Workshop on Selected Areas in Cryptography

SAC 2004 Program

August 8–10, 2004
University of Waterloo, Waterloo, Canada

Event locations: Registration, Welcome Reception and Coffee Breaks are in EIT Foyer. All lectures are in EIT 1015. Luncheons on Aug. 9 and 10 are in EIT 3142. Banquet on Aug. 9 is in Festival Hall, SCH.

Sunday, August 8, 2004
18:00–20:00 Registration and Welcome Reception (wine and cheese)

Monday, August 9, 2004
8:00-8:50 Registration and Morning Coffee
8:50–9:00 Welcome Remarks

Session 1: Stream Cipher Cryptanalysis

9:00–9:25 An improved correlation attack on A5/1
Alexander Maximov, Thomas Johansson and Steve Babbage

9:25–9:50 Extending the Framework of the Resynchronization Attack
Frederik Armknecht, Joseph Lano and Bart Preneel

9:50–10:15 A new simple technique to attack filter generators and related ciphers
Håkan Englund and Thomas Johansson

10:15–10:45 Coffee break

Session 2: Side-channel Analysis

10:45–11:10 On XTR and Side-Channel Analysis
Daniel Page and Martijn Stam

11:10–11:35 Provably Secure Masking of AES
Johannes Blömer, Jorge Guajardo Merchán and Volker Krummel
Invited Talk 1: Stafford Tavares Lecture

11:35–12:30 New Results on SHA-0 and SHA-1
   Eli Biham

12:30–14:00 Lunch

Session 3: Block cipher design

14:00–14:25 Perfect Diffusion Primitives for Block Ciphers - Building Efficient MDS Matrices
   Pascal Junod and Serge Vaudenay

14:25–14:50 Security of the MISTY Structure in the Luby-Rackoff Model: Improved Results
   Gilles Piret and Jean-Jacques Quisquater

14:50–15:15 FOX: a new family of block ciphers
   Pascal Junod and Serge Vaudenay

15:15–15:45 Coffee break

Session 4: Efficient Implementations

15:45–16:10 A Note on the Signed Sliding Window Integer Recoding and its Left-to-Right Analogue
   Roberto Maria Avanzi

16:10–16:35 Fast Irreducibility Testing for XTR Using a Gaussian Normal Basis of Low Complexity
   Soonhak Kwon, Chang Hoon Kim and Chun Pyo Hong

16:35–17:00 Modular number systems: beyond the Mersenne family
   Jean-Claude Bajard and Laurent Imbert and Thomas Plantard

17:00–17:25 Efficient Doubling on Genus Two Curves over Binary Fields
   Marc Stevens and Tanja Lange

18:30–21:00 Banquet

Tuesday, August 10, 2004

Session 5: Secret Key Cryptography I

8:00–8:30 Morning Coffee

8:35–9:00 About the Security of Ciphers (Semantic Security and Pseudo-Random Permutations)
   Duong Hieu Phan and David Pointcheval
9:00–9:25  A Subliminal Channel in Secret Block Ciphers  
Adam Young and Moti Yung  

9:25–9:50  Blockwise Adversarial Model for On-line Ciphers and Symmetric Encryption Schemes  
Pierre-Alain Fouque, Antoine Joux and Guillaume Poupard  

9:50–10:20  Coffee break  

Session 6: Cryptanalysis  

10:20–10:45  Cryptanalysis of a White Box AES Implementation  
Olivier Billet, Henri Gilbert and Charaf Ech-Chatbi  

10:45–11:10  Predicting Subset Sum Pseudorandom Number Generators  
Joachim von zur Gathen and Igor E. Shparlinski  

11:10–11:35  Collision Attack and Pseudorandomness of Reduced-Round Camellia  
Wu WenLing, Feng Dengguo and Chen Hua  

Invited Talk 2  

11:35–12:30  Basing Cryptography on Biometrics and Other Noisy Data  
Yevgeniy Dodis  

12:30–14:00  Lunch  

Session 7: Cryptographic Protocols  

14:00–14:25  Password Based Key Exchange With Mutual Authentication  
Shaoquan Jiang and Guang Gong  

14:25–14:50  Product Construction of Key Distribution Schemes for Sensor Networks  
Reizhong Wei and Jiang Wu  

14:50–15:15  Deterministic Key Predistribution Schemes for Distributed Sensor Networks  
Jooyoung Lee and Douglas R. Stinson  

Svetla Nikova and Ventzislav Nikov  

15:40–16:10  Coffee break  

Session 8: Secret Key Cryptography II  

16:10–16:35  Efficient Constructions of Variable-Input-Length Block Ciphers  
Sarvar Patel, Zulfikar Ramzan and Ganesh Sundaram  

16:35–17:00  Optimal Domain Extension of UOWHF and a Sufficient Condition  
Mridul Nandi