Implementation of Post Quantum Cryptographic algorithms using High Level Synthesis tools on FPGAs

Keywords: High Level Synthesis, Hardware attacks, FPGA, Applied Cryptography, Security

Many aspects of our current life rely on the exchange of data through electronic media. Powerful encryption algorithms guarantee the security, privacy and authentication of these exchanges. Nevertheless, those algorithms are not secure under an attack by a quantum computer.

The main goal of the proposed internship is to implement one or more post quantum algorithms on Field Programmable Gate Arrays (FPGAs) and verify its correct functionality. For the implementation of the algorithm the intern will use a High Level Synthesis tool of Mentor Graphics called Catapult. The cryptographic algorithm will be implemented in C or C++ and synthesized using Catapult to obtain a Register Transfer Level description of the digital circuit in either VHDL or Verilog. Then the design will be implemented on FPGA using Xilinx Tools.

This internship offers the opportunity to work in the development of secure post quantum cryptographic accelerators within the field of security & applied cryptography. It will take place at the LCIS Laboratory of Grenoble INP at Valence (France) with duration of **six months**.

Applicants must be enrolled in the 5th year of an Applied Mathematics and/or Physics five year degree or to a master degree in the same fields. In order to be able to conduct this project, the candidate must have:

- Good mathematical background to be able to handle Post-Quantum Cryptography mathematics
- Background using C and/or C++
- Willingness to learn the flow of High Level Synthesis Tools and FPGA implementation flows
- A good command of the English language will be appreciated.

The intern will be paid ~550 euros per month by the LCIS Lab.
An Erasmus+ (Erasmus for internship) agreement with the Home University of the candidate is possible (if the Home University agrees) and the Erasmus funding can be extra to the 550 euros per month paid by the LCIS lab.

Bibliography:

- Post-Quantum Cryptography 2009 Edition – Springer – Daniel J. Bernstein (Editor), Johannes Buchmann (Editor), Erik Dahmen (Editor)

Contact:
Athanasios PAPADIMITRIOU
athanasios.papadimitriou@lcis.grenoble-inp.fr