Mohammadtaghi Badakhshan

Doctor of Philosophy		Email:	mbadakhshan@uwaterloo.ca
Applied Cryptographer (zkSNARK and PQC)		Personal Website:	taghi.io
Department of Electrical and Computer Engineering		Github:	github.com/mtbadakhshan
University of Waterloo		LinkedIn:	linkedin.com/in/mtbadakhshan
Waterloo, ON, Canada			

SUMMARY

Ph.D. with 4 years of specialization in **post-quantum** secure **zkSNARKs** and over 7 years of **blockchain** research experience. Contributed as both a team member and a leader to accelerate the Aurora post-quantum secure zkSNARK protocol by **40%** through optimization of **FFT algorithms** in **C++**. Conducted research on the design and implementation of **privacy-preserving** frameworks on Ethereum using zero-knowledge proofs.

TECHNICAL SKILLS

Languages: C/**C++**/C#, Python, **Rust**, SageMath, Bash, Solidity (Familiar: Java, Javascript, Verilog)
Libraries: libff, libiop, libsnark, libsodium, gf2x, bitpolymul, Bitcoin Core, Google benchmark, Google test
Tools: Docker, Git, CMake
Domains: zero-knowledge proofs (Aurora, Groth16, GKR, etc.), post-quantum cryptography (hash-based), abstract algebra, privacy-preserving protocol design, threat modeling, elliptic curve cryptography, and decentralized systems (Familiar: provable security, code-based, and lattice-based cryptogrpahy)

PROFESSIONAL EXPERIENCE

Research Internship (MITACS), BTQ Technologies Corp., Canada — May 2024 – Apr 2025

- Led a research team composed of a postdoctoral researcher and a master's student, to analyze and improve the Aurora **post-quantum secure zkSNARK** runtime, and delivered 3 technical reports.
- Pioneered novel **additive FFT** optimizations for zkSNARKs, resulting in a **40%** reduction in prover runtime for *Aurora* and *Ligero*.
- Implemented and benchmarked **additive FFT algorithms** in C, C++, and SageMath.

Research Assistant, University of Waterloo, Canada — Sep 2020 – Aug 2024

- Developed and threat-modeled a privacy-preserving ownership protocol for supply chains on Ethereum, implemented using **Aurora** and **Groth16** zkSNARKs in **C++** and **Solidity**.
- Designed and implemented application-specific zkSNARK circuits in C++ using the `libsnark` library.
- Introduced an arithmetic circuit for the **GKR protocol** to enhance efficiency of the Polaris zkSNARK.

Teaching Assistant, University of Waterloo, Canada — May 2021 - Apr 2024

- Conducted tutorial sessions and provided guidance to students for various courses, including Computer Security, Digital Circuits and Systems, Digital Computers, and Digital Computation.

EDUCATION

Ph.D. Computer Software Engineering. **University of Waterloo**, Canada — Jan 2021 – Jun 2025
Thesis: Accelerating Post-Quantum Secure zkSNARKs and Privacy-Preserving Frameworks. (GPA: 4/4)

M.Sc. Secure Communication and Cryptography. **University of Tehran**, Iran — Sep 2017 – Aug 2020
Thesis: Security Analysis of Lightweight Clients in a Blockchain Based Peer-to-Peer Network.(GPA: 3.6/4)

B.Sc. Electrical Engineering. **University of Tehran**, Iran. — Sep 2013 – Aug 2017
Project: Network Traffic Classification and Industrial Control System Intrusion Detection. (GPA: 3.6/4)

PUBLICATIONS

Accelerating Post-quantum Secure zkSNARKs by Optimizing Additive FFT (SAC 2025)
Evaluating the Integration of Aurora zkSNARK in the Zupply Framework (EnCyCriS 2025)
Ursa Minor: The Implementation Framework for Polaris (WAIFI 2024)
Privacy-Preserving Ownership Transfer (DePIN 2023)
Improvement on Bitcoin's Verifiable Public Randomness with Semi-Trusted Delegates (IST 2018)
Zupply: Anonymously Maintained Decentralized DAG Data Record Over Public Blockchains (Preprint)

TRAINING

XRPL Core Developer Bootcamp June 2025
Hands-on training on `rippled` source code for high-proficiency C++ developers

HONOR

Ripple Graduate Fellowship May 2023 - Apr 2024

HACKATHONS

ETHGlobal Waterloo Jun 2023
Finalist and Winner of *Hyperlane Best Use*
OlympiHacks May 2023
Winner of *Axelar GMP* for sending Interchain Messages / Tokens

PRESENTATIONS

Evaluating the Integration of Aurora zkSNARK in the Zupply Framework May 2025
6th International Workshop on Engineering and Cybersecurity of Critical Systems, Ottawa, Canada
Decentralized Anonymous Authenticated Data Storage Nov 2024
Waterloo Blockchain, University of Waterloo, Canada
Ursa Minor: The Implementation Framework for Polaris Jun 2024
International Workshop on the Arithmetic of Finite Fields, Ottawa, Canada
Privacy-Preserving Ownership Transfer Oct 2023
International Workshop on Decentralized Physical Infrastructure Networks, Virtual
Hands-On Introduction to zkSNARKs with Libsnark Mar 2023
Ripple Get-together, University of Waterloo, Canada

VOLUNTEER

Research Circle Coordinator, University of Waterloo Blockchain Club, Canada Jan 2024 - Dec 2024
Organized weekly research discussions for graduate and undergraduate blockchain enthusiasts.
Campus Ambassador, XRP Ledger, University of Waterloo, Canada Jan 2023 - Dec 2023
Collaborated in organizing Ripple Get-togethers for graduate students conducting blockchain research.
Event Director, Iranian Students' Association of Waterloo (ISAW), Canada Sep 2021 - Dec 2021
Led and coordinated cultural and social events for Iranian students at the University of Waterloo.
Chair, Student Branch of Iranian Society of Cryptology, University of Tehran, Iran Apr 2018 - Aug 2020
Led the organization of a workshop on blockchain technologies, focusing on Hyperledger.
Managing Director, JARYAN Electrical Engineering Student Magazine, Iran Aug 2016 - Feb 2018
Led an editorial team of 10+ members to publish two volumes of the magazine.