KARTA PRZEDMIOTU

Nazwa przedmiotu: ***Kwantowe systemy teleinformatyki (TIAu-TCH>SM1-KST-19)***
Nazwa w języku polskim:
Nazwa w jęz. angielskim: ***Quantum ICT systems***

Dane dotyczące przedmiotu:

Jednostka oferująca przedmiot: Wydział Automatyki, Elektroniki i Informatyki
Przedmiot dla jednostki: Politechnika Śląska

Domyślny typ protokołu dla przedmiotu:

EGZ

Język wykładowy:

polski

Strona WWW:

https://platforma2.polsl.pl/rau3/course/view.php?id=307

Skrócony opis:

Celem przedmiotu jest przedstawienie metod 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 omawiane są protokoły kwantowej dystrybucji klucza, bezpośredniej poufnej komunikacji kwantowej (utajnienie informacji bez szyfrowania) oraz kontrfaktycznej (komunikacja bez przesyłania nośników informacji).

Opis:

Wykład

1. Wprowadzenie: a) geneza mechaniki kwantowej, b) przestrzeń Hilberta,
c) qubity, bazy, bramki kwantowe, d) notacja Diraca, e) układy złożone. f) qudity.
2. Opis układów izolowanych: a) pomiar kwantowy, b) dekompozycja Schmidt'a, c) splątanie stanów,
3. Układy kwantowe oddziałujące z otoczeniem: a) Operator gęstości stanów, b) Układ jednoskładnikowy c) Układy złożone, d) Operacje kwantowe, e) Reprezentacja Kraussa, f) Rozszerzenie Stinespringa
4. Kanały kwantowe: a) Kanoniczne kanały kwantowe, b) Modelowanie szumu.
5. Powtórka z klasycznej teorii Shannona, a) Entropia systemów klasycznych (Shannon), b) Informacja wzajemna, c) Rozróżnialność zmiennych losowych
6. Dyskryminacja stanów: a) Miary podobieństwa stanów kwantowych, b) Pomiar dwuznaczny (niewykluczający), c) Pomiar jednoznaczny (wykluczający),
7. Kwantowa teoria Shannona: a) Informacja klasyczna systemów kwantowych, b) Entropia kwantowa systemów kwantowych (von Neumann), c) Kres Holevo, d) Teoria Shannona a kryptografia
8. Elementy komunikacji kwantowej: a) Zakazy kwantowe / Twierdzenia No-Go, b) Protokoły podstawowe: Dystrybucja splątania, Kodowanie gęste, Teleportacja kwantowa, c) Wprowadzenie do kryptografii kwantowej
9. Kwantowa dystrybucja klucza: a) Teoria Shannona a bezpieczeństwo informacji, b) Protokół BB84, c) Postprocessing informacji przesłanej kwantowo, d) Ataki na BB84, e) Inne protokoły QKD
10. Bezpośrednia poufna komunikacja kwantowa: a) informacje wstępne, b) blokowe przetwarzanie stanów kwantowych, c) protokoły sekwencyjne, d) komunikacja w kanałach nieidealnych.
11. Kontrfaktyczna komunikacja kwantowa: a) Eksperyment Younga, b) Interferometr Macha-Zehndera, c) Sygnalizacja bez przesyłania cząstek, d) Kontrfaktyczne protokoły QKD.
12. Protokoły semi-kwantowe: a) motywacja, b) semi-kwantowy protokół QKD.
13. Kwantowe kody korekcyjne: a) Klasyfikacja błędów, b) powtórka z klasycznej teorii kodowania, c) kwantowy kod powtórzeniowy, d) kody CSS, e) kod Steane.
14. Algorytm Shora: a) Kwantowa transformacja Fouriera, b) Kwantowy algorytm wyznaczania rzędu liczby, c) Algorytm Shora, d) perspektywy realizacji praktycznej.
15. Kwantowy transfer utajniony: a) algorytm klasyczny, b) historia rozwiązań kwantowych, c) algorytmy hybrydowe kwantowo-klasyczne.

Projekt
Szczegółowe zadanie projektowe jest określane osobno dla każdego cyklu. Szczegółowe informacje znajdują się na stronie przedmiotu.
Zadania projektowe obejmują takie zagadnienia jak
1. Symulacje i analizy działania wybranych protokołów kryptograficznych z wykorzystaniem ogólnodostępnych symulatorów,
2. Symulacje wybranych algorytmów kwantowych.
3. Analizy teoretyczne wybranych zagadnień przedstawianych na wykładzie.

Liczba godzin zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów
Wykład: 30h
Projekt: 30h
Zaliczenie wykładu: 2h
Zaliczenie projektu: 4h
Liczba godzin przeznaczonych na pracę własną studenta
Przygotowanie do zaliczenia wykładu: 20h
Przygotowanie projektu: 10h
Przygotowanie prezentacji projektu: 4h
Całkowita liczba godzin: 100
Liczba punktów ECTS: 4
w tym
Liczba punktów ECTS uzyskanych w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów: 2,7

Literatura:

Obowiązkowa:

[1] P. Zawadzki, Mechanika kwantowa dla studentów teleinformatyki, materiał udostępniony na stronie kursu,
[2] M. Sawerwain, J. Wiśniewska: Informatyka kwantowa, PWN, 2021

Uzupełniająca:
[1] S. Aaronson, Quantum computing since Democritus, Cambridge University Press, 2013
[2] M. Wilde, Quantum Information Theory, Cambridge University Press, 2013, https://arxiv.org/abs/1106.1445

Efekty uczenia się:

Wiedza
student zna i rozumie:
notację Diraca oraz istotę reprezentacji obiektów kwantowych jako elementów przestrzeni Hilberta (K2A_W01)
zasady kryptograficznej ochrony warstwy fizycznej sieci teleinformatycznych za pomocą technik kwantowych (K2A_W05)
istotę wykorzystania komputerów kwantowych do jakościowego przyspieszenie niektórych algorytmów oraz zagrożenia jakie to przyspieszenie niesie dla bezpieczeństwa współczesnych sieci teleinformatycznych (K2A_W09)

Umiejętności
Student potrafi:
opisać za pomocą wyrażeń algebraicznych stan układu fizycznego realizującego popularny algorytm obliczeniowy lub protokół komunikacyjny (K2A_U01)
w języku polskim sporządzić raport z komputerowej symulacji ewolucji układu kwantowego (K2A_U04)
potrafi w symulatorze Qiskit (język Python) opisać ewolucję układu kwantowego realizującego proste obliczenie lub protokół kryptograficzny (K2A_U05)

Metody i kryteria oceniania:

Wykład
Egzamin. Praca pisemna omawiające wybrane zagadnienia poruszane na wykładzie oraz rozwiązywanie zadań. Elementem egzaminu jest ustna obrona udzielonych odpowiedzi.
Kryterium zaliczenia: ocena powyżej 50%.

Projekt
Zaliczenie pisemne w formie pracy projektowej
Kryterium zaliczenia: dostarczenie i zaprezentowanie pracy projektowej zgodnej z określonymi wymaganiami zadania projektowego.

Ocena końcowa: 0.75*Egzamin+0.25*Projekt

Sylabus obowiązuje od roku akademickiego 2024/2025, a jego zawartość nie podlega zmianom w trakcie trwania semestru

Punkty przedmiotu w cyklach:

Teleinformatyka, stacjonarne II stopnia magisterskie 3 sem. (TIAu-SM3)

Typ punktów	Liczba	Cykl pocz.	Cykl kon.
Europejski System Transferu Punktów (ECTS)	4	2020/2021-Z	