

Joshua Erin Hill

Curriculum Vitæ

(805) 440-4471
✉ josh-cv@untruth.org
🌐 www.untruth.org



The machine does not isolate man from the great problems of nature but plunges him more deeply into them.
– Antoine de Saint-Exupéry

Education

- Doctor of Philosophy in Mathematics**, *University of California, Irvine*, February 9, 2015.
2010–2014
- Masters of Science in Mathematics**, *University of California, Irvine*, December 10, 2010.
2008–2010
- Masters of Science in Mathematics**, *California Polytechnic State University, San Luis Obispo*, June 16, 2007.
2005–2007
- Bachelor of Science in Computer Science**, *California Polytechnic State University, San Luis Obispo*, December 11, 1999.
1993–1999

Doctoral Dissertation

Title *On Calculating the Cardinality of the Value Set of a Polynomial (and some related problems)*
Adviser Professor Daqing Wan

Teaching Training

- Two years of a weekly teaching seminar, Cal Poly, San Luis Obispo, 2005 – 2007.
- In-classroom evaluations and reviews by the Cal Poly, San Luis Obispo Mathematics Department.
- Two years of fortnightly teaching assistant seminars, UC Irvine, 2008 – 2012.
- In-classroom evaluation by the UC Irvine Teaching, Learning & Technology Center, April 2009.
- Advanced Teaching Assistant Seminar, Spring 2012.

Teaching and Advising Experience

Teaching Assistant.
2009–2014
Teaching Assistant, at *University of California at Irvine, Department of Mathematics*. Concentration: Algorithmic Algebraic Number Theory. Teaching assistant for 26 sections, each with 15 – 40 students, in the subjects of calculus (differential, integral, multi-dimensional), differential equations, linear algebra, introduction to abstract mathematics, group theory, ring theory, field theory, number theory, and cryptography. Co-instructor for a one-year, graduate-level algebra series. Organized and conducted the first mathematics department-initiated qualifying exam preparation problem-solving session to prepare graduate students for the algebra qualifying exam.

Graduate Student Mentor.
2012–2014
Graduate Student Mentor, at *University of California at Irvine, Department of Mathematics*. Advised 4 students during weekly hour-long advising meetings. Discussed time management, graduate student commitments, life / work balance, how to prepare for qualifying exams, and highlighted department and university requirements. Additionally discussed how their teaching assistant sections were proceeding, including strategies for testing, cheating detection and classroom management.

Graduate Teaching Associate.

Graduate Teaching Associate, at California Polytechnic State University, San Luis Obispo. Instructor for nine quarter-long university mathematics courses (Pre-calculus Algebra and Business Calculus). Developed syllabi, lectures, tests, quizzes, graded all student assignments and exams, and assigned final grades.

Awards

- *Outstanding Mathematics Teaching Assistant Award*, for 2010 – 2011.
- *Outstanding Contributions to the Department*, for 2013 – 2014.

Papers

1. *An Analysis of the RADIUS Authentication Protocol*, first published on the BUGTRAQ list in 2001, <http://untruth.org/s/p1.html>.
2. *Paul Erdős: Mathematical Genius, Human (in that order)*, <http://untruth.org/s/p2.html>.
3. *A Recurrence Relation for Pi*, <http://untruth.org/s/p4.html>.
4. *Ciphertext stealing Wikipedia entry* (principal author), http://en.wikipedia.org/wiki/Ciphertext_stealing.
5. *An analysis of the “Guess 2/3 of the Average” game*, <http://untruth.org/s/p5.html>.
6. *A Description of the Number Field Sieve*, <http://untruth.org/s/p6.html>.
7. *The Minimum of n Independent Normal Distributions*, <http://untruth.org/s/p7.html>.
8. *The 7–11 Problem and its Solutions*, <http://untruth.org/s/p8.html>.
9. *Weil Image Sums (and some related problems)*, my 2011 advancement, <http://untruth.org/s/p9.html>.
10. *Counting Value Sets: Algorithm and Complexity* (with Qi Cheng and Daqing Wan), presented at the ANTS x conference 2012, <http://arxiv.org/pdf/1111.1224>.

Translated Papers

I translated (with help from Google Translate) Saburô Uchiyama’s *Sur le Nombre des Valeurs Distinctes d’un Polynôme à Coefficients dans un Corps Fini*. My translation is *The Number of Distinct Values of a Polynomial with Coefficients in a Finite Field*, <http://untruth.org/s/p11.html>.

Public Presentations

- *The Zen of Information Security*, invited talk March 19th, 1999, for an undergraduate networking class.
- *Securing a Linux Box: It’s mine, and You Can’t Use It*, 2000, invited talk to the Cal Poly Linux Users Group.
- *Network Security: A Quick Overview*, 2002, invited talk to an undergraduate networking class, <http://untruth.org/s/p1002.html>
- *Cryptographic Foibles and Missteps*, 2008, invited talk to the Cuesta Computer Club, <http://untruth.org/s/p1003.html>
- *Coppersmith’s Theorem: Background, Generalizations and Applications*, 2010 invited talk in the UCI Number Theory Seminar, <http://untruth.org/s/p1004.html>
- *Weil Image Sums (and some related problems)*, my 2011 advancement presentation, <http://untruth.org/s/p1005.html>
- *Weil Image Sums and Counting Image Sets over Finite Fields*, 2011, invited talk to the UCI Math Graduate Student Colloquium. <http://untruth.org/s/p1014.html>
- *Counting Value Sets: Algorithm and Complexity*, my 2012 ANTS x presentation, <http://untruth.org/s/p1006.html>
- *Block Ciphers: Modes of Use, DES and AES*, 2012, a four hour-long presentation to a graduate cryptography class, <http://untruth.org/s/p1007.html>
- *Random Bit Generation: Theory and Practice*, 2013, an hour-long presentation to a graduate cryptography class, <http://untruth.org/s/p1008.html>
- *The Dual Elliptic Curve Deterministic RBG*, 2013, an hour-long presentation to a graduate cryptography class, <http://untruth.org/s/p1009.html>

- *Joux's Recent Index Calculus Results*, 2013, an invited two hour-long presentation to the uci Number Theory Seminar, <http://untruth.org/s/p1010.html>
- *Substitution Ciphers*, 2013, an hour-long presentation to an undergraduate cryptography course, <http://untruth.org/s/p1011.html>
- *Harvey's Average Polynomial Time Algorithms*, 2014, an invited presentation to a uci Arithmetic Geometry topics course, <http://untruth.org/s/p1012.html>
- *LaTeX for Mathy Endeavors: (Somewhat) Advanced LaTeX (and Related Matters)*, 2014, an invited presentation to the Anteater Mathematics Club, <http://untruth.org/s/p1013.html>
- *On Calculating the Cardinality of the Value Set of a Polynomial (and some related problems)*, 2014, my Dissertation Defense presentation.

Internal Training Presentations

Authored a series of internal training presentations. Each of these presentations was designed to run 2–8 hours.

- *Basic Cryptography*. Touches on historical uses of cryptography, the recent development of modern cryptography, cryptographic goals, cryptographic primitives, attack classes, security evaluation models, and a theoretical framework for symmetric and asymmetric cryptography.
- *Cryptographic Algorithms*. General principals of symmetric cipher design. Key schedules, general cipher design (Feistel and product ciphers). Detailed presentation of the design of DES, including weak/semi-weak keys and known attacks. Detailed presentation of the design of AES. Overview of internals of Skipjack, and SHA family.
- *Randomness Theory*. General theoretical background for RNG analysis and review, with emphasis on entropy evaluation of non-deterministic RNGs. Discussion on Shannon entropy and min-entropy. Summary of the SP800-22 testing requirements and use of the NIST STS tool.
- *Randomness Practice*. General PRNG design and characteristics. Detailed presentation on ANSI X9.31 A.2.4 PRNG, with emphasis on the algorithm's cycle properties. Implementation of the ANSI X9.31 A.2.4 PRNG using other symmetric algorithms. Detailed presentation on FIPS 186-2 Appendix 3.1 PRNG, with emphasis on XSEED attacks. Detailed presentation on SP800-90 HASH_DRBG, HMAC_DRBG, CTR_DRBG. Summary of the findings for DUAL_EC_DRBG.
- *Algorithm modes*. Discussion of symmetric algorithm confidentiality modes (ECB, CBC, CFB, OFB, CTR), including error propagation and plaintext malleability. Discussion of authentication modes (CBCMAC, CMAC, HMAC), including susceptibility to extension attacks. Discussion of combined modes (CCM, GCM).
- *Public/Private Key Cryptography*. Discussion of general properties of public/private systems, security strengths, and complete mathematical detail for RSA, DSA, ECDSA, DH, ECCDH, MQV and ECMQV. Demonstration of an example calculation for RSA, Diffie-Hellman, and ECDSA.
- *Error Detection Codes*. Basic error detection properties of parity, (ones' complement) checksum, and CRC. Examples of the calculation for each method.
- *Penetration Testing, The Path to Fun and Profit (through the inevitable)*. An overview of the techniques of penetration testing, with emphasis on the shortcomings of this testing technique.

Professional Experience

2010 2014 Senior Security Analyst.

Senior Security Analyst, on retainer for *InfoGard Laboratories*. Created white papers outlining current patterns in the information security industry. Consulting technical expert for the areas of network security evaluation, penetration testing, evaluation of random number generator entropy, wireless security standards, security standards production, e-prescribing security, NIST Computer Security Division and CMVP standards and interpretation, auditing statistical sampling, simple and differential power analysis and testing.

2008
2010

Information Security Consultant.

Technical consulting on hard problems. Performed standards interpretation and assessed design impacts on existing systems. Performed support for algorithm testing, including independent implementation of cryptographic algorithms to aid client testing. Assessed strength of cryptographic systems and protocols. Assisted in random number generator testing. Conducted design review of PED wireless protocols.

2004
2008

Senior Security Engineer.

Senior Security Engineer, for *InfoGard Laboratories*. In addition to the responsibilities of Security Engineer: Company technical lead. Provided technical guidance and training to security engineers and customers on complex technical issues. Evaluated formal models for high assurance systems. Performed design analysis and statistical evaluation of RNGs. Evaluated correctness and meaning of statistical tests. Authored, evaluated, and edited public ANSI/NIST security standards. Programmed and supported internal test tools. Performed simple and differential power analysis (SPA/DPA) and timing attack testing. Performed cryptographic protocol and algorithmic analysis. Developed FIPS 140-3 requirements and testing procedures. Participated in PCI scan vendor accreditation testing. Created InfoGard's Penetration Testing Laboratory, and was responsible for its operation.

1998
2004

Security Engineer.

Security Engineer, for *InfoGard Laboratories*. Performed FIPS 140-1 and 140-2 cryptographic module validation. Performed initial laboratory Common Criteria qualification test, and participated in Common Criteria testing of vendor products. Performed VISA PED and PCI testing. Performed USPS testing for electronic and mechanical indicia production. Conducted network security analysis. Produced written summaries of security vulnerabilities. Evaluated firewall and IDS designs and setup. Audited code as a portion of security evaluation. Performed system and network administration.

1997
1998

Systems Developer.

Systems Developer, for *The Grid*, a national ISP. Programmed and supported internal and external user administrative and account management interfaces. Supported DNS, mail, and web servers. Responsible for system and network security, including firewall design and implementation.

1996
1998

System Administrator.

System Administrator, for *Robert E. Kennedy Library, Cal Poly, San Luis Obispo*. Initially set up and administered UNIX- and Windows NT-based computers. Installed and supported web, mail, DNS, Gopher, and various custom network servers. Performed custom programming and scripting.

Computer Languages

C, C++, Java, Perl, Bourne Shell, SQL, 80x86 Assembly, 680x0 Assembly, LaTeX, Mathematica, Z.

Academic References

Professor Daqing Wan, Adviser, dwan@math.uci.edu.

Professor Alice Silverberg, Committee Member, asilverb@math.uci.edu.

Professor Vladimir Baranovsky, Committee Member, vbaranov@math.uci.edu.

Professor Tommy Occhipinti, co-instructor in a year long graduate algebra class, tocchipinti@carleton.edu.