Alireza Shirzad

Mobile: +98-911-737-1097 | **Mail**: alr.shirzad@gmail.com
Webpage: ee.sharif.edu/ alireza.shirzad | **Git**: github.com/alireza-shirzad

Education

Sharif University Of Technology (GPA=*4.00/4.00*, Rank=*2/9*) Tehran, Iran
Master of Secure Communications and Cryptography *2020 – ongoing*

Sharif University Of Technology (GPA=*3.53/4.00*) Tehran, Iran
Bachelor of Electrical Engineering, Minor in Computer science *2016 – 2020*

Research Interest

Applied Cryptography & Cryptanalysis
zk proofs, Proof of Computation, zkSNARKs
Network Security, Blockchain

Research & Internship Experience

Research Assistant(MS Thesis) 2020 – ongoing
Sharif University Of Technology *Tehran, Iran*
- Collaborating with Dr. Taraneh Eghlidosto implementing an efficient GKR proof system framework in Rust
- Researching about techniques to reduce prover time in SNARKs of large circuits

Researcher 2021 – 2022
Kara Group *Tehran, Iran*
- Reported the current Zero-Knowledge neural network techniques
- Worked on frameworks like ZEN, zkCNN, Rosetta

Researcher 2021 – 2021
Telefonica Telecommunication Company *Barcelona, Spain*
- Worked on implementing and performance measuring of cryptographic primitives on data plane
- We leverage P4 programmable switches

Research Assistant (BS Project) 2019 – 2020
Cloud-Native Telecommunication Lab *Tehran, Iran*
- Worked there for my B.S final project in collaboration with Dr Babak Khalaj and Dr Azad Ravanshid
- Setup OAI (Open Air Interface) and Flex-RAN testbed and tested our Network slicing policies

Work Experience

Lecturer 2021 – ongoing
Sharif ICT *Tehran, Iran*
- Teaching blockchain, cryptography and smart contracts
- Web3 development

Publications

Preprint

1. Goodarzi, S., Kayvanfar, V., Haji, A., & Shirzad, A. (2022). Cold supply chain planning including smart contracts: An intelligent blockchain-based approach. *arXiv moderation*.

Teaching Assistance Experience

- **Provable Security**
  Dr. Mahmoud Salmasizadehi
- **Security in IOT**
  Dr. Siavaosh Ahmadi
- **Linux/Python Lab**
  Dr. Matin Hashemi
- **Advanced Programming Lab**
  Dr. Matin Hashemi
- **Object Oriented Programming (2 times)**
  Dr. Bijan Vosoughi Vahdat,Dr. Matin Hashemi
- **Data Communication Network(2 times)**
  Dr Mohammadreza Pakravan
- **Signals and Systems(2 times)**
  Dr Babak Khalaj, Dr Hamid Behrouzi
- **Numerical Computation(2 times)**
  Dr Taraneh Eghlidos

Honors and Awards

- Granted membership of National Elite Foundation for seven consecutive years
- Ranked in the top 25% in B.S and Granted Master Scholarship, Sharif University of Technology: Link
- Ranked 32nd among 200000 participants in Iranian Nationwide Mathematics University Entrance Exam

Related Coursework (Cryptography & Network Security)

Course title	**Score**	**Course title**	**Score**
Cryptography Principles	*18.7/20*	Cryptography Mathematics	*18.4/20*
Provable Security	*19.7/20*	Advanced Cryptography	*18.7/20*
Blockchain and Cryptocurrencies	*17.9/20*	Network Security	*18.2/20*
Advanced Network Security	*18/20*	Cryptography Seminar	*18.4/20*
Lattice-Based Cryptography	*TBD*	Information theory and Coding	*TBD*

Technical Skills

Crypto&Blockchain: Circom, Zokrates, Solidity, Hardhat

Web/General Programming: Django, Flask(amature), React Js, Rust, Java, Matlab, Python, C/C++

Linux/Virtualization/VCS: Docker, Git, Vagrant, Bash Scripting, LPIC1&2

Talks & Reports

1. Shirzad, A. (2021b). *Deep packet inspection over encrypted traffic.* Retrieved from `https://alireza-shirzad.ir/doc/dpi.pptx` (Sharif Electrical Engineering Seminar Series)
2. Shirzad, A. (2022a). *Boomerang attacks on symmetric ciphers.* ppt,pdf(fa)
3. Shirzad, A. (2022b). *Secure verifiable computation.* pdf(fa)
4. Shirzad, A. (2021c). *zk-snarks.* ppt,pdf(fa)
5. Shirzad, A. (2021a). *Data plane programming, beyound openflow.* ppt,pdf(fa)
6. Shirzad, A. (2019). *Bitcoin game-theoretic equilibrium.* pdf(fa)

Service

- Pre-reviewer at The ISC International Journal of Information Security

References

Dr. Taraneh Eghlidos Webpage
Associate professor of applied mathematics, Sharif University of Technology *teghlidos@sharif.edu*

Dr. Mahmoud Salmasizadeh Webpage
Associate Professor Electronics Research Institute, Sharif University of Technology *Salmasi@sharif.ac.ir*

Dr. Bijan Vosoughi Vahdat Webpage
Assistant Professor of Electrical Engineering department, Sharif University of Technology *vahdat@sharif.edu*