CHES 2013 Program

Tuesday, August 20 University Center Flying A Room			
Time	**Event**		
	Session	**Authors**	**Title**
10:00 - 13:00	CHES Tutorial 1	Emmanuel Prouff, (French Network and Information Security Agency)	Side-channel Attacks and Dedicated Countermeasures
14:30 - 17:30	CHES Tutorial 2	Colin O'Flynn, (Dalhousie University)	Power Analysis using Low-Cost Hardware: Lab Setup & Simple Targets
18:00 - 20:00	CHES Registration Manzanita Village		

18:00 - 20:30	**CHES Reception and Registration Manzanita Village**

Wednesday, August 21 University Center Corwin Pavilion			
Time	**Event**		
	Session	**Authors**	**Title**
08:00 - 15:45	**Registration Corwin Lobby**		
08:50 - 09:00	**Opening Remarks**		
9:00 - 10:40	Session 1 Side-Channel Attacks Chair: Matthieu Rivain	Amir Moradi and Oliver Mischke (Horst Görtz Institute for IT Security, Ruhr Universität Bochum, Germany)	On the Simplicity of Converting Leakages from Multivariate to Univariate - Case Study of a Glitch-Resistant Masking Scheme
		Adrian Thillard, Emmanuel Prouff and Thomas Roche (ANSSI, France).	Success through confidence: Evaluating the effectiveness of a side-channel attack
		Carolyn Whitnall and Elisabeth Oswald (University of Bristol, Department of Computer Science)	Profiling DPA: Efficacy and efficiency trade-offs
		Yasser Shoukry, Paul Martin, Paulo Tabuada, Mani Srivastava (UC Los Angeles)	Noninvasive Spoofing Attacks For Anti-lock Braking Systems
10:40 - 11:10	**Joint Coffee Break with CRYPTO 2013 Campbell Hall**		
11:10 - 12:10	Joint invited talk with Crypto 2013. Chair: Juan Garay	Adam Langley (Google)	Why the web still runs on RC4
12:10 - 14:00	**Lunch**		

14:00 - 15:15	Session 2: PUF Chair: Tim Güneysu	Roel Maes (Intrinsic-ID)	An Accurate Probabilistic Reliability Model for Silicon PUFs
		Mudit Bhargava and Ken Mai (Carnegie Mellon University)	A High Reliability PUF Using Hot Carrier Injection Based Response Reinforcement
		Yossef Oren (Tel-Aviv University, Israel), Ahmad-Reza Sadeghi (TU Darmstadt/CASED, Germany) and Christian Wachsmann (Intel CRI-SC at TU Darmstadt, Germany)	On the Effectiveness of the Remanence Decay Side-Channel to Clone Memory-based PUFs
15:15 - 15:35	**Coffee Break**		
15:35 - 16:25	Session 3: Lightweight cryptography Chair: Ahmad-Reza Sadeghi	Peter Pessl and Michael Hutter (Institut for Applied Information Processing and Communications (IAIK), Graz University of Technology, Austria)	Pushing The Limits of SHA-3 Hardware Implementations to Fit on RFID
		Begul Bilgin (KU Leuven, Belgium, iMinds, Belgium, University of Twente, The Netherlands), Andrey Bogdanov (Technical University of Denmark, Denmark), Miroslav Knezevic (NXP Semiconductors, Belgium), Florian Mendel (Graz University of Technology, Austria), Qingju Wang (KU Leuven, Belgium, iMinds, Belgium, Shanghai Jiao Tong University, China)	FIDES: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware
16:40 - 17:40	**IACR Membership Meeting**		
18:00 - 20:30	**Catered BBQ** **Santa Rosa Courtyard**		

Thursday, August 22nd University Center Corwin Pavilion			
Time	**Event**		
	Session	**Authors**	**Title**
08:00 - 15:15	**Registration Corwin Lobby**		
9:00 - 10:40	Session 4: Hardware implementations and fault attacks Chair: Lejla Batina	Takeshi Sugawara (Mitsubishi Electric Corporation), Daisuke Suzuki (Mitsubishi Electric Corporation), Minoru Saeki (Mitsubishi Electric Corporation), Mitsuru Shiozaki (Ritsumeikan University), Takeshi Fujino (Ritsumeikan University)	On Measurable Side-Channel Leaks inside ASIC Design Primitives
		Abdelkarim Cherkaoui (Laboratoire Hubert Curien, Saint-Etienne, France), Viktor Fischer (Laboratoire Hubert Curien, Saint-Etienne, France), Alain Aubert (Laboratoire Hubert Curien, Saint-Etienne, France) and Laurent Fesquet (Laboratoire TIMA, Grenoble, France)	A Very High Speed True Random Number Generator with Entropy Assessment
		Georg T. Becker (University of Massachusetts Amherst, USA), Francesco Regazzoni (TU Delft, Netherlands and ALaRI - University of Lugano, Switzerland), Christof Paar (Horst Görtz Institute for IT-Security, Ruhr-Universität Bochum, Germany and University of Massachusetts Amherst, USA) and Wayne P. Burleson (University of Massachusetts Amherst, USA)	Stealthy Dopant-Level Hardware Trojans
		Subhadeep Banik and Subhamoy Maitra (Applied Statistics Unit, Indian Statistical Institute, India)	A Differential Fault Attack on MICKEY 2.0
10:40 - 11:10	**Coffee Break + Poster Session**		
11:10 - 12:10	Invited Talk	John Kelsey (NIST)	The Future of SHA-3

12:10 - 14:00	**Lunch**		
14:00 - 15:40	Session 5: Efficient and secure implementations Chair: Bo-Yin Yang	Karim Bigou (INRIA Centre Rennes Bretagne Atlantique, IRISA, Université Rennes 1) and Arnaud Tisserand (CNRS, IRISA, Université Rennes 1)	Improving Modular Inversion in RNS using the Plus-Minus Method
		Daniel J. Bernstein (University of Illinois at Chicago and Technische Universiteit Eindhoven), Tung Chou (Technische Universiteit Eindhoven) and Peter Schwabe (Radboud University Nijmegen).	McBits: fast constant-time code-based cryptography
		Stefan Heyse, Ingo von Maurich, Tim Güneysu (Horst Görtz Institute for IT-Security, Ruhr-Universität Bochum, Germany)	Smaller Keys for Code-based Cryptography: QC-MDPC McEliece Implementations on Embedded Devices
		Ali Galip Bayrak (EPFL, Switzerland), Francesco Regazzoni (TU Delft, Netherlands and ALaRI - University of Lugano, Switzerland), David Novo (EPFL, Switzerland), Paolo Ienne (EPFL, Switzerland)	Sleuth: Automated Verification of Software Power Analysis Countermeasures
15:40 - 16:10	**Coffee Break + Poster Session**		
18:00 - 22:00	**Reception and Rump Session** **Chair: Christof Paar** **Buses depart at 5:30 to Fess Parker DoubleTree**		

Friday, August 23 University Center Corwin Pavilion			
Time	**Event**		
	Session	**Authors**	**Title**
08:00 - 15:45	**Registration Corwin Lobby**		
9:00 - 10:40	Session 6: ECC Chair: Mehdi Tibouchi	Thomaz Oliveira (CINVESTAV-IPN, Mexico), Julio Lopez (University of Campinas, Brazil), Diego F. Aranha (University of Brasilia, Brazil) and Francisco Rodriguez-Henriquez (CINVESTAV-IPN, Mexico)	Lambda coordinates for binary elliptic curves (Best Paper Award)
		Joppe W. Bos (Microsoft Research), Craig Costello (Microsoft Research), Huseyin Hisil (Yasar University), and Kristin Lauter (Microsoft Research)	High-Performance Scalar Multiplication using 8-Dimensional GLV/GLS Decomposition
		Santosh Ghosh (Security Center of Excellence, Intel Corporation, OR, US), Amit Kumar (Department of Electrical Engineering, IIT Kharagpur, WB, India), Amitabh Das (COSIC, KU Leuven, Belgium), Ingrid Verbauwhede (COSIC, KU Leuven, Belgium)	On the Implementation of Unified Arithmetic on Binary Huff Curves
		Ronan Lashermes (CEA-Leti Minatec, Gardanne, France and UVSQ, Versailles, France) and Jacques Fournier (CEA-Leti Minatec, Gardanne, France) and Louis Goubin (UVSQ, Versailles, France)	Inverting the final exponentiation of Tate pairings on ordinary elliptic curves using faults
10:40 - 11:10	**Coffee Break**		

11:10 - 12:25	Session 7: Masking Chair: Emmanuel Prouff	Vincent Grosso, François-Xavier Standaert and Sebastian Faust (UCL Crypto Group and EPFL, Switzerland)	Masking vs. Multiparty Computation: How Large is the Gap for AES?
		Benoît Gérard, Vincent Grosso, Maria Naya-Plasencia and François-Xavier Standaert (DGA and UCL Crypto Group and INRIA)	Block Ciphers that are Easier to Mask: How Far Can we Go?
		Arnab Roy and Srinivas Vivek (Université du Luxembourg)	Analysis and Improvement of the Generic Higher-Order Masking Scheme of FSE 2012
12:25 - 14:00	**Lunch**		
14:00 - 15:15	Session 8: Side-channel Attacks and countermeasures Chair: Francesco Regazzoni	Elke De Mulder (Cryptography Research), Michael Hutter (Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Austria), Mark E. Marson (Cryptography Research), Peter Pearson (Cryptography Research)	Using Bleichenbacher's Solution to the Hidden Number Problem to Attack Nonce Leaks in 384-Bit ECDSA.
		Zhenqi Li, Bin Zhang, Junfeng Fan and Ingrid Verbauwhede (Institute of Software, Chinese Academy of Sciences, State Key Laboratory of Information Security (SKLOIS), Institute of Information Engineering, Chinese Academy of Sciences, Katholieke Universiteit Leuven, ESAT SCD/COSIC)	A New Model for Error-Tolerant Side-Channel Cube Attacks
		Michel Abdalla, Sonia Belaïd and Pierre-Alain Fouque (Ecole Normale Supérieure, Thales Communications and Security, Rennes University)	Leakage-Resilient Symmetric Encryption via Re-keying
15:15 - 15:20	**Concluding remarks**		