Schedule

Sunday 18 March 2012

- 17:30 - 19:00: **Welcome reception**

Monday 19 March 2012

- 9:00 - 9:55: **Registration**
- 9:55 - 10:00: **General Chair's Opening Remarks**

Session I — Block ciphers

(Chair: Anne Canteaut)

- 10:00 - 10:25: **Improved Attacks on Full GOST**
  Itai Dinur, Orr Dunkelman and Adi Shamir
  The Weizmann Institute, Rehovot, Israel
  University of Haifa, Israel
- 10:25 - 10:50: **Zero Correlation Linear Cryptanalysis with Reduced Data Complexity**
  Andrey Bogdanov and Meiqin Wang
  KU Leuven, Belgium
  Shandong University, China

- 10:50 - 11:20: **Coffee Break**

Invited Talk I

(Chair: Anne Canteaut)

- 11:20 - 12:20: **"Provable" security against differential and linear cryptanalysis**
  Kaisa Nyberg
  Aalto University and Nokia, Finland

- 12:20 - 14:00: **Lunch**

Session II — Differential cryptanalysis

(Chair: Bruce Schneier)

- 14:00 - 14:25: **A Model for Structure Attacks, with Applications to PRESENT and Serpent**
  Meiqin Wang, Yue Sun, Elmar Tischhauser and Bart Preneel
  Shandong University, China
  Tsinghua University, China
  KU Leuven, Belgium
- 14:25 - 14:50 **A Methodology for Differential-Linear Cryptanalysis and Its Applications**
  Jiqiang Lu
  Institute for Infocomm Research, Singapore
- 14:50 - 15:15 **New Observations on Impossible Differential Cryptanalysis of Reduced-Round Camellia**
  Ya Liu, Leibo Li, Dawu Gu, Xiaoyun Wang, Zhiqiang Liu, Jiazhe Chen and Wei Li
  Shanghai Jiao Tong University, China
  Shandong University, China
  Tsinghua University, China
  Donghua University, China
  Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, China

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

Session III — Hash functions I

(Chair: Stefan Lucks)

- 15:45 - 16:10: **Improved Rebound Attack on the Finalist Grøstl**
  Jérémy Jean, María Naya-Plasencia and Thomas Peyrin
  Ecole Normale Supérieure, France
  University of Versailles Saint-Quentin-en-Yvelines, France
  Nanyang Technological University, Singapore
- 16:10 - 16:35: **(Pseudo) Preimage Attack on Reduced-Round Grøstl Hash Function and Others**
  Shuang Wu, Dengguo Feng, Wenling Wu, Jian Guo, Le Dong and Jian Zou
  State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences
  Institute for Infocomm Research, Singapore
- 16:35 - 17:00: **Practical Cryptanalysis of ARMADILLO2**
  María Naya-Plasencia and Thomas Peyrin
  University of Versailles Saint-Quentin-en-Yvelines, France
  Nanyang Technological University, Singapore
- 17:00 - 17:25: **On the (In)Security of IDEA in Various Hashing Modes**
  Lei Wei, Thomas Peyrin, Przemyslaw Sokolowski, San Ling, Josef Pieprzyk and Huaxiong Wang
  Nanyang Technological University, Singapore
  Macquarie University, Australia

Tuesday 20 March 2012

Session IV — Modes of operation

(Chair: Gilles van Assche)

- 9:00 - 9:25: **The Security of Ciphertext Stealing**
  Phillip Rogaway, Mark Wooding and Haibin Zhang
  UC Davis, USA
  Thales e-Security Ltd, UK
- 9:25 - 9:50: **McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes**
  Ewan Fleischmann, Christian Forler and Stefan Lucks
  Bauhaus-University, Germany
- 9:50 - 10:15: **Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes**
  Markku-Juhani Olavi Saarinen
  Revere Security, USA

- 10:15 - 10:45: **Coffee Break**

Session V — Hash functions II

(Chair: Yu Sasaki)

- 10:45 - 11:10: **Collision Attacks on the Reduced Dual-Stream Hash Function RIPEMD-128**
  Florian Mendel, Tomislav Nad and Martin Schläffer
  KU Leuven, Belgium
  Graz University of Technology, Austria
- 11:10 - 11:35: **Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family**
  Dmitry Khovratovich, Christian Rechberger and Alexandra Savelieva
  Microsoft Research Redmond, USA
  DTU, Denmark
  Higher School of Economics, Russia
- 11:35 - 12:00: **Converting Meet-in-the-Middle Preimage Attack into Pseudo Collision Attack: Application to SHA-2**
  Ji Li, Takanori Isobe and Kyoji Shibutani
  Sony China Research Laboratory
  Sony Corporation

- 12:00 - 14:00: **Lunch Break**

Session VI — New tools for cryptanalysis

(Chair: Pascal Junod)

- 14:00 - 14:25: **UNAF: A Special Set of Additive Differences with Application to the Differential Analysis of ARX**
  Vesselin Velichkov, Nicky Mouha, Christophe De Cannière and Bart Preneel
  ESAT/SCD-COSIC, KU Leuven, Belgium
  University of Luxembourg, Luxembourg
  IBBT, Belgium
- 14:25 - 14:50: **ElimLin Algorithm Revisited**
  Nicolas T. Courtois, Pouyan Sepehrdad, Petr Susil and Serge Vaudenay
  University College London, UK
  EPFL, Switzerland

- 14:50 - 15:20: **Coffee Break**

Invited Talk II

(Chair: Pascal Junod)

- 15:20 - 16:20: **The history of linear cryptanalysis**
  Mitsuru Matsui
  Mitsubishi Electric Corporation, Japan

- 16:30 - ...: **Rump session** *(Chairs: Dan Bernstein and Tanja Lange)*

- 18:00 - ...: **Conference dinner**

Wednesday 21 March 2012

Session VII — New designs

(Chair: Serge Vaudenay)

- 9:00 - 9:25: **Short-output universal hash functions and their use in fast and secure message authentication**
  Long Hoang Nguyen and Andrew William Roscoe
  Oxford University, UK
- 9:25 - 9:50: **Lapin: An Efficient Authentication Protocol Based on Ring-LPN**
  Stefan Heyse, Eike Kiltz, Vadim Lyubashevsky, Christof Paar and Krzysztof Pietrzak
  Ruhr-Universität Bochum, Germany
  INRIA / ENS, France
  IST, Austria
- 9:50 - 10:15: **Higher-Order Masking Schemes for S-Boxes**
  Claude Carlet, Louis Goubin, Emmanuel Prouff, Michael Quisquater and Matthieu Rivain
  Université de Paris 8, France
  Université de Versailles Saint-Quentin-en-Yvelines, France
  Oberthur Technologies, France
  CryptoExperts, France
- 10:15 - 10:40: **Recursive Diffusion Layers for Block Ciphers and Hash Functions**
  Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala and Pouyan Sepehrdad
  Isfahan University of Technology, Iran
  University of Isfahan, Iran
  EPFL, Switzerland

- 10:40 - 11:10: **Coffee Break**

Session VIII — Keccak

(Chair: John Kelsey)

- 11:10 - 11:35: **Unaligned Rebound Attack: Application to Keccak**
  Alexandre Duc, Jian Guo, Thomas Peyrin and Lei Wei
  EPFL, Switzerland
  Institute for Infocomm Research, Singapore

Nanyang Technological University, Singapore

- 11:35 - 12:00: **Differential propagation analysis of Keccak**
  Joan Daemen and Gilles Van Assche
  STMicroelectronics, Belgium
- 12:00 - 12:25: **New attacks on Keccak-224 and Keccak-256**
  Itai Dinur, Orr Dunkelman and Adi Shamir
  The Weizmann Institute, Rehovot, Israel
  University of Haifa, Israel