SAC 2006 *Preliminary* Program

All events, except the Banquet, are held at the EV building (1515 St. Catherine W.)

All the presentations will be held at EV2.260

The Wednesday reception will be held at EV2.184

The board meeting (open only to board members) will be held at EV9.221

Wednesday August 16, 2006

18:30-20:00 Light social reception (EV2.184)

Thursday August 17, 2006

08:00 Registration and Morning Coffee
08:50-09:00 Welcome Remarks

Block Cipher Cryptanalysis

Chair: Bart Preneel

09:25-09:50 Improved DST Cryptanalysis of IDEA
Eyup Serdar Ayaz, Ali Aydin Selcuk

09:50-10:15 Improved Related-Key Impossible Differential Attacks on Reduced-Round AES-192
Wentao Zhang, Wenling Wu, Lei Zhang, Dengguo Feng

09:00-09:25 Related-Key Rectangle Attack on the Full SHACAL-1
Orr Dunkelman, Nathan Keller, Jongsung Kim

10:15-10:45 Coffee Break

Stream Cipher Cryptanalysis I

Chair: Helena Handschuh

10:45-11:10 Cryptanalysis of Achterbahn-Version 2
Martin Hell, Thomas Johansson

11:10-11:35 Cryptanalysis of the Stream Cipher ABC v2
Hongjun Wu, Bart Preneel

Invited Talk I: The Stafford Tavares Lecture

Chair: Eli Biham

11:35-12:30 A Top View of Side Channels
Adi Shamir

12:30-14:00 Lunch (EV2.184)

Block and Stream Ciphers

Chair: Orr Dunkelman

14:00-14:25 The Design of a Stream Cipher Lex
Alex Biryukov

14:25-14:50 Dial C for Cipher
Thomas Baignères, Matthieu Finiasz

14:50-15:15 Tweakable Block Cipher Revisited
Kazuhiko Minematsu

15:15-15:45 Coffee Break

Side-Channel Attacks

Chair: Carlisle Adams

15:45-16:10 Extended Hidden Number Problem and its Cryptanalytic Applications
Martin Hlaváč, Tomáš Rosa

16:10-16:35 Changing the Odds against Masked Logic
Kris Tiri, Patrick Schaumont

16:35-17:00 Advances on Access-driven Cache Attacks on AES
Michael Neve, Jean-Pierre Seifert

17:00-17:25 Blind Differential Cryptanalysis for Enhanced Power Attacks
Helena Handschuh, Bart Preneel

18:30-21:00 Banquet at BOCCA D'ORO restaurant (1448 rue St-Mathieu, H3H 2H9)

Friday August 18, 2006

08:00-08:30 Morning Coffee

Efficient Implementations I

Chair: Doug Stinson

08:35-09:00 Efficient Implementations of Multivariate Quadratic Systems
Come Berbain, Olivier Billet, Henri Gilbert

09:00-09:25 Unbridle the Bit-Length of a Crypto-Coprocessor with Montgomery Multiplication
Masayuki Yoshino, Katsuyuki Okeya, Camille Vuillaume

09:25-09:50 Delaying and Merging Operations in Scalar Multiplication: Applications to Curve-Based Cryptosystems
Roberto Avanzi

09:50-10:20 Coffee Break

Stream Cipher Cryptanalysis II

Chair: Alex Biryukov

10:20-10:45 On the Problem of Finding Linear Approximations and Cryptanalysis of Pomaranch Version 2
Martin Hell, Thomas Johansson

10:45-11:10 Multi-Pass Fast Correlation Attack on Stream Ciphers
Bin Zhang, Dengguo Feng

11:10-11:35 Crossword Puzzle Attack on NLS
Joo Yeon Cho, Josef Pieprzyk

Invited Talk II

Chair: Stafford Tavares

11:35-12:30 When Stream Cipher Analysis Meets Public-Key Cryptography
Serge Vaudenay

12:30-14:00 Lunch (EV2.184)

Efficient Implementations II

Chair: Michael Wiener

14:00-14:25 On Redundant tau-adic Expansions and Non-Adjacent Digit Sets
Roberto Avanzi, Clemens Heuberger, Helmut Prodinger

14:25-14:50 Pairing Calculation on Supersingular Genus 2 Curves
Colm Ó hÉigeartaigh, Michael Scott

14:50-15:15 Efficient Divisor Class Halving on Genus Two Curves
Peter Birkner

15:15-15:45 Coffee Break

Message Authentication Codes

Chair: Jean-Jacques Quisquater

15:45-16:10 Message Authentication on 64-bit Architectures
Ted Krovetz

16:10-16:35 Some Notes on the Security of the Timed Efficient Stream Loss-tolerant Authentication Scheme
Goce Jakimoski

Hash Functions

Chair: Amr Youssef

16:35-17:00 Constructing an Ideal Hash Function from Weak Ideal Compression Functions
Moses Liskov

17:00-17:25 Provably Good Codes for Hash Function Design
Charanjit S. Jutla, Anindya C. Patthak

17:25-17:30 Closing Remarks