Jana Sotáková, PhD

Curriculum Vitæ
Current as of August 13, 2024

Aert van Neslaan 504, 2341 HS Oegstgeest
ja.sotakova@gmail.com , janasotakova.eu

Positions

2019–2024 **PhD at QuSoft, ILLC at the University of Amsterdam**, PhD thesis
isogeny-based cryptography, advisors: Christian Schaffner, Serge Fehr, and Peter Bruin
Full list of publications at `https://jana-sotakova.github.io/research.html`.

2022–2023 **Meta AI**, 4-month research internship, working on applying machine learning to analyzing the security of cryptographic schemes, published in CCS 2023.

Interests

- *cryptography, post-quantum cryptography:* focusing on isogeny-based cryptography and lattices. I have collaborated on projects studying hard problems underlying cryptographic protocols as well as (constant-time) implementations and fault attacks.
- *quantum:* studying quantum algorithms that will be used to break cryptographic schemes.
- *machine learning:* especially with applications to cryptographic attacks.

Education

2019–2024 **PhD at QuS supportingoft, ILLC at the University of Amsterdam**, PhD thesis
isogeny-based cryptography, advisors: Christian Schaffner, Serge Fehr, and Peter Bruin

2017-2019 **University of California, Berkeley**, supported by Fulbright Student scholarship

2015-2017 **ALGANT Master Programme**, University of Regensburg and Leiden University
graduated July 2017 (*cum laude*, *Sehr gut*) (thesis)

2012-2015 **Bachelor of Mathematics, Masaryk University**, Brno
graduated August 2015 with honours; (thesis); Erasmus+ at Leiden University (2015).

Skills

analytical thinking	I am a strong problem solver; performed academic research in mathematics and cryptography. I work with the abstract and concrete, and find new connections.
coding	my research involved writing lots of proof of concept code I collaborated on projects writing high-performance code, primarily using Python/Sage, C, Magma
teamwork	I have lots of experience working in and managing groups. I have collaborated with many researchers from diverse areas of expertice during my PhD.
presentation	I have ample experience teaching and giving scientific presentations at workshops and conferences. I enjoy adapting presentations on complex topics to the particular audience.
organization	I strongly believe in diversity, equity and inclusion, and have supported initiatives for women in science (NRing, WIQD), organizing events and community building.
languages	English (C2), Dutch (C1), Spanish (B2), German (A2), Czech (native)