10th Workshop on Fault Diagnosis and Tolerance in Cryptography

General Co-chairs:

Luca Breveglieri[1] and Israel Koren[2]

Program Co-chairs:

Jöern-Marc Schmidt[3] and Wieland Fischer[4]

Invited papers Chair: David Naccache[5]

[1] Politecnico di Milano, Milano, Italy
[2] University of Massachusetts, Amherst, USA
[3] Graz University, Austria
[4] Infineon, Germany
[5] École Normale Supérieure de Paris, France

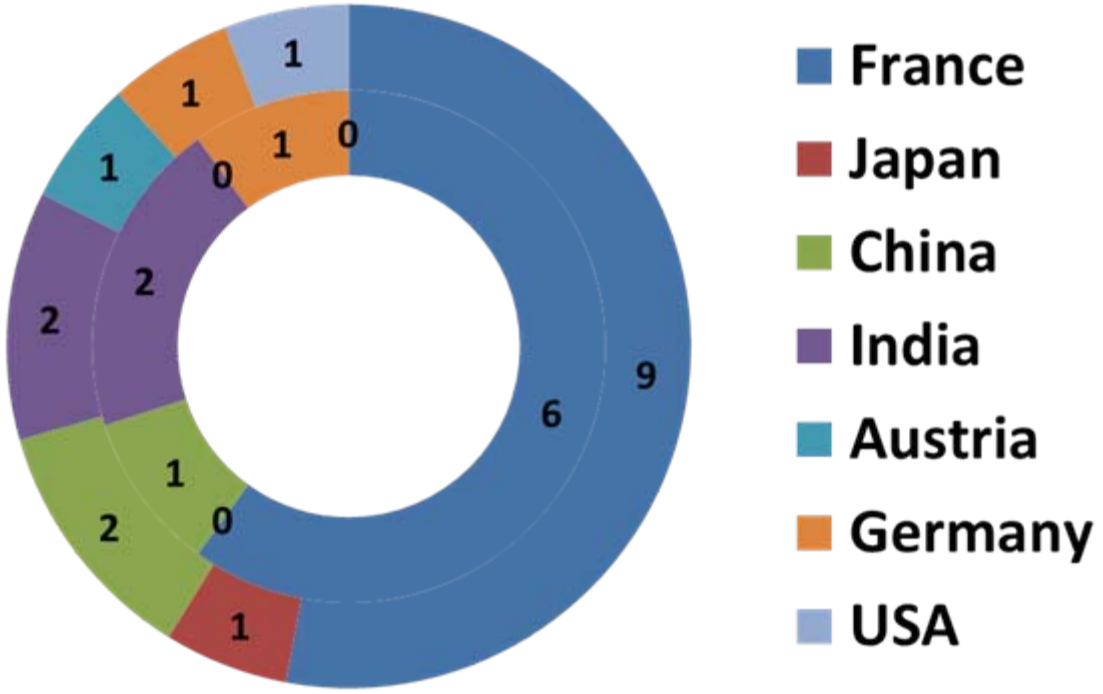
FDTC 2013

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

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

Submissions

- Manuscripts submitted: 17 (From 7 countries)
- Accepted: 10

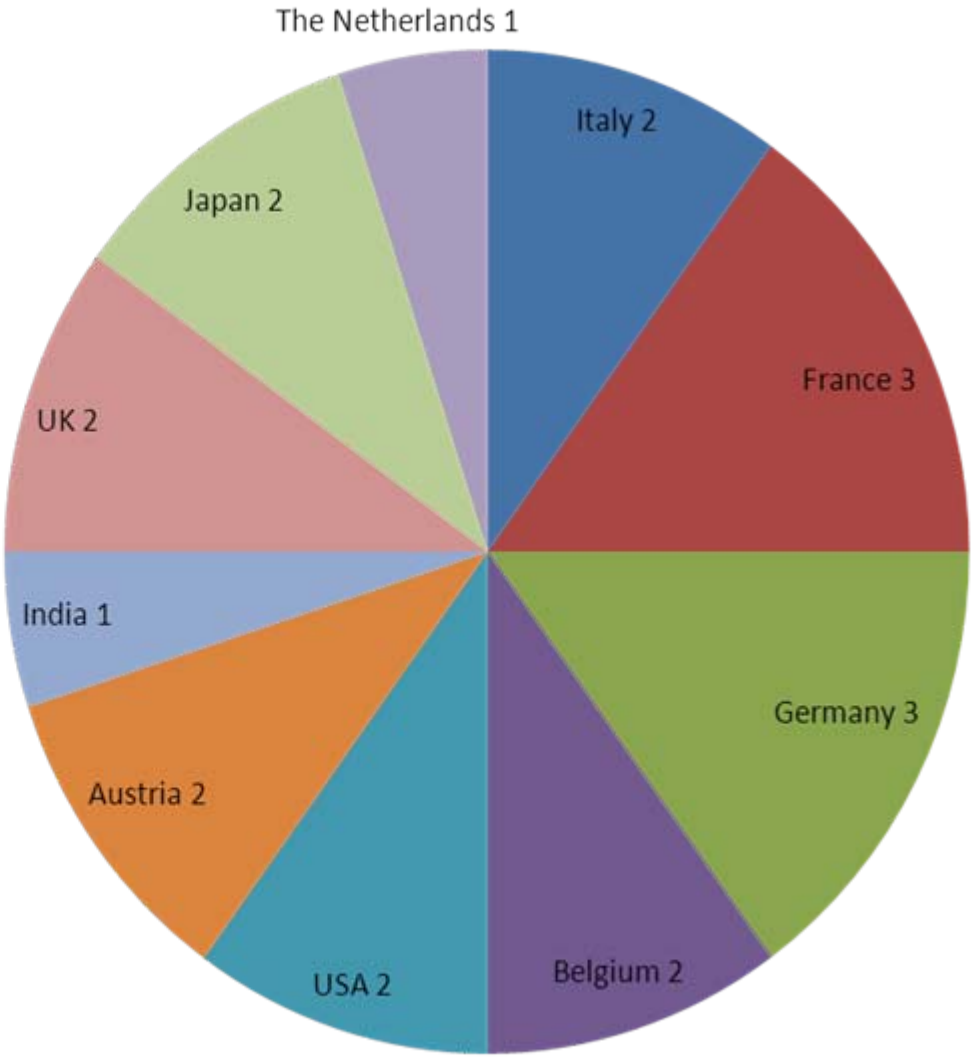


Papers selection

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

Program Committee

- 20 PC Members
  - 10 Countries
  - ½ Academia, ½ Industry
  - 20 External reviewers



Program Committee

- Guido Bertoni
- Benedikt Gierlichs
- Christophe Giraud
- Jorge Guajardo
- Sylvain Guilley
- Helena Handschuh
- Ilya Kizhvatov
- Kerstin Lemke-Rust
- Marcel Medwed
- Debdeep Mukhopadhyay
- David Oswald
- Gerardo Pelosi
- Matthieu Rivain
- Sergei Skorobogatov
- Tsuyoshi Takagi
- Junko Takahashi
- Michael Tunstall
- Ingrid Verbauwhede

Program co-chairs:

Jöern-Marc Schmidt
Graz University, Austria

Wieland Fischer
Infineon, Germany

External reviewers

- Rajat Subhra Chakraborty
- Elke De Mulder
- Job de Haas
- Dmitry Khovratovich
- Alexandre Berzati
- Shiho Moriai
- Jake Longo Galea
- Kazuo Sakiyama
- Nicolas Morin
- Falk Schellenberg
- Andrea Palomba
- Vladimir Rozic
- Jeroen Delvaux
- Zouha Cherif Jouini
- Jeroen Delvaux
- Marcin Wójcik
- Jing Pan
- Timo Kasper
- Shivam Bhasin
- Emmanuel Prouff

105 Participants

- France 27
- Germany 20
- USA 20
- Japan 8
- The Netherlands 7
- South Korea 7
- Austria, Sweden 3
- Italy, India, Switzerland 2
- Canada, China, Israel, UK 1

Special Thanks

UCSB Campus Conference Services:

Sally J. Vito, Director

Eriko MacDonald

Fatima Mendez

09:05-09:15	**Welcome and Opening Remarks** ***Israel Koren*, *Luca Breveglieri***
09:15-09:55	**1st Keynote Talk:** ***Chair: Jean-Pierre Seifert*** **Security Risks Posed by Modern IC Debug and Diagnosis Tools** ***Christian Boit***
09:55-10:45	**Session 1: IC-Security** ***Chair: Marcel Medwed*** **1. Hardware Trojan Horses in Cryptographic IP Cores** ***Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, Xuan Thuy Ngo and Laurent Sauvage*** **2. Invasive PUF Analysis** ***Dmitry Nedospasov, Clemens Helfmeier, Jean-Pierre Seifert and Christian Boit***
10:45-11:10	**Coffee break**
11:10-12:25	**Session 2: Differential fault analysis** ***Chair: Christophe Giraud*** **1. Improving and Evaluating Differential Fault Analysis on LED with Algebraic Techniques** ***Xinjie Zhao, Shize Guo, Fan Zhang, Zhijie Shi and Tao Wang*** **2. Differential Fault Analysis of MICKEY-128 2.0** ***Sandip Karmakar and Dipanwita Roy Chowdhury*** **3. Improved Differential Fault Analysis of CLEFIA** ***Sk Subidh Ali and Debdeep Mukhopadhyay***

12:25-13:40	**Lunch**
13:40-14:20	**2nd Invited Talk:** ***Chair: Joern-Marc Schmidt*** **Elliptic Curve Cryptosystems in the Presence of Faults** ***Marc Joye***
14:20-15:10	**Session 3: Fault Attack Modeling** ***Chair: Marc Witteman*** **1. Electromagnetic Fault Injection: towards a Fault Model on a 32-bit Microcontroller** ***Nicolas Moro, Amine Dehbaoui, Karine Heydemann, Bruno Robisson and Emmanuelle Encrenaz*** **2. Fault Model Analysis of Laser-induced Faults in SRAM Memory Cells** ***Cyril Roscian, Alexandre Sarafianos, Jean-Max Dutertre and Assia Tria***
15:10-15:35	**Coffee break**
15:35-16:50	**Session 4: Attacks on AES** ***Chair:Debdeep Mukhopadhyay*** **1. Fault Analysis of Infective AES Computations** ***Alberto Battistello and Christophe Giraud*** **2. Fault Attacks on AES with Faulty Ciphertexts Only** ***Thomas Fuhr and Eliane Jaulmes and Victor Lomne and Adrian Thillard*** **3. Reverse Engineering of a Secret AES-like Cipher by Ineffective Fault Analysis** ***Christophe Clavier and Antoine Wurcker***

2004-2013: 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