2011 Workshop on Fault Diagnosis and Tolerance in Cryptography

(FDTC 2011)

Nara, Japan
28 September 2011
2011 Workshop on Fault Diagnosis and Tolerance in Cryptography
FDTC 2011
Table of Contents

Invited Paper
The Fault Attack Jungle - A Classification Model to Guide You .........................................................3
Ingrid Verbauwhede, Duško Karaklajić, and Jörn-Marc Schmidt

Session 1: Fault Attacks on Elliptic Curve Cryptosystems
Fault Sensitivity Analysis Against Elliptic Curve Cryptosystems .........................................................11
Hikaru Sakamoto, Yang Li, Kazuo Ohta, and Kazuo Sakiyama
A Cost-Effective FPGA-based Fault Simulation Environment ...............................................................21
Angelika Janning, Johann Heyszl, Frederic Stumpf, and Georg Sigl

Session 2: Differential Fault Attacks on Symmetric Cryptosystems
A Differential Fault Analysis on AES Key Schedule Using Single Fault ...............................................35
Sk. Subidh Ali and Debdeep Mukhopadhyay
From AES-128 to AES-192 and AES-256, How to Adapt Differential Fault Analysis
Attacks on Key Expansion ..................................................................................................................43
Noémie Floissac and Yann L’Hyver
Differential Fault Analysis on the SHA1 Compression Function ............................................................54
Ludger Hemme and Lars Hoffmann

Invited Paper
Fault Injection, A Fast Moving Target in Evaluations ...........................................................................65
Rob Bekkers and Hans König
Session 3: Algebraic Fault Detection

On Protecting Cryptographic Applications Against Fault Attacks Using Residue Codes ..................................................69
  Kazim Yumbul, Serdar Süer Erdem, and Erkay Savaş

A High-Performance Fault Diagnosis Approach for the AES SubBytes Utilizing Mixed Bases .................................................................80
  Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh

Session 4: Fault Injection in Practice

Practical Optical Fault Injection on Secure Microcontrollers ...........................................................................................................91
  Jasper G.J. van Woudenberg, Marc F. Witteman, and Federico Menarini

Local and Direct EM Injection of Power Into CMOS Integrated Circuits .........................................................................................100
  F. Poucheret, K. Tobich, M. Lisarty, L. Chusseauz, B. Robissonx, and P. Maurine

An In-depth and Black-box Characterization of the Effects of Clock Glitches on 8-bit MCUs ..........................................................................................105
  Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede

Author Index ..........................................................................................................................................................................................115