Fast Software Encryption 2011

Program All technical sessions take place in the Oticon-salen at DTU in Lyngby.

Sunday 13 February 2011

- *(Hotel Kong Arthur)* 19:00 - 21:00: **Registration**
- *(Hotel Kong Arthur)* 19:00 - 21:00: **Welcome reception**

Monday 14 February 2011

- *(Hotel Kong Arthur)* 9:00: **Buses to Conference Venue**
- *(Oticon-salen)* 9:00 - 9:55: **Registration**

Session I — Differential Cryptanalysis *(Chair: Kaisa Nyberg)*

- 10:00 - 10:25: **Differential Cryptanalysis of Round-Reduced PRINTcipher: Computing Roots of Permutations**
  Mohamed Ahmed Abdelraheem, Gregor Leander and Erik Zenner
  DTU Mathematics, Technical University of Denmark
- 10:25 - 10:50: **Search for Related-key Differential Characteristics in DES-like ciphers**
  Alex Biryukov and Ivica Nikolic
  University of Luxembourg
- 10:50 - 11:15: **Multiple Differential Cryptanalysis: Theory and Pratice**
  Céline Blondeau and Benoît Gérard
  SECRET Project-Team - INRIA Paris-Rocquencourt, France

- 11:15 - 11:40: **Coffee Break** *(Oticon-salen)*

Invited Talk I *(Chair: Greg Rose)*

- 11:40 - 12:40: **Fast correlation attacks: Methods and countermeasures**
  Willi Meier
  FHNW Switzerland

- 12:45 - 14:00: **Lunch Break** *(Glassalen)*

Session II — Hash Functions I *(Chair: Stefan Lucks)*

- 14:00 - 14:25: **Analysis of reduced-SHAvite-3-256 v2**
  Marine Minier, María Naya-Plasencia and Thomas Peyrin
  Université de Lyon, INRIA, INSA Lyon, France
  FHNW, Switzerland
  Nanyang Technological University, Singapore
- 14:25 - 14:50: **An Improved Algebraic Attack on Hamsi-256**
  Itai Dinur and Adi Shamir
  Computer Science department, The Weizmann Institute, Rehovot, Israel
- 14:50 - 15:15: **Practical Near-Collisions and Collisions on Round-Reduced ECHO-256 Compression Function.**
  Jérémy Jean and Pierre-Alain Fouque
  ENS, Paris, France

- 15:15 - 15:45: **Coffee Break** *(Oticon-salen)*

Session III — Security and Models *(Chair: Tetsu Iwata)*

- 15:45 - 16:10: **On Cipher-Dependent Related-Key Attacks in the Ideal-Cipher Model**
  Pooya Farshim, Kenny Paterson, Martin Albrecht and Gaven Watson
  SALSA Project - INRIA Paris-Rocquencourt, France
  Information Security Group, Royal Holloway, University of London, UK.
  Department of Computer Science, University of Calgary, Australia
- 16:10 - 16:35: **On the Security of Hash Functions Employing Blockcipher Postprocessing**
  Donghoon Chang, Mridul Nandi, and Moti Yung
  National Institute of Standards and Technology (NIST), USA
  C R Rao AIMSCS Institute, Hyderabad, India, and Google Inc.
  Department of Computer Science, Columbia University, New York, USA.

Best Paper Award Ceremony (Chair: Antione Joux)

- 16:35 - 16:40 (Oticon-salen)

Rump Session *(Chair: V. Rijmen)*

- 16:40 - 17:40: **...** *(Oticon-salen)*

- 18:00 **Buses to Hotel Kong Arthur** *(Oticon-salen)*

Tuesday 15 February 2011

- 9:00: **Buses to Conference Venue** *(Hotel Kong Arthur)*

Session IV — Stream Ciphers *(Chair: Anne Canteaut)*

- 9:45 - 10:10: **Breaking Grain-128 with Dynamic Cube Attacks**
  Itai Dinur and Adi Shamir
  Computer Science department, The Weizmann Institute, Rehovot, Israel
- 10:10 - 10:35: **Cryptanalysis of the Knapsack Generator**
  Simon Knellwolf and Willi Meier
  FHNW Switzerland
- 10:35 - 11:00: **Attack on Broadcast RC4 Revisited**
  Subhamoy Maitra, Goutam Paul and Sourav Sen Gupta
  Applied Statistics Unit, Indian Statistical Institute, Kolkata, India
  Department of Computer Science & Engineering, Jadavpur University, Kolkata, India

- 11:00 - 11:30: **Coffee Break** *(Oticon-salen)*

Session V — Hash Functions II *(Chair: Thomas Peyrin)*

- 11:30 - 11:55: **Boomerang Attacks on BLAKE-32**
  Alex Biryukov, Ivica Nikolic and Arnab Roy
  University of Luxembourg
- 11:55 - 12:20: **Practical Partial-Collisions on the Compression Function of BMW**
  Gaëtan Leurent and Søren Thomsen
  University of Luxembourg
  DTU Mathematics, Technical University of Denmark
- 12:20 - 12:45: **Higher-order differential properties of Keccak and Luffa**
  Christina Boura, Anne Canteaut and Christophe De Cannière
  SECRET Project-Team, INRIA Paris-Rocquencourt, France
  Gemalto, France

Department of Electrical Engineering ESAT/SCD-COSIC, Katholieke Universiteit Leuven, Belgium

- 12:45 - 14:00: **Lunch Break** *(Glassalen)*

Session VI — Block Ciphers and Modes *(Chair: Christian Rechberger)*

- 14:00 - 14:25: **Cryptanalysis of PRESENT-like ciphers with secret S-boxes**
  Julia Borghoff, Lars Ramkilde Knudsen, Gregor Leander and Søren Steffen Thomsen
  DTU Mathematics, Technical University of Denmark
- 14:25 - 14:50: **A Single-Key Attack on the Full GOST Block Cipher**
  Takanori Isobe
  Sony Corporation, Japan
- 14:50 - 15:15: **The Software Performance of Authenticated-Encryption Modes**
  Ted Krovetz and Phillip Rogaway
  California State University, Sacramento, USA
  University of California, Davis, USA

- 15:15 - 15:45: **Coffee Break** *(Oticon-salen)*

Invited Talk II *(Chair: Antoine Joux)*

- 15:45 - 16:45: **The past, present and future of hash functions - a rehash of some old and new results.**
  Ivan Damgård
  Aarhus University, Denmark

- 17:00 **Buses to Hotel Kong Arthur** *(Oticon-salen)*

- 18:00 - 19:00: **Cocktail and Exhibition** *(Danish Design Center)*
- 19:00 - 23:00: **Dinner** *(Danish Design Center)*

Wednesday 16 February 2011

- 9:00: **Buses to Conference Venue** *(Hotel Kong Arthur)*

Session VII — Linear and Differential Cryptanalysis *(Chair: Marion Videau)*

- 9:45 - 10:10: **Cryptanalysis of Hummingbird-1**
  Markku-Juhani O. Saarinen
  Revere Security, Addison, USA
- 10:10 - 10:35: **The Additive Differential Probability of ARX**
  Vesselin Velichkov, Nicky Mouha, Christophe De Cannière and Bart Preneel
  Department of Electrical Engineering ESAT/SCD-COSIC, Katholieke Universiteit Leuven, Belgium
  Interdisciplinary Institute for BroadBand Technology (IBBT), Belgium
- 10:35 - 11:00: **Linear Approximations of Addition Modulo 2^n-1**
  Chunfang Zhou, Xiutao Feng and Chuankun Wu
  Institute of Software, Chinese Academy of Sciences,Beijing, China

- 11:00 - 11:30: **Coffee Break** *(Oticon-salen)*

Session VIII — Hash Functions III *(Chair:* María Naya-Plasencia*)*

- 11:30 - 11:55: **Meet-in-the-Middle Preimage Attacks on AES Hashing Modes and an Application to Whirlpool**
  Yu Sasaki
  NTT Corporation, Japan
- 11:55 - 12:20: **Known-Key Distinguishers for 11-Round Feistel Ciphers: Application to Collision Attacks on Their Hashing Modes**
  Yu Sasaki and Kan Yasuda
  NTT Corporation, Japan

- 12:30 - 13:30: **Lunch Break** *(Glassalen)*

- 14:00: **Beginning of SKEW 2011** *(separate registration required)*

  - 19:00 - 21:00: **Reception at the City Hall Copenhagen, joint with SKEW 2011**

    (City Hall Copenhagen)