

# **2011 Workshop on Fault Diagnosis and Tolerance in Cryptography**

**(FDTC 2011)**

**Nara, Japan  
28 September 2011**



**IEEE Catalog Number: CFP1186C-PRT  
ISBN: 978-1-4577-1463-4**

# 2011 Workshop on Fault Diagnosis and Tolerance in Cryptography

## FDTC 2011

### Table of Contents

Preface.....	vii
Program Committee.....	ix
Acknowledgments.....	x
Contact Information.....	xi

---

#### Invited Paper

The Fault Attack Jungle - A Classification Model to Guide You .....	3
<i>Ingrid Verbauwhede, Duško Karaklajić, and Jörn-Marc Schmidt</i>	

#### Session 1: Fault Attacks on Elliptic Curve Cryptosystems

Fault Sensitivity Analysis Against Elliptic Curve Cryptosystems .....	11
<i>Hikaru Sakamoto, Yang Li, Kazuo Ohta, and Kazuo Sakiyama</i>	
A Cost-Effective FPGA-based Fault Simulation Environment .....	21
<i>Angelika Janning, Johann Heyszl, Frederic Stumpf, and Georg Sigl</i>	

#### Session 2: Differential Fault Attacks on Symmetric Cryptosystems

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

#### Invited Paper

Fault Injection, A Fast Moving Target in Evaluations .....	65
<i>Rob Bekkers and Hans König</i>	

### **Session 3: Algebraic Fault Detection**

On Protecting Cryptographic Applications Against Fault Attacks Using Residue Codes .....	69
<i>Kazim Yumbul, Serdar Süer Erdem, and Erkey Savaş</i>	
A High-Performance Fault Diagnosis Approach for the AES SubBytes Utilizing Mixed Bases .....	80
<i>Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh</i>	

### **Session 4: Fault Injection in Practice**

Practical Optical Fault Injection on Secure Microcontrollers .....	91
<i>Jasper G.J. van Woudenberg, Marc F. Witteman, and Federico Menarini</i>	
Local and Direct EM Injection of Power Into CMOS Integrated Circuits .....	100
<i>F. Poucheret, K. Tobich, M. Lisarty, L. Chusseauz, B. Robissonx, and P. Maurine</i>	
An In-depth and Black-box Characterization of the Effects of Clock Glitches on 8-bit MCUs .....	105
<i>Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede</i>	
<b>Author Index</b> .....	115