



STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
Kvantinė informacija ir kriptografija	

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantis: doc. dr. Mindaugas Mačernis	Fizikos fakultetas

Studijų pakopa	Dalyko (modulio) tipas
Antra	Pasirenkamas

Igyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Auditorinė	2 semestras	Lietuvių, anglų

Reikalavimai studijuojančiajam	
Išankstiniai reikalavimai: Studentas turi būti išklaušęs kvantinės mechanikos ir struktūrinio programavimo pagrindus, lygiagrečiųjų skaičiavimų žinias.	Gretutiniai reikalavimai (jei yra): nėra

Dalyko (modulio) apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	140	64	76

Dalyko (modulio) tikslas: studijų programos ugdomos kompetencijos		
Suvokti pagrindinius kvantinio kompiuterio veikimo ir su juo skaičiavimo principus. Suprasti kvantinę informaciją ir kriptografiją. Gebėti atlikti kvantinės informacijos eksperimentus su kvantiniu kompiuteriu ar jo simulatoriumi.		
Dalyko (modulio) studijų siekiniai	Studijų metodai	Vertinimo metodai
Gebės paaiškinti kvantinio kompiuterio ir kvantinės informacijos principus.	Paskaitos, seminarai, savarankiškas darbas.	Savarankiškas darbas, egzaminas.
Gebės projektuoti ir programuoti nesudėtingus kvantinio kompiuterio programų projektus	Paskaitos, seminarai, savarankiškas darbas.	Savarankiškas darbas, egzaminas.
Studentas gebės pasirinkti optimaliausius kvantinės informacijos perdavimo metodikas.	Paskaitos, seminarai, savarankiškas darbas.	Savarankiškas darbas, egzaminas.

Temos	Kontaktinio darbo valandos							Savarankiškų studijų laikas ir užduotys	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai darbai	Praktika	Visas kontaktinis darbas	Savarankiškas darbas	Užduotys
1. Kvantiniai skaičiavimai Skaičiavimo modeliai: Tiuringo (Turing) mašina, teorinė kompiuterinė algebra. Kompiuterinių taikymų analizė: kompiuterinis kompleksiskumas, loginiai sprendimų uždaviniai, sudėtingos perteklinės klasės ir pertekliniai skaičiavimai. Kvantinė	4		8	8			12	11	Literatūra, užduotys.

mechanika: Šmidto (Schmidt) dekompozija, EPR (Einstein-Podolsky-Rosen) paradoksas. Belo (Bell) nelygybė. Kvantinė teorinė kompiuterinė algebra. Kvantiniai algoritmai. Kubitas. Kubito operacija. Universalūs kvantiniai elementai. Kvantinis kompiuterinės algebros modelis. Kvantinių sistemų simuliacija. Kvantinė Furje transformacija. Fazės įvertinimas. Kvantinės Furje transformacijos algoritmai. Kvantinės paieškos algoritmai. Kvantinė paieška kaip kvantinė simuliacija. Kvantinė paieška nestruktūrizuotai duomenų bazei. Juodos dėžės algoritmų ribos.									
2. Informacijos teorija ir duomenų glaudinimo samprata. Duomenų kodavimas. Informacija ir entropija. Nuostolingas ir nenuostolingas glaudinimas. Statinis ir dinaminis kodavimas. Glaudintų duomenų perdavimas.	4		2				10	10	Literatūra, užduotys.
3. Kvantinė informacija. Kvantinis triukšmas ir kvantinės operacijos. Kvantinis triukšmo ir kvantinių operacijų pavyzdžiai. Kvantinių operacijų formalizmo ribos. Atstumas ir kvantinė informacija. Klaidoms palankus kvantinis skaičiavimas. Kvantinis informacijos perdavimas per triukšmingus kvantinius kanalus. Kvantinis supainiojimas (entanglement). Kvantinės teleportacijos kodas. Entropija ir informacija.	8		2	6			14	11	Literatūra, užduotys.
4. Kriptografija. Užkodavimas ir saugumas. Atakos. Simetriniai kodavimo raktai. Viešo rakto kriptografija. Kriptografijos protokolai. Vienakryptės funkcijos. Atakos ir saugumo lygiai.	4			2			10	6	Literatūra, užduotys.
5. Kvantinė kriptografija Kriptosistemų kvantinės atakos. DNA biologinis užkodavimas. Kvantinių raktų perdavimas ir saugumas.	6		4				12	14	Literatūra, užduotys.
6. Kvantinių ryšių beklaidis (Zero-Error) kanalas. Kvantinės būsenos ir kanalai. Koreliacijos. Būsenų suliejimas. Kvantinė informacija per trriukšmingus kanalus. Supainiojimas.	6						6	4	Literatūra, užduotys.
Iš viso	32		16	16			64	76	

Vertinimo strategija	Svoris proc.	Atsiskaitymo laikas	Vertinimo kriterijai
Savarankiškas darbas	70	1–16 semestro savaitės	Pratybų metu atliekamos pavyzdinės užduotys, išsiaiškinamos jų programinio įgyvendinimo galimybės. Studentai privalo atlikti ir atsiskaityti 80% visų pateiktų atsiskaityti užduočių. Rašomas vienas kontrolinis darbas (K1) ir vienas rašto darbas (K2).
Egzaminas	30	16-a semestro savaitė	Egzaminas: atsakymai į klausimus raštu ir žodžiu. Egzamino metu pateikiami 2 klausimai (K3). Gautinis įvertinimas: $P = 0,35 K1 + 0,35 K2 + 0,3 K3$.

Autorius	Leidimo metai	Pavadinimas	Periodinio leidinio Nr. ar leidinio tomas	Leidimo vieta ir leidykla ar internetinė nuoroda
Privaloma literatūra				
Radhika Vathsan	2015	Introduction to Quantum Physics and Information Processing		CRC Press
Michael A. Nielsen, Issac L. Chuang	2011	Quantum Computation and Quantum Information		Cambridge University Press
Ved Prakash Gupta, Prabha Mandayam, V.S. Sunder	2015	The Functional Analysis of Quantum Information Theory: A Collection of Notes Based on Lectures		Springer
Stephen Barnett	2009	Quantum Information		Oxford University Press
Papildoma literatūra				
Hans Delfs, Helmut Knebl.	2015	Introduction to Cryptography: Principles and Applications (Information Security and Cryptography)		Springer
Song Y. Yan	2013	Quantum Attacks on Public-Key Cryptosystems		Springer
Jack D. Hidary	2019	Quantum Computing: An Applied Approach		Springer
Christine Corbett Moran	2019	Mastering Quantum Computing with IBM QX : Explore the World of Quantum Computing Using the Quantum Composer and Qiskit		Packt Publishing



COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
Quantum Information and Cryptography	

Lecturer(s)	Department(s) where the course unit (module) is delivered
Coordinator: Assoc. Prof. Dr. Mindaugas Mačernis	Faculty of Physics

Study cycle	Type of the course unit (module)
Second	Optional

Mode of delivery	Period when the course unit (module) is delivered	Language(s) of instruction
Face-to-face	2 nd semester	Lithuanian, English

Requirements for students	
Prerequisites: Quantum mechanics; Structural programming; Parallel computing	Additional requirements (if any): None

Course (module) volume in credits	Total student's workload	Contact hours	Self-study hours
5	140	64	76

Purpose of the course unit (module): programme competences to be developed		
Students will learn information theory of quantum computation and quantum information. He will be able execute quantum information experiments with quantum computer or its simulator.		
Learning outcomes of the course unit (module)	Teaching and learning methods	Assessment methods
The student could understand quantum computing and quantum informations.	Lectures, seminars, works, independent work.	Independent works, exam.
The student could choose optimal quantum code model for various tasks.	Lectures, seminars, works, independent work.	Independent works, exam.
The student could make quantum information programs with quantum computer.	Lectures, seminars, works, independent work.	Independent works, exam.

Content: breakdown of the topics	Contact hours							Self-study work: time and assignments	
	Lectures	Tutorials	Seminars	Exercises	Laboratory work	Internship/work placement	Contact hours	Self-study hours	Assignments
1. Quantum computation. Models for computation: Turing machines, circuits. The analysis of computational problems: computational complexity, decision problems, a plethora of complexity classes, energy and computation. Quantum mechanics: the Schmidt decomposition and purifications, EPR and the Bell	4		8	8			1 2	11	Literature, seminars, tasks.

inequality. Quantum circuits. Quantum algorithms. Qubit. Single qubit operations. Universal quantum gates. The quantum circuit model of computation. Simulation of quantum systems. The quantum Fourier transform. Phase estimation. Applications of the quantum Fourier transform. Quantum search algorithms. Quantum search as a quantum simulation. Quantum search of an unstructured database. Black box algorithm limits.									
2. Information theory and data compression. Data compression. Information and entropy. Lossy and lossless data compression. Static and dynamic compression.	4		2				10	10	Literature, seminars, tasks.
3. Quantum information. Quantum noise and quantum operations. Operator Systems. Examples of quantum noise and quantum operations. Limitations of the quantum operations formalism. Distance measures for quantum information. Fault-tolerant quantum computation. Code for quantum teleportation. Entropy and information.	8		2	6			14	11	Literature, seminars, tasks.
4. Cryptography. Encryption and Secrecy. Attacks. Symmetric-Key Encryption. Public Key Cryptography. Cryptographic Protocols. One-Way Functions. Attacks and Levels of Security.	4			2			10	6	Literature, seminars, tasks.
5. Quantum cryptosystems. Quantum Attacks on Cryptosystems. Quantum Resistant Cryptosystems. DNA Biological cryptography. Quantum key distribution and security.	6		4				12	14	Literature, seminars, tasks.
6. Zero-Error Communication Via Quantum Channels. Norms on Quantum States and Channels. Destroying Correlations. State Merging. Quantum information over noisy quantum channels. Entanglement.	6						6	4	Literature, seminars, tasks.
Total	32		16	16			64	76	

Assessment strategy	Weight, %	Deadline	Assessment criteria
Laboratory work	70	1-16 weeks of semester	Students must complete and present reports for tasks. Work is completed during self-study hours. The 80% of the tasks must be presented until the end of semester. There one test (K1) and prepared report (K2) .
Exam	30	16th week of semester	Final exam (two questions from theory). Exam mode – written answer (K3). Final rating $P = 0,35 K1 + 0,35 K2 + 0.3 K3$.

Author	Year of publication	Title	Issue of a periodical or volume of a publication	Publishing place and house or web link
Compulsory reading				
Radhika Vathsan	2015	Introduction to Quantum Physics and Information Processing		CRC Press

Michael A. Nielsen, Issac L. Chuang	2011	Quantum Computation and Quantum Information		Cambridge University Press
Ved Prakash Gupta, Prabha Mandayam, V.S. Sunder	2015	The Functional Analysis of Quantum Information Theory: A Collection of Notes Based on Lectures		Springer
Stephen Barnett	2009	Quantum Information		Oxford University Press
Optional reading				
Hans Delfs, Helmut Knebl.	2015	Introduction to Cryptography: Principles and Applications (Information Security and Cryptography)		Springer
Song Y. Yan	2013	Quantum Attacks on Public-Key Cryptosystems		Springer
Jack D. Hidary	2019	Quantum Computing: An Applied Approach		Springer
Christine Corbett Moran	2019	Mastering Quantum Computing with IBM QX : Explore the World of Quantum Computing Using the Quantum Composer and Qiskit		Packt Publishing