

Jonathan Herzog

101 Woods Ave., Somerville MA 02144 • jherzog@jonathanherzog.com
Electronic version available at: <http://www.jonathanherzog.com>

Summary

Former computer-science professor with experience at both R&D labs and start-ups. Deep mathematical background; extensive background in computer security and cryptography. Skilled at programming and algorithm design. Experience with a variety of languages and technologies. Previous work in parallel computing and data mining.

Professional Experience

Technical Staff *2006 – present* *MIT Lincoln Laboratory*

- Analysis and standardization (using Cryptographic Message Syntax) of new group-keying protocol. Optimizations for low-bandwidth tactical networks.

Associate Professor, CS *2006 – 2009* *Naval Postgraduate School*

- Typical teaching: survey of programming paradigms (taught in OCaml, Prolog, Perl, Erlang, and Ada); object-oriented programming (taught in Java); intro to software development; algorithms and data structures; theory of cryptography; analysis of cryptographic protocols. Rated among top 5% of faculty for teaching.
- Research topics: parallelizing particular cryptographic algorithm (AES-GCM) on new architecture (IBM CellBE); applications of formal methods (*e.g.*, SPIN, FDR, Otter, PVS, *etc.*) to validation of security protocols (*e.g.*, SSH, Kerberos, TLS) and systems (IBM 4785 CCA, Trusted Platform Module).
- Notable service: re-design of three-quarter introductory programming sequence. Sequence now introduces students to seven programming languages and six broad types of programming tools.

Consultant *2006 – 2009* *Jonathan Herzog Consulting*

Recent projects:

- Development of resilient-system programming-language constructs for FFRDC. Project includes: Development of novel distributed algorithms using Trusted Computing infrastructure to detect Byzantine failures. Implementation of said algorithms as Erlang behaviours. Proofs of correctness, and publication of results.
- Evaluation of proprietary cryptographic algorithms.
- Development of technical roadmap for new client effort in data-mining.
- Review, testing, and validation of the LibTomCrypt open-source library for the One Laptop Per Child project. Required development of custom test-bed system. Both library and test-bed written in ANSI C. Identified and patched average of one to two serious bugs per algorithm. Bug reports and patches submitted back to library's author.

Senior Computer Scientist *2008* *Basho Technologies*

Primary responsibility: development of statistical machine-learning algorithms for sales forecasting and sales-agent guidance.

- Sole architect and developer for analytics department. Reported to CxOs.

- Developed, implemented, tested, and optimized analytical systems in Erlang and MATLAB.
- Implemented data-hygiene procedures; validated results against sale-force feedback; established data-collection procedures; helped protect resulting IP.
- At time of departure, analytical systems had achieved 90% accuracy rate with clear path to further improvement.

Secondary responsibility: development of data visualizations for customer-facing product.

Cryptographer 1997 – 2006 The MITRE Corporation

Responsibilities and achievements:

- Computer science research: Original author of strand-space approach, a mathematical technique by which to validate cryptographic protocols, infrastructures, and devices. Developer on two derived software products (domain-specific analyzer and compiler). Author of 18 conference and journal publications. Designer of new cryptographic algorithm (presented at CRYPTO).
- Analyst and consultant: Validated multiple IETF standards (TLS, SSH, DNSSec, IPSec, *etc.*) and made recommendations to sponsor and standards bodies. Acted as subject matter-expert on cryptographic protocols, Trusted Computing, cryptographic algorithms, and key-infrastructure issues (*e.g.*, certificate validation, identity-based cryptography). Influenced standard for SSHv2; advised both NSA and Air Force.
- Task management: Proposed work, managed research teams, mentored subordinates, accomplished goals on time and within budget. Proposed and managed three tasks with combined budget of \$600K and staff of five researchers.

Education

PhD	MIT <i>Advisor: Prof. R. Rivest. Readers: Profs. S. Micali, N. Lynch</i>	Computer Science	2002 – 2004
MS	MIT <i>Advisor: Prof. R. Rivest</i>	Computer Science	2000 – 2002
BS	Harvey Mudd College	Mathematics	1993 – 1997

Technologies

Languages	Ada, C, Erlang, Java, MATLAB, OCaml, Perl, Prolog
Tools	IDEs, source-control systems, unit-test frameworks, build systems, documentation generators, profilers & debuggers, parser/lexer generators, <i>etc.</i>
Systems	UNIX/Linux, OS X, CellBE, IBM 4758 CCA, Trusted Platform Module
Other	L ^A T _E X, standard unix tools (bash , emacs , <i>etc.</i>), model checkers & theorem provers (SPIN, FDR, Otter, PVS, <i>etc.</i>), content-management systems (Drupal)

Software

CPPL: the Cryptographic Protocol Programming Language. A domain-specific language for cryptographic protocols, with associated compiler, built on top of strand

spaces and logical programming. Uses external libraries for automated reasoning (Datalog) and cryptographic operations (OpenSSL). Compiler implemented in OCaml.

CPSA: the Cryptographic Protocol Shape Analyzer. An automated analysis tool for security protocols. Efficiently explores possible protocol executions; automatically detects and reports possible attacks. (Distribution limited to government agencies and contractors.) Implemented in OCaml.

AES-GCM on CellBE: Parallelized C implementation of NIST-standardized encryption algorithm (AES-GMC) on newly-introduced architecture (IBM CellBE). Achieved speeds of 10Gb/sec for plain AES, 1Gb/sec for AES-GCM.

Awards and Clearances

Naval Postgraduate School	Honorable Mention, RADM Schieffelin Award (<i>i.e.</i> , rated among top 5% of faculty in teaching)
IEEE Technical Committee, Security & Privacy	Outstanding Community Service Award
The MITRE Corporation	MITRE Best Paper Award, Program Innovation Award, Program Recognition Award, Spot Award
Harvey Mudd College	High honors, departmental honors, outstanding contribution to a clinic project
Clearances:	SECRET (with NATO access)

Editorial Activities

Program Committee	Foundations of Computer Security, Computer Security Foundations Workshop, Computer Security Foundations Symposium, Workshop on Issues in the Theory of Security, Workshop on Analysis of Security APIs
Publications Chair	Computer Security Foundations Symposium
Reviewer (Conferences)	CRYPTO, EUROCRYPT, IEEE Symposium on Security & Privacy, ACM Computer and Communications Security (CCS), Computer Security Foundations Workshop (CSFW), European Symposium on Programming (ESOP), Verification, Model Checking and Abstract Interpretation (VMCAI)
Reviewer (Journals)	Journal of Computer Security, Theory of Database Systems, IEEE Journal on Selected Areas in Communications, Theoretical Computer Science, The Computer Journal, IEEE Transactions on Computers, Transactions on Database Systems, Computers and Security, IEEE Transactions on Dependable and Secure Computing
Reviewer (Books)	Lecture Notes in Computer Science (Information and Cryptography Series)

Journal Publications

1. USING FOURIER TRANSFORMS TO UNDERSTAND SPECTRAL LINE SHAPES. *Journal of Chemical Education*, 72(3):210–214, 1995. Joint work with Ernest Grun-

wald and Colin Steel.

2. GENERALIZED k -MATCHES. *Statistics and Probability Letters*, 38:167–175, 1998. Joint work with Christopher McLaren and Anant Godbole.
3. STRAND SPACES: PROVING SECURITY PROTOCOLS CORRECT. *Journal of Computer Security*, 7(2/3):191–230, 1999. Joint work with F. Javier Thayer and Joshua D. Guttman.
4. A COMPUTATIONAL INTERPRETATION OF DOLEV-YAO ADVERSARIES. *Theoretical Computer Science*, 340:57–81, June 2005.
5. SOUNDNESS AND COMPLETENESS OF FORMAL ENCRYPTION: THE CASES OF KEY-CYCLES AND PARTIAL INFORMATION LEAKAGE. To appear in *The Journal of Computer Security*, Joint work with Pedro Adao, Gergei Bana, and Andre Scedrov.
6. UNIVERSALLY COMPOSABLE SYMBOLIC ANALYSIS OF MUTUAL AUTHENTICATION AND KEY EXCHANGE PROTOCOLS. In submission, Joint work with Ran Canetti.

**Conference
Publications**

1. STRAND SPACES: WHY IS A SECURITY PROTOCOL CORRECT?. In: *1998 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 1998. Joint work with F. Javier THAYER Fábrega and Joshua D. Guttman.
2. HONEST IDEALS ON STRAND SPACES. In: *Proceedings of the 11th IEEE Computer Security Foundations Workshop*. IEEE Computer Society Press, June 1998. Joint work with F. Javier THAYER Fábrega and Joshua D. Guttman.
3. STRAND SPACE PICTURES. In: *Proceedings, Workshop on Formal Methods and Security Protocols*, June 1998. Co-located with LICS'98, Joint work with F. Javier Thayer Fabrega and Joshua D. Guttman.
4. MIXED STRAND SPACES. In: *Proceedings of the 12th IEEE Computer Security Foundations Workshop*. IEEE Computer Society Press, June 1999. Joint work with F. Javier THAYER Fábrega and Joshua D. Guttman.
5. THE DIFFIE-HELLMAN KEY-AGREEMENT SCHEME IN THE STRAND-SPACE MODEL. In: *16th Computer Security Foundations Workshop*, pages 234–247, Asilomar, CA, June 2003. IEEE CS Press.
6. A COMPUTATIONAL INTERPRETATION OF DOLEV-YAO ADVERSARIES. In: Roberto Gorrieri, editor, *Proceedings, Workshop on Issues in the Theory of Security (WITS'03)*, pages 146–155, April 2003. Co-located with ETAPS 2003.
7. PLAINTEXT AWARENESS VIA KEY REGISTRATION. In: Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 548–564. Springer-Verlag, August 2003. Joint work with Moses Liskov and Silvio Micali.
8. TRUST MANAGEMENT IN STRAND SPACES: A RELY-GUARANTEE METHOD. In: David Schmidt, editor, *Programming Languages and Systems: 13th European Symposium on Programming*, number 2986 in LNCS, pages 325–339. Springer, 2004. Joint work with Joshua D. Guttman, F. Javier Thayer, Jay A. Carlson, John D. Ramsdell, and Brian T. Sniffen.
9. PROGRAMMING CRYPTOGRAPHIC PROTOCOLS. In: Rocco Nicola and Davide Sangiorgi, editors, *Trustworthy Global Computing (TGC 2005)*, volume 3702 of *Lecture Notes in Computer Science*, pages 116–145. Springer-Verlag GmbH, April 2005. Joint work with Joshua D. Guttman, John D. Ramsdell, and Brian T. Sniffen.

10. SOUNDNESS OF ABADI-ROGAWAY LOGICS IN THE PRESENCE OF KEY-CYCLES. In: *Proceedings of the 10th European Symposium On Research In Computer Security (ESORICS 2005)*. Springer, September 2005. Joint work with Pedro Adao, Gergei Bana, and Andre Scedrov.
11. UNIVERSALLY COMPOSABLE SYMBOLIC ANALYSIS OF MUTUAL AUTHENTICATION AND KEY EXCHANGE PROTOCOLS. In: *Proceedings, Theory of Cryptography Conference (TCC)*, March 2006. Joint work with Ran Canetti.

Technical Reports

1. FORMAL METHODS APPLIED TO SPACECRAFT SUBSYSTEMS. Technical report, Harvey Mudd College, 1997. Joint work with Erin Conley and Everett Bull.
2. A COMPARISON OF CERTIFICATE VALIDATION METHODS FOR USE IN A WEB ENVIRONMENT. MITRE Technical Report MTR98B0000093, The MITRE Corporation, November 1998. Joint work with Shimshon Berkovitz.
3. A STRAND SPACE ANALYSIS OF THE SSH VERSION 2 PROTOCOL. MITRE Product MP98B0000056, The MITRE Corporation, January 1999. Joint work with Joshua D. Guttman and Fred Chase.
4. A SAYING-LOGIC ANALYSIS OF CORE DNS SECURITY. MITRE Product MP99B0000039, The MITRE Corporation, 1999. Joint work with Fred Chase and Joshua D. Guttman.
5. THE SECURE DNS PROTOCOLS. MITRE Product MP99B0000035, The MITRE Corporation, July 1999. Joint work with Fred Chase.
6. SOME SECURITY CONCERNS REGARDING PPP-EAP-TLS. MITRE Product MP00B0000019, The MITRE Corporation, August 2000.
7. A STRAND-SPACE ANALYSIS OF TLS 1.0. MITRE Technical Report MTR 0B00000110, The MITRE Corporation, July 2000. Joint work with Laura Feinstein and Joshua D. Guttman.
8. MOBILE IP SECURITY. MITRE Product MP00B063, The MITRE Corporation, November 2000.
9. SECURE INTERNET PROTOCOL ANALYSIS CONCLUSIONS. MITRE Product MP 01B0000054, The MITRE Corporation, August 2001.
10. UNIVERSALLY COMPOSABLE SYMBOLIC ANALYSIS OF CRYPTOGRAPHIC PROTOCOLS (THE CASE OF ENCRYPTION-BASED MUTUAL AUTHENTICATION AND KEY EXCHANGE). *Cryptology ePrint Archive*, Report 2004/334, 2004. Joint work with Ran Canetti.
11. IMPLEMENTING AES ON THE CELLBE. Technical Report NPS-MA-09-001, Naval Postgraduate School, Monterey, CA, January 2009. Joint work with David Canright, George Dinolt, Simson Garfinkel, and Bruce Allen.

Popular Press

1. APPLYING PROTOCOL ANALYSIS TO SECURITY DEVICE INTERFACES. *IEEE Security and Privacy*, 4(4):84–87, July/August 2006.

Theses

- | | |
|-----|---|
| MS | COMPUTATIONAL SOUNDNESS FOR FORMAL ADVERSARIES. Massachusetts Institute of Technology, October 2002. |
| PhD | COMPUTATIONAL SOUNDNESS FOR STANDARD ASSUMPTIONS OF FORMAL CRYPTOGRAPHY. Massachusetts Institute of Technology, May 2004. |
-