfaktyczna (ang. counterfactual communication).

17. Efekty kształcenia:[1]

Nr	Opis efektu kształcenia	Metoda sprawdzenia efektu kształcenia	Forma prowadzenia zajęć	Odniesienie do efektów dla kierunku studiów
W1	Zna aksjomaty kwantowej teorii informacji	wykonanie projektu	wykład	RAU_CyPhiS_W01
W2	Zna podstawowe protokoły QKD	wykonanie projektu	wykład	RAU_CyPhiS_W05
W3	Zna zasady przetwarzania informacji w komputerach kwantowych	wykonanie projektu	wykład	RAU_CyPhiS_W09
U1	Potrafi stosować notację Diraca	wykonanie projektu	projekt	RAU_CyPhiS_U01
U2	Potrafi przeanalizować prosty kwantowy protokół kryptograficzny	wykonanie projektu	projekt	RAU_CyPhiS_U04
U3	Potrafi przeanalizować działanie obwodu kwantowego	wykonanie projektu	projekt	RAU_CyPhiS_U05

[1] należy wskazać ok. 5 – 8 efektów kształcenia

18. Formy zajęć dydaktycznych i ich wymiar (liczba godzin)

W.: 10 P.: 0

19. Treści kształcenia:

Wykład

1. Aksjomatyczne sformułowanie mechaniki kwantowej. Pojęcie stanu, operatora, wielkości mierzalnej. Specyfika pomiaru kwantowego. Notacja Diraca. Twierdzenie o nieklonowaniu stanów kwantowych.
2. Pojęcie qubitu. Podstawowe operacje na qubitach. Reprezentacja macierzowa. Iloczyn tensorowy przestrzeni i stanów. Operacje na dwóch qubitach. Pojęcie splątania stanów.
3. Obwody kwantowe. Kwantowa transformacja Fouriera. Algorytm Grovera
4. Algorytm Shora faktoryzacji liczb w czasie wielomianowym i jego konsekwencje dla współczesnych systemów kryptograficznych.
5. Stany mieszane. Entropia von Neumanna. Kres Holevo.
6. Kanał kwantowy. Fidelity. Rozróżnialność stanów kwantowych.
7. Szumy w kanałach kwantowych i pojemność informacyjna kanału kwantowego.
8. Idea działania protokołów kwantowej dystrybucji klucza (QKD)
9. Protokoły BB84, B92, SARG04 i EPR .
10. Praktyczne realizacje systemów QKD i zagadnienie oceny ich bezpieczeństwa.
11. Idea działania protokołów bezpośredniej komunikacji kwantowej na przykładzie protokołu Ping-Pong.
12. Przesyłanie stanów kwantowych. Protokół teleportacji kwantowej.
13. Komunikacja kontrfaktyczna.

Projekt

Zadania projektowe obejmują następujące grupy problemów:

1. Analiza wybranych obwodów kwantowych
2. Badanie ataków na wybrane protokoły kwantowe.
3. Numeryczna symulacja działania obwodów kwantowych w środowisku Matlab/Octave

20. Egzamin: nie

21. Literatura podstawowa:

[1] M. L. Bellac, Wstęp do informatyki kwantowej, Wydawnictwa Naukowe PWN, 2012

22. Literatura uzupełniająca:

[1] E. Desurvire: Classical and Quantum Information Theory, Cambridge University Press, 2009

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

[3] http://www.theory.caltech.edu/~preskill/ph219/

23. Nakład pracy studenta potrzebny do osiągnięcia efektów kształcenia

Lp.	Forma zajęć	Liczba godzin kontaktowych / pracy studenta
1	Wykład	10/10
2	Ćwiczenia	/
3	Laboratorium	/
4	Projekt	0/10
5	Seminarium	/
6	Inne	/
	Suma godzin	10/20

24. Suma wszystkich godzin: 30

25. Liczba punktów ECTS: 2

26. Liczba punktów ECTS uzyskanych na zajęciach z bezpośrednim udziałem nauczyciela akademickiego: 1

27. Liczba punktów ECTS uzyskanych na zajęciach o charakterze praktycznym (laboratoria, projekty): 1

26. Uwagi:

Zatwierdzono:

……. ……

(data i podpis prowadzącego) (*data i podpis kierownika studiów doktoranckich)*