5th Workshop on **F**ault **D**iagnosis and **T**olerance in **C**ryptography

General Co-chairs:

Luca Breveglieri[1] and Israel Koren[2]

Program Co-chairs:

David Naccache,[3] Jean Pierre Seifert[4] and Shay Gueron[5]

[1] Politecnico di Milano, Milano, Italy
[2] University of Massachusetts, Amherst, USA
[3] École Normale Supérieure de Paris, France
[4] Sisa, Samsung, USA
[5] University of Haifa and Intel, Israel

1st Workshop on Fault Diagnosis and Tolerance in Cryptography

Florence, ITALY, June 30, 2004

DSN 2004 – 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

118 participants No official proceedings

IEEE Transactions on Computers, Sept. 2006,
Special Section on FDTC

3rd Workshop on Fault Diagnosis and Tolerance in Cryptography

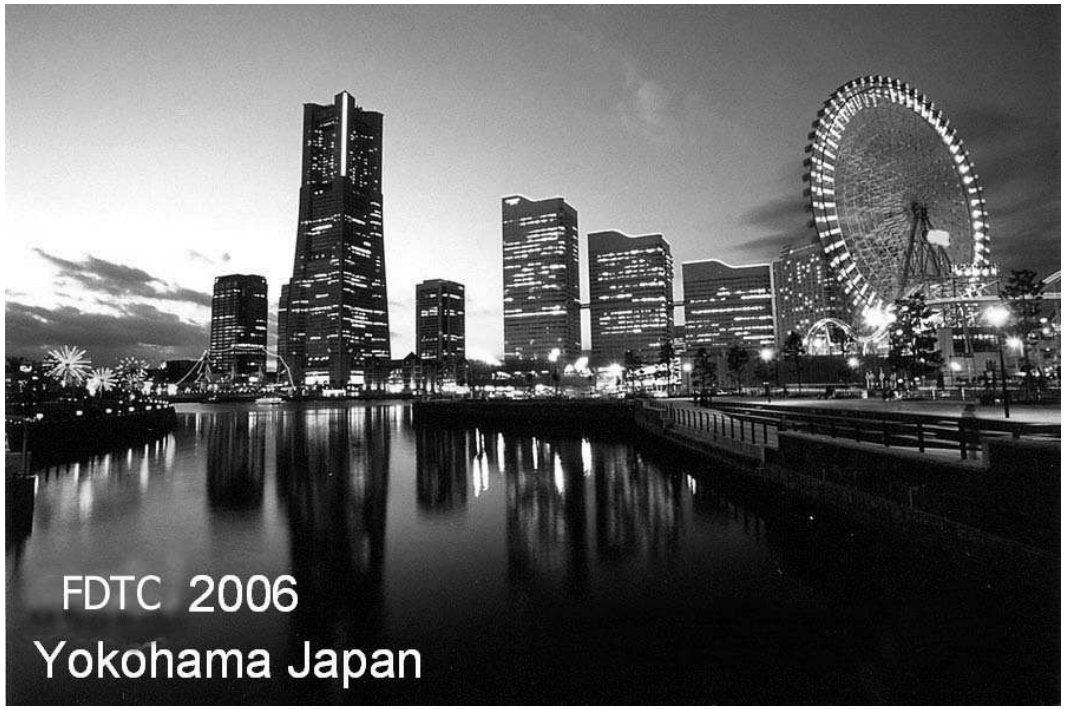
Yokohama, Japan October 10, 2006

CHES 2006 – Workshop on Cryptographic Hardware and Embedded Systems

103 participants

FDTC 2006

Fault Diagnosis and Tolerance in Cryptography



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

5th Workshop on Fault Diagnosis and Tolerance in Cryptography

Washington, DC. USA August 10, 2008

CHES 2008 – Workshop on Cryptographic Hardware and Embedded Systems

84 participants

FDTC 2008

Fault Diagnosis and Tolerance in Cryptography

Official proceedings by IEEE Computer Society Press

8:30 – 8:45	**Welcome and Opening Remarks** ***Israel Koren*, *Luca Breveglieri***
8:45 – 9:25	**1st Invited Talk: Silicon-Level Solutions to counteract Passive and Active Attacks, *Sylvain Guilley*, *Laurent Sauvage, Jean-Luc Danger, Nidhal Selmane, Renaud Pacalet***
9:25 – 10:40	**Session 1: Differential Fault Analysis chair: *G. Bertoni*** **1. Improved Differential Fault Analysis on CLEFIA** ***Junko Takahashi*, *Toshinori Fukunaga*** **2. Masking does not protect against Differential Fault Attacks** ***Helena Handschuh, Arnaud Boscher*** **3. Comparative Analysis of Robust Fault Attack Resistant Architectures for Public and Private Cryptosystems** ***Konrad J. Kulikowski, Zhen Wang, Mark G. Karpovsky***
10:40 - 11:00	**Coffee break**
11:00 - 12:15	**Session 2:Fault Security of HW and SW chair: *M. Joye*** **1. A Practical Attack on Square and Multiply** ***Jörn-Marc Schmidt*, *Christoph Herbst*** **2. Register Exploiting Hardware Performance Counters** ***Leif Uhsadel*, *Andy Georges, Ingrid Verbauwhede*** **3. A Generic Fault Countermeasure providing Data and Program Flow Integrity, *Marcel Medwed*, *Jörn-Marc Schmidt***

12:15 – 13:45	**Lunch (East Room)**
13:45 – 14:25	**2nd Invited Talk: Aspects of the Development of Fault Resistant Hardware *Wieland Fischer***
14:25 – 15:40	**Session 3: Fault Security of Elliptic Curves chair: J-P Seifert** **1. Fault-Tolerant ECC Unit using Parity preserving Logic Gates** ***Julien Francq, Jean-Baptiste Rigaud, Pascal Manet, Assia Tria*** **2. On the Security of a Unified Countermeasure** ***Marc Joye*** **3. Fault Attack on Elliptic Curve with Montgomery Ladder Implementation** ***Pierre-Alain Fouque, Reynald Lercier, Denis Réal, Frédéric Valette***
15:40 – 16:00	**Coffee break**
16:00 – 16:50	**Session 4: Fault Security of Public Key chair: A. Tria** **1. Security against Fault Injection Attacks for CRT-RSA Implementations *Alexandre Berzati, Cecile Canovas, Louis Goubin*** **2. Attacks on Authentication and Signature Schemes involving Corruption of Public Key (Modulus)** ***Michael Kara-Ivanov, Eran Iceland, Aviad Kipnis***
16:50 – 17:00	**Closing remarks and Farewell**

Program co-chairs:

David Naccache
École Normale Supérieure de Paris, France

Jean Pierre Seifert
SISA, Samsung, USA

Shay Gueron
University of Haifa and Intel, Israel

Program committee:

Jean-Marc Robert	École Tech. Sup. Monreal
David M'Raihi	VeriSign
Wieland Fischer	Infineon Corporation, Germany
Ramesh Karri	Polytechnic University of Brooklyn, USA
Christof Paar	University of Ruhr, Germany
Johannes Bloemer	University of Paderborn
Régis Leveugle	TIMA Lab., France
Çetin Kaya Koç	Oregon State University, USA
Guido Bertoni	STMicroelectronics Corporation, Italy
Nathalie Feyt	Thalès Corporation, France
Mathieu Ciet	Private
Christophe Bidan	NISS, France
Helena Handschuh	Spansion
Jean-Sebastien Coron	Univ. of Luxembourg
Kaiji Wu	University of Illinois at Chicago, USA
Julien Brouchier	ISEN, France
Benoit Chevallier-Mames	DCSSI, France
Onur Aciicmez	Samsung, USA
Jean-Louis Lanet	University of Limoges
Marc Joye	Thomson
Assia Tria	CEA-LETI, France
Pascal Guterman	LAM, France

Statistics

22 manuscripts submitted

11 papers accepted for presentation

Participants:

- France 16
- Japan 15
- Germany 11
- USA 8
- S. Korea 7
- UK, Netherlands 4
- Austria, Czech Republic, Singapore 3
- Belgium, Israel, Italy 2
- Canada, Switzerland, Turkey 1