
# 8th Workshop on Fault Diagnosis and Tolerance in Cryptography


## General Co-chairs:

**Luca Breveglieri[1] and Israel Koren[2]**

## Program Co-chairs:

**Junko Takahashi[3] and Sylvain Guilley[4]**

## Invited papers Chair: David Naccache[5]

[1] Politecnico di Milano, Milano, Italy
[2] University of Massachusetts, Amherst, USA
[3] NTT Information Laboratories, Tokyo, Japan
[4] Telecom ParisTech, Paris, France
[5] École Normale Supérieure de Paris, France

# FDTC 2011

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

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

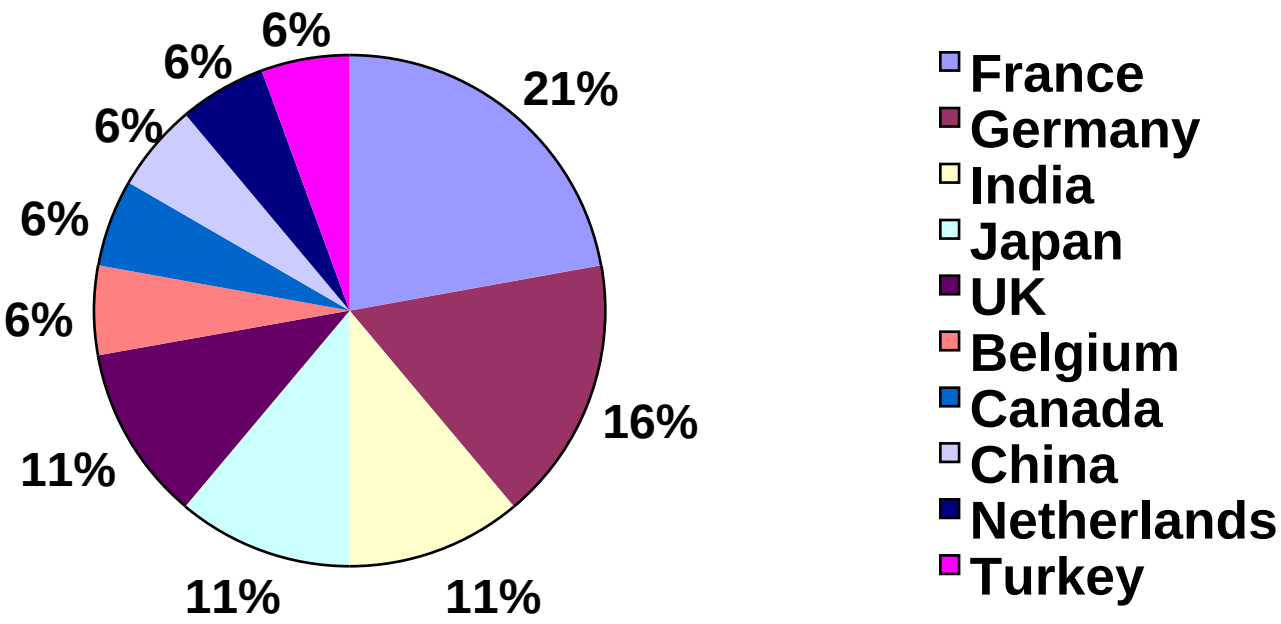
# 2004-2011: Participation

| # | 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 |

# Submissions

- Manuscripts submitted: 18
- Accepted submissions: 10

## Submissions per country



# Papers selection

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

- 1 week of discussions following the acceptance of reviews

- 68 reviews in total
- 45 discussions

# Participants

- Japan 41
- France 23
- Germany 11
- USA 9
- The Netherlands 6
- Belgium, Korea 4
- Iran, Singapore 3
- Canada, Israel, Italy, Sweden 2
- India, Switzerland, Turkey 1

## *Program co-chairs:*

**Junko Takahashi**
NTT Information Laboratories, Tokyo, Japan

**Sylvain Guilley**
Telecom ParisTech, Paris, France

## *Invited talks chair:*

**David Naccache**
École Normale Supérieure de Paris, France

## *Program committee:*

- *Guido Bertoni ,ST Microelectronics, Italy*
- *Wieland Fischer, Infineon Technologies, Germany*
- *Christophe Giraud, Oberthur Technologies, France*
- *Helena Handschuh, K.U.Leuven, Belgium & Intrinsic-ID Inc., USA*
- *Naofumi Homma, Tohoku University, Japan*
- *Marc Joye, Technicolor, France*
- *Ramesh Karri, Polytechnic University, USA*
- *Régis Leveugle TIMA, France*
- *Debdeep Mukhopadhyay, IIT Kharagapur, India*
- *Gerardo Pelosi, Politecnico di Milano, Italy*
- *Denis Real, Ministry of Defense, France*
- *Kazuo Sakiyama, University of Electro Communication, Japan*
- *Jörn-Marc Schmidt, Technische Universität Graz, Austria*
- *Sergei Skorobogatov, University of Cambridge, UK*
- *Francois-Xavier Standaert, Univ. Catholique de Louvain, Belgium*
- *Michael Tunstall, University of Bristol, UK*
- *Ingrid Verbauwhede, Katholieke Universiteit Leuven, Belgium*

# Special Thanks

Local arrangements provided by

- Tetsuya Izu, Fujitsu
- Yumi Sakemi, Fujitsu

- Junko Takahashi, NTT Information Laboratories

| | |
|---|---|
| **09:09-09:15** | **Welcome and Opening Remarks**<br>***Israel Koren*, *Luca Breveglieri*** |
| **09:15-09:55** | **1st Keynote Talk:** ***Chair: Christophe Giraud***<br>**The Fault Attack Jungle – A Classification Model to Guide You**<br>***Ingrid Verbauwhede, Joern-Marc Schmidt and Dusko Karaklajic*** |
| **09:55-10:45** | **Session 1: Fault attacks on elliptic curves** ***Chair: Naofumi Homma***<br>**1. Fault Sensitivity Analysis Against Elliptic Curve Cryptosystems**<br>***Hikaru Sakamoto, Yang Li, Kazuo Ohta and Kazuo Sakiyama***<br>**2. A Cost-Effective FPGA-based Fault Simulation Environment**<br>***Angelika Janning, Johann Heyszl, Frederic Stumpf and Georg Sigl*** |
| **10:45-11:10** | **Coffee break** |
| **11:10-12:00** | **Session 2: Differential fault attacks** ***Chair: Francesco Regazzoni***<br>**1. A Differential Fault Analysis on AES Key Schedule using Single Fault**<br>***Sk Subidh Ali and Debdeep Mukhopadhyay***<br>**2. From AES-128 to AES-192 and AES-256: How to Adapt Differential Fault Analysis Attacks**<br>***Noémie Floissac and Yann L'Hyver***<br>**3. Differential Fault Analysis on the SHA1 compression function**<br>***Ludger Hemme and Lars Hoffmann*** |

| | |
|---|---|
| **12:25-13:40** | **Lunch** |
| **13:40-14:20** | **2nd Invited Talk:** ***Chair: Guido Bertoni***<br>**Fault Injection, a Fast Moving Target in Evaluations**<br>***Rob Bekkers and Hans König*** |
| **14:20-15:10** | **Session 3: Algebraic fault detection** ***Chair: Wieland Fischer***<br>**1. On Protecting Cryptographic Applications against Fault Attacks using Residue Codes**<br>***Kazim Yumbul, Serdar S. Erdem and Erkay Savas***<br>**2. A High-Performance Fault Diagnosis Approach for the AES SubBytes utilizing Mixed Bases**<br>***Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh*** |
| **15:10-15:35** | **Coffee break** |
| **15:35-16:50** | **Session 4: Fault injection in practice** ***Chair: Marc Joye***<br>**1. Practical Optical Fault Injection on Secure Microcontrollers**<br>***J. G. J. van Woudenberg, M. F. Witteman and F. Menarini***<br>**2. Local and Direct EM Injection of Power into CMOS Integrated Circuits**<br>***F. Poucheret, K. Tobich, M. Lisart, B. Robisson, L. Chusseau and P. Maurine***<br>**3. An in-Depth and black-Box Characterization of the Effects of Clock Glitches on 8-bit MCUs**<br>***Josep Balasch, Benedikt Gierlichs and Ingrid Verbauwhede*** |
| **16:50-17:00** | **Closing remarks and Farewell** |