FDTC 2022 Fault Diagnosis and Tolerance in Cryptography

Fault Diagnoses and Tolerance in Cryptography 2022

Shivam Bhasin[1] **Praveen Kumar Vadnala**[2]

[1]Nanyang technological University, Singapore & [2]RISCURE, Netherlands

16 September, 2022 – cyberspace

Chairs

• Program:	**Shivam Bhasin**	Nanyang Technological University, Singapore
	Praveen Vadnala	RISCURE, Netherlands
• General:	**Michael Tunstall**	*Rambus Cryptography Research*
• Publication:	**Luca Breveglieri**	*Politecnico di Milano*
• Finance:	**Israel Koren**	*University of Massachusetts*

Steering Committee:

• **Luca Breveglieri**	Politecnico di Milano
• **Israel Koren**	University of Massachusetts
• **David Naccache**	ENS de Paris
• **Jean-Pierre Seifert**	TU Berlin & T-Labs

Sponsors – Thank You!

POLITECNICO MILANO

UMASS AMHERST

NewAE Technology

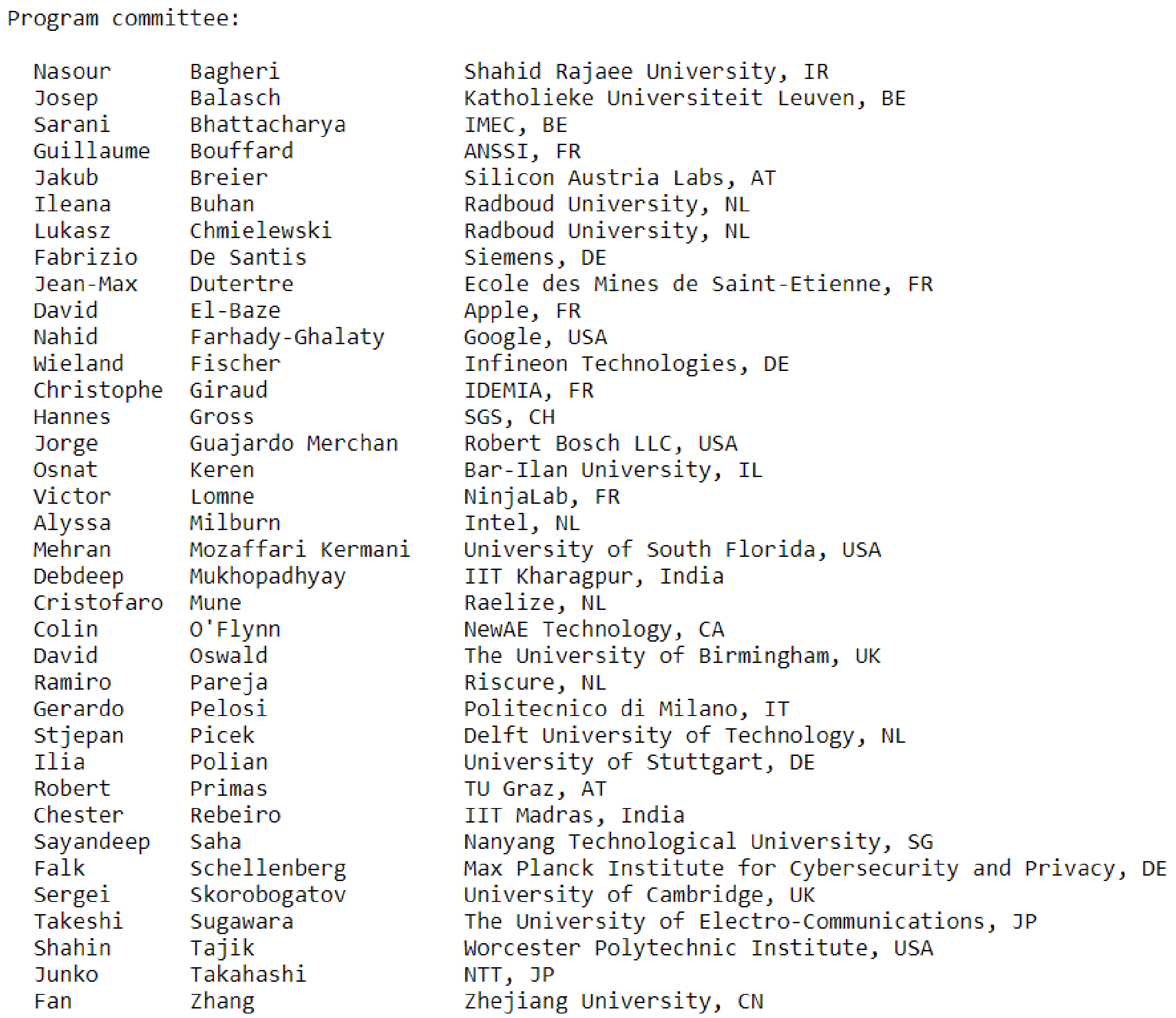
Rambus

infineon

riscure

Visit our free online workshop
www.riscure.com/workshop-live

Program Committee

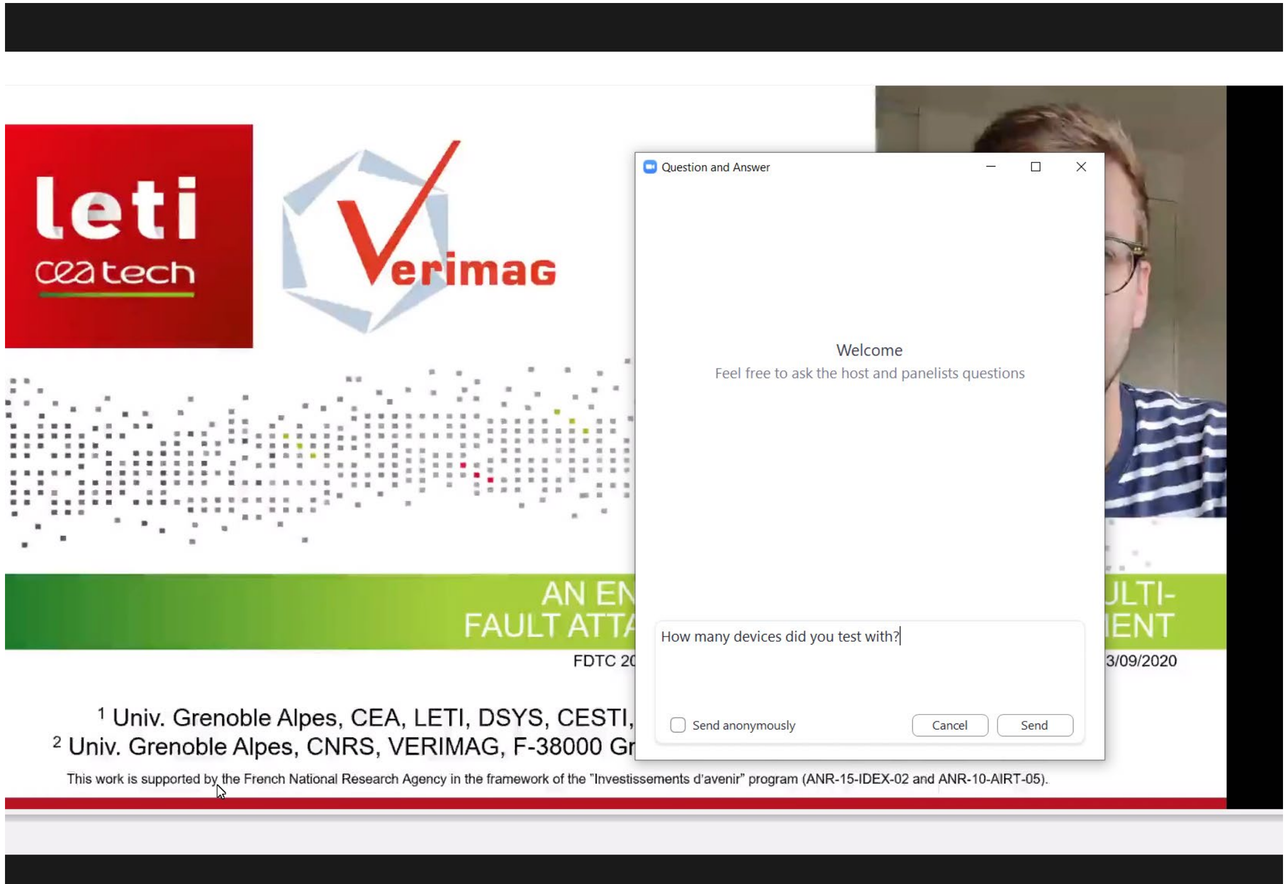


Program committee:

Nasour	Bagheri	Shahid Rajaee University, IR
Josep	Balasch	Katholieke Universiteit Leuven, BE
Sarani	Bhattacharya	IMEC, BE
Guillaume	Bouffard	ANSSI, FR
Jakub	Breier	Silicon Austria Labs, AT
Ileana	Buhan	Radboud University, NL
Lukasz	Chmielewski	Radboud University, NL
Fabrizio	De Santis	Siemens, DE
Jean-Max	Dutertre	Ecole des Mines de Saint-Etienne, FR
David	El-Baze	Apple, FR
Nahid	Farhady-Ghalaty	Google, USA
Wieland	Fischer	Infineon Technologies, DE
Christophe	Giraud	IDEMIA, FR
Hannes	Gross	SGS, CH
Jorge	Guajardo Merchan	Robert Bosch LLC, USA
Osnat	Keren	Bar-Ilan University, IL
Victor	Lomne	NinjaLab, FR
Alyssa	Milburn	Intel, NL
Mehran	Mozaffari Kermani	University of South Florida, USA
Debdeep	Mukhopadhyay	IIT Kharagpur, India
Cristofaro	Mune	Raelize, NL
Colin	O'Flynn	NewAE Technology, CA
David	Oswald	The University of Birmingham, UK
Ramiro	Pareja	Riscure, NL
Gerardo	Pelosi	Politecnico di Milano, IT
Stjepan	Picek	Delft University of Technology, NL
Ilia	Polian	University of Stuttgart, DE
Robert	Primas	TU Graz, AT
Chester	Rebeiro	IIT Madras, India
Sayandeep	Saha	Nanyang Technological University, SG
Falk	Schellenberg	Max Planck Institute for Cybersecurity and Privacy, DE
Sergei	Skorobogatov	University of Cambridge, UK
Takeshi	Sugawara	The University of Electro-Communications, JP
Shahin	Tajik	Worcester Polytechnic Institute, USA
Junko	Takahashi	NTT, JP
Fan	Zhang	Zhejiang University, CN

Zoom Conference Notes

- Please use the **Q&A function** to ask questions.
- Please use the **chat function** for general conference chat.



AN EN… ULTI-
FAULT ATTA… IENT

FDTC 20… 3/09/2020

[1] Univ. Grenoble Alpes, CEA, LETI, DSYS, CESTI,
[2] Univ. Grenoble Alpes, CNRS, VERIMAG, F-38000 Gr

This work is supported by the French National Research Agency in the framework of the "Investissements d'avenir" program (ANR-15-IDEX-02 and ANR-10-AIRT-05).

Question and Answer

Welcome
Feel free to ask the host and panelists questions

How many devices did you test with?

☐ Send anonymously

Papers

Submitted Papers:

- 15 papers submitted
- Reviewed with PC members and additional reviewers
- Most papers received 3 reviews.

Accepted Papers:

- 7 regular papers (around 54%)
- 1 short paper (around 25%)
- Overall, around 53% acceptance rate

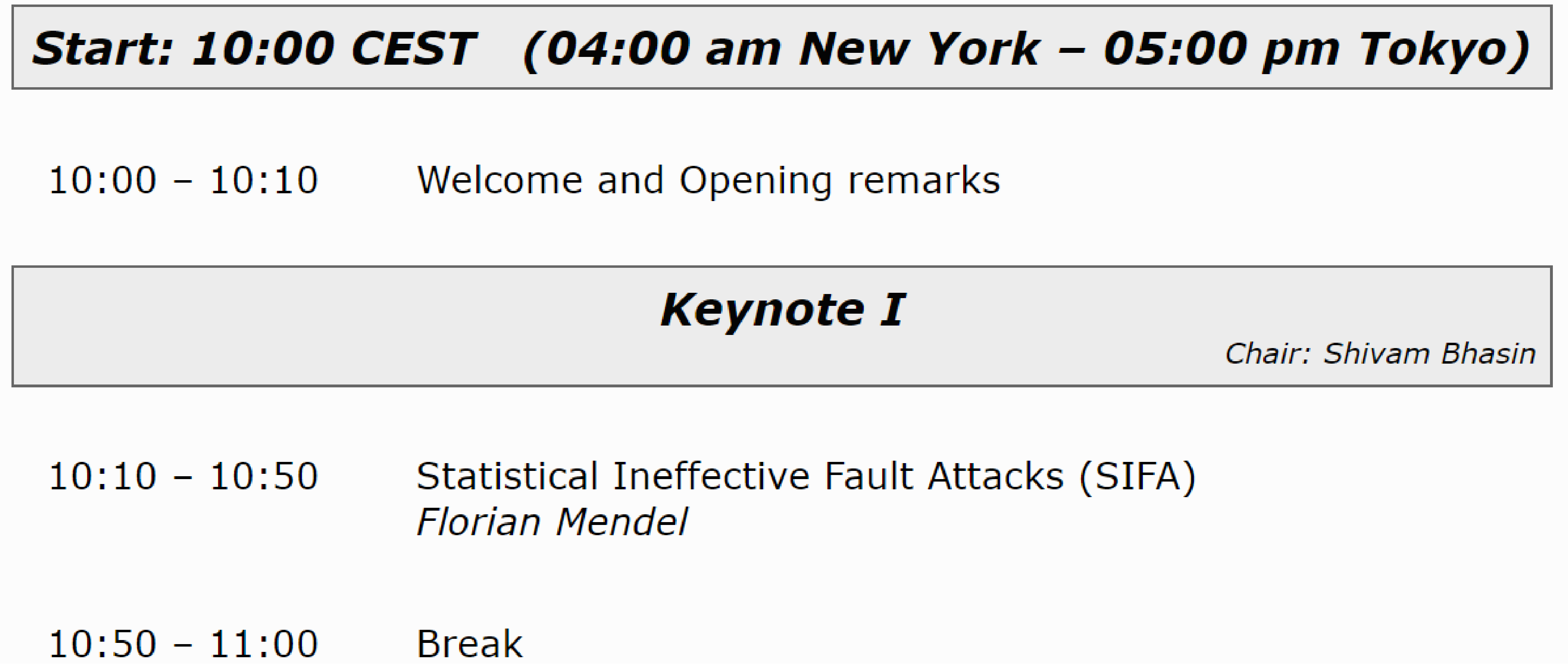
The proceedings will be published by CPS (on IEEExplore).

Invited Talks

- Statistical Ineffective Fault Attacks (SIFA)
  - Florian Mendel
  - Cryptographer & Security Architect, Infineon Technologies

- Pre-silicon fault simulation: Hard and Important
  - Jasper van Woudenberg
  - CTO North America, RISCURE

Program Schedule



Start: 10:00 CEST (04:00 am New York – 05:00 pm Tokyo)

10:00 – 10:10	Welcome and Opening remarks

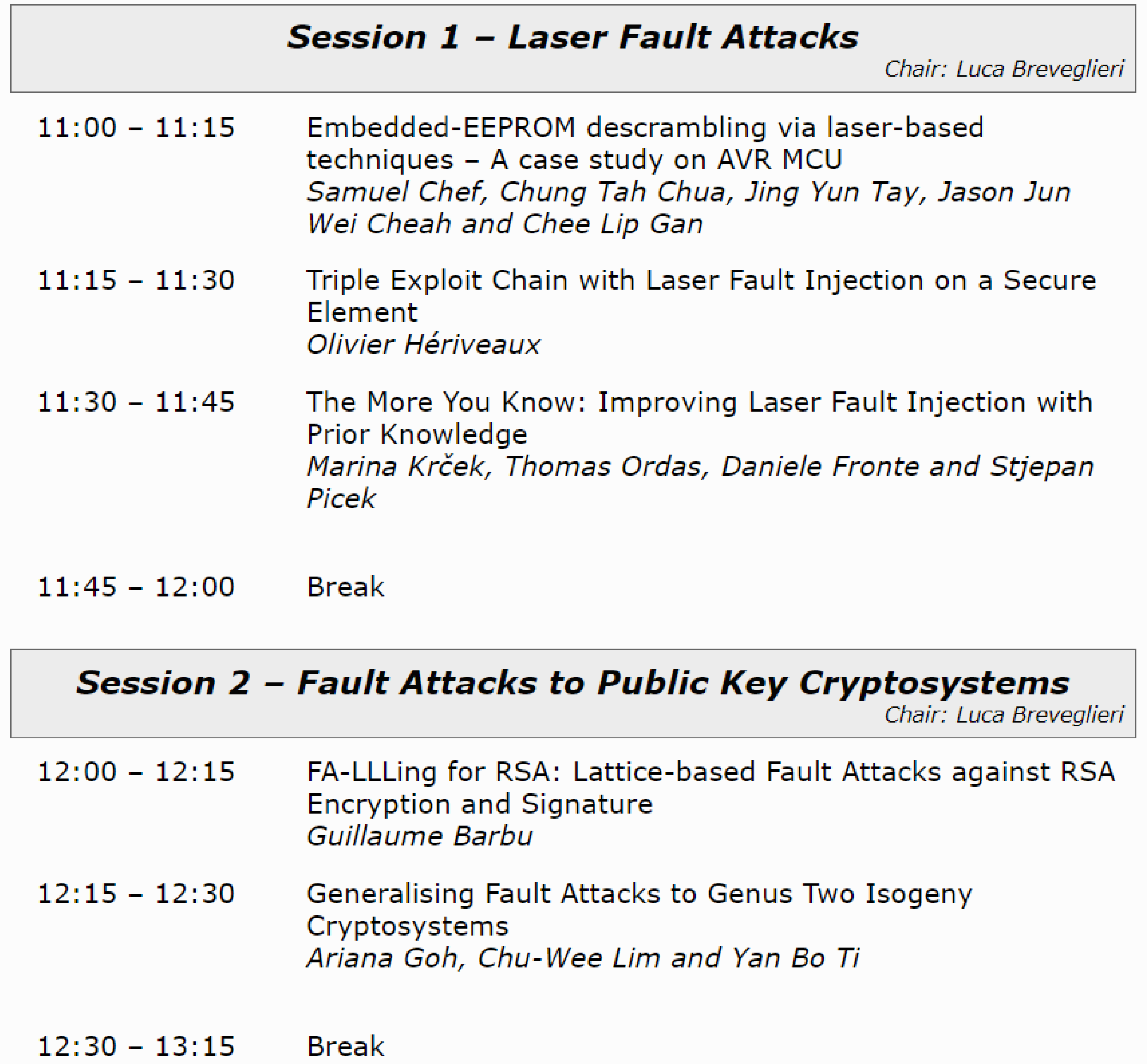
Keynote I

Chair: Shivam Bhasin

10:10 – 10:50	Statistical Ineffective Fault Attacks (SIFA) *Florian Mendel*
10:50 – 11:00	Break

FDTC 2022
Fault Diagnosis and
Tolerance in Cryptography

Program Schedule



Session 1 – Laser Fault Attacks

Chair: Luca Breveglieri

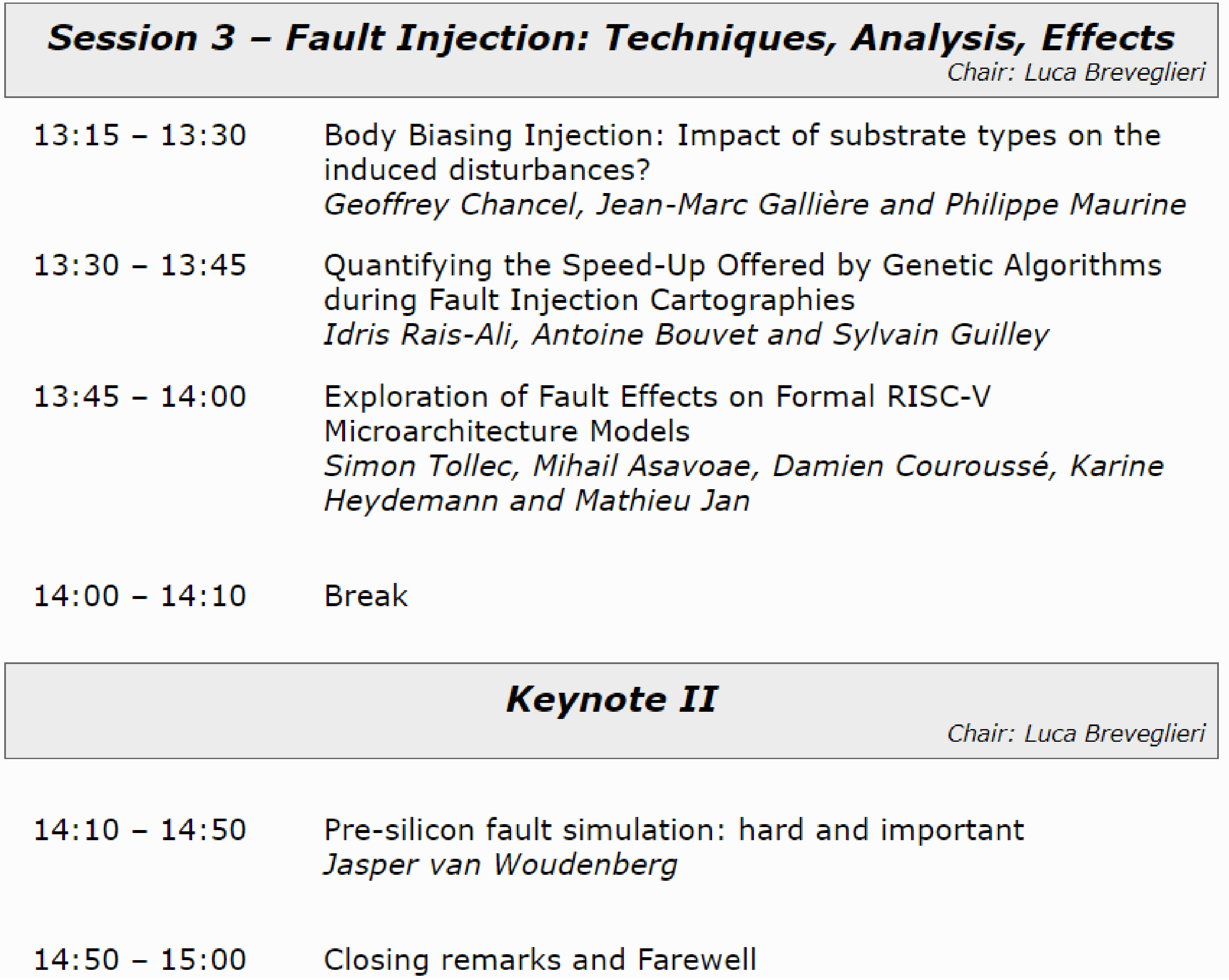
11:00 – 11:15	Embedded-EEPROM descrambling via laser-based techniques – A case study on AVR MCU *Samuel Chef, Chung Tah Chua, Jing Yun Tay, Jason Jun Wei Cheah and Chee Lip Gan*
11:15 – 11:30	Triple Exploit Chain with Laser Fault Injection on a Secure Element *Olivier Hériveaux*
11:30 – 11:45	The More You Know: Improving Laser Fault Injection with Prior Knowledge *Marina Krček, Thomas Ordas, Daniele Fronte and Stjepan Picek*
11:45 – 12:00	Break

Session 2 – Fault Attacks to Public Key Cryptosystems

Chair: Luca Breveglieri

12:00 – 12:15	FA-LLLing for RSA: Lattice-based Fault Attacks against RSA Encryption and Signature *Guillaume Barbu*
12:15 – 12:30	Generalising Fault Attacks to Genus Two Isogeny Cryptosystems *Ariana Goh, Chu-Wee Lim and Yan Bo Ti*
12:30 – 13:15	Break

Program Schedule



Session 3 – Fault Injection: Techniques, Analysis, Effects

Chair: Luca Breveglieri

13:15 – 13:30	Body Biasing Injection: Impact of substrate types on the induced disturbances? *Geoffrey Chancel, Jean-Marc Gallière and Philippe Maurine*
13:30 – 13:45	Quantifying the Speed-Up Offered by Genetic Algorithms during Fault Injection Cartographies *Idris Rais-Ali, Antoine Bouvet and Sylvain Guilley*
13:45 – 14:00	Exploration of Fault Effects on Formal RISC-V Microarchitecture Models *Simon Tollec, Mihail Asavoae, Damien Couroussé, Karine Heydemann and Mathieu Jan*
14:00 – 14:10	Break

Keynote II

Chair: Luca Breveglieri

14:10 – 14:50	Pre-silicon fault simulation: hard and important *Jasper van Woudenberg*
14:50 – 15:00	Closing remarks and Farewell

Congratulations to all the Authors
Wishing you a wonderful FDTC 2022!