Mahdi Sedaghat | February 2022

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

Homepage Github Twitter email Linkedin Phone

EDUCATION

Ku Leuven **Leuven, Belgium**
Doctoral Student at COSIC *Jan 2020-Present*
Privacy-Preserving in Distributed Systems, Supervisor: Prof. Bart Preneel

Charles University in Prague **Prague, CZ**
Visiting Researcher at Computer Science Institute *Jan 2019-Dec 2019*
Transparent and Scalable Argument of Knowledge systems (STARK), Supervisor: Prof. Pavel Hubáček

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

University of Birjand **Birjand, Iran**
Bachelor of Electrical Engineering-Telecommunication *Sept 2010- Sept 2014*
Deep Image Processing Implementation, Supervisor: Prof. Hasan Farsi

RESEARCH INTERESTS

- Cryptography and Network security.
- Cryptocurrencies and Blockchain security.
- Zero-Knowledge proof systems.
- Threshold cryptography.
- Homomorphic Encryption schemes.
- ID-based, Attribute-based Encryption schemes and Access Control.
- Smart Grid and Internet of Things (IoT) Security.

EXPERIENCE

Computer Science Institute at Charles University in Prague. **Prague, Czech Republic**
Visiting Researcher *Jan 2019 - Jan 2020*
- Working on the transparent and scalable Zero-Knowledge proofs in the Random Oracle Model based on the Algebraic Geometry codes.
- Access Control Encryption schemes based on the Attribute-Based Encryption schemes and their implementations.
- Computational complexity methods and worked on the Verifiable Delay Functions.

Information Systems and Security Lab. (ISSL) **Tehran, Iran**
Research Assistant *June 2017 - Sept 2018*
- Managing a group of bachelor and master students at Information Systems and Security LAB (ISSL), Electrical Engineering department, SUT.
- Assisting five different academic projects contain as, Cloud Computing Security, Private Set Intersection Protocols, Broadcast and Anonymous Authentication, Secure Auction Protocol in Smart Grid, Physical unclonable functions and applications.

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

- This Company is a private joint stock company incorporated in Iran. This company was trying to find the possible improvements in the existing power network with regards to the Smart Grid features.
- The principal activities of the Company are the development, construction, owning, operating and management of clean energy power plants, including but not limited to, wind power generation, CHP (natural gas) power generation, photovoltaic power generation.

Iran Workshop on Communication and Information Theory (IWCIT) **Tehran, Iran**
Executive member *Feb 2015 - Sept 2017*

- IWCIT features world-class speakers, plenary talks and technical sessions on a diverse range of topics in communication and information theory.

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

- **Master Thesis Supervision**: Privacy assessment of current business practices using blockchains in banking and financial sector, Jowhar Ding, 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 **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.

EXTRA

- Udemy, "Blockchain A-Z^{TM}: Learn How To Build Your First Blockchain", "Learn Ethical Hacking From Scratch", "GoLang".
- Coursera, "Google Cloud Platform Fundamentals: Core Infrastructure", "IT Security: Defense against the digital dark arts", "Crypto I".

- Passing the course, "Advanced methods in Cryptography" with Prof. Bart Preneel, Prof. Nigel Smart, Prof. Frederik Vercauteren, Ku Leuven.
- Passing the course, "Basics of information transmission and processing" with Prof. Michal Koucký, CUNI.
- Passing the course, " Foundations of theoretical cryptography" with Prof. Pavel Hubacek, CUNI.

LANGUAGES

- Persian: Native Language.
- English: Fluent.
- Dutch: Basic.

INTERESTS

- Persian Musical Instruments: Playing Santur and Setar.
- Sport: Table Tennis, Football.
- Extra: History, Persian Poetry.

Publications

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.

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.

Akash Madhusudan, Mahdi Sedaghat, Philipp Jovanovic, and Bart Preneel. Nirvana: Instant, Anonymous and Unlinkable Payment-Guarantees. Under Submission, 2022.

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. IEEE, 2020.

Seyyed Mahdi Sedaghat, Mohammad Hassan Ameri, Mahshid Delavar, Javad Mohajeri, and Mohammad Reza Aref. An efficient and secure Attribute-Based Signcryption scheme for smart grid applications. Technical report, Cryptology ePrint Archive, Report 2018/263, Under Review, 2018.

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. IEEE, 2017.

Mahdi Sedaghat, Behzad Abdolmaleki, Daniel Slamanig, and Bart Preneel. Threshold Structure-Preserving Signatures and Applications to Cross-Domain Access Control. Under Submission, 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.