Mohammed Alghazwi

Applied Cryptography · Security and Privacy Researcher

Groningen, Netherlands

(+31) 618895880 | m.ghazwi@gmail.com | www.mghazwi.com | mghazwi | mghazwi

Summary

Ph.D. candidate at the University of Groningen, graduating in December 2023. In my research, I study various cryptographic methods to identify their strengths and weaknesses in terms of security and privacy when applied in decentralized settings. Additionally, I develop protocols to improve these existing methods by combining cryptographic primitives with Blockchain and smart contracts. Prior to that, I earned an MSc. degree in Cybersecurity from RMIT University and a BSc. degree in Computer Science from the University of Auckland where I developed a strong background in software development and security analysis.

Education

Doctor of Philosophy (Ph.D.) - Computer Science *Nov 2019 - Dec 2023*

University of Groningen *Groningen, Netherlands*

- Applying cryptographic methods specifically Zero-Knowledge Proofs (ZKP) and Homomorphic encryption for secure and privacy-preserving sharing and processing private data (health and genomic data)
- Decentralized private computation using blockchain and smart contracts
- Self-sovereign identity, and identity privacy.

Master of Applied Science (MSc) - Cybersecurity *Mar 2014 - Dec 2015*

RMIT University *Melbourne, Australia*

- Thesis: Design of multimodal biometric authentication system on mobile environment for access to sensitive personal data using fido alliance standards *GPA: 3.3/4*

Bachelor of Science (BSc) in Computer Science *Feb 2010 - Sept 2013*

University of Auckland *Auckland, New Zealand*

Publications

Privacy-preserving Genome Analysis using Verifiable Off-Chain Computation. *2022*

ACM SIGSAC Conference on Computer and Communications Security

Blockchain for Genomics: a Systematic Literature Review. *2022*

Journal: Distributed Ledger Technologies - Research and Practice.

Academic Projects

2022 **Decentralized Private Genome Analysis using HE and ZKP,** Developed a set of protocols for performing statistical analysis on genome data in decentralized settings using Homomorphic encryption (HE) and zero-knowledge proofs (ZKP) in combination with a blockchain system

2021 **Data Sharing Consent for Health-Related Data Using Smart Contracts,** Our solution won the 1st place in IDASH - Privacy and Security Workshop

2021 **A Self-Sovereign Identity Framework for Patient-Centric Access Management,** Abstract and presentation were accepted at ICT-Open Workshop

2021 **Decentralized Electronic Voting System using Blockchain & Zero-Knowledge Proofs (ZKPs),** A project in collaboration with Blockchainlab Drenthe

Teaching

MSc Course: Advanced Topics in Privacy and Security *2020-2022*

University of Groningen

- Teaching activities include:
  - Lecture on decentralization, blockchain, smart contracts, and Self-Sovereign Identity.
  - Creating and supervising the lab on blockchain and smart contracts.
  - Providing student projects and evaluating the outcome.

Bachlor and Master Project Supervision *2020-2023*

University of Groningen

- Supervised 6 successful projects, 3 Master projects and 3 Bachelor projects.
  Description of these projects and outcome can be found on my personal website.

Technical Skills

Python, JavaScript, Rust, Solidity, Circom, Java, C, git.