SAC Summer School (S3) Program

All sessions will take place in room DMS 1110 in the Desmarais Building

Monday, August 14, 2017

08:30 – 09:10 **Registration** (in the main floor lobby of the Desmarais Building)

09:10 – 09:15 **Opening Remarks**

Full-day session: Introduction to Post-Quantum Cryptography
Michele Mosca, Douglas Stebila, David Jao

09:15 - 10:30 Post-Quantum Cryptography Session 1

10:30 - 11:00 **Coffee/Nutrition Break**

11:00 - 12:15 Post-Quantum Cryptography Session 2

12:15 - 13:45 **Lunch** (various options on campus and at nearby downtown locations)

13:45 - 15:00 Post-Quantum Cryptography Session 3

15:00 - 15:30 **Coffee/Nutrition Break**

15:30 - 16:45 Post-Quantum Cryptography Session 4

Tuesday, August 15, 2017

Half-day session: Introduction to Public Key Cryptography
Tanja Lange, Daniel J. Bernstein

09:15 - 10:30 Public Key Cryptography Session 1

10:30 - 11:00 **Coffee/Nutrition Break**

11:00 - 12:15 Public Key Cryptography Session 2

12:15 - 13:45 **Lunch** (various options on campus and at nearby downtown locations)

Half-day session: Introduction to Symmetric Cryptography
Orr Dunkelman

13:45 - 15:00 Symmetric Cryptography Session 1

15:00 - 15:30 **Coffee/Nutrition Break**

15:30 - 16:45 Symmetric Cryptography Session 2

SAC Conference Program

All talks will take place in room DMS 1160 in the Desmarais Building

Tuesday, August 15, 2017

17:00 – 19:00 **Welcome Reception** (in the main floor lobby of the Desmarais Building)

Wednesday, August 16, 2017

08:30 – 09:20 **Registration** (in the main floor lobby of the Desmarais Building)

09:20 – 09:30 **Opening Remarks**

09:30 - 10:20 ***Discrete Logarithms*** (Chair: Doug Stinson)

Second Order Statistical Behavior of LLL and BKZ
Yang Yu and Léo Ducas

Refinement of the Four-Dimensional GLV Method on Elliptic Curves
Hairong Yi, Yuqing Zhu and Dongdai Lin

10:20 - 10:40 **Coffee/Nutrition Break**

10:40 - 11:30 ***Key Agreement*** (Chair: Doug Stinson)

Post-quantum static-static key agreement using multiple protocol instances
Reza Azarderakhsh, David Jao and Christopher Leonardi

Side-Channel Attacks on Quantum-Resistant Supersingular Isogeny Diffie-Hellman
Brian Koziel, Reza Azarderakhsh and David Jao

11:30 - 11:40 **Short Break**

11:40 - 12:30 **Invited Talk #1: Chris Peikert** (Chair: Orr Dunkelman)

12:30 - 14:00 **Lunch** (various options on campus and at nearby downtown locations)

14:00 - 14:50 ***Theory*** (Chair: Petr Lisonek)

Computing discrete logarithms over GF(p^6)
Laurent Grémy, Aurore Guillevic, François Morain and Emmanuel Thomé

Computing Low-Weight Discrete Logarithms
Bailey Kacsmar, Sarah Plosker and Ryan Henry

14:50 - 15:10 **Coffee/Nutrition Break**

15:10 - 16:00 ***Panel Session on Post-Quantum Cryptography:*** (Moderator: Tanja Lange)
Daniel J. Bernstein, David Jao, Michele Mosca, Chris Peikert

Thursday, August 17, 2017

09:30 - 10:20 ***Efficient Implementation I*** (Chair: Maryam Eneim)

sLiSCP: Simeck-based Permutations for Lightweight Sponge Cryptographic Primitives

Riham Altawy, Raghvendra Rohit, Morgan He, Kalikinkar Mandal, Gangqiang Yang and Guang Gong

Efficient reductions in cyclotomic rings - Application to Ring-LWE based FHE schemes

Jean-Claude Bajard, Julien Eynard, Anwar Hasan, Paulo Martins, Leonel Sousa and Vincent Zucca

10:20 - 10:40 **Coffee/Nutrition Break**

10:40 - 11:30 ***Efficient Implementation II*** (Chair: Maryam Eneim)

How to (pre-)compute a ladder

Thomaz Oliveira, Julio López, Hüseyin Hisil, Armando Faz-Hernandez and Francisco Rodríguez-Henríquez

HILA5: On Reliability, Reconciliation, and Error Correction for Ring-LWE Encryption

Markku-Juhani Olavi Saarinen

11:30 - 13:00 **Lunch** (various options on campus and at nearby downtown locations)

13:00 - 13:50 ***Public Key Encryption*** (Chair: Mike Jacobson)

A Public-key Encryption Scheme based on Non-linear Indeterminate Equations

Koichiro Akiyama, Yasuhiro Goto, Shinya Okumura, Tsuyoshi Takagi, Koji Nuida and Goichiro Hanaoka

NTRU Prime: Reducing Attack Surface at Low Cost

Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange and Christine van Vredendaal

13:50 - 14:10 **Coffee/Nutrition Break**

14:10 - 15:25 ***Signatures*** (Chair: Mike Jacobson)

Leighton-Micali Hash-Based Signatures in the Quantum Random-Oracle Model

Edward Eaton

Efficient Post-Quantum Undeniable Signature on 64-bit ARM

Amir Jalali, Reza Azarderakhsh and Mehran Mozaffari-Kermani

"Oops, I did it again'' -- Security of One-Time Signatures under Two-Message Attacks

Leon Groot Bruinderink and Andreas Huelsing

15:25 - 16:30 **Break to get ready for the evening**

16:30 - 23:00 **Social Event and Banquet** (Canadian Museum of History and Ottawa River Boat Cruise)
The first bus will leave Desmarais at 16:30 for those that wish to visit the Canadian Museum of History from 17:00 – 18:30; it will then continue on to the boat dock at 799 rue Jacques Cartier in Gatineau.
The second bus will leave Desmarais at 18:15 for those that choose to omit the Museum and go straight to the boat dock.
All banquet attendees must be at the dock by 18:45 – the boat will leave at 19:00 sharp. The cruise will end at the same dock at 23:00; two buses will then take all attendees back to the Desmarais Building.

Friday, August 18, 2017

09:30 - 10:20 ***Cryptanalysis I*** (Chair: Miguel Vargas Martin)

Low-communication parallel quantum multi-target preimage search
Gustavo Banegas and Daniel J. Bernstein

Lattice Klepto - Turning Post-Quantum Crypto Against Itself
Robin Kwant, Tanja Lange and Kimberley Thissen

10:20 - 10:40 **Coffee/Nutrition Break**

10:40 - 11:30 ***Cryptanalysis II*** (Chair: Miguel Vargas Martin)

Total Break of the SRP Encryption Scheme
Ray Perlner, Albrecht Petzoldt and Daniel Smith-Tone

Approximate short vectors in ideal lattices of Q(zeta_{p^e}) with precomputation of the class group
Jean-Francois Biasse

11:30 - 11:40 **Short Break**

11:40 - 12:30 **Invited Talk #2 (Stafford Tavares Lecture): Helena Handschuh** (Chair: Bart Preneel)

12:30 - 14:00 **Lunch** (various options on campus and at nearby downtown locations)

14:00 - 14:50 ***Cryptanalysis III*** (Chair: Stefan Treatman-Clark)

Quantum Key-Recovery on full AEZ
Xavier Bonnetain

Quantum Key Search with Side Channel Advice
Daniel P. Martin, Ashley Montanaro, Elisabeth Oswald and Dan Shepherd

14:50 - 15:10 **Coffee/Nutrition Break**

15:10 - 16:00 ***Cryptanalysis IV*** (Chair: Stefan Treatman-Clark)

Multidimensional Zero-Correlation Linear Cryptanalysis of Reduced Round SPARX-128
Mohamed Tolba, Ahmed Abdelkhalek and Amr Youssef

Categorising and Comparing Cluster-Based DPA Distinguishers
Xinping Zhou, Carolyn Whitnall, Elisabeth Oswald, Degang Sun and Zhu Wang