FDTC 2006
Fault Diagnosis and
Tolerance in Cryptography

Call for Participation

3d WORKSHOP ON FAULT DIAGNOSIS AND TOLERANCE IN CRYPTOGRAPHY - FDTC 2006

Yokohama, Japan - Tuesday October 10, 2006
(one day prior to CHES 2006 – same location)

FINAL PROGRAMME AND PRESENTATION SLIDES

LIST OF ATTENDEES

FDTC 2006 PROCEEDINGS - LNCS vol. 4236 - ORDER

in Association with CHES 2006:
WORKSHOP ON CRYPTOGRAPHIC HARDWARE IN EMBEDDED SYSTEMS

CHES 2006 WEB SITE

FDTC 2006 has taken place in the Annex Hall, on the left side of the convention center in Pacifico Yokohama (map). The room numbers are F201 + F202 (floorplan).

In recent years applied cryptography has developed considerably, to satisfy the increasing security requirements of various information technology disciplines, e.g., telecommunications, networking, data base systems and mobile applications.

Cryptosystems are inherently computationally complex and in order to satisfy the high throughput requirements of many applications, they are often implemented by means of either VLSI devices (crypto-accelerators) or highly optimized software routines (crypto-libraries) and are used via suitable (network) protocols.

The high complexity of such implementations raises concerns regarding their reliability. Research is therefore needed to develop methodologies and techniques for designing robust cryptographic systems (both hardware and software), and to protect them against both accidental faults and intentional intrusions and attacks, in particular those based on the malicious injection of faults into the device for the purpose of extracting the secret key.

This annual workshop was started in 2004 and included 10 papers. The 2nd workshop was held in September 2005 and included 13 papers. See:

http://www.elet.polimi.it/res/FDTC04 and http://www.elet.polimi.it/conferences/FDTC05

This year's workshop will feature two invited talks:

Raphael Bauduin (EDSI) "Fault Attacks, an Intuitive Approach"

Bruno Robisson (CEA) "Safe Design Methodologies against Fault Attacks"

Contributions to the workshop describing theoretical studies and practical case studies of fault diagnosis and tolerance in cryptographic systems (HW and SW) and protocols are solicited. Topics of interest include, but are not limited to:

- Modelling the reliability of cryptographic systems and protocols.
- Inherently reliable cryptographic systems and algorithms.
- Faults and fault models for cryptographic devices (HW and SW).
- Reliability-based attack procedures on cryptographic systems (fault-injection based attacks) and protocols.
- Adapting classical fault diagnosis and tolerance techniques to cryptographic systems.
- Novel fault diagnosis and tolerance techniques for cryptographic systems.
- Case studies of attacks, reliability and fault diagnosis and tolerance techniques in cryptographic systems.

The workshop proceedings will be published in Springer's Lecture Notes in Computer Science (LNCS) series and distributed at the workshop. In order to be included in the proceedings, the authors of an accepted paper must guarantee to present their contribution at the workshop.

FDTC 2006

Fault Diagnosis and Tolerance in Cryptography

Important Dates:

- **Submission deadline**: May 1, 2006 – **CLOSED**
- **Notification deadline**: June 10, 2006 – **CLOSED**
- **Final paper deadline**: July 20, 2006 – **CLOSED**
- **Submissions**: extended abstracts of 10 pages or less, PDF format is preferred.

E-mail the extended abstract to david.naccache@ens.fr and jeanpierreseifert@yahoo.com

Please provide name, affiliation, telephone, fax number and email address.

Final papers will have to be formatted according to the LNCS format instructions.

Program committee:

Bao Feng	I2R	**Cetin Kaya Koç**	Oregon State U
Luca Breveglieri	Politecnico di Milano	**Israel Koren**	U of Mass. at Amherst
Ernie Brickell	Intel	**Pierre-Yvan Liardet**	STMicroelectronics
Hervé Chabannes	Sagem Défense Sécurité	**Wenbo Mao**	HP
Christophe Clavier	Gemplus	**Sandra Marcello**	Thalès
Wieland Fischer	Infineon	**Elisabeth Oswald**	Graz U of Technology
Christophe Giraud	Oberthur	**Elena Trichina**	Spansion
Shay Gueron	U Haifa, and Intel Corp.	**Michael Tunstall**	Royal Holloway U London
Louis Goubin	U de Versailles	**Wen-Guey Tzeng**	National Chiao Tung U
Mohaned Kafi	Axalto	**Claire Whelan**	Dublin City U
Ramesh Karri	Brooklyn Poly	**Kaiji Wu**	U of Illinois at Chicago
Jong Rok Kim	Samsung	**Moti Yung**	Columbia U
Vanessa Gratzer	U Paris 2 Panthéon Assas		

Organizers and workshop series founders:

Prof. Luca Breveglieri
✉ Dept. of Electronic and Information Sciences
Politecnico di Milano, Piazza Leonardo Da Vinci n. 32, I-20133, Milano, ITALY
☎ + 39 (0)2 2399 3653
🖷 + 39 (0)2 2399 3411
⌨ breveglieri@elet.polimi.it

Prof. Israel Koren
✉ Dep. of Electrical & Computer Engineering
University of Massachusetts
Amherst, MA 01003, USA
☎ + 01 (413) 545-2643
🖷 + 01 (413) 545-1993
⌨ koren@ecs.umass.edu

Scientific Program co-Chairs for the 2006 workshop:

Prof. David Naccache
✉ Ecole Normale Supérieure,
Département d'Informatique
Equipe de Cryptographie, 45 rue d'Ulm,
F-75005, Paris, France
☎ + 33 6 11 56 69 05

Dr. Jean-Pierre Seifert
✉ Applied Security Research Group
Center for Comp. Mathematics and Sci. Comp.
Faculty of Science and Science Education
University of Haifa
Haifa 31905, Israel
☎ + 1 (503) 608 7347

Local conference organisers:

Dr. Yukiyasu Tsunoo - NEC	Dr. Natsume Matsuzaki - Panasonic
Dr. Tetsuya Izu - Fujitsu	Dr. Akashi Satoh - IBM