# 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography

**FDTC 2013**

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>vii</td>
</tr>
<tr>
<td>Program Committee</td>
<td>viii</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>ix</td>
</tr>
<tr>
<td>Contact Information</td>
<td>x</td>
</tr>
</tbody>
</table>

## Invited Paper

Security Risks Posed by Modern IC Debug and Diagnosis Tools ........................................3  
*Christian Boit, Clemens Helfmeier, and Uwe Kerst*

## Session 1: IC-Security

Hardware Trojan Horses in Cryptographic IP Cores .........................................................15  
*Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, Xuan Thuy Ngo, and Laurent Sauvage*

Invasive PUF Analysis ........................................................................................................30  
*Dmitry Nedospasov, Jean-Pierre Seifert, Clemens Helfmeier, and Christian Boit*

## Session 2: Differential Fault Attacks on Symmetric Cryptosystems

Improving and Evaluating Differential Fault Analysis on LED with Algebraic Techniques .................................................................41  
*Xinjie Zhao, Shize Guo, Fan Zhang, Zhijie Shi, Chujiao Ma, and Tao Wang*

Differential Fault Analysis of MICKEY-128 2.0 .................................................................52  
*Sandip Karmakar and Dipanwita Roy Chowdhury*

Improved Differential Fault Analysis of CLEFIA .....................................................................60  
*Sk. Subidh Ali and Debdeep Mukhopadhyay*

## Invited Paper

Elliptic Curve Cryptosystems in the Presence of Faults ....................................................73  
*Marc Joye*
Session 3: Fault Attack Modeling

Electromagnetic Fault Injection: Towards a Fault Model on a 32-bit Microcontroller
Nicolas Moro, Amine Dehbaoui, Karine Heydemann, Bruno Robisson, and Emmanuelle Encrenaz

Fault Model Analysis of Laser-Induced Faults in SRAM Memory Cells
Cyril Roscian, Alexandre Sarafianos, Jean-Max Dutertre, and Assia Tria

Session 4: Attacks on AES

Fault Analysis of Infective AES Computations
Alberto Battistello and Christophe Giraud

Fault Attacks on AES with Faulty Ciphertexts Only
Thomas Fuhr, Eliane Jaulmes, Victor Lomné, and Adrian Thillard

Reverse Engineering of a Secret AES-like Cipher by Ineffective Fault Analysis
Christophe Clavier and Antoine Wurcker

Author Index