Cybersecurity Institute
Univ. Grenoble Alpes

INSTITUT FOURIER

LCIS
Laboratoire de Conception et d'Intégration des Systèmes

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

Reference	CYBERINSTITUTE-INT-19006
Description	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. However, those algorithms are not secure under an attack by a quantum computer. The main goal of the proposed internship is to contribute to the evaluation of post quantum algorithms qualified to second round of the NIST call for standardization of Post Quantum Cryptography algorithms by using HLS design tools. The internship objective is – for a given algorithm – to propose a HLS description in order to finally get a hardware implementation which will be used to characterize both the implementation properties of the algorithm and its security properties. 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. Within the Grenoble Alpes Cybersecurity Institute, this internship offers the opportunity to work in the development of secure post quantum cryptographic accelerators within the field of security & applied cryptography.
Prerequisites	Applicants must be enrolled in a master or the last year of a 5-year diploma degree on Applied Mathematics, Applied Physics or Electrical engineering. 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 use of the english language will be appreciated. *Bibliography* • Post-Quantum Cryptography 2009 Edition – *Springer* – Daniel J. Bernstein (Editor), Johannes Buchmann (Editor), Erik Dahmen (Editor)

Tutors	Athanasios Papadimitriou
Applications	Please send your resume, application letter with two recommendations (including education director), first year master's degree grades (mandatory) and second year grades (if possible) to cyberalps-contact@univ-grenoble-alpes.fr For more information on the internship, please contact athanasios.papadimitriou@lcis.grenoble-inp.fr
Location	LCIS Laboratory, Valence (France)
Starting date	February 2019
Duration	5 to 6 months
Allowance	In accordance with existing regulations (approx. 560€/month). Part of travel expenses can be covered.

financed by
IDEX Université Grenoble Alpes