12th Workshop on Fault Diagnosis and Tolerance in Cryptography

General Co-chairs:

Luca Breveglieri[1] and Israel Koren[2]

Program Co-chairs:

Naofumi Homma[3] and Victor Lomne[4]

Invited papers Co-chairs: David Naccache[5] and Jean-Pierre Seifert[6]

[1] Politecnico di Milano, Italy; [2] Univ. of Massachusetts, Amherst, USA

[3] Tohoku University, Sendai, Japan; [4] ANSSI, Paris, France

[5] École Normale Supérieure de Paris, France; [6] Technische Universität Berlin, Germany

FDTC 2015

- In cooperation with IACR
- sponsored by
  - Politecnico di Milano
  - University of Massachusetts at Amherst
  - Riscure
  - Micron
  - Alphanov

- Proceedings by the CS Press
  - Included in the IEEE Digital Library (IEEE Explore)

Submissions

- Manuscripts submitted: 26 (12 countries)
- Accepted: 10
- Acceptance rate: 38%

Papers selection

- At least 3 reviewers per paper
- Discussions following the review completion

Program Committee (from 10 countries)

- Josep Balasch
- Oliver Benoit
- Dooho Choi
- Wieland Fischer
- Christophe Giraud
- Jorge Guajardo Merchan
- Sylvain Guilley
- Jaecheol Ha
- Ilya Kizhvatov
- Pierre-Yvan Liardet
- Philippe Loubet Moundi
- Philippe Maurine
- Mehran Mozaffari Kermani
- Debdeep Mukhopadhyay
- David Oswald
- Gerardo Pelosi
- Arash Reyhani
- Jörn-Marc Schmidt
- Jean-Pierre Seifert
- Sergei Skorobogatov
- Tsuyoshi Takagi
- Junko Takahashi
- Michael Tunstall
- Vincent Verneuil

Program co-chairs:

Naofumi Homma
Tohoku University, Japan

Victor Lomné
ANSSI, France

External reviewers

- Sk Subidh Ali
- Alessandro Barenghi
- Alberto Battistello
- Luk Bettale
- Jakub Breier
- Martin Butkus
- Karin Greimel
- Job de Haas
- Michael Hutter
- Walter Mergler
- Sikhar Patranabis
- Falk Schellenberg
- Yosuke Todo
- Harshal Tupsamudre
- Rajesh Velegalati

114 Participants

- France 38
- Germany 26
- USA 14
- The Netherlands 8
- Japan 7
- Korea 7
- Italy, Switzerland 4
- China 2
- Austria, Belgium, Brazil, Israel, Sweden 1

Special Thanks

Benoit Gerard – FDTC Local Arrangements Chair

Emmanuel Prouff (CHES Co-General Chair)

09:05-09:15	**Welcome and Opening Remarks** ***Israel Koren*, *Luca Breveglieri***
09:15-09:55	**Keynote Talk I:** ***Chair: Sylvain Guilley*** **Fault Attacks at the System Level – The Challenge of Securing Application Software** ***Stefan Mangard***
09:55-10:45	**Session 1: Fault Injection: Models and Techniques** ***Chair: Philippe Loubet-Moundi*** **1. EM Injection: Fault Model and Locality** ***Sebastien Ordas, Ludovic Guillaume-Sage and Philippe Maurine*** **2. On the Complexity Reduction of Laser Fault Injection Campaigns using OBIC Measurements** ***Falk Schellenberg, Markus Finkeldey, Bastian Richter, Maximilian Schaepers, Nils Gerhardt, Martin Hofmann and Christof Paar***
10:45-11:10	**Coffee break**
11:10-12:25	**Session 2: DFA: Models and Techniques** ***Chair: Guido Bertoni*** **1. Improved Differential Fault Attack on the Block Cipher SPECK** ***Yuming Huo, Fan Zhang, Xiutao Feng and Li-Ping Wang*** **2. J-DFA: A Novel Approach for Robust Differential Fault Analysis** ***Luca Magri, Silvia Mella, Filippo Melzani, Pasqualina Fragneto and Beatrice Rossi*** **3. Lost in Translation: Fault Analysis of Infective Security Proofs** ***Alberto Battistello and Christophe Giraudy***

12:25-13:40	**Lunch**
13:40-14:20	**Keynote Talk II:** ***Chair: Francesco Regazzoni*** **The Need for Intrinsic Hardware Security below 65 nm** ***Mathias Wagner***
14:20-15:10	**Session 3: Fault Injection Attacks to Cipher Families** ***Chair: Naofumi Homma*** **1. To Exploit Fault Injection on non-Injective Sboxes** ***Guillaume Bethouart and Nicolas Debande*** **2. An Efficient One-Bit Model for Differential Fault Analysis on Simon Family** ***Juan Grados, Fabio Borges, Renato Portugal and Pedro Lara***
15:10-15:35	**Coffee break**
15:35-16:50	**Session 4: Fault Attacks to Cryptographic Devices** ***Chair: Victor Lomné*** **1. Singular Curve Point Decompression Attack** ***Johannes Blomer and Peter Gunther*** **2. Laser Fault Attack on Physically Unclonable Functions** ***Shain Tajik, Heiko Lohrke, Fatemeh Ganji, Jean-Pierre Seifert and Christian Boit*** **3. Improving Fault Attacks on Embedded Software using RISC Pipeline Characterization** ***Bilgday Yuca, Nahid Farhady Ghalaty and Patrick Schaumont***
16:50-17:00	**Closing remarks and Farewell**

2004-2015: Participation

#	Year	Location	Participants
1	2004	Florence, Italy	25
2	2005	Edinburgh, UK	118
3	2006	Yokohama, Japan	103
4	2007	Vienna, Austria	73
5	2008	Washington, USA	82
6	2009	Lausanne, Switzerland	95
7	2010	Santa Barbara, USA	100
8	2011	Nara, Japan	116
9	2012	Leuven, Belgium	113
10	2013	Santa Barbara, USA	105
11	2014	Busan, Korea	115
12	2015	Saint Malo, France	114