PhD thesis proposal in **post-quantum cryptography**.

Subject:
Adaptation of post-quantum primitives to constrained environments and FPGA implementation.

Start date:
November 2021

Background:
In late 2016, US National Institute of Standards and Technology (NIST) issued a call for proposals for the standardization of **cryptographic systems** resistant to a **quantum computer** for encryption, key exchange and signature primitives. The standardization process is currently in its third phase.

Each submission comes with a software implementation, targeting standard security levels for widespread applications, such as e-commerce.

Topic:
During this thesis, the successful candidate will study code-based and/or lattice-based proposals, and propose modifications to the protocols (resulting thus in alternative schemes with new proofs to be provided etc.) so that their hardware implementation can be improved. The candidate will then propose such implementations on a commodity Field Programmable Gate Array (FPGA). The development will be done in C and High-Level Synthesis will be used to transform automatically the C implementation into VHDL. As a consequence the candidate does not need to be proficient in VHDL.

Partner company:
The thesis is financed by **Atos** company, through « convention industrielle de formation par la recherche » (CIFRE).

How to apply:
Applicants should express their interest before July 15th- 23h59 (CEST time) by email to :

* carlos.aguilar-melchor@isae-supaero.fr

* arnaud.dion@isae-supaero.fr

* philippe.gaborit@unilim.fr