University of Windsor

SAC2022

SAC2022 Main Program

(All talks/breaks/lunch/reception will take place in Room 1100)

Wednesday, 24 August 2022

08:20-08:50 **Registration**
08:50-09:00 **Opening Remarks (Dr. van Heyst)**
09:00-10:00 *Invited Talk: On the passive compromise of TLS keys and other cryptanalytic adventures*
Nadia Heninger
10:00-10:30 **Coffee Break**
10:30-12:00 **Presentations: Lattices and ECC**

6097: Profiling Side-Channel Attacks on Dilithium: A Small Bit-Fiddling Leak Breaks It All
Vincent Ulitzsch, Soundes Marzougui, Mehdi Tibouchi and Jean-Pierre Seifert
6639: On the Weakness of Ring-LWE mod Prime ideal q by Trace Map (on Zoom)
Tomoka Takahashi, Shinya Okumura and Atsuko Miyaji
1096: 2D-GLS: Faster and exception-free scalar multiplication in the GLS254 binary curve
Marius A. Aardal and Diego F. Aranha

12:00-14:00 **Lunch Break**
14:00-15:30 **Presentations: Differential Cryptanalysis**

0332: Key-Recovery Attacks on CRAFT and WARP (on Zoom)
Ling Sun, Wei Wang and Meiqin Wang
0902: Differential analysis of the ternary hash function Troika
Christina Boura, Margot Funk and Yann Rotella
1990: Another Look at Differential-Linear Attacks
Orr Dunkelman and Ariel Weizman

15:30-16:00 **Coffee Break**
16:00-17:30 **Presentations: Cryptographic Primitives**

4437: Rank Metric Trapdoor Functions with Homogeneous Errors (on Zoom)
Etienne Burle, Philippe Gaborit, Younes Hatri and Ayoub Otmani
6751: PERKS: Persistent and Distributed Key Acquisition for Secure Storage from Passwords
Gareth T. Davies and Jeroen Pijnenburg
2411: Improved Circuit-based PSI via Equality Preserving (on Zoom)
Kyoohyung Han, Dukjae Moon and Yongha Son

17:30-18:30 **Reception**

University of Windsor

SAC2022

SAC2022 Main Program

(All talks, breaks, and lunch will take place in Room 1100)

Thursday, 25 August 2022

09:00-10:00 *Invited Talk: Hard problems for isogeny-based cryptography*
Benjamin Wesolowski

10:00-10:30 **Coffee Break**

10:30-12:00 **Presentations: Isogeny-based cryptography I**

1117: Revisiting Meet-in-the-Middle Cryptanalysis of SIDH/SIKE with Application to the $IKEp182 Challenge
Aleksei Udovenko and Giuseppe Vitto

7227: Patient Zero: Zero-Value Attacks on CSIDH and Variants
Fabio Campos, Michael Meyer, Krijn Reijnders and Marc Stöttinger

2904: An Effective Lower Bound on the Number of Orientable Supersingular Elliptic Curves (on Zoom)
Antonin Leroux

12:00-14:00 **Lunch Break**

14:00-15:30 **Presentations: Block ciphers**

4344: Finding All Impossible Differentials When Considering the DDT (on Zoom)
Kai Hu, Thomas Peyrin and Meiqin Wang

6039: A Three-Stage MITM Attack on LowMC from a Single Plaintext-Ciphertext Pair (on Zoom)
Lulu Zhang, Meicheng Liu and Dongdai Lin

9983: Collision-Based Attacks on White-Box AES Implementations (on Zoom)
Jiqiang Lu, Mingxue Wang, Can Wang and Chen Yang

15:30-16:00 **Coffee Break**

16:00-17:00 **Presentations: Differential cryptanalysis II**

6955: Advancing the Meet-in-the-Filter Technique: Applications to CHAM and KATAN
Alex Biryukov, Je Sen Teh and Aleksei Udovenko

9181: Improving the Automated Evaluation Algorithm against Differential Attacks and Application to WARP (on Zoom)
Jiali Shi, Guoqiang Liu and Chao Li

17:00-18:00 **lightning talks, announcements, job ads, etc**

18:00-21:00 **Banquet at University Club**

University of Windsor

SAC2022

SAC2022 Main Program

(All talks, break and lunch will take place in Room 1100)

Friday, 26 August 2022

09:00-10:00 *Invited Talk: Efficient key recovery attacks on SIDH*
Wouter Castryck

10:00-10:30 **Coffee Break**

10:30-11:00 **Presentation: Isogeny-based cryptography II**

6663: Faster Cryptographic Hash Function from Supersingular Isogeny Graphs
Javad Doliskani, Geovandro Pereira and Paulo Barreto

11:00-12:30 **Presentations: Protocols and PRFs**

0945: From Plaintext-extractability to IND-CCA Security (on Zoom)
Ehsan Ebrahimi

6175: Farasha: A Provable Permutation-based Parallelizable PRF
Ravindra Jejurikar, Najwa Aaraj, Marc Manzano, Raghvendra Rohit, Emanuele Bellini, Santos Merino del Pozo and Eugenio Salazar

6527: A Sponge-Based PRF with Good Multi-user Security (on Zoom)
Arghya Bhattacharjee, Ritam Bhaumik and Mridul Nandi

12:30- **Lunch and Goodbye**