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 (1)

Ataskaitinė doktorantų konferencija

2025 m. kovo 28 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).
  - „Atvirosios prieigos kompetencijų ugdymas“ (0.5 ECTS).

Konferencijos:

- Pristatytas pranešimas „Towards Understanding the Application Areas of Zero Knowledge Proof: A Comprehensive Analysis“ 19-oje prof. Vlado Gronsko tarptautinė mokslinėje konferencijoje.
- Pateikti pranešimai konferencijoms:

  1. „Blockchain Selection for Decentralized Digital Identity“ svarstymui tarptautinėje konferencijoje „25th International Conference on Business Information Systems“. https://bisconf.org/2025/

  2.„Privacy-preserving model for Decentralized Digital Identity under EU compliance“ svarstymui tarptautinėje konferencijoje „30th International Conference IVUS 2025“. https://ivus.vdu.lt/

  3.„Comparative Analysis and Implementation of Zero-Knowledge Proof Libraries for Digital Identity“ svarstymui tarptautinėje konferencijoje „30th International Conference IVUS 2025“. https://ivus.vdu.lt/

Projektai ir paraiškos:

- Pateikta paraiška VU jaunųjų mokslininkų ir tyrėjų įdėjų konkursui 2025-2026 metams. Projekto tema „**Design and Implementation of Compliant Zero Knowledge Proof Based Framework for IoT Access Control**“. Tikimasi gauti iki 18 000 eurų papildomų lėšų tyrimams. Tarpdisciplininis projektas su istorijos fakulteto doktorantu.

Akademinė veikla:

- 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 (pateikti pranešimai svarstymui konferencijose: *„Blockchain Selection for Decentralized Digital Identity“ , „Privacy-preserving model for Decentralized Digital Identity under EU compliance“, „Comparative Analysis and Implementation of Zero-Knowledge Proof Libraries for Digital Identity“*.

Doktorantūros studijų planas ir jų vykdymo suvestinė

Studijų metai	**Egzaminai**	
	Planas	**Įvykdyta**
I (2024/2025)	**2**	**0 (egzaminai numatomi 2025 06)**
II (2025/2026)	2	0
III (2026/2027)		
IV (2027/2028)		
Iš viso:	4	0

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**	**1** **Papildomai pateikta 2 konferencijoms:** • **IVUS 2025 – 2025 m. gegužės 15d.** • **BIS 2025 – 2025 m. birželio 25-27 d.**								
II (2025/2026)					1	0	Įteikta			
III (2026/2027)	1	0								
IV (2027/2028)					1	0				
Iš viso:	2	1			2	0				

Ataskaitinio pusmečio planas ir jo vykdymas (1)

Egzaminai 2024/2025 (I pusmetis)		
Planas	**Įvykdyta**	**Būklė**
0	0	-

Dalyvavimas konferencijose 2024/2025 (I pusmetis)		
Planas	Įvykdyta	Konferencijos tipas
19-oji prof. Vlado Gronsko tarptautinė mokslinė konferencija 2024 2024 m. lapkričio 29 d., Kaunas, Lietuva	Atmanavičiūtė, L., Masteika, S. (2024). Towards Understanding the Application Areas of Zero Knowledge Proof: A Comprehensive Analysis. *19th Prof. Vladas Gronskas International Scientific Conference 29th of November 2024.* Kaunas, Lithuania	Tarptautinė
25th International Conference on Business Information Systems 2025 m. birželio 25-27 d. Poznanė, Lenkija	<u>Pateikta svarstymui:</u> Atmanavičiūtė, L., Rutkauskas, M., Končius, A.L., Masteika, S. (2025). Blockchain Selection for Decentralized Digital Identity.	Tarptautinė
30th International Conference IVUS 2025 2025 m. gegužės 15 d. Kaunas, Lietuva	<u>Pateikta svarstymui:</u> Končius, A.L., Košubienė, G., Atmanavičiūtė, L., Masteika, S. (2025). Comparative Analysis and Implementation of Zero-Knowledge Proof Libraries for Digital Identity.	Tarptautinė

Ataskaitinio pusmečio planas ir jo vykdymas

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	Įteikta: 2025 m. vasario mėn.	Impact Factor: 3.4 Q2 Clarivate Analytics Web of Science
Blockchain: Research and Applications	Atmanavičiūtė, L., Vanagas, T., Masteika, S. Quantitative Analysis of Centralization in the Bitcoin Lightning Network Through Centrality Metrics	Įteikta (gautos pirmos recenzijos): 2025 m. vasario mėn. *Publikacija buvo priimta su rekomendacija atlikti korekcijas („accepted with revisions“), tačiau dėl žurnalo redkolegijos sudėtyje esančių sankcionuotų šalių mokslininkų buvo nuspręsta publikavimo atsisakyti.*	Impact Factor: 6.9 Q1 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 29th of November 2024. Kaunas, Lithuania
2.	Pateikta svarstymui: Atmanavičiūtė, L., Rutkauskas, M., Končius, A.L., Masteika, S. (2025). Blockchain Selection for Decentralized Digital Identity.
3.	Pateikta svarstymui: Končius, A.L., Košubienė, G., Atmanavičiūtė, L., Masteika, S. (2025). Comparative Analysis and Implementation of Zero-Knowledge Proof Libraries for Digital Identity.

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 dalis mokslinės literatūros apžvalgos.
	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 įteikta žurnalui „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.	

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.	
	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

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 skaitmeninės informacijos autentiškumo tikrinimo metodų, naudojančių nulinio žinojimo įrodymo protokolą, teorinę analizę.
2. Ištirti nulinio žinojimo įrodymo protokolų taikymo patirtis įvairiose srityse, išskiriant efektyviausius principus skaitmeninės informacijos autentifikavimo kontekste.
3. Sukurti teorinį skaitmeninės informacijos autentiškumo tikrinimo metodo modelį, grindžiamą nulinio žinojimo įrodymo protokolu, ir pagrįsti jo veikimą teoriškai.
4. Realizuoti siūlomo metodo prototipą bei atlikti jo eksperimentinį tyrimą, įvertinant metodo veiksmingumą, patikimumą ir privatumo išsaugojimą naudojant sintetinius ir realius duomenis.
5. Atlikti lyginamąją analizę, įvertinant siūlomo metodo pranašumus ir trūkumus lyginant su kitais egzistuojančiais skaitmeninės informacijos autentiškumo tikrinimo metodais.

Esami skaitmeninio turinio autentiškumo patvirtinimo metodai

- **Kriptografiniai parašai:** Užtikrina turinio autentiškumą, tačiau pažeidžiami rakto kompromitavimui ir kvantinių kompiuterių keliamoms grėsmėms (Gillmor and Stanley, 2021), (Wan et al., 2022), (Saini and Ahuja, 2024), (Xu, 2025).
- **Blokų grandinė:** Užtikrina nekintamumą, decentralizuota. Patvirtina turinio kilmę, tačiau negali tiesiogiai patvirtinti pakeitimų teisėtumo (Fraga-Lamas et al., 2020), (Atlam et al., 2024), (Edwardsson and Al-Saqaf, 2024).
- **Dirbtinio intelekto (AI) metodai:** Efektyviai aptinka turinio klastojimus, tačiau kyla problemų dėl klaidingai teigiamų ar neigiamų signalų ir ribotos adaptacijos (Shi et al., 2023), (Gupta et al., 2024), (Edwardsson and Al-Sawaf, 2024), (Kunova, 2024), (Wang et al., 2025).
- **Skaitmeniniai vandens ženklų technologijos (angl. Watermarking):** Plačiai naudojamos turinio autentiškumo įrodymui, tačiau yra jautrios specialiai nukreiptoms atakoms ir pakartotiniams turinio keitimams (Wan et al., 2022), (Yun et al., 2024).

1. Gillmor, D.K., Stanley, J. (2024). Attempts at a technological solution to disinformation will do more harm than good. ACLU. Retrieved from https://www.aclu.org/news/privacy-technology/attempts-at-a-technological-solution-to-disinformation-will-do-more-harm-than-good
2. Wan, W., Wang, J., Zhang, Y., Li, J., Yu, H., & Sun, J. (2022). A comprehensive survey on robust image watermarking. Neurocomputing (Amsterdam), 488, 226–247. https://doi.org/10.1016/j.neucom.2022.02.083
3. Saini, P., & Ahuja, R. (2024). Robust and Secure Video Authentication: A Hash-Based Watermarking Approach. IAENG International Journal of Computer Science, 51(9), 1291-.
4. Xu, J. (2025). A Comprehensive Study of Digital Signatures: Algorithms, Challenges and Future Prospects. ITM Web of Conferences, 73, 3009-. https://doi.org/10.1051/itmconf/20257303009
5. Fraga-Lamas, P., & Fernandez-Carames, T. M. (2020). Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality. IT Professional, 22(2), 53–59. https://doi.org/10.1109/MITP.2020.2977589
6. Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. Electronics (Basel), 13(17), 3568-. https://doi.org/10.3390/electronics13173568
7. Edwardsson, M.P., & Al-Saqaf, W. (2024). Blockchain solutions for generative AI challenges in journalism. Frontiers in Blockchain, 7, Article 1440355. https://doi.org/10.3389/fbloc.2024.1440355
8. Shi, C., Chen, L., Wang, C., Zhou, X., & Qin, Z. (2023). Review of Image Forensic Techniques Based on Deep Learning. Mathematics (Basel), 11(14), 3134-. https://doi.org/10.3390/math11143134
9. Gupta, G., Raja, K., Gupta, M., Jan, T., Whiteside, S. T., & Prasad, M. (2024). A Comprehensive Review of DeepFake Detection Using Advanced Machine Learning and Fusion Methods. Electronics (Basel), 13(1), 95-. https://doi.org/10.3390/electronics13010095
10. Kunova, M. (2024). Blockchain can help news publishers fight risks posed by fake news websites. Media News. Available at: https://www.journalism.co.uk/news/blockchain-can-help-news-publishers-fight-risks-posed-by-fake-news-websites/s2/a1171234/
11. Wang, T., Liao, X., Chow, K. P., Lin, X., & Wang, Y. (2025). Deepfake Detection: A Comprehensive Survey from the Reliability Perspective. ACM Computing Surveys, 57(3), 1–35. https://doi.org/10.1145/3699710
12. Yun, J., Liu, X., Lu, Y., Guan, J., & Liu, X. (2024). DRPChain: A new blockchain-based trusted DRM scheme for image content protection. PloS One, 19(9), e0309743-. https://doi.org/10.1371/journal.pone.0309743

Autentiškumo patikra naudojant nulinio atskleidimo įrodymus (ZKP)

Tyrimo svarba: Sprendžia esamus metodų trūkumus – didelės skaičiavimo sąnaudos, ilgas įrodymų generavimo laikas, mastelio plėtimo sudėtingumai, techninio įgyvendinimo bei ekosistemos kūrimo klausimai (Datta et al., 2025), (Naveh and Tromer, 2016), (Kang et al., 2022), (Visconti et al., 2024).

1. Datta, T., Chen, B., & Boneh, D. (2025). VerITAS: Verifying Image Transformations at Scale. 2025 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2025, pp. 97-97, doi: 10.1109/SP61157.2025.00097
2. Naveh, A., & Tromer, E. (2016). PhotoProof: Cryptographic Image Authentication for Any Set of Permissible Transformations. 2016 IEEE Symposium on Security and Privacy (SP), 255–271. https://doi.org/10.1109/SP.2016.23
3. Kang, D., Hashimoto, T., Stoica, I., & Sun, Y. (2022). ZK-IMG: Attested Images via Zero-Knowledge Proofs to Fight Disinformation. https://doi.org/10.48550/arxiv.2211.04775
4. Visconti, I., Della Monica, P., Vitaletti, A., & Zecchini, M. (2024). Do not trust anybody: ZK proofs for image transformations tile by tile on your laptop [Conference presentation]. Real World Crypto Symposium 2024, Toronto, Canada.

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 (1)

Ataskaitinė doktorantų konferencija

2025 m. kovo 28 d.