SAC 2007 Program

Wednesday August 15, 2007

18:30-20:00 Light social reception

Thursday August 16, 2007

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

Stream Cipher Cryptanalysis I

09:00-09:25 Reduced Complexity Attacks on the Alternating Step Generator
Shahram Khazaei, Simon Fischer, and Willi Meier
09:25-09:50 Extended BDD-based Cryptanalysis of Keystream Generators
Dirk Stegemann
09:50-10:15 Two Trivial Attacks on Trivium
Alexander Maximov and Alex Biryukov

10:15-10:45 **Coffee Break**

Hash Function Attacks

10:45-11:10 Collisions for 70-step SHA-1: On the Full Cost of Collision Search
Christophe De Cannière, Florian Mendel, and Christian Rechberger
11:10-11:35 Cryptanalysis of the CRUSH Hash Function
Matt Henricksen and Lars R. Knudsen

Invited Talk I

11:35-12:30 Edwards Coordinates for Elliptic Curves
Dan Bernstein

12:30-14:00 **Lunch**

Side-Channel Attacks

14:00-14:25 Improved Side-Channel Collision Attacks on AES
Andrey Bogdanov
14:25-14:50 Analysis of countermeasures against access driven cache attacks on AES
Johannes Blömer and Volker Krummel
14:50-15:15 Power Analysis for Secret Recovering and Reverse Engineering of Public Key Algorithms
Frederic Amiel, Benoit Feix, and Karine Villegas

15:15-15:45 **Coffee Break**

Efficient Implementations

15:45-16:10 Koblitz Curves and Integer Equivalents of Frobenius Expansions
Billy Bob Brumley and Kimmo Järvinen
16:10-16:35 Another Look at Square Roots (and Other Less Common Operations) in Fields of Even Characteristic
Roberto M. Avanzi
16:35-17:00 Efficient Explicit Formulae for Genus 2 Hyperelliptic Curves over Prime Fields and Their Implementations
Xinxin Fan and Guang Gong
17:00-17:25 Explicit formulas for multiplication in GF(3^(6m))
Elisa Gorla, Christoph Puttmann, and Jamshid Shokrollahi

18:30-23:00 **Ottawa River Cruise and Banquet**

Friday August 17, 2007

08:00-08:30 Morning Coffee

Block Cipher Cryptanalysis

08:35-09:00 Linear Cryptanalysis of Non Binary Ciphers with an Application to SAFER
Thomas Baignères, Jacques Stern, and Serge Vaudenay
09:00-09:25 The Delicate Issues of Addition with Respect to XOR Differences
Gaoli Wang, Nathan Keller, and Orr Dunkelman
09:25-09:50 MRHS Equation Systems
Håvard Raddum

09:50-10:20 **Coffee Break**

A New Stream Cipher

10:20-10:45 A fast stream cipher with huge state space and quasigroup filter for software
Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita

White Box Cryptanalysis

10:45-11:10 Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings
Brecht Wyseur, Wil Michiels, Paul Gorissen, and Bart Preneel
11:10-11:35 Cryptanalysis of White Box DES Implementations
Louis Goubin, Jean-Michel Masereel, and Michael Quisquater

Invited Talk II: The Stafford Tavares Lecture

11:35-12:30 Cryptography and Virology Inter-Relationships
Moti Yung

12:30-14:00 **Lunch**

Message Authentication Code Attack

14:00-14:25 Attacks on the ESA-PSS-04-151 MAC Scheme
Georg Illies and Marian Margraf

Modes of Operation

14:25-14:50 The Security of the Extended Codebook (XCB) Mode of Operation
David A. McGrew and Scott R. Fluhrer
14:50-15:15 A Generic Method to Design Modes of Operation Beyond the Birthday Bound
David Lefranc, Philippe Painchault, Valérie Rouat, and Emmanuel Mayer

15:15-15:45 **Coffee Break**

Stream Cipher Cryptanalysis II

15:45-16:10 Passive-only Key Recovery Attacks on RC4
Serge Vaudenay and Martin Vuagnoux
16:10-16:35 Permutation After RC4 Key Scheduling Reveals the Secret Key
Goutam Paul and Subhamoy Maitra
16:35-17:00 Revisiting correlation-immunity in filter generators
Aline Gouget and Hervé Sibert
17:00-17:25 Distinguishing Attack against TPypy
Yukiyasu Tsunoo, Teruo Saito, Takeshi Kawabata, and Hiroki Nakashima

17:25-17:30 **Closing Remarks**