Development of an FPGA fault injection emulation platform for the evaluation of secure RTL designs and processor architectures against fault attacks

Keywords: Digital IC design, Fault attack, Laser Attack, Emulation, FPGA, Hardware 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 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 have been reported to be important and effective means to perform attacks. The principle is to use fault injection equipment, as lasers or electromagnetic pulses to induce an erroneous behavior.

The main goal of the proposed internship is to assist to the implementation of a fault injection emulation platform, in order to perform accelerated fault injection campaigns, at the Register Transfer Level of abstraction. The modeling of such attacks at RTL is important in order to provide to circuit designers the capability to evaluate a circuit early in the design stage and avoid costly and time-consuming design iterations. The internship student will have the opportunity to take part in the development of an FPGA based fault emulation platform and perform fault injection campaigns to state of the art cryptographic implementations as well as to RISC-V processor implementations. Concerning RISC-V evaluation the fault injection platform should also be able to evaluate the effect of each fault on the functionality of the processor. Additionally the student will have the opportunity to use existing or define new fault models and characterize the resilience of cryptographic implementations according to these models and compare. Experience will also be gained by the student in CAD development tools and methods including: automatic testbench generation and VHDL manipulation tools.

This internship offers the opportunity to work in the development of fault injection tools and fault modeling applied to the field of hardware security. It will take place at the LCIS Laboratory of Grenoble INP at Valence (France) with a duration of six months. This work will take place in the framework of a European research project including multiple partners, from France, Spain and Germany both from academia and industry, including ST Microelectronics.

Applicants must be enrolled in a Master's degree or 5-year diploma degree in Microelectronics, Applied Physics, Embedded systems or Computer Science. In order to be able to conduct this project, the candidate will have knowledge in digital circuit design and in particular: VHDL or Verilog, FPGA, C or C++ and MATLAB. Experience with cryptographic devices and hardware security will be a plus and a good command of the English language will be appreciated.

Contact and Application by email to:

Athanasios PAPADIMITRIOU

athanasios.papadimitriou@lcis.grenoble-inp.fr

Please join to your application: CV and a short motivation letter