FDTC 2012: Call for Papers

The 9th Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2012) will be held in **Leuven**, Belgium, on **September 9, 2012**. FDTC 2012 is one day before CHES 2012 (September 10 –12, 2012). The Call for Papers is available for download as a PDF file.

Motivation & Scope

Fault injection is one of the most exploited means for extracting confidential information from embedded devices or for compromising their intended behavior.
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. Of particular interest is protection against malicious injection of faults into the device for the purpose of extracting confidential information.
FDTC is the reference event in the field of fault analysis, attacks and countermeasures.

Paper submission

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:

- modeling the reliability of cryptographic systems and protocols
- inherently reliable cryptographic systems and algorithms
- faults and fault models for cryptographic devices (HW and SW)
- novel fault diagnosis and tolerance techniques for cryptographic systems
- attacks exploiting micro-architecture components
- physical protection against attacks
- fault attacks using lasers, electromagnetic induction, and clock / power supply manipulation
- case studies of attacks, reliability, and fault diagnosis and tolerance techniques in cryptographic systems
- combined attacks
- fault injection: mechanisms, models and countermeasures
- fault exploitation: analysis, attacks and countermeasures
- fault resistant hardware, fault resistant implementations of cryptographic algorithms and fault resistant protocols

All submissions should be made using the online submission system:

http://fdtc.ws.dei.polimi.it

Submissions should conform to the instructions below.

Important dates

Paper submission deadline:	**May 10, 2012, 23:59 UTC**
Notification of acceptance:	**June 18, 2012**
Final version deadline:	**July 2, 2012**
Workshop:	**September 9, 2012**

Instructions for authors

Submissions must not substantially duplicate work that any of the authors have published elsewhere or that have been submitted in parallel in any other conference or workshop. Submissions should be anonymous, with no author names, affiliations, acknowledgments or obvious references. Papers should be at most 10 pages (including the bibliography and appendices), with at least 11pt font and reasonable margins.
Submission of final papers will be managed directly by Conference Publishing Services (CPS). Final papers must be formatted following the instructions in the related author kit (to be communicated). Conference Publishing Services (CPS) will contact directly the authors for instructions and will send links to the publishing services.
Accepted papers will be published in an archival proceedings volume by Conference Publishing Services (CPS) and will be distributed at the time of the workshop.
At least one author of each accepted paper must register with the workshop and present the paper in order to be included in the proceedings.

Program committee (co-chair contact pc2012@fdtc-workshop.eu)

- Alessandro Barenghi, Politecnico di Milano, Italy
- **Guido Bertoni**, STMicroelectornics, Italy (**co-chair**)
- Christophe Clavier, University of Limoges, France
- Wieland Fischer, Infineon Technologies, Germany
- **Benedikt Gierlichs**, KU Leuven, Belgium (**co-chair**)
- Christophe Giraud, Oberthur Technologies, France
- Jorge Guarjardo, Bosch, USA
- Sylvain Guilley, Telecom ParisTech, France
- Helena Handschuh, Cryptography Research Inc., USA
- Dusko Karaklajic, KU Leuven, Belgium
- Kerstin Lemke-Rust, HBRS, Germany
- Marcel Medwed, UCL Crypto Group, Belgium
- Debdeep Mukhopadhyay, Indian Institute of Technology Kharagpur, India
- Matthieu Rivain, CryptoExperts, France
- Jörn-Marc Schmidt, TU Graz, Austria
- Sergei Skorobogatov, University of Cambridge, UK
- Junko Takahashi, NTT Corporation, Japan
- Michael Tunstall, University of Bristol, UK
- Marc Witteman, Riscure, The Netherlands

Steering committee

- Luca Breveglieri, Politecnico di Milano, Italy
- Israel Koren, University of Massachusetts, USA
- David Naccache (chair), Ecole Normale Supérieure, France
- Jean-Pierre Seifert, TU Berlin & T-Labs, Germany

FDTC 2012 is in cooperation with IACR - http://www.iacr.org