EITC/IS/QCF

Kryptografia kwantowa

Szczegółowa zawartość programowa kursu (15 godz.):

- Klasyczne podejście do bezpiecznego przesyłania informacji
    - Ogólna koncepcja bezpiecznych kanałów informacyjnych
    - Kryptografia z kluczem prywatnym
    - Kryptografia z kluczem publicznym
    - Uwierzytelnianie
    - Kanały z szumem – detekcja i korekcja błędów
    - Słabości kryptografii klasycznej
- Koncepcja absolutnie bezpiecznych kanałów kwantowych
    - Informacja kwantowa
        - Podstawowe idee informacji kwantowej (pojęcie qbitu, twierdzenie No-Cloning)
        - Kwantowe przetwarzanie informacji w praktyce
    - Wykorzystanie mechaniki kwantowej do ochrony informacji klasycznej
- Kwantowa dystrybucja klucza
    - Kwantowa dystrybucja klucza bez splątania
        - Kluczowe własności spolaryzowanych fotonów
        - Protokół BB84
        - Protokół B92
    - Kwantowa dystrybucja klucza ze splątaniem
        - Splątanie kwantowe i twierdzenie Bella
        - Protokół splątaniowy Ekerta
- Bezpieczne kanały informacyjne z wykorzystaniem QKD
    - Potencjalne ataki na schemat kwantowej dystrybucji klucza
    - Kanały kwantowe z szumem
    - Wzmacnianie prywatności
    - Uwierzytelnianie
    - Kompletny schemat bezpiecznej komunikacji
    - Teoretyczna analiza bezpieczeństwa
- Praktyczne realizacje kryptografii kwantowej
    - Praktyczne realizacje kryptografii kwantowej
    - Sieć kwantowa DARPA
        - Struktura sieci
        - Zaimplementowane technologie
        - Warstwa programowa sieci
        - Rozszerzenia protokołu IPSec
    - Projekt SECOQC
    - Rozwiązania komercyjne
- Inne zastosowania i podsumowanie
    - Inne zastosowania mechaniki kwantowej w kryptografii
        - Zobowiązanie bitowe i kwantowy rzut monetą
        - Generatory liczb losowych
    - Nietypowe alternatywne próby uzyskania odpornych na podsłuch kanałów informacyjnych – protokół Kisha
    - Przyszłość kryptografii kwantowej
    - Podsumowanie