General information

Company name *INESC-ID*

Web site *http://www.inesc-id.pt/*

Contact name *Paulo Martins (PhD Student) / Leonel Sousa (Senior Researcher)*

Email *paulo.sergio@netcabo.pt / las@inesc-id.pt*

Telephone number *+351968548205 / +351969737935*

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ **Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography**	Y
○ **Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices**	Y
○ Authenticated encrypted token research for mobile payment solution	N
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	N
○ **New techniques, such as quantum safe cryptography, which are secure from quantum computers**	Y
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	N

Competencies

- *Organisation competencies*
  - *Excellent Research*
  - *Integration with Advanced Education*
  - *Experience in Technology-Transference*

- *Organisation experience in the European project*
  - *Ongoing European Projects:*
    - *Personalised Centralized Authentication System (PCAS)*
    - *Towards the dependable cloud: Building the foundations for tomorrow (DependableCloud)*
    - *Trustful hyper-linked entities in dynamic networks (reThink)*

- *The skills you can bring*
  - *Expertise in Computer Architectures*
  - *Experience in Developing Highly Performant Cryptography*

inesc id lisboa

Project idea

- *Alternative number representations have been used with RSA and ECC*
  - *e.g. Residue Number System*
    - *High-throughput*
    - *Improve resistence against side-channel attacks*
- *Extend these ideas to Post-Quantum Cryptosystems, such as GGH*
- *Exploit emerging High Performance Computing platforms, such as*
  - *GP-GPUs*
  - *FPGAs*