

Jana Sotáková

Curriculum Vitæ

Current as of February 12, 2021

L228, Science Park 123, 1098 XG Amsterdam

j.s.sotakova@uva.nl

Academic Positions

2019–2023 QuSoft and ILLC, University of Amsterdam
PhD student supervised by Christian Schaffner, Serge Fehr and Peter Bruin

Areas of Research

number theory and arithmetic geometry in cryptography (11T71, 14G50)
isogeny-based cryptography, post-quantum cryptography
quantum algorithms in cryptanalysis

Publications

Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. [Breaking the Decisional Diffie-Hellman Problem for Class Group Actions Using Genus Theory](#). In *Advances in Cryptology – CRYPTO 2020*, LNCS vol. 12171, pp. 92–120.

Laia Amorós, Annamaria Iezzi, Kristin Lauter, Chloe Martindale, and Jana Sotáková. **Explicit connections between supersingular isogeny graphs and Bruhat–Tits trees**. To appear in *Women in Numbers Europe III: Research Directions in Number Theory*. *Association for Women in Mathematics Series*. Springer.

Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Jana Sotáková, and Travis Scholl. [Adventures in Supersingularland](#). Accepted to Experimental Mathematics.

Education

- 2019– **QuSoft, ILLC at the University of Amsterdam**
PhD student, topic: quantum cryptanalysis of isogeny-based cryptography,
advisors: Christian Schaffner, Serge Fehr, and Peter Bruin
- 2017-2019 **University of California, Berkeley**
graduate student
supported in part by the Fulbright Student scholarship (academic year 2017/2018)
- 2015-2017 **ALGANT Master Programme in Algebra, Geometry and Number theory**
Master of Science, joint degree at University of Regensburg and Leiden University
graduated July 2017 (*cum laude, Sehr gut*)
Thesis: Eta quotients and class invariants of imaginary quadratic fields ([link](#))
- 2012-2015 **Bachelor of Mathematics, Masaryk University**
The Department of Mathematics and Statistics, Faculty of Science
graduated August 2015 with honours
bachelor thesis: The Number Field Sieve Method ([link](#))
- Spring 2015 **Erasmus+ mobility**
The Mathematical Institute of Leiden University.

Awards

- 2020 [Best Paper Award](#) at Crypto 2020
2017/2018 [Fulbright](#) student scholarship
2015/2017 [ALGANT](#) master scholarship
2015 Prize of the Head of the Department of Mathematics and Statistics, Masaryk University
2010–2015 [JCMM PPNS](#) Scholarship for talented students

Talks

- Oct 2020 **Elliptic curves over finite fields and their endomorphism rings**
Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties
- Jun 2020 **Elliptic curves, isogenies, and endomorphism rings**
ANTS 2020 Summer School ([video](#))
- Jun 2020 **Isogenies of elliptic curves over finite fields and genus theory**
[Linfoot Number Theory Seminar](#), Bristol
- Nov 2019 **Adventures in Supersingularland**
[Diamant symposium 2019](#)
- Nov 2019 **Adventures in Supersingularland**
Public-key crypto group seminar, COSIC Leuven
- Oct 2019 **Adventures in Supersingularland: A Look at Isogeny Graphs**
Ei/PSI Seminar, Eindhoven
- 2019 **Isogeny graphs and quaternion algebras**
QuSoft seminar, Amsterdam
- 2017 **Eta quotients and class invariants of imaginary quadratic fields**
Algant graduation talks, Leiden
- 2016 **Tate-Shafarevic group (expository)**
workshop on ranks of elliptic curves, Heidelberg Laureate Forum 2016
- 2016 **Elliptic curves and complex multiplication (expository)**
Number theory seminar, Prague

Conferences, summer schools, research visits (recent)

- 2020 **Post-Quantum Cryptography for Embedded Systems**
Lorentz Center workshop, October 5-9, 2020
- 2020 **The Quantum Wave in computing (visitor)**
Simons Institute program on quantum computing, 3 week visit Jan-Feb 2020
- 2019 **Workshop on Elliptic Curve Cryptography**
Dec 2-4, 2019, Bochum
- 2019 **research visit at COSIC Leuven**
November 2019, 1 week, results in preparation
- 2019 **Isogeny-Based Cryptography Workshop**
September 16-17, 2019, Birmingham

- 2019 **Women in Numbers - Europe III workshop**
August 26-30, 2019, Rennes, project: Isogeny graphs. Project leaders: Kristin Lauter and Chloe Martindale.
- 2019 **Conference on Applied Algebraic Geometry**
July 9-13, 2019, Bern
- 2019 **CMI-HIMR Summer School In Computational Number Theory**
June 17-28, 2019, Bristol
- 2019 **research visit at Microsoft Research**
June 2019, 1 week, results: Adventures in Supersingularland, submitted

Seminar Talks (Expository)

- Fall 2020 **Isogenies: the why and the what**
two separate talks: QuSoft junior meeting and Student cryptography seminar, CWI Amsterdam
- Spring 2020 **The DDH problem for class group actions**
Student cryptography seminar, CWI Amsterdam
- Fall 2019 **An introduction to isogenies**
Student cryptography seminar, CWI Amsterdam.
- Spring 2018 **Hecke algebras**
Number theory seminar, Berkeley. Topic: modularity lifting
- Spring 2018 **Classical Iwasawa theory, Selmer groups in Iwasawa theory (2 talks)**
Iwasawa theory seminar in preparation for the AWS
- Fall 2017 **Elliptic curves and modular forms**
Number theory seminar, Berkeley. Topic: Introduction to the Langlands Program

Teaching

University of Amsterdam (as teaching assistant)

- Fall 2020 Mathematical Proof Methods for Logic (teacher: Julian Schlöder)
- Fall 2020 Modern Cryptography (teacher: Christian Schaffner)
- Fall 2019 Modern Cryptography (teacher: Christian Schaffner)

UC Berkeley (as graduate student instructor)

- Spring 2019 Math 16B Analytic Geometry and Calculus (teacher: Kelli Talaska)
- Fall 2018 Math 16A Analytic Geometry and Calculus (teacher: Kelli Talaska)
- Spring 2018 Math 1A Calculus (teacher: Richard Bamler)

Service

- 2020– [Women in Quantum Development](#), organizing committee member
- 2020– [Women in the Faculty](#) mentoring program for students at UvA (mentor)
- 2019 [The Noetherian Ring](#) at UC Berkeley, organizer
- 2018–2019 [Math Graduate Student Association](#) officer at UC Berkeley
- Spring 2018 Iwasawa theory seminar organizer
- Fall 2017 [Directed reading program](#) at UC Berkeley, mentor
- 2012–2015 Mentoring for Czech NKC – Women and Science project