

FIȘA DISCIPLINEI

Tehnici de calcul cuantice cu aplicații în criptografie și IA

Anul universitar 2026-2027

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Babeș-Bolyai
1.2. Facultatea	Facultatea de Matematică și Informatică
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclu de studii	Licență
1.6. Programul de studii / Calificarea	Informatică
1.7. Forma de învățământ	Cu frecvență

2. Date despre disciplină

2.1. Denumirea disciplinei	Tehnici de calcul cuantice cu aplicații în criptografie și IA	Codul disciplinei	MLE5216		
2.2. Titularul activităților de curs	Lector Univ. dr. Mihoc Tudor Dan				
2.3. Titularul activităților de seminar	Lector Univ. dr. Mihoc Tudor Dan				
2.4. Anul de studiu	6	2.5. Semestrul	2	2.6. Tipul de evaluare	Colocviu
2.7. Regimul disciplinei	Opțional	2.8. Tipul disciplinei	DS		

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1. Număr de ore pe săptămână	5	din care: 3.2. curs	2	3.3. seminar/ laborator/ proiect	0/1/2
3.4. Total ore din planul de învățământ	60	din care: 3.5. curs	24	3.6 seminar/laborator	0/12/24
Distribuția fondului de timp pentru studiul individual (SI) și activități de autoinstruire (AI)					ore
Studiul după manual, suport de curs, bibliografie și notițe (AI)					24
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					20
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii și eseuri					16
Tutoriat (consiliere profesională)					2
Examinări					3
Alte activități					0
3.7. Total ore studiu individual (SI) și activități de autoinstruire (AI)				65	
3.8. Total ore pe semestru				125	
3.9. Numărul de credite				5	

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	Cunoștințe de bază de Analiză și Algebră liniară.
4.2. de competențe	Cunoștințe de bază de programare în Python.

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Proiector.
5.2. de desfășurare a seminarului/ laboratorului	Laborator cu calculatoare. Software: Anaconda, Python, Qiskit.

6.1. Competențele dobândite în urma absolvirii programului de studii (se preiau din planul de învățământ)¹

Competențe profesionale	
Codul competenței	Competență
CP1	Creează softuri
CP2	Aliniaza software-ul la arhitecturile de sistem
CP10	Utilizează biblioteci de software
Competențe transversale	
Codul competenței	Competență
CT2	Soluționează probleme
CT3	Gândește analitic

6.2. Rezultatele învățării specifice programului de studii (se preiau din planul de învățământ)²

Rezultatele învățării vizate prin disciplină		
Codul competenței	Cunoștințe și înțelegere (Knowledge and understanding)	Abilități academice specifice (Specific academic skills)
CP2 CP3	Studentul/absolventul numește, oferă exemple, concluzionează, specifică, recunoaște și argumentează critic metodele de proiectare și management al proiectelor informatice complexe, utilizând strategii moderne.	Studentul/absolventul inițiază, pregătește, realizează, propune metode de dezvoltare a proiectelor informatice complexe. Studentul/absolventul realizează rapoarte profesionale specifice.

7. Rezultatele învățării specifice disciplinei

Cunoștințe și înțelegere (Knowledge and understanding)
1. Înțelegerea principiilor fundamentale ale calculului cuantic: qubiți, porți cuantice, circuite cuantice și sfera Bloch.
2. Cunoașterea algoritmilor cuantici de bază, precum Deutsch, Deutsch-Jozsa, Grover, Shor și transformata Fourier cuantică.
3. Înțelegerea aplicațiilor calculului cuantic în criptografie, criptografie post-cuantică și distribuția cheilor cuantice.
4. Cunoașterea conceptelor de bază din quantum machine learning: clusterizare, pattern recognition, clasificare, regresie și rețele neuronale cuantice.
5. Înțelegerea limitărilor practice ale calculului cuantic, inclusiv zgomotul, constrângerile de simulare și diferența dintre circuitele cuantice ideale și hardware-ul cuantic real.
Abilități academice specifice (Specific academic skills)
1. Implementarea circuitelor și algoritmilor cuantici în Python folosind instrumente precum Qiskit.
2. Analiza impactului calculului cuantic asupra criptografiei clasice și utilizarea conceptelor de QKD în scenarii simple.
3. Construirea și testarea unor aplicații elementare de calcul cuantic și quantum machine learning.

¹ Se vor prelua din Planul de învățământ al programului de studii acele competențe profesionale și/sau transversale la dezvoltarea cărora contribuie disciplina pentru care se elaborează fișa disciplinei. Pentru fiecare competență se va prelua întregul enunț, inclusiv codul competenței, cu formularea care apare în planul de învățământ, fără modificări. Dacă nu se preia nici o competență din oricare din cele două categorii, se șterge linia din tabel aferentă acelei categorii.

² Se menționează rezultatele învățării specifice programului de studiu la dezvoltarea cărora contribuie disciplina pentru care se elaborează fișa. Enunțurile, preluate fără modificări din Planul de învățământ în funcție de tipul disciplinei (DF/DS/DC) se trec în dreptul competenței asociate.

4. Evaluarea și interpretarea rezultatelor algoritmilor cuantici implementați și ale modelelor de învățare automată cuantică, utilizând criteriile computaționale și experimentale adecvate.

8. Conținuturi

8.1 Curs	Metode de predare - învățare	Observații ³
1. Introducere - premise matematice.	Expoziție; dialog; prezentare; expunere interactivă; demonstrație practică.	Activități cu suport vizual și exemple aplicative în Python/Qiskit.
2. Noțiuni fundamentale de calcul cuantic: qubiți și sfera Bloch.		
3. Porți cuantice. Circuite cuantice.		
4. Fenomenul de fază kick-back.		
5. Algoritmi de căutare cuantică.		
6. Algoritmul lui Shor.		
7. Criptografie cuantică și criptografie post-cuantică. Atacuri prin calcul cuantic asupra RSA.		
8. Distribuția cheilor cuantice (QKD). Zgomot în QKD și eavesdropper.		
9. Clusterizare în calculul cuantic.		
10. Quantum Pattern Recognition.		
11. Clasificarea cuantică.		
12. Regresia cuantică.		
Bibliografie		
<p>1. Nielsen, Michael A., and Isaac Chuang. Quantum computation and quantum information, 2002.</p> <p>2. Gisin, Nicolas, et al. Quantum cryptography. Reviews of Modern Physics 74.1 (2002): 145.</p> <p>3. Yan, Song Yuan. Cryptanalytic attacks on RSA, 2007.</p> <p>4. Bruß, Dagmar, and Norbert Lütkenhaus. Quantum key distribution: from principles to practicalities. Applicable Algebra in Engineering, Communication and Computing 10.4 (2000): 383-399.</p> <p>5. Shor, Peter W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review 41.2 (1999): 303-332.</p> <p>6. P. Wittek, Quantum Machine Learning: What Quantum Computing Means to Data Mining, Academic Press, Elsevier, 2014.</p> <p>7. S. D. Sarma, D. Dong-Ling, and D. Lu-Ming, Machine learning meets quantum physics, arXiv:1903.03516, 2019.</p>		
8.2 Seminar / laborator	Metode de predare - învățare	Observații
1. Generatoare cuantice de numere aleatoare.	Exemplu; implementarea algoritmilor; exerciții practice; proiecte individuale.	Lucrări practice în Python, Qiskit sau Pennylane și teme de laborator.
2. Transformată Fourier cuantică.		
3. Algoritmul lui Deutsch. Algoritmul lui Deutsch-Jozsa.		
4. Algoritmul de căutare al lui Grover.		
5. Algoritmul cuantic de factorizare.		
6. Algoritmul cuantic pentru logaritmi discreți.		

³ De exemplu aspecte organizatorice, recomandări pentru studenți, aspecte specifice legate de curs/seminar cum ar fi invitarea unor practicieni în domeniu etc.



















7. Rețele neuronale cuantice.		
-------------------------------	--	--

1. Nielsen, Michael A., and Isaac Chuang. Quantum computation and quantum information, 2002.
2. Gisin, Nicolas, et al. Quantum cryptography. Reviews of Modern Physics 74.1 (2002): 145.
3. Yan, Song Yuan. Cryptanalytic attacks on RSA, 2007.
4. Bruß, Dagmar, and Norbert Lütkenhaus. Quantum key distribution: from principles to practicalities. Applicable Algebra in Engineering, Communication and Computing 10.4 (2000): 383-399.
5. Shor, Peter W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review 41.2 (1999): 303-332.
6. P. Wittek, Quantum Machine Learning: What Quantum Computing Means to Data Mining, Academic Press, Elsevier, 2014.
7. S. D. Sarma, D. Dong-Ling, and D. Lu-Ming, Machine learning meets quantum physics, arXiv:1903.03516, 2019.

9. Evaluare

Tip activitate	9.1 Criterii de evaluare	9.2 Metode de evaluare	9.3 Pondere din nota finală
9.4 Curs	Studentii trebuie să fie capabili să exemplifice și să utilizeze concepte de bază și avansate ale calculului cuantic.	Colocviu	50%
9.5 Seminar/laborator	Studentii trebuie să fie capabili să implementeze algoritmi descriși în curs și discutați în cadrul demonstrațiilor din laboratoare.	Evaluarea temelor de laborator	50%
9.6 Standard minim de promovare			
Cel puțin nota 5 (pe o scală de la 1 la 10) pentru ambele tipuri de evaluare.			

10. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)

	Eticheta generală pentru Dezvoltare durabilă							
								
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
								Nu se aplică nici o etichetă
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Data completării:
20.05.2025

Semnătura titularului de curs
Lector Univ. dr. Mihoc Tudor Dan

Semnătura titularului de seminar
Lector Univ. dr. Mihoc Tudor Dan

Data avizării în departament:

...

Semnătura directorului de departament

Conf.dr. Adrian STERCA