Vojtěch Suchánek

Résumé

Contact information

E-mail	vojtechsu@mail.muni.cz
Github	`github.com/vojtechsu`

Areas of expertise

Elliptic curve cryptography, side-channel attacks, post-quantum cryptography

Education

2020 –	Ph.D. Study Programme, Masaryk University, Faculty of Informatics, Topic: Analysis of the security of elliptic curve cryptography
2020 – 2023	Ph.D. Talent: Scholarship for talented Ph.D. students
2018 – 2020	Master of Science, Masaryk University, Faculty of Science Study program: Algebra and discrete mathematics Thesis: Post-quantum cryptography: Isogeny volcanoes
2015 – 2018	Bachelor of Science, Masaryk University, Faculty of Science Study program: Mathematics, Thesis: Permutation groups
2014	English CAE certificate (level C1)

Research projects

2024 – **ECTester.** Tool for testing and reverse-engineering elliptic curve implementations on smart cards using invalid inputs. Results accepted to CHES 2025 [3]. I originated the core idea of the reverse-engineering methods and performed the measurements.

2023 – **Fast signatures.** Lead developer of an acceleration of the verification of digital signatures on a Cortex M4 device. Accepted to ACNS 2026 [5]. I originated all of the core ideas and was responsible for the implementation and measurements.

2021 – **DiSSECT.** Python tool for generating cryptographic elliptic curves, analyzing standards, and maintaining a standardized curve database. Results presented at AfricaCrypt 2022 [2], see `https://dissect.crocs.fi.muni.cz`. I co-developed the main ideas and have been the maintainer of the implementation.

2023 – 2024 **pyecsca.** A side-channel analysis toolkit for reverse-engineering elliptic curve algorithms; results presented at CHES 2024 [1], see `https://pyecsca.org`. I participated in the main research analysis and contributed to the development of the toolkit.

2022 – 2024 **Security tools.** Participation in the development of tools for the verification of the security of cryptographic devices for the Czech national cyber and information security agency (NUKIB).

Internships and further experiences

Fall 2022 Research visit to Prof. Steve Miller at Rutgers University. Focus on the analysis of standardized elliptic curves.

2021 – 2022 Supervision of two student research projects focused on post-quantum isogeny-based protocols. One of them won the Czech Head prize 2021 for high school students (category Ingenium).

2018 – Teaching or helping with courses on information security, mathematical cryptography, and fundamentals of mathematics at the Faculty of Informatics at MUNI.

2015 – 2018 The main organizer of mathematical seminars for high school students.

Publications

1. Vojtech Suchanek, Jan Jancar, Jan Kvapil, Petr Svenda, and Łukasz Chmielewski. "ECTester: Reverse-engineering side-channel countermeasures of ECC implementations". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2025.4 (2025), pp. 290–316.

2. Vojtěch Suchánek, Marek Sýs, and Łukasz Chmielewski. *Faster signature verification using 3-dimensional GLV*. Accepted to Applied Cryptography and Network Security. 2026.

3. Vojtěch Suchánek, Vladimír Sedláček, and Marek Sýs. "Decompose and Conquer: ZVP Attacks on GLV Curves". In: *Applied Cryptography and Network Security*. Ed. by Marc Fischlin and Veelasha Moonsamy. Cham: Springer Nature Switzerland, 2025, pp. 49–73. ISBN: 978-3-031-95764-2.

4. Jan Jancar, Vojtech Suchanek, Petr Svenda, Vladimir Sedlacek, and Łukasz Chmielewski. "pyecsca: Reverse engineering black-box elliptic curve cryptography via side-channel analysis". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2024.4 (Sept. 2024), pp. 355–381. DOI: `10.46586/tches.v2024.i4.355-381`. URL: `https://tches.iacr.org/index.php/TCHES/article/view/11796`.

5. Vladimir Sedlacek, Vojtech Suchanek, Antonin Dufka, Marek Sys, and Vashek Matyas. "DiSSECT: Distinguisher of Standard and Simulated Elliptic Curves via Traits". In: *Progress in Cryptology - AFRICACRYPT 2022*. Ed. by Lejla Batina and Joan Daemen. Cham: Springer Nature Switzerland, 2022, pp. 493–517. ISBN: 978-3-031-17433-9.