SAC 2010 Program

All talks will take place in EIT 1015.

Wednesday, August 11, 2010

18:30 - 20:30 Reception and Registration. EIT atrium, first floor.

Thursday, August 12, 2010

8:00 - 8:55 Registration and light breakfast.

8:55 - 9:05 Opening remarks and announcements.

Hash Functions I

9:05 - 9:30 *Zero-sum Distinguishers for Iterated Permutations and Application to* KECCAK-*f and Hamsi-256.* **Christina Boura and Anne Canteaut.**

9:30 - 9:55 *Attacks on Hash Functions Based on Generalized Feistel – Application to Reduced-Round Lesamnta and SHAvite-3*$_{512}$*.* **Charles Bouillaguet, Orr Dunkelman, Gaëtan Leurent, and Pierre-Alain Fouque.**

9:55 - 10:20 *The Differential Analysis of S-functions.* **Nicky Mouha, Vesselin Velichkov, Christophe De Cannière and Bart Preneel.**

10:20 - 10:45 Coffee Break.

Stream Ciphers

10:45 - 11:10 *Hill Climbing Algorithms and Trivium.* **Julia Borghoff, Lars R. Knudsen, and Krystian Matusiewicz.**

11:10 - 11:35 *Discovery and Exploitation of New Biases in RC4.* **Pouyan Sepehrdad, Serge Vaudenay and Martin Vuagnoux.**

The Stafford Tavares Lecture

11:35 - 12:30 *The Rise and Fall and Rise of Combinatorial Key Predistribution.* **Keith Martin.**

12:30 - 14:00 Lunch, University Club.

Efficient Implementations

14:00 - 14:25 *A Low-Area yet Performant FPGA Implementation of Shabal.* **Jérémie Detrey, Pierrick Gaudry, and Karim Khalfallah.**

14:25 - 14:50 *Implementation of Symmetric Algorithms on a Synthesizable 8-Bit Microcontroller Targeting Passive RFID Tags.* **Thomas Plos, Hannes Groß, and Martin Feldhofer.**

14:50 - 15:15 *Batch Computations Revisited: Combining Key Computations and Batch Verifications.* **René Struik.**

15:15 - 15:40 Coffee Break.

Codes and Combinatorics

15:40 - 16:05 *Wild McEliece.* **Daniel J. Bernstein, Tanja Lange and Christiane Peters.**

16:05 - 16:30 *Parallel-CFS – Strengthening the CFS McEliece-Based Signature Scheme.* **Matthieu Finiasz.**

16:30 - 16:55 *A Zero-knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem.* **Pierre-Louis Cayrel, Pascal Véron, and Sidi Mohamed El Yousfi Alaoui.**

16:55 - 17:20 *Optimal Covering Codes for Finding Near-Collisions.* **Mario Lamberger and Vincent Rijmen.**

18:30 Banquet, University Club

Friday, August 13, 2010

8:00 - 8:55 Registration and light breakfast.

8:55 - 9:05 Announcements.

Block Ciphers

9:05 - 9:30 *Tweaking AES.* **Ivica Nikolić.**

9:30 - 9:55 *On the Diffusion of Generalized Feistel Structures Regarding Differential and Linear Cryptanalysis.* **Kyoji Shibutani.**

9:55 - 10:20 *Generalizing Meet-in-the-Middle Attacks: Cryptanalysis of the Lightweight Block Cipher KTANTAN.* **Andrey Bogdanov and Christian Rechberger.**

10:20 - 10:45 Coffee Break.

Side Channel Attacks

10:45 - 11:10 *Optimizing DPA by Peak Distribution Analysis.* **Jing Pan, Jerry I. den Hartog, Jasper G. J. van Woudenberg, and Marc F. Witteman.**

11:10 - 11:35 *Affine Masking Against Higher-Order Side Channel Analysis.* **Guillaume Fumaroli, Ange Martinelli, Emmanuel Prouff, and Matthieu Rivain.**

Invited Talk

11:35 - 12:30 *Search on Encrypted Data in the Symmetric-Key Setting.* **Alexandra Boldyreva.**

12:30 - 14:00 Lunch, University Club.

Mathematical Aspects

14:00 - 14:25 *Preimages for the Tillich-Zémor Hash Function.* **Christophe Petit and Jean-Jacques Quisquater.**

14:25 - 14:50 *One-time Signatures and Chameleon Hash Functions.* **Payman Mohassel.**

14:50 - 15:15 *On the Minimum Communication Effort for Secure Group Key Exchange.* **Frederik Armknecht and Jun Furukawa.**

15:15 - 15:40 Coffee Break.

Hash Functions II

15:40 - 16:05 *Deterministic Differential Properties of the Compression Function of BMW.* **Jian Guo and Søren S. Thomsen.**

16:05 - 16:30 *Security Analysis of SIMD.* **Charles Bouillaguet, Pierre-Alain Fouque, and Gaëtan Leurent.**

16:30 - 16:55 *Subspace Distinguisher for 5/8 Rounds of the ECHO-256 Hash Function.* **Martin Schläffer.**

16:55 - 17:20 *Cryptanalysis of Luffa v2 Components.* **Dmitry Khovratovich, María Naya-Plasencia, Andrea Röck, and Martin Schläffer.**