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): 1 (2)

Ataskaitinė doktorantų konferencija

2025 m. spalio 3 d.

Ataskaitinio pusmečio planas ir jo vykdymas

Bendrųjų gebėjimų ugdymas:

- Dalyvavimas VU Mokslo ir inovacijų departamento organizuojamuose mokymuose, skirtuose bendrųjų gebėjimų ugdymui – *„Informacijos saugojimas ir citavimas naudojantis programa „Zotero““* (0.15 ECTS).

Konferencijos:

- Pristatyti pranešimai konferencijose:
  - *„Privacy-preserving model for Decentralized Digital Identity under EU compliance“*, tarptautinėje konferencijoje „30th International Conference Information Society And University Studies IVUS2025“.
  - *„Blockchain-based solution for decentralized identity aligned with EU and W3C standards“*, tarptautinėje konferencijoje „25th International Conference on Business Information Systems“.

Akademinė veikla:

- Dalyvavimas Finansų ir apskaitos taikomųjų sistemų programos studentų bakalauro darbų gynimo komisijoje ir baigiamųjų darbų recenzavimas.
- Dalyvavimas Fintech magistro studijų programos komiteto (SPK) veikloje.
- Įsitraukimas mokslinių tyrimų ir eksperimentinės plėtros (MTEP) veiklose.
- Bendradarbiavimas su magistrantais, jų konsultavimas ir mentorystė atliekant tyrimus (pristatyti pranešimai konferencijose: „Privacy-preserving model for Decentralized Digital Identity under EU compliance“, „Comparative Analysis and Implementation of Zero-Knowledge Proof Libraries for Digital Identity“ ir „Blockchain-based solution for decentralized identity aligned with EU and W3C standards“).

Doktorantūros studijų planas ir jų vykdymo suvestinė

Studijų metai	**Egzaminai**	
	Planas	**Įvykdyta**
I (2024/2025)	**2**	**2**
II (2025/2026)	2	0
III (2026/2027)		
IV (2027/2028)		
Iš viso:	4	2

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)					1	0				
III (2026/2027)	1	0								
IV (2027/2028)					1	0				
Iš viso:	2	2			2	1				

Ataskaitinio pusmečio planas ir jo vykdymas (1)

Egzaminai 2024/2025 (I pusmetis)		
Planas	**Įvykdyta**	**Būklė**
Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika (2025 m. birželio mėn.)	Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika, 2025 m. birželio 30 d.	Egzaminas išlaikytas, įvertinimas 9.
Blokų grandinių technologijos (2025 m. birželio mėn.)	Blokų grandinių technologijos, 2025 m. rugsėjo 16 d.	Egzaminas išlaikytas, įvertinimas 9.

Dalyvavimas konferencijose 2024/2025 (I pusmetis)		
Planas	Įvykdyta	Konferencijos tipas
25th International Conference on Business Information Systems, 2025 m. birželio 25-27 d., Poznanė, Lenkija	Atmanavičiūtė, L., Rutkauskas, M., Končius, A.L., Košubienė, G., Masteika, S. *Blockchain-based solution for decentralized identity aligned with EU and W3C standards*, 2025 m. birželio 25 d., Poznanė, Lenkija	Tarptautinė

Ataskaitinio pusmečio planas ir jo vykdymas (2)

Publikacijos 2024/2025 (I pusmetis)			
Planas	**Įvykdyta**	**Būklė**	**Publikacijos tipas**
IEEE Access	Atmanavičiūtė, L., Vanagas, T., Masteika, S. Quantitative Analysis of Centralization in the Bitcoin Lightning Network Through Centrality Metrics	Priimta: 2025 m. rugsėjo 22 d.	Impact Factor: 3.4 Q2 Clarivate Analytics Web of Science

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

Mokslinių tyrimų ir disertacijos rengimo etapai (1)

	Darbo pavadinimas	Atlikimo terminai	Pastabos
1.	**Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje):**		
	1.1. Atlikti literatūros ir esamų sprendimų analizę apie skaitmeninio turinio autentiškumo tikrinimo metodus ir skaitmeninės tapatybės dėkles.	2024 m. spalio mėn. – 2025 m. balandžio mėn.	Parengta mokslinės literatūros apžvalga.
	1.2. Atlikti mokslinius tyrimus, skirtus išanalizuoti blokų grandinės technologija paremto antrojo lygio tinklo mazgų architektūrą, siekiant įvertinti jų poveikį sistemos (de)centralizacijai ir transakcijų privatumui.	2024 m. spalio mėn. – 2025 m. balandžio mėn.	Parengta. Publikacija priimta žurnale „IEEE Access“.
	1.3. Išsamiai ištirti nulinio žinojimo įrodymo protokolus skirtingose taikymo srityse, tokiose kaip kriptovaliutų mokėjimai, skaitmeninė tapatybė, biometrika ir kitos).	2025 m. balandžio mėn. – 2025 m. spalio mėn.	Parengta mokslinės literatūros apžvalga.

Mokslinių tyrimų ir disertacijos rengimo etapai (2)

	Darbo pavadinimas	Atlikimo terminai	Pastabos
2.	Mokslinio tyrimo vykdymas:		
	2.1. Tyrimo metodikos sudarymas:		
	2.1.1. Apsibrėžti disertacijos tikslus ir uždavinius, iškelti hipotezes, nustatyti mokslinius neapibrėžtumus.	2025 m. balandžio mėn. – 2025 m. spalio mėn.	Apibrėžti disertacijos tikslai ir uždaviniai, iškeltos hipotezės, nustatyti moksliniai neapibrėžtumai.
	2.1.2. Parengti teorinę metodologiją.	2025 m. spalio mėn. – 2026 m. balandžio mėn.	
	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.	
	2.3. Empirinis tyrimas:		
	2.3.1. Pasiūlyti nulinio žinojimo įrodymo sprendimo prototipą, skirtą skaitmeninės informacijos verifikavimui.	2026 m. balandžio mėn. – 2026 m. spalio mėn.	
	2.3.2. Ištestuoti sukurtą prototipą su sintetiniais duomenimis.	2026 m. balandžio mėn. – 2026 m. spalio mėn.	
	2.3.3. Analizuoti gautus rezultatus ir tobulinti metodą.	2026 m. balandžio mėn. – 2026 m. spalio mėn.	
	2.4. Gautų duomenų analizė, apibendrinimas, išvadų parengimas:		
	2.4.1. Atlikti išsamesnę metodo analizę su realiais duomenimis.	2026 m. spalio mėn. – 2027 m. balandžio mėn.	
	2.4.2. Palyginti sukurtą metodą su kitais autentifikavimo metodais.	2026. spalio mėn. – 2027 m. balandžio mėn.	

Mokslinių tyrimų ir disertacijos rengimo etapai (3)

Darbo pavadinimas		Atlikimo terminai	Pastabos
3.	**Atskirų daktaro disertacijos dalių (tyrimo metodikos, rezultatų, ginamų teiginių, išvadų, ir kt.) parengimas:** 3.1. Teorinė dalis. 3.2. Analitinė dalis. 3.3. Eksperimentinė dalis.	 2025 m. spalio mėn. – 2026 m. balandžio mėn. 2026 m. balandžio mėn. – 2026 m. spalio mėn. 2026 m. spalio mėn. – 2027 m. balandžio mėn.	
4.	Daktaro disertacijos parengimas ir svarstymas padalinyje:	2028 m. birželio mėn.	
5.	Daktaro disertacijos gynimas:	2028 m. rugsėjo mėn.	

Ataskaitinio pusmečio moksliniai rezultatai

Motyvacija

Skaitmeninių vaizdų autentiškumas tampa vis sunkiau patikrinamas. Šiandien bet kas gali redaguoti nuotraukas ar pasitelkti generatyvinį dirbtinį intelektą, todėl klausimas yra labai aktualus: kaip galime įsitikinti, kad publikuotas paveikslėlis yra tikrai autentiškas, bet tuo pačiu neišduoti pradinio failo?

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 ir esamų sprendimų 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 teoriškai pagrįsti patobulintą skaitmeninės informacijos autentiškumo tikrinimo metodo modelį bei realizuoti jo prototipą, išbandant jį su sintetiniais ir realiais duomenimis.

Interaktyvūs vs. Neinteraktyvūs įrodymai

Table 1. Comparison of interactive and non-interactive ZKP systems

Feature	Interactive ZKPs	Non-interactive ZKPs (NIZKs)
Proof form	Multiple rounds	Single message
Example protocols	Schnorr, Feige–Fiat–Shamir	zk-SNARKs, zk-STARKs, Bulletproofs
Trusted setup	Not required	CRS (system-dependent)
Transferability	No	Yes
Typical use cases	Identification, authentication	Blockchain transactions, signatures

Table 2. Comparative overview of modern proof systems

System	Example use cases	Trusted setup	Proof size	Proving time	Verification time	Scalability	Post-quantum secure
Groth16 zkSNARK (Groth, 2016)	Zcash, Tornado cash, Loopring	Yes (circuit-specific)	~192 bytes	O(N), efficient with FFT + multi-exp	Constant (~ 2–3 pairings, ~ 10 ms)	Linear with circuit size; new circuit needs a new setup	No
PLONK zkSNARK (Gabizon et al, 2019)	Polygon zkEVM, zkSync	Yes (universal /updatable)	~300 bytes in practice	O (N log N) (FFT-based)	Constant (a few pairings/group checks)	Linear; single setup covers many circuits	No
zkSTARK (Ben-Sasson et al, 2018)	StarkEx, StarkNet	None (transparent)	Polylogarithmic (tens of kB)	O (N · polylog N) (hash/FFT-based)	O (polylog N) (tens of ms)	Excellent for large circuits; scales slowly with size	Yes
Bulletproofs (Bünz et al, 2018)	Monero (confidential transactions)	None (transparent)	Logarithmic (~1–2 KB)	O(N) (no FFT needed, but many multiexponentiations)	O(N), linear in constraints	Suitable for small/medium circuits; less practical at scale	No
Halo (Halo 2) (Bowe et al., 2019), (Electric Coin Company, 2023)	Zcash, Mina Protocol	None (transparent)	Small (SNARK-sized, recursive)	Higher, due to recursive composition	Constant, supports recursion	Highly scalable; recursive aggregation of many proofs	No
Nova (Kothapalli, Setty, & Chatterjande, 2021)	zk-VMs, zk-IMG, content verification	None (transparent)	Few kB (logarithmic growth)	Moderate to high, folding overhead	Constant (final proof succinct)	Very high; efficient for incremental proofs and pipelines	No

ZKP sistemų analizė

Table 3. Comparison of ZKP systems for digital media authenticity

System	Media	ZKP system	Trusted setup	Scalability	Proof size	Verification time	Quantum resistant
PhotoProof (Naveh & Tromer, 2016)	Image	Pinocchio (SNARK)	Yes	Low (tiny images)	Few hundred bytes	< 1 s	No
VerITAS (Datta, Chen, & Boneh, 2024)	Image	PLONK (SNARK)	Yes	High (30 MP, ~90 MB)	Few hundred bytes	< 1 s	No
zk-IMG (Kang et al., 2022)	Image	Nova	No	High (HD, chained proofs)	~1 KB	< 10 ms	No
Trust Nobody (Della Monica et al., 2025)	Image	Halo2	No	High (30 MP on laptop, <4 GB RAM)	Few KB	< 1 s	No
VIMz (Dziembowski, Ebrahimi, & Hassanzadeh, 2025)	Image	Folding zk-SNARK	No	High (up to 8K, ~100 MB)	< 11 KB	< 1 s	No
zk-REAL (Koyama et al., 2025)	Image	zk-SNARK + lattice hash	No	Medium–high (optimized for repeated edits)	Compact	< 1 s	Yes
Eva (Zhang et al., 2025)	Video	Folding IVC	No	High (2 min HD, ~2.4 h proving)	~448 B	< 1 s	No

ZKP sprendimai skaitmeninei informacijai

2025/2026 mokslo metų pirmojo pusmečio darbo planas

Studijų planas:

• Egzaminų laikymas – „Fundamentalieji informatikos ir informatikos inžinerijos metodai„ (8 ECTS) ir „Didžiųjų duomenų analitika“ (7 ECTS).

Moksliniai tyrimai:

• Parengti teorinę metodologiją ir atlikti teorinį tyrimą apie nulinio žinojimo protokolą ir blokų grandinių technologijų taikymą skaitmeninio turinio autentiškumo tikrinimui.

• Parengti pirminę disertacijos teorinę dalį.

• Eksperimento plano pasiruošimas/ eksperimento pradžia.

Kita akademinė veikla:

• Dalyvavimas konferencijoje 16th Conference Data Analysis Methods for Software Systems, lapkričio 27-29 dienomis.

• Publikacijos rengimas disertacijos tematika.

• Įsitraukimas į Fintech magistro studijų programos veiklą: magistro baigiamojo darbo temos pasiūlymas/ vadovavimas.

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): 1 (2)

Ataskaitinė doktorantų konferencija

2025 m. spalio 3 d.