FDTC 2017
Fault Diagnosis and Tolerance in Cryptography

Fourteenth Workshop on Fault Diagnosis and Tolerance in Cryptography

September 25, 2017 • Taipei, Taiwan

(co-located with CHES 2017)

FDTC 2017 is held in cooperation with IACR (`www.iacr.org`)

Program chairs

Francesco Regazzoni *Alari - USI, CH*
Patrick Shaumont *Virginia Tech, USA*

Program committee

Reza Azarderakhsh *Florida Atlantic Univ.*
Josep Balasch *KU Leuven*
Shivam Bhasin *NTU Singapore*
Ileana Buhan *Riscure*
Rosario Cammarota *Qualcomm*
Giorgio Di Natale *LIRMM*
Nahid Farhady *Qualcomm*
Yunsi Fei *Northeastern Univ.*
Christophe Giraud *Oberthur Technologies*
Jorge Guajardo Merchan *Bosch LLC*
Sylvain Guilley *Telecom ParisTech*
Jaecheol Ha *Hoseo Univ.*
Johann Heyszl *Faaunhofer Inst.*
Michael Hutter *Cryptography Research*
Ryan Kastner *UCSD*
Juliane Krämer *TU Darmstadt*
Pierre-Yvan Liardet *STMicroelectronics*
Victor Lomné *LIRMM / Univ. Montpellier*
Philippe Maurine *Univ. of Montpellier*
Philippe Loubet Moundi *Gemalto*
Mehran M. Kermani *Roch. Inst. of Tech.*
Debdeep Mukhopadhyay *IIT Kharagpur*
David Oswald *Univ. of Birmingham*
Gerardo Pelosi *Politecnico di Milano*
Ilia Polian *Univ. of Passau*
Arash Reyhani *Univ. of Western Ontario*
Jörn-Marc Schmidt *Secunet*
Sergei Skorobogatov *Univ. of Cambridge*
Takeshi Sugawara *UEC Tokyo*
Junko Takahashi *NTT Laboratories*
Michael Tunstall *Cryptography Research*
Vincent Verneuil *NXP Semiconductors*
Qiaoyan Yu *Univ. of New Hampshire*

Chairs (general, publication, finance)

Guido Marco Bertoni *STMicroelectronics*
Luca Breveglieri *Politecnico di Milano*
Israel Koren *Univ. of Massachusetts*

Steering committee

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

Important dates

Submission deadline: June 9 , 2017
Notification of acceptance: July 6, 2017
Camera-ready version: July 12, 2017
Workshop: September 25, 2017

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, techniques, architectures and design tools for robust cryptographic systems (both hardware and software), and on protecting them against both accidental faults and intentional attacks is essential. Of particular interest are the models and metrics for quantifying the protection of systems and protocols against the malicious injection of faults and for estimating the leaked 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 and exploitation:
  - mechanisms (e.g., lasers, EM induction, clock / power supply manipulation)
  - attacks on cryptographic devices (HW and SW) or protocols
  - combined implementation attacks
- countermeasures:
  - fault resistant hardware / implementations of cryptographic algorithms
  - countermeasures to detect fault injections
  - techniques providing fault tolerance (inherent reliability)
  - fault resistant protocols
  - measures to prevent fault injection (e.g., physical protection, fault diagnosis)
- models and metrics for fault attack analysis:
  - metrics for fault attacks robustness and the leaked information
  - models of fault injection
  - modeling and analysis (e.g., modeling the reliability of systems or protocols)
- fault attack resistant architectures:
  - fault attack resistant processor designs
  - fault attack resistant hardware
  - fault attack resistant software
- design tools supporting analysis of fault attacks and countermeasures:
  - early estimation of fault attack robustness
  - automatic applications of fault countermeasures
- fault attacks and reliability
- 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 up to 8 pages (including the bibliography and appendices), and must be formatted following the instructions in the provided template.

Submission of final papers will be managed by Conference Publishing Services (CPS). 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. Authors of accepted papers with outstanding results of particular interest for the community will receive an invitation to submit an extended version of their work to an invited section of IEEE Transactions on Computers.

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`