PhD Position: FPGA Emulation of Laser Attacks Against Secure IC

Keywords: *Hardware Security, Digital IC design, Fault attack, Laser Attack, FPGA prototyping*

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 (for instance analysis of the correlation between the processed data and power consumption). 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. For instance, in so-called Differential Fault Analysis (DFA), an attacker can deduce the secret key used in the crypto-algorithms by comparing the faulty result and the correct one. Other types of attacks exist, also based on fault injection but not requiring a differential analysis; the safe error attacks or clocks attacks are such examples.

The main goal of the PhD thesis is to provide efficient CAD tools to secure circuit designers in order to evaluate counter-measures against such laser attacks early in the design process. The PhD thesis will be driven by two Grenoble INP laboratories: LCIS and TIMA. The main location is the LCIS at Valence (France). The work will be carried out in the frame of a collaborative project involving several other partners, including STMicroelectronics.

The PhD student will develop high level models of laser effects capable of emulating any laser attacks according to experimental results (other partners of the project will be in charge of laser attacks characterization on state of the art STMicroelectronics IC). For instance, RT level models of laser effects will be developed. Such model will then either be used for simulation or FPGA emulation in order to evaluate the robustness of a circuit at the RT level development stage. The PhD student will be in charge of integrating his models in CAD tools in order to propose a complete evaluation platform. Also, in order to accelerate the evaluation process, emulation will be taken into account: generic tools are already available in LCIS and TIMA and they will be refined and adapted.

Another goal is to anticipate new attacks based on the effects on advanced technologies and thus to propose proper counter-measures for future circuits. The PhD student will use the developed platform in order to propose and validate countermeasures against laser attacks.

This project offers the opportunity to work in the growing field of hardware security. Indeed, many SOC used for wireless communications or set top box require an increase of the security level to insure robust and safe data exchange. SOC designers are thus more and more looking for CAD tools able to evaluate the security level of their system under design.

Applicants must hold a Master's degree in Microelectronics, 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, C, scripts, SOPC architecture, FPGA, microprocessor based systems, embedded software.

Contact and Application by email to: David HELY, david.hely@lcis.grenoble-inp.fr
Please join to your application: Covers letters + Resume + Master marks and ranking + References