# Jonathan Herzog: Publications

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

## Journal Publications

[1] Using fourier transforms to understand spectral line shapes. *Journal of Chemical Education*, 72(3):210–214, 1995. Joint work with Ernest Grunwald 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. *Journal of Computer Security*, 17(5):773–797, 2009. Joint work with Pedro Adão, Gergei Bana, and Andrej Scedrov.

[6] Universally composable symbolic security analysis. *Journal of Cryptology*, 24(1):83–147, 2011. Joint work with Ran Canetti.

[7] Automated assessment of secure search systems. *ACM SIGOPS Operating Systems Review*, 49(1):22–30, January 2015. Joint work with Mayank Varia, Benjamin Price, Nicholas Hwang, Ariel Hamlin, Jill Poland, Michael Reschly, Sophia Yakoubov, and Robert K. Cunningham.

## 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, Workship 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.

[12] Robbing the bank with a theorem prover (abstract). In: *Security Protocols Workshop*, volume 5964 of *Lecture Notes in Computer Science*, page 17. Springer, 2007. Joint work with Paul Youn, Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Ronald L. Rivest, and Ross Anderson.

[13] On the robustness of cognitive networking mechanisms to malicious insiders. In: *Proceedings, Military Communications Conference (MILCOM 2011)*. IEEE Communications Society, November 2011. Joint work with Gabriel Wachman and Dan Liu.

[14] A comprehensive key management architecture for small unmanned aircraft systems and other tactical applications. In: *Proceedings, Military Communications Conference (MILCOM 2011)*. IEEE Communications Society, November 2011. Distribution authorized to U.S. Government agencies and their contractors. Joint work with Roger Khazan, Adam Petcher, and Daniil Utin.

[15] Usable identity management fortactical devices. In: *Proceedings, Military Communications Conference (MILCOM 2011)*. IEEE Communications Society, November 2011. Distribution authorized to U.S. Government agencies and their contractors. Joint work with Sophia Yuditskaya and Roger Khazan.

[16] A test-suite generator for database systems. In: *High Performance Extreme Computing Conference (HPEC)*, pages 1–6. IEEE, September 2014. Joint work with Ariel Hamlin.

---

**Standards**

[1] Use of static-static elliptic curve diffie-hellman key agreement in cryptographic message syntax. Request For Comments (RFC) 6278, June 2011. Joint work with Roger Khazan.

---

**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] Robbing the bank with a theorem prover. Technical report, University of Cambridge Computer Laboratory, August 2005. Joint work with Paul Youn, Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Ronald L. Rivest, and Ross Anderson.

[12] 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.

[13] Using attestation to lift crash resilience to byzantine resilience. MITRE technical report, The MITRE Corporation, 2009. Joint work with Jonathan Millen, Brian O'Hanlon, John D. Ramsdell, and Ariel Segall.

[14] Small unmanned aircraft systems: Key management architecture. Technical report, MIT Lincoln Laboratory, Lexington, MA, August 2011. Joint work with Roger Khazan, Sean O'Melia, Adam Petcher, and Dan Utin.

---

**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.

---