FPGA Emulation of Laser Attacks Against Secure Deep Submicron Integrated Circuits

A. Papadimitriou[1], D. Hély[1], V. Beroulle[1], P. Maistri[2], R. Leveugle[2]
Univ. Grenoble Alpes, LCIS[1] and TIMA[2]
50, rue Barthélémy de Laffemas BP54 26902 Valence, France
Email: Athanasios.Papadimitriou@lcis.grenoble-inp.fr http://lcis.grenoble-inp.fr

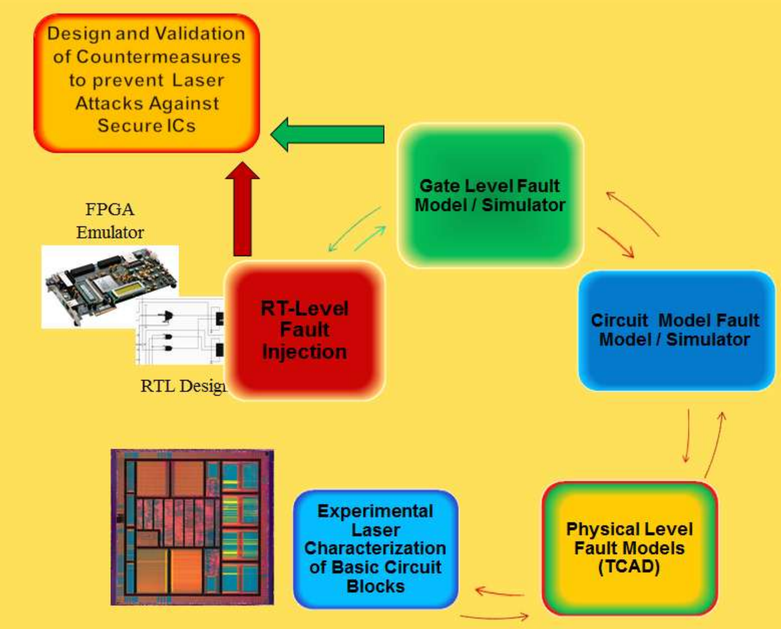
Summary

Register Transfer - Level Laser Fault Injection Modeling and the implementation of a Simulation – Emulation Platform, for the Evaluation of Countermeasures for Cryptographic ASICs

Introduction

- **Laser Fault Injection (LFI) enables attackers to perform fault injection in Cryptographic circuits characterized by:**
  - High precision locality
  - Accurate timing
  - High occurrence probability of faults
- **Laser Fault injection Modeling in the RT-Level provides evaluation of Security ASICs early in the design flow**
  - Avoidance of costly feedback runs
  - Fault injection close to the design process
  - Efficient Design and evaluation of countermeasures

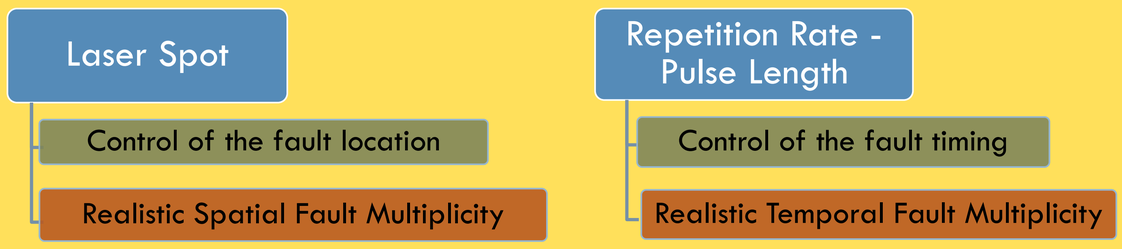
LIESSE Project



Fault Modeling

Classical approaches

- **Single Bit-flipping**
  - Originates from SEU resulting from high energy particles with the assumption that the deposited charge affects a single flip-flop
- **Time consuming analysis for Multiple Bit-Flipping, even for circuits of moderate complexity, leads to the simplification of the models.**
- **Laser Fault Injection is approached with classical fault models, which are not well adapted to new technology IC sizes, and generic simulator or emulator architectures**



Our Approach

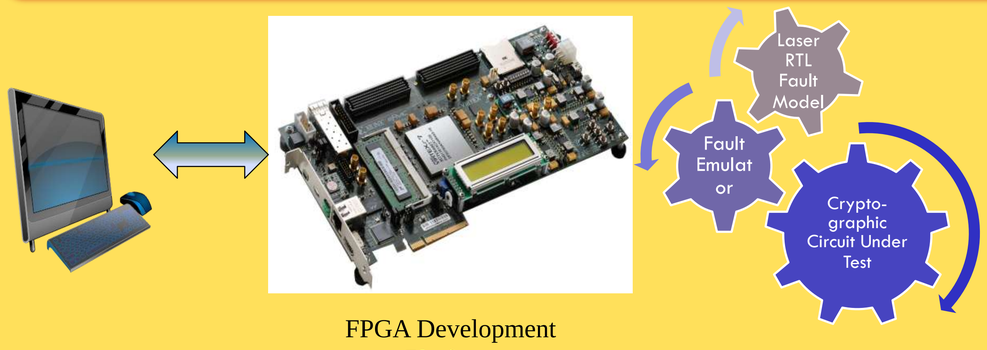
- **Reduction of the gap between the characteristics of the laser beam and classical fault models (SEU, SET) for recent semiconductor technology nodes (28nm)**
- **Testing and Refinement of the Model by evaluation with a gate-level fault simulator developed within the project**
- **Validation of the model by performing fault injections on state of the art cryptographic circuits**
  - **Advantages : Early in, and close to, the design flow, faster than a gate level model**
  - **Challenges : Maintain the necessary accuracy besides the lacking of synthesis and placement information**

Fault Simulator & Emulator

Emulation based fault injection

- **Utilization of powerful emulation techniques in FPGA platforms**
  - **Run Time – Dynamic FPGA Reconfiguration**
  - **Instrumentation with RTL code mutation**
- **Goals**
  - **Observability maximization**
  - **Fault Injection Campaign duration reduction**

Thus making feasible the application of a realistic laser fault model to the ASIC under analysis including the accuracy and complexity it requires



FPGA Development Platform

Design and Validation of Countermeasures

- **The design and integration of efficient countermeasures in a cryptographic circuit against an attack depends highly on the means available to validate them early in the design stage**
- **Therefore the RTL analysis tools will provide the means to efficiently expose vulnerabilities of security circuits, and at the same time assist the implementation of both defensive and preventive mechanisms**