# Vojtech Suchanek

vojtechsu@mail.muni.cz


I am a Ph.D. student at the Faculty of Informatics at Masaryk University as a member of the team at the Centre for Research on Cryptography and Security (CRoCS) under the supervision of prof. RNDr. Václav Matyáš, M.Sc., Ph.D.

## Areas of research

Elliptic curve cryptography, isogeny-based cryptography
Lattice attacks, Coppersmith algorithm

## Education

| | |
|---|---|
| 2020 – | Ph.D. Study Programme, Masaryk University<br>Fakulty of Informatics |
| 2018 – 2020 | Masters of mathematics, Masaryk University<br>Faculty of Science, Study program: Algebra and discrete mathematics<br>Thesis: Isogeny volcanoes in cryptography<br>Focus: Number theory, abstract algebra, mathematical cryptography,<br>practical implementations in Python and C |
| 2015 – 2018 | Bachelor of mathematics, Masaryk University<br>Faculty of Science, Study program: Mathematics<br>Thesis: Permutation groups |
| 2014 | CAE certificate (level C1) |

## Academic awards

| | |
|---|---|
| 2020 | Winner of the JCMM PhD talent scholarship |
| 2015 | Winner of the prize Ceska hlavicka in the category Ingenium |
| 2014–2017 | JCMM PPNS Scholarship for talented students |

## Conferences, summer schools (recent)

| | |
|---|---|
| 2020 | Algorithmic Number Theory Symposium (ANTS) |
| 2020 | The Eleventh International Conference on Post-Quantum Cryptography (PQCrypto) |
| 2020 | Selected Areas in Cryptography (SAC) |
| 2019 | Workshop on Elliptic Curve Cryptography (ECC) |

## Further experiences

- From 2017 I have been actively participating in the preparation of the book Brisk guide of mathematics led by prof. Jan Slovak.
- From 2018, I have been teaching the first-year course on the basics of mathematics and a course on information security and cryptography at the Faculty of Informatics at MUNI.
- From 2015 to 2017, I was the head organizer of the mathematical seminar Brkos. I gained useful experience as a leader of 10 people and general team skills. The seminar prepares an annual math competition, including summer and winter courses for high school students.