FDTC 2015
Fault Diagnosis and Tolerance in Cryptography

Twelfth Workshop on Fault Diagnosis and Tolerance in Cryptography

September 13, 2015 • Saint Malo, France

(co-located with CHES 2015)

FDTC 2015 is held in cooperation with IACR (`www.iacr.org`)

Fault injection is one of the most exploited means for extracting confidential information from embedded devices and for compromising their intended operation. 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:
  - mechanisms (e.g., using lasers, electromagnetic induction, or clock / power supply manipulation)
  - models of fault injection
  - measures to prevent fault injection (e.g., physical protection, fault diagnosis)
- fault exploitation:
  - attacks on cryptographic devices (HW and SW) or protocols
  - combined implementation attacks
  - models and analysis (e.g., modeling the reliability of systems or protocols)
- countermeasures:
  - fault resistant hardware / implementations of cryptographic algorithms
  - countermeasures to detect fault injections and techniques providing fault tolerance (inherent reliability)
  - 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 has 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, to be provided, author kit. Conference Publishing Services(CPS) will contact directly the authors with instructions and will send links for uploading the manuscripts.

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. Additional submission instructions and further information can be found at:

`www.fdtc-workshop.eu`

Program chairs

Naofumi Homma *Tohoku University*
Victor Lomne *ANSSI*

Program committee

Josep Balasch *KU Leuven*
Olivier Benoit *Qualcomm*
Dooho Choi *ETRI*
Wieland Fischer *Infineon Technologies*
Christophe Giraud *Oberthur Technologies*
Jorge Guajardo Merchan *Bosch LLC*
Sylvain Guilley *Telecom ParisTech*
Jaecheol Ha *Hoseo University*
Ilya Kizhvatov *Riscure*
Pierre-Yvan Liardet *STMicroelectronics*
Philippe Loubet Moundi *Gemalto*
Philippe Maurine *CEA*
Mehran M. Kermani *Roch. Inst. of Tech.*
Debdeep Mukhopadhyay *IIT Kharagpur*
David Oswald *Univ. of Birmingham*
Gerardo Pelosi *Politecnico di Milano*
Arash Reyhani *Univ. of Western Ontario*
Joern-Marc Schmidt *Secunet*
Jean-Pierre Seifert *TU Berlin & T-Labs*
Sergei Skorobogatov *Univ. of Cambridge*
Tsuyoshi Takagi *Kyushu University*
Junko Takahashi *NTT Laboratories*
Michael Tunstall *Cryptography Research*
Vincent Verneuil *NXP Semiconductors*

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*

Saint Malo

Important dates

Submission deadline: May 11, 2015
Notification of acceptance: June 15, 2015
Camera-ready version: July 6, 2015
Workshop: September 13, 2015