



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

### Publications

- 2022 *Checking Websites GDPR Consent Compliance for Marketing Emails*, Proceedings on Privacy Enhancing Technologies
- 2022 *Automating Cookie Consent and GDPR Violation Detection*, USENIX Security, best artifact award
- 2022 *Large-scale Randomness Study of Security Margins for 100+ Cryptographic Functions*, SECRIPT
- 2019 *BoolTest: The Fast Randomness Testing Strategy Based on Boolean Functions with Application to DES, 3-DES, MD5, MD6 and SHA-256*, E-Business and Telecommunications, Springer International Publishing
- 2017 *New results on reduced-round Tiny Encryption Algorithm using genetic programming*, Infocommunications journal

### Awards

- 2022 1st place in CSAW'22 Europe Applied Research Competition for our USENIX paper *Automating Cookie Consent and GDPR Violation Detection*.
- 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.

Auhofstrasse 9 – Zurich, Switzerland

☎ (+41) 79 200 22 37 • ✉ karel.kubicek@inf.eth.ch

## 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 automated 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 ednka "emailsymbols", Martin Stehlik "emailsymbols"
- 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	L <sup>A</sup> T <sub>E</sub> X, automata's theory, optimisation methods, data science, process mining
Advanced	PYTHON, C, C++, algorithm design, symmetric and asymmetric cryptography

## Languages

Czech	Mother tongue	
English	Full professional proficiency	C1
German	Limited working proficiency	B1
Norwegian	Basic words and phrases only	A1

## Interests

- Paragliding, mountaineering
- Outdoor sports
- Work in education system
- Puzzlehunting