







Mahdi Sedaghat | October 2024

Post-Doc at COSIC & Freelance at Keleed Labs, Leuven, Belgium

 Homepage  Github  Twitter  email  LinkedIn  Phone

EDUCATION

KU Leuven

Postdoctoral Researcher at COSIC (Part-time)
Privacy-Enhancing Techniques in Distributed Systems.

Leuven, Belgium
August 2024-Present

KU Leuven

Ph.D. Candidate at COSIC
Privacy-Enhancing Techniques in Distributed Systems, Supervisor: Prof. Bart Preneel

Leuven, Belgium
Jan 2020-July 2024

Sharif University of Technology

Master of Secure Telecommunication and Cryptography
Attribute-Based Encryption, Supervisors: Prof. MR Aref & Prof. Javad Mohajeri

Tehran, Iran
Sept 2015- Sept 2017

EXPERIENCE

Foundations of Cryptography, ETH Zürich

Visiting Researcher, hosted by Prof. Dennis Hofheinz

Switzerland
June 2024

Department of Information Engineering, CUHK

Visiting Researcher, hosted by Prof. Sherman S. M. Chow

Hong Kong
Dec 2023

Mysten Labs.

Research Scientist, Internship, Crypto team

Remote
Apr 2023 - Aug 2023

ZK-Lab, University of Edinburgh

Visiting Researcher, hosted by Prof. Markulf Kohlweiss

Edinburgh, UK
Feb 2023 - Apr 2023

Computer Science Institute at Charles University

Visiting Researcher, hosted by Prof. Pavel Hubáček

Prague, Czech Republic
Jan 2019 - Jan 2020

Information Systems and Security Lab. (ISSL), SUT

Research Assistant

Tehran, Iran
Sept 2017 - Dec 2018

OPEN SOURCE PROJECTS


• Unlinkable Policy-Compliant Signatures

Prototyping the PCS and several implementations for ul-PCS schemes.

Python, Docker



• Groth-Sahai Proofs

An efficient implementation for the seminal work of Jens Groth and Amit Sahai proof system.

Python



• Nirvana Payment

A distributed implementation of an anonymous and reusable payment guarantee system.

Python


• Cross-Domain Attribute-Based Access Control Encryption (CD-ABACE)

Proof of concept for the cross-domain access control encryption scheme.

Python


PROGRAMMING SKILLS

- Familiar: Linux/Unix Programming, Latex, Python, Rust
- Some familiarity: Solidity, Sage, GoLang

TEACHING

- **Internship mentoring:** Anonymous Credentials, Student: Peter Schwarz, COSIC, KU Leuven (2023).
- **Lecturer** in Privacy course on Anonymous Credential systems, COSIC, KU Leuven (2022-2023).
- **Mentoring** in CyberSecurity Basics course, COSIC, KU Leuven (2022-2023 & 2023-2024).
- **Internship mentoring:** Decentralized e-Voting systems, Student: Sermin Kocaman, COSIC, KU Leuven (2022).
- **Master's Thesis Supervision:** Privacy assessment of current business practices using blockchains in banking and financial sector, Jowhar Ding, COSIC, KU Leuven (2020-2021).

PROFESSIONAL SERVICE

I have served on the **AC-2024, CANS-2024, CRYPTO-2024, PKC-2024, IEEE TDSC-2024, LatinCrypt-2023, ACM CCS-2023, IEEE TDSC-2023, IEEE TIFS-2022, EC-2022, AC-2020, TCC-2019** and **ISCISC-2018** as reviewer.

AWARDS AND ACHIEVEMENTS

- The best proposal for the Virtual design challenge for authentication and protecting Full Motion Video system, University of British Columbia, Canada, 2019. 🌐
- Ranked 46th in M.Sc. national university entrance exam in Communications branch among about 20,000 participants, 2015.
- Ranked 36th in Iranian National Olympiad in Electrical Engineering among all bachelor students of Electrical Engineering, 2014.

EXTRA

- Blogpost, Eurocrypt 2024: Twinkle (A Fully Adaptive Threshold Signature from DDH) 🌐
- Blogpost, Groth-Sahai Proofs: Zero to Hero. 🌐
- Technical consultant in the Groth'16 Ceremonial Setup for zkLogin project at Mysten Labs. 🌐

TALKS

- zkLogin, Foundations and Applications of Zero-Knowledge Proofs, Edinburgh UK, 04 Sept 2024.
- Unlinkable Policy-Compliant Signatures for Compliant and Decentralized Anonymous Payments; Privacy-Enhancing Technologies Symposium (PETS) 2024 in Bristol, UK, 18 July 2024.
- Threshold Structure-Preserving Signatures: Done and Ongoing Projects, Foundations of Cryptography, ETH Zürich, Switzerland, 04 June 2024.
- Subset-optimized BLS Multi-signature with Key Aggregation, Financial Crypto 2024, Curacao, 5 March 2024.
- Unlinkable Policy-Compliant Signatures for Compliant and Decentralized Anonymous Payments, CUHK, Hong Kong, 12 Dec 2023. [link](#)
- Threshold Structure-Preserving Signatures, Asiacrypt, Guangzhou, China, 6 Dec 2023. [link](#)
- Trusted Setups for zkSNARKs, Mysten Labs Paris offsite, 4 August 2023.
- Unlinkable Policy-Compliant Signatures, Blockchain Technology Lab (BTL), Edinburgh, 20 March 2023.
- Cross-Domain Attribute-Based Access Control Encryption, CANS'21, Online, 13 December 2021.

Publications

Foteini Baldimtsi, Konstantinos Kryptos Chalkias, Yan Ji, Jonas Lindstrøm, Deepak Maram, Ben Riva, Arnab Roy, Mahdi Sedaghat, and Joy Wang. zkLogin: Privacy-Preserving Blockchain Authentication with Existing Credentials. *ACM CCS'24 and presented at SBC'24, NY*, 2024. <https://arxiv.org/pdf/2401.11735>.

Christian Badertscher, Mahdi Sedaghat, and Hendrik Waldner. Fine-Grained Accountable Privacy via Unlinkable Policy-Compliant Signatures. *Cryptology ePrint Archive*, Paper 2023/1070 (PETS'24 and presented at CTB workshop at EC'24), 2023. <https://eprint.iacr.org/2023/1070>.

Aikaterini Mitrokotsa, Sayantan Mukherjee, Mahdi Sedaghat, Daniel Slamanig, and Jenit Tomy. Threshold Structure-Preserving Signatures: Strong and Adaptive Security Under Standard Assumptions. In Qiang Tang and Vanessa Teague, editors, *Public-Key Cryptography – PKC 2024*, pages 163–195, Cham, 2024. Springer Nature Switzerland.

Foteini Baldimtsi, Konstantinos Kryptos Chalkias, Francois Garillot, Jonas Lindstrom, Ben Riva, Arnab Roy, Mahdi Sedaghat, Alberto Sonnino, Pun Waiwitlikhit, and Joy Wang. Subset-optimized BLS Multi-Signature with Key Aggregation. *Cryptology ePrint Archive*, Paper 2023/498 (Financial Crypto 2024), 2024. <https://eprint.iacr.org/2023/498>.

Elizabeth Crites, Markulf Kohlweiss, Bart Preneel, Mahdi Sedaghat, and Daniel Slamanig. Threshold Structure-Preserving Signatures. In *International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'23)*, pages 348–382. Springer, 2023. <https://eprint.iacr.org/2022/839>.

Karim Bagheri, Axel Mertens, and Mahdi Sedaghat. Benchmarking the Setup of Updatable Zk-SNARKs. In *Progress in Cryptology – LATINCRYPT 2023*, pages 375–396, Cham, 2023. Springer Nature Switzerland. <https://eprint.iacr.org/2023/1161>.

Akash Madhusudan, Mahdi Sedaghat, Samarth Tiwari, Kelong Cong, and Bart Preneel. Reusable, Instant and Private Payment Guarantees for Cryptocurrencies. In *Information Security and Privacy – 28th Australasian Conference, ACISP 2023, Brisbane, QLD, Australia, July 5-7, 2023, Proceedings*, volume 13915 of *Lecture Notes in Computer Science*, pages 580–605. Springer, 2023. <https://eprint.iacr.org/2023/583>.

Seyed Farhad Aghili, Mahdi Sedaghat, Dave Singelee, and Maanak Gupta. MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme. *Future Generation Computer Systems*, 2022. <https://www.sciencedirect.com/science/article/pii/S0167739X22000115>.

Karim Bagheri and Mahdi Sedaghat. Tiramisu: Black-Box Simulation Extractable NIZKs in the Updatable CRS Model. In *Cryptology and Network Security (CANS)*, pages 531–551, Cham, 2021. Springer International Publishing. <https://eprint.iacr.org/2020/474>.

Mahdi Sedaghat and Bart Preneel. Cross-Domain Attribute-Based Access Control Encryption. In *Cryptology and Network Security (CANS)*, pages 3–23. Springer International Publishing, 2021. <https://eprint.iacr.org/2021/074>.