Monday, July 2

8:30-9:30 FEDFRO Opening Session
  Welcome Message
  Keynote Wally Rhines, Mentor Graphics President
  Emerging Discontinuities in Design and Verification Methodologies

9:30-9:45 Break

9:45-11:00 Session 1: IVSW opening
  Welcome and program introduction
  Session Chair: Ilia Polian, University of Stuttgart, Germany
  Keynote Rolf Drechsler, DFKI and University of Bremen, Germany:
  Towards Self-Explaining Digital Systems: A Design Methodology for the Next Generation
  Invited talk Alexander Schaub (TELECOM-ParisTech & French Department of Defense), with
  Youssef Souissi (Threat Analysis Business Line Director, Secure-IC S.A.S, France)
  Post-quantum cryptography cache-timing analysis
  (Joint work with Adrien Facon, Sylvain Guilley and Matthieu Lec'hvien)

11:00-12:00 Posters and coffee break

12:00-13:00 Session 2: Reverse engineering and camouflaging
  Welcome and program introduction
  Session Chair: Sohrab Aftabjahani, Intel Corp., USA
  Reverse Engineering of Cryptographic Cores by Structural Interpretation through Graph Analysis
  Michael Werner¹, Bernhard Lippmann², Johanna Baehr² and Helmut Gräb², ¹Infineon
  Technologies AG, Germany, ²TU Munich, Germany
  Software-only Reverse Engineering of Physical DRAM Mappings for Rowhammer Attacks Alessandro Barenghi, Luca Breveglieri, Niccolò Izzo and Gerardo Pelosi, Politecnico di Milano, Italy
  Timing Camouflage for Digital Circuits against Counterfeiting Bing Li, TU Munich, Germany

13:00-14:30 Lunch

14:30-15:30 Session 3: System-level security (joint session with IOLTS)
  Welcome and program introduction
  Session Chair: Sohrab Aftabjahani, Intel Corp., USA
  Detecting and Resolving Security Violations in Reconfigurable Scan Networks Pascal Raiola¹, Michael Kochte², A.Atteya³, L.Rodriguez Gomez², H.-J.Wunderlich³, Bernd Becker³, Matthias Sauer¹, ¹University of Freiburg, Germany, ²University of Stuttgart, Germany
  Detecting the Existence of Malfunctions in Microcontrollers Utilizing Power Analysis, K.
  Hasegawa, M. Yanagisawa, N. Togawa, Waseda University, Japan
  Effective Control Flow Integrity Checks for Intrusion Detection, A. Chaudhari, J. Abraham,
  University of Texas at Austin, USA

15:30-15:45 Break
15:45-16:45 Session 4: Security of embedded systems

Session Chair: Matteo Sonza Reorda, Politecnico di Torino

**Authentication of Microcontroller board using non-invasive EM emission technique** Mosabbah Mushir Ahmed¹, David Hely¹, Etienne Perret¹, Nicolas Barbot¹, Romain Siragus¹, Maxime Bernier² and Fredric Garet³, ¹LCIS Grenoble University, France, ²IMEP LAHC Univ. Savoie, France

**On the mitigation of Hardware Trojan attacks in embedded systems by exploiting a Hardware-based obfuscator** Andrea Marcelli, Ernesto Sanchez, Luca Sasselli and Giovanni Squillero, Politecnico di Torino, Italy

**Lightweight PUF-Based Authentication Protocol for IoT Devices** Yildiran Yilmaz, Basel Halak and Steve Gunn, University of Southampton, UK

16:45-17:15 Coffee break

17:15-18:15 Session 5: Security validation and verification

Session Chair: Luca Breveglieri, Politecnico di Milano, Italy

**Verification and Security: Friends but no free lunch** Matthias Sauer and Bernd Becker, University of Freiburg, Germany

**Is EDA Industry Ready for Design for Security and Security Validation Challenges?** Sohrab Aftabjahani, Intel Corp., USA

**Physical Inspection for Trust Verification** Navid Asadi Zanjani, University of Florida, USA

20:00-22:00 Welcome Reception

---

**Tuesday, July 3**

8:30-9:00 Session 6: Keynote

Session Chair: Sohrab Aftabjahani, Intel Corp., USA

Yervant Zorian, Synopsys, USA:

**Maintaining Safety & Security in today’s SOC**

9:00-9:30 Session 7: Invited talk

Session Chair: Atefeh Einafshar, Intel Corp.

Nele Mentens, KU Leuven, Belgium

**Configurable computing for cryptographic implementations**

9:30-9:45 Break

9:45-10:45 Session 8: Emerging security technologies

Session Chair: David Hely, University Grenoble Alpes, France

**Security Analysis of Chaotic Baker Maps** Amira El-Hamshary, Yehea Ismail and Said El-Khamy, American University of Cairo, Egypt

**Security Primitives using Inorganic Electrolyte-Gated Inkjet Printed Transistors** Mehdi Tahoori, Karlsruhe Institute of Technology, Germany

**Architectural Diversity: Bio-Inspired Hardware Security for FPGAs** Shakil Mahmud, Brooks Olney and Robert Karam, University of South Florida, USA

10:45-11:15 Coffee break
11:15-12:15 Session 9: Panel
Funding Hardware Security Research: Taxpayer’s Money to Support Malicious Hackers?
Panelists: Lejla Batina (Radboud University, NL), Giorgio Di Natale (CNRS, FR), Youssef Souissi (Secure-IC, FR), Nele Mentens (KU Leuven, BE), Francesco Regazzoni (ALARI, CH)

12:15-12:30 Break

12:30-13:10 Session 10: Countering attacks on hardware blocks
Session Chair: Lejla Batina, Radboud University, The Netherlands
Compact Protection Codes Hila Rabii, Yaara Neumeier, Osnat Keren, Bar-Ilan University, Israel
A Machine Learning Attacks Resistant Two Stage Physical Unclonable Functions Design Haibo Su, Mark Zwolinski and Basel Halak, University of Southampton, UK

13:10-14:30 Lunch

14:30-15:30 Session 11: Hardware Trojans
Session Chair: Marie-Lise Flottes, LIRMM
Hardware Trojan Detection and Functionality Determination for Soft IPs Thao Le¹, Lucas Weaver¹, Jia Di², Yier Jin³ and Shaojie Zhang³, ¹University of Arkansas, USA, ²University of Florida, USA, ³University of Central Florida, USA
Property Based Formal Security Verification for Hardware Trojan Detection Maoyuan Qin, Wei Hu, Dejun Mu and Yu Tai, Northwestern Polytechnical University, China
A New Design of RTL Hardware Trojan Based on Uncertain X-Values and Improved Prevention Method Bowen Luo and Jianhua Feng, Peking University, China

16:00-22:00 Social event

Wednesday, July 4

8:30-9:00 Session 12: Keynote
Session Chair: Magdy Abadir, Helic, USA
Yehea Ismail, American University of Cairo, Egypt
Inductance effects in High-Speed Integrated Circuits

9:00-10:00 Session 13: Cryptographic solutions
Session Chair: Nele Mentens, KU Leuven, Belgium
OmniLedger: A Secure, Scale-Out, Decentralized Blockchain via Sharding Eleftherios Kokoris-Kogias¹, Philipp Jovanovic¹, Linus Gasser¹, Nicolas Gailly¹, Ewa Syta² and Bryan Ford³, ¹Ecole Polytechnique Fédérale de Lausanne, Switzerland, ²Trinity College, USA
A new secure stream cipher for scan chain encryption Mathieu Da Silva, Emanuele Valea, Marie-Lise Flottes, Sophie Dupuis, Giorgio Di Natale and Bruno Rouzeyre, LIRMM, France
Design of quantum resistant cyber-physical systems and IoT devices Francesco Regazzoni, ALARI, Switzerland

10:00-10:30 Posters and coffee break
10:30-11:30 Session 14: Evaluation and validation

Session Chair: Lorena Anghel, TIMA, Grenoble, France

*Pre-Silicon Embedded System Evaluation as new EDA for Security Verification* Sofiane Takarabt¹, Kais Chibani², Youssef Souissi¹, Laurent Sauvage¹, Sylvain Guilley¹, Adrien Facon¹ and Yves Mathieu², ¹Secure-IC S.A.S, France, ²TELECOM-Paristech, France

*Using Physical and Functional Comparisons to Assure 3rd-Party IP for Modern FPGAs* Adam Hastings, Sean Jensen, Jeffrey Goeders and Brad Hutchings, Brigham Young University, USA

*Hardware Security Evaluation Platform for MCU Based Connected Devices: Application to healthcare IoT* Zahra Kazemi¹, Athanasios Papadimitriou¹, David Hely¹, Mahdi Fazeli² and Vincent Beroulle¹, ¹Univ. Grenoble Alpes, ²Iran University of Science and Technology

11:30-11:45 Break

11:45-12:45 Session 15: Circuit-level security (joint session with IOLTS)


*Benchmarking the Capabilities and Limitations of SAT Solvers in Defeating Obfuscation Schemes* S. Roshanisefat, H. Thirumala, H. Homayoun, K. Gaj, A. Sasan, George Mason University, USA

*On the Effect of Aging in Detecting Hardware Trojan Horses with Template Analysis,* N. Karimi¹, J.-L. Danger², S. Guilley², ¹U Maryland Baltimore County, ²Telecom ParisTech, U Paris-Saclay

12:45-14:00 Lunch

14:00-14:30 Session 16: Invited talk

Session Chair: Bernd Becker, University of Freiburg, Germany

Lejla Batina, Radboud University, The Netherlands

*Physical attacks on IoT systems*

14:30-15:00 Session 17: Invited talk

Session Chair: Magdy Abadir, Helic, USA

Amir Moradi, Ruhr University Bochum, Germany

*Threshold Implementation as a Substrate for Hardware Trojan*

15:00-15:40 Session 18: Embedded tutorial

Session Chair: Amir Moradi, Ruhr University Bochum, Germany

*Physically Unclonable Functions: Design Principles and Outstanding Challenges* Basel Halak, University of Southampton, UK

15:40-15:50 Closing remarks