2010 Workshop on Fault Diagnosis and Tolerance in Cryptography

(FDTC 2010)

Santa Barbara, California, USA
21 August 2010
2010 Workshop on Fault Diagnosis and Tolerance in Cryptography

FDTC 2010

Table of Contents

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

Session 1: Attacks on AES

Differential Fault Analysis against AES-192 and AES-256 with Minimal Faults..............................................................................................................3

*Chong Hee Kim*

Passive and Active Combined Attacks on AES—Combining Fault Attacks and Side Channel Analysis........................................................................................10

*Christophe Clavier, Benoit Feix, Georges Gagnerot, and Mylène Roussellet*

Session 2: Fault Injection

Optical Fault Masking Attacks.................................................................................................................................23

*Sergei Skorobogatov*

Memory Address Scrambling Revealed Using Fault Attacks.................................................................................................30

*Jacques J.A. Fournier and Philippe Loubet-Moundi*

Invited Paper

Generic Analysis of Small Cryptographic Leaks...........................................................................................................39

*Itai Dinur and Adi Shamir*
Session 3: Countermeasures

Fault Injection Resilience

Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, and Nidhal Selmane

A Continuous Fault Countermeasure for AES Providing a Constant Error Detection Rate

Marcel Medwed and Jörn-Marc Schmidt

Invited Paper

Multi Fault Laser Attacks on Protected CRT-RSA

Elena Trichina and Roman Korkikyan

Session 4: Public-Key Techniques

Fault Attacks and Countermeasures on Vigilant’s RSA-CRT Algorithm

Jean-Sébastien Coron, Christophe Giraud, Nicolas Morin, Gilles Piret, and David Vigilant

Low Cost Built in Self Test for Public Key Crypto Cores

Duško Karaklajic, Miroslav Kneževic, and Ingrid Verbauwhede

Author Index