SASC 2007
Workshop Program (preliminary)

Tuesday, January 30, 2007: 19.00 h Reception and Registration at the Park Inn Hotel

Wednesday, January 31, 2007

8.15 Registration
9.00 Opening Remarks

Cryptanalysis I

9.10-9.30 Two Trivial Attacks on Trivium
Alexander Maximov and Alex Biryukov

9.30-9.45 Some Thoughts on Trivium
Steve Babbage

9.45-10.00 Linear Approximations for 2-round Trivium
Meltem Sönmez Turan and Orhun Kara

10.00-10.20 Cryptanalysis of Hermes8F
Steve Babbage, Carlos Cid, Norbert Pramstaller and Havard Raddum

10.20-10.40 Differential Cryptanalysis of Salsa20/8
Yukiyasu Tsunoo, Teruo Saito, Hiroyasu Kubo, Tomoyasu Suzaki and Hiroki Nakashima

Coffee Break

Cryptanalysis II

11.00-11.20 Attacking the Filter Generator over GF(2^m)
Sondre Rønjom and Tor Helleseth

11.20-11.35 Assessing the Security of Key Length
Iain Devlin and Alan Purvis

11.35-11.50 A Note on Distinguishing Attacks
Håkan Englund, Martin Hell and Thomas Johansson

11.50-12.10 Differential Power Analysis of Stream Ciphers
Wieland Fischer, Berndt M. Gammel, Oliver Kniffler and Joachim Velten

Lunch

Software performance

14.00-14.15 eSTREAM update on software performance
Christophe De Cannière

14.15-14.30 Cycle counts for authenticated encryption
Daniel J. Bernstein

14.30-14.45 Studying hardware/software codesign for stream ciphers
Patrick Schaumont and Ingrid Verbauwhed

14.45-15.05 Software Implementation of eSTREAM Profile I Ciphers on embedded 8-bit AVR Microcontrollers
Gordon Meiser, Thomas Eisenbarth, Kerstin Lemke-Rust and Christof Paar

15.05-15.20 Throughput/code size tradeoff for stream ciphers
Cédric Lauradoux

Coffee break

Cryptanalysis III

15.45-16.05 Cryptanalysis of Achterbahn-128/80
María Naya Plasencia

16.05-16.20 Achterbahn-128/80: Design and Analysis
Berndt M. Gammel, Rainer Goettfert and Oliver Kniffler

16.20-16.40 Overtaking VEST
Antoine Joux and Jean-René Reinhard

16.40-16.55 On the security of FCSR-based pseudorandom generators
François Arnault and Thierry P. Berger and Marine Minier

19.30 Dinner

Thursday, February 1, 2007

Hardware performance

9.00-9.20 Hardware results for selected stream cipher candidates
T. Good and M. Benaissa

9.20-9.40 FPGA Implementations of eSTREAM Phase-2 Focus Candidates with Hardware Profile
Philippe Bulens, Kassem Kalach, François-Xavier Standaert and Jean-Jacques Quisquater

9.40-10.00 Hardware evaluation of eSTREAM Candidates: Grain, Lex, Mickey128, Salsa20 and Trivium
Marcin Rogawski

10.00-10.20 Comparison of hardware performance of selected Phase II eSTREAM candidates
Kris Gaj, Gabriel Southern and Ramakrishna Bachimanchi

10.20-10.40 Comparison of Low-Power Implementations of Trivium and Grain
Martin Feldhofer

Coffee break

Designs and theory

11.00-11.15 CryptMT Stream Cipher Version 3
Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura and Mariko Hagita

11.15-11.35 A Word-Oriented Stream Cipher Using Clock Control
Shinsaku Kiyomoto, Toshiaki Tanaka and Kouichi Sakurai

11.35-11.55 MV3: A new word based stream cipher using rapid mixing and revolving buffers
Nathan Keller, Stephen D. Miller, Ilya Mironov and Ramarathnam Venkatesan

11.55-12.10 Adding MAC functionality to Edon80
Danilo Gligoroski and Svein Johan Knapskog

12.10-12.25 A Note on Algebraic Properties of Quasigroups in Edon80
Milan Vojvoda, Marek Sýs and Matúš Jókay

Lunch

Cryptanalysis IV

14.00-14.20 On a bias of Rabbit
Jean-Philippe Aumasson

14.20-14.40 Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy
Hongjun Wu and Bart Preneel

14.40-14.55 How to Break Py and Pypy by a Chosen-IV Attack
Takanori Isobe, Toshihiro Ohigashi, Hidenori Kuwakado and Masakatu Morii

Rump session

14.55-15.20 Rump session

Coffee break

Discussion

15.45-17.00 Discussion on IP, performance, security requirements, eSTREAM process, others

17.00-17.05 Closing remarks