Nikolay Kaleyski

Michael Krohnsgate 75, D 701, 5057 Bergen, Norway
E-mail: nikolay.kaleyski@gmail.com

PRESENT POSITION

From 1 May 2017 PhD Candidate at Department of Informatics, University of Bergen
Project title: *"Properties of optimal Boolean functions"*; an investigation of the properties and constructions of Boolean functions that are of practical and theoretical interest in cryptography
Supervisor: Dr. Habil. Lilya Budaghyan
Co-supervisors: Prof. Claude Carlet, Dr. Marco Calderini

EDUCATION

2014 – 2016 Master's Degree in Theoretical Computer Science, Charles University in Prague
Master's thesis: "*Boolean methods in knowledge compilation*"; presents a solution to an **open problem** in knowledge compilation; nominated for the dean's award (see appendix)
Average grade: 1.00 (1 being the highest and 3 being the lowest passing grade)
Passed with honours

2011 – 2014 Bachelor's Degree in General Computer Science, Charles University in Prague
Bachelor's thesis: "*Eigenvalues of symmetric interval matrices*"; extension and implementation of algorithms for interval arithmetic in **MATLAB**
Average grade: 1.09 (1 being the highest and 3 being the lowest passing grade)
Passed with honours

2004 – 2009 High School of Mathematics "Dr Petar Beron", Varna, Bulgaria
Main subjects: Mathematics, Physics and German language
Average grade: 5,93 (6 being the highest and 3 being the lowest passing grade)

PUBLICATIONS

- Yuyin Yu, Nikolay Kaleyski, Lilya Budaghyan, Yongqiang Li, "Classification of quadratic APN functions with coefficients in GF(2) for dimensions up to 9", submitted to Finite Fields and Their Applications, pre-print at https://eprint.iacr.org/2019/1491
- L. Budaghyan, T. Helleseth, N. S. Kaleyski, "A new family of APN quadrinomials", submitted to IEEE Transactions on Information Theory, pre-print at https://eprint.iacr.org/2019/994
- L. Budaghyan, C. Carlet, T. Helleseth, N. S. Kaleyski, "On the distance between APN functions", submitted to IEEE Transactions on Information Theory, pre-print at "Changing points in APN functions" at https://eprint.iacr.org/2018/1217
- *L. Budaghyan, N.S. Kaleyski, C. S. Riera, P. Stanica, "Partially APN functions with APN-like polynomial representations", submitted to Designs, Codes and Cryptography*
- *L. Budaghyan, N.S. Kaleyski, S. Kwon, C. S. Riera, P. Stanica, "Partially APN Boolean functions and classes of functions that are not APN infinitely often", 2019, Cryptography and Communications*
- *N. S. Kaleyski, "Changing APN Functions at Two Points", 2019, Cryptography and Communications*
- *L. Budaghyan, N. S. Kaleyski, S. Kwon, C. Riera, and P. Stanica, "Partially APN Boolean Functions", 2019, Cryptography and Communications*

CONFERENCE TALKS

- *"An Update on Known Invariants of Vectorial Boolean Functions", IWSDA (International Workshop on Signal Design and its Applications in Communications) 2019, Dongguan, China*

- *"Generalized Binomial APN Functions", BFA (Boolean Functions and Their Applications) 2019, Florence, Italy*
- *"On a Relationship between Gold and Kasami Functions and other Power APN Functions", BFA (Boolean Functions and Their Applications) 2019, Florence, Italy*
- *"Changing APN functions at two points"*, SETA (Sequences and Their Applications) 2018, Hong Kong
- *"Changing points in APN functions"*, BFA (Boolean Functions and their Applications) 2018, Loen, Norway
- *"Changing Points of APN Functions"*, Emil Artin International Conference, Yerevan, Armenia
- *"PI is not at least as succinct as MODS"*, BFA (Boolean Functions and their Applications) 2017, Solstrand, Norway
- *"PI is not at least as succinct as MODS"*, Boolean Seminar Liblice 2017, Czech Republic

OTHER ACTIVITIES

- Member of the organizing committee for WAIFI (International Workshop on the Arithmetic of Finite Fields) 2018, BFA (International Workshop on Boolean Functions and their Applications) 2019, and BFA 2020
- Lecturer for the Basic Tools for Coding theory and Cryptography (INF240) course at the University of Bergen, 2019
- Teaching assistant for the Basic Tools for Coding theory and Cryptography (INF240) course a the University of Bergen, 2020
- Co-supervisor of two master students at the University of Bergen
- Supervisor of two master students on short-term research projects

SKILLS

Computing skills:

- **Programming languages (good knowledge):** Magma, Python, TeX (LaTeX), Java, MATLAB, JavaScript, C#, Prolog, Haskell
- **Programming languages (basic knowledge):** C, C++, R
- **Web design:** HTML, CSS, PHP
- **Applications:** Vim**,** Libre Office, Microsoft Office, Photoshop
- **Operating Systems**: Microsoft Windows (multiple versions), Linux Mint, Ubuntu

Language skills:

- **English**: written – fluent, spoken – fluent
- **Russian**: written – fluent, spoken – fluent
- **Czech**: written – excellent, spoken – very good
- **Norwegian:** written – basic, spoken – basic
- **German**: written – basic, spoken – basic (have not used German in more than 5 years and out of practice, hence only basic level)
- **Bulgarian**: native language

RESEARCH INTERESTS

Boolean functions, cryptography, discrete mathematics, computer science.