Side-Channel improvement by laser stimulation

Jerome Di Battista , Bruno Rouzeyre,
Lionel Torres, Jean-Christophe Courrege

Abstract

The purpose of failure analysis is to locate the source of a defect in order to characterize it, using different techniques (light emission, electromagnetic emission, laser stimulation, ...). A part of my research is to find how it is possible to use the failure analysis tools and methods for security purposes. During cryptarchi 2009, I presented the possibility to use the leakage due to the light emitted during normal operation of a CMOS circuit, to set up a successfull attack on a part of a DES cipher algorithm implemented on an FPGA.
In this talk a second method based on laser stimulation is presented. Indeed, Sergei Skorobogatov demonstrates the possibility to increase the power consumption of a SRAM cell in a microcontroller, by applying a photocurrent on its transistors. The experiment presented here, consist to extend the Skorobogatov method's to a DES cipher implemented on an FPGA in order to improve the "traditional" side-channel attack by injecting a photocurrent on a chosen specific area (contain SBOXs, XOR operation...). This additional current should increase the consumption of the circuit during the algorithm encryption, and thus improve the attack by reducing the number of power consumption acquisitions.