11th Workshop on Fault Diagnosis and Tolerance in Cryptography

General Co-chairs:

Luca Breveglieri[1] and Israel Koren[2]

Program Co-chairs:

Dooho (Davy) Choi[3] and Assia Tria[4]

Invited papers Chair: David Naccache[5]

[1] Politecnico di Milano, Milano, Italy
[2] University of Massachusetts, Amherst, USA
[3] Cyber Security Research Lab., ETRI, Korea
[4] CEA-Tech, France
[5] École Normale Supérieure de Paris, France

FDTC 2014

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

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

Submissions

- Manuscripts submitted: 20 (10 countries)
- Accepted: 12

Papers selection

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

Program Committee (from 10 countries)

- Oliver Benoit
- Jae CheolHa
- Wieland Fischer
- Benedikt Gierlichs
- Christophe Giraud
- Jorge Guajardo
- Sylvain Guilley
- Howon Kim
- Ilya Kizhvatov
- Kerstin Lemke-Rust
- Paolo Maistri
- Marcel Medwed
- Mehran Mozaffari
- David Oswald
- Gerardo Pelosi
- Matthieu Rivain
- Sergei Skorobogatov
- Tsuyoshi Takagi
- Junko Takahashi
- Michael Tunstall

Program co-chairs:

Dooho (Davy) Choi
ETRI, Korea

Assia Tria
CEA-Tech, France

External reviewers

- Michel Agoyan
- Josep Balasch
- Alessandro Barenghi
- Alberto Battistello
- Luk Bettale
- Elke De Mulder
- Sho Endo
- Jake Longo Galea
- Laurie Genelle
- Dmitry Khovratovich
- Silvia Mella
- Federico Menarini
- Guilherme Perin
- Falk Schellenberg
- Yosuke Todo

115 Participants

- France 23
- Korea 23
- Germany 19
- Japan, USA 13
- The Netherlands 7
- Iran , Switzerland 3
- Austria, China 2
- Brazil, India, Israel, Italy, Russia, Sweden, UAE 1

Special Thanks

Kyung-Hyune Rhee

Kwangjo Kim (CHES General Chair)

09:05-09:15	**Welcome and Opening Remarks** ***Israel Koren*, *Luca Breveglieri***
09:15-09:55	**Keynote Talk:** ***Chair:*** **Jean-Pierre Seifert** **Tampering Attacks in Pairing-Based Cryptography** ***Johannes, Blömer, Peter Günther, Gennadij Liske***
09:55-10:45	**Session 1: Physical and Design Security of ICs** ***Chair: Jean-Luc Danger*** **1. On the Effects of Clock and Power Supply Tampering on Two Microcontroller Platforms** ***Michael Hoefler, Thomas Korak*** **2. Parametric Trojans for Fault-Injection Attacks on Cryptographic Hardware** ***Raghavan Kumar, Philipp Jovanovic, Wayne Burleson, Ilia Polian***
10:45-11:10	**Coffee break**
11:10-12:25	**Session 2: Algebraic & Differential Fault Analysis** ***Chair: Olivier Benoit*** **1. Algebraic Fault Analysis on GOST for Key Recovery and Reverse Engineering** ***Xinjie Zhao, Shize Guo, Fan Zhang, Tao Wang, Zhijie Shi, Dawu Gu*** **2. Differential Fault Analysis on the Families of SIMON and SPECK Ciphers** ***Harshal Tupsamudre, Shikha Bisht, Debdeep Mukhopadhyay*** **3. Differential Fault Intensity Analysis** ***Nahid F. Ghalaty, Bilgiday Yuce, Mostafa Taha, Patrick Schaumont***

12:25-13:40	**Lunch**
13:40-14:55	**Session 3: Fault Models and Countermeasures** ***Chair: Wieland Fischer*** **1. Fault Sensitivity Analysis Meets Zero-Value Attack** ***Oliver Mischke, Amir Moradi, Tim Güneysu*** **2. Countermeasures against High-Order Fault-Injection Attacks on CRT-RSA** ***Pablo Rauzy, Sylvain Guilley*** ***3.* On Fault Injections in Generalized Feistel Networks** ***Hélène Le Bouder, Gaël Thomas, Yanis Linge, Assia Tria***
14:55-15:20	**Coffee break**
15:20-16:50	**Session 4: Simulated and Experimental Attacks** ***Chair: Naofumi Homma*** ***H.* 1. Blind Fault Attack against SPN Ciphers** ***Roman Korkikian, Sylvain Pelissier, David Naccache*** **2. Clock Glitch Attacks in the Presence of Heating** ***Baris Ege, Thomas Korak, Michael Hutter, Lejla Batina*** **3. Practical Validation of Several Fault Attacks against the Miller Algorithm** ***Nadia El Mrabet, Jacques Fournier, Louis Goubin, Ronan Lashermes, Marie Paindavoine*** **4. A Practical Second-Order Fault Attack against a Real-World Pairing Implementation** ***Johannes Blömer, Ricardo Gomes da Silva, Peter Günther, Juliane Krämer, Jean-Pierre Seifert***
16:50-17:00	**Closing remarks and Farewell**

Pale de CZ

Paradise

The Party

2004-2014: 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