



## Internship: Development of a FPGA emulation-based fault injection tool for RTL designs

<b>Reference</b>	CYBERINSTITUTE-INT-19004
<b>Description</b>	<p>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 implemented in electronic devices that may be the target of attacks despite their proven robustness. Several means of attacking integrated circuits are reported in the literature. Among them, fault attacks and side channel attacks are important and effective means to bypass security mechanisms.</p> <p>The main goal of the proposed internship is to implement an emulation based fault injection tool for RTL implementations. Such evaluation techniques are important in order to provide circuit designers with the capability to evaluate a secure design and to integrate appropriate countermeasures. The internship student will have the opportunity to take part in the development of digital circuits on FPGA and to implement a fault injection tool for the evaluation of state of the art cryptographic implementations and modern RISC-V processors. The internship will include:</p> <ul style="list-style-type: none"> <li>• Bibliography on state of the art fault injection techniques</li> <li>• Development of a demonstrator including the capability to inject single-bit and multi-bit faults to RTL implementations running on an FPGA</li> <li>• Development of monitoring capabilities to analyze the fault propagation into a complex architectures and to quantify the number of silent faults</li> <li>• The intern will then perform fault injection campaigns on specific secure circuits and applications</li> </ul> <p>Within the Grenoble Alpes Cybersecurity Institute, this internship offers the opportunity to work on the development of secure circuit evaluation tools within the field of hardware security.</p>
<b>Prerequisites</b>	Applicants must be enrolled in an electronics engineering degree. In order to be able to conduct this project, the candidate will have a strong knowledge in digital circuit design on FPGA. A good use of the english language will be appreciated.

<b>Tutors</b>	Vincent Beroulle, Athanasios Papadimitriou
<b>Applications</b>	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 <a href="mailto:cyberalps-contact@univ-grenoble-alpes.fr">cyberalps-contact@univ-grenoble-alpes.fr</a> For more information on the internship, please contact <a href="mailto:athanasios.papadimitriou@lcis.grenoble-inp.fr">athanasios.papadimitriou@lcis.grenoble-inp.fr</a>
<b>Location</b>	LCIS Laboratory, Valence (France)
<b>Starting date</b>	February 2019
<b>Duration</b>	5 to 6 months
<b>Allowance</b>	In accordance with existing regulations (approx. 560€/month). Part of travel expenses can be covered.

