Call for Participation

4th WORKSHOP ON FAULT DIAGNOSIS AND TOLERANCE IN CRYPTOGRAPHY - FDTC 2007

http://conferenze.dei.polimi.it/FDTC07/

Vienna, Austria – Monday, September 10, 2007

Renaissance Penta Vienna Hotel

(one day prior to CHES 2007 – 10 minutes walking distance from CHES hotel)

REGISTRATION DESK WILL BE LOCATED AT CHES Vienna Marriott HOTEL

CHES 2007 WEB SITE

LIST OF PAPERS TO BE PRESENTED AT FDTC 2007

FINAL PROGRAMME AND PRESENTATION SLIDES

LIST OF ATTENDEES

FDTC 2007 PROCEEDINGS

(free access if subscriber to the IEEE CS digital library)

HOW TO REACH THE FDTC HOTEL FROM THE CHES HOTEL
directions & map

REGISTRANTS PLEASE READ CAREFULLY THESE INSTRUCTIONS

Early registration rates (before August 17):

- 150 euro regular
- 120 euro student

Late registration rates (after August 17):

- 200 euro regular
- 160 euro student

Since the registration page was down for a few days, the deadline for early registration has been extended to August 17. The registration fee includes proceedings, lunch and coffee breaks. If you have registered online, please collect your name tag and proceedings on Sunday afternoon 14:00-16:00 at the SHARCS registration desk in the Vienna Marriott Hotel (the CHES hotel). We will have only very limited registration services on Monday at the Renaissance Penta Vienna Hotel where FDTC will take place. If you have to register and pay onsite you must do it on Sunday at the SHARCS registration desk.

ON-LINE REGISTRATION PAGE

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 optimised 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. The 3rd workshop was held in October 2006 and included 12 papers. See the following links:

http://risorse.dei.polimi.it/FDTC04

http://conferenze.dei.polimi.it/FDTC05

http://conferenze.dei.polimi.it/FDTC06

This year's workshop will feature two invited talks by:

"Securing Flash Technology"
Helena Handschuh, Elena Trichina - Spansion

"Secure Smartcard Design against Laser Fault Injection Attacks"
Odile Derouet, Samsung

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.
Micro-architectural side-channels that exploit micro-architecture components like caches and branch predictors.
Case studies of attacks, reliability and fault diagnosis and tolerance techniques in cryptographic systems.

The workshop proceedings will be published by IEEE-CS Press, will be available as a printed volume at the workshop and will be included in the IEEE Computer Society online store in due time. This will be the 2nd FDTC volume, after that of FDTC 2006 (published by Springer-Verlag). In order to be included in the FDTC 2007 proceedings, the authors of an accepted paper must guarantee to present their contribution at the workshop. To format the final paper, see IEEE-CPS Author Kit.

Due to desagreements with Springer-Verlag, the FDTC 2007 proceedings will not be published any longer in the LNCS series, as announced initially.

Important Dates:

Submission deadline: 15 April, 2007 – **EXTENDED TO 27 APRIL 2007 – NOW CLOSED**

Notification deadline: 30 May, 2007 – **NOTIFIED**

Final paper deadline: 29 June, 2007 (electronic submission, see the IEEE-CPS author kit) – **NOW CLOSED**

Submissions: extended abstracts of 10 pages or less, PDF format is preferred.

E-mail the extended abstract to david.naccache@ens.fr and Jean-Pierre.Seifert@uibk.ac.at

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

Final papers will have to be formatted according to the instructions of the IEEE-CPS Author Kit.

Program committee to include:

Hervé Chabannes	Sagem Défense Sécurité	**Sandra Marcello**	Thalès
Christophe Clavier	Gemalto	**Elisabeth Oswald**	University of Graz
Wieland Fischer	Infineon	**Elena Trichina**	Spansion
Shay Gueron	Univ. of Haifa and Intel	**Helena Handschuh**	Spansion
Ramesh Karri	Brooklyn Polythecnic	**Michael Tunstall**	University of Cork
Christof Paar	University of Ruhr	**Kaiji Wu**	University of Illinois
Johannes Bloemer	University of Paderborn	**Mehdi Laurent Akkar**	Texas Instruments
Régis Leveugle	TIMA Lab. Grenoble	**Nora Dabbous**	Ingenico
Paul Karger	IBM	**Onur Aciicmez**	Samsung
Pierre-Yvan Liardet	ST Microelectronics	**Eran Tromer**	Weizman Institute
Cetin Kaya Koç	Oregon State University		

Organizers and workshop series founders:

Prof. Luca Breveglieri
Dep. of Electronic and Information Sciences
Politecnico di Milano - Piazza L. Da Vinci n. 32
Milano I-20133 – ITALY
Tel: + 39 (0) 2 2399 3653
Fax: + 39 (0) 2 2399 3411
Email: breveglieri@elet.polimi.it

Prof. Israel Koren
Dep. of Electrical & Computer Engineering
University of Massachusetts
Amherst MA 01003 – USA
Tel: + 01 (413) 545 2643
Fax: + 01 (413) 545 1993
Email: koren@ecs.umass.edu

Scientific Program co-Chairs for the 2007 workshop:

Prof. David Naccache
Ecole Normale Supérieure
Département d'Informatique
Equipe de Cryptographie – 45 rue d'Ulm
Paris F-75005 – France
Tel: + 33 (0) 6 11 56 69 05
Email: david.naccache@ens.fr

Prof. Jean-Pierre Seifert
University of Innsbruk
Institut für Informatik
Christoph-Probst-Platz – Innrain 52
Innsbruck 6020 – AUSTRIA
Tel: + 43 (0) 512 507 6101
Email: Jean-Pierre.Seifert@uibk.ac.at

Publicity Chair for the 2007 workshop:

Prof. Shay Gueron
University of Haifa
Dep. of Mathematics – Mount Carmel
Haifa 31905 – ISRAEL
Tel: + 972 (0) 4 824 0161
Email: shay@math.haifa.ac.il

Local arrangement:

Prof. Jean-Pierre Seifert
University of Innsbruck
Institut für Informatik
Innsbruck 6020 – AUSTRIA