FSE 2013 Program

Welcome reception will be at poolside of Novotel, and all technical sessions will be at Cinnamon Room of Novotel. The program is available in PDF.

Sunday, 10 March 2013

- 18:30 - 21:00 **Registration** *(Novotel@Clarke Quay - poolside)*
- 19:00 - 21:00 **Welcome Reception** *(Novotel@Clarke Quay - poolside)*

Monday, 11 March 2013

- 08:30-09:30 **Registration** *(Novotel@Clarke Quay - Cinnamon Room)*
- 09:30-09:40 **General Co-Chairs' Opening Remarks** *(Novotel@Clarke Quay - Cinnamon Room)*

Session 1 --- Block ciphers *(Chair: Shiho Moriai)*

- 09:40-10:05 **Complementing Feistel Ciphers**
  Alex Biryukov and Ivica Nikolic
  University of Luxembourg, Luxembourg
  Nanyang Technological University, Singapore
- 10:05-10:30 **On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui's Algorithm 2**
  Andrey Bogdanov and Elmar Tischhauser
  Technical University of Denmark, Denmark
  Katholieke Universiteit Leuven, Belgium
- 10:30-10:55 **Cryptanalysis of WIDEA**
  Gaetan Leurent
  Université Catholique de Louvain, Belgium
- 10:55-11:20 **Coffee Break**

Session 2 --- Invited Talk I *(Chair: Shiho Moriai)*

- 11:20-12:20 **Towards Secure Distance Bounding**
  Serge Vaudenay
  École Polytechnique Fédérale de Lausanne, Switzerland
- 12:20-14:00 **Lunch** *(Novotel@Clarke Quay - The Square)*

Session 3 --- Lightweight block ciphers *(Chair: Jian Guo)*

- 14:00-14:25 **Reflection Cryptanalysis of PRINCE-like Ciphers**
  Hadi Soleimany, Céline Blondeau, Xiaoli Yu, Wenling Wu, Kaisa Nyberg, Huiling Zhang, Lei Zhang and Yanfeng Wang
  Aalto University School of Science, Finland
  Institute of Software, Chinese Academy of Sciences, China
- 14:25-14:50 **Security Analysis of PRINCE**
  Jeremy Jean, Ivica Nikolic, Thomas Peyrin, Lei Wang and Shuang Wu
  Ecole Normale Superieure, France
  Nanyang Technological University, Singapore
- 14:50-15:15 **Cryptanalysis of Round-Reduced LED**
  Ivica Nikolic, Lei Wang and Shuang Wu
  Nanyang Technological University, Singapore
- 15:15-15:40 **Coffee Break**

Session 4 --- Modes and Tweakable block ciphers *(Chair: Tetsu Iwata)*

- 15:40-16:05 **Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes**
  David Mcgrew
  Cisco Systems, Inc., USA

- *16:05-16:30* **Tweakable Blockciphers with Asymptotically Optimal Security**
  Rodolphe Lampe and Yannick Seurin
  University of Versailles, France
  ANSSI, France

Session 5 --- Stream ciphers I *(Chair: Yu Sasaki)*

- 16:30-16:55 **Smashing WEP in A Passive Attack**
  Pouyan Sepehrdad, Petr Susil, Serge Vaudenay and Martin Vuagnoux
  Intel Collaborative Research Institute for Secure Computing, Germany
  École Polytechnique Fédérale de Lausanne, Switzerland
- 16:55-17:20 **Full Plaintext Recovery Attack on Broadcast RC4**
  Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe and Masakatu Morii
  Kobe University, Japan
  Hiroshima University, Japan
- 18:30 **Assemble at Novotel for the social event to Singapore Night Safari**

Tuesday, 12 March 2013

Session 6 --- Hash functions *(Chair: Thomas Peyrin)*

- 08:30-08:55 **Time-memory Trade-offs for Near-collisions**
  Gaetan Leurent
  Université Catholique de Louvain, Belgium
- 08:55-09:20 **Collision Attacks on Up to 5 Rounds of SHA-3 Using Generalized Internal Differentials**
  Itai Dinur, Orr Dunkelman and Adi Shamir
  The Weizmann Institute, Israel
  University of Haifa, Israel
- 09:20-09:45 **Rotational cryptanalysis of round-reduced Keccak**
  Pawel Morawiecki, Josef Pieprzyk and Marian Srebrny
  Kielce University of Commerce, Poland
  Polish Academy of Sciences, Warsaw, Poland
  Macquarie University, Australia
- 09:45-10:10 **Partial-Collision Attack on the Round-Reduced Compression Function of Skein-256**
  Hongbo Yu, Jiazhe Chen and Xiaoyun Wang
  Tsinghua University, China
  Shandong University, China
- 10:10-10:35 **Coffee Break**

Session 7 --- Invited Talk II *(Chair: Bart Preneel)*

- 10:35-11:35 **Failures of secret-key cryptography**
  Daniel Bernstein
  University of Illinois at Chicago, USA, and Technische Universiteit Eindhoven, Netherlands

Session 8 --- Message Authentication Codes *(Chair: Mitsuru Matsui)*

- 11:35-12:00 **On Weak Keys and Forgery Attacks against Polynomial-based MAC Schemes** (Best Paper Award)
  Gordon Procter and Carlos Cid
  Royal Holloway, University of London, United Kingdom
- 12:00-12:25 **Secure Message Authentication against Related-Key Attack**
  Rishiraj Bhattacharyya and Arnab Roy
  ENS de Lyon, France
  University of Luxembourg, Luxembourg
- 12:25-14:00 **Lunch** *(Novotel@Clarke Quay - The Square)*

Session 9 --- Provable security *(Chair: Anne Canteaut)*

- 14:00-14:25 **Attacks and Security Proofs of EAX-Prime**
  Kazuhiko Minematsu, Stefan Lucks, Hiraku Morita and Tetsu Iwata
  NEC Corporation, Japan

Bauhaus-Universitat Weimar, Germany
Nagoya University, Japan

- 14:25-14:50 **Towards Understanding the Known-Key Security of Block Ciphers**
  Elena Andreeva, Andrey Bogdanov and Bart Mennink
  Katholieke Universiteit Leuven, Belgium
  Technical University of Denmark, Denmark
- 14:50-15:15 **On Symmetric Encryption with Distinguishable Decryption Failures**
  Alexandra Boldyreva, Jean Paul Degabriele, Kenny Paterson and Martijn Stam
  Georgia Tech, USA
  Royal Holloway, United Kingdom
  University of Bristol, United Kingdom
- 15:15-15:40 **Coffee Break**

Session 10 --- Implementation aspects *(Chair: Axel Poschmann)*

- 15:40-16:05 **Minimalism of Software Implementation - Extensive Performance Analysis of Symmetric Primitives on the RL78 Microcontroller**
  Mitsuru Matsui and Yumiko Murakami
  Mitsubishi Electric, Japan
- 16:05-16:30 **Higher-Order Side Channel Security and Mask Refreshing**
  Jean-Sebastien Coron, Emmanuel Prouff, Matthieu Rivain and Thomas Roche
  Tranef, France
  ANSSI, France
  CryptoExperts, France
- 16:30-16:55 **Masking Tables---An Underestimated Security Risk**
  Michael Tunstall, Carolyn Whitnall and Elisabeth Oswald
  University of Bristol, United Kingdom

- 17:00-18:00 **Rump Session** *(Chairs: Tanja Lange and Daniel J. Bernstein)*
- 18:50-22:00 **Banquet** *(Swissotel Merchant Court)*

Wednesday, 13 March 2013

Session 11 --- Lightweight authenticated encryption *(Chair: Seokhie Hong)*

- 08:30-08:55 **ALE: AES-Based Lightweight Authenticated Encryption**
  Andrey Bogdanov, Florian Mendel, Francesco Regazzoni, Vincent Rijmen and Elmar Tischhauser
  Technical University of Denmark, Denmark
  TU Graz, Austria
  ALaRI – USI, Switzerland
  Katholieke Universiteit Leuven, Belgium
- 08:55-09:20 ***Related-key Attacks Against Full Hummingbird-2***
  Markku-Juhani Olavi Saarinen
  Indie, Finland

Session 12 --- Stream ciphers II *(Chair: Christian Rechberger)*

- 09:20-09:45 **A Low Data Complexity Attack on the GMR-2 Cipher Used in the Satellite Phones**
  Ruilin Li, Heng Li, Chao Li and Bing Sun
  National University of Defence Technology, Changsha, China
- 09:45-10:10 **Improving Key Recovery to 784 and 799 rounds of Trivium using Optimized Cube Attacks**
  Pierre-Alain Fouque and Thomas Vannet
  Université de Rennes 1, France
  NTT Secure Platform Laboratories, Japan
- 10:10-10:35 **Near Collision Attack on the Grain v1 Stream Cipher**
  Bin Zhang and Zhenqi Li
  Chinese Academy of Sciences, China
- 10:35-11:00 **Coffee Break**

Session 13 --- Automated cryptanalysis *(Chair: María Naya-Plasencia)*

- 11:00-11:25 **Exhausting Demirci-Selcuk Meet-in-the-Middle Attacks against Reduced-Round AES**
  Patrick Derbez and Pierre-Alain Fouque
  École Normale Supérieure, France
  Université de Rennes 1, France
- 11:25-11:50 **A Framework for Automated Independent-Biclique Cryptanalysis**
  Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks and Jakob Wenzel
  Bauhaus-University Weimar, Germany

Session 14 --- Boolean functions *(Chair: María Naya-Plasencia)*

- 11:50-12:15 **A new criterion for avoiding the propagation of linear relations through an Sbox**
  Christina Boura and Anne Canteaut
  INRIA Paris-Rocquencourt, France
  Gemalto, France
- 12:15-14:00 **Lunch** *(Novotel@Clarke Quay - The Square)*

--- End of program ---