Seyyed Mahdi Sedaghat

Univerzita Karlova, Informatický ústav UK, Malostranské nám. 25, 118 00 Praha 1

mahdisedaghat   ✉ s.m.sedaghat@gmail.com

EDUCATION

Charles University in Prague	**Prague, CZ**
Visiting student of security and informatics	*Jan 2019-Present*
Sharif University of Technology	**Tehran, Iran**
Master of Secure Telecommunication and Cryptography	*September 2017*
University of Birjand	**Birjand, Iran**
Bachelor of Electrical Engineering- Telecommunication	*June 2014*

RESEARCH INTERESTS

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

ACADEMIC PROJECTS

Transparent and succinct Zero-Knowledge proofs *Jan 2019 - Present*

- This project aims to propose a Scalable ZK scheme without third trusted party (CRS).
- By considering the Algebraic Geometry codes' properties.
- Although there is not any agreed public parameters between the verifier and the prover we can satisfy the critical features for ZK schemes.
- This scheme is implemented but we are trying to make it more efficient.

Anonymous consensus group in Blockchain *Feb 2019 - Present*

- Bitcoin as a decentralized and peer to peer cryptocurrency network does not preserve the privacy of the committee members.
- The transaction should be confirmed by the majority of honest miners with regards to the Byzantine Fault Tolerance.
- 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.
- This scheme presents a scheme to prevent revealing the identity of the consensus group members with the aim of the honestly updated keys.

Light-weight Blockchain ledger verification *June 2019 - Present*

- To ensure the validity of the whole transactions in Blockchain schemes takes days and needs gigabytes of storage.
- How is it possible to just check the validity of some blocks in the chain in logarithmic in the scale of blockchain size?
- In the proof of works we have a structure for the confirmed blocks and the verifier can follow an optimal distribution to reach to this target.
- We are trying to make it general for other models such as proof of stake and proof of space schemes.

Smart Grid security *Sept 2016 – Sept 2017*

- How is it possible to securely and efficiently share a message amongst numerous smart meters while they have a low computational capacity in 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

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.
- **General**: Microsoft Office, Visio, MS Project, Photoshop.

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 **TCC-2019** and **ISCISC-2018** as reviewer.

AWARDS AND ACHIEVEMENTS

- 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.
- Udemy, "Learn Ethical Hacking From Scratch"
- Passing the course, "Basics of information transmission and processing" with Prof. Michal Koucký.
- Passing the course, " Foundations of theoretical cryptography" with Prof. Pavel Hubacek.
- Theory and Practice of Blockchains 2019 Workshop, Aarhus, Denmark.

PUBLICATIONS

- S. M. Sedaghat, M. H. Ameri, J. Mohajeri, and M. R. Aref, "An efficient and secure Data Sharing in Smart Grid: ciphertext-policy Attribute-Based Signcryption.", accepted for 25th Iranian Conference on Electrical Engineering (ICEE2017), 2017.
- S. M. Sedaghat, M. H. Ameri, M. Delavar J. Mohajeri, and M. R. Aref, "An efficient and secure ciphertext-policy Attribute-Based Signcryption scheme for Smart Grid applications.", Transactions on Emerging Topics in Computing, Under Review. Available in https://iacr/2018/263.
- S. M. Sedaghat, P. Hubacek. "low-degree PRoximity testing for Algebraic Geometry codes- Interactive oracle proof based (PRAGI)", Under submision.
- S. M. Sedaghat, T. Krnak, P. Hubacek. "Committee agreement protocol based on anonymous verifiable random functions", Under submision.
- Peter Gazi, P. Hubacek, S. M. Sedaghat. " Blockchain Light verification", Under submision.
- S. M. Sedaghat, P. Hubacek. "An efficient and secure Access Policy Encryption scheme", Under submision.
- S. M. Sedaghat, R. Rabaninejhad, M. Ahmadian Attari and M. R. Aref. "An ID-Based Shared Data Integrity Auditing Protocol in Cloud Storage", Under submision.