RTU studiju kurss "Kvantu kriptogrāfija un protokoli"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	DE1003
Nosaukums	Kvantu kriptogrāfija un protokoli
Studiju kursa statuss programmā	Obligātais/Ierobežotās izvēles; Brīvās izvēles
Atbildīgais mācībspēks	Andis Supe - Doktors, Vadošais pētnieks
Mācībspēks	Jurģis Poriņš - Doktors, Profesors Rihards Mūrnieks - Doktors, Docents Ints Murāns - Pētnieks
Apjoms daļās un kredītpunktos	1 daļa, 3.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV, EN
Anotācija	Studiju kursā tiek apskatīti dažādi kvantu atslēgu izplatīšanas (QKD) protokoli un metodes, informācijas pēcapstrāde izmantojot kļūdu labojošos kodus, QKD protokolu drošības analīze un praktiskās ieviešanas aspekti. Kvantu kriptogrāfija jeb kvantu atslēgas pārraide risina vienu no būtiskām sakaru sistēmu problēmām, kā nodrošināt lietotāju autentificēšanu un drošu datu pārraidi. Principiem, kas izriet no kvantu teorijas, ir potenciāls pielietojums slepenu šifrēšanas atslēgu izveidošanai starp diviem lietotājiem. Tādējādi kvantu sakaru sistēmu drošība ir balstīta uz fizikas likumiem. Šobrīd notiek strauja sistēmu drošības pārbaudes paņēmienu un inovatīvu kvantu sakaru protokolu attīstība un arvien plašāk ir sastopami šādu tehnoloģiju prototipu praktiskās pielietošanas piemēri. Studiju kurss ietver tādas tēmas kā kvantu informācijas apstrāde, kvantu skaitļošana, kvantu sakari un kvantu kriptogrāfija.
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Studiju kursa mērķis ir sniegt teorētiskas un praktiskas zināšanas par kvantu informācijas pārraidi, kvantu atslēgu ģenerēšanu, kvantu kriptogrāfiju, QKD protokoliem un informācijas pēcapstrādi, kā arī izprast kvantu sakaru sistēmu galvenos elementus un to praktiskās pielietošanas ierobežojumus. Studiju kursa uzdevumi: - iemācīt ar kvantu sakariem saistītos algoritmus un matemātiskās kodēšanas metodes; - sniegt zināšanas par kodu izvēli un to novērtēšanu; - sniegt pamatzināšanas par kvantu kriptogrāfiju un kvantu protokoliem, kā piemēram, BB84, BB92, u.c.; - iemācīt izstrādāt un pielietot vienkāršus kvantu algoritmus kvantu signālu apstrādei; - iemācīt kodēšanas un kvantu kriptogrāfijas sistēmu simulācijas pamatus; - attīstīt prasmes izvērtēt esošo sakaru sistēmu infrastruktūras piemērotību kvantu sakaru sistēmu tālākai ieviešanai.
Patstāvīgais darbs, tā organizācija un uzdevumi	Studiju kursa ietvaros studentu patstāvīgais darbs tiks organizēts šādi: - jāatrisina mācībspēka definētie uzdevumi, parādot lekcijās iegūto zināšanu izmantošanu; - jāapkopo un jāizanalizē jaunākie publicētie pētījumu rezultāti par kvantu kriptogrāfiju un protokoliem; - pielietojot iegūtās teorētiskās zināšanas jāizveido kvantu kriptogrāfijas un protokolu simulācijas matemātisko modeli.
Literatūra	Obligātā/Obligatory: 1. R. Wolf. Quantum Key Distribution, Springer Nature Switzerland AG, 2021. 2. F. Gracelli. Quantum Cryptography (From Key Distribution to Conference Key Agreement), Springer Cham, 2021. 3. H. Knospe. A Course in Cryptography (Pure and Applied Undergraduate Texts), AMS, 2019. Papildu/Additional: 1. Y. Billig. Quantum Computing for High School Students, Qubit Publishing, 2018. 2. W. Frazer. Quantum Information Theory: The Future of Quantum Cryptography and Computing, CreateSpace Independent Publishing Platform, 2017. 3. M. Nielsen and I. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2000 (1st ed.), 2010 (2nd ed.) 4. F. J. MacWilliams, N. J. A. Sloane. The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977. 5. T. K. Moon. Error Correction Coding, 1st Edition, Wiley-Interscience, 2006.
Nepieciešamās priekšzināšanas	Fizika, informācijas optiskās apstrādes fizika, kvantu sakaru sistēmu pamati, programmēšana un augstākā matemātika.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
Ievads kvantu informācijas teorijā, kvantu pārraide un matemātiskie rīki.	4	4	0	0
Kvantu sistēmu apraksts un to īpašības: kubiti, kvantu kanāls, kvantu mērījumi.	4	4	0	0
QKD protokoli: sagatavošanas un mērīšanas (prepare-and-measure) protokoli un uz kvantu saistīto stāvokli balstīti (entanglement-based) protokoli.	8	8	0	0
Ar QKD protokoliem saistīta informācijas pēcapstrāde: kļūdu labojošie kodi, parametru novērtējums, datu pārraides privātuma uzlabošana.	8	8	0	0

QKD protokolu drošības analīze: uzbrukumu klasifikācija, kodēšanas atslēgas pārraides ātrums, galīga garuma (finite-key) atslēgas analīze.	4	4	0	0
Praktiski sastopamās QKD sistēmas: no mērierīces neatkarīgs QKD (measurement device-Independent QKD) un nepārtraukta mainīgā (continuous-variable) QKD.	8	8	0	0
QKD ieviešanas praktiskie aspekti: kvantu avoti un uztvērēji, signāla vājinājums.	4	4	0	0
Kopā:	40	40	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Spēj orientēties kvantu kriptogrāfijas metodēs un risināt ar tām saistītus uzdevumus.	Kontroldarbs. Jautājumi eksāmenā.
Pārzina biežāk sastopamos QKD protokolus un izprot QKD protokolu drošības analīzi.	Kontroldarbs. Jautājumi eksāmenā.
Spēj patstāvīgi analizēt jaunākās zinātniskās publikācijas par kvantu kriptogrāfijas protokoliem.	Praktiskais darbs.
Pielietojot iegūtās teorētiskās zināšanas, spēj izveidot kvantu kriptogrāfijas datorsimulācijas modeli ietverot arī QKD protokolu pēcapstrādes paņēmienus.	Praktiskais darbs. Jautājumi eksāmenā.
Saprot QKD protokolu praktiskās ieviešanas aspektus un ar tiem saistītos tehniskos izaicinājumus.	Kontroldarbs. Jautājumi eksāmenā.

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Kontroldarbi	40
Praktiskie darbi	30
Eksāmens	30
Kopā:	100

Studiju kursa plānojums

Daļa	KP	Stundas			Pārbaudījumi			Brīvās izvēles pārbaudījumi		
		Lekcijas	Prakt d.	Laborat	Ieskaite	Eksām.	Darbs	Ieskaite	Eksām.	Darbs
1.	3.0	16.0	16.0	0.0		*			*	