SAC 2014 Program

***All the presentations will be held at* EV2.260**
Board meeting will be held in room EV002.301

Wednesday, August 13/2014

18:00-20:00 Light social reception (EV2.184)

Thursday, August 14/2014

08:00-9:00 **Registration and Morning Coffee**
9:00-09:10 **Opening Remarks**
9:100-10:10 **Invited Talk I: Practical Multi-Party Computation,** Nigel Smart, University of Bristol, United Kingdom. (Chair: Antoine Joux)
10:10-10:40 Coffee Break

MODE OF OPERATIONS (Chair: Gaetan Leurent)

10:40-11:05 Practical Cryptanalysis of PAES.
- Jérémy JEAN (Nanyang Technological University, Singapore)
- Ivica Nikolić (Nanyang Technological University, Singapore)
- Yu Sasaki (NTT Secure Platform Laboratories, Japan)
- Lei Wang (Nanyang Technological University, Singapore)

11:05-11:30 OMD: A Compression Function Mode of Operation for Authenticated Encryption
- Simon Cogliani (ENS, France)
- Diana Maimut (ENS, France)
- David Naccache (ENS, France)
- Rodrigo Portella do Canto (Université Paris II - Panthéon-Assas, France)
- Reza Reyhanitabar (EPFL, Switzerland)
- Serge Vaudenay (EPFL, Switzerland)
- Damian Vizár (EPFL, Switzerland)

SIDE-CHANNEL ATTACKS (Chair: Orr Dunkelman)

11:40-12:05 Error-Tolerant Side-Channel Cube Attack Revisited
- Zhenqi Li (TCA, Institute of Software, Chinese Academy of Sciences, China)
- Bin Zhang (TCA, Institute of Software, Chinese Academy of Sciences, China)
- Arnab Roy (University of Luxembourg, Luxembourg)
- Junfeng Fan (Nationz Technologies Inc, China)

12:05-12:30 Side-Channel Analysis of Montgomery's Representation Randomization
- Eliane Jaulmes (ANSSI, France)
- Emmanuel Prouff (ANSSI, France)
- Justine Wild (ANSSI, France)

LUNCH (12:30 - 14:00, Hall Building H-763)

HASH FUNCTIONS (Chair: Yu Sasaki)

14:00-14:25 Differential Cryptanalysis of SipHash
- Christoph Dobraunig (Graz University of Technology, Austria)
- Florian Mendel (Graz University of Technology, Austria)
- Martin Schläffer (Graz University of Technology, Austria)

14:25-14:50 The Usage of Counter Revisited: Second-Preimage Attack on New Russian Standardized Hash Function
- Jian Guo (Nanyang Technological University, Singapore)
- Jérémy Jean (Nanyang Technological University, Singapore)
- Gaëtan Leurent (INRIA, France)
- Thomas Peyrin (Nanyang Technological University, Singapore)
- Lei Wang (Nanyang Technological University, Singapore)

14:50-15:15 Malicious Hashing: Eve's Variant of SHA-1
- Ange Albertini (Corkami, Germany)
- Jean-Philippe Aumasson (Kudelski Security, Switzerland)
- Maria Eichlseder (Graz University of Technology, Austria)
- Florian Mendel (Graz University of Technology, Austria)
- Martin Schläffer (Graz University of Technology, Austria)

15:15-15:45 **Coffee Break**

NUMBER THEORY I (Chair: Michael Jacobson)

15:45-16:10 Binary Elligator Squared
- Diego F. Aranha (University of Campinas, Brazil)
- Pierre-Alain Fouque (Université de Rennes 1 and Institut Universitaire de France)
- Chen Qian (ENS Rennes, France)
- Mehdi Tibouchi (NTT Secure Platform Laboratories, Japan)
- Jean-Christophe Zapalowicz (Inria, France)

16:10-16:35 Fast point multiplication algorithms for binary elliptic curves with and without precomputation
- Thomaz Oliveira (Computer Science Department, CINVESTAV-IPN, Mexico)
- Diego F. Aranha (Institute of Computing, University of Campinas, Brazil)
- Julio López (Institute of Computing, University of Campinas, Brazil)
- Francisco Rodríguez-Henríquez (Computer Science Department, CINVESTAV-IPN, Mexic)

16:35-17:00 Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster
- Erich Wenger (Graz University of Technology, Austria)
- Paul Wolfger (Graz University of Technology, Austria)

17:00-18:00 **The Stafford Tavares Lecture: Scott Vanstone and the Early Years of Elliptic Curve Cryptography,** Alfred Menezes, University of Waterloo, Canada (Chair: Daniel Bernstein)

DINNER (18:30 - 20:30, Hall Building H-763)

Friday, August 15/2014

8:30-9:00 **Morning Coffee**
9:00-10:00 **Invited Talk II: NFS: similarities and differences between integer factorization and discrete logarithm,** Pierrick Gaudry, Université de Lorraine, France. (Chair: Tanja Lange)

10:00-10:30 **Coffee Break**

NUMBER THEORY II (Chair: Roberto Avanzi)

10:30-10:55 A Generic Algorithm for Small Weight Discrete Logarithms in Composite Groups
- Alexander May (Horst Görtz Institute for IT Security and Faculty of Mathematics, Ruhr-Universität Bochum, Germany)
- Ilya Ozerov (Horst Görtz Institute for IT Security and Faculty of Mathematics, Ruhr-Universität Bochum, Germany)

10:55-11:20 Partial Key Exposure Attacks on RSA: Achieving Boneh-Durfee's Bound
- Atsushi Takayasu (The University of Tokyo, Japan)
- Noboru Kunihiro (The University of Tokyo, Japan)

11:20-11:50 Batch NFS
- Daniel J. Bernstein (University of Illinois at Chicago, USA; Technische Universiteit Eindhoven, the Netherlands)
- Tanja Lange (Technische Universiteit Eindhoven, the Netherlands)

11:50-12:15 Weak Instances of PLWE
- Kirsten Eisentraeger (Penn State University and Harvard University, USA)
- Sean Hallgren (Penn State University, USA)
- Kristin Lauter (Microsoft Research, USA)

LUNCH (12:30 – 14:00, Library Building, LB Atrium)

CONSTRUCTIONS (Chair: Douglas Stinson)

14:00-14:25 Diffusion matrices from algebraic-geometry codes with efficient SIMD implementation
- Daniel Augot, (Inria and LIX, France)
- Pierre-Alain Fouque (Université de Rennes 1 and Institut universitaire de France, France)
- Pierre Karpman (Inria, France and Nanyang Technological University, Singapore)

14:25-14:50 Security Amplification for the Composition of Block Ciphers: Simpler Proofs and New Results
- Benoît Cogliati (University of Versailles, France)
- Jacques Patarin (University of Versailles, France)
- Yannick Seurin (ANSSI, France)

14:50-15:15 Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers
- Nicky Mouha (ESAT/COSIC, KU Leuven and iMinds, Belgium)
- Bart Mennink (ESAT/COSIC, KU Leuven and iMinds, Belgium)
- Anthony Van Herrewege (ESAT/COSIC, KU Leuven and iMinds, Belgium)
- Dai Watanabe (Yokohama Research Laboratory, Hitachi, Japan)
- Bart Preneel (ESAT/COSIC, KU Leuven and iMinds, Belgium)
- Ingrid Verbauwhede (ESAT/COSIC, KU Leuven and iMinds, Belgium)

15:15-15:40 Faster binary-field multiplication and faster binary-field MACs
- Daniel J. Bernstein (University of Illinois at Chicago, USA; Technische Universiteit Eindhoven, the Netherlands)
- Tung Chou (Technische Universiteit Eindhoven, the Netherlands)

15:40-16:00 **Coffee Break**

BLOCK-CIPHER CRYPTANALYSIS (Chair: Nicky Mouha)

16:00-16:25 An Improvement of Linear Cryptanalysis with Addition Operations with Applications to FEAL-8X
- Eli Biham (Technion - Israel Institute of Technology, Haifa, Israel)
- Yaniv Carmeli (Technion - Israel Institute of Technology, Haifa, Israel)

16:25-16:50 Improved Differential Cryptanalysis of Round-Reduced Speck
- Itai Dinur (Ecole Normale Superieure, Paris, France)

16:50-17:15 Colliding Keys for SC2000-256
- Alex Biryukov (University of Luxembourg, Luxembourg)
- Ivica Nikolic (Nanyang Technological University, Singapore)

17:15-17:40 Linear Biases in AEGIS Keystream
- Brice Minaud (ANSSI)

17:40-17: 45 **Closing Remarks**