David Mandell Freeman — *Curriculum Vitae*

(+1) 650.644.8192 dfreeman@cs.stanford.edu http://cs.stanford.edu/∼dfreeman

RESEARCH INTERESTS

Cryptographic applications of number theory and arithmetic geometry. Specific interests include elliptic and hyperelliptic curve cryptography, pairing-based systems, homomorphic cryptosystems, functional encryption, and lattice-based cryptography.

EDUCATION

University of California, Berkeley Berkeley, California USA

Ph.D. in Mathematics, May 2008.

- Dissertation: *Constructing Abelian Varieties for Pairing-Based Cryptography*.
- Advisors: Kenneth A. Ribet (UC Berkeley), `ribet@math.berkeley.edu`, and Edward F. Schaefer (Santa Clara University), `eschaefer@scu.edu`.

University of Cambridge Cambridge, United Kingdom

Master of Advanced Study in Mathematics (Part III of the Mathematical Tripos), with Distinction, June 2003.

Harvard University Cambridge, Massachusetts USA

A.B. Summa Cum Laude in Chemistry and Physics and Mathematics, June 2002.

- GPA 3.97, math and science GPA 4.00.

EMPLOYMENT

Stanford University Computer Science Department Stanford, California USA

NSF Postdoctoral Scholar *2008, 2010–present*

Studied security of applications including network routing, cloud computing, and electronic voting. Published 7 original research papers on cryptography. Presented work at international conferences. Taught masters-level course on elliptic curve cryptography. Supervisor: Dan Boneh.

Centrum Wiskunde & Informatica (CWI) Amsterdam, Netherlands
Mathematisch Instituut, Universiteit Leiden Leiden, Netherlands

NSF International Postdoctoral Fellow *2009*

Studied mathematical foundations of computer security. Published 5 original research papers. Presented work at international conferences. Supervisor: Ronald Cramer.

Microsoft Research Redmond, Washington USA

Summer Intern *Summer 2006*

Conducted original research in computational number theory and cryptography. Designed and implemented new algorithms. Co-authored MSR Technical Report. Patented new invention. Supervisor: Kristin Lauter.

Hewlett-Packard Laboratories Palo Alto, California USA

Summer Intern *Summer 2005*

Conducted original cryptographic research. Authored two HP Technical Reports. Gave introductory lecture series on cryptography. Supervisor: Gadiel Seroussi.

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. Supervisor: Art Drisko.

CERN (European Organization for Nuclear Research) Geneva, Switzerland

Summer Research Student *Summer 2001*

Wrote C programs to analyze experimental particle physics data. Supervisor: Augusto Cecucci.

David Mandell Freeman — *Curriculum Vitae*

(+1) 650.644.8192 dfreeman@cs.stanford.edu http://cs.stanford.edu/∼dfreeman

PUBLICATIONS

1. D. M. Freeman, "Improved Security for Linearly Homomorphic Signatures: A Generic Framework," *Public Key Cryptography — PKC 2012*, Springer LNCS **7293** (2012), 697–714
2. S. Agrawal, D. M. Freeman, and V. Vaikuntanathan, "Predicate Encryption from Learning With Errors," *Advances in Cryptology — Asiacrypt 2011*, Springer LNCS **7073** (2011), 21–40.
3. D. Boneh and D. M. Freeman, "Homomorphic Signatures for Polynomial Functions," in *Advances in Cryptology — Eurocrypt 2011*, Springer LNCS **6632** (2011), 149–168.
4. M. Dürmuth and D. M. Freeman, "Single-Algorithm Sender-Deniable Encryption with Negligible Detection Probability," in *Advances in Cryptology — Eurocrypt 2011*, Springer LNCS **6632** (2011), 610–626.
5. D. M. Freeman and T. Satoh, "Constructing Pairing-Friendly Hyperelliptic Curves using Weil Restriction," *Journal of Number Theory* **131**:5 (May 2011), 959–983.
6. D. Boneh and D. M. Freeman, "Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures," in *Public Key Cryptography — PKC 2011*, Springer LNCS **6571** (2011), 1–16.
7. S. Meiklejohn, H. Shacham, and D. M. Freeman, "Limitations on Transformations from Composite-Order to Prime-Order Groups: The Case of Round-Optimal Blind Signatures," in *Advances in Cryptology — ASIACRYPT 2010*, Springer LNCS **6477** (2010), 519–538.
8. D. M. Freeman, "Converting Pairing-Based Cryptosystems From Composite-Order Groups to Prime-Order Groups," in *Advances in Cryptology — EUROCRYPT 2010*, Springer LNCS **6110** (2010), 44–61.
9. S. Agrawal, D. Boneh, X. Boyen, and D. M. Freeman, "Preventing Pollution Attacks in Multi-Source Network Coding," in *Public Key Cryptography — PKC 2010*, Springer LNCS **6056** (2010) 161–176.
10. D. M. Freeman, O. Goldreich, E. Kiltz, A. Rosen, and G. Segev, "More Constructions of Lossy and Correlation-Secure Trapdoor Functions," in *Public Key Cryptography — PKC 2010*, Springer LNCS **6056** (2010) 279–295.
11. D. Freeman, M. Scott, and E. Teske, "A Taxonomy of Pairing-Friendly Elliptic Curves," *Journal of Cryptology* **23**:2 (Apr 2010), 224–280.
12. N. Benger, M. Charlemagne, and D. M. Freeman, "On the Security of Pairing-Friendly Abelian Varieties over Non-Prime Fields," in *Pairing-Based Cryptography — Pairing 2009*, Springer LNCS **5671** (2009), 52–65.
13. D. Boneh, D. Freeman, J. Katz, and B. Waters, "Signing a Linear Subspace: Signature Schemes for Network Coding," in *Public-Key Cryptography — PKC 2009*, Springer LNCS **5443** (2009), 68–87.
14. D. Freeman, "A Generalized Brezing–Weng Method for Constructing Pairing-Friendly Ordinary Abelian Varieties," in *Pairing-Based Cryptography — Pairing 2008*, Springer LNCS **5209** (2008), 146–163.
15. 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.
16. 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.
17. D. Freeman, "Constructing Pairing-Friendly Genus 2 Curves with Ordinary Jacobians," in *Pairing-Based Cryptography — Pairing 2007*, Springer LNCS **4575** (2007), 152–176.
18. D. Freeman, "Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10," in *Algorithmic Number Theory Symposium — ANTS-VII*, Springer LNCS **4076** (2006), 452–465.
19. 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.
20. 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.

David Mandell Freeman — *Curriculum Vitae*

(+1) 650.644.8192 dfreeman@cs.stanford.edu http://cs.stanford.edu/∼dfreeman

HONORS AND AWARDS

NSF Mathematical Sciences Postdoctoral Research Fellowship, 2008–12.

NSF International Research Postdoctoral Fellowship, 2008–09.

Bernard Friedman Memorial Prize in Applied Mathematics, UC Berkeley, 2008.

National Defense Science and Engineering Graduate Fellowship, 2005–08.

NSF Graduate Research Fellowship, 2002–05.

Braithwaite-Batty Prize from Emmanuel College, Cambridge (top result on Mathematics Part III exam), 2003.

Bachelor Scholarship from Emmanuel College, Cambridge (Distinction result on exams), 2003.

Herchel Smith Harvard Scholarship to Emmanuel College, Cambridge, 2002–03.

Rhodes Scholarship state finalist, 2001.

Junior Phi Beta Kappa (top 1.5% in graduating class), Harvard University, 2001.

Top 100 in nation on William Lowell Putnam Mathematical Competition, 2000.

Detur Prize (top 10% in freshman class), Harvard University, 1999.

INVITED PRESENTATIONS

- "Homomorphic Signatures for Polynomial Functions," Foundations of Computational Mathematics 2011, Budapest, Hungary, July 2011.
- "Constructing Abelian Varieties for Pairing-Based Cryptography," Workshop on Pairings in Arithmetic Geometry and Cryptography, Essen, Germany, May 2009.
- "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 USA, 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.

TEACHING EXPERIENCE

Stanford University Stanford, California USA

Principal Instructor *Fall 2011*

Designed and taught masters-level course on elliptic curves in cryptography.

- CS 259c/Math 250, Elliptic Curves in Cryptography, Fall 2011.

University of California, Berkeley Berkeley, California USA

Graduate Student Instructor *Fall 2005, Fall 2007*

Led weekly discussion sections for intro calculus courses. Wrote quizzes; graded exams 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.

David Mandell Freeman — *Curriculum Vitae*

(+1) 650.644.8192 dfreeman@cs.stanford.edu http://cs.stanford.edu/∼dfreeman

PROFESSIONAL SERVICE

Program Committees

- *Pairing-Based Cryptography — Pairing 2009*, Stanford, California USA, August 2009.
- "Public Key Cryptography and the Geometry of Numbers," Amsterdam, Netherlands, May 2010.
- *Pairing-Based Cryptography — Pairing 2010*, Ishikawa, Japan, December 2010.
- 15th Workshop on Elliptic Curves in Cryptography (ECC 2011), Nancy, France, September 2011.
- *Financial Cryptography 2012*, Bonair, Netherlands Antilles, February 2012.
- *Pairing-Based Cryptogrphy — Pairing 2012*, Cologne, Germany, May 2012.

Publications Refereed (selected)

- *Designs, Codes, and Cryptography*
- *Journal of Cryptology*
- *Journal of Mathematical Cryptology*
- Reviewer for *FOCS 2008*, *STOC 2009*, *Crypto 2010*, *Asiacrypt 2010*, *Crypto 2011*, *Eurocrypt 2012*.

Standards Bodies

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

Professional Organizations

- International Association for Cryptologic Research

OTHER SKILLS AND INTERESTS

Computer Skills

- Programming languages: some experience with C, Python, Perl, Visual Basic.
- Mathematical software: Mathematica, Maple, PARI, MAGMA, Sage, R.

Languages

- English (native), French (proficient), Dutch (elementary), German (elementary)

Other Interests

- Music theory and history, piano, singing (UC Berkeley University Chorus, Studentenkoor Amsterdam, Stanford University Singers).
- Classical music education: creator of `http://www.ClassicalCDGuide.com`.
- Hiking, bicycling, foreign travel.