2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2015)

Saint Malo, France
13 September 2015
# 2015 Workshop on Fault Diagnosis and Tolerance in Cryptography

**FDTC 2015**

## 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>Additional Reviewers</td>
<td>ix</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>x</td>
</tr>
<tr>
<td>Organizers' Contact Information</td>
<td>xi</td>
</tr>
</tbody>
</table>

## Invited Papers

- Fault Attacks at the System Level - The Challenge of Securing Application Software  
  Stefan Mangard  
  Page 1

- The Need for Intrinsic Hardware Security Below 65nm  
  Mathias Wagner  
  Page 2

## Session 1: Fault Injection: Models and Techniques

- EM Injection: Fault Model and Locality  
  S. Ordas, L. Guillaume-Sage, and Philippe Maurine  
  Page 3

- On the Complexity Reduction of Laser Fault Injection Campaigns Using OBIC Measurements  
  Falk Schellenberg, Markus Finkeldey, Bastian Richter, Maximilian Schäpers, Nils Gerhardt, Martin Hofmann, and Christof Paar  
  Page 14

## Session 2: DFA: Models and Techniques

- Improved Differential Fault Attack on the Block Cipher SPECK  
  Yuming Huo, Fan Zhang, Xiu Tao Feng, and Li-Ping Wang  
  Page 28

- J-DFA: A Novel Approach for Robust Differential Fault Analysis  
  Luca Magri, Silvia Mella, Pasqualina Fragneto, Filippo Melzani, and Beatrice Rossi  
  Page 35
Lost in Translation: Fault Analysis of Infective Security Proofs .........................................................45
   Alberto Battistello and Christophe Giraud

**Session 3: Fault Injection Attacks to Cipher Families**

To Exploit Fault Injection on Non-injective Sboxes ........................................................................54
   Guillaume Bethouart and Nicolas Debande

An Efficient One-Bit Model for Differential Fault Analysis on Simon Family ..................................61
   Juan del Carmen Grados Vásquez, Fábio Borges, Renato Portugal,
   and Pedro Lara

**Session 4: Fault Attacks to Cryptographic Devices**

Singular Curve Point Decompression Attack .....................................................................................71
   Johannes Blömer and Peter Günther

Laser Fault Attack on Physically Unclonable Functions ..................................................................85
   Shahin Tajik, Heiko Lohrke, Fatemeh Ganji, Jean-Pierre Seifert, and Christian Boit

Improving Fault Attacks on Embedded Software Using RISC Pipeline Characterization ..................97
   Bilgiday Yuce, Nahid Farhady Ghalaty, and Patrick Schaumont

**Author Index** ....................................................................................................................................109