Miguel Quaresma

LinkedIn | Github | Website
Email: miguelquaresma.w@gmail.com

Professional Experience

Max Planck Institute for Security and Privacy - PhD Student Feb 2021 – Present
Research on high-assurance post-quantum cryptography.

University of Melbourne - Visiting Researcher Oct 2023 – Dec 2023
Research on optimization of cryptographic implementations.

Goldman Sachs - Cyber Security Analyst Aug 2020 – Jan 2021
Responsible for penetration tests, cloud security and security research.

Aptoide - Security Engineer Intern Jul 2019 – Aug 2019
Responsible for developing a malware detection engine.

Closer Consulting - Software Engineer Intern Aug 2018
Fullstack development in NodeJS, .NET, Bootstrap and Angular.

Education

PhD in Cryptographic Engineering at Radboud University and Ruhr University Bochum Feb 2021 – Present
Supervised by Gilles Barthe and Peter Schwabe.

MSc in Computer Engineering at Universidade do Minho Sept 2018 – Jul 2020
Specialization: *Cryptography and Information Security*, *Parallel and Distributed Computing*
Thesis: "TrustZone based Attestation in Secure Runtime Verification in Embedded Systems"

BSc in Computer Engineering at Universidade do Minho, Braga Sept 2015 – Jun 2018

Publications

Formally verifying Kyber Episode V: Machine-checked IND-CCA security and correctness of ML-KEM in EasyCrypt, 2024, CRYPTO 2024 code | paper

Swoosh: Efficient Lattice-Based Non-Interactive Key Exchange, 2024, USENIX Security 2024 code | paper

Formally verifying Kyber Episode IV: Implementation Correctness, 2023, TCHES 2023 code | paper

Projects

Libjade: formally verified cryptographic library written in Jasmin.

Jasmin: framework designed for writing high-assurance and high-speed cryptography.

CryptOpt: optimizer for implementation of cryptographic primitives.

OPTEE: fork with attested computation capability for Trusted Applications running in the Secure World.

ARM Trusted Firmware: fork with support for attestation services via device specific certificate and encrypted signing key loaded at boot time.

High-speed Certified Crypto: fast and certified implementation of Keccak (SHA-3) using Jasmin and Easycrypt.

Key Skills

Cryptographic Engineering: Jasmin, CryptoLine
Formal Methods: EasyCrypt, Coq
Security: Yara, Androguard, BurpSuite, Wireshark
Programming Languages: Haskell, C/C++, Java, Python, Assembly (x86 and ARM), Rust
Performance Analysis: PAPI, OpenMP, OpenMPI, CUDA
Sofware Frameworks: NodeJS, DJango, Celery, Redis, .NET, Docker
Database Technologies: MySQL, SQL Server, PostgreSQL, Neo4j, MongoDB

Languages

Portuguese: Native proficiency, **English:** Full professional proficiency, **Spanish:** Limited working proficiency