Selmer Center in Secure Communication

Nikolay Kaleyski

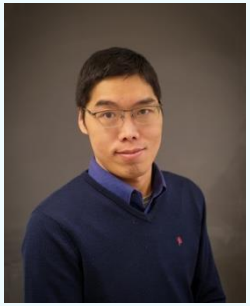
Norsk Kryptoseminar 2024

Members of the Selmer Center

- 5 faculty members (professors and associate professors)
- 5 adjunct professors/consultants
- 3 postdocs/researchers
- 11 PhD candidates
- 10-15 master students
- Organized into *research groups*

Lilya Budaghyan
Professor

Igor Semaev
Professor



Chunlei Li
Professor

Nikolay Kaleyski
Assoc. Professor

Oleksandr Kholosha
Senior Lecturer

Tor Helleseth
Prof. Emeritus

Claude Carlet
(Paris VIII)

Lejla Batina
(Radboud Univ.)

Vincent Rijmen
(KU Leuven)

Sondre Rønjom
(NSM)

Øyvind Ytrehus
(Simula@UiB)

Mohit Pal
Postdoc

Palash Sarkar
Postdoc

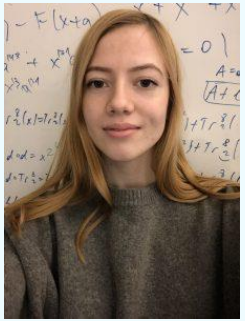
Ermes Franch
Researcher

Samuele Andreoli
PhD candidate

Amund Askeland
PhD candidate

Enrico Piccione
PhD candidate

Dian Li
PhD candidate



Nadiia Ichanska
PhD candidate

Martin Feussner
PhD candidate

Joakim Sunde
PhD candidate

Irene di Muzio
PhD candidate

Martin Grenouilloux
PhD candidate

Niki Spithaki
PhD candidate

Emre Balci
PhD candidate

Arne Sandrib
PhD candidate

Research groups

Mathematical Methods for Cryptology

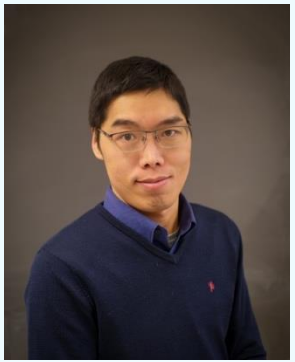
cryptographic Boolean functions, discrete mathematics

Cryptography and Cryptanalysis

post-quantum cryptography, Groebner basis algorithms and ECDLP, searchable encryption

Research groups

Reliable Communications



error correction codes,
Signal design for resource-efficient
Wireless communications

Algorithmic and Computational Methods

design and efficient implementation of algorithms, large-scale computational searches

Cybersecurity

network security,
intrusion detection

Projects

- **Cryptographic elements of trustworthy AI** (2025 – 2028, NFR, 12 MNOK, V. Rijmen)
  - New *Trustworthy AI* research group with S. Picek and L. Batina
- **Cryptographic Boolean Functions and Threshold Implementations** (2021 – 2024, NFR – FRIPRO, 10.5 MNOK, L. Budaghyan)
- **Sequences and their Applications** (2020 – 2024, NFR – IKTPLUSS, 8.7 MNOK, C. Li)
- **Construction of Optimal Boolean Functions** (2017 – 2021, TMS, 24.3 MNOK, L. Budaghyan)
- **Modern Methods and Tools for Theoretical and Applied Cryptology** (2015 – 2020, NFR – IKTPLUSS, 23.1 MNOK, Tor Helleseth)

Courses

- INF140 – Introduction to Cybersecurity
- INF143A – Applied Cryptography
- INF240A – Basic Tools for Coding theory and Cryptography
- INF243 – Algebraic Coding Theory
- INF245 – Computational Number Theory and Asymmetric Cryptography
- INF247 – Introduction to Cryptanalysis of Symmetric Ciphers
- INF249 – Advanced Cybersecurity
- INF347A – Selected Topics in Cryptology
- DIGI112, DIGI612 – ICT-security
- DIGI640 – Attacks and Countermeasures for Web applications

Events

- BFA 2024 (International Workshop on Boolean Functions and their Applications, annual event), 9-13 September, 2024, Dubrovnik, Croatia
- International Conference on Algebra, Logic, and their Applications, 13-19 October 2024, Yerevan, Armenia
- NISK 2024 (Norwegian Information Security Conference), 25 – 27 November 2024, Bergen, Norway
- SETA 2024 (Sequence and Their Applications), 1-5 July 2024, Colchester, UK

https://www.uib.no/en/rg/selmer

uib.no