13th Workshop on Fault Diagnosis and Tolerance in Cryptography

General Co-chairs:

Luca Breveglieri[1] and Israel Koren[2]

Program Co-chairs:

Philippe Maurine[3] and Michael Tunstall[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] LIRMM, France ; [4] Cryptography Research, USA

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

FDTC 2016

- In cooperation with IACR
- sponsored by
  - Infineon
  - Micron
  - Rambus Cryptography Research
  - Riscure
  - Politecnico di Milano
  - University of Massachusetts at Amherst

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

Submissions

- Manuscripts submitted: 16 (14 countries)
- Accepted: 10
- Acceptance rate: 62%

Papers selection

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

Program Committee (from 10 countries)

- Josep Balasch
- Oliver Benoit
- Wieland Fischer
- Christophe Giraud
- Jorge Guajardo Merchan
- Sylvain Guilley
- Jaecheol Ha
- Naofumi Homma
- Michael Hutter
- Pierre-Yvan Liardet
- Victor Lomne
- Philippe Loubet Moundi
- Mehran Mozaffari Kermani
- Debdeep Mukhopadhyay
- David Oswald
- Gerardo Pelosi
- Arash Reyhani
- Jörn-Marc Schmidt
- Sergei Skorobogatov
- Junko Takahashi
- Vincent Verneuil

Program co-chairs:

Philippe Maurine
ULIMM, France

Michael Tunstall
Cryptography Research, US

External reviewers

- Thomas Schmidt
- Rei Ueno
- Patrick Haddad
- Shahrier B. Shokouhi
- Daniele Fronte
- Thomas De Cnudde
- Sikhar Patranabis
- Nicolas Moro
- Mostafa Taha
- Martin Butkus

100 Participants

- France 23
- Germany 20
- USA 21
- The Netherlands 8
- China 4
- Israel, Japan, Korea, UK 3
- Canada, Belgium, Italy 2
- Austria, Czech Republic, Norway, Singapore, Switzerland 1

Special Thanks

UCSB Conference Services - Local Arrangements

Çetin Kaya Koç (CHES Co-General Chair)

09:05-09:15	**Welcome and Opening Remarks** ***Israel Koren, Luca Breveglieri***
09:15-09:55	**Keynote Talk I:** ***Chair: Jean-Pierre Seifert*** **Attacks on encrypted memory and constructions for memory protection** ***Shay Gueron***
09:55-10:45	**Session 1: Differential Fault Analysis** ***Chair: Debdeep Mukhopadhyay*** **1. Differential fault analysis of SHA3-224 and SHA3-256** ***Pei Luo, Yunsi Fei, Liwei Zhang, A. Adam Ding*** **2. Improved fault analysis on SIMON block cipher family** ***Hua Chen, Jingyi Feng, Vincent Rijmen, Yunwen Liu, Limin Fan, Wei Li***
10:45-11:10	**Coffee break**
11:10-12:25	**Session 2: Fault Injection-based Attacks** ***Chair: Wieland Fischer*** **1. Controlling PC on ARM using fault injection** ***Niek Timmers, Albert Spruyt, Marc Witteman*** **2. Attack on a DFA protected AES by simultaneous laser fault injections** ***Bodo Selmke, Johann Heyszl, Georg Sigl*** **3. Software fault resistance is futile: effective single-glitch attacks** ***Bilgiday Yuce, Nahid Farhady, Harika Santapuri, Chinmay Deshpande, Conor Patrick, Patrick Schaumont***

12:25-13:40	Lunch
13:40-14:20	Keynote Talk II: *Chair: Elke De Mulder* Continuous-time computational aspects of cyber-physical security *Sam Green, Ihsan Cicek, Çetin Koç*
14:20-15:10	Session 3: Fault Sensitivity and Fault Detection *Chair: Sylvain Guilley* 1. Lattice-based signature schemes and their sensitivity to fault attacks *Nina Bindel, Johannes Buchmann, Juliane Krämer* 2. An embedded digital sensor against EM and BB fault injection *David El-Baze, Jean-Baptiste Rigaud, Philippe Maurine*
15:10-15:35	Coffee break
15:35-16:50	Session 4: Countermeasures against Fault Attacks *Chair: Michael Hutter* 1. Fault tolerant implementations of delay-based physically unclonable functions on FPGA *Durga Prasad Sahoo, Sikhar Patranabis, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty* 2. Ring oscillator under laser: potential of PLL based countermeasure against laser fault injection *Wei He, Jakub Breier, Shivam Bhasin, Noriyuki Miura, Makoto Nagat* 3. More efficient private circuits II through threshold implementations *Thomas De Cnudde, Svetla Nikova*
16:50-17:00	Closing remarks and Farewell

2004-2016: 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
13	2016	Santa Barbara, USA	100