Mohammadtaghi Badakhshan

Doctor of Philosophy Candidate
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, ON, Canada

Email: mbadakhshan@uwaterloo.ca
mtbadakhshan@gmail.com
Personal Website: taghi.io
Github: github.com/mtbadakhshan
LinkedIn: linkedin.com/in/mtbadakhshan
Phone: (+1) 226 899-1954

EDUCATION

Ph.D. Computer Software Engineering. Jan 2021 – May 2025
Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada.
THESIS - Design and Implementation of a Privacy-Preserving Decentralized Framework and Accelerating Post-Quantum Secure zkSNARKs.

M.Sc. Secure Communication and Cryptography. Sep 2017 – Aug 2020
Department of Electrical and Computer Engineering, University of Tehran, Tehran, Iran.
THESIS - Security Analysis of a Blockchain Based Peer-to-Peer Network (Lightweight Clients).

B.Sc. Electrical Engineering. Sep 2013 – Aug 2017
Department of Electrical and Computer Engineering, University of Tehran, Tehran, Iran.
PROJECT - Network Traffic Classification and Industrial Control System (ICS) Intrusion Detection.

PROFESSIONAL EXPERIENCE

Internship (MITACS), BTQ Technologies Corp., Canada May 2024 – Apr 2025
- Optimized implementation and comparison of additive fast Fourier transform (FFT) algorithms in SageMath, C, and C++ .
- Accelerated post-quantum secure zkSNARKs (e.g., Aurora) using Cantor special basis and Cantor additive FFT.

Research Assistant, University of Waterloo, Canada Sep 2020 – Aug 2024
- Designed an anonymous authentication token and an unlinkable anonymous authentication token ownership transfer scheme for supply chain management applications over the Ethereum blockchain. Implemented the zero-knowledge prover algorithm using Groth16 and Aurora zkSNARKs in C++ and the verifier algorithm using Groth16 in Solidity.
- Developed an optimized arithmetic circuit for the GKR protocol, enhancing the efficiency of Polaris zkSNARKs.

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.

TECHNICAL SKILLS

Programming Languages: C/C++ /C#, Python, SageMath, Bash, Solidity (Familiar with: Rust, Java, Javascript, Verilog)
Libraries: libff, libiop, libsnark, NTL, bitpolymul
Cryptography and Security: zkSNARKs (Groth16, Aurora, GKR, etc.), post-quantum cryptography, finite fields, privacy-preserving protocol design, and decentralized systems (Familiar with: provable security)

PUBLICATIONS

- M. Badakhshan, G. Luo, T. Jandhyala, G. Gong, "Ursa Minor: The Implementation Framework for Polaris," Arithmetic of Finite Fields. WAIFI 2024. Lecture Notes in Computer Science, vol 15176. Springer, Cham. doi: 10.1007/978-3-031-81824-0_16
- M. Badakhshan, G. Gong, "Zupply: Anonymously Maintained Decentralized DAG Data Record Over Public Blockchains," TechRxiv, 2024, doi:10.36227/techrxiv.171821776.63453406/v1
- M. Badakhshan and G. Gong, "Privacy-Preserving Ownership Transfer: Challenges and An Outlined Solution Based on Zero-Knowledge Proofs," 2023 IEEE 9th World Forum on Internet of Things (WF-IoT), Aveiro, Portugal, 2023, pp. 1-9, doi: 10.1109/WF-IoT58464.2023.10539396.
- H. Yajam, E. Ebadi, M. Badakhshan and M. Akhaee, "Improvement on Bitcoin's Verifiable Public Randomness with Semi-Trusted Delegates," 2018 9th International Symposium on Telecommunications (IST), Tehran, Iran, 2018, pp. 53-57, doi: 10.1109/ISTEL.2018.8661008.

HONORS

Ripple Graduate Fellowship May 2023 - Apr 2024

HACKATHONS

ETHGlobal Waterloo Jun 2023
Winner of Hyperlane Best Use and ETHGlobal Waterloo 2023 Finalist

OlympiHacks May 2023
Winner of Axelar GMP for sending Interchain Messages / Tokens

PRESENTATIONS

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, Waterloo Blockchain Club Jan 2024 - Dec 2024
University of Waterloo, Canada

Campus Ambassador, XRP Ledger Jan 2023 - Dec 2023
University of Waterloo, Canada

Event Director, Iranian Students' Association of Waterloo (ISAW) Sep 2021 - Dec 2021
University of Waterloo, Canada

Chairman, Student Branch of Iranian Society of Cryptology Apr 2018 - Aug 2020
University of Tehran, Iran

Managing Director, JARYAN Electrical Engineering Student Magazine Aug 2016 - Feb 2018
University of Tehran, Iran