2009 Workshop on Fault Diagnosis and Tolerance in Cryptography

(FDTC 2009)

Lausanne, Switzerland
6 September 2009
# 2009 Workshop on Fault Diagnosis and Tolerance in Cryptography

FDTC 2009

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
</tr>
<tr>
<td>Program Committee</td>
</tr>
</tbody>
</table>

### Invited Paper

Blinded Fault Resistant Exponentiation Revisited .................................................................3
  
  *Arnaud Boscher, Helena Handschuh, and Elena Trichina*

### Session 1: Novel Fault Attacks I

Optical Fault Attacks on AES: A Threat in Violet .................................................................13
  
  *Jörn-Marc Schmidt, Michael Hutter, and Thomas Plos*

Low Voltage Fault Attacks on the RSA Cryptosystem ...........................................................23
  
  *Alessandro Barenghi, Guido Bertoni, Emanuele Parrinello, and Gerardo Pelosi*

Fault Attack on Schnorr Based Identification and Signature Schemes .................................32
  
  *Pierre-Alain Fouque, Delphine Masgana, and Frédéric Valette*

### Session 2: Protecting against Fault Attacks

Protecting RSA against Fault Attacks: The Embedding Method ............................................41
  
  *Marc Joye*

Securing the Elliptic Curve Montgomery Ladder against Fault Attacks ...............................46
  
  *Nevine Ebeid and Rob Lambert*

Securing AES Implementation against Fault Attacks .............................................................51
  
  *Laurie Genelle, Christophe Giraud, and Emmanuel Prouff*

### Invited Paper

KeeLoq and Side-Channel Analysis-Evolution of an Attack ..................................................65
  
  *Christof Paar, Thomas Eisenbarth, Markus Kasper, Timo Kasper, and Amir Moradi*

### Session 3: Novel Fault Attacks II

WDDL is Protected against Setup Time Violation Attacks ....................................................73
  
  *Nidhal Selmane, Shivam Bhasin, Sylvain Guilley, Tarik Graba, and Jean-Luc Danger*
Practical Fault Attack on a Cryptographic LSI with ISO/IEC 18033-3 Block
Ciphers .........................................................................................................................................................84
  Toshinori Fukunaga and Junko Takahashi
A Fault Attack on ECDSA ................................................................................................................................93
  Jörn-Marc Schmidt and Marcel Medwed

Session 4: Tools for Implementing Fault Attacks
Fault Analysis of the Stream Cipher Snow 3G .............................................................................................103
  Blandine Debraize and Irene Marquez Corbella
Using Optical Emission Analysis for Estimating Contribution to Power Analysis ......................................111
  Sergei Skorobogatov
Differential Fault Analysis on SHACAL-1 .................................................................................................120
  Ruilin Li, Chao Li, and Chunye Gong

Author Index ...............................................................................................................................................127