SAC 2018 Program

all talks will take place in the University of Calgary, ICT Building, room 121

UNIVERSITY OF CALGARY

Tuesday, 14 Aug 2018

18:00 – 20:00: **SAC 2018 Welcome Reception & Registration**
(Senate Room, Hotel Alma, 7th floor)

Wednesday, 15 Aug 2018

08:30 – 09:20: **Registration** (ICT Building, room 114)

09:20 – 09:30: **Opening Remarks**

09:30 – 10:20: **Session 1: Side Channel Attacks I**

Sliding-Window Correlation Attacks Against Encryption Devices with an Unstable Clock
Dor Fledel and Avishai Wool

Cache-Attacks on the ARM TrustZone implementations of AES-256 and AES-256-GCM via GPU-based analysis
Ben Lapid and Avishai Wool

10:20 – 10:40: **coffee break** (ICT Building, room 114)

10:40 – 11:30: **Session 2: Post-Quantum Cryptography I**

EFLASH: A New Multivariate Encryption Scheme
Ryann Cartor and Daniel Smith-Tone

Provably secure NTRUEncrypt over any cyclotomic field
Yang Wang and Mingqiang Wang

11:30 – 11:40: **break**

11:40 – 12:30: **SAC 2018 Stafford Tavares Lecture**

Machine Learning in Security: Applications and Implications
Adi Shamir (Weizmann Institute of Science, Israel)

12:30 – 14:00: **LUNCH**

14:00 – 15:15: **Session 3: Cryptanalysis of Symmetric Key Primitives I**

Integral Attacks on Round-Reduced Bel-T-256
Muhammad Elsheikh, Mohamed Tolba and Amr Youssef

Cryptanalysis of Reduced sLiSCP Permutation in Sponge-Hash and Duplex-AE Modes
Yunwen Liu, Yu Sasaki, Ling Song and Gaoli Wang

Finding Integral Distinguishers with Ease
Zahra Eskandari, Andreas Brasen Kidmose, Stefan Kölbl and Tyge Tiessen

15:15 – 15:35: **coffee break** (ICT Building, room 114)

15:35 – 16:25: **Session 4: Classical Public Key Cryptography**

A Generalized Attack on Some Variants of the RSA Cryptosystem
Abderrahmane Nitaj, Yanbin Pan and Joseph Tonien

Injective Encodings to Binary Ordinary Elliptic curves
Reza Rezaeian Farashahi, Mojtaba Fadavi and Soheila Sabbaghian

Thursday, 16 Aug 2018

09:10 – 10:00: **Session 5: Lattice-based Cryptography**

A Full RNS Variant of Approximate Homomorphic Encryption
Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim and Yongsoo Song

Analysis of Error-Correcting Codes for Lattice-Based Key Exchange
Tim Fritzmann, Thomas Pöppelmann and Johanna Sepulveda

10:00 – 10:20: **coffee break** (ICT Building, room 114)

10:20 – 11:10: **Session 6: Machine Learning and Cryptography**

Unsupervised Machine Learning on Encrypted Data
Angela Jäschke and Frederik Armknecht

Profiled Power Analysis Attacks using Convolutional Neural Networks with Domain Knowledge
Benjamin Hettwer, Stefan Gehrer and Tim Güneysu

11:10 – 11:20: **break**

11:20 – 12:10: **SAC 2018 Invited Talk I**

SAC^{25}: A Retrospective – Carlisle Adams (University of Ottawa)

12:10 – 13:00: **bag lunch, short break before afternoon tour**

13:00 – 23:00: **SAC 2018 Social Event: Tour and Banquet at Lake Louise**

In the afternoon of the second day, SAC 2018 participants will be taken on a tour to Lake Louise in Banff National Park in the Canadian Rockies. Pick up at Hotel Alma will be at 1pm, with arrival at Lake Louise expected for 3.15pm. Participants will have two hours to explore the area, and we will convene at 5.15pm at the Chateau Lake Louise for pre-dinner drinks, with the banquet starting at 6pm. The evening will also feature a brief talk by Prof Stafford Tavares, in commemoration of the 25th anniversary of the SAC conference. The bus will leave back to Calgary at 8.45pm, arriving at Hotel Alma at 10.45pm and Motel Village (Holiday Inn Express and Suites) at 11.00pm.

Friday, 17 Aug 2018

09:10 – 10:00: **Session 7: Side Channel and Fault Attacks II**

Assessing the Feasibility of Single Trace Power Analysis of Frodo

Joppe Bos, Simon Friedberger, Marco Martinoli, Martijn Stam, Elisabeth Oswald

Fault Attacks on Nonce-based Authenticated Encryption: Application to Keyak and Ketje

Christoph Dobraunig, Stefan Mangard, Florian Mendel and Robert Primas

10:00 – 10:15: **coffee break** (ICT Building, room 114)

10:15 – 11:30: **Session 8: Design of Symmetric Key Primitives**

Targeted Ciphers for Format Preserving Encryption

Sarah Miracle and Scott Yilek

Variants of the AES Key Schedule for Better Truncated Differential Bounds

Patrick Derbez, Pierre-Alain Fouque, Jérémy Jean and Baptiste Lambin

Analysis and Improvement of an Authentication Scheme in Incremental Cryptography

Louiza Khati and Damien Vergnaud

11:30 – 11:40: **break**

11:40 – 12:30: **SAC 2018 Invited Talk II**

Whitebox Cryptography – Andrey Bogdanov (DTU, Denmark)

12:30 – 14:00: **LUNCH**

14:00 – 14:50: **Session 9: Post-Quantum Cryptography II**

Public Key Compression for Constrained Linear Signature Schemes

Ward Beullens, Alan Szepieniec and Bart Preneel

On the cost of computing isogenies between supersingular elliptic curves

Gora Adj, Daniel Cervantes-Vázquez, Jesús-Javier Chi-Domínguez, Alfred Menezes and Francisco Rodríguez-Henríquez

14:50 – 15:10: **coffee break** (ICT Building, room 114)

15:10 – 16:00: **Session 10: Cryptanalysis of Symmetric Key Primitives II**

Mind the Gap - A closer look at the Security of Block Ciphers against Differential Cryptanalysis

Ralph Ankele and Stefan Kölbl

Towards Key-Dependent Integral and Impossible Differential Distinguishers on AES

Kai Hu, Tingting Cui, Chao Gao and Meiqin Wang

16:00: **SAC 2018 Conference Closing**