Internship Position

Development of a fault injection platform towards the modeling of laser attacks against secure ICs at the Register Transfer Level

Keywords: Digital IC design, Fault attack, Laser Attack, Electronic Design Automation

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, laser illumination of the device has been reported to be one important and effective mean to perform attacks. The principle is to illuminate the circuit by mean of a laser and then to induce an erroneous behavior.

The main goal of the proposed internship is to assist to the implementation of a fault injection platform, in order to perform fault injection campaigns, according to Laser Attacks, 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 fault simulation and emulation platforms and perform fault injection campaigns to state of the art cryptographic implementations. Additionally the results of the RTL analysis will have to be compared with gate level pre-layout and post-layout fault injection campaigns (28nm technology). Experience will also be gained by the student in CAD development tools and methods including: automatic testbench generation, VHDL manipulation tools and early design stage approximations. Furthermore the results of this work will aid in the refinement of the proposed Laser Fault Modeling methodology.

This internship offers the opportunity to work in CAD development 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 minimum duration of five months.

Applicants must be enrolled in a Master's 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, FPGA, good knowledge of C++, experience with IC design tools 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