

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 Helleseeth (tor.helleseeth@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.



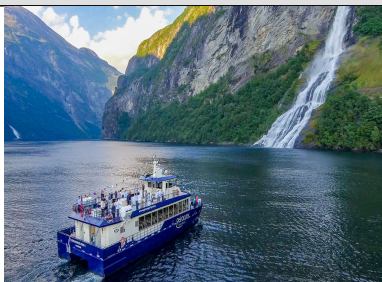
Monday, 22nd of August

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	Chunlei Li Selmer Center	Linear codes from nonlinear functions
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 Institute of Mathematics of NAS of RA	An equivalence relation as a method of secondary construction for Niho 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

08:45		Departure from the Hotel Union Geiranger	
08:45 - 12:00	Personal guided bus tour to the panoramic highlights as Flydalsjuvet, Dalsnibba and Ørnesvingen		
12:00	Drop at the Hole Hytter	A short mountain hike to the restaurant	
12:30 – 14:00	Lunch at the Westerås restaurant		
14:00-14:30	A downhill walk to the bus		
14:30-14:45	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
12:05–12:30	Sachin Valera NYU Abu, Dhabi	Quantum key distribution
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	Testing equivalence of uniformly distributed 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 Storebrand	Data exfiltration and prevention techniques
14:45–15:30	Eirik Rosnes Simula UiB	Straggler mitigation and privacy in decentralized learning
Closing remarks by Tor Helleseeth		
15:30–16:00	Coffee Break	
19:00–21:30	Buffet Dinner at the Hotel Union Geiranger	

List of Abstracts – Talks

Monday, August 22nd

Decoding on a very bad channel

Øyvind Ytrehus

Simula UiB and Selmer Center

The wiretap channel was introduced by Wyner in 1975 and has received a lot of attention from the information theoretic community, and some from coding theorists. In this talk we discuss and compare coding strategies, and analyze the possibilities for an eavesdropper with a very bad channel.

On decoding of rank-metric codes

Chunlei Li

Selmer Center

The construction of linear codes with optimal and good parameters has been an interesting and fruitful topic in the past decades. While it's generally challenging to determine the parameters, such as minimum distance, covering radius, weight enumerator, of a given linear code, it is possible to investigate the problem when the code is derived in some way from nonlinear functions with special properties, like optimal differential uniformity and few-value Walsh spectra. Consequently, researchers have proposed a great number of linear codes from nonlinear functions with desirable cryptographic properties, for which the parameters can be determined. In this talk, I will survey some important results that have stimulated researches on the topic and some of our contributions in this area.

Some big open problems on Almost Perfect Nonlinear functions

Claude Carlet

University of Paris VIII and Selmer Center

Almost perfect nonlinear (APN) functions are those functions F from the finite field of order 2^n to itself such that each equation $F(x) + F(x + a) = b$ (with a nonzero and b in the finite field) has at most two solutions (two being a minimum). These functions play an important role in symmetric cryptography and in coding theory. In this talk, we shall visit the main open questions on them. We shall recall what is known on general APN functions and show that this is too little for determining whether the known classes of APN functions can give a good picture of all APN functions or whether they are in fact peculiar. We shall also visit the open question whether their graphs, which are Sidon sets (an important notion in combinatorics), are all optimal, and relate this question to the existence of pairs of APN functions at Hamming distance 1 from each other.

On APN Extensions

Christof Beierle

Ruhr University Bochum

Let H be an APN function in dimension $n + 1$ that can be restricted to a linear hyperplane of dimension n and projected to an n dimensional linear space such that the resulting function G in dimension n is also APN. We call H an APN extension of G . In this talk, we present some recent results on APN extensions. At first, we explain how the 6,368 new quadratic APN functions in dimension eight from (C. Beierle, G. Leander, L. Perrin, Trims and extensions of quadratic APN functions, *Designs, Codes and Cryptography* (2022) 90:1009–1036) have been found as APN extensions of quadratic APN functions in dimension seven. We then discuss how quadratic APN functions with smallest possible nonlinearity are necessarily APN extensions and present some recent negative results on their existence. Finally, we present some open problems and ongoing work which aims at finding a secondary construction of APN functions by finding an infinite family of APN extensions.

On decodable evaluation rank metric codes

Wrya Kadir

Simula UiB

Gabidulin codes were introduced by Delsarte , Gabidulin and Roth, independently and they are the most well known family of rank metric codes. They are based on evaluation of linear maps on \mathbb{F}_q -linearly independent points in \mathbb{F}_{q^m} . Singleton-like bound is an upper bound on the size of rank metric codes and codes that achieve this bound, are called optimal rank metric codes. Optimal linear codes are important since for a fixed length n and dimension k , they have the greatest error correcting and detecting capabilities.

Decoding algorithms for optimal rank metric codes can be classified into syndrome-based and interpolation-based decoding algorithms. Syndrome-based decoding algorithm can be applied on codes that are linear over the main extension field \mathbb{F}_{q^m} and hence it has been applied on Gabidulin codes and generalized Gabidulin (GG) codes.

Interpolation-based decoding algorithms have been used to decode twisted Gabidulin (TG), generalized twisted Gabidulin (GTG), partition codes, additive generalized twisted Gabidulin (AGTG), alternating, symmetric and Hermitian codes. None of these codes are linear in general but interpolation-based decoding can be applied on \mathbb{F}_{q^m} -linear codes and also on codes that are linear over a subfield of \mathbb{F}_{q^m} .

In this talk we consider interpolation-based decoding algorithms for optimal rank metric codes. For this purpose we recall Berlekamp-Massey algorithm and also the properties of the Dickson matrix associated with linearized polynomials. We explain encoding and decoding procedures for different optimal rank metric codes and also the properties that are common between the decodable codes.

Secure Decentralized OpenIaC: the Network is my Computer

Chunming Rong

University of Stavanger

Modern information systems are built from a complex composition of networks, infrastructure, devices, services, and applications, interconnected by data flows that are often private and financially sensitive. The 5G networks, which can create hyperlocalized services, have highlighted many of the deficiencies of current practices in use today to create and operate information systems. Emerging cloud computing techniques, such as Infrastructure-as-Code (IaC) and elastic computing, offer a path for a future re-imagining of how we create, deploy, secure, operate, and retire information systems. In this paper, we articulate the position that a comprehensive new approach is needed for all OSI layers from layer 2 up to applications that are built on underlying principles that include reproducibility, continuous integration/continuous delivery, auditability, and versioning. There are obvious needs to redesign and optimize the protocols from the network layer to the application layer. Our vision seeks to augment existing Cloud Computing and Networking solutions with support for multiple cloud infrastructures and seamless integration of cloud-based microservices. To address these issues, we propose an approach named Open Infrastructure as Code (OpenIaC), which is an attempt to provide a common open forum to integrate and build on advances in cloud computing and blockchain to address the needs of modern information architectures. The main mission of our OpenIaC approach is to provide services based on the principles of Zero Trust Architecture (ZTA) among the federation of connected resources based on Decentralized Identity (DID). Our objectives include the creation of an open-source hub with fine-grained access control for an open and connected infrastructure of shared resources (sensing, storage, computing, 3D printing, etc.) managed by blockchains and federations. Our proposed approach has the potential to provide a path for developing new platforms, business models, and a modernized information ecosystem necessary for 5G networks.

Tuesday, August 23rd

Rationality of four-valued Walsh spectra of power permutations

Daniel Katz

California State University, Northridge

A power permutation over a finite field F is a function of the form $f(x) = x^d$ that permutes F . The Walsh spectrum measures the nonlinearity of f , which determines the resistance to linear cryptanalysis of protocols that employ f . The values in the Walsh spectrum are binomial Weil sums, which also determine the crosscorrelation spectrum of pairs of maximal linear sequences and the weight distribution of certain error-correcting codes. Since one sums roots of unity in the complex plane to obtain the Walsh spectrum values, these are always algebraic integers. When the characteristic of the underlying finite field F is 2 or 3, these will always be rational integers, but this is not always the case in higher characteristics. A rational Walsh spectrum is one whose values are all rational integers. A v -valued Walsh spectrum is one that has precisely v distinct values. If one sets aside degenerate cases, Helleseeth showed that all Walsh spectra of power permutations have at least three distinct values, and it has been shown that the three-valued spectra are always rational. In this talk, we show that four-valued Walsh spectra of power permutations are also always rational. This is joint work with Allison E. Wong.

Differential and c-differential spectrum

Constanza Riera

Western Norway University of Applied Science

This talk will be about the differential spectrum and some papers in the subject, as well as the difficulty of the determining the differential spectrum for most functions. We will also discuss the extension of this concept to c-derivatives.

An equivalence relation as a method of secondary construction for Niho bent functions

Diana Davidova

Institute of Mathematics of NAS of RA

In this talk we will discuss a more general equivalence relation than CCZ-equivalence, that is defined for a special class of bent functions. We will see that this more general equivalence relation produces inequivalent Niho bent functions from a given one.

On some TU-decomposition generalizations: more branches, and prime fields

Léo Perrin

INRIA

CCZ-equivalence is one of the most general form of equivalence between functions that preserve their linear and differential properties. It was one of the key ingredients of Dillon et al.'s discovery of the only APN permutation operating on an even number bits, but its practical use does not stop there. In this talk, I will present to recent results that crucially rely on CCZ-equivalence as well, and in particular on its underlying concepts of t-twist and TU-decompositions.

The first result was obtained with Beierle, Carlet, and Leander. While investigating a 9-bit quadratic APN permutation obtained in a previous work by Beierle and Leander, we were able to identify a 3-branch structure, effectively redefining the function over \mathbb{F}_8^3 . This allowed us to generalize it to higher dimension, and unfortunately played a key role in a 3rd party proof that they cannot be APN unless operating on exactly 9 bits. This raises the algorithmic question of the efficient recovery of such 3-branched TU-decomposition-like structures.

The second result is a new cryptographic permutation called Anemoi, which was co-designed with Bouvier, Briaud, Chaidos and Velichkov. It is intended for use in advanced protocols that require cryptographic hash functions operating on finite fields of large size q , q being often a prime number. Such hash functions are called arithmetization-oriented. The main insight behind our work is an unexpected relationship between arithmetization-orientation and CCZ-equivalence, which lead us to use a butterfly structure in our design when $q = 2^n$ (n odd), and to design a new family of permutations of \mathbb{F}_p^2 called "open Flystels" which are CCZ-equivalent to low degree functions (the closed Flystels) via a simple twist. While its differential properties are well understood, we could only conjecture its linear properties.

Integral attacks on some arithmetization-friendly primitives

Anne Canteaut

INRIA

Integral attacks, including higher-order differential attacks, exploit some properties of the algebraic normal form of some component of a (round-reduced) symmetric primitive, typically a low algebraic degree. More precisely, it makes use of the particular value taken by the sum of the images of the function over some well-chosen input set.

In this talk, we analyze the resistance against such integral attacks of some variants of MIMC. These primitives, named arithmetization-friendly primitives, are characterized by a round function with a very simple univariate polynomial representation over a very large finite field of size p or 2^m .

Most notably, we analyze the growth of the algebraic degree of MIMC over $GF(2^m)$ when the number of rounds increases. We also show how integral attacks can be mounted based on multiplicative subgroups of the field instead of linear subspaces in the usual case.

Some of these results have been obtained in joint works with Beyne, Bouvier, Dinur, Eichlseder, Leander, Leurent, Naya-Plasencia, Perrin, Sasaki and Todo.

On Decompositions of Permutation Polynomials into Quadratic and Cubic Power Permutations

George Petrides

Decomposing permutation polynomials into power permutations of small algebraic degrees facilitates the reduction of hardware area requirements when symmetric cryptographic algorithms are implemented with countermeasures to side channel attacks in mind. This talk will be based on the results of a recent paper on the topic (accepted in CCDS) with the same title. More specifically, I will talk about: - a simple generic construction for such decompositions into power permutations of degree at most 2 in an infinite family of finite fields, which, to the best of my knowledge, is the first result of its kind. - the improvements to the complexity of an existing search algorithm for shortest decompositions that enable it to run with larger parameters. - why always considering degrees at most 3 can lead to shorter lengths or smaller area requirements.

Thursday, August 25th

Extending the zero-difference attack on AES by using related differences

Vincent Rijmen

KU Leuven and Selmer Center

A new fundamental 4-round property of AES, called the zero-difference property, was introduced by Rønjom, Bardeh and Hellesest at Asiacrypt 2017. Our work characterizes it in a simple way by exploiting the notion of related differences which was introduced and well analyzed by the AES designers. We extend the 4-round property by considering some further properties of related differences over the AES linear layer, generalizing the zero-difference property. This results in a new key-recovery attack on 7-round AES which is the first attack on 7-round AES by exploiting the zero-difference property.

New symmetric crypto for new applications

Christian Rechberger

Graz University of Technology

We review new use-cases for symmetric-key cryptography and cryptographic hashing in applications of homomorphic encryption, zero-knowledge proofs, and secure multiparty computation. Then we survey recently proposed designs aiming at these use-cases and their cryptanalysis while highlighting various open problems. To support further developments in use-case implementations, design, and cryptanalysis, we describe a recently open-sourced zoo of implementations.

Fault analysis - overview and recent attacks

Svetla Nikova

KU Leuven and Selmer Center

I will introduce fault attacks on implementations and will focus on recent zero-value attacks and potential countermeasures.

Open problems in TI sharings

Ventzislav Nikov

NXP Semiconductors

I will present existing open problems in TI sharings.

The Uncertain Fault Model

Siemen Dhooghe

KU Leuven

In this talk, we present a new adversary model which better reflects the practice of fault analysis. We use the new adversary (and security models) to evaluate known fault countermeasures. From this analysis, we find potential attacks against some countermeasures and we find some new countermeasures which promise high security when placed in practice.

Attacks on the Firekite cipher

Thomas Johansson

Lund University

Firekite is a synchronous stream cipher using a pseudo-random number generator (PRNG) whose security is conjectured to rely on the hardness of the Learning Parity with Noise (LPN) problem. It is one of a few LPN-based symmetric encryption schemes, and it can be very efficiently implemented on a low-end SoC FPGA. The designers, Bogos, Korolija, Locher and Vaudenay, demonstrated appealing properties of Firekite.

We propose distinguishing and key-recovery attacks on Firekite by exploiting the structural properties of its PRNG.

Side-Channel-Assisted Key-Recovery Chosen-Ciphertext Attacks on Several NIST PQC KEMs

Qian Guo

Lund University

In this talk, we survey the recent results on side-channel-assisted key-recovery chosen-ciphertext attacks (CCAs) on several candidates for Public Key Encryption (PKE) or Key Encapsulation Mechanism (KEM) in the NIST post-quantum cryptography standardization process. Specially, we discuss the general attack model and show timing attacks against implementations of FrodoKEM, HQC, and BIKE using leakages from the Fujisaki-Okamoto transform. We also show key-recovery power/EM attacks on software/hardware implementations of the code-based finalist Classic McEliece.

Do Not Bound to a Single Position: Near-Optimal Multi-Positional Mismatch Attacks Against Kyber and Saber

Erik Mårtensson

Selmer Center

Misuse resilience is an important security criterion in the evaluation of the NIST Post-quantum cryptography standardization process. In this paper, we propose new key mismatch attacks against Kyber and Saber, NIST's selected scheme for encryption and one of the finalists in the third round of the NIST competition, respectively. Our novel idea is to recover partial information of multiple secret entries in each mismatch oracle call. These multi-positional attacks greatly reduce the expected number of oracle calls needed to fully recover the secret key. They also have significance in side-channel analysis. From the perspective of lower bounds, our new attacks falsify the Huffman bounds proposed in [Qin et al. ASIACRYPT 2021], where a one-positional mismatch adversary is assumed. Our new attacks can be bounded by the Shannon lower bounds, i.e., the entropy of the distribution generating each secret coefficient times the number of secret entries. We call the new attacks near-optimal since their query complexities are close to the Shannon lower bounds.

Trail Search with CRHS Equations

Håvard Raddum

Simula UiB

Evaluating a block cipher's strength against differential or linear cryptanalysis can be a difficult task. Several approaches for finding the best differential or linear trails in a cipher have been proposed, such as using mixed integer linear programming or SAT solvers. At FSE in 2018 a different approach was suggested, modelling the problem as a staged, acyclic graph and exploiting the large number of paths the graph contains.

This talk follows up on the graph-based approach and explains how to model the problem via compressed right-hand side equations. The graph we build contains paths which represent differential or linear trails in a cipher with few active S-boxes. Our method incorporates control over the memory usage, and the time complexity scales linearly with the number of rounds of the cipher being analysed. The proposed method is made available as a tool, and using it we are able to find differential trails for the Klein and Prince ciphers with higher probabilities than previously published.

Friday, August 26th

Testing equivalence of uniformly distributed functions

Nikolay S. Kaleyski

Selmer Center

We discuss how to test linear equivalence for certain classes of functions that cover many cases of planar and APN functions encountered in practice. We also discuss how the approach can be adapted to more general equivalence notions, and comment on the running times of our implementation and how it can be used in practice. We discuss some related invariants and other relevant questions.

Enumeration of some vectorial recursive sequences over finite fields

Sartaj Hasan

Indian Institute of Technology, Jammu

The sequences produced by a linear homogeneous recurrence relation over finite fields are useful in coding theory and cryptography. We shall talk about some generalizations of linear homogeneous recurrence relations that produce vector sequences over finite fields, as well as some results on enumerating these sequences and their connections to matrices and polynomials.

Pairs of Sequences: The Known and The Unknown

Zilong Liu

University of Essex

I will introduce the known and the unknown on complementary and almost-complementary pairs of sequences from both mathematical and telecommunication points of view. I will share some open problems on their existence and algebraic properties as well as several new requirements arising from beyond-5G mobile communication networks.

Data exfiltration and prevention techniques

Oleksandr Kazymyrov

Storebrand

One of the common actions during an attack on an organization is to exfiltrate data for further ransom or sale to a third party. Depending on organization and adversary maturity level, exfiltration techniques can vary from simple remote database dump to some sophisticated methods such as covert channels. During the presentation, some real methods are highlighted, and prevention methods are discussed.

Straggler Mitigation and Privacy in Decentralized Learning

Eirik Rosnes

Simula UiB

We consider straggler mitigation and user data privacy in decentralized learning. In particular, we present two novel federated learning schemes that mitigate the effect of straggling devices by introducing redundancy on the devices' data across the network. Compared to other schemes in the literature, which deal with stragglers or device dropouts by ignoring their contribution, the proposed schemes do not suffer from the client drift problem. If time permits, we will also consider the fully decentralized learning setting without a parameter server.

