FDTC 2023
Fault Diagnosis and Tolerance in Cryptography

FAULT DIAGNOSES AND TOLERANCE IN CRYPTOGRAPHY 2023

Chong-Hee Kim[1], Pascal Sasdrich[2]

[1]NXP Semiconductors, [2]Ruhr-University Bochum

September 10, 2023 - Prague, Czech Republic

CHAIRS

FDTC 2023
Fault Diagnosis and Tolerance in Cryptography

Program:	**Chong-Hee Kim**	*NXP Semiconductors*
	Pascal Sasdrich	*Ruhr-University Bochum*
General:	**Michael Tunstall**	*Google*
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 (chair)	*University of Massachusetts*
	Jean-Pierre Seifert	*TU Berlin & T-Labs*

SPONSORS - THANK YOU

FDTC 2023
Fault Diagnosis and Tolerance in Cryptography

University of Massachusetts Amherst

Google

Rambus

PROGRAMM COMMITTEE

FDTC 2023
Fault Diagnosis and Tolerance in Cryptography

Nasour Bagheri	*Shahid Rajaee Univ.*
Josep Balasch	*Katholieke Univ. Leuven*
Noémie Beringuier-Boher	*SGS Brightsight*
Sarani Bhattacharya	*IMEC*
Guillaume Bouffard	*ANSSI*
Jakub Breier	*Silicon Austria Labs*
Ileana Buhan	*Radboud Univ.*
Lukasz Chmielewski	*Radboud Univ.*
Fabrizio De Santis	*Siemens*
Jean-Max Dutertre	*Ecole des Mines S. Etienne*
David El-Baze	*Apple*
Wieland Fischer	*Infineon Technologies*
Christophe Giraud	*IDEMIA*
Dong-Guk Han	*Kookmin Univ.*
Victor Lomne	*NinjaLab*
Alyssa Milburn	*Intel*
Mehran Mozaffari Kermani	*Univ. South Florida*
Cristofaro Mune	*Raelize*
Colin O'Flynn	*NewAE Technology*
David Oswald	*Univ. Birmingham*
Ramiro Pareja	*Riscure*
Gerardo Pelosi	*Politecnico di Milano*
Ilia Polian	*Univ. Stuttgart*
Robert Primas	*TU Graz*
Chester Rebeiro	*IIT Madras*
Sayandeep Saha	*Nanyang Tech. Univ.*
Falk Schellenberg	*Max Planck Inst.*
Alexander Schlösser	*NXP Semiconductors*
Sergei Skorobogatov	*Univ. Cambridge*
Takeshi Sugawara	*Univ. Electro-Comm.*
Shahin Tajik	*Worcester Polytechnic Inst.*
Junko Takahashi	*NTT*
Michael Tunstall	*Google*
Praveen Vadnala	*Riscure*
Fan Zhang	*Zhejiang Univ.*

PAPERS

FDTC 2023
Fault Diagnosis and Tolerance in Cryptography

Submitted Papers:

- 13 papers submitted (11 regular / 2 short)
- most papers received 3 reviews

Accepted Papers:

- 9 accepted (regular) papers
- 69% acceptance ratio

Proceedings

- Paper URL: https://conferences.computer.org/fdtcpub
- Login: fdtcpub23
- Password: to be communicated on the workshop day

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

PROGRAM SCHEDULE

FDTC 2023
Fault Diagnosis and Tolerance in Cryptography

09:15 - 09:30 Welcome and Opening remarks

Keynote

Chair: Pascal Sasdrich

09:30 - 10:30 Fault attack friendliness of post-quantum cryptosystems
Alessandro Barenghi and Gerardo Pelosi

10:30 - 11:00 Break

PROGRAM SCHEDULE

FDTC 2023
Fault Diagnosis and Tolerance in Cryptography

Session 1 – Fault Attack Models and Countermeasures

Chair: Łukasz Chmielewski

11:00 - 11:30	A tale of two models: discussing the timing and sampling EM fault injection models *Jean-Luc Danger, Jean-Max Dutertre,* ***Roukoz Nabhan*** *Jean-Baptiste Rigaud and Laurent Sauvage*
11:30 - 12:00	Voronoi based multidimensional parameter optimization for fault injection attacks *Marius Eggert and* ***Marc Stöttinger***
12:00 - 12:30	A compositional methodology to harden programs against multi-faults attacks ***Etienne Boespflug****, Abderrahmane Bouguern, Mounier Laurent and Marie-Laure Potet*
12:30 - 14:00	Lunch

PROGRAM SCHEDULE

FDTC 2023
Fault Diagnosis and Tolerance in Cryptography

Session 2 – Fault Injection Analysis and Tools

Chair: Falk Schellenberg

14:00 - 14:30 Analysis of arbitrary waveform generation for voltage glitches
Vincent Immler *and Stanislav Lyakhov*

14:30 - 15:00 A better practice of body biasing injection
Geoffrey Chancel*, Jean-Marc Gallière and Philippe Maurine*

15:00 - 15:30 PicoEMP: a low-cost EMFI platform compared to BBI and voltage fault injection using TDC & external VCC measurements
Colin O'Flynn

15:30 - 16:00 Break

PROGRAM SCHEDULE

FDTC 2023
Fault Diagnosis and Tolerance in Cryptography

Session 3 – Fault Attacks on SW and HW Devices

Chair: Alessandro Barenghi

16:00 - 16:30	Fault attacks on a cloud-assisted ECDSA white-box based on the residue number system *Christophe Giraud and* ***Agathe Houzelot***
16:30 - 17:00	Forging DILITHIUM and FALCON signatures by single fault injection ***Sven Bauer*** *and Fabrizio De Santis*
17:00 - 17:30	DeepCover DS28C36: a hardware vulnerability identification and exploitation using T-test and double laser fault injection ***Karim Abdellatif*** *and Olivier Hériveaux*
17:30 - 17:40	Closing remarks and Farewell

WISHING YOU A WONDERFUL FDTC 2023!