

FDTC 2007

**Fault Diagnosis and
Tolerance in Cryptography**

**4th Workshop
on Fault Diagnosis and
Tolerance in Cryptography**

General Co-chairs:

Luca Breveglieri¹ and Israel Koren²

Program Co-chairs:

David Naccache³ and Jean Pierre Seifert⁴

¹ Politecnico di Milano, Milano, Italy

² University of Massachusetts, Amherst, USA

³ École Normale Supérieure de Paris, France

⁴ Sisa, Samsung, USA

1st Workshop on Fault Diagnosis and Tolerance in Cryptography

Florence, ITALY June 30, 2004

DSN 2004 – Intern'l
Conference
on Dependable
Systems and Networks



25 participants

No official proceedings

2nd Workshop on Fault Diagnosis and Tolerance in Cryptography

Edinburgh, UK

September 2, 2005

CHES 2005 – Workshop
on Cryptographic
Hardware and
Embedded Systems

118 participants

No official proceedings



IEEE Transactions on Computers, Sept. 2006
SPECIAL SECTION ON FAULT DIAGNOSIS AND TOLERANCE
IN CRYPTOGRAPHY

3rd Workshop on Fault Diagnosis and Tolerance in Cryptography

Yokohama, Japan

October 10, 2006

CHES 2006 – Workshop
on Cryptographic
Hardware and
Embedded Systems

103 participants



The 1st FDTC to have official proceedings (by Springer-Verlag)

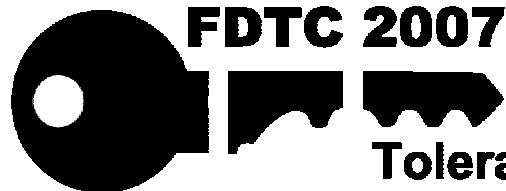
4th Workshop on Fault Diagnosis and Tolerance in Cryptography

Vienna, Austria

September 10, 2007

CHES 2007 – Workshop
on Cryptographic
Hardware and
Embedded Systems

73 participants



FDTC 2007

**Fault Diagnosis and
Tolerance in Cryptography**

Official proceedings by IEEE Computer Society Press

8:45 – 9:00	<p>Welcome and Opening Remarks <i>Israel Koren, University of Massachusetts, Amherst, MA, USA</i> <i>Luca Breveglieri, Politecnico di Milano, Milano, Italy</i></p>
9:00 – 9:40	<p>1st Invited Talk: Securing Flash Technology <i>Helena Handshuh, <u>Elena Trichina</u></i></p>
9:40 – 10:55	<p>Session 1: Fault Attacks on Public Key Cryptosystems chair: <i>Luca Breveglieri</i></p> <p>1. How can we overcome both Side Channel Analysis and Fault Attacks on RSA-CRT ? <i><u>Chong Hee Kim</u>, Jean-Jacques Quisquater</i></p> <p>2. Montgomery Multiplication with Redundancy Check <i>Michael Tunstall</i></p> <p>3. Fault Detection Structures for the Montgomery Multiplication over Binary Extension Fields <i><u>Arash Hariri</u>, Arash Reyhani-Masoleh</i></p>
10:55 - 11:15	<p>Coffee break</p>
11:15 - 12:05	<p>Session 2: Fault Attacks on ECCs chair: <i>Shay Gueron</i></p> <p>1. Tate Pairing with Strong Fault Resiliency <i><u>Erdinc Ozturk</u>, Gunnar Gaubatz, Berk Sunar</i></p> <p>2. Register Transfer Level Concurrent Error Detection in Elliptic Curve Crypto Implementations <i><u>Richard Stern</u>, Nikhil Joshi, Kaijie Wu, Ramesh Karri</i></p>

12:05 – 13:40	Lunch
13:40 – 14:20	2nd Invited Talk: Smartcard Design against Laser Fault Injection Attacks <i>Odile Derouet</i>
14:20 – 15:35	<p>Session 3: Fault Attacks on AES chair: <i>JP Seifert</i></p> <p>1. A Structure-independent Approach for Fault Detection Hardware Implementations of the AES <i>M. Mozaffari-Kermani, A. Reyhani-Masoleh</i></p> <p>2. A Novel Double-Data-Rate AES Architecture Resistant against Fault Injection <i>P. Maistri, P. Vanhauwaert, R. Leveugle</i></p> <p>3. DFA Mechanism on the AES Key Schedule <i>Junko Takahashi, Toshinori Fukunaga, Kimihiro Yamakoshi</i></p>
15:35 – 16:00	Coffee break
16:00 – 17:15	<p>Session 4: Countermeasures and Attack Techniques chair: <i>Guido Bertoni</i></p> <p>1. Countermeasures Against Branch Target Buffer Attacks <i>G. Agosta, L. Breveglieri, I. Koren, G. Pelosi, M. Sykora</i></p> <p>2. Cheap Hardware Parallelism Implies Cheap Security <i>Onur Acicmez, Jean-Pierre Seifert</i></p> <p>3. Passive and Active Combined Attacks Combining Fault Attacks and Side Channel Analysis (Presented by <u>Michael Tunstall</u>) <i>Frederic Amiel, Benoit Feix, Louis Marcel, Karine Villegas</i></p>
17:15 – 17:30	Closing remarks and Farewell

Program co-chairs:

David Naccache

École Normale
Supérieure de Paris,
France

Jean Pierre Seifert

SISA, Samsung, USA

Program committee:

Hervé Chabannes	Sagem Défense Sécurité, France
Christophe Clavier	Gemplus Corporation, France
Wieland Fischer	Infineon Corporation, Germany
Shay Gueron	University of Haifa and Intel Corporation, Israel
Ramesh Karri	Polytechnic University of Brooklyn, USA
Christof Paar	University of Ruhr
Johannes Bloemer	University of Paderborn
Régis Leveugle	TIMA Lab. Grenoble
Paul Karger	IBM
Çetin Kaya Koç	Oregon State University, USA
Pierre-Yvan Liardet	STMicroelectronics Corporation, France
Sandra Marcello	Thalès Corporation, France
Elisabeth Oswald	Graz University of Technology, Austria
Elena Trichina	Spansion Corporation, USA
Helena Handschuh	Spanion
Michael Tunstall	Royal Holloway University of London, UK
Kaiji Wu	University of Illinois at Chicago, USA
Mehdi Laurent Akkar	Texas Instruments
Nora Dabbous	Ingenico
Onur Aciicmez	Samsung
Eran Tromer	Weizman Institute

Special Thanks to the registration support

Mrs. Irmgard Kühn, Communication Security Center,
Ruhr University, Bochum, Germany

Prof. Christof Paar, General Chair, SHARCS

Statistics

16 manuscripts submitted

11 papers accepted for presentation

Participants:

- France 18
- Germany 14
- Japan 9
- USA 7
- Belgium, Czech Republic 4
- UK, Israel 3
- Canada, Italy, Netherlands 2
- Austria, Slovakia, Ireland, S. Korea, Switzerland, Singapore, Iran 1