Mohammed Alghazwi

Applied Cryptography · Security and Privacy Researcher

Groningen, Netherlands

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

Summary

Researcher specializing in applied cryptography and privacy-enhancing technologies. My work focuses on the design and implementation of various zero-knowledge proofs (ZKPs) for practical applications. I have also worked on related topics such as multi-party computation (MPC) and homomorphic encryption (HE).

Aside from my research, I'm an experienced software developer with a strong background in implementing cryptographic protocols in Rust. I'm also passionate about writing educational content and have experience in teaching and supervising students.

Experience

Institute of Free Technology (IFT) *Sept 2024 - current*

Applied Cryptography Researcher

- Research, design, implementation, and technical documentation of Zero-knowledge proof (ZKP) systems for remote auditing schemes for decentralized storage, specifically for the Codex project.
- Write specifications and design documentation.
- Perform security analysis and audit ZKP circuits

University of Groningen *Nov 2019 - Aug 2024*

Teaching Assistance and Student Supervision

- MSc Course: Advanced Topics in Privacy and Security. Teaching activities include:
  - Giving lectures on decentralization, blockchain, smart contracts, and Zero-Knowledge Proofs.
  - Creating and supervising the labs.
  - Providing student projects and evaluating the outcome.
- Supervised more than 10 successful student projects including 3 Master projects.
  Description of these projects and outcomes can be found on my personal website.

Education

Ph.D. - Computer Science *Nov 2019 - Aug 2024*

University of Groningen *Groningen, Netherlands*

- PhD thesis: Secure, privacy-preserving, and publicly verifiable collaborative data analysis

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 authentication protocol

BSc in Computer Science *Feb 2010 - Sept 2013*

University of Auckland *Auckland, New Zealand*

Publications

2024	**Collaborative CP-NIZKs: Modular, Composable Proofs for Distributed Secrets,** Under review - paper
2024	**VPAS: Publicly Verifiable and Privacy-Preserving Aggregate Statistics on Distributed Datasets,** Under review - paper
2023	**DARC: Decentralized Anonymous Researcher Credentials for Access to Federated Genomic Data,** International Workshop on Trends in Digital Identity (TDI), paper
2022	**Privacy-preserving Genome Analysis using Verifiable Off-Chain Computation (Poster),** ACM CCS Conference on Computer and Communications Security
2022	**Blockchain for Genomics: a Systematic Literature Review.,** Journal: Distributed Ledger Technologies - Research and Practice. Paper

Technical Skills

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

Selected Projects

2024 **Codex storage proof aggregation (code) ,** Researched, designed, and implemented custom Plonly2-based proof system and circuits for the Codex storage zk-proofs in Rust.

2024 **Collaborative CP-NIZK (code available in request) ,** Developed an MPC protocol in Rust (Arkworks) along with distributed (collaborative) Groth16, LegoGro16, and Bulletproofs by adapting these schemes into MPC

2023 **Distributed Verifiable Encryption (code) ,** Developed a distributed protocol for verifiable encryption in Rust (Arkworks) by extending the SAVER scheme with distributed key generation and key-switching protocols

2023 **In-Circuit Elgamal (Homomorphic) Encryption (code) ,** Developed an efficient In-Circuit Elgamal (Homomorphic) Encryption using Arkworks and Circom by optimizing the cryptographic operations done inside the zk-SNARKs circuit

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

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