3rd 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] and Jean Pierre Seifert[4]

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

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

FDTC 2006
Fault Diagnosis and Tolerance in Cryptography

The first FDTC to have official proceedings

8:40 – 8:50	**Welcome and Opening Remarks** ***Israel Koren*, University of Massachusetts, Amherst, MA, USA** ***Luca Breveglieri*, Politecnico di Milano, Milano, Italy**
8:50 – 9:20	**1st Invited Talk: Fault attacks, an intuitive approach** ***Raphael Bauduin***
9:25 – 10:25	**Session 1: Public key fault attacks** chair: ***Luca Breveglieri*** **1. Is it wise to publish your Public RSA Keys?** ***Shay Gueron, Jean-Pierre Seifert*** **2. Attacking right-to-left Modular Exponentiation with Timely Random Faults, *Michele Boreale*** **3. Java Type Confusion and Fault Attacks** ***Olli Vertanen***
10:25 - 11:10	**Coffee break**
11:10 - 12:10	**Session 2: Secret key fault attacks** chair: ***Shay Gueron*** **1. A Fault Attack Against the FOX Cipher Family** ***Luca Breveglieri, Israel Koren, Paolo Maistri*** **2. Fault Based Collision Attacks on AES** ***Johannes Blömer, Volker Krummel*** **3. Collision Fault Analysis of DPA-Resistant Algorithms** ***Frederic Amiel, Christophe Clavier, Michael Tunstall***

12:10 – 14:00	**Lunch (lunch boxes)**
14:00 – 14:30	**2nd Invited Talk: Safe design methodologies against fault attacks** ***Bruno Robisson***
14:35 – 15:15	**Session 3: Secret key fault protection** **chair: *Akashi Satoh*** **1. An Easily Testable and Reconfigurable Pipeline for Symmetric Block Ciphers, *Myeong-Hyeon Lee, Yoon-Hwa Choi*** **2. Case Study of a Fault Attack on Asynchronous DES Crypto-Processors** ***Yannick Monnet, Marc Renaudin, Régis Leveugle, Christophe Clavier, Pascal Moitrel***
15:15 – 15:55	**Coffee break**
15:55 – 16:55	**Session 4: Public key fault attack protection** **chair: *Guido Bertoni*** **1. Wagner's Attack on a Secure CRT-RSA Algorithm Reconsidered** ***Johannes Blömer, Martin Otto*** **2. Blinded Fault Resistant Exponentiation** ***Guillaume Fumaroli, David Vigilant*** **3. Non-linear Residue Codes for Robust Public-Key Arithmetic** ***Gunnar Gaubatz, Mark Karpovsky, Berk Sunar***
16:55 – 17:10	**Closing remarks and Farewell**

Program co-chairs:

David Naccache
École Normale Supérieure de Paris, France

Jean Pierre Seifert
University of Innsbruck and Haifa, Austria and Israel

Program committee:

Bao Feng	I2R Corporation, France
Ernie Brickell	Intel Corporation, USA
Hervé Chabannes	Sagem Défense Sécurité, France
Christophe Clavier	Gemplus Corporation, France
Wieland Fischer	Infineon Corporation, Germany
Christophe Giraud	Oberthur Card Systems, France
Shay Gueron	University of Haifa and Intel Corporation, Israel
Louis Goubin	University of Versailles, France
Mohaned Kafi	Axalto Corporation, France
Ramesh Karri	Polytechnic University of Brooklyn, USA
Jong Rok Kim	Samsung Corporation, Korea
Vanessa Gratzer	University of Paris 2, France
Çetin Kaya Koç	Oregon State University, USA
Pierre-Yvan Liardet	STMicroelectronics Corporation, France
Wenbo Mao	HP Corporation, USA
Sandra Marcello	Thalès Corporation, France
Elisabeth Oswald	Graz University of Technology, Austria
Elena Trichina	Spansion Corporation, USA
Michael Tunstall	Royal Holloway University of London, UK
Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Claire Whelan	Dublin City University, Ireland
Kaiji Wu	University of Illinois at Chicago, USA
Moti Yung	Columbia University, USA

Special Thanks to the Local Arrangement Team

Mr. Tetsuya Izu, Fujitsu

Ms. Ayako Komatsu, NEC

Dr. Natsume Matsuzaki, Panasonic

Dr. Akashi Satoh, IBM

and

Prof. Tsutomu Matsumoto, National Yokohama University - CHES 2006 General Chair

Statistics

23 manuscripts submitted

12 papers accepted for presentation

Participants:

- Japan 28
- France 17
- Germany 16
- S. Korea 6
- Czech, Singapore 4
- Belgium, China, Israel, Italy, Russia, UK, USA 3
- Austria, Netherlands, Slovakia, Switzerland 2
- Brazil, Canada, Finland, Ghana, Turkey 1