Mahdi Sedaghat

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

Mahdi Sedaghat ssedagha@esat.kuleuven.be +32 16326964

EDUCATION

Ku Leuven **Leuven, Belgium**
Doctoral Student at COSIC *Jan 2020-Present*

Charles University in Prague **Prague, CZ**
Visiting Researcher at Computer Science Institute *Jan 2019-Jan 2020*

Sharif University of Technology **Tehran, Iran**
Master of Secure Telecommunication and Cryptography *Sept 2015- Sept 2017*

University of Birjand **Birjand, Iran**
Bachelor of Electrical Engineering-Telecommunication *Sept 2010- Sept 2014*

RESEARCH INTERESTS

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

ACADEMIC PROJECTS

Transparent and succinct Zero-Knowledge proofs *Jan 2020 - Present*

- This project aims to propose a Scalable ZK scheme without third trusted party (CRS generator).
- We have considered the Algebraic Geometry codes instead the Reed-Solomon codes.
- Although there is no need for agreed public parameters between the verifier and the prover, we constructs a quantum-secure zero-knowledge proof system.
- This scheme is implemented but we are trying to make it more efficient.

Anonymous consensus group in Blockchain *April 2019 - Present*

- Bitcoin as a decentralized and peer to peer cryptocurrency network does not preserve users' privacy.
- The transaction should be confirmed by the majority of honest miners with regards to the Byzantine Fault Tolerance agreement.
- Anonymous verifiable random functions are considered as a primitive to check the validity of a randomly generated number without revealing any information about the identity of the users in the committee.
- This scheme aims to prevent revealing the identity of the consensus group members with regards to the honestly updated keys.

Privacy-Preserving fast on-chain payment method *June 2020 - Present*

- Non-Turing permissionless cryptocurrencies like Bitcoin besides multiple advantages have high latency.
- There are some solutions to tackle this problem but they are either based on the smart contracts or do not protect the users' privacy.
- In this project, we aim to propose a privacy preserving low-latency on-chain method to address this issue.

Private-Flex *Jan 2020 - Present*

- Global environment concerns, decreasing the fossil fuel consumption and sustainability of the power network requires a Flexible power distribution.
- Costumers' security concerns in both cases message secrecy and users' privacy aim to take the cryptography solutions into account.
- In this project, we use the multi-party computation schemes such that the rewarding phase is based on a distributed currency network under Zero-Knowledge methods.

Light-weight Blockchain ledger verification *June 2020 - Present*

- To ensure the validity of the whole blocks in the Blockchain, it takes days and needs gigabytes of storage.
- How is it possible to just check the validity of some blocks in the Blockchain in the order of logarithmic than the Blockchain size?
- In the proof-of-work, we have a structure for the validated blocks and the verifier can follow an optimum distribution to reach to this target.
- In this project, We are trying to make it generalize for Proof of Stake and Proof of Space mechanisms.

Smart Grid security *Sept 2016 – Sept 2017*

- How is it possible to securely and efficiently share a message amongst a huge number of smart meters while they have a low-computational capacity in the Smart Grid.
- Attribute-Based Signcryption (ABSC) schemes as a powerful primitive are considered to tackle this problem.
- Regarding the SCADA network we can outsource the computational cost to a data center.
- The number of bilinear pairing in this scheme is independent of the number of attributes.

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 Programming).
- **Electronic and digital processing**: Proteus, Codevision (AVR Programming), MATLAB (Programming Simulink).
- **Programming**: C, C++, Linux/Unix Programming, Latex, Python, Solidity, Sage, GoLang.
- **General**: Microsoft Office, Visio, MS Project, Photoshop, Davinci Resolve.

TEACHING

- **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: Dr. neda

PROFESSIONAL SERVICE

I have served on the **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.
- Theory and Practice of Blockchains Workshop, Aarhus, Denmark, 2019.
- 3rd Zero-Knowledge Proof Workshop, London, UK, 2020.

Publications

Karim Baghery and Mahdi Sedaghat. Tiramisu: Black-box simulation extractable nizks in the updatable crs model. Technical report, Cryptology ePrint Archive, Report 2020/474, Under Review, 2020.

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.

Mahdi Sedaghat and Bart Preneel. Policy-updatable attribute-based access control for cloud computing. Under Review, 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.