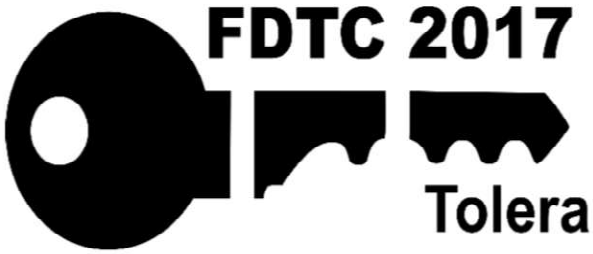

Fault Diagnosis and Tolerance in Cryptography

14th Workshop on **F**ault **D**iagnosis and **T**olerance in **C**ryptography

FDTC 2017

Fault Diagnosis and Tolerance in Cryptography

Program Co-chairs:

Francesco Regazzoni[1] and Patrick Schaumont[2]

Publication Chair:

Luca Breveglieri[3]

Financial Chair:

Israel Koren[4]

Invited papers Co-chairs:

David Naccache[5] and Jean-Pierre Seifert[6]

General Chair:

Guido Bertoni[7]

[1] Alari, Switzerland
[2] Virginia Tech, USA
[3] Politecnico di Milano, Italy
[4] Univ. of Massachusetts, Amherst, USA
[6] École Normale Supérieure de Paris, France
[7] Technische Universität Berlin, Germany
[1] Consultant, Italy

FDTC 2017

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


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

Submissions

- Manuscripts submitted: 19 (11 countries)
- Accepted: 9
- Acceptance rate: 47%

Papers selection

- 96 reviews
  - 1 paper with 4 reviews
  - 16 papers with 5 reviews
  - 2 papers with 6 reviews

More data on submissions

country	authors	submitted	accepted	acceptance rate
Belgium	3	1.00	0.00	0.00
Canada	1	1.00	0.00	0.00
China	4	1.00	0.00	0.00
France	12	3.00	1.00	0.33
Germany	8	1.00	1.00	1.00
India	6	1.68	0.93	0.55
Japan	6	1.00	1.00	1.00
Netherlands	7	3.00	2.00	0.67
Singapore	4	1.32	1.07	0.81
Switzerland	2	1.00	1.00	1.00
USA	15	4.00	1.00	0.25

Data from easychair

Invited talk and Panel

Giorgio Di Natale

Hardware security and trust:

where we are and where we should go.

Controlled fault injection:

wishful thinking, thoughtful engineering, or just luck?

J. Heyszl, M. Joye, I. Polian, M. Witteman, I. Verbauwhede

Program Committee

- Reza Azarderakhsh
- Josep Balasch
- Shivam Bhasin
- Ileana Buhan
- Rosario Cammarota
- Giorgio Di Natale
- Nahid Farhady
- Yunsi Fei
- Christophe Giraud
- Jorge Guajardo Merchan
- Sylvain Guilley
- Johann Heyszl
- Jaecheol Ha
- Michael Hutter
- Mehran M. Kermani
- Juliane Krämer
- Ryan Kastner
- Pierre-Yvan Liardet
- Victor Lomne
- Philippe Loubet Moundi
- Philippe Maurine
- Debdeep Mukhopadhyay
- David Oswald
- Gerardo Pelosi
- Ilia Polian
- Arash Reyhani
- Takeshi Sugawara
- Jörn-Marc Schmidt
- Sergei Skorobogatov
- Junko Takahashi
- Michael Tunstall
- Vincent Verneuil
- Qiaoyan Yu

Special Thanks

Support for local arrangement:

- Wei-Chih Hong, Feng Chia University

CHES Co-General Chairs

- Chen-Mou Cheng, NTU Taiwan
- Bo-Yin Yang, Academia Sinica Taiwan

09:05-09:15	**Welcome and Opening Remarks** *Guido Bertoni, Luca Breveglieri, Israel Koren*
09:15-10:00	**Keynote Talk:** *Chair: Francesco and Patrick* **Hardware security and trust: where we are and where we should go** *Giorgio Di Natale (LIRMM)*
10:00-10:50	**Session 1: System-Level Fault Attacks** *Chair: Elif Bilge Kavun* 1.**Escalating privileges in Linux using voltage fault injection** *Niek Timmers and Cristofaro Mun* 2. **Safety != security. On the resilence of ASIL-D certified microcontrollers against fault injection attacks** *Ramiro Pareja, Nils Wiersma and Marc Witteman*
10:50-11:10	**Coffee break**
11:10-12:25	**Session 2: Fault Attacks on Primitives** *Chair: Erich Wenger* 1. **Practical fault attack against the Ed25519 and EdDSA signature schemes** *Sylvain Pelissier and Yolan Romailler* 2. **One plus one is more than two: a practical combination of power and fault analysis attacks on PRESENT and PRESENT-like block ciphers** *Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay and Shivam Bhasin* 3. **A practical fault attack on ARX-like ciphers with a case study on ChaCha20** *S.V. Dilip Kumar, Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay, Shivam Bhasin, Anupam Chattopadhyay and Anubhab Baksi*

12:25-13:30	Lunch
13:40-14:20	**Session 3: Laser Fault Attacks** *Chair: Michael Hutter* 1. Laser-induced fault injection on smartphone bypassing the secure boot *Aurélien Vasselle, Hugues Thiebeauld, Adèle Morisset, Quentin Maouhoub and Sebastien Ermeneux* 2. Exploiting bitflip detector for non-invasive probing and its application to ineffective fault analysis *Takeshi Sugawara, Natsu Shoji, Kazuo Sakiyama, Kohei Matsuda, Noriyuki Miura and Makoto Nagata*
14:20-15:10	**Session 4: Design Tools** *Chair: Shivam Bhasin* 1. CAMFAS: a compiler approach to mitigate fault attacks via enhanced SIMDization *Zhi Chen, Junjie Shen, Alexandru Nicolau, Alexander V. Veidenbaum, Rosario Cammarota and Nahid Farhady Ghalaty* 2.AutoFault: towards automatic construction of algebraic fault attacks *Jan Burchard, Maël Gay, Ange Salome Messeng Ekossono, Jan Horacek, Bernd Becker, Tobias Schubert, Martin Kreuzer and Ilia Polian*

15:10-15:35	**Coffee break**
15:35-16:50	**Panel** ***Moderators: Francesco Regazzoni and Patrick Schaumont*** **Controlled fault injection: wishful thinking, thoughtful engineering, or just luck?** ***Johann Heyszl (Fraunhofer AISEC), Marc Joye (NXP Semiconductors), Ilia Polian (University of Passau), Marc Witteman (Riscure), Ingrid Verbauwhede (KU Leuven)***
16:50-17:00	**Closing remarks and Farewell**