Fast Software Encryption 2016

Program

The program is available as a pdf here.

All technical sessions, coffee and lunch breaks take place in the event center at the Ruhr University Bochum.

Sunday 20 March 2016

- 18:00 - 20:00: **Welcome Reception and Registration at the Mercure Hotel close to the Bochum main station.**
  You will get the ticket for the subway here as well.

Monday 21 March 2016

- 8:00 - 9:00: **Registration**

(Chair: Tetsu Iwata)

Session I — Operating Modes *09:25 - 10:40*

- 09:25 - 09:50: **New Bounds for Keyed Sponges with Extendable Output: Independence between Capacity and Message Length**
  Yusuke Naito, Kan Yasuda
  Mitsubishi Electric Corporation
  NTT Secure Platform Laboratories
- 09:50 - 10:15: **RIV for Robust Authenticated Encryption**
  Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks, Jakob Wenzel
  Bauhaus-Universität Weimar
  Hochschule Schmalkalden
  Bauhaus-Universität Weimar
  Bauhaus-Universität Weimar
  Bauhaus-Universität Weimar
- 10:15 - 10:40: **A MAC Mode for Lightweight Block Ciphers**
  Atul Luykx, Bart Preneel, Elmar Tischhauser, Kan Yasuda
  Department of Electrical Engineering, ESAT/COSIC, KU Leuven, Belgium and iMinds, Belgium
  Department of Electrical Engineering, ESAT/COSIC, KU Leuven, Belgium and iMinds, Belgium
  Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark
  NTT Secure Platform Laboratories, NTT Corporation, Japan
- 10:40 - 11:10: **Coffee Break**

(Chair: Yu Sasaki)

Session II — Stream-Cipher Cryptanalysis *11:10 - 12:00*

- 11:10 - 11:35: **Cryptanalysis of the Full Spritz Stream Cipher**
  Subhadeep Banik, Takanori Isobe
  DTU Compute, Technical University of Denmark, Lyngby
  Sony Corporation, Japan

- 11:35 - 12:00: **Attacks against Filter Generators Exploiting Monomial Mappings**
  Anne Canteaut, Yann Rotella
  Inria
  Inria

(Chair: Thomas Peyrin)

Invited Talk I

- 12:00 - 13:00: **Low entropy crypto**
  Ross Anderson
  University of Cambridge, UK

- 13:00 - 14:15: **Lunch Break**

(Chair: Gregor Leander)

Session III — Components *14:15 - 15:30*

- 14:15 - 14:40: **Lightweight MDS Generalized Circulant Matrices**
  Meicheng Liu, Siang Meng Sim
  Nanyang Technological University, Singapore and Institute of Information Engineering of Chinese Academy of Sciences, China
  Nanyang Technological University, Singapore
- 14:40 - 15:05: **On the Construction of Lightweight Circulant Involutory MDS Matrices**
  Yongqiang Li, Mingsheng Wang
  The State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China
- 15:05 - 15:30: **Optimizing S-box Implementations for Several Criteria using SAT Solvers**
  Ko Stoffelen
  Radboud University, Digital Security, Nijmegen, The Netherlands

- 15:30 - 16:00: **Coffee Break**

(Chair: Svetla Nikova)

Session IV — Side-Channels and Implementations *16:00 - 17:40*

- 16:00 - 16:25: **Verifiable side-channel security of cryptographic implementations: constant-time MEE-CBC**
  José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, François Dupressoir
  HASLab, INESC TEC and University of Minho
  HASLab, INESC TEC and DCC-FC, University of Porto
  IMDEA Software Institute
  IMDEA Software Institute
- 16:25 - 16:50: **White-Box Cryptography in the Gray Box - A Hardware Implementation and its Side Channels**
  Pascal Sasdrich, Amir Moradi, Tim Güneysu
  Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Germany
  Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Germany
  University of Bremen and DFKI, Germany
- 16:50 - 17:15: **Detecting flawed masking schemes with leakage detection tests**
  Oscar Reparaz
  KU Leuven and iMinds
- 17:15 - 17:40: **There is Wisdom in Harnessing the Strengths of your Enemy: Customized Encoding to Thwart Side-Channel Attacks**
  Houssem Maghrebi, Victor Servant, Julien Bringer
  SAFRAN Morpho
  SAFRAN Morpho
  SAFRAN Morpho

Tuesday 22 March 2016

(Chair: Gaetan Leurent)

Session V — Automated Tools for Cryptanalysis *09:25 - 10:40*

- 09:25 - 09:50: **Automatic Search for Key-Bridging Technique: Applications to LBlock and TWINE**
  Li Lin, Wenling Wu, Yafei Zheng
  TCA Laboratory, SKLCS, Institute of Software, Chinese Academy of Sciences, Beijing, China
  State Key Laboratory of Cryptology, Beijing, China
  University of Chinese Academy of Sciences, Beijing, China
- 09:50 - 10:15: **MILP-Based Automatic Search Algorithms for Differential and Linear Trails for Speck**
  Kai Fu, Meiqin Wang, Yinghua Guo, Siwei Sun, Lei Hu
  Shandong University
  Shandong University
  Shandong University
  Institute of Information Engineering,Chinese Academy of Sciences
  Institute of Information Engineering,Chinese Academy of Sciences
- 10:15 - 10:40: **Automatic Search for the Best Trails in ARX: Application to Block Cipher Speck**
  Alex Biryukov, Vesselin Velichkov, Yann Le Corre
  University of Luxembourg
  University of Luxembourg
  University of Luxembourg

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

(Chair: Yannick Seurin)

Session VI — Designs *11:10 - 12:00*

- 11:10 - 11:35: **Stream ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression**
  Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, Renaud Sirdey
  Inria, France
  CEA LIST, France
  CNRS/Lab-STICC and Telecom Bretagne and UEB, France
  CryptoExperts, France
  Inria, France
  CryptoExperts, France
  CEA LIST, France
- 11:35 - 12:00: **Efficient Design Strategies Based on the AES Round Function**
  Jérémy Jean, Ivica Nikolic
  Nanyang Technological University, Singapore and ANSSI, France
  Nanyang Technological University, Singapore

(Chair: Marc Stevens)

Invited Talk II

- 12:00 - 13:00: **On White-Box Cryptography**
  Henri Gilbert
  ANSSI, France

- 13:00 - 14:15: **Lunch Break**

(Chair: Christina Boura)

Session VII — Block-Cipher Cryptanalysis *14:15 - 16:20*

- 14:15 - 14:40: **Bit-Based Division Property and Application to Simon Family**
  Yosuke Todo, Masakatu Morii
  NTT/Kobe University
  Kobe University
- 14:40 - 15:05: **Algebraic Insights into the Secret Feistel Network**
  Léo Perrin, Aleksei Udovenko
  SnT, University of Luxembourg
  SnT, University of Luxembourg

- 15:05 - 15:30: **Integrals go Statistical: Cryptanalysis of Full Skipjack Variants**
  Meiqin Wang, Tingting Cui, Huaifeng Chen, Ling Sun, Long Wen, Andrey Bogdanov
  Shandong University
  Shandong University
  Shandong University
  Shandong University
  Shandong University
  Technical University of Denmark

- 15:30 - 15:55: **Note on Impossible Differential Attacks**
  Patrick Derbez
  Université de Rennes 1, IRISA, France

- 15:55 - 16:20: **Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-guessing Techniques**
  Huaifeng Chen, Xiaoyun Wang
  Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan , China
  Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China and Institute of Advanced Study, Tsinghua University, Beijing, China

- 16:20 - 16:40: **Coffee Break**

- 16:40 - 17:30: **Rump Session** *(Chair: Daniel Bernstein and Tanja Lange)*

- 17:30 - 22:00: **Excursion and Gala Dinner at Zeche Zollverein and Casino Zollverein**
  Details follow

Wednesday 23 March 2016

(Chair: TBA)

Session VIII — Foundations and Theory *09:25 - 11:05*

- 09:25 - 09:50: **Modeling Random Oracles under Unpredictable Queries**
  Pooya Farshim, Arno Mittelbach
  ENS, France
  TU Darmstadt, Germany

- 09:50 - 10:15: **Practical Order-Revealing Encryption with Limited Leakage**
  Nathan Chenette, Kevin Lewi, Stephen A. Weis, David J. Wu
  Rose-Hulman Institute of Technology
  Stanford University
  Facebook, Inc.
  Stanford University

- 10:15 - 10:40: **Strengthening the Known-Key Security Notion for Block Ciphers**
  Benoît Cogliati, Yannick Seurin
  University of Versailles, France
  ANSSI, France

- 10:40 - 11:05: **Related-Key Almost Universal Hash Functions: Definitions, Constructions and Applications**
  Peng Wang, Yuling Li, Liting Zhang, Kaiyan Zheng
  Institute of Information Engineering, Chinese Academy of Sciences
  Institution of Software, Chinese Academy of Sciences

- 11:05 - 11:35: **Coffee Break**

(Chair: Christian Rechberger)

Session IX — Authenticated-Encryption and Hash Function Cryptanalysis
11:35 - 12:50

- 11:35 - 12:00: **Key Recovery Attack against 2.5-round π-Cipher**
  Christina Boura, Avik Chakraborti, Gaëtan Leurent, Goutam Paul, Dhiman Saha, Hadi Soleimany, Valentin Suder

Université de Versailles, France
Indian Statistical Institute, Kolkata, India
Centre de recherche Inria de Paris, France
Indian Statistical Institute, Kolkata, India
Indian Institute of Technology Kharagpur, India
Shahid Beheshti University, Iran
University of Waterloo, Canada

- 12:00 - 12:25: **Cryptanalysis of Reduced NORX**
  Nasour Bagheri, Tao Huang, Keting Jia, Florian Mendel, Yu Sasaki
  SRTTU and IPM, Iran
  Nanyang Technological University, Singapore
  Tsinghua University, China
  Graz University of Technology, Austria
  NTT Secure Platform Laboratories, Japan

- 12:25 - 12:50: **Analysis of the Kupyna-256 Hash Function**
  Christoph Dobraunig, Maria Eichlseder, Florian Mendel
  Graz University of Technology, Austria
  Graz University of Technology, Austria
  Graz University of Technology, Austria