PhD fellowship on Quantum-Resistant Trusted Platform Modules

We are seeking applications for PhD students to work in the Signal Processing System Group of INESC-ID on the EU Horizon2020-funded FutureTPM project.

The goal of FutureTPM is to design a quantum-resistant (QR) Trusted Platform Module (TPM) by designing and developing QR cryptographic algorithms suitable for integration in a TPM. The algorithm design will be accompanied with implementations and performance and security evaluations, as well as formal security analyses in the full range of TPM environments: hardware, software and virtual. The lead users will be in the online banking, activity tracking and device management domains, which will provide environments and applications to validate the FutureTPM framework.

Applicants should have expertise in one or more of the following topics: digital system design, computer architecture, cryptography and formal analysis.

Enquiries can be made to Professor Leonel Sousa (las@inesc-id.pt)

INESC-ID

Rua Alves Redol, 9
1000-029 Lisboa
Portugal

E-mail address: las@inesc-id.pt