

2009 Workshop on Fault Diagnosis and Tolerance in Cryptography

(FDTC 2009)

**Lausanne, Switzerland
6 September 2009**



**IEEE Catalog Number: CFP0986C-PRT
ISBN: 978-1-4244-4972-9**

2009 Workshop on Fault Diagnosis and Tolerance in Cryptography

FDTC 2009

Table of Contents

Preface.....	vii
Program Committee.....	viii

Invited Paper

Blinded Fault Resistant Exponentiation Revisited	3
<i>Arnaud Boscher, Helena Handschuh, and Elena Trichina</i>	

Session 1: Novel Fault Attacks I

Optical Fault Attacks on AES: A Threat in Violet	13
<i>Jörn-Marc Schmidt, Michael Hutter, and Thomas Plos</i>	
Low Voltage Fault Attacks on the RSA Cryptosystem	23
<i>Alessandro Barenghi, Guido Bertoni, Emanuele Parrinello, and Gerardo Pelosi</i>	
Fault Attack on Schnorr Based Identification and Signature Schemes	32
<i>Pierre-Alain Fouque, Delphine Masgana, and Frédéric Valette</i>	

Session 2: Protecting against Fault Attacks

Protecting RSA against Fault Attacks: The Embedding Method	41
<i>Marc Joye</i>	
Securing the Elliptic Curve Montgomery Ladder against Fault Attacks	46
<i>Nevine Ebeid and Rob Lambert</i>	
Securing AES Implementation against Fault Attacks	51
<i>Laurie Genelle, Christophe Giraud, and Emmanuel Prouff</i>	

Invited Paper

KeeLoq and Side-Channel Analysis-Evolution of an Attack	65
<i>Christof Paar, Thomas Eisenbarth, Markus Kasper, Timo Kasper, and Amir Moradi</i>	

Session 3: Novel Fault Attacks II

WDDL is Protected against Setup Time Violation Attacks	73
<i>Nidhal Selmane, Shivam Bhasin, Sylvain Guilley, Tarik Graba, and Jean-Luc Danger</i>	

Practical Fault Attack on a Cryptographic LSI with ISO/IEC 18033-3 Block Ciphers	84
<i>Toshinori Fukunaga and Junko Takahashi</i>	
A Fault Attack on ECDSA	93
<i>Jörn-Marc Schmidt and Marcel Medwed</i>	
Session 4: Tools for Implementing Fault Attacks	
Fault Analysis of the Stream Cipher Snow 3G	103
<i>Blandine Debraize and Irene Marquez Corbella</i>	
Using Optical Emission Analysis for Estimating Contribution to Power Analysis	111
<i>Sergei Skorobogatov</i>	
Differential Fault Analysis on SHACAL-1	120
<i>Ruilin Li, Chao Li, and Chunye Gong</i>	
Author Index	127