ARCTICCRYPT 2025

Program Schedule

Monday, 7 July 2025 | 8:50 to 17:00
Radisson Blu Polar Hotel

8:50 - 9:00:

Opening remarks by Håvard Raddum, Simula UiB

9:00 - 10:30: CRYPTANALYSIS I

- **Black-box Collision Attacks on the NeuralHash Perceptual Hash Function** by Diane Leblanc-Albarel (KU Leuven), Bart Preneel (KU Leuven)
- **Solving Multivariate Coppersmith Problems with Known Moduli** by Keegan Ryan (University of California, San Diego)
- **An Improved Algorithm for Code Equivalence** by Julian Nowakowski (Ruhr University Bochum)

10:30 - 11:00: BREAK

11:00 - 12:00: MPC I

- **Communication-Efficient Multi-Party Computation for RMS Programs** by Pedro Capitão (CWI; Leiden University), Aron van Baarsen (Aarhus University; Leiden University), Vincent Dunning (TNO), Thomas Attema (TNO; CWI), Lisa Kohl (CWI Amsterdam), Stefan van den Berg (TNO)
- **Non-Interactive Distributed Point Functions** by Elette Boyle (NTT), Lalita Devadas (MIT), Sacha Servan-Schreiber (MIT)

12:00 - 13:30: LUNCH BREAK

13:30 - 14:30: DIGITAL SIGNATURES

- **Ring Verifiable Random Functions** by Jeffrey Burdges (Web3 Foundation), Oana Ciobotaru (OpenZeppelin), Elizabeth Crites (Web3 Foundation), Handan Kılınç Alper (Nil Foundation), Alistair Stewart (Web3 Foundation), Sergey Vasilyev (Web3 Foundation)
- **Unforgeability of Blind Schnorr in the Limited Concurrency Setting** by Franklin Harding (Brown University), Jiayu Xu (Oregon State University)

14:30 - 15:00: BREAK

15:00 - 17:00: ISOGENY-BASED CRYPTOGRAPHY

- **Simple Two-Message OT in the Explicit Isogeny Model** by Riccardo Zanotto (CISPA), Emmanuela Orsini (Università Bocconi)
- **More Efficient Isogeny Proofs of Knowledge via Canonical Modular Polynomials** by Thomas den Hollander, Sören Kleine, Marzio Mula, Daniel Slamanig, Sebastian A. Spindler (All from Universität der Bundeswehr München)
- **Finding Practical Parameters for Isogeny-based Cryptography** by Maria Corte-Real Santos (University College London), Jonathan Komada Eriksen (COSIC, KU Leuven), Michael Meyer (University of Regensburg), Francisco Rodríguez-Henríquez (Cryptography Research Center, Technology Innovation Institute)
- **Computing Orientations from the Endomorphism Ring of Supersingular Curves and Applications** by Jonathan Komada Eriksen (COSIC, KU Leuven), Antonin Leroux (DGA-MI and Université de Rennes)

BREAK UNTIL MIDNIGHT SESSIONS

23:00: ALLISON BISHOP: FINDING CRYPTOGRAPHY PROBLEMS OUTSIDE OF CRYPTOGRAPHY

00:00: KENNY PATERSON: LIVING IN A PARALLEL UNIVERSE: THE QUANTUM INTERNET AND QUANTUM KEY DISTRIBUTION

Tuesday, 8 July 2025 | 10:00 to 17:30
Radisson Blu Polar Hotel

10:00 - 11:30:
ADVANCED PROTOCOLS AND PUBLIC KEY PRIMITIVES I

- **Reinventing BrED: A Practical Construction Formal Treatment of Broadcast Encryption with Dealership** by Avishek Majumder (UPES, Dehradun), Sayantan Mukherjee (IIT Jammu)
- **Towards Optimal Parallel Broadcast under a Dishonest Majority** by Daniel Collins (Purdue University and Georgia Tech), Sisi Duan (Tsinghua University), Julian Loss (CISPA Helmholtz Center for Information Security), Charalampos Papamanthou (Yale University), Giorgos Tsimos (University of Maryland, College Park), Haochen Wang (Tsinghua University)
- **Simple Watermarking Pseudorandom Functions from Extractable Pseudorandom Generators** by Estuardo Alpirez Bock (Independent), Chris Brzuska (Aalto University), Russell W. F. Lai (Aalto University)

11:30 - 12:00: BREAK

12:00 - 13:00: SYMMETRIC DESIGN AND ANALYSIS

- **Efficient Algorithm for Generating Optimal Inequality Candidates for MILP Modeling of Boolean Functions** by Alexander Bille (University of Marburg), Elmar Tischhauser (University of Marburg)
- **Sonikku: Gotta Speed, Keed! A Family of Fast and Secure MACs** by Amit Singh Bhati (COSIC, KU Leuven), Elena Andreeva (TU Wien), Simon Müller (TU Wien), Damian Vizár (Swiss Center for Electronics and Microtechnology (CSEM))

13:00 - 14:30: LUNCH BREAK

14:30 - 15:30: MPC II

- **Efficient Maliciously Secure Oblivious Exponentiations** by Carsten Baum (DTU), Jens Berlips (SecureDNA Foundation), Walther Chen (SecureDNA Foundation), et.al.
- **Highly-Efficient Fully Secure MPC in the Two-Thirds Honest Majority Setting** by Matan Hamilis (Reichman University), Ariel Nof (Bar-Ilan University)

15:30 - 16:00: BREAK

16:00 - 17:30: ZERO KNOWLEDGE PROTOCOLS

- **Robust Combiners for Non-Interactive Zero-Knowledge Proofs** by Michele Ciampi (The University of Edinburgh), Lorenzo Magliocco (Sapienza University of Rome), Daniele Venturi (Sapienza University of Rome), Yu Xia (The University of Edinburgh)
- **Compact Proofs of Partial Knowledge for Overlapping CNF Formulae** by Gennaro Avitabile (IMDEA Software Institute) and Vincenzo Botta, Daniele Friolo, Daniele Venturi, Ivan Visconti (all from Sapienza University of Rome)
- **Lattice-Based Polynomial Commitments: Towards Asymptotic and Concrete Efficiency** by Giacomo Fenzi (EPFL), Hossein Moghaddas (NP Labs), Ngoc Khanh Nguyen (King's College London)

EXCURSION DAY

08:15: Pick up at the conference hotel

09:00: The Wildlife and Glacier Cruise starts

Lunch

Ca 14:30: Return to the harbour
(the precise timing is weather dependent)

Information about the trip

You will travel with the hybrid electric catamaran MS Bard. The engine and propellers are specially designed to minimise the noise and vibration. This not only takes you closer to nature; More importantly, the surrounding wildlife is less disturbed by our presence.

Early in the season, parts of Billefjorden may still be covered in ice. By the use of only the electric motor, we will then silently follow the ice edge where the opportunity to see wildlife is great! Here we will also enjoy the beautiful glacier front of Nordenskiöldbreen. In addition, we will see the ghost town Pyramiden from a distance and drive by Skansbukta, a bay with a lot of interesting history.

Photo by Annie Spratt

Thursday, 10 July 2025 | 9:30 to 17:00
Radisson Blu Polar Hotel

9:30 - 11:00:
MATHEMATICAL ASPECTS OF CRYPTOGRAPHY

- **How (not) to hash into class groups of imaginary quadratic fields?** by István András Seres, Péter Burcsi, Péter Kutas (All from Eötvös Loránd University)
- **Revisiting the Slot-to-Coefficient Transformation for BGV and BFV** by Robin Geelen (COSIC, KU Leuven)
- **Discrete gaussian sampling for BKZ-reduced basis** by Amaury Pouly (CNRS), Yixin Shen (INRIA)

11:00 - 11:30: BREAK

11:30 - 12:30: CRYPTANALYSIS II

- **Attacking trapdoors from matrix products** by Valerie Gilchrist (ULB - Université Libre de Bruxelles), Thomas Decru (ULB), Tako Boris Fouotsa (EPFL), Paul Frixons (ULB), Christophe Petit (ULB)
- **Analysis of Layered ROLLO-I: A BII-LRPC code-based KEM** by Seongtaek Chee (The Affiliated Institute of ETRI), Kyung Chul Jeong (The Affiliated Institute of ETRI), Tanja Lange (Eindhoven University of Technology and Academia Sinica), Nari Lee (The Affiliated Institute of ETRI), Alex Pellegrini (Eindhoven University of Technology), Hansol Ryu (The Affiliated Institute of ETRI)

12:30 - 13:00: BREAK
13:00 - 14:00: LUNCH

14:00 - 15:00:
REAL-WORLD PROTOCOLS AND IMPLEMENTATIONS

- **A Comprehensive Survey on Post-Quantum TLS** by Jan Oupický (University of Luxembourg), Nouri Alnahawi (Darmstadt University of Applied Sciences), Johannes Müller (CNRS/INRIA Nancy), Alexander Wiesmaier (Darmstadt University of Applied Sciences)
- **Efficient Boolean-to-Arithmetic Mask Conversion in Hardware** by Aein Shahmirzadi (PQShield), Michael Hutter (PQShield)

15:00 - 15:30: BREAK

15:30 - 17:00:
ADVANCED PROTOCOLS AND PUBLIC KEY PRIMITIVES II

- **Secure Offline Payments with Blockchain Access** by Mihai Christodorescu (Google), Sourav Das (UIUC), Ranjit Kumaresan (Visa Research), Mohsen Minaei (Visa Research), Mustafa Ozdayi (Qualtrics), Srinivasan Raghuraman (Visa Research and MIT), Muhammad Saad (X), Mahdi Zamani (Visa Research)
- **Lattice-based Multi-Authority/Client Attribute-based Encryption for Circuits** by Valerio Cini (NTT Research), Russell W. F. Lai (Aalto University), Ivy K. Y. Woo (Aalto University)
- **Registered Matchmaking Encryption** by Danilo Francati (Royal Holloway, University of London), Valeria Huang (Sapienza University of Rome), Daniele Venturi (Sapienza University of Rome)

BREAK UNTIL DINNER AT 19:00 AT HUSET

Friday, 10 July 2025

CHECK-OUT

Organised by

Simula UiB

Photo by Hans-Jurgen Mager

Photo by Annie Spratt

- HÅVARD RADDUM
- MARTHA NORBERG HOVD
- MORTEN ØYGARDEN
- IRATI MANTEROLA AYALA

Designed by Åsfrid Persson, Simula UiB