Selmer Center

Crypto Research and Security Education at the University of Bergen

Lilya Budaghyan

Selmer Center (Secure Communication Group)
Department of Informatics, UiB
Yerevan, September 25, 2019

Primary research fields

- **cryptography** (design and analysis of crypto-systems)
- coding theory, sequences and their applications
- Boolean functions and discrete structures
- quantum information theory and quantum computations

Group status

- Highly competitive areas of research
- Among the best in the world
- One of only two ICT groups in Norway which have always got the very best evaluation from Norwegian Research Council.
  - excellent in 1992, 2002
  - highest grade in 2012 (only 5 in Norway out of 63 groups)
- 25 members:
  - 4 (+1) professors and 2 emeritus
  - 5 adjunct professors/consultants (1 in a project)
  - 4 postdocs/researchers (all in projects)
  - 10 PhD students (6 in projects)

Current Projects

- More than 12,5 million euro grants during the last 10 years
- Half of the group is currently supported by projects
- 5,5 million euro in current projects:
  - Theoretical and Applied Cryptology 2015-2020 from NFR
  - Quantum Machine Learning 2016-2019 from NFR
  - Cryptographic Boolean functions 2017-2021 from TMS

International Activities

- Organisation or/and program chairing of international workshops and conferences
  - Annual Boolean functions and Their Applications workshops,
  - Annual Finse winter school in information security
  - SETA 2018, WAIFI 2018, Emil Artin 2018, MMC 2017, C2SI, Eurocrypt 2019…
- Special issues in international journals
  - Annual for Boolean functions and applications
  - 2019th sequences and applications
  - Mathematical methods for cryptography
- Boolean functions wikipedia and database
- George Boole prize initiation

New Study Program

New Courses:

- INF 140 **Introduction to Cybersecurity**
- INF 143 Applied Cryptography
- INF 240 Basic Tools for Coding Theory and Cryptography
- INF 245 Computational Number Theory and Asymmetric Cryptography
- INF 247 Introduction to Cryptanalysis of Symmetric Ciphers
- INF 241 Quantum Information, Quantum Computation and Quantum Cryptography

Preserved courses:

- INF 242 Information Theory
- INF 243 Applied algebraic Coding
- INF 244 Graph based codes

Cryptographic Algorithms

- Recommended for use: Cryptographic ciphers well studied and recommended by scientists and accepted as standards by different well-known standardisation organisations.
- Possible but not recommended: Secrete ciphers - may have faults unknown to the designers.