# FDTC 2017: Final Program (PDF)

08:45 – 09:05 Registration and Early Morning Break

09:05 – 09:15 Opening remarks

***Keynote Talk I***
*Chair(s): Program Chairs*

09:15 – 10:00 Hardware security and trust: where we are and where we should go
*Giorgio Di Natale (LIRMM)*

***Session 1 – System-Level Fault Attacks***
*Chair: Elif Bilge Kavun (Infineon)*

10.00 – 10:25 Escalating privileges in Linux using voltage fault injection
*Niek Timmers and Cristofaro Mune*

10:25 – 10:50 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 Morning break

***Session 2 – Fault Attacks on Primitives***
*Chair: Erich Wenger (Infineon)*

11:10 – 11:35 Practical fault attack against the Ed25519 and EdDSA signature schemes
*Sylvain Pelissier and Yolan Romailler*

11:35 – 12:00 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*

12:00 – 12:25 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

***Session 3 – Laser Fault Attacks***
*Chair: Michael Hutter (Cryptography Research)*

13:30 – 13:55 Laser-induced fault injection on smartphone bypassing the secure boot
*Aurélien Vasselle, Hugues Thiebeauld, Adèle Morisset, Quentin Maouhoub and Sebastien Ermeneux*

13:55 – 14:20

13:55 – 14:20 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*

***Session 4 – Design Tools***
*Chair: Shivam Bhasin (NTU)*

14:20 – 14:45 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*

14:45 – 15:10 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 – 15:30 Afternoon break

***Panel***
*Moderator(s): Program Chairs*

15:30 – 17:00 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)*

17:00 – 17:10 Closing remarks and Farewell