



**Vilniaus
universitetas**

Kvantinėms grėsmėms atsparios skaitmeninės ekosistemos modeliavimas

Ataskaitinės konferencijos pranešimas

Vadovė: Prof. dr. Agnė Brilingaitė

Doktorantė: Simona Zavackė

Doktorantūros pradžios/pabaigos metai: 2025 – 2029

Ataskaitinis studijų pusmetis (I metų 2025/2026 – II pusmetis)

Studijų planas ir jo vykdymo suvestinė

**Vilniaus
universitetas**

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

Egzaminai Ataskaitinis studijų pusmetis (I metų 2025/2026 – II pusmetis)		
Planas	Įvykdyta	Būklė
Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika (2026 m. II ketv.)	Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika (2026 m. liepos 3 d.)	Išlaikytas

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	-	1	priimta
II (2026/2027)										
III (2027/2028)	1				1					
IV (2028/2029)	1				1					
Iš viso:	2				3	1				

Publikacijos Ataskaitinis studijų pusmetis (I: 2025/2026 – II pusmetis)			
Planas	Įvykdyta	Būklė	Publikacijos tipas
-	Zavackė S., Brilingaitė A., „Towards Quantum-Resilient Enterprises by Addressing Packet Fragmentation“	Priimta, bus publikuota	Konferencinis straipsnis, peer reviewed straipsnis IEEE formatu, 6 psl.

Dalyvavimas konferencijose		
Planas	Įvykdyta	Konferencijos tipas
-	numatyta 2026-10-08/10*	Tarptautinė konferencija: 2026 IEEE 67th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS'2026)

*VU mokslo prorektorius 2026-09-17 įsakymas Nr. D-1157 dėl išvykų

Studijų planas ir jo vykdymo suvestinė

Stažuotė RTU (Riga Technical University) 09.27–10.10 ir 11.01–11.07
(VU mokslo prorektorius 2026-09-01 įsakymas Nr. D-1025 dėl išvykų)

Tikslas:

Modeliavimo praktikų įsisavinimas ir pritaikymas kvantinėms grėsmėms atsparios skaitmeninės ekosistemos modeliavimui.

Doktorantūros studijų pasiekimai

Publikacijos (tik su citavimo rodikliu)		
	Bibliografinis aprašas	Būklė
1.	Zavackė S., Bukauskas L. "Practical Assessment of the SSH Services' Transition to Post-Quantum Cryptography", Baltic Journal of 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 2026-09-30).	publikuota (publikacija užregistruota eLABa sistemoje https://talpykla.elaba.lt).

Dalyvavimas tarptautinėse konferencijose	
	Aprašas
1.	Zavackė S., Brilingaitė A. „Towards Quantum-Resilient Enterprises by Addressing Packet Fragmentation“, 2026 IEEE 67th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS'2026), 2026-10-08, Riga, Latvija.

Visų mokslinių tyrimų ir disertacijos rengimo etapai

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	Idėjos detalizavimas
1.3.	Disertacijos tyrimo objekto detalizavimas ir tyrimo tikslo suformavimas.	2026 m. I ketvirtis	2026 m. IV ketvirtis	Vykdomas detalizavimas
2.	Mokslinio tyrimo vykdymas:			
2.1.	Tyrimo metodikos sudarymas:	2026 m. spalio	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. spalio	
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. spalio	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 – perėjimas prie postkvantinės kriptografijos (PQC) skaitmeninėse ekosistemose.

Tikslas – sukurti skaitmeninės ekosistemos modelį, skirtą kvantinių grėsmių atsparumui vertinti ir stiprinti.

Pagrindiniai uždaviniai (I metai):

- Išanalizuoti skaitmeninių ekosistemų sampratas ir modeliavimo metodus.
- Įvertinti jų tinkamumą PQC migracijos kontekste.
- Identifikuoti mokslinę problemą ir praktinio taikymo poreikį.
- Suformuoti tyrimo objektą ir tikslą.

Prielaida

PQC pasirengimas neturėtų būti vienkartinis migracijos projektas. Tai turėtų tapti nuolat valdoma skaitmeninės ekosistemos kibernetinės higienos ir atsparumo būseną.

Mokslinė problema

Kaip modeliuoti ekosistemą taip, kad PQC naudojimas ir atsparumas kvantinėms grėsmėms būtų nuolat matuojami, stebimi ir integruoti į technologinius, organizacinius, tiekimo grandinės bei valdymo procesus?

Pagrindinis klausimas modeliui:

Ar mūsų gebėjimas išlikti atspariems kvantinėms grėsmėms gerėja ar blogėja, ir kas tai lemia?

Galimos modelio dimensijos:

Tematika	Dabartinis požiūris	Sprendžiama problema
Technologijos	PQC algoritmai / protokolai	Kaip nuolat stebėti kriptografijos vystymą/pokytį?
Turtas	Kriptografinė inventorizacija	Kaip valdyti kriptografinius pajėgumus?
Organizacija	Migracijos planai	Kaip PQC valdymą integruoti į kasdienes procesus?
Priklausomybės	Tiekėjai / paslaugos	Kaip įvertinti priklausomybių poveikį atsparumui?
Laikas	Migracijos etapai	Kaip valdyti kriptografinį pokytį laikui bėgant?

Praktinio pritaikymo poreikis

Skaitmeninės ekosistemos nuolat keičiasi:

- technologijos ir programinės įrangos komponentai;
- tiekėjai ir tinklo paslaugos;
- kriptografinės konfigūracijos.

Todėl **vienkartinio *PQC readiness assessment* nepakanka.**

Reikalingas mechanizmas, kuris:

- ✓ nuolat identifikuotų kriptografinius pokyčius;
- ✓ vertintų jų poveikį kvantiniam atsparumui;
- ✓ prioretizuotų veiksmus;
- ✓ pateiktų sprendimų priėmėjams matuojamą atsparumo būklę.

Taikymas: *PQC readiness monitoring, cryptographic hygiene, risk prioritization, ecosystem resilience.*

Išanalizuotas PQC naudojimo poveikis tinklo lygmenyje ir IP fragmentacijos rizikai.
Paruoštas konferencinis straipsnis: „*Towards Quantum-Resilient Enterprises by Addressing Packet Fragmentation*“.

PQC algoritmams reikalingi didesni duomenų paketai



viršijamos tinklo standartinės perdavimo (MTU) ribos



atsiranda IP fragmentacija

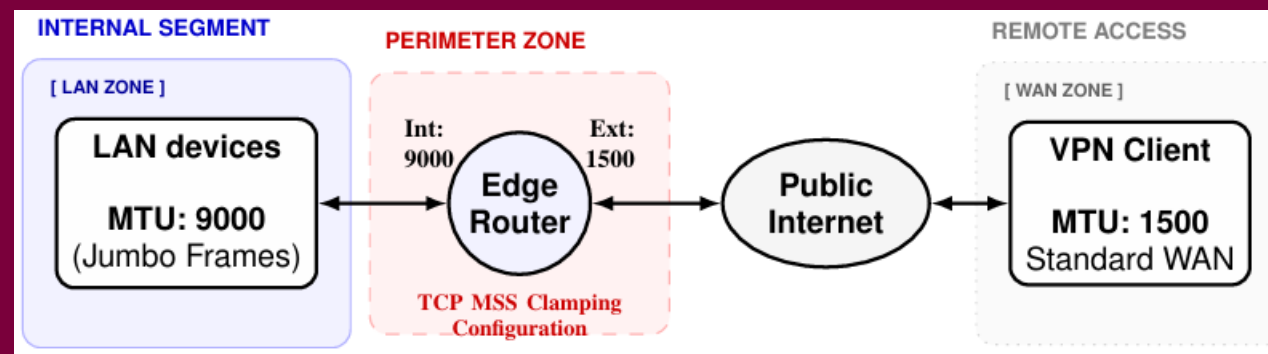
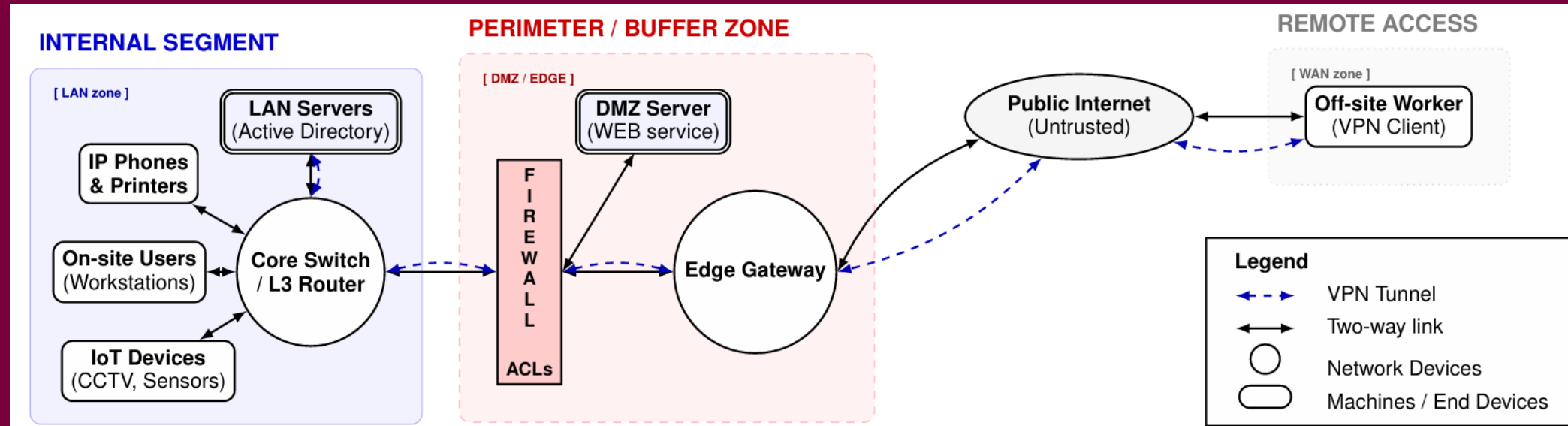


ryšio sutrikimai ir saugumo rizikos

Algorithm	Public Key Size (B)	Signature or Ciphertext Size (B)	IP Packets Required (1460)	Fragm. Risk Level
ECDSA	29 to 133	56 to 132	1	None
ECDH	29 to 133	28 to 66	1	None
ML-KEM	800 to 1568	768 to 1568	1 to 2	Low
ML-DSA	1312 to 2592	2420 to 4627	2 to 4	Moderate
SLH-DSA	32 to 66	7856 to 49856	6 to 35	High
FN-DSA	897 to 1793	666 to 1280	1 to 2	Low

Rezultatai: Pasiūlytas asimetrinis MTU valdymo modelis

Tikslas – pritaikyti PQC migraciją SME infrastruktūroje, naudojant praktiškai prieinamus tinklo valdymo mechanizmus.



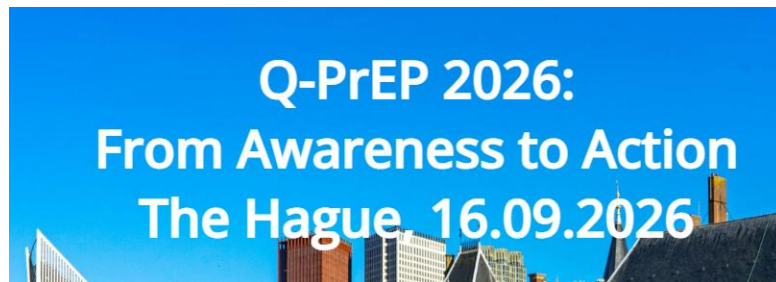
Kita veikla:

2026-04-10 tarptautiniame internetiniame seminare „QPrEP webinar“ pristatyti publikuoto tyrimo rezultatai.

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



Webinars



2026-09-16 dalyvauta Q-PrEP 2026 konferencijoje Hagoje, informacijos susirinkimui apie praktinius PQC migracijos aspektus bei užmegzti ryšius su Europos PQC srities ekspertais.

**Vilniaus
universitetas**

———— Kito pusmečio planas:

Tęsti tyrimus:

1. Detalizuoti mokslinę problemą, tyrimo objektą ir tikslą.
2. Parinkti tyrimo metodiką.
3. Pradėti kvantinėms grėsmėms atsparios skaitmeninės ekosistemos modelio kūrimą.

Studijuoti du mokomuosius dalykus:

- Reikalavimų inžinerijos metodai ir priemonės
- Sprendimų priėmimo strategijos

Atlikti stažuotę RTU

09.27–10.10 ir 11.01–11.07

Tikslas – modeliavimo praktikų įsisavinimas ir pritaikymas PQC ekosistemos modeliavimui.



**Vilniaus
universitetas**

KONTAKTAI

doktorantė

Simona Zavackė

MIF Informatikos instituto Kompiuterinio ir
duomenų modeliavimo katedra

simona.zavacke@mif.stud.vu.lt