

Side-Channel Improvement by Laser Stimulation

Jérôme Di Battista, Philippe Perdu, Jc Courrège, Bruno Rouzeyre, Lionel
Torres

► **To cite this version:**

Jérôme Di Battista, Philippe Perdu, Jc Courrège, Bruno Rouzeyre, Lionel Torres. Side-Channel Improvement by Laser Stimulation. Crypt'Archi'10: 8th Workshop on Cryptographic Architectures, Jun 2010, France. pp.N/A, 2010, <<http://labh-curien.univ-st-etienne.fr/cryptarchi/workshop10/index.html>>. <lirmm-00575124>

HAL Id: lirmm-00575124

<https://hal-lirmm.ccsd.cnrs.fr/lirmm-00575124>

Submitted on 9 Mar 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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 successful 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.