EITC/QI/QIF

Informatyka kwantowa w kontekście bezpieczeństwa

Szczegółowa zawartość programowa kursu (15 godz.):

- Wprowadzenie do mechaniki kwantowej
    - Formalizm informatyki kwantowej
        - Przestrzeń Hilberta
        - Funkcje falowe i wektory (ortogonalne i nieortogonalne)
        - Baza
        - Operatory unitarne i hermitowskie
        - Rozkład spektralny
        - Notacja Diraca
    - Postulaty
        - Stan kwantowy
        - Ewolucja unitarna i równanie Schrödingera
        - Pomiar kwantowy (rzutowanie von Neumana)
        - Iloczyn tensorowy i splątanie kwantowe
- Kwantowy paradygmat informacji
    - Definicja (stan kwantowy, źródła wiadomości)
    - Jednostka (qubit), sfera Blocha
    - Splątanie qubitów, stany Bella
    - Miara splątania i informacji kwantowej (entropia von Neumanna)
    - Pomiar kwantowy qubitów
- EPR i złamanie zasady realizmu lub lokalności
    - Nierówności Bella
    - Teleportacja kwantowa
- Kwantowa teoria obwodów
    - Bramki kwantowe
        - Bramki jednoqubitowe (Pauliego, Hadamarda, Fazy)
        - Bramki wieloqubitowe (CNOT, Toffola)
    - Zbiór uniwersalny (CNOT i bramki jednoqubitowe)
    - Odwracalność
    - Realizacja algorytmów kwantowych
        - Układ realizujący kwantową transformatę Fouriera – wykładnicze przyspieszenie
        - Układ realizujący teleportację kwantową
- Kwantowe aspekty bezpieczeństwa
    - Algorytm faktoryzacji Shora
    - Twierdzenia no-cloning, no-deleting, no-broadcasting
    - Kwantowa dystrybucja klucza QKD
- Realizacje praktyczne komputera kwantowego
    - Dekoherencja
    - Kryteria DiVincenzo
    - Technologia pułapkowanych jonów
    - Technologia NMR
    - Technologia kropek kwantowych
        - Orbitalne stopnie swobody
        - Spinowe stopnie swobody
    - Topologiczne stopnie swobody