João Diogo Duarte

PhD Student · Faculdade de Ciências da Universidade do Porto

(+351) 928 126 957 | joao@diogoduarte.pt | joaodduarte97

Education

Universidade do Porto
Porto, Portugal

Doctoral Program in Computer Science — *Oct. 2023 - PRESENT*

- Demonstrating security of post-quantum schemes and researching post-quantum migration of systems through the design, security proofs, verification and validation of optimized high-assurance implementations and specifications of PQC and hybrid protocols in the eAuthentication domain. The first publication was a collaborative process that lead to the introduction and rigorous security proofs a practical and efficient hybrid KEM to use during post-quantum migration. It has been submitted as an Internet-Draft to the IETF.

Royal Holloway, University of London
Egham, United Kingdom

Information Security MSc — *Sep. 2018 - Sept. 2019*

- Achieved a high level Distinction (86%).

University of Bath
Bath, United Kingdom

Computer Science BSc (Hons) — *Sep. 2015 - Jul. 2018*

- Achieved a First Class with Honours (70%).

St. Julian's School
Carcavelos, Portugal

International Baccalaureate — *Sep. 2013 - Jun. 2015*

- Maths HL: 6 | Computer Science HL: 6 | Physics HL: 5 | English Literature and Language SL: 6 | Business and Management SL: 6 | French B SL: 6.

Experience

TNO
The Hague, Netherlands

Junior Crypto Specialist — *Aug. 2021 - Aug. 2023*

- Worked within the Applied Crypto & Quantum Algorithms group where we applied the latest academic research to solve real-world issues using various domains in cryptography, such as computer-aided cryptography and post-quantum cryptography. This included research on the HAPKIDO project about migrating PKI to post-quantum cryptography and a detailed post-quantum cryptography migration manual that covers technical and organisational requirements. In HAPKIDO, I implemented ITU-T X.509 compliant hybrid certificates. We frequently collaborated with different departments and companies to employ other topics such as machine-learning to our projects.

Brightsight B.V
Delft, Netherlands

Junior Side Channel Analyst — *Sep. 2020 - Jun. 2021*

- Worked with in-house tools to perform various forms of side-channel attacks such as DPA, CPA, TA and deep-learning to break real-world systems. A report is then written describing and analysing the attack and its outcome.

Arm
Cambridge, UK

IT Security Graduate — *Sep. 2019 - Jul. 2020*

- Worked in the Vulnerability Management team, where I automated processes such as producing scorecards to further understand and prioritise vulnerabilities identified in Arm's infrastructure, applications and web applications. Also worked in the Enterprise Security Architecture team, where I helped write and develop security requirements for various domains across Arm and visualise these requirements.

Happy Code
Carcavelos, Portugal

Teacher — *Apr. 2018 - Sep. 2019*

- Taught weekly app development using MIT App Inventor 2 to children between the ages of 10 and 12 as well as Minecraft modding to children between the ages of 6 and 10. In these particularly difficult age groups, I managed to spark their interest in computer science and encouraged further learning at home.

CERN

Geneva, Switzerland

Intern

Jun. 2013

- Watched presentations about Computer Security and met with the Deputy Computer Security Officer who explained to me the details of his job. Also followed web tutorials on Python and configured Linux laptops

Skills

Programming Languages

- Computer-aided cryptography tools such as EasyCrypt and Jasmin.
- Experience working with cryptographic libraries, primarily BouncyCastle. Some experience with OpenSSL.
- Scripting in Python/SageMath and software development with Java. Experience with Go, Matlab and C.

Information Security

- Provable security of post-quantum cryptographic schemes.
- Migration to post-quantum cryptography.
- Knowledge of common side channel analysis attack vectors such as DPA, TA, TDPA.
- Experience in enterprise security and network security.
- Worked with security software such as Kenna, Netsparker and Twistlock.

Other

- Windows, Linux, Git, Gradle, Maven, Microsoft Office, LaTeX.

Extracurricular Activity

Dierenasiel en pension 't Julialaantje

Rijswijk, The Netherlands

Volunteer

Jan. 2022 - Jun. 2022

- Helped take care of the dogs in the shelter, which included walking, playing and cleaning their kennels.

RH100

Egham, United Kingdom

RH100 Student Panelist

Oct. 2018 - Sep. 2019

RH100 is a focus group that is made of 100 students panellists who all study in Royal Holloway. This panel ensures that a range of student views are taken into consideration when the College makes strategic decisions.

Bibliography and Code

Scientific papers and publications

- Barbosa, M., Connolly, D., Duarte, J. D., Kaiser, A., Schwabe, P., Varner, K. & Westerbaan, B. *X-Wing: The Hybrid KEM You've Been Looking For* Cryptology ePrint Archive, Paper 2024/039. `https://eprint.iacr.org/2024/039`. 2024.
- Duarte, J. D. *On the Complexity and Admissible Parameters of the Crossbred Algorithm in* $\mathbb{F}_{q\geq 2}$ Cryptology ePrint Archive, Paper 2023/1664 `https://eprint.iacr.org/2023/1664`. 2023.
- Amadori, A., Duarte, J. D. & Spini, G. Literature Overview of Public-Key Infrastructures, with Focus on Quantum-Safe Variants Deliverable 4.1, HAPKIDO Project. *TNO Repository*, 28. `https://repository.tno.nl/SingleDoc?find=UID%20d33a3b1a-1a7b-4367-9b6d-1e746db2d96a`. 2022.
- Attema, T., Duarte, J. D., Dunning, V., van der Schoot, W., Stevens, M. & Lequesne, M. The PQC Migration Handbook: Guidelines for Migration to Post-quantum Cryptograpy. *TNO Repository*, 62. `62.https://ir.cwi.nl/pub/32988/`. 2023.

Code

- Duarte J. D. *Optimal Parameters and Complexity for Crossbred Algorithm*. version v1.0.0. January 2024. `https://github.com/JoaoDDuarte/Optimal-Parameters-and-Complexity-for-Crossbred-Algorithm/`.
- TNO MPC Lab. *TNO MPC Lab - MPyC - Statistics*. version v0.1.1. May 2022. `https://github.com/TNO-MPC/mpyc.statistics`.
- TNO MPC Lab. *TNO MPC Lab - MPyC - Secure Learning*. version v1.1.1. May 2022. `https://github.com/TNO-MPC/mpyc.secure_learning`.