JOÃO RODRIGUES

joaocpereirar@gmail.com +351 969817624 joao-cp-rodrigues JoaoCPereira joaorodrigues.pages.dev

Hello, my name is João Rodrigues, and I have a solid background in **Software Engineer**, having completed my **Bachelor's degree in Computer Science** at the University of Minho in 2021. Currently, I am in the final stage of my **Master's degree in Computer Science**, specializing in **Post-Quantum Cryptography**, **Information Security**, and **Computer Graphics**.

EXPERIENCE

Dissertation

Universidade do Minho

2022-2023 Braga, Portugal

My master's thesis focused on examining recent advancements in **post-quantum cryptography**, specifically exploring the Post-Quantum Cryptography project by the **NIST**. I set up a working environment to handle algorithms with **cryptographic keys** and **certificates** larger than traditional security algorithms, achieving this by replacing the standard operating system's OpenSSL with **OQS-OpenSSL**. Using the **LiboQS** library in **C**, I integrated post-quantum algorithms into the **Cryptography** and **AsynIO** libraries in **Python**. In the comparative analysis, I assessed the security and performance of each algorithm and examined the efficiency loss when using Python compared to C. Additionally, I investigated advancements in **smart cards**, focusing on the **Portuguese National Identity Card**. This exploration covered limitations such as **RAM size**, **lack of accelerators** for new algorithms, large-scale implementation, and **masking techniques**.

Academic Environment

Universidade do Minho

2017-2022 Braga, Portugal

Throughout this five-year period, I engaged in various projects, both independently and collaboratively. These projects encompassed tasks such as **planning**, **design**, **implementation**, and **monitoring**, spanning diverse areas including **SQL** (MySQL) and **NoSQL** (Neo4j) database management, object-oriented programming in **Java** and **C++**, parallel computing, functional programming, imperative programming, turing machine and formal languages, language processing, and compilers. During this time frame, I advanced my mathematical proficiency in numerical **analysis**, **logic**, **geometry**, and **algebra**.

ACADEMIC EDUCATION

Master of Computer Science

Universidade do Minho

2021 – Present Braga, Portugal

Cryptography and Information Security

- Identification of risks and security requirements for systems;
- Development of threat models in software systems;
- Classical Cryptography, including cyclic groups, elliptic curves, knowledge proofs, and digital signatures;
- Post-Quantum Cryptography, Lattice-Based, Hash-Based;

Computer Graphics

- Models for local and global illumination, empirical and physics-based (Phong, Cook-Torrance, Ward);
- Light transport mechanisms, BRDF, and the rendering equation;
- Programming of the graphics pipeline using languages like GLSL;
- Deep Learning Networks for image generation and object recognition in images;

Bachelor's Degree in Computer Science

Universidade do Minho

2017 – 2021 Braga, Portugal

- Apply different computing paradigms to craft innovative solutions, such as, multi-clause function definitions and polymorphism;
- Develop robust computational solutions, writing code across various programming languages, in **Python**, **C**, **C++**, **Java**;
- Utilizing efficient data structures and designing algorithms upon them (**AVL trees**, **hash tables**, and **heaps**);
- Strategically plan, implement, and oversee dynamic database systems, **SQL** (**MySQL**), **NoSQL** (**Neo4j** and **MongoDB**);
- Knowledge of **Graph Theory** in the modeling and resolution of problems;
- Apply advanced calculation, logical reasoning, and mathematical insight to construct compelling arguments, including formal proofs;

PROGRAMMING SKILLS

C C++ Python Java SQL UML Diagramas

Linux Git MySQL MongoDB SQLServer Neo4j

LANGUAGES

Português (idioma nativo)

Italiano (C1)

Inglês (B1)