Mahdi Sedaghat | February 2025

Post-Doc at COSIC & Co-Founder at Soundness Labs, Leuven, Belgium

Homepage   Github   Twitter   email   Linkedin   ☎ Phone

EDUCATION

KU Leuven — **Leuven, Belgium**
Postdoctoral Researcher at COSIC (Part-time) — *August 2024-Present*
Privacy-Enhancing Techniques in Distributed Systems.

KU Leuven — **Leuven, Belgium**
Ph.D. Candidate at COSIC — *Jan 2020-July 2024*
Privacy-Enhancing Techniques in Distributed Systems, Supervisor: Prof. Bart Preneel

Sharif University of Technology — **Tehran, Iran**
Master of Secure Telecommunication and Cryptography — *Sept 2015- Sept 2017*
Attribute-Based Encryption, Supervisors: Prof. MR Aref & Prof. Javad Mohajeri

EXPERIENCE

Soundness Labs Ltd — **UK, London (Remote)**
Co-Founder, Cheif Scientist at Soundness Labs — *August 2024- present*

Foundations of Cryptography, ETH Zürich — **Switzerland**
Visiting Researcher, hosted by Prof. Dennis Hofheinz — *June 2024*

Department of Information Engineering, CUHK — **Hong Kong**
Visiting Researcher, hosted by Prof. Sherman S. M. Chow — *Dec 2023*

Mysten Labs. — **US (Remote)**
Research Scientist, Internship, Crypto team — *Apr 2023 - Aug 2023*

ZK-Lab, University of Edinburgh — **Edinburgh, UK**
Visiting Researcher, hosted by Prof. Markulf Kohlweiss — *Feb 2023 - Apr 2023*

Computer Science Institute at Charles University — **Prague, Czech Republic**
Visiting Researcher, hosted by Prof. Pavel Hubáček — *Jan 2019 - Jan 2020*

Information Systems and Security Lab. (ISSL), SUT — **Tehran, Iran**
Research Assistant — *Sept 2017 - Dec 2018*

GRANTS

Towards a Quantum Safe Digital Future — *Jan 2025 - Present*
Global Seed Fund 2025, joint proposal in collaboration with Prof. Bart Preneel (KUL) and Prof. Sushmita Ruj (UNSW Sydney).

- Developing zk-friendly PQ digital signatures tailored for privacy-preserving technologies (PETs).
- Analyzing and optimizing the performance of network protocols with PQC-based key encapsulation and signature schemes.
- Transitioning authentication mechanisms such as OpenID Connect, OAuth, and TLS to quantum-resistant solutions while maintaining efficiency and compatibility with existing infrastructures.

OPEN SOURCE PROJECTS

- **SP1 proofs on Sui** **Rust**
  A SP1 Groth16 Proof Verifier for Sui.
- **Unlinkable Policy-Compliant Signatures** **Python, Docker**
  Prototyping the PCS and several implementations for ul-PCS schemes.
- **Groth-Sahai Proofs** **Python**
  An efficient implementation for the seminal work of Jens Groth and Amit Sahai proof system.
- **Nirvana Payment** **Python**
  A distributed implementation of an anonymous and reusable payment guarantee system.
- **Cross-Domain Attribute-Based Access Control Encryption (CD-ABACE)** **Python**
  Proof of concept for the cross-domain access control encryption scheme.

PROGRAMMING SKILLS

- Familiar: Linux/Unix Programming, Latex, Python, Rust, Move Smart contract.
- Some familiarity: Solidity, Sage, GoLang, Move smart contract.

STUDENTS & TEACHING EXPERIENCES

- **Hossein Moghaddas** (PhD student, co-Supervisor with Prof. Bart Preneel)
- **Kiran Deep Ghosh** (ISI Kolkata), master thesis supervisor.
- **Theresa Wakonig** (ETH Zurich), master thesis co-supervisor.

- **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 am serving as a PC member at:

- **Information Security Conference** (ISC 2025), Seoul, Korea.
- **PrivCrypt-2025** workshop, co-located with ACNS-2025.

I have served on the **TIFS-2025**, **PETS-2025**, **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, SP1 Verifier on Sui 🌍
- 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

- Zero-Knowledge proofs: Applications to Blockchain, Cybersecurity Industry Day 2024, Mechelen, Belgium.
- 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

Karim Baghery, Ehsan Ebrahimi, Omid Mirzamohammadi, and Mahdi Sedaghat. Traceable verifiable secret sharing and applications. Cryptology ePrint Archive, Paper 2025/318, 2025. `https://eprint.iacr.org/2025/318.pdf`.

Omid Mirzamohammadi, Jan Bobolz, Mahdi Sedaghat, Emad Heydari Beni, Aysajan Abidin, Dave Singelee, and Bart Preneel. Keyed-verification anonymous credentials with highly efficient partial disclosure. Cryptology ePrint Archive, Paper 2025/041, 2025. `https://eprint.iacr.org/2025/041.pdf`.

Mahdi Sedaghat and Bart Preneel. Privacy-Enhancing Techniques in Distributed Systems. *PhD Thesis*, 2024. `https://cosicdatabase.esat.kuleuven.be/backend/publications/files/these/514`.

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, and RWC'25, Sofia)*, 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 Assump-

tions. 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 Baghery, 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 Baghery 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`.

Reyhaneh Rabaninejad, Seyyed Mahdi Sedaghat, Mohamoud Ahmadian Attari, and Mohammad Reza Aref. An id-based privacy-preserving integrity verification of shared data over untrusted cloud. In *2020 25th International Computer Conference, Computer Society of Iran (CSICC)*, pages 1–6, 2020.

Seyyed Mahdi Sedaghat, Mohammad Hassan Ameri, Javad Mohajeri, and Mohammad Reza Aref. An efficient and secure data sharing in smart grid: Ciphertext-policy attribute-based signcryption. In *2017 Iranian Conference on Electrical Engineering (ICEE)*, pages 2003–2008, 2017.