

- Education**
- **University of California, Berkeley**, Ph.D., Mathematics, May 2003. *Hilbert's Tenth Problem and Arithmetic Geometry*. Advisor: Professor Bjorn Poonen.
  - **University of California, Berkeley**, M.A., Mathematics, May 1998.
  - **Eberhard-Karls-Universität Tübingen**, Germany, Vordiplom in Mathematics, August 1996.
- Employment**
- Assistant Professor, The Pennsylvania State University, 2007-present.
  - NSF Postdoctoral Fellow, 2005-2008.
  - T.H. Hildebrandt Assistant Professor, University of Michigan, 2005-2007.
  - VIGRE Assistant Professor, University of Michigan, 2004-2005.
  - Member at the Institute for Advanced Study, Princeton, 2003-2004.
  - Visiting researcher at Microsoft Research in the Cryptography and Anti-Piracy Group, Summer 2003, and Summer 2004.
  - Summer internship at Microsoft Research in the Cryptography and Anti-Piracy Group, Summer 2001, and Summer 2002.
- Areas of Interest**
- Number Theory, Arithmetic Geometry, Applications to Cryptography.
- Fellowships**
- Alfred P. Sloan Research Fellowship, 2008-2010.
  - NSF Postdoctoral Fellowship, 2005-2008.
  - Studienstiftung des Deutschen Volkes Fellowship 1995-1999.
- Other Awards**
- Alexander Prize for outstanding Berkeley dissertation in pure mathematics, May 2003.
- Publications**
1. *A CRT algorithm for constructing genus 2 curves over finite fields*, with Kristin Lauter. To appear in *Arithmetic, Geometry and Coding Theory (AGCT-10)*, Proceedings of the conference AGCT-10, held in Marseille in September 2005. Séminaires et Congrès 21 (2009), pages 161–176. Société Mathématique de France, Paris, 2009.
  2. *Undecidability in function fields of positive characteristic*, with Alexandra Shlapentokh. *Int. Math. Res. Not.*, Vol. 2009: article ID rnp079, 36 pages, doi: 10.1093/imrn/rnp079, 2009.
  3. *Descent on elliptic curves and Hilbert's Tenth Problem*, with Gra-

- ham Everest. *Proc. Amer. Math. Soc.*, 137(6):1951–1959, 2009.
4. *Computing the Cassels pairing on Kolyvagin classes in the Shafarevich-Tate group*, with Dimitar Jetchev and Kristin Lauter. *Pairing-Based Cryptography – Pairing 2008*, Springer LNCS volume 5209, 2008, pages 113-125.
  5. *Hilbert’s Tenth Problem for function fields of characteristic zero. Model Theory with Applications to Algebra and Analysis, Volume 2*, Cambridge University Press, 2008, pages 237-254.
  6. *Hilbert’s Tenth Problem for function fields of varieties over number fields and  $p$ -adic fields*, *J. Algebra*, 310(2007), pages 775-792. Available at arXiv:math.NT/0610132.
  7. *Integrality at a prime for global fields and the perfect closure of global fields of characteristic  $p > 2$* , *J. Number Theory*, Volume 114(1), 2005, pages 170-181. Available at arXiv:math.NT/0310224.
  8. *Hilbert’s Tenth Problem for function fields of varieties over  $\mathbb{C}$* , *International Mathematics Research Notices*, Issue 59, 2004, pages 3191–3205. Available at arXiv:math.NT/0609540.
  9. *Improved Weil and Tate pairings for elliptic and hyperelliptic curves*, with Kristin Lauter and Peter L. Montgomery, *Algorithmic Number Theory, 6th International Symposium, ANTS-VI Proceedings*, 2004, pages 169–183. Available at arXiv:math.NT/0311391.
  10. *Hilbert’s Tenth Problem for algebraic function fields of characteristic 2*, *Pacific J. Math.*, 210 (2), pages 261–281, 2003.
  11. *Fast elliptic curve arithmetic and improved Weil pairing evaluation*, with Kristin Lauter and Peter L. Montgomery, *Topics in Cryptology-CT-RSA 2003*, pages 343–354.

## Invited Talks

- Hausdorff Research Institute for Mathematics, Bonn, Germany, January 2009.
- MAA Invited Paper Session on the Beauty and Power of Number Theory, Annual meeting of the AMS, Washington, DC, January 2009.
- University of Michigan, Group Theory - Lie Theory - Number Theory Seminar, November 2008.
- Banff Workshop, Women in Numbers, Banff International Research Station, Canada, November 2008.
- Penn State, Algebra and Number Theory Seminar, October 2008.
- Pairing 2008 conference, Royal Holloway, University of London, September 2008 (Kristin Lauter, presenter).

- Penn State, Algebra and Number Theory Seminar, November 2007.
- Clay Mathematics Institute, Cambridge, Workshop on Rational Curves and Diophantine Problems over Function Fields, November 2007.
- ICMS, Edinburgh, Workshop on Number Theory and Computability, June 2007.
- Clay Mathematics Institute, Cambridge, Workshop on Hilbert's Tenth Problem, March 2007.
- East Carolina University, Department Colloquium, February 2007.
- UIC, Department Colloquium, January 2007.
- UIUC, Department Colloquium, January 2007.
- Penn State, Combinatorics and Partitions Seminar, January 2007.
- University of Virginia, Department Colloquium, January 2007.
- UT Austin, Number Theory Seminar, December 2006.
- Southern California Number Theory Day, UC Irvine, October 2006.
- IPAM workshop on Number Theory and Cryptography - Open Problems, October 2006.
- University of Oxford, Number Theory Seminar, June 2006.
- University of Leuven (Belgium), Number Theory and Algebraic Geometry Seminar, May 2006.
- UIUC, Logic Seminar, May 2006.
- Special Session on Model Theory and Computability, AMS Central sectional meeting, Notre Dame, April 2006.
- Penn State, Algebra and Number Theory Seminar, April 2006.
- UC Berkeley, Number Theory Seminar, March 2006.
- AWM Workshop, San Antonio, January 2006.
- Special session on arithmetic geometry and modular forms, Annual meeting of the AMS, San Antonio, January 2006.
- Five College Number Theory Seminar, Amherst, November 2005.
- McMaster University, Model Theory Seminar, November 2005.
- Midwest Number Theory Day, University of Wisconsin, Madison, November 2005.
- Midwest Model Theory Meeting, The Ohio State University, Columbus, October 2005.
- UIC Model Theory Seminar, October 2005.
- Workshop on Recent Applications of Model Theory, Isaac Newton Institute, Cambridge, March 2005.

- Workshop on Extensions of Hilbert's Tenth Problem, AIM, March 2005.
- University of Michigan, Number Theory Seminar, December 2005.
- Special Session on automorphic forms and analytic number theory, AMS Eastern sectional meeting, Lawrenceville, April 2004.
- University of Pennsylvania, Number Theory Seminar, February 2004.
- Special session on arithmetic geometry, Annual meeting of the AMS in Phoenix, January 2004.
- Princeton/IAS Number Theory Seminar, October 2003.
- Texas A&M University, Number Theory Seminar, October 2003.
- Workshop on Hilbert's Tenth Problem, Mazur's Conjecture and Divisibility Sequences, Oberwolfach, January 2003.
- UC Berkeley, Number Theory Seminar, September 2002.

## **Teaching**

### **The Pennsylvania State University:**

- Instructor for Math 568, Number Theory II, Spring 2009.
- Instructor for Math 497A, Elliptic Curves and Applications to Cryptography, Fall 2008.
- Instructor for Math 536, Algebra, Spring 2008.
- Instructor for Math 485, Graph Theory, Fall 2007.

### **University of Michigan:**

- Instructor for Math 175, Introduction to Cryptology, Fall 2006.
- Instructor for Math 425, Introduction to Probability, Winter 2005.
- Instructor for Math 115, Calculus, Fall 2004.

### **University of California, Berkeley:**

- Teaching Assistant for Math 185, Complex Analysis, Spring 2003.
- Teaching Assistant for Math 54, Linear Algebra and Differential Equations, Fall 2002.
- Teaching Assistant for Math 16A, Calculus for non-majors, Spring 2000.
- Teaching Assistant for Math 1B, Calculus, Fall 1999.
- Teaching Assistant for CS 170, Efficient Algorithms and Intractable Problems, Fall 1997, Spring 1998, Fall 1998 and Spring 1999.

## **Memberships**

- AMS (American Mathematical Society).