The Ernst Selmer International Workshop

21-27 August, 2022

Geirangerfjord, Norway

About

The Selmer Center was established in the honor of Prof. Ernst Sejersted Selmer on the foundation of the coding and cryptography group in 2003. The group currently conducts research in cryptology, coding theory, discrete mathematics and data security.

This international workshop is dedicated to the anniversary of Prof. Selmer. It was previously planned in 2020 for Selmer's 100th anniversary and postponed to this year due to COVID.

The Selmer Center organizes this workshop to bring together international collaborators and friends of the Selmer Center to celebrate Selmer's anniversary.

General Chairs

- Lilya Budaghyan (lilya.budaghyan@uib.no)

- Tor Helleseth (tor.helleseth@uib.no)

- Chunlei Li (chunlei.li@uib.no)

- Sondre Rønjom (Sondre.Ronjom@uib.no)

- Øyvind Ytrehus (oyvindy@simula.no)

Organizing Committee

- Ermes Franch (ermes.franch@uib.no, +47 91880689)

- Nadiia Ichanska (nadiia.ichanska@uib.no +47 41262589)

- Nikolay Kaleyski (nikolay.kaleyski@uib.no, +47 40562107)

- Erik Mårtensson (erik.martensson@uib.no, +46 768474340)

Timetable

In this workshop we will have scientific talks on Monday, Tuesday, Thursday, Friday, and have excursion on Wednesday, 24th of August.

Monday, 22nd of August

Time	Speaker	Title
09:00–09:05	**Welcome remarks by Lilya Budaghyan**	
09:05–10:05	**Tor Helleseth** Selmer Center	Some works and life Stories of Ernst Sejersted Selmer
10:05–10:50	**Øyvind Ytrehus** Simula-UiB and Selmer Center	Decoding on a very bad channel
10:50–11:15	**Coffee Break**	
11:15–12:00	**Sihem Mesnager** Univ. of Paris VIII, France	On an algebraic equation over finite fields and applications
12:00–12:25	**PhDs** Selmer Center	Self-Introductions
12:30–14:00	**Lunch**	
14:00–14:45	**Claude Carlet** Univ. of Paris VIII, France and Selmer Center	Some big open problems on Almost Perfect Nonlinear functions
14:45–15:30	**Christof Beierle** Ruhr University Bochum, Germany	ON APN Extensions
15:30–16:00	**Coffee Break**	
16:00–16:20	**Wrya K. Kadir** Simula-UiB	On decodable evaluation rank metric codes
16:20–17:05	**Chunming Rong** Univ. of Stavanger, Norway	Secure decentralized OpenIaC: the network is my computer
19:00–21:30	**Buffet Dinner at the Hotel Union Geiranger**	

Tuesday, 23nd of August

09:00–09:45	**Lilya Budaghyan** Selmer Center	The Selmer Center Nowadays
09:45–10:30	**Daniel Katz** California State University Northridge, USA	Rationality of four-valued Walsh spectra of power permutations
10:30–11:00	**Coffee Break**	
11:00–11:45	**Constanza Riera** Western Norway Univ. of Applied Science, Norway	Differential and c-differential spectrum
11:45–12:05	**Diana Davidova** Yerevan State University, Armenia	Generalizations of bent functions
12:05–12:25	**Mohit Pal** Selmer Center	Some classes of (almost) perfect c-nonlinear permutations
12:30–14:00	**Lunch**	
14:00–14:45	**Léo Perrin** INRIA, France	On some TU-decomposition generalizations: more branches, and prime fields
14:45–15:30	**Anne Canteaut** INRIA, France	Integral attacks on some arithmetization-friendly primitives
15:30–16:00	**Coffee Break**	
16:00–16:20	**George Petrides**	On decompositions of permutation polynomials into quadratic and cubic power permutations
16:20–17:05	**Pante Stănică** Naval Postgraduate School, USA	Differential properties and twists of cryptographic Boolean functions
19:00–21:30	**Buffet Dinner at the Hotel Union Geiranger**	

Wednesday, 24th of August

09:30 sharp	**Departure from the Hotel Union Geiranger**
9:30 - 12:30	**Personal guided bus tour** to the panoramic highlights as Flydalsjuvet, Dalsnibba and Ørnesvingen
12:30	**Drop at the Hole Hytter** A short mountain hike to the restaurant
13:00 – 14:20	**Lunch at the Westerås restaurant**
14:20-14:40	**A downhill walk to the bus**
14:40-15:00	**Driving to the Harbour**
15:00-16:30	**Exclusive Fjordsightseeing with a boat** 16 km along the whole Geirangerfjord, including the most famous waterfalls and fjordfarms
16:30-17:00	**Walking back to the Hotel Union Geiranger**
19:00–21:30	**Buffet Dinner at the Hotel Union Geiranger**

Thursday, 25th of August

09:00–09:45	**Vincent Rijmen** KU Leuven, Belgium and Selmer Center	Extending the zero-difference attack on AES by using related differences
09:45–10:30	**Christian Rechberger** Graz University of Technology, Austria	New symmetric crypto for new applications
10:30–11:00	**Coffee Break**	
11:00–11:25	**Svetla Nikova** KU Leuven, Belgium and Selmer Center	Fault analysis - overview and recent attacks
11:25–11:45	**Ventzislav Nikov** NXP Semiconductors, Belgium	Open problems in TI sharings
11:45–12:05	**Siemen Dhooghe** KU Leuven, Belgium	StaTI: Protecting against fault attacks using stable threshold implementations
12:05–12:25	**Enrico Piccione** Selmer Center	To be added
12:30–14:00	**Lunch**	
14:00–14:45	**Thomas Johansson** Lund University, Sweden	Attacks on the Firekite cipher
14:45–15:30	**Qian Guo** Lund University, Sweden	Side-channel-assisted key-recovery chosen-ciphertext attacks on several NIST PQC KEMs
15:30–16:00	**Coffee Break**	
16:00–16:20	**Erik Mårtensson** Selmer Center	Do not bound to a single position: near-optimal multi-positional mismatch attacks against Kyber and Saber
16:20–17:05	**Håvard Raddum** Simula-UiB	Trail search with CRHS Equations
19:00–21:30	**Banquet Dinner at the Hotel Union Geiranger**	

Friday, 26th of August

09:00–09:45	**Nikolay S. Kaleyski** Selmer Center	Representations of discrete functions
09:45–10:30	**Sartaj Hasan** Indian Institute of Technology, Jammu	Enumeration of some vectorial recursive sequences over finite fields
10:30–11:00	**Coffee Break**	
11:00–11:45	**Zilong Liu** Univ. of Essex, UK	Pairs of sequences: the known and the unknown
11:45–12:05	**Palash Sarkar** Selmer Center	Construction of complementary sequences using multivariate functions
12:30–14:00	**Lunch**	
14:00–14:45	**Oleksandr Kazymyrov** Western Norway Univ. of Applied Science, Norway	Data exfiltration and prevention techniques
14:40–15:30	**Eirik Rosnes** Simula-UiB	Straggler mitigation and privacy in decentralized learning
15:30–16:00	**Coffee Break**	
16:00–16:20	**Sachin Valera** NYU Abu, Dhabi	Quantum key distribution
16:20–17:05	**Chunlei Li** Selmer Center	Decoding of rank-metric codes
Closing remarks by Tor Helleseth		
19:00–21:30	**Buffet Dinner at the Hotel Union Geiranger**	