Joshua Erin Hill

Résumé

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

Education

2010
2014

Doctor of Philosophy in Mathematics, *University of California, Irvine*, February 9, 2015.

2008
2010

Masters of Science in Mathematics, *University of California, Irvine*, December 10, 2010.

2005
2007

Masters of Science in Mathematics, *California Polytechnic State University, San Luis Obispo*, June 16, 2007.

1993
1999

Bachelor of Science in Computer Science, *California Polytechnic State University, San Luis Obispo*, December 11, 1999.

Doctoral Dissertation

Title — *On Calculating the Cardinality of the Value Set of a Polynomial (and some related problems)*

Adviser — Professor Daqing Wan

Topic Area — Algorithmic Algebraic Number Theory

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.

2009
2014

Teaching Assistant.

Teaching Assistant, at *University of California at Irvine, Department of Mathematics*. Teaching assistant for 26 sections, each with 15 – 40 students, in the subjects of calculus (differential, integral, multidimensional), differential equations, linear algebra, introduction to abstract mathematics, group theory, ring theory, field theory, number theory, and cryptography.

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.

2005 2007 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.

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 for high value systems. 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.

Papers

- *An Analysis of the* RADIUS *Authentication Protocol*, first published on the BUGTRAQ list in 2001, `http://untruth.org/s/p1.html`.
- *Paul Erdős: Mathematical Genius, Human (in that order)*, `http://untruth.org/s/p2.html`.
- *A Recurrence Relation for Pi*, `http://untruth.org/s/p4.html`.
- *An analysis of the "Guess 2/3 of the Average" game*, `http://untruth.org/s/p5.html`.
- *A Description of the Number Field Sieve*, `http://untruth.org/s/p6.html`.
- *The Minimum of n Independent Normal Distributions*, `http://untruth.org/s/p7.html`.
- *The 7–11 Problem and its Solutions*, `http://untruth.org/s/p8.html`.
- *Weil Image Sums (and some related problems)*, my 2011 advancement, `http://untruth.org/s/p9.html`.
- *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`.

Public Presentations

- *The Zen of Information Security*, March 19th, 1999, for an undergraduate networking class.
- *Securing a Linux Box: It's mine, and You Can't Use It*, 2000, to the Cal Poly Linux Users Group.
- *Network Security: A Quick Overview*, 2002, to an undergraduate networking class, `http://untruth.org/s/p1002.html`
- *Cryptographic Foibles and Missteps*, 2008, to the Cuesta Computer Club, `http://untruth.org/s/p1003.html`
- *Coppersmith's Theorem: Background, Generalizations and Applications*, 2010 in the UCI Number Theory Seminar, `http://untruth.org/s/p1004.html`
- *Weil Image Sums and Counting Image Sets over Finite Fields*, 2011, 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, a 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 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 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 which 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.

Software

- *fidentd*, an identd program that always identifies any network communication as associated with a specified user (generally a fake user).
- *rpasswd*, a random password generator whose passwords are based on the S/Key dictionary.
- *ketchup*, a utility that keeps track of the changes in a log file between views.
- *sts 1.5* (with errata), a statistical testing suite for the evaluation of random number generators. NIST no longer supports the UNIX version of sts, so I keep its statistical tests current with the current windows version (and my version runs six times faster than the NIST version). I have also added configuration file support, parameter checking, and fixed numerous bugs.
- A rewrite of the *ent* program for assessing entropy. Includes several of the SP800-22 tests, as well as a likely upper bound calculation for Shannon and min-entropy (for various block sizes, with arbitrary offsets).
- A reference implementation of the ECDSA algorithm in Mathematica, with support for all NIST-approved curves (on both prime-ordered and binary fields).
- A reference implementation of the FIPS 186-3 RSA key generation procedure in Mathematica.

Computer Languages

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