TRUDEVICE final conference (FCTRU'16)

Final program

Monday 14th

			Length
08:00 - 08:45	Registration		0:45
08:45 - 09:15	Opening session		0:30
09:15 - 10:15	**Keynote speech (Richard Marshall, Xitex)**		1:00
Session chair:	Ilia Polian		
10:15 - 11:10	**Posters I (coffee break)**		0:55
Topic: PUFs and TRNGs			
Paper #			
14	Ugo Mureddu, Lilian Bossuet and Viktor Fischer	A comparison of PUF cores suitable for FPGA devices	
15	Brisbane Ovilla and Lilian Bossuet	Device Authentication Based on PUF Noise Characterization	
28	Thomas Sarno, Romain Wacquez, Philippe Maurine, Khalil Jradi, Jean-Michel Portal, Driss Aboulkassimi, Sarra Souiki-Figuigui, Jérémy Postel-Pellerin, Pierre Canet, Maxime Chambonneau and David Grojo	Electromagnetic Analysis Perturbation using Chaos Generator	
30	Honorio Martin, Giorgio Di Natale and Pedro Peris-Lopez	Poster: A Self-Repairable TRNG	
31	Yoav Weizman, Batya Karp and Osnat Keren	Modeling SRAM cell stability for randomness evaluation of PUF cells	
42	Linus Feiten, Matthias Sauer and Bernd Becker	Using LUT-specific delays to mitigate biases in delay-based PUFs and increase area efficiency on FPGAs	
48	Domenico Amelino and Mario Barbareschi	A software PUF-based Chain-of-Trust for IoT Devices	
11:10 - 12:30	**Session I**		1:20
Session chair:	Daniel Arumí		
Topic: STSM presentations			
Paper #			
STSM-1	Ke Jiang	Real-Time Scheduling as a Countermeasure Against DPA	
STSM-2	Maria Méndez Real	Investigation on Spatial Isolation against Logical Cache-based Side-Channel Attacks in Multi/Many-Core Architectures	
STSM-3	Tania Richmond	DPA Aiming the Secret Permutation in the McEliece Cryptosystem	
STSM-4	Airo Farulla Giuseppe	Model Driven Design of Secure Properties for Vision-Based Applications	
12:30 - 14:30	**Lunch**		2:00
14:30 - 16:10	**Session II**		1:40
Session chair:	Nele Mentens		
Topic: PUFs and TRNGs			
Paper #			
5	Oto Petura, Ugo Mureddu, Nathalie Bochard, Lilian Bossuet and Viktor Fischer	Evaluation of AIS-20/31 compliant TRNG cores implemented on FPGAs	
12	Raimondo Luzzi, Marco Bucci, Christoph Böhm and Maximiliam Hofer	A Reliable Low-area Low-power PUF-based Key Generator	
20	Matthias Hiller, Aysun Gurur Önalan and Georg Sigl	Enhanced PUF Key Derivation through Multiple Readouts and ECC Decodings	
41	Christine Utz, Johannes Tobisch and Georg T. Becker	Extended Abstract: Analysis of 1000 Arbiter PUF based RFID Tags	
57	Elena Ioana Vatajelu and Giorgio Di Natale	High-Entropy STT-MTJ-based TRNG	
16:10 - 17:30	**Posters II (coffee break)**		1:20
Topic: Validation and Evaluation / Detection of malicious components			
Paper #			
11	Erica Tena-Sánchez, Salvador Canas, Irene Duran and Antonio Acosta	Vulnerability Evaluation and Secure Design Methodology of Cryptohardware for ASIC-embedded Secure Applications to Prevent Side-Channel Attacks	
36	Mosabbah Mushir Ahmed, David Hely, Etienne Perret and Romain Siragusa	Authentication of IC based on Electromagnetic Signature	
44	Matteo Bollo and Giorgio Di Natale	On the randomness of Field Coupled Nanomagnets	
54	Laurent Sauvage, Youssef Souissi and Sofiane Takarabt	Secure Silicon: Towards Virtual Prototyping	
60	Núria Carrió, Víctor Montilla, Raul Suarez and Jordi Mujal	OP-TEE Resistance against Side Channel and Fault Injection Attacks	
29	Jelena Milosevic and Nicolas Sklavos	Malware in IoT Hardware Devices	
17:30 - 20:00	Welcome reception		2:30

Tuesday 15th

			Length
08:00 - 09:40	**Session III**		1:40
Session chair:	Salvador Manich		
Topic: Validation and Evaluation			
Paper #			
25	Pascal Sasdrich, Amir Moradi and Tim Gũneysu	Hiding Higher-Order Side-Channel Leakage - Randomizing Threshold Implementations in Reconfigurable Hardware	
40	Florian Wilde, Berndt Gammel and Michael Pehl	Spatial Correlations in Physical Unclonable Functions	
51	Viacheslav Izosimov and Martin Törngren	Security Evaluation of Cyber-Physical Systems in Society-Critical Internet of Things	
59	Natalia Mendo, Rubén Nuevo and David Hernandez	Experimental results on smartcards' IC EM radiation	
39	Michael Weiner and Salvador Manich	The SALVADOR simulation framework	
09:40 - 10:50	**Posters III (coffee break)**		1:10
Topic: Fault attack injection, detection and protection / Reconfigurable devices for secure functions			
Paper #			
10	Francisco Eugenio Potestad-Ordóñez, Carlos Jesus Jiménez-Fernández and Manuel Valencia-Barrero	Fault Injection on FPGA implementations of Trivium Stream Cipher using Clock Attacks	
13	Timothé Riom, Jean-Max Dutertre and Olivier Potin	Practical results on laser-induced instruction-skip attacks into microcontrollers	
22	Apostolos Fournaris, Louiza Papachristodoulou, Lejla Batina and Nicolas Sklavos	Secure and Efficient RNS Approach for Elliptic Curve Cryptography	
46	Yaara Neumeier and Osnat Keren	Robust Error Detecting Codes for Detecting Fault Injections in Multilevel Memories	
50	Shlomo Engelberg and Osnat Keren	Trustworthy Communications across Parallel Asynchronous Channels with Glitches	
21	Madalin Neagu and Salvador Manich	Random masking interleaved scrambling technique as a countermeasure for DPA/DEMA attacks in cache memories	
45	Vojtech Miškovský, Hana Kubatova and Martin Novotny	Influence of Fault-tolerant Design Methods on Resistance against Differential Power Analysis in FPGA	
52	Domenico Amelino, Mario Barbareschi and Alessandro Cilardo	Extending Device Security and Trust adopting Intel SGX	
56	Alberto Carelli, Giorgio Di Natale, Tiziana Margaria, Paolo Prinetto and Antonio Varriale	Securing data via the SEcube(TM) open security platform	
61	Ofer Hadar, Rami Segal and Raz Birman	H.264 Motion Vectors Based Cyber Defense/Attack Techniques	
10:50 - 12:30	**Session IV**		1:40
Session chair:	Michael Pehl		
Topic: Fault attack injection, detection and protection			
Paper #			
7	Jan Burchard, Maël Gay, Jan Horácek, Ange-Salomé Messeng Ekossono, Tobias Schubert, Bernd Becker, Ilia Polian andMartin Kreuzer	Small Scale AES Toolbox: Algebraic and Propositional Formulas, Circuit-Implementations and Fault Equations	
17	Baris Ege, Pedro Maat Massolino and Lejla Batina	Smart Card Fault Injections with High Temperatures	
24	Juvenal Araujo, Pedro Matutino and Ricardo Chaves	Residue Number System Hardware Emulator and Instructions Generator	
34	Hila Rabii, Yaara Neumeier and Osnat Keren	Low Complexity High Rate Robust Codes	
53	Yang Cao, Vladimir Rozic, Bohan Yang, Josep Balasch and Ingrid Verbauwhede	Exploring active manipulation attacks on the TERO random number generator	
12:30 - 14:30	**Lunch**		2:00
14:30 - 20:50	Cultural visit and dinner		6:20

Wednesday 16th

			Length
08:00 - 09:00	**Invited speaker (Michael Pehl, EISEC - TUM)**		1:00
Session chair:	Rosa Rodríguez		
09:00 - 10:20	**Session V**		1:20
Session chair:	Ioana Vatajelu		
Topic: Reconfigurable devices for secure functions			
Paper #			
16	Johanna Sepulveda, Ramon Fernandes, Cesar Marcon and Georg Sigl	Dynamic Security-aware Routing for Zone-based data Protection in Multi-Processor System-on-Chips	
19	Matej Bartík and Jirí Bucek	A Low-Cost Unified Experimental FPGA Board for Cryptography Applications	
26	Jori Winderickx, Joan Daemen and Nele Mentens	On the parallelization of slice-based Keccak implementations on Xilinx FPGAs	
35	Nicolas Sklavos, Paris Kitsos and Artemios G. Voyiatzis	On the Hardware Implementation Efficiency of CAESAR Authentication Ciphers for FPGA Devices	
10:20 - 11:10	**Posters IV (coffee break)**		0:50
Topic: Manufacturing test of secure devices / Reverse engineering countermeasures / Other topics			
Paper #			
6	Marek Laban, Miloš Drutarovský, Viktor Fischer and Michal Varchola	Platform for testing and evaluation of PUFs and TRNGs implemented in FPGAs	
9	Fabien Majeric, Eric Bourbao and Lilian Bossuet	Reversing the field to attack the SoCs - Double use of EM-fields to defeat the complexity-	
33	Papa-Sidy Ba, Sophie Dupuis, Marie-Lise Flottes, Giorgio Di Natale and Bruno Rouzeyre	Detection and Prevention of Hardware Trojan through Logic Testing	
18	Anton Biasizzo and Franc Novak	JTAG Security Extension Design Tool	
27	Moshe Avital, Alexander Fish and Osnat Keren	From Full-Custom to Fully-Standard Cell Power Analysis Countermeasures	
8	Jo Vliegen, Bob Koninckx, Dave Singelée and Nele Mentens	Real-time encryption and authentication of medical video streams on FPGA	
43	Stefano Di Mascio, Marco Ottavi, Gianluca Furano and Selcuk Baktir	Enabling Cubesat Commercial Applications by Low-Power Encryption	
58	Stjepan Picek, Annelie Heuser, Sylvain Guilley, Domagoj Jakobovic and Nele Mentens	On the Machine Learning Techniques for Side-channel Analysis	
11:10 - 12:30	**Session VI**		1:20
Session chair:	Carles Ferrer		
Topic: Manufacturing test of secure devices / Reverse engineering countermeasures / Hardware Trojans in IPs and ICs			
Paper #			
49	Hermann Seuschek, Fabrizio De Santis and Oscar Guillen	Side-Channel Leakage Models for IoT Processors	
23	Arash Nejat, David Hely and Vincent Beroulle	Reusing Logic Masking to Facilitate Hardware Trojan Detection	
38	Johanna Baehr and Michael Tempelmeier	Circuit Clustering Methods for Netlist Reverse Engineering	
55	Francesco Regazzoni, Georg T Becker and Ilia Polian	Trojans in Early Design Steps - An Emerging Threat	
12:30 - 14:30	**Lunch**		2:00
14:30 - 14:50	Closing session		0:20
14:50 - 15:10	MC Meeting Session		0:20
15:10 - 17:10	Open meeting follow up for other projects in future		2:00