



## PUBLICATIONS

- D. Freeman, “A Generalized Brezing-Weng Method for Constructing Pairing-Friendly Ordinary Abelian Varieties,” to appear in *Pairing-Based Cryptography — Pairing 2008*, 2008.
- D. Freeman, P. Stevenhagen, and M. Streng, “Abelian Varieties with Prescribed Embedding Degree,” in *Algorithmic Number Theory Symposium — ANTS-VIII*, Springer LNCS **5011** (2008), 60–73.
- D. Freeman and K. Lauter, “Computing Endomorphism Rings of Jacobians of Genus 2 Curves over Finite Fields,” in *Symposium on Algebraic Geometry and its Applications*, World Scientific, 2008, 29–66.
- D. Freeman, M. Scott, and E. Teske, “A Taxonomy of Pairing-Friendly Elliptic Curves,” submitted to *Journal of Cryptology*, 2007.
- D. Freeman, “Constructing Pairing-Friendly Genus 2 Curves with Ordinary Jacobians,” in *Pairing-Based Cryptography — Pairing 2007*, Springer LNCS **4575** (2007), 152–176.
- D. Freeman, “Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10,” in *Algorithmic Number Theory Symposium — ANTS-VII*, Springer LNCS **4076** (2006), 452–465.
- A. Cotton, D. Freeman, A. Gnepp, T. Ng, J. Spivack, and C. Yoder, “The Isoperimetric Problem on Singular Surfaces,” *Journal of the Australian Mathematical Society* **78:2** (Apr 2005), 167–199.
- A. Cotton and D. Freeman, “The Double Bubble Problem in Spherical and Hyperbolic Space,” *International Journal of Mathematics and Mathematical Sciences* **32:11** (15 Dec 2002), 641–699.

INVITED  
CONFERENCE  
PRESENTATIONS

- “Constructing Abelian Varieties for Pairing-Based Cryptography,” Foundations of Computational Mathematics 2008, Hong Kong, June 2008.
- “Implementing the Genus 2 CM Method,” AMS Special Session on Low Genus Curves and Applications, San Diego, California, January 2008.
- “Constructing Pairing-Friendly Elliptic Curves for Cryptography,” 2nd KIAS-KMS Summer Workshop on Cryptography, Seoul, Korea, June 2007.
- “Methods for Constructing Pairing-Friendly Elliptic Curves,” 10th Workshop on Elliptic Curves in Cryptography (ECC 2006), Toronto, Canada, September 2006.
- “Double Bubbles in  $S^n$ ,” MathFest 2005 Special Session on Double Bubbles in Spheres and Gauss Space, Albuquerque, New Mexico, August 2005.

RESEARCH  
EXPERIENCE**Microsoft Research**

Redmond, Washington USA

*Summer Intern**Summer 2006*

Conducted original research in computational number theory and cryptography. Co-authored MSR Technical Report, “Computing Endomorphism Rings of Jacobians of Genus 2 Curves over Finite Fields.” Filed for patent on new invention.

**Hewlett-Packard Laboratories**

Palo Alto, California USA

*Summer Intern**Summer 2005*

Conducted original cryptographic research. Authored two HP Technical Reports, “Pairing-Based Identification Schemes” and “Constructing Families of Pairing-Friendly Elliptic Curves.” Gave lecture series on pairing-based cryptography.

**National Security Agency**

Fort George G. Meade, Maryland USA

*Director’s Summer Program**Summer 2002*

Conducted original cryptomathematics research. Designed and implemented algorithms for automated language processing. Wrote programs in Perl and C. Held Top Secret security clearance.

RESEARCH  
EXPERIENCE  
(CONTINUED)

**CERN (European Organization for Nuclear Research)** Geneva, Switzerland  
*Summer Research Student* Summer 2001  
Wrote C programs to analyze experimental particle physics data. Authored CERN internal report, “Measurement of the CP Violation Parameter  $\eta_{000}$ .”

**Williams College Department of Mathematics** Williamstown, Massachusetts USA  
*Summer Research Student* Summer 2000  
Performed original research on minimal surfaces with SMALL Geometry Group. Co-authored two papers published in research journals. Presented results at regional and national math conferences.

TEACHING  
EXPERIENCE

**University of California, Berkeley** Berkeley, California USA  
*Graduate Student Instructor* Fall 2005, Fall 2007  
Led weekly discussion sections for first-year calculus courses. Wrote weekly quizzes; graded exams, quizzes, and homework.

- Math 16A, Analytic Geometry and Calculus (Prof. J. Wagoner), Fall 2007.
- Math 1A, Calculus (Prof. V.F.R. Jones), Fall 2005.

**Harvard University** Cambridge, Massachusetts USA  
*Course Assistant* Fall 2000, Fall 2001  
Led weekly discussion sections and graded homework for multivariable calculus and linear algebra courses.

- Math 21A, Multivariable Calculus (Instructor M. Liu), Fall 2001.
- Math 21B, Linear Algebra and Differential Equations (Instructor E. Lee), Fall 2000.

*Peer Tutor* Spring 2000  
Tutored students in math and physics courses for Harvard Bureau of Study Counsel.

PROFESSIONAL  
SERVICE

Publications Refereed

- *Designs, Codes, and Cryptography*
- *Discrete Applied Mathematics*
- *Foundations of Computer Science 2008*
- *International Workshop on the Arithmetic of Finite Fields — WAIFI 2007*
- *Journal of Mathematical Cryptology*
- *Pairing-Based Cryptography — Pairing 2007*
- *Pairing-Based Cryptography — Pairing 2008*

Standards Bodies

- Contributed to ISO/IEC Standard 15946-5 (Elliptic curve generation)

Professional Organizations

- American Mathematical Society
- International Association for Cryptologic Research

LEADERSHIP  
EXPERIENCE

**Harvard Radio Broadcasting (WHRB 95.3 FM)** Cambridge, Massachusetts USA  
*Classical Music Director, Station Clerque, Program Guide Editor, “Orgy®” Producer* 2000–02  
Managed 25-member department. Directed programming and staffing for 65 hours per week of classical music. Produced multi-day “Orgy” programs on music of F.J. Haydn and D. Shostakovich. Served on station’s Administrative Board.

**Harvard Society of Physics Students** Cambridge, Massachusetts USA  
*President, Vice-President* 2000–02  
Increased club’s involvement in freshman advising. Enhanced club’s profile on campus through sponsorship of science-related activities.

SKILLS AND  
INTERESTS

Computer Skills

- Proficient in C; some experience with Perl and Visual Basic.
- Experienced in Mathematica, Maple, PARI, and MAGMA.
- Proficient on Macintosh, PC, and UNIX platforms.

Languages

- Proficient in written and spoken French.
- Basic knowledge of written and spoken German.

Other Interests

- Music theory and history, piano, singing (4 years with UC Berkeley University Chorus).
- Classical music education: creator of <http://www.ClassicalCDGuide.com>.
- Hiking, bicycling, foreign travel.