Joshua Erin Hill

Résumé

✉ *josh-res2018@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

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

2016–2018 **TS Lead Principal**, *UL, LLC*.

In addition to the duties of Information Security Scientist for *InfoGard Laboratories* (acquired by UL, LLC.). Chaired for UL's Transaction Security North America Security Industry Council. Founded and led the UL Entropy Analysis Group. Developed UL's Entropy Analysis product offering, including pricing, forms, internal interfaces and procedures, and training material. Coordinated legal, sales and marketing for new Entropy Analysis business area. Performed analysis of diverse entropy source designs. Created and evaluated stochastic models for entropy assessment and modeled entropy reduction due to post-processing. Authored entropy analysis reports for NIST / CMVP and NSA/IA review. Developed and supported a high speed SP800-90B statistical testing tool. Performed statistical analysis of the SP800-90B tests, detected statistical test construction problems, and formulated analogous new statistical tests with the desired chance of false reject. Provided extensive feedback to NIST on existing SP800-90B documents. Represented UL at FIDO SRWG and Biometric working groups and at plenary meetings. Created a FIDO / FIPS 140-2 mapping that allows for integration of a FIDO security evaluation within a FIPS 140-2 validation. Performed threat analysis and AVA activities for Point of Interaction Protection Profile. Conducted code and design review of IoT devices for general good security practice. Performed cryptographic analysis of Z-Wave protocol. Authored test procedures for UL 5500, a UL standard covering firmware updates. Performed pilot testing and extensive comments for CTIA's IoT Cybersecurity Requirements; authored internal procedures to support this testing.

2015–2016 **Information Security Scientist**, *InfoGard Laboratories*.

Supported SPA/DPA testing. Aided in adapting CRI's Test Vector Leakage Assessment (TVLA) to the PCI Pin Transaction Security (PTS) terminal testing program. Produced internal assessment of InfoGard's network

security posture. Developed computable upper bound estimates for the likelihood of birthday collisions in random maps, and authored a white paper to support NIST CMVP guidance development for GCM mode. Developed analysis techniques for assessing the min-entropy produced by ring-oscillator based random number generators, and used these techniques to evaluate several of the prominent commercially available random number generators. Information-theoretic analysis of cryptographic-, CASR-, and LFSR-based conditioning. Authored PCI PTS DTR appendix on STS usage. Smartcard app security architecture and code review. Principal architect and author of the FIDO Authenticator Security Certification Program. Extracted security-relevant requirements from the FIDO UAF and U2F specifications, performed a threat analysis, created a set of security measures to protect against the modeled threats, and authored security requirements pertaining to the security measures.

Senior Security Analyst.

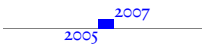
On retainer for *InfoGard Laboratories*. Created white papers outlining current patterns in the information security industry. Consulting technical expert for the areas of network security evaluation, penetration testing, evaluation of random number generator entropy, wireless security standards, security standards production, NIST Computer Security Division and CMVP standards and interpretation, simple and differential power analysis and testing. Produced an evaluation of the security requirements of the DEA's Electronic Prescriptions for Controlled Substances (EPCS) program. Produced sampling plan and statistical justification for conducting a representational sampling of a large scale network for the purpose of security evaluation.

Teaching and Research Assistant, *University of California at Irvine*.

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.

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.



Graduate Teaching Associate, *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.

Senior Security Engineer, *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. Helped develop a program to perform PCI scan vendor accreditation testing. Created InfoGard's Penetration Testing Laboratory, and was responsible for its operation. Performed security analysis of CA$HLINK II, a large federal payment clearing network and its supporting applications, including penetration testing, documentation review, and code

security review.

1998–2004 **Security Engineer**, *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. Evaluated the security of a distributed HSM-based payment architecture and fielded system. 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**, *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**, *Robert E. Kennedy Library, California Polytechnic State University, San Luis Obispo*.

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

- *NIST Special Publication 800-90B Comments* (with Ben Jackson), submitted to NIST/CMVP/NSA, `https://www.untruth.org/~josh/sp80090b/`.
- *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`.
- *Weil Image Sums (and some related problems)*, my 2011 advancement, `http://untruth.org/s/p9.html`.
- *The 7–11 Problem and its Solutions*, `http://untruth.org/s/p8.html`.
- *The Minimum of n Independent Normal Distributions*, `http://untruth.org/s/p7.html`.
- *A Description of the Number Field Sieve*, `http://untruth.org/s/p6.html`.
- *An analysis of the "Guess 2/3 of the Average" game*, `http://untruth.org/s/p5.html`.
- *A Recurrence Relation for Pi*, `http://untruth.org/s/p4.html`.
- *Paul Erdős: Mathematical Genius, Human (in that order)*, `http://untruth.org/s/p2.html`.
- *An Analysis of the RADIUS Authentication Protocol*, first published on the BUGTRAQ list in 2001, `http://untruth.org/s/p1.html`.

Public Presentations

- *Care and Feeding of the SP800-90B Statistical Tests*, 2018, a presentation to the the International Cryptographic Module Conference, 2018 (ICMC18).
- *Assessment, Certification, Evaluation* panel at the *Second Workshop on Enhancing Resilience of the Internet and Communications Ecosystem*.
- *An Approach for Entropy Assessment of Ring Oscillator-Based Noise Sources*, 2016, a presentation to the the International Cryptographic Module Conference, 2016 (ICMC16).
- *On Calculating the Cardinality of the Value Set of a Polynomial (and some related problems)*, 2014, my Dissertation Defense presentation.
- *LaTeX for Mathy Endeavors: (Somewhat) Advanced LaTeX (and Related Matters)*, 2014, a presentation to the Anteater Mathematics Club, `http://untruth.org/s/p1013.html`
- *Harvey's Average Polynomial Time Algorithms*, 2014, an presentation to a UCI Arithmetic Geometry topics course, `http://untruth.org/s/p1012.html`
- *Substitution Ciphers*, 2013, an hour-long presentation to an undergraduate cryptography course, `http:`

//untruth.org/s/p1011.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
- *The Dual Elliptic Curve Deterministic RBG*, 2013, an hour-long presentation to a graduate cryptography class, http://untruth.org/s/p1009.html
- *Random Bit Generation: Theory and Practice*, 2013, an hour-long presentation to a graduate cryptography class, http://untruth.org/s/p1008.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
- *Counting Value Sets: Algorithm and Complexity*, my 2012 ANTS X presentation, http://untruth.org/s/p1006.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
- *Weil Image Sums (and some related problems)*, my 2011 advancement presentation, http://untruth.org/s/p1005.html
- *Coppersmith's Theorem: Background, Generalizations and Applications*, 2010 in the UCI Number Theory Seminar, http://untruth.org/s/p1004.html
- *Cryptographic Foibles and Missteps*, 2008, to the Cuesta Computer Club, http://untruth.org/s/p1003.html
- *Network Security: A Quick Overview*, 2002, to an undergraduate networking class, http://untruth.org/s/p1002.html
- *Securing a Linux Box: It's mine, and You Can't Use It*, 2000, to the Cal Poly Linux Users Group.
- *The Zen of Information Security*, March 19th, 1999, for an undergraduate networking class.

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.
- *Analysis of Noise Sources*. Presentation of approaches for entropy assessment for various styles of noise source. Concentration on ring-oscillator based sources, including discussions of failure modes and reasonable analysis assumptions.

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. A refinement of the NIST sts tool, which runs 6 times faster, and contains numerous bug fixes.
- 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.
- A re-implementation of the NIST SP800-90B tests, with a view toward multi-threading, speed, better algorithm selection, and good numerical methods practice. Runs orders of magnitude faster than the reference NIST tool.

Computer Languages

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