Fast Software Encryption 2009

Program

All technical sessions take place in the Promotiezaal, Naamsestraat 22.

Sunday 22 February 2009

17:00 – 20:00 **Registration** *(Promotiezaal)*

19:00 – 20:00 **Welcome reception** *(Town hall, Stadhuis)*

Monday 23 February 2009

8:30 – 9:15 **Registration** *(Museumzaal)*

9:15 – 9:25 **Opening**
Orr Dunkelman (program chair), Bart Preneel (general chair)

Session I — Stream Ciphers

Chair: Kaisa Nyberg

9:25 – 9:50 **Cube Testers and Key Recovery Attacks On Reduced-Round MD6 and Trivium**
Jean-Philippe Aumasson, Willi Meier, Itai Dinur and Adi Shamir
FHNW, Windisch, Switzerland and The Weizmann Institute, Israel

9:50 – 10:15 **An Efficient State Recovery Attack on X-FCSR-256**
Paul Stankovski, Martin Hell and Thomas Johansson
Lund University, Sweden

10:15 – 10:40 **Key Collisions of the RC4 Stream Cipher**
Mitsuru Matsui
Mitsubishi Electric, Japan

10:40 – 11:15 **Coffee Break** *(Museumzaal)*

Session II — Invited Talk

Chair: Steve Babbage

11:15 – 12:15 **Intel's New AES Instructions for Enhanced Performance and Security**
Shay Gueron
Intel Corporation, Haifa, Israel and University of Haifa, Israel

12:15 – 14:00 **Lunch Break** *(Salons Georges)*

Session III — Theory of Hash Functions

Chair: Tetsu Iwata

14:00 – 14:25 **Blockcipher Based Hashing Revisited**
Martijn Stam
EPFL, Switzerland

14:25 – 14:50 **On the Security of Tandem-DM**
Ewan Fleischmann, Michael Gorski and Stefan Lucks
Bauhaus-University Weimar, Germany

14:50 – 15:15 **Indifferentiability of Permutation-Based Compression Functions and Tree-Based Modes of Operation, with Applications to MD6**
Yevgeniy Dodis, Leonid Reyzin, Ronald L. Rivest and Emily Shen
New York University, USA, Boston University, USA and Massachusetts Institute of Technology, USA

15:15 – 15:45 **Coffee Break** *(Museumzaal)*

Session IV — Hash Functions Analysis I

Chair: Christian Rechberger

15:45 – 16:10 **Cryptanalysis of RadioGatún**
Thomas Fuhr and Thomas Peyrin
DCSSI, France and Ingenico, France

16:10 – 16:35 **Preimage Attacks on Reduced Tiger and SHA-2**
Takanori Isobe and Kyoji Shibutani
Sony Corporation, Japan

16:35 – 17:00 **Collisions of the LAKE Hash Family**
Alex Biryukov, Praveen Gauravaram, Jian Guo, Dmitry Khovratovich, San Ling, Krystian Matusiewicz, Ivica Nikolic, Josef Pieprzyk and Huaxiong Wang
University of Luxembourg, Luxembourg, Technical University of Denmark, Denmark, Nanyang Technological University, Singapore and Macquaire University, Australia

19:00 – 20:00 **Cultural event** *(STUK, Naamsestraat 96)*

Tuesday 24 February 2009

Session V — Block Ciphers Analysis

Chair: Mitsuru Matsui

9:15 – 9:40 **New Cryptanalysis of Block Cipher with Low Algebraic Degree**
Bing Sun, Longjiang Qu and Chao Li
Science College of National University of Defence Technology, China and Southeast University, China

9:40 – 10:05 **Algebraic Techniques in Differential Cryptanalysis**
Martin Albrecht and Carlos Cid
Royal Holloway, University of London, United Kingdom

10:05 – 10:30 **Multidimensional Extension of Matsui's Algorithm 2**
Miia Hermelin, Joo Yeon Cho and Kaisa Nyberg
Helsinki University of Technology (TKK), Finland and Nokia Finland

10:30 – 11:00 **Coffee Break** *(Museumzaal)*

Session VI — Hash Functions Analysis II

Chair: Christophe De Cannière

11:00 – 11:25 **Meet-in-the-Middle Attacks on SHA-3 Candidates**
Dmitry Khovratovich, Ivica Nikolic and Ralf-Philipp Weinmann
University of Luxembourg, Luxembourg

11:25 – 11:50 **Practical collisions for EnRUPT**
Sebastiaan Indesteege and Bart Preneel
Katholieke Universiteit Leuven and IBBT, Belgium

11:50 – 12:15 **The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl**
Florian Mendel, Christian Rechberger, Martin Schläffer and Søren S. Thomsen
Graz University of Technology, Austria and Technical University of Denmark, Denmark

12:15 – 14:00 **Lunch Break** *(Salons Georges)*

Session VII — Block Ciphers

Chair: Håvard Raddum

14:00 – 14:25 **Revisiting the IDEA Philosophy**
Pascal Junod and Marco Macchetti
University of Applied Sciences Western, Switzerland and Nagracard SA, Switzerland

14:25 – 14:50 **Cryptanalysis of the ISDB Scrambling Algorithm (MULTI2)**
Jean-Philippe Aumasson, Jorge Nakahara Jr. and Pouyan Sepehrdad
FHNW, Windisch, Switzerland and EPFL, Lausanne, Switzerland

14:50 – 15:20 **Coffee Break** *(Museumzaal)*

Session VIII — Theory

Chair: Stefan Lucks

15:20 – 15:45 **Beyond-Birthday-Bound Security Based on Tweakable Block Ciphers**
Kazuhiko Minematsu
NEC Corporation, Japan

15:45 – 16:10 **Enhanced Target Collision Resistant Hash Functions Revisited**
Mohammad Reza Reyhanitabar, Willy Susilo and Yi Mu
University of Wollongong, Australia

Rump Session

Chair: Dan Bernstein

16:15 – 18:00 **Rump Session**

19:30 – ... **Banquet** *(Restaurant Faculty Club)*

Wednesday 25 February 2009

Session IX — Message Authentication Codes

Chair: Bart Preneel

9:15 – 9:40 **MAC Reforgeability**
John Black and Martin Cochran
University of Colorado at Boulder, USA and Google, Inc, USA

9:40 – 10:05 **New Distinguishing Attack on MAC using Secret-Prefix Method**
Xiaoyun Wang, Wei Wang, Keting Jia, and Meiqin Wang
Tsinghua University, China and Key Laboratory of Cryptologic Technology and Information Security, China

10:05 – 10:30 **Fast and Secure CBC Type MAC Algorithms**
Mridul Nandi
National Institute of Standards and Technology, USA

10:30 – 10:55 **HBS: A Single-Key Mode of Operation for Deterministic Authenticated Encryption**
Tetsu Iwata and Kan Yasuda
Nagoya University, Japan and NTT Corporation, Japan

10:55 – 11:25 **Coffee Break** *(Museumzaal)*

Session X — Invited Talk

Chair: Willi Meier

11:25 – 12:10 **Looking back at the eSTREAM Project**
Matt Robshaw
France Telecom, France

12:10 – 12:15 **Concluding Remarks**
Orr Dunkelman (program chair), Bart Preneel (general chair)

12:15 – 14:00 **Lunch Break** *(Salons Georges)*

14:00 – **Opening of the First SHA-3 Candidate Conference**
(separate registration required)