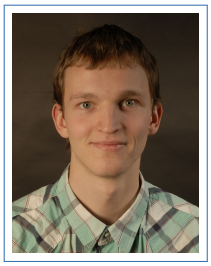

Karel Kubíček

Curriculum Vitae

Education

2018–Present **Doctoral student**, *Department of Computer Science, ETH Zurich*, Zurich.
Information Security Group

2015–2017 **Master's Studies**, *Faculty of Informatics, Masaryk University (FI MU)*, Brno.
Information Technology Security (English study program)

2016 **Exchange student**, *Faculty of Computer Science and Media Technology, Norwegian University of Science and Technology (NTNU)*, Trondheim.
Information Technology. Student of PhD course Cryptographic Protocols and Their Applications with resulting paper draft on analysis of communication anonymisation tools (Tor, I2P, cMix and Vuvuzela).

2012–2015 **Bachelor's Studies**, *Faculty of Informatics, Masaryk University (FI MU)*, Brno.
Computer Systems and Data Processing

Publications

Research paper — *BoolTest: The Fast Randomness Testing Strategy Based on Boolean Functions with Application to DES, 3-DES, MD5, MD6 and SHA-256*

Contributors — Marek Sýs, Dušan Klinec, Karel Kubíček, Petr Švenda

Published in — Communications in Computer and Information Science

Master's Thesis — *Optimisation heuristics in randomness testing*

Supervisor — Assistant Professor Petr Švenda ✉

Description — This thesis explored the optimisation methods (heuristics, ANN) for increasing capabilities of automatic analysis of cryptoprimitives. Awarded the second place in the contest for the best thesis in the field of IT Security.

Research paper — *New results on reduced-round Tiny Encryption Algorithm using genetic programming*

Contributors — Karel Kubíček, Jiří Novotný, Petr Švenda, Martin Ukrop

Published in — Infocommunications journal 2017

Saatlenstrasse 32A – Zurich, Switzerland
(+41) 79 200 22 37 • *karel.kubicek@inf.eth.ch*

Awards

2017 Awarded the second place in the contest for the best thesis in the field of IT Security.

2013–2017 Various scholarships for contribution in student projects (Czech Science Foundation, university foundation), merit scholarships.

Experience

2018–Present **Doctoral student at ETH Zurich**, Information Security Group, Zurich.

- The research goal is automation of GDPR auditing
- Teaching Information security, Algorithms
- Board member of Academic staff organisation VMI

2014–2018 **Development of randomness testing framework EACirc for analysis of cryptographic primitives**, Centre for Research on Cryptography and Security, FI MU, Brno.

- Implementation and comparison of optimisation methods into EACirc (framework for automatized randomness testing).
- Analysis of Tiny Encryption Algorithm (TEA) using EACirc framework.

2017 Jan–Sep **Network security researcher**, NEXA Technologies CZ, Brno.

- Working on research and development project in the area of cryptography, security and machine learning.
- Reference: Jaroslav Šeděnka ✉ , Martin Stehlík ✉

2013–2017 **Seminar tutor of Algorithms and Automata's theory courses**, FI MU, Brno.

- 2013–2017 Algorithms and data structures course.
- 2015–2016 Automata, Grammars, and Complexity course.
- Writing exercise book – 160 pages book with exercises and their sample results.
- Preparing and correcting assignments and final programming tasks.

2013–2017 **Contribution on organizing informatics seminar, competitions and puzzle hunts for both secondary-school and university students**, FI MU, Brno.

- 2015 – Head of secondary-school competition InterSob (leading 30 members team for four months).

Featured Skills

Basic Haskell, Java, R, Assembler, secure coding

Intermediate LaTeX, automata's theory, optimisation methods, data science, process mining

Advanced Python, C, C++, algorithm design, symmetric and asymmetric cryptography

Languages

Czech Mothertongue

English Full professional proficiency *C1-B2*

German Elementary communication and comprehension *A2*

Norwegian Basic words and phrases only *A1*

Interests

- Water sports
- Work in education system
- Mountaineering
- Puzzlehunting

Saatlenstrasse 32A – Zurich, Switzerland
(+41) 79 200 22 37 • karel.kubicek@inf.eth.ch