

# Curriculum Vitae

Edward F. Schaefer  
Associate Professor  
Department of Mathematics and Computer Science  
Santa Clara University  
Santa Clara, CA 95053  
USA  
1-408-554-6899  
Fax: 1-408-554-2370  
eschaefer@scu.edu

## Education

Ph.D. Mathematics, University of California, Berkeley, 1992.

B.S. Mathematics, University of California, Davis, 1984.

B.S. Psychology, mathematics emphasis, University of California, Davis, 1984.

## Employment

(Visiting professor, Department of Mathematics, Mzuzu University, Malawi, 2005 - 2006).

Associate Professor, Department of Mathematics and Computer Science, Santa Clara University, 1998 - present.

Visiting Scholar, Department of Mathematics, University of Leiden, the Netherlands, January - May, 1999.

Cryptography Consultant, RSA Labs, Fall, 1998.

Assistant Professor, Department of Mathematics and Computer Science, Santa Clara University, 1992 - 1998.

National Science Foundation Research Assistantship directed by Hendrik W. Lenstra, Jr. 1990, 1991.

Research Assistant, Department of Psychology, Stanford University, 1984 - 1986.

## Scholarship

### Research grants

National Security Agency's Standard Grant, 2003 - 2004, \$24,740.

National Security Agency's Young Investigators Award, 1999 - 2000, \$28,191.

National Security Agency's Young Investigators Award, 1995 - 1996, \$28,000.

### Conference grants

National Science Foundation Conference Grant, 2003, \$15,000, for Lenstra Treurfeest.

National Security Agency Conference Grant, 2003, \$9,975, for Lenstra Treurfeest.

Number Theory Foundation Conference Grant, 2003, \$8,400, for Lenstra Treurfeest.

National Security Agency Conference Grant, 1997, \$10,000, for West Coast Number Theory Conference.

National Security Agency Conference Grant, 1995, \$9,956, for West Coast Number Theory Conference.

### Publications

1. Schaefer, E.F. and Stoll, M. *How to do a  $p$ -descent on an elliptic curve*, Trans. Amer. Math. Soc. **356**, 2004, 1209–1231.
2. Schaefer, E.F. *When is an integer the product of two and three consecutive integers?*, in David F. Hayes and Tatiana Shubin (eds.): *Mathematical Adventures for Students and Amateurs*, Mathematical Association of America, Washington DC, 2004, 65–71.
3. Kloosterman, R. and Schaefer, E.F. *Selmer groups of elliptic curves that can be arbitrarily large*, J. Number Theory, **99**, 2003, 148–163.
4. Musa, M.A., Schaefer, E.F. and Wedig, S. *A simplified AES algorithm and its linear and differential cryptanalyses*, Cryptologia, **17**, 2003, 148–177.
5. Flynn, E.V., Leprévost, F. Schaefer, E.F. Stein, W.A., Stoll, M. and Wetherell, J.L. *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp., **70**, 2001, 1675–1697.
6. Djabri, Z., Schaefer, E.F. and Smart, N. *Computing the  $p$ -Selmer group of an elliptic curve*, Trans. Amer. Math. Soc., **352** 2000, 5583–5597.
7. Schaefer, E.F. *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann., **310**, 1998, 447–471.
8. Poonen, B. and Schaefer, E.F. *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math., **488**, 1997, 141–188.
9. Flynn, E.V., Poonen, B. and Schaefer, E.F. *Cycles of quadratic polynomials and rational points on a genus-2 curve*, Duke Math. J., **90**, 1997, 435–463.
10. Schaefer, E.F. *A simplified Data Encryption Standard algorithm*, Cryptologia, **20**, 1996, 77–84.

11. Klassen, M.J. and Schaefer, E.F. *Arithmetic and geometry of the curve  $1 + y^3 = x^4$* , Acta Arith., **74**, 1996, 241–257.
12. Schaefer, E.F. *Class groups and Selmer groups*, J. Number Theory, **56**, 1996, 79–114.
13. Schaefer, E.F. *2-descent on the Jacobians of hyperelliptic curves*, J. Number Theory, **51**, 1995, 219–232.
14. Clark, H.H. and Schaefer, E.F. *Dealing with overhearers*, in H.H. Clark, *Arenas of Language Use*. University of Chicago Press, 1991.
15. Clark, H.H. and Schaefer, E.F. *Contributing to discourse*, Cognitive Science, **13**, 1989, 259–294.
16. Clark, H.H. and Schaefer, E.F. *Concealing one's meaning from overhearers*, Journal of Memory and Language, **26**, 1987, 209–225.
17. Clark, H.H. and Schaefer, E.F. *Collaborating on contributions to conversation*, Language and Cognitive Processes, **2**, 1987, 19–41. Reprinted in R. Dietrich & C.F. Graumann (eds), *Language processing in a social context*. Amsterdam: North Holland, 1989.

### Articles submitted

Schaefer, E.F. and Wetherell, J.L. *Computing the Selmer group of an isogeny between abelian varieties using a further isogeny to a Jacobian*, submitted to J. Number Theory, June 2004.

### Articles in preparation

Poonen, B., Schaefer, E.F. and Stoll, M. *The primitive solutions to  $X^2 + Y^3 = Z^7$* , to be submitted in September, 2004.

Schaefer, E.F. *Using descent techniques on subabelian varieties to solve Thue equations*, to be submitted in 2005.

### Honors for articles

The article [8] received a featured review (98k: 11087) in *Mathematical Reviews*.

There was a small workshop (attended by people from four countries) in December 2001 organized by John Cremona, whose purpose was to study and generalize the results in [1] and [5].

The article [10] was incorporated in Stallings' textbook *Cryptography and Network Security*, which won the 1999 TAA Award for best Computer Science and Engineering Textbook of the year. The article [4] will be incorporated in the next edition of the textbook.

The following dissertations were based (almost entirely) on the articles cited.

Bending, P. *The Mordell-Weil rank of the Jacobian of a curve of genus 2 with  $\sqrt{2}$  multiplication*, Ph.D. dissertation, University of Kent at Canterbury. This was based on [7].

Chang, S. University of Georgia, Ph.D. dissertation in progress is based on [1].

Djabri, Z.  *$p$ -descent on elliptic curves over number fields*, Ph.D. dissertation, University of Kent at Canterbury. This was based on [7].

Dokchitser, T. *Deformations of  $p$ -divisible groups and  $p$ -descent on elliptic curves*, Ph.D. dissertation, University of Utrecht. The second part on  $p$ -descent was based on [5].

Girard, M. *Groupe des points de Weierstrass sur une famille de quartiques lisses*, Ph.D. dissertation, University of Paris. This was based on [11].

van der Heiden, G.J. *2-Selmer groups associated with  $y^2 = x(x^2 - p^2)(x^2 - 4p^2)$* , Masters dissertation, University of Groningen. This was based on [13].

Kloosterman, R. *Elliptic curves with large Selmer groups*, Masters dissertation, University of Groningen. This was based on a talk I gave at the pre-ANTS workshop in June 2000 in Leiden, and turned into [3].

Schneiders, U. *Estimating the 2-rank of cubic fields by Selmer groups of elliptic curves*, Ph.D. dissertation, University of Saarbrücken. This was based on [12].

## Papers presented

*$p$ -Selmer groups that can be arbitrarily large*, **Workshop on Computational Arithmetic Geometry**, Vancouver, July 2004.

*$p$ -Selmer groups that can be arbitrarily large*, Berkeley Number Theory Seminar, March 2003.

*The curve and the equation  $1 + y^3 = x^4$* , Center for Communications Research in La Jolla, September 2002.

*When is an integer the product of two and three consecutive integers?* Pomona College, March 2002.

*When is an integer the product of two and three consecutive integers?* Bay Area Mathematical Adventures series, December 2001.

**¿ Cuando es el producto de dos enteros consecutivos tambien el producto de tres enteros consecutivos?** in Spanish at **Universidad Nacional de San Antonio Abad del Cusco**, Cuzco Peru, June 2001.

*Computing the  $p$ -Selmer group of an elliptic curve*, **Pacific Northwest Number Theory Conference** in Seattle, April 2001.

*The Birch and Swinnerton-Dyer conjectures for elliptic curves*, U.C. Santa Cruz Number Theory Seminar, February 2001.

*The curve  $1 + y^3 = x^4$* , Stanford Number Theory Seminar, January 2001.

*Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, **American Mathematical Society Meeting** in San Francisco, October 2000.

*The Birch and Swinnerton-Dyer conjecture*, University of Georgia, Athens Arithmetic Geometry Seminar, September 2000.

*Explicit descent for cyclic covers of the projective line*, University of Georgia, Athens Number Theory Seminar, September 2000.

*The curve  $1 + y^3 = x^4$* , University of Georgia, Athens Number Theory Seminar, September 2000.

*Elliptic curve cryptography*, University of Georgia, Athens Student Number Theory Seminar, September 2000.

*When is the product of two consecutive integers equal to the product of three consecutive integers?* University of Georgia, Athens Mathematics Department Colloquium, September 2000.

*Can the 5-part of the Shafarevich-Tate group of an elliptic curve be arbitrarily large?*, **pre-ANTS workshop**, Leiden, the Netherlands, June 2000.

*The curve  $1 + y^3 = x^4$* , **University of Leiden** Department of Mathematics colloquium series, October, 1999.

*When is the product of two consecutive integers equal to the product of three consecutive integers?* **University of Groningen** Department of Mathematics colloquium series, the Netherlands, May 1999.

*The equation  $1 + y^3 = x^4$* , **Chalmers Technical University** Algebra Seminar, Gothenberg Sweden, May 1999.

*When is the product of two consecutive integers equal to the product of three consecutive integers?* **Chalmers Technical University** Department of Mathematics colloquium, May 1999.

*The Frey-Rück attack*, **Technische Hochschule Darmstadt** Department of Computer Science colloquium series, Darmstadt Germany, April 1999.

*Néron models*, two talks at the **Workshop on Advances in Number Theory** in Leiden, April 1999.

*Tamagawa numbers*, **SECANTS conference**, Nottingham England. February 1999.

*Wann ist das Produkt zweier aufeinanderfolgender ganzer Zahlen gleich dem Produkt dreier aufeinanderfolgender ganzer Zahlen*, (lecture given in English at the last minute due to visitor in audience) **University of Duesseldorf** Department of Mathematics colloquium series, Germany, February 1999.

*Rational points on algebraic curves*, a **10 hour lecture series in the Intercity Getaltheorie Seminar**, Amsterdam and Leiden, January - March 1999.

*Elliptic curve cryptography*, **5 hour series, at RSA Labs**, September 1998.

*When is the product of two consecutive integers equal to the product of three consecutive integers?* Reed College in Portland, April 1998.

*The curve and the equation  $x^4 = y^3 + 1$* , University of Southern California Department of Mathematics Colloquium, September 1997.

**La reforma de calculus**, in Spanish at **Landivar University** in Guatemala City, June 1997.

**Una presentación de DERIVE**, in Spanish at **Landivar University** in Guatemala City, June 1997.

*Computing a Selmer group of a Jacobian using functions on the curve*, U.C. Berkeley Number Theory Seminar, April 1997.

*When is an integer the product of two and three consecutive integers?*, the **MAA Student Lecture at the Joint Meetings of the American Mathematical Society and the Mathematical Association of America** in San Diego, January 1997.

*Elliptic curves to avoid in cryptography*, **West Coast Number Theory Conference**, Las Vegas, December 1996.

*Rational periodic points of quadratic polynomials*, Intercity Getaltheorie Seminar, **University of Amsterdam**, September 1996.

*The curve and the equation  $y^3 + 1 = x^4$* , **University of Amsterdam** Department of Mathematics Colloquium Series, September 1996.

*There are infinitely many Carmichael Numbers*, **University of Liverpool** Department of Mathematics Colloquium Series, August 1996.

*Descent on a Jacobian using functions on a curve*, **Workshop on Curves and Computation**, Edinburgh, Scotland, March 1996.

*Rational periodic points of quadratic polynomials*, **West Coast Number Theory Conference**, Asilomar California, December 1995.

*Weierstrass points on smooth plane quartic curves with large automorphism groups*, **Cambridge University** Department of Mathematics Arithmetic Afternoon, July 1995.

*The equation  $y^3 + 1 = x^4$* , **University of Liverpool** Department of Mathematics Colloquium Series, June 1995.

*The curve  $1 + y^3 = x^4$* , U.C. Berkeley Department of Mathematics Number Theory Seminar, March 1995.

*Using geometry to solve quartic diophantine problems*, University of Michigan Department of Mathematics Number Theory Seminar, March 1995.

*On the equation and the curve  $1 + y^3 = x^4$* , **Western Number Theory Conference**, U.C. San Diego, December 1994.

*Wiles' approach to Fermat's Last Theorem*, Northern Arizona University Department of Mathematics Colloquium Series, September 1994.

*2-descent on Jacobians of the curves  $y^2 = \text{quintic}$* , **Arithmétique des courbes de genre deux** (conference), Luminy France, August 1994.

*Wiles' approach to Fermat's Last Theorem* U.C. Davis Department of Mathematics Colloquia, April 1994.

*Wiles' proof of Fermat's Last Theorem*, **Mathematical Association of America, Northern California Section meeting**, February 1994 and the **Southern California Section meeting**, March 1994.

**Die Berechnung des Mordell-Weil Rangs einer hyper-elliptischen Kurve**, in German at the **Institut für experimentelle Mathematik, Essen**, Germany, September 1993.

### **Mathematics departments visited**

University of Georgia, September 2000, guest of Andrew Granville.

University of Leiden, January - May 1999, guest of Hendrik W. Lenstra Jr.

Cambridge University, England, July 1995, September 1996, guest of J.W.S. Cassels.

University of Liverpool, England, June 1995, August 1996, guest of E. Victor Flynn.

University of Michigan, March 1995, guest of Everett Howe and Trevor Wooley.

Institut für experimentelle Mathematik, Essen Germany, September 1993, guest of Gerhard Frey.

## Teaching

### Courses taught

Calculus 1, 2, 3, 4 for science majors, Calculus 1, 2 for business majors, Nature of Mathematics, Linear Algebra, Advanced Calculus, Probability, Statistics, Number Theory, Cryptography, Cryptanalysis, Putnam Seminar, (Abstract Algebra 1 and 2 in 2004 - 2005).

Teach six courses per year, not including Putnam seminars.

### Student evaluations

Average response to *The instructor presents class material clearly* over the past five years: 4.62 out of 5.

### Curricular innovation

Designed two quarter sequence in cryptography from scratch. Wrote all homework, computer labs and much of the software. The lecture notes (which will be revised during Winter 2005) are posted on-line and have been used as the text for a graduate course at the University of Seoul and by many faculty worldwide to help design their own courses. The articles [4] and [10] are used widely in cryptography courses for teaching DES, AES, and linear and differential cryptanalysis. I have received e-mails concerning these articles from faculty on six continents (I'm still being snubbed by Antarctica after the penguin incident).

### Student mentoring

Directed Honors Thesis of Stephanie Basha and helped her prepare her colloquium talk. This fall she will be a Ph.D. student in Mathematics at Johns Hopkins University.

Wrote [4] with Stephen Wedig, now a Ph.D. student in Computer Science at U.C.L.A., and Mohammad Musa, now working before applying for a Ph.D. program in Computer Science.

Directed Honors Thesis of Alex Dow, now a Ph.D. student in Computer Science at U.C.L.A.

Created two reading courses on elliptic curves and number fields for Brian Sittinger and helped him prepare one of his colloquium talks. He is now a Ph.D. student in Number Theory at U.C. Santa Barbara.

Used nine students as peer educators in calculus courses. One, near the end of the experience, interviewed for a job as a high school teacher and was offered the job during the interview. Another was the only first-year graduate student in mathematics at the University of Illinois at Champaign-Urbana to be assigned her own class to teach.

## Service

### Service to profession

Organizer of Lenstra Treurfeest (an international number theory conference honoring Hendrik W. Lenstra Jr.), Berkeley, March 2003, with Everett Howe, Bjorn Poonen and Sara Robinson. Was in charge of all financial matters and on-site registration (as well as numerous other details).

Organizer of West Coast Number Theory Conference, Asilomar California, December 1995, with Vlad Drobot and December 1997, with Jerry Burgum. Applied for and distributed grant money and was in charge of on-site registration.

Published ten article reviews in *Mathematical Reviews*, American Mathematical Society.

Published book review of Blake, I., Seroussi, G. and Smart, N. *Elliptic Curves in Cryptography*, Cambridge University Press, Cambridge, 1999, for *Nieuw Archief voor Wiskunde*, **5-1-3**, 2000, p. 322.

Refereed articles for Acta Arithmetica, College Mathematics Journal, Cryptologia, Experimental Mathematics, Indagationes Mathematicae, Journal für die Reine und Angewandte Mathematik, Journal of Number Theory, Journal of Symbolic Computation, Magma book, Manuscripta Mathematica, Mathematics of Computation, Mathematics Magazine, and Proceedings of the Algorithmic Number Theory Symposium-V and VI.

Refereed two National Science Foundation Grant proposals.

Refereed two books, on number theory (in English) and on cryptography (in German), for Springer-Verlag.

Made hundreds of comments on manuscript that became Cassels, J.W.S. and Flynn, E.V. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge University Press, Cambridge, 1996.

Served as a secondary Ph.D. dissertation advisor to Nils Bruin at Leiden University.

Served on Ph.D. dissertation committee of Tim Dokchitser, Utrecht University.

Helped organize a new Department of Mathematics at Landivar University, Guatemala City.

Was solicited to write an opinion piece for the National Institute for Standards and Technology on whether or not to include certain elliptic curves for the elliptic curve cryptography standards.

## **Service to University**

Director of Peer Educator Program (2 years). Peer educators are students who help with the running of a course. Two common activities for them are leading in-class discussions and meeting with students outside of class. As director, I hold workshops, create pedagogical materials for the peer educators, read and respond to reflections, meet with faculty working with peer educators and take care of all administrative duties.

Director of Safe Space Program (4 years). This is the university program which provides education and support with respect to gay, lesbian, bisexual and transgender students.

Member (current or former) of College Rank and Tenure Committee for Sciences and Social Sciences (1 year), Faculty Senate Council (3 years), Core Curriculum Committee (3 years), Multicultural Curriculum Committee (5 years).

Advisor for summer orientation (4 years).

## **Service to department**

Visited Reed College as part of department's self-evaluation process.

Putnam Examination grader (5 years).

Taught and co-taught Putnam seminar eight times (the last two earned half a course release each).

Created web pages for department site on Mathematics Subject GRE, Preparing for Graduate School, and Top 50 Graduate Programs in Mathematics.

Organized department's Honors/IIME Banquet (2 years).

Department of Mathematics and Computer Science Colloquium Chair (4 years).

Task force for the technology requirement in the mathematics/computer science majors (1 year).

Task force for the writing requirement in the mathematics major (2 years).

Reorganized syllabi for Calculus 3 and 4 (1 year).

## **Service to community**

Six years of volunteer work with Spanish-speaking and deaf people with AIDS in Santa Clara County, 300 hours per year.

## **Member**

American Mathematical Society

Wiskundig Genootschap

## **Languages**

English, German, Spanish, American Sign Language