Curriculum Vitae– Kristin Lauter

Academic Credentials:

Affiliate Professor: University of Washington, Department of Mathematics
Ph.D. Mathematics, University of Chicago, 1996
Ray class field constructions of curves over finite fields with many rational points
Advisor: Niels Nygaard
M.S. Mathematics, University of Chicago, 1991
B.A. Mathematics with honors, University of Chicago, 1990

Research Areas: Number Theory, Algebraic Geometry, Cryptography, Coding Theory, Machine Learning

Professional Experience:

- Principal Researcher, Research Manager, Cryptography Group, Microsoft Research, 2008—present
- Senior Leadership Team, XCG Xtreme Computing Group Lab, Microsoft Research, 2010—2013
- Senior Researcher, Microsoft Research, Redmond, 2006—2008
- Researcher, Microsoft Research, Redmond, 2000-2006
- MSRI-Microsoft Research Postdoctoral Fellowship, 1999-2000
- Visiting Researcher, Institut de Mathematiques Luminy, France, June—August, 1999
- Visiting Scholar, Max Planck Institut für Mathematik, Bonn, Germany, 1997
- T. H. Hildebrandt Research Assistant Professor, University of Michigan, 1996-1999

Refereed Publications: 80
U.S. Patents held: 30
U.S. Patent applications filed: 20+

Fellowships and Honors:

- National Merit Scholar, 1986-1990
- Graves Memorial Lectureship Award, 1994
- AWM Mentoring Grant with Jean-Pierre Serre, College de France, May 1999
- Selfridge Prize in Computational Number Theory, May 2008
- Fellow of the American Mathematical Society (AMS), Class of 2015

Leadership positions:

- **President**, Association for Women in Mathematics (AWM), February 2015—January 2017.
- AMS Council member 2014—2017, serving on Committee on the Profession
- **Lead PI**, NSF AWM ADVANCE Grant (5-years, $750,000 for AWM)
- International Mathematical Union (IMU), member of Committee for Women in Mathematics
- **Executive Committee member**, Conference Board of Mathematical Sciences (CBMS)
- **Editor and Founder**: AWM-Springer Series

Editorial Boards:

- SIAM Journal on Applied Algebra and Geometry (SIAGA)
- Journal of Mathematical Cryptology
- Journal of Algebra and Its Applications (2010-2015)
- International Journal of Information and Coding Theory (2008-2015)

Program Chair:

- SAC 2013: Selected Areas in Cryptography 2013, 20th Anniversary Proceedings
- LatinCrypt 2015 Guadalajara, Mexico, August 23rd to 26th, 2015 Proceedings

Program committees:

Crypto 2007, ICISC 2007, ANTS 2008, Pairing 2008, Crypto 2008, SAC 2008, GeoCrypt 2009, Pairing 2009, Pairing 2010, Pairing 2012, ANTS 2012, ECC2012, IndoCrypt2012, Crypto2013 ANTS 2014

Advisory Boards :

- Scientific Advisory Board for BIRS (Banff International Research Station)
- SIAM BIG Math Network: Business Industry and Government
- Proof School: http://www.proofschool.org/lauter/
- Strategic Heathcare IT Advanced Research Projects on Security (2010-2013)

Steering Committees:

- ACM Cloud Computing Security Workshop
- WINN Women In Numbers Network
- Workshop on Elliptic Curve Cryptography (ECC)

Selected Press:

Homomorphic Encryption:

American Scientist, PNAS: Core Concept, The Register, The Register(2), Financial Times, Slashdot, Softpedia, iTnews, HealthAim, HEAT Project Blog, TechEye, MIT Technology Review, Fusion, MSR, GenomeWeb, Donga Science, Nature

Interviews: ACM Crossroads, Interview on Channel 9 WAFB, SCC 54: Strongly Connected Components, MIT Technology Review Interview: The Cryptographic Solution

Genomic Privacy:

A Cipher for Your Genome, GeneWatch, January-April 2014
How to Hide Your Genome, Science News, February 2014

Cryptographic Hash Functions:

Science magazine article by Dana Mackenzie, March, 2008.

Cryptographic Cloud Storage:

A Cloud that Can't Leak, Technology Review Magazine, Tom Simonite, August 2011
Security in the Ether Technology Review Magazine, David Talbot, December, 2009.
Security in the Cloud Communications of the ACM, Gary Anthes, November 2010.

Selected Publications in Mathematics:

1. An arithmetic intersection formula for denominators of Igusa class polynomials. With Bianca Viray. **American Journal of Math** 137 (2015), no. 2, 497–533. arXiv:1210.7841
2. On singular moduli for arbitrary discriminants, With Bianca Viray, **Int. Math. Res. Notices** (2015), Volume 2015, Issue 19, pp. 9206-9250. arXiv:1206.6942
3. A Gross-Zagier formula for quaternion algebras over totally real fields. With Eyal Goren. **Algebra and Number Theory**, **5** (2011), 495-528.
4. Genus 2 Curves with Complex Multiplication. **Int. Math. Res. Notices** (2011) With Eyal Z. Goren.
5. Explicit CM-theory for level 2-structures on abelian surfaces. **Algebra and Number Theory** (2011) With Reinier Broker, David Gruenewald.
6. Class invariants for quartic CM fields. **Ann. Inst. Fourier** (Grenoble) 57 (2007) With Eyal Goren.
7. Evil primes and superspecial moduli. **Int. Math. Res. Notices** (2006) With Eyal Goren.
8. Improved upper bounds for the number of points on curves over finite fields. **Ann. Inst. Fourier** (Grenoble) 53 (2003) With Everett Howe.
9. The maximum or minimum number of rational points on genus three curves over finite fields. **Compositio Math.** 134 (2002) With an appendix by Jean-Pierre Serre.
10. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. **J. Algebraic Geom.** (2001) With an appendix by J.-P. Serre.

Books

- *Topics in Algebraic Geometry,* Contemporary Mathematics Series 324, AMS 2003.
- *Computational Arithmetic Geometry,* Contemporary Mathematics Series 463, AMS 2008.
- *WIN--Women in Numbers: Research Directions in Number Theory,* Fields Institute Comm Series 60, 2011.
- *Selected Areas in Cryptography 2013*, Lecture Notes in Computer Science, Springer 2014.
- *Advances in the Mathematical Sciences: Research from the 2015 Association for Women in Mathematics Symposium*, AWM Springer Series, Vol. 5 (2016).
- *Progress in Cryptology -- LATINCRYPT 2015*, Lecture Notes in Computer Science 9230, Springer.

Selected Conference Organization:

- IPAM Workshop on Algebraic Geometry for Coding Theory and Cryptography, February 22-26, 2016 (Research Collaboration Conference, for men and women ~43% female) Blog Post: IPAMania!
- Dagstuhl Seminar: Modern Cryptography and Security: An Inter-Community Dialogue, January 31 – February 5 , 2016, Dagstuhl Seminar 16051. An innovative interactive format.
- ICERM Workshop: Modular Forms and Curves of Low Genus: Computational Aspects, September 28 - October 2, 2015 (~30% Female Invited Speakers)
- AWM Research Symposium, University of Maryland, April 2015
- AWM Workshop in Number Theory, Joint Mathematical Meetings, San Diego 2013
- ANTS 10 10th Algorithmic Number Theory Symposium, San Diego, July 2012
- AWM Association for Women in Mathematics 40th Anniversary Conference, Brown University, September 2011
- SIAM Conference on Applied Algebraic Geometry, UNC, October 2011
- ECC 2010, 25th anniversary of Elliptic Curve Cryptography, MSR, October 2010
- Computer Security and Cryptography, CRM, Montreal, April 12-16, 2010
- Cryptography Retrospective, Fields Institute, Toronto, May 2009
- WIN: Women in Numbers, Banff International Research Station, November 2008
- IPAM Workshop on Number Theory and Cryptography - Open Problems, Oct. 2006

Selected Plenary Addresses:

- British Math Colloquium 2016, Public Lecture, March 21, 2016
- AMS-MAA Invited Address, Joint Math Meetings 2016, Seattle, Washington, January 8, 2016.
    - AMS Notices Cover, Slides, AMS Notices Lecture Sampler, Invited Speakers - A Closer Look, Interview
- Invited Talk, Eurocrypt 2015, Sofia, Bulgaria, April 29, 2015
    - Slides, Bristol Blog, Wikipedia
- Plenary Speaker, London Math Society 150 Anniversary Celebration: It All Adds Up, University of Oxford Mathematical Institute, How to Keep Your Secrets in a Post-Quantum World, April 17, 2015
    - +Plus Magazine article
- Keynote Address, Secure Genome Analysis iDASh Workshop, March 16, 2015 [slides] [video]
- Keynote Address, Biological Data Sciences Meeting, Cold Spring Harbor Laboratories, November 6, 2014. Genome Web article.
- Invited Speaker, LatinCrypt 2014, Florianópolis, Brazil, September 18, 2014.
- Invited Speaker, ICISC 2012, 15th Annual International Conference on Information Security and Cryptology, November 28, 2012, Seoul, Korea
- Invited Address, SIAM 2012 Annual Meeting, July 9, 2012.
    - Day1 Overview, SIAM Connect Interview, Talk, Slides, AMS Coverage
- Invited Speaker, Heilbronn Annual Conference 2012.
- Arnold Family Public Lecture, Institute for Mathematics and Its Applications, October 2012.
- Keynote, ACM Cloud Computing Security Workshop, CCSW 2012
- Invited MAA Address, Spring 2012 SoCal-Nev Section Meeting, April 14, 2012
- Keynote speaker at SAC 2011 (Selected Areas of Cryptography) on Security issues for Cloud Computing.
- UT-Austin Distinguished Women in Mathematics Series, February 2010 (3 talks)
- Invited Plenary lecture, Canadian Number Theory Association (CNTA XI), July 2010
- Invited Plenary lecture, Korean Institute for Advanced Study, KWMS 6th annual conference, June 2009

Invited Lectures

- Stanford Genomics and Patient Privacy Conference, Invited Speaker and Panelist, Palo Alto, March 11, 2016, Video
- Invited Speaker, AGNES: Algebraic Geometry North Eastern Series, Brown University, Cryptographic Problems in Algebraic Geometry, October 2, 2015
- Invited Speaker, Conference on Mathematics of Cryptography, UC Irvine, August 31-September 3, 2015. Talk 1: slides video, Talk 2: slides video
- Invited Speaker, The Mathematics of Modern Cryptography Workshop, Simons Institute, Berkeley, California, July 7, 2015. Video
- Invited Speaker, AGCT 2015, CIRM Luminy, May 22, 2015
- Speaker, Columbia-CUNY-NYU Number Theory Seminar, April 23, 2015
- Speaker, Algorithmic Number Theory Symposium, ANTS-XI, GyeongJu, Korea, August 2014.
- Introduction to Modern Mathematics Lecture Series, Mathematical Sciences Center, Tsinghua University, Beijing, China, August 1, 2014.
- Morningside Center of Mathematics, Chinese Academy of Science, Number Theory Seminar, Beijing, China, July 31, 2014.
- EDGE Colloquium Speaker, 2014 EDGE Program, Harvey Mudd, June 2014.
- Project Group Leader, Women In Numbers 3, BIRS Banff, Canada, April 2014.
- Plenary Speaker, Applications of Automorphic Forms in Number Theory and Combinatorics, Louisiana State University, April 2014.
- Invited Speaker, AAAS Annual Meeting 2014, Panel and News Briefing, Genomic Privacy, Chicago, February 2014. Genetic Privacy Blog, BioIT World
- Project Group Leader and Invited Speaker, WINE Women In Numbers-Europe, CIRM Luminy, France, October 2013. AMS Blog
- Invited Speaker, 17th Workshop on Elliptic Curve Cryptography, Leuven, Belgium, September 2013
- Mini-course lecturer and Invited Speaker, Algebraic and Explicit Methods in Number Theory, Summer School and Conference, Besancon, France, September 2013.
- Invited Speaker, Arithmetic, Geometry, Cryptography and Coding Theory, CIRM Luminy, June 2013.
- Invited Speaker, Stanford Number Theory Seminar, Palo Alto, February, 2013.

- Colloquium Speaker, UC Berkeley Colloquium and Number Theory Seminar speaker, Berkeley, February 2013.
- Colloquium, Math Department, Ewha Women's University, November 30, 2012, Seoul, Korea
- Number Theory Seminar, University of Maryland, May 1, 2012
- Homomorphic Computing Conference, National Intelligence Council, May 2012
- Cryptography Seminar, University of Bristol, September 21, 2012
- Keynote Speaker, 4th Annual Women in Mathematics Symposium, January 21, 2012
- UW-PIMS Mathematics Colloquium, University of Washington, January 13, 2012 video
- WIN2 Women in Numbers, speaker and project leader, BIRS, Banff, November 2011. Video
- Keynote Address, FMI Forum for Mathematics in Industry, University of Hawaii, October 2011.
- Invited Speaker, BC/MIT Number Theory seminar, Boston, September 20, 2011.
- Colloquium Speaker, Boston University CS Department, September 19, 2011.
- AWM Association for Women in Mathematics 40th anniversary, invited speaker, Number Theory Special Session, Brown University, September 2011.
- Faculty Summit Panel, Cryptographic Cloud Storage and Services, July 2011. Video
- MSR/INRIA Joint Center, talk on Elliptic Curve Cryptography, Paris, June 2011
- IML Institut de Mathematiques de Luminy, Marseille, May 2011 (2 talks)
- Invited Speaker, Mathematics of Information-Theoretic Cryptography. February 2011 IPAM, UCLA
- Caltech Number Theory Seminar, February 2011.
- Invited Speaker, Connections for Women, Arithmetic Statistics, Hard Problems in Number Theory arising from Cryptography, MSRI, Berkeley, January 2011
- Invited Speaker, Southern California Number Theory Day, UC Irvine, November 2010.
- Invited Speaker, Number Theory Special Session, Western Sectional Meetings AMS, UCLA October 2010
- Speaker, ECC 2010, 25th anniversary of Elliptic Curve Cryptography, Microsoft Research, October 2010 Video
- Invited Speaker, Counting points: theory, algorithms and practice, April 2010 CRM, Montréal

- AMS National Meetings San Francisco, CA, January 2010 (2 Special Sessions) Arithmetic of Function Fields, Arithmetic Geometry
- UC Berkeley Colloquium and Number Theory Seminar, October 2009
- NIH mHealth, Washington D.C., October 2009, Panelist on Ethics, Privacy, and Security.

- Invited Lectures (2) 4th International Workshop on Mathematical Cryptology, Korea, June 2009.
- Speaker, GeoCrypt 2009, Guadeloupe, May 2009
- Invited Opening lecture, AGCT-12, Algebraic Geometry, Coding Theory, and Cryptography, March 2009.
- Distinguished Researcher, CRA-W Advanced Career Mentoring Workshop (CAPP), November, 2008, Santa Fe, New Mexico
- AMS meeting, Vancouver, October 2008, Special session on Number Theory
- WIN, Women in Numbers, speaker and project leader, BIRS, Banff, November 2008.
- Pairing08, 2 talks, Royal Holloway, London, September 2008
- C4: Computations on Curves for Cryptography and Coding, Paris, June, 2008.

- MSR/INRIA Joint Center, talk on Cryptographic Hash Functions, Paris, June 2008

- IML Institut de Mathematiques de Luminy, Marseille, May 2008 (2 talks)
- University of Chicago, Colloquium and Number Theory Seminar, September 2007
- Invited Speaker, 4th Spring Conference on Siegel Modular Forms and Abelian Varieties, Hamana Lake, Japan, February 2007. Slides
- 2nd NIST Hash Function Workshop Cryptographic Hash Functions from Expander Graphs, August, 2006. slides
- Invited talk, Inaugural ITA Information Theory and Applications conference, UCSD, February 2006, slides
- CISS06 Talk by Denis Charles Slides
- PKC2006 Talk by Anton Mityagin Slides
- SAGE Days 1 Conference, UCSD, February 2006. Slides
- Invited Speaker, Intersection of Arithmetic Cycles and Automorphic Forms, CRM Montreal, December, 2005. Slides
- NIST Hash Function Workshop, Talk by Josh Benaloh, NIST Gaithersburg, MD, October, 2005 slides

Selected Past Invited Talks.

ANTS II: Algorithmic Number Theory Symposium, Universite de Bordeaux, May 20, 1996.

Oberwolfach Meeting on Finite Fields, Oberwolfach, Germany, January 20, 1997.

Connecticut Valley Undergraduate Colloquium Series, UMass, Amherst, April 23, 1997.

AGCT-6: Arithmetic, Geometry, and Coding Theory, C.I.R.M. Luminy, France, June 24, 1997.

AMS Summer Research Conference, Applications of Curves over Finite Fields, Seattle, 1997.

European Research Conference, Number Theory and Arithmetical Geometry, Spain, Oct 1997.

ICCC: 2nd International Conference on Coding Theory and Cryptography, Mexico, April, 1998.

AMS Fall Western Section Meeting, Tucson, Arizona, November 14-15, 1998

Oberwolfach Meeting on Explicit Methods in Number Theory, Oberwolfach, July, 1999.

AGCT-7: Arithmetic, Geometry, and Coding Theory, October, 1999, C.I.R.M., Luminy, France

AMS Western Section Regional Meeting, Invited Address, October, 2000, San Francisco

Workshop on Unusual Applications of Number Theory, 10-14 January 2000, DIMACS

MSRI Workshop on Number Theory, Genus three curves over finite fields *October, 2000*

Sixth Pacific North West Number Theory Conference Vancouver, March 2002.

IPAM New Trends in Cryptography, April 2002

University of Michigan Undergraduate Colloquium, April 2002

High Primes and Misdemeanours, Lectures in honour of Hugh Williams, Banff 2003

Pacific Northwest Number Theory Conference, Vancouver, April 2004

BIRS Workshop: Explicit Methods in Number Theory, November, 2004

BIRS Workshop Number Theory Inspired by Cryptography November, 2005.

More information available at: http://research.microsoft.com/en-us/people/klauter/