

Bohan Zhang

bohan.zhang@uwaterloo.ca • LinkedIn • GitHub • Mobile: (+1)2268998825

ABOUT

Experienced in security, cryptography, blockchain, AI, and 5G, with a strong aptitude for quickly mastering new technologies.

EDUCATION

Master of Mathematics, Computer Science *University of Waterloo, Canada (Fully-funded)* Sep 2024, GPA: 96/100

Advisor: Raouf Boutaba. Thesis: Mitigating Signaling Storms in 5G

Bachelor of Computer Science, Data Science *University of Waterloo, Canada (Dean's list)* Sep 2021, GPA: 91/100

Combinatorics and Optimization Minor

SKILLS

Languages | Python, Golang, Solidity, Java, Javascript, C, C++, SQL, R, Scala, Bash Script

Frameworks | PyTorch, Truffle, Docker, Kubernetes, Git, SimPy, Go-ethereum, Gurobi, Hadoop, Spark, Mininet, Android

Field Knowledge | Protocol Design, Cryptography, Blockchain, PKI, Code Audit, 5G, Visualization, Forecasting, UI

ACADEMIC EXPERIENCE

Graduate Research Assistant | *University of Waterloo, Full-time student* Sep 2022 - Present

- Investigated security threats in 5G protocols by analyzing over 200 3GPP documents, white papers, and research articles.
- Enhanced 5G authentication security by integrating blockchain technology, improving the protocol's resilience against DDoS attacks, and developing a Kubernetes emulation environment using free5GC and Geth.
- Designed a 5G LEO secure group handover protocol and built a discrete event simulator to show the performance.
- Designed a load-aware conditional handover protocol for 5G LEO, reducing signaling peak by 50%..
- Delivered persuasive and compelling conference-level presentations. Taught group members.

Teaching Assistant/Instructional Apprentice | *University of Waterloo, Part-time Contract* Sep 2022 - Present

- **Courses:** CS245(CS Logic), CS479/679(Neural Network), CS451/651(Distributed Computing), CS486/686(AI).

Undergraduate Research Assistant | *University of Waterloo, Part-time contract* Jan 2021 - Oct 2021

- Built a threshold signature ecosystem (Flexible Round-Optimized Schnorr Threshold Signatures) in Golang.
- Developed a solution for the Ethereum Front-Running problem (MEV) and built a prototype in Solidity (Fairblock).
- Reproduced and improved CamoGAN, which simulates the evolution of prey's camouflage using GAN.

INDUSTRIAL EXPERIENCE

Security Engineer | *QuantStamp Inc., Full-time permanent, remote* May 2022 - Sep 2022

- Performed security audits for 12 blockchain smart contract projects, including ERC-725 and Klap Finance.
- Discussed technical details, potential threats and fixing best practices with clients, including Lukso, Visa, KLAP, and HTC.
- Researched and extended Slither's capabilities to identify nine smart contract threats, including deviations from EIP-712 types and signature replay attacks. Developed guidelines for future implementation.

HONORS & ACCOLADES

Graduate Research Studentship | *72,000 CAD* 2022-2024

International Master's Award of Excellence | *12,500 CAD* 2022-2024

University of Waterloo International Student Entrance and President's Scholarship | *12,000 CAD* 2018

PUBLICATIONS

1. P Momeni, S Gorbunov, **B Zhang**, **FairBlock: Preventing Blockchain Front-running with Minimal Overheads**, EAI International Conference on Security and Privacy in Communication Systems (18th EAI SecureComm), 2022
2. **B Zhang**, P Zeinaty, N Limam, R Boutaba, **"Mitigating Signaling Storms in 5G with Blockchain-assisted 5GAKA"**, IEEE International Conference on Network and Service Management (19th IEEE CNSM), 2023
3. **B Zhang**, P Hu, A Azirani, M Salahuddin, D Barradas, N Limam, R Boutaba, **"Secure and Efficient Group Handover Protocol in 5G Non-Terrestrial Networks"** IEEE International Conference on Communication (IEEE ICC), 2024