SAC 2015 Program *(revised 2015-08-11)*

All talks will take place in Crabtree Auditorium (M14). Crabtree is Building 4 on the campus map.

WEDNESDAY, AUGUST 12

14:00 – 14:10 ● Opening Remarks

14:10 – 15:25 ● Session #1: Privacy Enhancing Technologies (Chair: Carlisle Adams)

Formal Treatment of Privacy-Enhancing Credential Systems
- Jan Camenisch (IBM Research – Zurich, Switzerland)
- Stephan Krenn (Austrian Institute of Technology, Austria)
- Anja Lehmann (IBM Research – Zurich, Switzerland)
- Gert Læssøe Mikkelsen (Alexandra Institute, Denmark)
- Gregory Neven (IBM Research – Zurich, Switzerland)
- Michael Østergaard Pedersen (Miracle A/S, Denmark)

Minimizing the Number of Bootstrappings in Fully Homomorphic Encryption
- Marie Paindavoine (Université Claude Bernard Lyon 1, LIP, France)
- Bastien Vialla (Université Montpellier, LIRMM, France)

Privacy-Preserving Fingerprint Authentication Resistant to Hill-Climbing Attacks
- Haruna Higo (NEC Corporation, Japan)
- Toshiyuki Isshiki (NEC Corporation)
- Kengo Mori (NEC Corporation)
- Satoshi Obana (Hosei University)

15:25 – 15:45 ● Coffee Break

15:45 – 17:25 ● Session #2: Cryptanalysis of Symmetric-Key Primitives (Chair: Christian Rechberger)

Practical Cryptanalysis of Full Sprout with TMD Tradeoff Attacks
- Muhammed F. Esgin (TÜBİTAK BİLGEM UEKAE, Turkey)
- Orhun Kara (TÜBİTAK BİLGEM UEKAE, Turkey)

Related-Key Attack on Full-Round PICARO
- Anne Canteaut (Inria, France)
- Virginie Lallemand (Inria, France)
- María Naya-Plasencia (Inria, France)

Cryptanalysis of Feistel Networks with Secret Round Functions
- Alex Biryukov (University of Luxembourg, Luxembourg)
- Gaëtan Leurent (Inria, France)
- Léo Perrin (SnT and University of Luxembourg, Luxembourg)

Improved Meet-in-the-Middle Distinguisher on Feistel Schemes
- Li Lin (Chinese Academy of Sciences, China)
- Wenling Wu (Chinese Academy of Sciences, China)
- Yafei Zheng (Chinese Academy of Sciences, China)

18:30 – 21:00 ● Welcome Reception
Foyer of Purdy Crawford Centre for the Arts (Building 22 on campus map)

THURSDAY, AUGUST 13

9:00 – 10:15 ● Session #3: Implementation of Cryptographic Schemes (Chair: Howard Heys)

Sandy2x: New Curve25519 Speed Records
- Tung Chou (Technische Universiteit Eindhoven, The Netherlands)

ECC on Your Fingertips: A Single Instruction Approach for Lightweight ECC Design in GF(p)
- Debapriya Basu Roy (Indian Institute of Technology Kharagpur, India)
- Poulami Das (Indian Institute of Technology Kharagpur, India)
- Debdeep Mukhopadhyay (Indian Institute of Technology Kharagpur, India)

Exploring Energy Efficiency of Lightweight Block Ciphers
- Subhadeep Banik (Technical University of Denmark, Denmark)
- Andrey Bogdanov (Technical University of Denmark, Denmark)
- Francesco Regazzoni (University of Lugano, Italy)

10:15 – 10:35 ● Coffee Break

10:35 – 11:20 ● Session #4: Short Papers Session (Chair: Kaisa Nyberg)

Forgery and Subkey Recovery on CAESAR Candidate iFeed
- Willem Schroé (KU Leuven, Belgium)
- Bart Mennink (KU Leuven, Belgium)
- Elena Andreeva (KU Leuven, Belgium)
- Bart Preneel (KU Leuven, Belgium)

Key-Recovery Attacks against the MAC Algorithm Chaskey
- Chrysanthi Mavromati (Capgemini Sogeti, R&D Lab, France and Université de Versailles Saint-Quentin-en-Yvelines, France)

Differential Forgery Attack against LAC
- Gaëtan Leurent (Inria, France)

11:25 – 12:25 ● Stafford Tavares Lecture
Paul Syverson – "Trust Aware Traffic Security"

12:25 – 14:00 ● Lunch (Jennings Dining Hall, Building 25 on campus map)
NOTE: SAC Board meeting starts in upstairs meeting room in Jennings Hall at 12:50pm

14:00 – 14:50 ● Session #5: Privacy Preserving Data Processing (Chair: Mike Jacobson)

Private Information Retrieval with Preprocessing Based on the Approximate GCD Problem
- Thomas Vannet (The University of Tokyo, Japan)
- Noboru Kunihiro (The University of Tokyo, Japan)

Dynamic Searchable Symmetric Encryption with Minimal Leakage and Efficient Updates on Commodity Hardware
- Attila A. Yavuz (Oregon State University, USA)
- Jorge Guajardo Merchan (Robert Bosch LLC – RTC, USA)

14:50 – 15:10 ● Coffee Break

15:10 – 16:50 ● Session #6: Side Channel Attacks and Defenses (Chair: Howard Heys)

Affine Equivalence and its Application to Tightening Threshold Implementations
- Pascal Sasdrich (Ruhr-Universität Bochum, Germany)
- Amir Moradi (Ruhr-Universität Bochum, Germany)
- Tim Güneysu (Ruhr-Universität Bochum, Germany)

Near Collision Side Channel Attacks
- Baris Ege (Radboud University, Nijmegen, The Netherlands)
- Thomas Eisenbarth (Worcester Polytechnic Institute, USA)
- Lejla Batina (Radboud University, Nijmegen, The Netherlands)

Masking Large Keys in Hardware: A Masked Implementation of McEliece
- Cong Chen (Worcester Polytechnic Institute, USA)
- Thomas Eisenbarth (Worcester Polytechnic Institute, USA)
- Ingo von Maurich (Ruhr-Universität Bochum, Germany)
- Rainer Steinwandt (Florida Atlantic University, USA)

Fast and Memory-Efficient Key Recovery in Side-Channel Attacks
- Andrey Bogdanov (Technical University of Denmark, Denmark)
- Ilya Kizhvatov (Riscure, The Netherlands)
- Kamran Manzoor (Technical University of Denmark, Denmark and Riscure, The Netherlands)
- Elmar Tischhauser (Technical University of Denmark, Denmark)
- Marc Witteman (Riscure, The Netherlands)

Conference Dinner (Captain Dan's Seafood Patio Bar, 50 Pointe Du Chêne Road, Shediac)

18:00 ● Buses arrive in "The Loop" (between Buildings 19 and 17 on the campus map)

18:15 ● Buses depart

19:00 ● Arrival at Captain Dan's Restaurant

19:00 – 19:30 ● Drinks

19:30 – 21:30 ● Dinner

21:45 (approximate) ● Buses depart to return to Mount Allison University

FRIDAY, AUGUST 14

9:00 – 10:15 ● Session #7: New Cryptographic Constructions (Chair: Petr Lisonek)

Efficient One-Time Signatures
- Kassem Kalach (University of Waterloo, Canada)
- Reihaneh Safavi-Naini (University of Calgary, Canada)

Constructing Lightweight Optimal Diffusion Primitives with Feistel Structure
- Zhiyuan Guo (Chinese Academy of Sciences, China)
- Wenling Wu (Chinese Academy of Sciences, China)
- Si Gao (Chinese Academy of Sciences, China)

Construction of Lightweight S-Boxes using Feistel and MISTY Structures
- Anne Canteaut (Inria, France)
- Sébastien Duval (Inria, France)
- Gaëtan Leurent (Inria, France)

10:15 – 10:35 ● Coffee Break

10:35 – 11:25 ● Session #8: Authenticated Encryption (Chair: Kaisa Nyberg)

A New Mode of Operation for Incremental Authenticated Encryption with Associated Data
- Yu Sasaki (NTT Secure Platform Laboratories, Japan)
- Kan Yasuda (NTT Secure Platform Laboratories, Japan)

SCOPE: On the Side Channel Vulnerability of Releasing Unverified Plaintexts
- Dhiman Saha (Indian Institute of Technology Kharagpur, India)
- Dipanwita Roy Chowdhury (Indian Institute of Technology Kharagpur, India)

11:25 – 12:25 ● Invited Talk
Gaëtan Leurent – "Generic Attacks against MAC Algorithms"

12:25 – 14:00 ● Lunch (Jennings Dining Hall, Building 25 on campus map)

14:00 – 14:50 ● Session #9: On the Hardness of Mathematical Problems (Chair: Mike Jacobson)

Bit Security of the CDH Problems over Finite Fields
- Mingqiang Wang (Shandong University, China),
- Tao Zhan (Shandong University, China),
- Haibin Zhang (University of North Carolina, Chapel Hill, USA)

Towards Optimal Bounds for Implicit Factorization Problem
- Yao Lu (State Key Laboratory of Information Security, China and The University of Tokyo, Japan)
- Liqiang Peng (State Key Laboratory of Information Security, China)
- Rui Zhang (State Key Laboratory of Information Security, China)
- Lei Hu (State Key Laboratory of Information Security, China)
- Dongdai Lin (State Key Laboratory of Information Security, China)

14:50 – 15:10 ● Coffee Break

15:10 – 16:25 ● Session #10: Cryptanalysis of Authenticated Encryption Schemes
(Chair: Gaëtan Leurent)

Forgery Attacks on round-reduced ICEPOLE-128
- Christoph Dobraunig (IAIK, Graz University of Technology, Austria)
- Maria Eichlseder (IAIK, Graz University of Technology, Austria)
- Florian Mendel (IAIK, Graz University of Technology, Austria)

Analysis of the CAESAR Candidate Silver
- Jérémy Jean (Nanyang Technological University, Singapore)
- Yu Sasaki (NTT Secure Platform Laboratories, Tokyo, Japan and Nanyang Technological University, Singapore)
- Lei Wang (Shanghai Jiao Tong University, China and Nanyang Technological University, Singapore)

Differential-Linear Cryptanalysis of COFFE
- Ivan Tjuawinata (Nanyang Technological University, Singapore)
- Tao Huang (Nanyang Technological University, Singapore)
- Hongjun Wu (Nanyang Technological University, Singapore)

16:25 – 16:30 ● Concluding Remarks