

Research articles by area:

Cryptography

1. Full Cryptanalysis of LPS and Morgenstern Hash Function, by *Christophe Petit, Kristin Lauter, Jean-Jacques Quisquater*, in **Security and Cryptography of Networks 2008**
2. The Elliptic Curve Discrete Logarithm Problem and Equivalent Hard Problems for Elliptic Divisibility Sequences by *Kristin E. Lauter and Katherine E. Stange*, in **Selected Areas in Cryptography 2008**
3. Evaluating large degree isogenies and applications to pairing based cryptography, by *Reinier Brooker, Denis Charles, Kristin Lauter*, in **Pairing 2008**
4. Stronger Security of Authenticated Key Exchange, by *Brian LaMacchia, Kristin Lauter, Anton Mityagin*, in **ProvSec2007**
5. Signatures for Network Coding, by *Denis Charles, Kamal Jain, Kristin Lauter*, Invited paper for **CISS06**, to appear in Int. J. Information and Coding Theory (IJCoT)
6. Security Analysis of KEA Authenticated Key Exchange, by *Kristin Lauter and Anton Mityagin*, In **PKC2006**
7. Cryptographic hash functions from expander graphs, by *Denis Charles, Eyal Goren, Kristin Lauter*, **Second NIST Hash Function Workshop**, to appear in Journal of Cryptology.
8. The Advantages of Elliptic Curve Cryptography for Wireless Security , **IEEE Wireless Comm. Magazine**, Feb. 2004.

Arithmetic Geometry

1. The distance between superspecial abelian varieties with real multiplication, by *Eyal Goren, Kristin Lauter*, to appear in **Journal of Number Theory**.
2. Explicit Heegner Points: Kolyvagin's Conjecture and Non-trivial Elements in the Shafarevich-Tate Group. by *Dimitar Jetchev, Kristin Lauter, William Stein*, to appear in **Journal of Number Theory**.
3. Families of Ramanujan graphs and quaternion algebras, by *Denis Charles, Eyal Goren, Kristin Lauter*, to appear in AMS-CRM volume "**Groups and Symmetries**" in honor of John McKay.
4. Computing the Cassels pairing on Kolyvagin classes in the Shafarevich-Tate group, by *Kirsten Eisentraeger, Dimitar Jetchev, Kristin Lauter*, in **Pairing 2008**.
5. Evil Primes and Superspecial Moduli, by *Eyal Goren, Kristin Lauter*, **International Mathematics Research Notices**, volume 2006, Article ID 53864, pages 1–19.
6. Class invariants of quartic CM fields, by *Eyal Goren, Kristin Lauter*, **Annales de l'Institut Fourier**, Vol. 57 no. 2 (2007), p. 457-480.
7. Primes in the denominators of Igusa class polynomials, by *Kristin Lauter*. Preprint, 2003. (<http://www.arxiv.org/math.NT/0301240>)

Cryptographic implementation improvements

1. Improved Weil and Tate pairings for elliptic and hyperelliptic curves, by *K. Eisentraeger, K. Lauter, P.L. Montgomery*, In: **Algorithmic Number Theory - ANTS-VI**, Buell (Ed.), LNCS 3076, 169-183.
2. Trading Inversions for Multiplications in Elliptic Curve Cryptography, by *Mathieu Ciet, Marc Joye, Kristin Lauter and Peter L. Montgomery*, In **Designs, Codes, and Cryptography**, volume 39, no. 2, 2006, pp. 189-206.
3. Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation, by *K. Eisentraeger, K. Lauter, P.L. Montgomery*, In: **Topics in Cryptology - CT-RSA 2003**, M. Joye (Ed.): LNCS 2612, 343-354, Springer, Berlin 2003.
4. The equivalence of the geometric and algebraic group laws for Jacobians of genus 2 curves, by *K. Lauter*, **Topics in Algebraic and Noncommutative Geometry**, AMS Contemporary Mathematics Series 324 (2003) 165--171.

Algorithmic number theory

1. Modular polynomials for genus 2, by *Reinier Brooker and Kristin Lauter*, submitted to London Math Society Journal of Mathematics and Computation.
2. Computing Hilbert class polynomials, by *Juliana Belding, Reinier Brooker, Andreas Enge, Kristin Lauter*, in **ANTS 2008**, Selfridge Prize for best paper.
3. Computing endomorphism rings of Jacobians of genus 2 curves over finite fields, by *David Freeman, Kristin Lauter*, in **Proceedings of SAGA 2007**, Number Theory and its applications, World Scientific.
4. Computing Modular Polynomials, by *Denis Charles, Kristin Lauter*, **London Math Society Journal of Computation and Mathematics**, The LMS JCM, (8) 195-204.
5. A CRT algorithm for constructing genus 2 curves over finite fields, by *Kirsten Eisentraeger, Kristin Lauter*, to appear in **Proceedings of AGCT 2005**.
6. Constructing elliptic curves with a known number of points over a prime field, by *A. Agashe, K. Lauter, R. Venkatesan*, **High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams**, Fields Institute Communications Series, Volume 42, pp. 1-17.

Number of points on curves over finite fields

1. Pointless curves of genus 3 and 4, by *Everett W. Howe, Kristin E. Lauter, Jaap Top*, in **Arithmetic, geometry and coding theory**, Yves Aubry - Gilles Lachaud (Éd.) Séminaires et Congrès **11** (2005), xviii+216 pages, pp. 125--141.
2. Improved upper bounds for the number of points on curves over finite fields, by *Everett W. Howe, Kristin E. Lauter*, **Annales de l'Institut Fourier**, volume 53, 6 (2003), 1677--1737.
3. The maximum number of points on a curve of genus 4 over F_8 is 25, by *David Savitt*, with an Appendix by *K. Lauter*, **Canad. J. Math.**, 55 (2003), 331--352.
4. The maximum or minimum number of rational points on genus three curves over finite fields, by *Kristin Lauter with an Appendix by J-P. Serre*, **Compositio Math.** 134 (2002) 87--111.

5. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. Lauter, Kristin, with an appendix in French by J.-P. Serre. **J. Algebraic Geom.** 10 (2001), no. 1, 19--36.
6. Zeta functions of curves over finite fields with many rational points. Lauter, Kristin, **Coding theory, cryptography and related areas (Guanajuato, 1998)**, 167--174, Springer, Berlin, 2000.
7. Non-existence of a curve over \mathbf{F}_3 of genus 5 with 14 rational points. Lauter, Kristin, **Proc. Amer. Math. Soc.** 128 (2000), no. 2, 369--374.
8. Improved upper bounds for the number of rational points on algebraic curves over finite fields. Lauter, Kristin, **C. R. Acad. Sci. Paris Sér. I Math.** 328 (1999), no. 12, 1181--1185.
9. A formula for constructing curves over finite fields with many rational points. Lauter, Kristin, **J. Number Theory** 74 (1999), no. 1, 56--72.
10. Deligne-Lusztig curves as ray class fields. Lauter, Kristin, **Manuscripta Math.** 98 (1999), no. 1, 87--96.
11. Ray Class Field Constructions of Curves over Finite Fields with Many Rational Points, K. Lauter, **Algorithmic Number Theory Symposium** (ed. by H. Cohen), Lecture Notes in Computer Science 1122, 187-195 Springer, Berlin 1996.

In preparation:

1. Evaluating Igusa Class Polynomials, R. Brooker, K. Lauter.
2. Improved CRT method in Genus 2, R. Brooker, D. Gruenewald, K. Lauter.
3. Improved upper bounds for the number of points on curves over finite fields II, E. Howe, K. Lauter.
4. Gross-Zagier formulas in Genus 2, E. Goren, K. Lauter.

Volumes edited:

Computational Arithmetic Geometry, Edited by Kristin Lauter and Kenneth Ribet, Contemporary Mathematics, 463. *American Mathematical Society, Providence, RI*, 2008.

Topics in algebraic and noncommutative geometry. Edited by Caroline Grant Melles, Jean-Paul Brasselet, Gary Kennedy, Kristin Lauter and Lee McEwan. Contemporary Mathematics, 324. *American Mathematical Society, Providence, RI*, 2003.