

Tenth Workshop on Fault Diagnosis and Tolerance in Cryptography

August 20, 2013 • Santa Barbara, CA, USA

(co-located with *CRYPTO 2013* and *CHES 2013*)

FDTC 2013 is held in cooperation with IACR (www.iacr.org)

Program chairs

Wieland Fischer *Infineon*
Jörn-Marc Schmidt *TU Graz*

Program committee

Guido Bertoni *STMicroelectronics*
Benedikt Gierlichs *KU Leuven*
Christophe Giraud *Oberthur Technologies*
Jorge Guajardo *Robert Bosch LLC*
Sylvain Guilley *Telecom ParisTech*
Helena Handschuh *Cryptog. Research*
Ilya Kizhvatov *Riscure*
Kerstin Lemke-Rust *HBRS*
Marcel Medwed *NXP Semiconductors*
Debdeep Mukhopadhyay *IIT Kharagpur*
David Oswald *HGI, Ruhr-Univ. Bochum*
Gerardo Pelosi *Politecnico di Milano*
Matthieu Rivain *CryptoExperts*
Sergei Skorobogatov *Univ. of Cambridge*
Tsuyoshi Takagi *Kyushu University*
Junko Takahashi *NTT Laboratories*
Michael Tunstall *University of Bristol*
Ingrid Verbauwhede *KU Leuven*

General chairs

Luca Breveglieri *Politecnico di Milano*
Israel Koren *University of Massachusetts*

Steering committee

Luca Breveglieri *Politecnico di Milano*
Israel Koren *University of Massachusetts*
David Naccache (chair) *ENS*
Jean-Pierre Seifert *TU Berlin & T-Labs*



Santa Barbara

Important dates

Submission deadline: **April 22, 2013**
Notification of acceptance: May 10, 2013
Camera-ready version: May 24, 2013
Workshop: August 20, 2013

Fault injection is one of the most exploited means for extracting confidential information from embedded devices and for compromising their intended behavior. Therefore, research on developing methodologies and techniques for the design of robust cryptographic systems (both hardware and software), and on protecting them against both accidental faults and intentional attacks is essential. Of particular interest is the 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.

Topics of interest include but are not limited to:

- fault injection:
 - o mechanisms (e.g., using lasers, electromagnetic induction, or clock / power supply manipulation)
 - o models of fault injection
 - o measures to prevent fault injection (e.g., physical protection, fault diagnosis)
- fault exploitation:
 - o attacks on cryptographic devices (HW and SW) or protocols
 - o combined implementation attacks
 - o models and analysis (e.g., modeling the reliability of systems or protocols)
- countermeasures:
 - o fault resistant hardware / implementations of cryptographic algorithms
 - o countermeasures to detect fault injections and techniques providing fault tolerance (inherent reliability)
 - o fault resistant protocols
- case studies of attacks, fault diagnosis, and tolerance techniques

Instructions for authors

Submissions must not substantially duplicate work that any of the authors have published elsewhere or that have been submitted in parallel to any other conference or workshop. Submissions should be anonymous, with no author names, affiliations, acknowledgments, or obvious references. Papers should be from 10 to at most 15 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 for the workshop and present the paper in order to be included in the proceedings.

For submission instructions and further information please point your web-browser to:

www.fdtc-workshop.eu