UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Kryptografia kwantowa i postkwantowa

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Informatyka kwantowa **Specjalność** - **Jednostka organizacyjna** Wydział Fizyki i Astronomii **Poziom studiów** studia inżynierskie pierwszego stopnia **Forma studiów** studia stacjonarne **Profil studiów** profil ogólnoakademicki	**Cykl dydaktyczny** 2025/26 **Kod zajęć** 04INKS.320.02442.25 **Języki wykładowe** polski **Obligatoryjność** Fakultatywny **Blok zajęciowy** Przedmioty specjalnościowe

Koordynator zajęć	Adam Miranowicz
Prowadzący zajęcia	Adam Miranowicz

Okres	**Forma zajęć / liczba godzin / forma zaliczenia**	**Liczba punktów ECTS**
Semestr 6	• Wykład: 30, Egzamin • Laboratorium: 30, Zaliczenie z oceną	5

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie studentów z algorytmami, metodami, narzędziami, zastosowaniami i ograniczeniami kryptografii kwantowej oraz postkwantowej (quantum secure) w zakresie określonym przez treści programowe.
C2	Uświadominie studentom powiązań między kryptografią klasyczną, kwantową i postkwantową oraz kierunków rozwoju tych rozwiązań.
C3	Rozwijanie u studentów umiejętności rozwiązywania prostych problemów w oparciu o uzyskaną wiedzę, w szczególności umiejętności implementacji prostych algorytmów kwantowych i postkwantowych w wybranym przez studentów języku programowania.
C4	Kształtowanie u studentów umiejętności samodzielnego i ustawicznego kształcenia oraz umiejętności pracy zespołowej.

Wymagania wstępne

znajomość podstaw mechaniki kwantowej oraz algebry dla informatyków kwantowych, znajomość języka angielskiego.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	zna protokoły dystrybucji kluczy kwantowych oraz prawa fizyki, na których są oparte.	INK_K3_W01, INK_K3_W02, INK_K3_W03, INK_K3_W05, INK_K3_W06_inz, INK_K3_W07, INK_K3_W08_inz	Egzamin pisemny
W2	zna algorytmy i kierunki rozwoju kryptografii postkwantowej (quantum secure) oraz założenia obliczeniowe, na których są oparte.	INK_K3_W01, INK_K3_W02, INK_K3_W03, INK_K3_W05, INK_K3_W06_inz, INK_K3_W07	Egzamin pisemny
W3	zna algorytmy kwantowe i klasyczne stosowane w kryptoanalizie kodów klasycznych i rozumie założenia obliczeniowe, na których są oparte	INK_K3_W01, INK_K3_W02, INK_K3_W03, INK_K3_W05, INK_K3_W06_inz, INK_K3_W07, INK_K3_W08_inz	Egzamin pisemny
Umiejętności – Student/ka:			
U1	potrafi przeanalizować i ocenić przydatność kwantowych protokołów kryptograficznych w obecności szumu.	INK_K3_U01_inz, INK_K3_U02, INK_K3_U04_inz, INK_K3_U06_inz, INK_K3_U07_inz, INK_K3_U08	Projekt

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
U2	potrafi przeanalizować i ocenić przydatność kwantowych algorytmów kryptoanalitycznych w odniesieniu do ograniczeń sprzętowych.	INK_K3_U01_inz, INK_K3_U02, INK_K3_U04_inz, INK_K3_U06_inz, INK_K3_U07_inz, INK_K3_U08	Projekt
U3	potrafi modelować lub implementować protokoły kryptograficzne kwantowe i postkwantowe (quantum-secure)	INK_K3_U01_inz, INK_K3_U02, INK_K3_U04_inz, INK_K3_U05_inz, INK_K3_U06_inz, INK_K3_U07_inz, INK_K3_U08	Projekt
Kompetencji społecznych – Student/ka:			
K1	jest gotów/gotowa wytłumaczyć potrzebę rozwoju technik kryptografii kwantowej i postkwantowej w kontekście rozwoju informatyki kwantowej, publikowania nowych standardów zabezpieczeń cyfrowych oraz zaleceń komisji eksperckich.	INK_K3_K03, INK_K3_K05, INK_K3_K06, INK_K3_K07	Egzamin pisemny

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Wstęp do kryptografii kwantowej: 1. Zastosowanie zakazu klonowania do bezpiecznego przesyłania informacji. 2. Protokół BB84 dystrybucji kluczy kwantowych. 3. Implementacje optyczne protokołu BB84. 4. Protokół Wiesnera pieniędzy kwantowych. 5. Optyczna implementacja pieniędzy kwantowych. 6. Protokoły Shora i Aaronsona pieniędzy kwantowych.	W1, U1	Wykład, Laboratorium
2.	Protokoły dystrybucji kluczy kwantowych: 1. Protokół BB84 - krótkie przypomnienie, 2. Protokół Ekerta E91 z wykorzystaniem stanów splątanych. 3. Protokół Bennetta B92 z wykorzystaniem interferometrów Macha-Zehndera, 4. Protokół Renesa R04. 5. Implementacje protokołów BB84 i E91 z wykorzystaniem satelity kwantowego.	W1, U1	Wykład, Laboratorium
3.	Zalecane długości klucza publicznego. Wyzwania i nagrody RSA. Klasyczne algorytmy faktoryzacji liczb: 1. Sito Eratostenesa, 2. Metoda Monte Carlo, 3. Metoda Fermata, 4. Uogólniona metoda Fermata, 5. Metoda Legendre'a ułamków łańcuchowych, 6. Metoda sita kwadratowego, 7. Porównanie efektywności algorytmów faktoryzacji liczb.	W3	Wykład

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
4.	Podstawowe algorytmy kwantowe w kryptoanalizie kodów klasycznych: 1. Algorytm Grovera wyszukiwania klucza w szyfrach symetrycznych. 2. Kwantowa transformata Fouriera. 3. Algorytm Simona. 4. Algorytm Shora faktoryzacji i jego zastosowanie do łamania kryptosystemów RSA i Rabina. 5. Algorytm Shora liczenia logarytmów dyskretnych i jego zastosowanie do łamania kryptosystemów ElGamala.	W3, U2, U3	Wykład, Laboratorium
5.	Niekonwencjonalne algorytmy kwantowe i DNA w kryptoanalizie kodów klasycznych: 1. Algorytm faktoryzacji metodą sum Gaussa i kociąt Schroedingera. 2. Implementacja tego algorytmu z wykorzystaniem spektroskopii NMR. 3. Kwantowe wyżarzanie (ang. quantum annealing). 4. Implementacja kwantowego wyżarzania z wykorzystaniem nadprzewodzacych kubitów. 5. Algorytm Adlemana oparty na obliczeniach DNA i technikach biochemicznych.	W3, U2, U3	Wykład, Laboratorium
6.	Liczby pierwsze: 1. Liczby pierwsze Mersenne'a. 2. Great Internet Mersenne Prime Search (GIMPS). 3. Test Lucasa-Lehmera liczb Mersenne'a. 4. Spirala Ulama - spirala liczb pierwszych.	W2, W3	Wykład
7.	Hipoteza Riemanna i liczby pierwsze: 1. Funkcja Z Eulera. 2. Funkcja zeta Riemanna. 3. Problemy milenijne (ang. Millennium Problems). 4. Zera funkcji zeta Riemanna i wartości własne hamiltonianowi. 5. PT-symetryczna mechanika kwantowa Bendera. 6. Problem Riemanna i komunikacja nadświetlna.	W2	Wykład
8.	Złożoność obliczeniowa problemów w kryptografii: 1. Deterministyczna maszyna Turinga i problemy typu P (algorytmy wielomianowe). 2. Niedeterministyczna maszyna Turinga i problemy typu NP (niedeterministyczny alg. czasu wielomianowego). 3. Problemy typu NTIME, NP, NEXPTIME, NSPACE, NPSPACE i NEXPSPACE. 4. Problemy NP trudne (ang. NP hard). 5. Problemy zupełne w klasie NP (problemy NP-zupełne, ang. NP complete). 6. Hipoteza P = NP. 7. Uniwersalna maszyna Turinga. 8. Kwantowa maszyna Turinga = uniwersalny komputer kwantowy. 9. Problemy typu BQP (ang. Bounded-error Quantum Polynomial-time).	W2	Wykład
9.	Problemy NP-trudne w kryptografii: 1. Kryptosystem McEliece'a. 2. NTRUEncrypt. 3. Kryptosystem Merkle'a-Hellmana. 4. Złożoność obliczeniowa algorytmów plecakowych. 5. Czy faktoryzacja liczb jest problemem NP-zupełnym?	W2	Wykład
10.	Kryptografia postkwantowa, tj. kryptografia klasyczna odporna na kryptoanalizę kwantową metodą Shora. Podstawowe kierunki rozwoju kryptografii postkwantowej: 1. Szyfry kratowe (ang. lattice-based ciphers) 2. Szyfry wielowartościowe (ang. Multivariate ciphers) 3. Szyfry oparte na funkcjach skrótu (ang. hash-based ciphers) 4. Szyfry oparte na kodach (ang. code-based ciphers, np. kryptosystem McEliece'a) 5. Szyfry na krzywych eliptycznych (np. supersingular elliptic curve isogeny ciphers) 6. Szyfry symetryczne.	W2, U3	Wykład, Laboratorium

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
11.	Standardy kryptografii postkwantowej. Technologie kwantowe I i II generacji. Przyszłość kryptografii kwantowej.	W1, W2, W3, K1	Wykład

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień
Laboratorium	Wykład z prezentacją multimedialną wybranych zagadnień, Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych), Metoda laboratoryjna

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Na końcową ocenę składa się wynik uzyskany podczas egzaminu pisemnego. Warunkiem przystąpienia do egzaminu jest zalicznie laboratorium. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.
Laboratorium	Na końcową ocenę składa się wynik uzyskany z projektu. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.

Literatura

Obowiązkowa

1. N. Gisin, G. Rinordy, W. Tittel, H. Zbinden, „Quantum cryptography", Reviews of Modern Physics, Vol. 74, 2002.
2. A. Kumar i S. Garhwal, „State-of-the-Art Survey of Quantum Cryptography", Archives of Computational Methods in Engineering 28, 3831 (2021).
3. wybrane rozdziały w: M. A. Nielsen i I.L. Chuang „Quantum Computation and Quantum Information", Cambridge University Press, Cambridge, 2000.
4. R. Bavdekar i in., „Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research", arXiv:2202.02826 (2022).
5. M. Kumar, „Post-Quantum Cryptography Algorithms Standardization and Performance Analysis", arXiv:2204.02571 (2022).
6. wybrane rozdziały w: A. J. Menezes, P.C. van Oorschot i S.A. Vanstone, „Kryptografia stosowana" („Handbook of Applied Cryptography"), WNT, Warszawa, 2005.

Dodatkowa

1. B. Schneier, „Kryptografia dla praktyków", Wiley-WNT, Warszawa, 2002.
2. R. Wobst, „Kryptologia", RM, Warszawa 2002.
3. R. Stinson, „Kryptografia", WNT, Warszawa, 2005.
4. S. Singh, ostatni rozdział „Księga szyfrów", Albatros, Warszawa, 2001.
5. G.J. Milburn, „Inżynieria kwantowa", Prószyński i S-ka, Warszawa, 1999.
6. C.H. Bennett, G. Brassard, A.K. Ekert, „Kryptografia kwantowa", Świat Nauki, grudzień 1992.

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	**Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć**
Wykład	30
Laboratorium	30
Czytanie wskazanej literatury	20
Przygotowanie projektu	25
Przygotowanie do egzaminu	25
Łączny nakład pracy studenta	**Liczba godzin** 130
Liczba punktów ECTS	**ECTS** 5

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
INK_K3_K03	Absolwent/ka jest gotów/gotowa do pełnienia roli zawodowej informatyka ze świadomością ciągłych zmian stosowanych paradygmatów i technologii
INK_K3_K05	Absolwent/ka jest gotów/gotowa do przedstawiania w sposób przystępny podstawowych zagadnień z zakresu informatyki i fizyki, porozumiewania się przy użyciu słownictwa technicznego w środowisku zawodowym, również w języku angielskim oraz z wykorzystaniem narzędzi informatycznych i technologii kwantowych
INK_K3_K06	Absolwent/ka jest gotów/gotowa do uczestniczenia w procesach gospodarczych związanych z informatyką i technologiami kwantowymi i świadczeniem wybranych usług informatycznych
INK_K3_K07	Absolwent/ka jest gotów/gotowa do pogłębiania świadomości roli informatyki i technologii kwantowych w kształtowaniu życia społecznego
INK_K3_U01_inz	Absolwent/ka potrafi zastosować wiedzę matematyczną do formułowania, modelowania, analizowania i rozwiązywania prostych zadań związanych z informatyką i fizyką
INK_K3_U02	Absolwent/ka potrafi pozyskiwać wiarygodne informacje z literatury, baz wiedzy, Internetu oraz innych źródeł, integrować je, interpretować oraz wyciągać wnioski i formułować opinie
INK_K3_U04_inz	Absolwent/ka potrafi opracować, przeanalizować, zaprojektować klasyczne i kwantowe algorytmy i systemy informatyczne
INK_K3_U05_inz	Absolwent/ka potrafi pisać, uruchamiać i testować programy w wybranym środowisku programistycznym
INK_K3_U06_inz	Absolwent/ka potrafi ocenić, na podstawowym poziomie, przydatność metod i narzędzi informatycznych oraz wybrać i zastosować właściwą metodę i narzędzia do typowych zadań informatycznych
INK_K3_U07_inz	Absolwent/ka potrafi zastosować wybrane metody wykorzystywane w wiodących kierunkach badań informatyki klasycznej i kwantowej
INK_K3_U08	Absolwent/ka potrafi posługiwać się językiem angielskim zgodnie z wymaganiami określonymi dla poziomu B2 Europejskiego Systemu Opisu Kształcenia Językowego oraz zna język angielski w stopniu umożliwiającym czytanie ze zrozumieniem dokumentacji oprogramowania, podręczników i artykułów informatycznych i fizycznych
INK_K3_W01	Absolwent/ka zna i rozumie w zaawansowanym stopniu pojęcia z działów matematyki niezbędne do modelowania i rozwiązywania problemów w informatyce i fizyce
INK_K3_W02	Absolwent/ka zna i rozumie zaawansowane pojęcia i problemy formujące kanon dyscypliny informatyka i fizyka
INK_K3_W03	Absolwent/ka zna i rozumie klasyczne i kwantowe narzędzia, technologie i urządzenia informatyczne właściwe dla wybranych obszarów zastosowań oraz fizyczne podstawy ich działania
INK_K3_W05	Absolwent/ka zna i rozumie w zaawansowanym stopniu pojęcia związane z klasycznymi i kwantowymi algorytmami i strukturami danych
INK_K3_W06_inz	Absolwent/ka zna i rozumie w zaawansowanym stopniu pojęcia związane z informatyczną i fizyczną architekturą sprzętowo-programową
INK_K3_W07	Absolwent/ka zna i rozumie w zaawansowanym stopniu pojęcia związane z klasycznymi i kwantowymi technologiami sieciowymi, bezpieczeństwem i protokołami kryptograficznymi
INK_K3_W08_inz	Absolwent/ka zna i rozumie w zaawansowanym stopniu pojęcia i problemy związane z wybranymi wiodącymi dziedzinami informatyki