DOKTORANTŪROS STUDIJŲ VEIKLOS ATASKAITA

Preliminarus daktaro disertacijos pavadinimas: Skaitmeninės informacijos autentiškumo tikrinimo metodas naudojant nulinio žinojimo įrodymo protokolą

Doktorantas: Laura Atmanavičiūtė

Doktoranto vadovas: Prof. Dr. Saulius Masteika

Doktorantūros pradžios ir pabaigos metai: 2024 – 2028 m.

Studijų metai (pusmetis): 2 (1)

Ataskaitinė doktorantų konferencija

2026 m. kovo 31 d.

Ataskaitinio pusmečio planas ir jo vykdymas

Bendrųjų gebėjimų ugdymas:

- Dalyvavimas VU Mokslo ir inovacijų departamento organizuojamuose mokymuose, skirtuose bendrųjų gebėjimų ugdymui – „R įvadas“ (1.25 ECTS).
- Dalyvavimas VU Mokslo ir inovacijų departamento organizuojamuose mokymuose, skirtuose bendrųjų gebėjimų ugdymui – „Akademinis raštingumas ir plagiato prevencija moksliniame darbe“ (0.15 ECTS).
- Dalyvavimas VU Mokslo ir inovacijų departamento organizuojamuose mokymuose, skirtuose bendrųjų gebėjimų ugdymui – „Įvadas į mokslometriją“ (0.15 ECTS).
- Dalyvavimas VU Mokslo ir inovacijų departamento organizuojamuose mokymuose, skirtuose bendrųjų gebėjimų ugdymui – „Lietuvos akademinė elektroninė biblioteka (eLABa): autoriaus sąsaja“ (0.15 ECTS).

Konferencijos:

- Pristatytas stendinis pranešimas konferencijoje „Zero-Knowledge Proofs for Digital Image Authenticity. Data Analysis Methods for Software Systems“ konferencijoje „16th Conference on Data Analysis Methods for Software Systems“.
- Parengtas ir pateiktas pranešimas „Tile-Based Zero-Knowledge Verification of Grayscale Image Transformations“ tarptautinei konferencijai „Third IEEE International Workshop on Programmable Zero-Knowledge Proofs for Decentralized Applications“.

Akademinė veikla:

- Fintech magistro studijų programos baigiamojo darbo recenzavimas.
- Dalyvavimas Fintech magistro studijų programos komiteto (SPK) veikloje.
- Bendradarbiavimas su magistrantais, jų konsultavimas ir mentorystė atliekant tyrimus.

Doktorantūros studijų planas ir jų vykdymo suvestinė

Studijų metai	**Egzaminai**	
	Planas	**Įvykdyta**
I (2024/2025)	2	2
II (2025/2026)	**2**	**2**
III (2026/2027)		
IV (2027/2028)		
Iš viso:	4	4

Mokslinių tyrimų planas ir jų vykdymo suvestinė

Studijų metai	Dalyvavimas konferencijose				Publikacijos					
	Tarptautinėse		Nacionalinėse		Su citav. rodikliu			Be citav. rodiklio		
	Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta	Būklė	Planas	Įvykdyta	Būklė
I (2024/2025)	1	2			0	1	Priimta			
II (2025/2026)	**0**	**1**			**1**	**0 (Įvykdyta I metais)**				
III (2026/2027)	1	0								
IV (2027/2028)					1	0				
Iš viso:	2	2			2	1				

Ataskaitinio pusmečio planas ir jo vykdymas (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.	Egzaminas išlaikytas.
Didžiųjų duomenų analitika (2026 m. I ketv.)	Didžiųjų duomenų analitika, 2026 m. kovo 23 d.	Egzaminas išlaikytas.

Dalyvavimas konferencijose 2025/2026 (I pusmetis)		
Planas	Įvykdyta	Konferencijos tipas
16th Conference „Data Analysis Methods for Software Systems“, 2025 m. lapkričio 27-29d., Druskininkai, Lietuva	Stendinis pranešimas: Atmanavičiūtė, L. *Zero-Knowledge Proofs for Digital Image Authenticity*, 2025 m. lapkričio 27 d., Druskininkai, Lietuva	Tarptautinė

Ataskaitinio pusmečio planas ir jo vykdymas (2)

Publikacijos 2025/2026 (I pusmetis)			
Planas	**Įvykdyta**	**Būklė**	**Publikacijos tipas**
-	-	-	-

Informacija apie tarptautinius renginius ir publikacijas, kuriose pateikti pagrindiniai disertacijos rezultatai

Dalyvavimas tarptautinėse konferencijose	
	Aprašas
1.	Atmanavičiūtė, L., Masteika, S. (2024). Towards Understanding the Application Areas of Zero Knowledge Proof: A Comprehensive Analysis. *19th Prof. Vladas Gronskas International Scientific Conference*, 2024 m. lapkričio 29 d., Kaunas, Lietuva
2.	Rutkauskas, M., Atmanavičiūtė, L., Masteika, S. (2025). Privacy-preserving model for Decentralized Digital Identity under EU compliance. *30th International Conference Information Society And University Studies IVUS2025,* 2025 m. gegužės 15 d., Kaunas, Lietuva
3.	Končius, A.L., Košubienė, G., Atmanavičiūtė, L., Masteika, S. (2025). Comparative Analysis and Implementation of Zero-Knowledge Proof Libraries for Digital Identity. *30th International Conference Information Society And University Studies IVUS2025*, 2025 m. gegužės 15 d.. Kaunas, Lietuva
4.	Atmanavičiūtė, L., Rutkauskas, M., Končius, A.L., Košubienė, G., Masteika, S. (2025). Blockchain-based solution for decentralized identity aligned with EU and W3C standards. *25th International Conference on Business Information Systems*, 2025 m. birželio 25-27 d., Poznanė, Lenkija
5.	Atmanavičiūtė, L. (2025). Zero-Knowledge Proofs for Digital Image Authenticity. Data Analysis Methods for Software Systems, 2025 m. lapkričio 27-29 d., Druskininkai, Lietuva

Mokslinių tyrimų ir disertacijos rengimo etapai

	Darbo pavadinimas	Atlikimo terminai	Pastabos
2.	Mokslinio tyrimo vykdymas:		
	2.1.2. Parengti teorinę metodologiją.	2025 m. spalio mėn. – 2026 m. balandžio mėn.	Parengta teorinė metodologija.
	2.2. Teorinis tyrimas: 2.2.1. Teorinis tyrimas apie nulinio žinojimo protokolą ir blokų grandinių technologijų taikymą skaitmeninio turinio autentiškumo tikrinimui.	2025 m. spalio mėn. – 2026 m. balandžio mėn.	Atliktas teorinis tyrimas apie nulinio žinojimo protokolą ir blokų grandinių technologijų taikymą skaitmeninio turinio autentiškumo tikrinimui.

Ataskaitinio pusmečio moksliniai rezultatai

Tyrimo objektas, tikslas ir uždaviniai

Tyrimo objektas: Skaitmeninės informacijos autentiškumo tikrinimo metodas, pagrįstas nulinio žinojimo įrodymo protokolu.

Tyrimo tikslas: Sukurti ir empiriškai pagrįsti nulinio žinojimo įrodymo protokolu paremtą metodą, leidžiantį patikimai patikrinti skaitmeninės informacijos autentiškumą, išsaugant duomenų privatumą ir konfidencialumą.

Tyrimo uždaviniai:

1. Atlikti literatūros analizę, nagrinėjant skaitmeninio turinio autentiškumo tikrinimo metodus bei nulinio žinojimo protokolų taikymą įvairiose srityse.
2. Parengti teorinį skaitmeninės informacijos autentiškumo tikrinimo metodo modelį, pagrįstą nulinio žinojimo įrodymu, bei atlikti esamų sprendimų analizę.
3. Atlikti empirinius tyrimus, pritaikant įvairius egzistuojančius ZKP sprendimus vienodomis sąlygomis, naudojant tuos pačius duomenis, ir įvertinti jų efektyvumą, patikimumą bei praktinį pritaikomumą.
4. Atlikti lyginamąją analizę, nustatant efektyviausią egzistuojantį sprendimą ir įvertinant jo pranašumus bei trūkumus lyginant su alternatyvomis.
5. Sukurti ir empiriškai pagrįsti patobulintą skaitmeninės informacijos autentiškumo tikrinimo metodo modelį bei realizuoti jo prototipą, išbandant jį su sintetiniais ir realiais duomenimis.

Ataskaitinio pusmečio moksliniai rezultatai

Šio pusmečio tikslas:

- Parengti teorinę metodologiją skaitmeninės informacijos autentiškumo tikrinimui, taikant nulinio žinojimo įrodymų protokolus.

Pagrindiniai pasiekti rezultatai:

- Atlikta skaitmeninio turinio autentiškumo metodų ir ZKP sistemų analizė.
- Suformuota teorinė metodologija siūlomam metodui.
- Apibrėžtas autentiškumas kaip verifikuojamas transformacijos teiginys.
- Sudarytas privatumą išsaugančio autentiškumo tikrinimo konceptualus modelis.
- Suformuluotas verifikavimo užduočių skaidymo principas dideliems skaitmeniniams objektams.

Rezultatas: sukurtas teorinis pagrindas tolesniam metodo ir prototipo kūrimui.

Pagrindinis teorinis rezultatas

Autentiškumas kaip verifikuojamas transformacijos teiginys

Šiame tyrimo etape autentiškumas apibrėžtas ne kaip vien tik failo nepakitimas, bet kaip galimybė kriptografiškai įrodyti, kad skaitmeninis objektas:

- Arba liko nepakitęs,
- Arba buvo gautas iš autentiškos pradinės būsenos pagal formaliai leistiną transformacijos taisyklę.

Esminė idėja

Tikrinamas ne tik galutinis rezultatas, bet ir ryšys tarp:

- Autentiškos pradinės būsenos,
- Transformacijos taisyklės,
- Ir pateikto rezultato.

Toks požiūris leidžia tikrinti autentiškumą ir tais atvejais, kai turinys yra teisėtai modifikuojamas, tačiau pirminiai duomenys negali būti pilnai atskleidžiami.

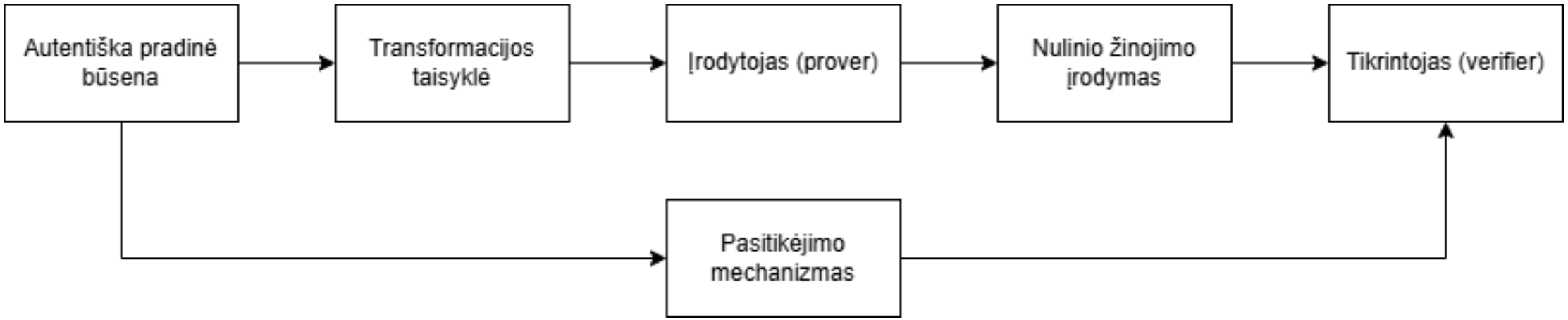
Teorinis pagrindas metodui

Siūlomo metodo principai

Kategorija	**Principai**
Saugumo principai	Korektiškumas
	Patikimumas
	Privatumo išsaugojimas
Semantiniai ir pasitikėjimo principai	Aiškiai apibrėžtos leistinos transformacijos
	Autentiškos pradinės būsenos patikimumo užtikrinimas
Praktiniai principai	Mastelio keičiamumas
	Moduliškumas
	Sąveikumas su kitomis autentiškumo infrastruktūromis

Šie principai sudaro teorinį pagrindą metodui, kuris turi būti ne tik kriptografiškai teisingas, bet ir praktiškai pritaikomas didelės apimties skaitmeniniams objektams.

Privatumą išsaugančio autentiškumo tikrinimo konceptualus modelis



Įrodytojas pateikia ZKP, kuriuo parodo, kad rezultatas buvo gautas iš autentiškos pradinės būsenos pagal leistiną transformaciją, neatskleidžiant pačios pradinės būsenos tikrintojui. Modelis leidžia suderinti autentiškumo tikrinimą, privatumo išsaugojimą ir verifikavimo formalumą.

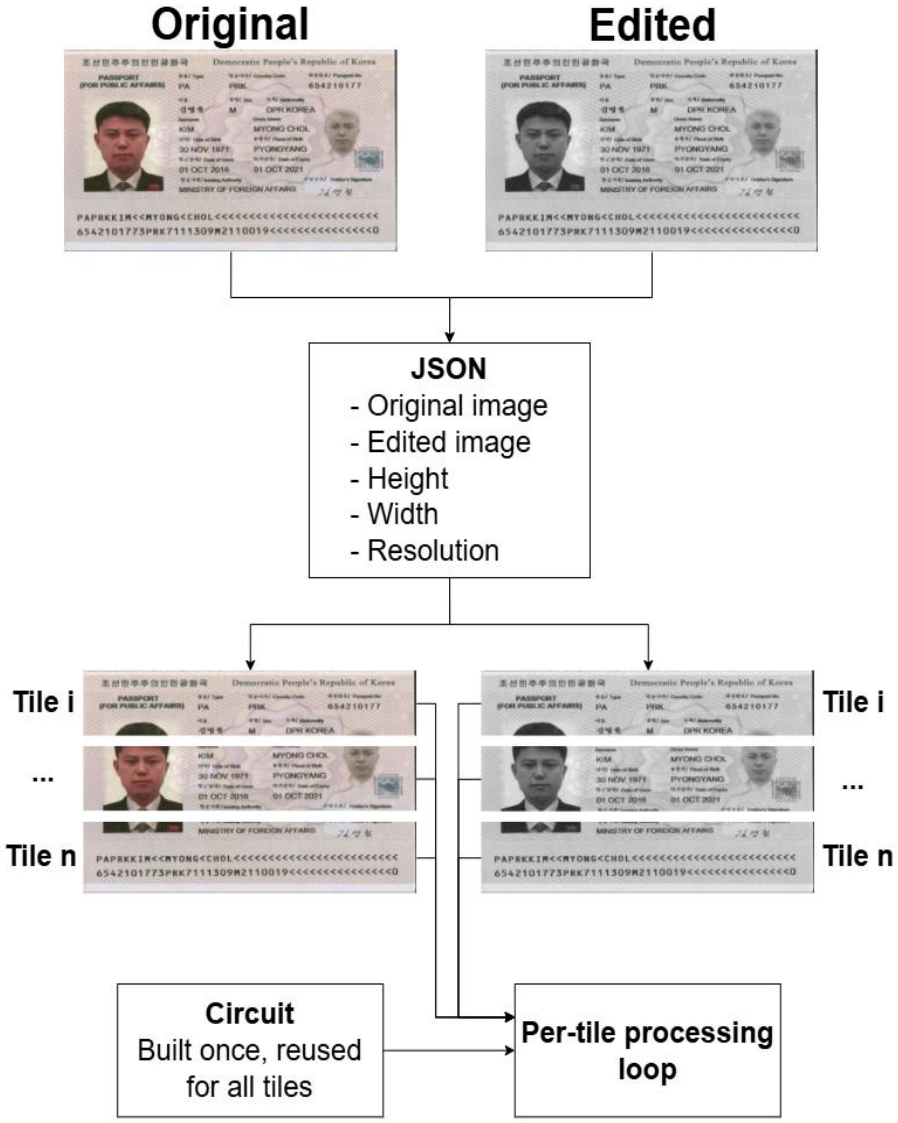
Siūlomo prototipo kryptis

Prototipo pasiūlymas grindžiamas šiomis prielaidomis:

- Autentiškumas tikrinamas kaip transformacijos korektiškumo teiginys.
- Pirminiai duomenys neturi būti atskleidžiami tikrintojui.
- Dideli objektai turi būti verifikuojami ne monolitiškai, o skaidant užduotį į mažesnius vienetus.

Siūloma kryptis:

- Transformacija tikrinama per mažesnes, struktūriškai vienodas dalis.
- Mažinamas atminties poreikis.
- Išlaikomas privatumą išsaugantis verifikavimas.



2025/2026 mokslo metų antrojo pusmečio darbo planas

Moksliniai tyrimai:

- Detalizuoti siūlomo metodo architektūrą.
- Sukurti tile-based prototipo loginę struktūrą.
- Apibrėžti eksperimentinį dizainą ir vertinimo rodiklius.
- Parengti prototipo realizacijos ir vertinimo pagrindą.

Kita akademinė veikla:

- Publikacijos rengimas disertacijos tematika.

DOKTORANTŪROS STUDIJŲ VEIKLOS ATASKAITA

Preliminarus daktaro disertacijos pavadinimas: Skaitmeninės informacijos autentiškumo tikrinimo metodas naudojant nulinio žinojimo įrodymo protokolą

Doktorantas: Laura Atmanavičiūtė

Doktoranto vadovas: Prof. Dr. Saulius Masteika

Doktorantūros pradžios ir pabaigos metai: 2024 – 2028 m.

Studijų metai (pusmetis): 2 (1)

Ataskaitinė doktorantų konferencija

2026 m. kovo 31 d.