Jana Sotáková

Curriculum Vitæ
Current as of September 12, 2019

L228 (CWI), University of Amsterdam
j.s.sotakova@uva.nl

Academic Positions

2019–2023 QuSoft and ILLC, University of Amsterdam
PhD student

Areas of Research

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

Publications

2019 **Adventures in Supersingularland**
with Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter Joelle Lim, Kristina Nelson and Travis Scholl

preprint available in late September 2019

Education

2019– **QuSoft, ILLC at the University of Amsterdam**
PhD student, topic: quantum cryptanalysis,
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 The Mathematical Institute of Leiden University.

Conferences attended

2019 **Isogeny-Based Cryptography Workshop**
September 16-17, 2019, Birmingham

2019 **Women in Numbers**
August 26-30, 2019, Rennes, project: Isogeny graphs. Lead by Kristin Lauter and Chloe Martindale, with Laia Amoros Carafi and Annamaria Iezzi.

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

Talks

Isogeny graphs and quaternion algebras
2019 QuSoft seminar, Amsterdam

Eta quotients and class invariants of imaginary quadratic fields
2017 Algant graduation talks, Leiden

Tate-Shafarevic group (expository)
2016 workshop on ranks of elliptic curves, Heidelberg Laureate Forum 2016

Elliptic curves and complex multiplication (expository)
2016 Number theory seminar, Prague

Departmental Talks (Expository)

Hecke algebras
Spring 2018 Number theory seminar, Berkeley. Topic: modularity lifting

Selmer groups in Iwasawa theory
Spring 2018 Iwasawa theory seminar in preparation for the AWS

Classical Iwasawa theory
Spring 2018 Iwasawa theory seminar in preparation for the AWS

Elliptic curves and modular forms
Fall 2017 Number theory seminar, Berkeley. Topic: topic: Introduction to the Langlands Program

Symbolic powers and the Eisenbud-Mazur conjecture
Fall 2017 Commutative algebra and algebraic geometry seminar at Berkeley.

Weil Pairing
Spring 2016 seminar on Elliptic curves and the Weil conjectures, Regensburg

Cup product and Tate's theorem
Spring 2016 seminar on Local class field theory, Regensburg

Coxeter groups
Spring 2016 seminar on Coxeter groups, Regensburg

Serre duality
Fall 2016 two talks, seminar on Riemann surfaces, Regensburg

Homotopy invariance of simplicial homology
Fall 2016 seminar on Simplicial topology, Regensburg

Awards

2017/2018	Fulbright student scholarship
2015/2017	ALGANT master scholarship
2012	Prize of the Head of the Department of Mathematics and Statistics, Masaryk University
2010–2015	JCMM PPNS Scholarship for talented students

Teaching

University of Amsterdam (as TA)

Fall 2019	Modern cryptography

with Christian Schaffner and Jan Czajkowski

UC Berkeley (as graduate student instructor)

Spring 2019	Math 16B Analytic Geometry and Calculus
Fall 2018	Math 16A Analytic Geometry and Calculus
Spring 2018	Math 1A Calculus

Service

2018–2019	Math Graduate Student Association officer
Spring 2018	Iwasawa theory seminar organizer
Fall 2017	Directed reading program at UC Berkeley
2012–2015	Mentoring for Czech NKC – Women and Science project