

Miguel Quaresma

[LinkedIn](#) | [GitHub](#) | [Website](#)
Email: miguelquaresma.w@gmail.com

Professional Experience

Least Authority – Security and Cryptography Researcher & Engineer	May 2025 – Present
Max Planck Institute for Security and Privacy – PhD Student Research on high-assurance post-quantum cryptography.	Feb 2021 – Jun 2025
University of Melbourne – Visiting Researcher Research on optimization of cryptographic implementations.	Oct 2023 – Dec 2023
Goldman Sachs – Cyber Security Analyst Responsible for penetration tests, cloud security and security research.	Aug 2020 – Jan 2021
Aptoide – Security Engineer Intern Responsible for developing a malware detection engine.	Jul 2019 – Aug 2019
Closer Consulting – Software Engineer Intern Fullstack development in NodeJS, .NET, Bootstrap and Angular.	Aug 2018

Education

PhD in Cryptographic Engineering at Radboud University and Ruhr University Bochum Supervised by Gilles Barthe and Peter Schwabe.	Feb 2021 – Present
MSc in Computer Engineering at Universidade do Minho Specialization: <i>Cryptography and Information Security, Parallel and Distributed Computing</i> Thesis: “ TrustZone based Attestation in Secure Runtime Verification in Embedded Systems ”	Sept 2018 – Jul 2020
BSc in Computer Engineering at Universidade do Minho, Braga	Sept 2015 – Jun 2018

Publications

Jazzline: Composable CryptoLine functional correctness proofs for Jasmin programs , 2025, ACM CCS 2025 code paper	
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: added attested computation capability for Trusted Applications running in the Secure World.
ARM Trusted Firmware: added attestation services via boot-time device specific certificate and encrypted signing key.
High-speed Certified Crypto: fast and certified implementation of Keccak (SHA-3) using Jasmin and EasyCrypt.

Key Skills

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

Languages

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