9th Workshop on Fault Diagnosis and Tolerance in Cryptography

General Co-chairs:

Luca Breveglieri[1] and Israel Koren[2]

Program Co-chairs:

Guido Bertoni[3] and Benedikt Gierlichs[4]

Invited papers Chair: David Naccache[5]

[1] Politecnico di Milano, Milano, Italy
[2] University of Massachusetts, Amherst, USA
[3] STMicroelectronics, Agrate Brianza, Italy
[4] Katholieke Universiteit Leuven - COSIC, Leuven, Belgium
[5] École Normale Supérieure de Paris, France

FDTC 2012

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

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

2004-2012: 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	103+

Submissions

- Manuscripts submitted: 20
- Accepted submissions: 10

Papers selection

- At least 3 reviewers per paper
- At least 5 reviewers for papers submitted by a member of the program committee

- 1 week of discussions following the completion of the review process

Participants

- France 28
- Germany 20
- Japan 15
- USA 10
- The Netherlands 4
- Belgium, Sweden, Israel 3
- Singapore, China 3
- Switzerland, Oman 2
- Italy, South Korea 2
- UK, Finland, Austria 1

Program co-chairs:

Guido Bertoni
STMicroelectornics, Italy

Benedikt Gierlichs
KU Leuven, Belgium

Invited talks chair:

David Naccache
École Normale Supérieure de Paris, France

Program committee:

- *Alessandro Barenghi, Politecnico di Milano, Italy*
- *Christophe Clavier, University of Limoges, France*
- *Wieland Fischer, Infineon Technologies, Germany*
- *Christophe Giraud, Oberthur Technologies, France*
- *Jorge Guarjardo, Bosch, USA*
- *Sylvain Guilley, Telecom ParisTech, France*
- *Helena Handschuh, Cryptography Research Inc., USA*
- *Dusko Karaklajic, KU Leuven, Belgium*
- *Kerstin Lemke-Rust, HBRS, Germany*
- *Marcel Medwed, UCL Crypto Group, Belgium*
- *Debdeep Mukhopadhyay, IIT Kharagapur, India*
- *Matthieu Rivain, CryptoExperts, France*
- *Jörn-Marc Schmidt, Technische Universität Graz, Austria*
- *Sergei Skorobogatov, University of Cambridge, UK*
- *Junko Takahashi, NTT Corporation, Japan*
- *Michael Tunstall, University of Bristol, UK*
- *Marc Witteman, Riscure, The Netherlands*

Special Thanks

Local arrangements provided by the KU Leuven team headed by

Benedikt Gierlichs

In charge today: Oscar Reparaz

09:05-09:15	**Welcome and Opening Remarks** ***Israel Koren, Luca Breveglieri***
09:15-09:55	**1st Keynote Talk:** ***Chair: Sylvain Guilley*** **Techniques for EM Fault Injection: Equipment and Experimental Results** ***Philippe Maurine***
09:55-10:45	**Session 1: Fault injection and simulation** ***Chair: Kerstin Lemke-Rust*** **1. Electromagnetic Transient Faults Injection on a Hardware and Software Implementation of AES** ***Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson and Assia Tria*** **2. Circuit Simulation for Fault Sensitivity Analysis and its Application to Cryptographic LSI** ***Takeshi Sugawara, Daisuke Suzuki and Toshihiro Katashita***
10:45-11:10	**Coffee break**
11:10-12:25	**Session 2: Differential fault analysis** ***Chair: Francesco Regazzoni*** **1. Differential Fault Analysis on Lightweight Blockciphers with Statistical Cryptanalysis Techniques** ***Dawu Gu, Juanru Li, Sheng Li, Zheng Guo and Junrong Liu*** **2. A DFA on AES based on the Entropy of Error Distributions** ***Ronan Lashermes, Guillaume Reymond, Jean-Max Dutertre, Jacques Fournier, Bruno Robisson and Assia Tria*** **3. Differential Fault Analysis on Groestl** ***Wieland Fischer and Christian A. Reuter***

12:25-13:40	Lunch
13:40-14:20	2nd Invited Talk: *Chair:* Helena Handschuh It's not my Fault – on Fault Attacks on Symmetric Cryptography *Bart Preneel*
14:20-15:10	Session 3: Fault analysis *Chair:* Luca Breveglieri 1. Combined Fault and Side-Channel Attacks on the AES Key Schedule *François Dassance and Alexandre Venelli* 2. Harnessing biased Faults in Attacks on ECC-based Signature Schemes *Celine Blondeau, Kimmo Jarvinen, Dan Page and Michael Tunstall*
15:10-15:35	Coffee break
15:35-16:50	Session 4: Countermeasures *Chair: Wieland Fischer* 1. On the Need of Randomness in Fault Attack Countermeasures – Application to AES *Adrian Thillard, Thomas Roche and Victor Lomne* 2. An Efficient Countermeasure against Fault Sensitivity Analysis using Configurable Delay Block *Sho Endo, Yang Li, Naofumi Homma, Kazuo Sakiyama, Kazuo Ohta and Takafumi Aoki* 3. Random Active Shield *Sylvain Guilley, Sébastien Briais, Thibault Porteboeuf, Jean-Luc Danger, Jean-Michel Cioranesco and David Naccache*
16:50-17:00	Closing remarks and Farewell