Vilniaus universitetas

Ataskaitinės konferencijos pranešimas

Kvantinėms grėsmėms atsparios skaitmeninės ekosistemos modeliavimas

Vadovė: Doc. dr. Agnė Brilingaitė

Doktorantė: Simona Zavackė
Doktorantūros pradžios/pabaigos metai: 2025-2029
Studijų metai: 2025/2026 pirmasis pusmetis

Studijų planas ir jo vykdymo suvestinė

Vilniaus universitetas

Studijų metai	Egzaminai	
	Planas	Įvykdyta
I (2025/2026)	**2**	1
II (2026/2027)	2	
III (2027/2028)		
IV (2028/2029)		
Iš viso:	4	1

Egzaminai 2025/2026 (I pusmetis)		
Planas	**Įvykdyta**	**Būklė**
Fundamentalieji informatikos ir informatikos inžinerijos metodai (2026 m. I ketv.)	Fundamentalieji informatikos ir informatikos inžinerijos metodai (2026 m. sausio 22 d.)	Išlaikytas
Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika (2026 m. II ketv.)	Vyksta	Vyksta, egzaminas numatomas 2026 m. birželį.

Studijų planas ir jo vykdymo suvestinė

Vilniaus universitetas

BENDRIEJI GEBĖJIMAI

	Dalyko pavadinimas	Kreditai (ECTS)	Atsiskaitymo data
1.	Mokslinės informacijos paieška: duomenų bazės ir DI įrankiai	0.2	2025 m. IV ketvirtis
2.	Duomenų vizualizavimas naudojant R	1.25	2025 m. IV ketvirtis
3.	Latex	1.25	2026 m. I ketvirtis
4.	Informacijos saugojimas ir citavimas naudojantis programa Zotero	0.15	2025 m. IV ketvirtis
5.	The FAIR data principles	0.55	2025 m. IV ketvirtis

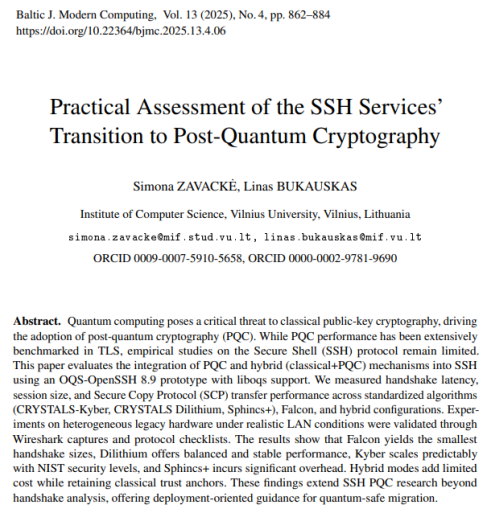
Bendrieji gebėjimai 2025/026 (I pusmetis)		
Kreditai	**Dalyko pavadinimas**	**Būklė**
0,55 ECTS	The FAIR Data Principles	Įvykdyta 2025-11-03
0,15 ECTS	Informacijos saugojimas ir citavimas naudojantis programa Zotero	Įvykdyta 2025-11-25
0,2 ECTS	Mokslinės informacijos paieška: duomenų bazėse ir DI įrankiai	Įvykdyta 2025-11-07
1,25 ECTS	Duomenų vizualizavimas naudojantis R	Įvykdyta 2025-11-20, 27 ir 2025-12-04
1,25 ECTS	LaTex	Mokymai nukelti į 2026-03-26/27

Studijų planas ir jo vykdymo suvestinė

Vilniaus universitetas

Studijų metai	Dalyvavimas konferencijose				Publikacijos					
	Tarptautinėse		Nacionalinėse		Su citav. rodikliu			Be citav. rodiklio		
	Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta	Būklė	Planas	Įvykdyta	Būklė
I (2025/2026)					1	1	publikuota			
II (2026/2027)										
III (2027/2028)	1				1					
IV (2028/2029)	1				1					
Iš viso:	2				3	1				

Publikacijos 2025/2026 (I pusmetis)			
Planas	**Įvykdyta**	**Būklė**	**Publikacijos tipas**
"Baltic Journal of Modern Computing",	ZAVACKE S., BUKAUSKAS L. "Practical Assessment of the SSH Services' Transition to Post-Quantum Cryptography", Baltic J. Modern Computing, Vol. 13 (2025), No. 4, pp. 862–884, DOI: 10.22364/bjmc.2025.13.4.06 Nuoroda internete: https://www.bjmc.lu.lv/fileadmin/user_upload/lu_portal/projekti/bjmc/Contents/13_4_06_Zavacke.pdf (paskutinį kartą žiūrėta 2026-02-01).	Publikuota	Turi cituojamumo rodiklį WoS Q4 JIF: 0.7, Scimagojr: Q3 SJR:0.24.



Baltic J. Modern Computing, Vol. 13 (2025), No. 4, pp. 862–884
https://doi.org/10.22364/bjmc.2025.13.4.06

Practical Assessment of the SSH Services' Transition to Post-Quantum Cryptography

Simona ZAVACKĖ, Linas BUKAUSKAS

Institute of Computer Science, Vilnius University, Vilnius, Lithuania

simona.zavacke@mif.stud.vu.lt, linas.bukauskas@mif.vu.lt

ORCID 0009-0007-5910-5658, ORCID 0000-0002-9781-9690

Abstract. Quantum computing poses a critical threat to classical public-key cryptography, driving the adoption of post-quantum cryptography (PQC). While PQC performance has been extensively benchmarked in TLS, empirical studies on the Secure Shell (SSH) protocol remain limited. This paper evaluates the integration of PQC and hybrid (classical+PQC) mechanisms into SSH using an OQS-OpenSSH 8.9 prototype with liboqs support. We measured handshake latency, session size, and Secure Copy Protocol (SCP) transfer performance across standardized algorithms (CRYSTALS-Kyber, CRYSTALS Dilithium, Sphincs+), Falcon, and hybrid configurations. Experiments on heterogeneous legacy hardware under realistic LAN conditions were validated through Wireshark captures and protocol checklists. The results show that Falcon yields the smallest handshake sizes, Dilithium offers balanced and stable performance, Kyber scales predictably with NIST security levels, and Sphincs+ incurs significant overhead. Hybrid modes add limited cost while retaining classical trust anchors. These findings extend SSH PQC research beyond handshake analysis, offering deployment-oriented guidance for quantum-safe migration.

Studijų planas ir jo vykdymo suvestinė

Vilniaus universitetas

Dalyvavimas konferencijose 2025/2026 (I pusmetis)		
Planas	**Įvykdyta**	**Konferencijos tipas**
-	-	-

European Conference on PQC Migration

This European conference on the subject of migration to post-quantum cryptography (PQC) is organized by our Dutch-French-German consortium consisting of ANSSI (the French Cybersecurity Agency), BSI (the German Federal Office for Information Security), MinBZK (the Ministry of the Interior & Kingdom Relations of The Netherlands), CWI (National Research Institute for Mathematics and Computer Science in The Netherlands) and TNO (Netherlands Organisation for Applied Scientific Research).

Dalyvavau kaip klausytoja konferencijoje „*European Conference on PQC Migration*“ (2025-12-02/03 Hagoje) siekdama susirinkti aktualią informaciją moksliniam tyrimui.

Visų mokslinių tyrimų ir disertacijos rengimo etapai

Vilniaus universitetas

Dalyko pavadinimas		Atlikimo terminai		Pastabos
1.	**Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje):**	**2025 m. gruodis**	**2026 m. gruodis**	**Padaryta dalis apžvalgos**
1.1.	Skaitmeninės ekosistemos apibrėžimų, sistemų architektūros projektavimo ir aktualių modeliavimo metodų analizė, įskaitant modelių vertinimą.	2025 m. IV ketvirtis	2026 m. II ketvirtis	Padaryta apžvalga
1.2.	Kvantinėms grėsmėms atsparios skaitmeninės ekosistemos modeliavimo mokslinės problemos, egzistuojančio poreikio versle ir valstybės valdyme bei praktinio pritaikymo atvejo identifikavimas.	2026 m. I ketvirtis	2026 m. IV ketvirtis	Padaryta dalis apžvalgos
1.3.	Disertacijos tyrimo objekto detalizavimas ir tyrimo tikslo suformavimas.	2026 m. I ketvirtis	2026 m. IV ketvirtis	Vykdomas idėjos detalizavimas
2.	**Mokslinio tyrimo vykdymas:**			
2.1.	**Tyrimo metodikos sudarymas:**	**2026 m. spalis**	**2027 m. liepa**	
2.1.1.	Tyrimo metodikos iškeltiems uždaviniams spręsti parinkimas.	2026 m. IV ketvirtis	2027 m. I ketvirtis	
2.1.2.	Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką.	2027 m. I ketvirtis	2027 m. II ketvirtis	

Visų mokslinių tyrimų ir disertacijos rengimo etapai

Vilniaus universitetas

Dalyko pavadinimas		Atlikimo terminai		Pastabos
2.2.	**Teorinis tyrimas:**	**2027 m. sausis**	**2027 m. spalis**	
2.2.1.	Kvantinėms grėsmėms atsparios skaitmeninės ekosistemos modelio kūrimas, modelio vertinimo strategijų parinkimas ir teorinis vertinimas.	2027 m. I ketvirtis	2027 m. IV ketvirtis	
2.2.2.	Ekosistemos modelio integravimas į kibernetinių grėsmių valdymo procesus, atsižvelgiant į veikėjus, politikos jurisdikcijos zonas, procesų sąveikas.	2027 m. II ketvirtis	2027 m. IV ketvirtis	
2.3.	**Empirinis tyrimas:**	**2027 m. spalis**	**2028 m. liepa**	
2.3.1.	Eksperimentinės aplinkos įgyvendinimas pagal pasirinktus modelio taikymo scenarijus.	2027 m. IV ketvirtis	2028 m. II ketvirtis	
2.3.2.	Scenarijų vykdymas ir eksperimentinių duomenų rinkimas sukurto modelio vertinimui.	2027 m. IV ketvirtis	2028 m. III ketvirtis	
2.4.	**Gautų duomenų analizė, apibendrinimas, išvadų parengimas:**	**2028 m. balandis**	**2028 m. gruodis**	
2.4.1.	Gautų rezultatų analizė, lyginant su susijusiais darbais, ir išvadų formulavimas.	2028 m. II ketvirtis	2028 m. IV ketvirtis	
2.4.2.	Atliktų mokslinių tyrimų apribojimų ir reikšmės identifikavimas.	2028 m. III ketvirtis	2028 m. IV ketvirtis	
3.	**Atskirų daktaro disertacijos dalių (tyrimo metodikos, rezultatų, ginamų teiginių, išvadų, ir kt.) parengimas:**	**2028 m. gruodis**	**2029 m. gegužė**	
4.	**Daktaro disertacijos parengimas ir svarstymas padalinyje**	**2029 m. sausis**	**2029 m. birželis**	
5.	**Daktaro disertacijos gynimas**	**2029 m. liepa**	**2029 m. rugsėjis**	

Tyrimo objektas – perėjimo prie postkvantinės kriptografijos (PQC) vyksmas skaitmeninėse ekosistemose.

Tikslas – sukurti skaitmeninės ekosistemos modelį, skirtą kibernetinėje erdvėje kylančių kvantinių grėsmių mažinimui.

Teorinės analizės ir problemos apibrėžimo uždaviniai:

- ✓ Išanalizuoti skaitmeninės ekosistemos apibrėžimus, sistemų architektūros projektavimo principus ir aktualius modeliavimo metodus mokslinėje literatūroje, įvertinant jų tinkamumą kvantinių grėsmių kontekste.
- ✓ Įvertinti esamus skaitmeninių ekosistemų modelius ir jų vertinimo metodus, nustatant jų apribojimus pereinant prie postkvantinės kriptografijos.
- ✓ Identifikuoti kvantinėms grėsmėms atsparios skaitmeninės ekosistemos modeliavimo mokslinę problemą, pagrindžiant jos aktualumą verslo ir valstybės valdymo kontekstuose bei nustatant praktinio taikymo poreikį.
- ✓ Detalizuoti disertacijos tyrimo objektą ir suformuoti tyrimo tikslą, atsižvelgiant į nustatytas teorines spragas ir praktinius poreikius.

Rezultatai:

Išanalizuoti skaitmeninės ekosistemos apibrėžimai ir aktualūs jos modeliavimo metodai mokslinėje literatūroje (49 šaltiniai).

Išvados:

1. Nėra vieno aiškaus skaitmeninės ekosistemos apibrėžimo, galima juos skirstyti pagal:
   - ✓ techno-centristinį požiūrį (vien technologijos ir jų sąveika apibūdina skaitmeninę ekosistemą)
   - ✓ socio-techninį požiūrį (socialiniais dariniai ir jų procesai veikia technologijų pagrindu).
2. Efektyviausiu skaitmeninių ekosistemų modeliavimo metodu galima laikyti skirtingų metodų taikymą konkrečiam tikslui pasiekti. Integruoti modeliavimo metodai padeda panaikinti atotrūkį tarp kokybinio aprašymo ir kiekybinio prognozavimo:
   - ✓ Konceptualusis ir vizualinis modeliavimas pateikia ekosistemos žemėlapį, nustato „kas“ ir „ką“.
   - ✓ Taikant tinklo analizės metodą ir grafų duomenų bazes, galima analizuoti ir apskaičiuoti rodiklius kaip centralumas ar tinklo tankis, atskleisti paslėptas priklausomybes ir sisteminius pažeidžiamumus. Šie struktūriniai žemėlapiai suteikia empirinį „skeletą“, ant kurio kuriamos simuliacijos.
   - ✓ Ekosistemos modeliavimas kaip simuliacija yra ta vieta, kur ekosistema „atgyja“ ir gali išbandyti „kas būtų, jeigu“ scenarijus.
3. Pasižiūrėjimas „iš paukščio skrydžio“ į skaitmeninės ekosistemos modeliavimo diskursą mokslinėje literatūroje duoda pagrindą galimoms tyrimo perspektyvoms, siekiant įvertinti skaitmeninės ekosistemos modeliavimo pritaikomumą kvantinių grėsmių kontekste.

Vilniaus universitetas

Kito pusmečio darbo planas:

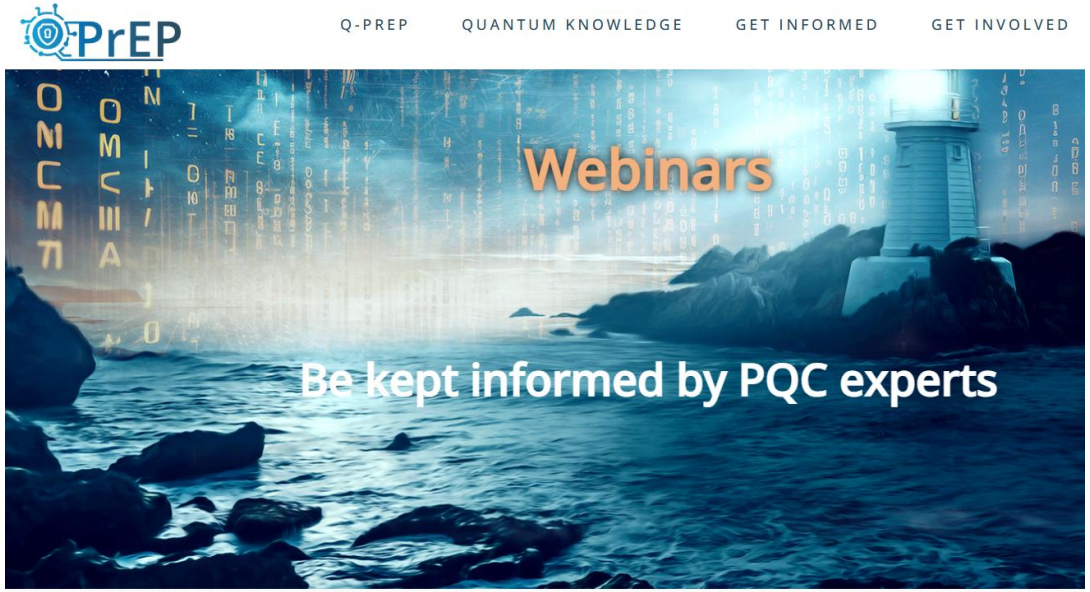
Tęsti tyrimus:

1. Parinkti metodą kvantinėms grėsmėms atsparios skaitmeninės ekosistemos modeliavimui.
2. Detalizuoti kvantinėms grėsmėms atsparios skaitmeninės ekosistemos modeliavimo mokslinę problemą, pagrindžiant jos aktualumą verslo ir valstybės valdymo kontekstuose bei nustatant praktinio taikymo poreikį.
3. Detalizuoti disertacijos tyrimo objektą ir suformuoti tyrimo tikslą, atsižvelgiant į nustatytas teorines spragas ir praktinius poreikius.

Išlaikyti dalyką: „Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika (2026 m. II ketv.)“

Atlikti stažuotę: RTU (Riga Technical University), trukmė 3 sav., numatoma 2026 m. rugsėjo mėn.

Balandžio 10 d. pristatyti publikuoto tyrimo rezultatus tarptautiniame internetiniame seminare „QPrEP webinar“



Webinars

April 10, 2026, 1:00 p.m. (CET)	Practical Assessment of the SSH Services' Transition to Post-Quantum Cryptography	Simona Zavackė (Vilnius University)

Vilniaus universitetas

KONTAKTAI

doktorantė

Simona Zavackė

MIF Informatikos instituto Kompiuterinio ir duomenų modeliavimo katedra

simona.zavacke@mif.stud.vu.lt