Mahdi Sedaghat | Aug 2023

B 01.13, COSIC, ESAT, KU Leuven, 3000 Leuven, Belgium

Homepage Github Twitter email Linkedin Phone

EDUCATION

Ku Leuven — **Leuven, Belgium**
Ph.D Student at COSIC — *Jan 2020-Present*
Privacy-Preserving 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 Encryptions, Supervisors: Prof. MR Aref & Prof. Javad Mohajeri

EXPERIENCE

Mysten labs. — **Remote**
Research SciInternship — *Apr 2023 - Aug 2023*

School of Informatics, University of Edinburgh. — **Edinburgh, UK**
Visiting Prof. Markulf Kohlweiss — *Feb 2023 - Apr 2023*

Computer Science Institute at Charles University in Prague. — **Prague, Czech Republic**
Visiting Researcher — *Jan 2019 - Jan 2020*

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

Alvand Powerplant Projects Development Company — **Tehran, Iran**
Technical Manager — *Nov 2016 - Dec 2018*

COMPUTER SKILLS

- **Power Engineering**: ETAP, DIgSILENT (Schematic & DPL), SIMATIC Manager (PLC).
- **Electronic and digital processing**: Proteus, Codevision (AVR Programming), MATLAB (Programming & Simulink).
- **Programming**: C, C++, Linux/Unix Programming, Latex, Python, Solidity, Sage, GoLang, Rust.
- **General**: Microsoft Office, Visio, MS Project, Photoshop, Davinci Resolve.

TEACHING

- **Lecturer** in Privacy course on Anonymous Credential systems, imec-Cosic, KU Leuven (2023-2024).
- **Mentoring** in CyberSecurity Basics course, imec-Cosic, KU Leuven (2022-2023).
- **Internship mentoring**: Decentralized e-Voting systems, Student: Sermin Kocaman, imec-Cosic, KU Leuven (2022).
- **Master Thesis Supervision**: Privacy assessment of current business practices using blockchains in banking and financial sector, Jowhar Ding, imec-Cosic, KU Leuven (2020-2021).
- **Network Security**: Teaching Assistant, Sharif University of Technology, Iran, Spring 2017, Graduate Course, Instructor: Prof. Javad Mohajeri.
- **Engineering Mathematics**: Teaching Assistant, Birjand University, Iran, Spring 2014, Undergraduate Course, Instructor: Prof. Zahiri.
- **Electrical Circuits Theory**: Lecturer, Youtube, 2016, Undergraduate Course, Konkur.

- **Signals and Systems**: Teaching Assistant, Birjand University, Iran, Fall 2013, Undergraduate Course, Instructor: Prof. Naser Neda.

PROFESSIONAL SERVICE

I have served on the **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 Colombia, Canada, 2019 Link.
- 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.
- Ranked 3st/38 in bachelor students of Electrical Engineering, 2014.

Publications

Karim Baghery, Axel Mertens, and Mahdi Sedaghat. Benchmarking the setup of updatable zk-snarks. Cryptology ePrint Archive, Paper 2023/1161, 2023. To appear at LatinCryp'23.

Christian Badertscher, Mahdi Sedaghat, and Hendrik Waldner. Fine-Grained Accountable Privacy via Unlinkable Policy-Compliant Signatures. Cryptology ePrint Archive, Paper 2023/1070, 2023. Under review.

Karim Baghery and Mahdi Sedaghat. Tiramisu: Black-Box Simulation Extractable NIZKs in the Updatable CRS Model. In Mauro Conti, Marc Stevens, and Stephan Krenn, editors, *Cryptology and Network Security (CANS)*, pages 531–551, Cham, 2021. Springer International Publishing.

Elizabeth Crites, Markulf Kohlweiss, Bart Preneel, Mahdi Sedaghat, and Daniel Slamanig. Structure-Preserving Threshold Signatures. Cryptology ePrint Archive, Paper 2022/839, 2022. Under review.

Akash Madhusudan, Mahdi Sedaghat, Samarth Tiwari, Kelong Cong, and Bart Preneel. Reusable, instant and private payment guarantees for cryptocurrencies. In Leonie Simpson and Mir Ali Rezazadeh Baee, editors, *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.

Akash Madhusudan, Mahdi Sedaghat, Philipp Jovanovic, and Bart Preneel. Nirvana: Instant and Anonymous Payment-Guarantees. *Cryptology ePrint Archive*, 2022. Under review.

Katerina Mitrokotsa, Sayantan Mukherjee, Mahdi Sedaghat, Daniel Slamanig, and Jenit Tomy. Threshold Structure Preserving Signatures: Strong and Adaptive Security under Standard Assumptions. *Cryptology ePrint Archive*, 2022. Under review.

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, 2023. Under review.

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. IEEE, 2017.

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.

Mahdi Sedaghat and Bart Preneel. Cross-Domain Attribute-Based Access Control Encryption. In Mauro Conti, Marc Stevens, and Stephan Krenn, editors, *Cryptology and Network Security (CANS)*, pages 3–23. Springer International Publishing, 2021.