

STEPHEN R. TATE

<http://www.cs.unt.edu/~srt/>
srt@cs.unt.edu

Dept. of Computer Science and Engineering
University of North Texas
Denton, TX 76203

332 Oak Forest Dr.
Highland Village, TX 75077

(972) 966-8579

(940) 565-4864

Areas of expertise: Computer Security and Cryptography, Algorithm Analysis, On-Line Algorithms, Algebraic Algorithms, Data Compression

EDUCATION

Year	Degree	Major	Institution
1991	Ph.D.	Computer Science	Duke University
1986	B.E.	Computer Science/Electrical Eng./Mathematics	Vanderbilt University

PROFESSIONAL EXPERIENCE

Dates	Position	Organization	Location
Sep 1999 – present	Associate Professor	University of North Texas	Denton, TX
Sep 1993 – Aug 1999	Assistant Professor	University of North Texas	Denton, TX
Sep 1991 – Aug 1993	Asst. Research Professor	Duke University	Durham, NC
Jan 1991 – Aug 1991	Research Associate	Duke University	Durham, NC
Sep 1987 – Dec 1990	Research Assistant	Duke University	Durham, NC

PROFESSIONAL ACTIVITIES

- Founder and director of the Center for Information and Computer Security (CICS) at UNT (founded in 2004).
- Founder and director of the Computer Privacy and Security (CoPS) Lab at UNT (founded in 2001).
- Editorial board, *Journal of Information Assurance and Security (JIAS)*.
- Recent program committee membership:
 - *Information Assurance and Security* track of the *IEEE International Conference on Information Technology: Coding and Computing (ITCC)*, 2004 and 2005.
 - *International Workshop on Security in Networks and Distributed Systems (SNDS05)*, 2005.
 - *IASTED International Conference on Communication, Network and Information Security (CNIS)*, 2005.

- *International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN)*, 2005.
- *International Conference on Information Warfare and Security (ICIW)*, 2006.
- *3rd International Conference on Autonomic and Trusted Computing (ATC)*, 2006.
- Program Committee, *Secure Knowledge Management Workshop (SKM)*, 2006.
- *South Central Information Security Symposium (SCISS)*, 2003, 2004, and 2005.
- Conference organization activities:
 - Chair, *IEEE Symposium on Security and Privacy*, May 2005.
 - Vice-chair, *IEEE Symposium on Security and Privacy*, May 2004.
 - Founder and organizer of the *South Central Information Security Symposium (SCISS '03)*, held at UNT in April 2003 (also a key organizer in the SCISS '04 in Houston, and SCISS '05 in Austin).
 - Chair (jointly with Wolfgang Bein of UTD) of the *Symposium on the Theory of Computing (STOC)*, held May 1998 in Dallas, TX.
 - Co-organizer of the *Workshop on Data and Image Compression Needs and Uses in the Scientific Community*, held Dec. 1992 in Greenbelt, MD (organized with Jim Tilton of NASA).
- Recent at-conference activities (session chair, etc.):
 - Session chair, *The 4th International Conference on Internet Computing*, 2003.
 - Session chair, *Information Assurance and Security*, 2004.
 - Session chair, *The 7th International Conference on Information Security (ISC)*, 2004.
- Participated in Microsoft Academic Days (Toronto, May 2005) and Microsoft Research Faculty Summit (Redmond, July 2005).
- Member of the SIGACT Electronic Publications Board — managed electronic conference submissions server 1997 – 2002.

HONORS AND AWARDS

- Recognized at UNT Board of Regents Luncheon (February 2004) for federal certifications (CNSS 4011 and 4013) for computer security course sequence.
- Created computer security program which won recognition from the National Security Agency (NSA) and the Department of Homeland Security (DHS) for UNT as a “Center of Academic Excellence in Information Assurance Education.”
- Received the “National Security Award” at the Fall 2004 Faculty Convocation — included receiving a certificate of recognition from Texas Governor Rick Perry.
- Ph.D. student Ke Xu received the “Best Dissertation Award” in the College of Engineering, 2005.

COMMITTEES

- C.S. Department Personnel Affairs Committee (Sep 1999 – May 2001, Sep 2002 – present; *Chair*: Sep 2000 – May 2001, Sep 2002 – Aug 2004)
- C.S. Department Research Enhancement Committee (Sep 2001 – Dec 2001, Sep 2002 – Aug 2005, Sep 2006 – present)
- C.S. Department Faculty Search Committee (Sep 1996 – Aug 1998, Sep 2002 – May 2003, Sep 2005 – Aug 2006)
- C.S. Department Graduate Committee (Sep 1993 – Aug 1994, Sep 1995 – Aug 2001; *Chair*: Sep 1996 – Aug 2001, Sep 2004 – Aug 2005, Sep 2006 – present)
- C.S. Department Undergraduate Committee (Sep 1994–Aug 1996, Sep 2001 – Dec 2001)
- C.S. Department Executive Committee (July 1995 – Aug 2000, Sep 2005 – present)
- Ad-hoc Department PhD Program Evaluation Committee (Sep 2005 – Aug 2006)
- Ad-hoc Department Committee on Merit Evaluation(May 2006 – present)
- C.S. Department Chair Search Committee (Oct 1999 – May 2001)
- Member of the Executive Committee, *Texas Center for Digital Knowledge (TxCDK)*, Nov 2003 – Aug 2005.
- Math Department Faculty Search Committee, external member (Sep 1999 – Aug 2000)
- UNT Committee for Implementation of Electronic Transmission of Theses and Dissertations (Dec 1997 – May 1998)
- UNT College of Engineering Founding Dean Search Committee (May 2002 – Dec 2002)
- College of Engineering tenure appeal committee member, Spring 2004.
- College of Engineering dismissal appeal committee member, Spring 2005.

Other service:

- Computer Science Graduate Coordinator/Advisor and chair of the graduate committee (Sep 1996 – Aug 2001).
- Area coordinator for Algorithms comprehensive exam. Spring 1994, Spring 1996, Fall 1996, Spring 1998, Spring 2001, Fall 2002, Fall 2004.
- Faculty advisor for the Computer Science Graduate Student Association (Dec 1996 – May 1998).
- Faculty advisor for the student ACM chapter (Feb 1995 – Aug 2001).

- Served as official Computer Science contact to the College of Education (Feb 1995 – Jan 1998). Involved preparation of materials for COE review by the National Council for Accreditation of Teacher Education (NCATE).

GRANTS, CONTRACTS, AND OTHER FUNDING (only funded proposals listed)

- June 1994 – Aug 1994, *A Proposal for Research on Molecular Dynamics Algorithms*, UNT Junior Faculty Summer Research Fellowship, \$3,500.
- July 1994 – July 1998, *On-Line and Dynamic Algorithms: Computing with an Uncertain Future*, National Science Foundation, \$67,544.
- Jan 1998 – Aug 2000, *Exploiting Coordinate Representation in Non-uniform Spatial Decomposition*, Texas Advanced Research Program, \$91,076.
- Dec 2001, UNT Faculty Research Grant to support establishment of the *Computer Privacy and Security (CoPS) Lab*, \$3,400.
- June 2002, Equipment donation from Intrusion.com, estimated value: \$6,000.
- Aug 2002 – July 2006, *Mobile Agent Security Through Multi-Agent Protocols*, National Science Foundation, \$249,222 (plus \$3,840 supplement for SCISS '03 support).
- July 2005 – June 2007, *Recruiting and Retention Strategies for Computer Science at UNT*, Texas Higher Education Coordinating Board, Texas Technology Workforce Development Grant, \$125,322 (Investigator; with PIs Robert Akl and David Keathly, and other Investigators Krishna Kavi, Kathleen Swigger, and Philip Sweany).
- Sep 2006 – Aug 2008, *Collaborative Research: A Regional Partnership to Build and Strengthen IA in North Texas*, National Science Foundation, \$247,183 (total budget — UNT portion is \$128,106); Principal Investigator; with co-PIs Ram Dantu and Matt Wright (University of Texas at Arlington).

PUBLICATIONS

Refereed Journal Papers:

1. J. H. Reif and S. R. Tate. "Optimal Size Integer Division Circuits", *SIAM Journal on Computing*, Vol. 19, No. 5, October 1990, pp. 912–924.
2. M. Kao and S. R. Tate. "Online Matching with Blocked Input", *Information Processing Letters*, Vol. 38, May 1991, pp. 113–116.
3. J. H. Reif and S. R. Tate. "On Threshold Circuits and Polynomial Computation", *SIAM Journal on Computing*, Vol. 21, No. 5, October 1992, pp. 896–908.
4. J. H. Reif and S. R. Tate. "Continuous Alternation", *Algorithmica*, Vol. 10, 1993, pp. 151–181.
5. J. H. Reif and S. R. Tate. "Approximate Kinodynamic Planning Using L_2 -norm Dynamic Bounds", *Computers and Mathematics with Applications*, Vol. 27, No. 5, 1994, pp. 29–44.

6. S. R. Tate. “Stable Computation of the Complex Roots of Unity”, *IEEE Transactions on Signal Processing*, Vol. 43, No. 7, 1995, pp. 1709–1711.
7. M. Kao, J. H. Reif, and S. R. Tate. “Searching in an Unknown Environment: An Optimal Randomized Algorithm for the Cow-Path Problem”, *Information and Computation*, Vol. 133, No. 1, 1996, pp. 63–80.
8. J. H. Reif and S. R. Tate. “On Dynamic Algorithms for Algebraic Problems”, *Journal of Algorithms*, Vol. 22, No. 2, 1997, pp. 347–371.
9. S. R. Tate. “Band Ordering in Lossless Compression of Multispectral Images”, *IEEE Transactions on Computers*, Vol. 46, No. 4, 1997, pp. 477–483.
10. M.-Y. Kao and S. R. Tate. “On-Line Difference Maximization”, *SIAM Journal on Discrete Mathematics*, Vol. 12, No. 1, 1999, pp. 78–90.
11. J. H. Reif and S. R. Tate. “Fast Spatial Decomposition and Closest Pair Computation for Limited Precision Input”, *Algorithmica*, Vol. 28, 2000, pp. 271–287.
12. M.-Y. Kao and S. R. Tate. “Designing Proxies for Stock Market Indices is Computationally Hard,” *Quantitative Finance*, Volume 1, Number 3, May 2001, pp. 361-371.
13. S. P. Joglekar and S. R. Tate. “ProtoMon: Embedded Monitors for Cryptographic Protocol Intrusion Detection and Prevention,” *Journal of Universal Computer Science (JUCS)*, Vol. 11, No. 1, 2005, pp. 83–103.

Book chapters:

14. S. R. Tate. “Newton Iteration and Integer Division”, Chapter 12 in *Synthesis of Parallel Algorithms*, edited by John H. Reif, pp. 539–572, 1993. San Mateo, CA: Morgan Kaufmann Publishers.
15. S. R. Tate. “Complexity Measures”, Chapter 2 in the *Lossless Compression Handbook*, Khalid Sayood editor, Academic Press, 2002.
16. M.-Y. Kao, A. Nolte, and S. R. Tate. “The risk profile problem for stock portfolio optimization,” Chapter 11 in *Computational Methods in Decision-Making, Economics, and Finance*, Erricos Kon-toghiorghes, Berc Rustem, and Stavros Siokos editors, by Kluwer Academic Publishers, 2002, pp. 211–228.

Refereed conference publications:

17. J. H. Reif and S. R. Tate. “Optimal Size Integer Division Circuits”, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC)*, 1989, pp. 264–270.
18. V. Pan, J. H. Reif, and S. R. Tate. “The Power of Combining the Techniques of Algebraic and Numerical Computing: Improved Approximate Multipoint Polynomial Evaluation and Improved Multipole Algorithms”, *Proceedings of the 33rd Annual Symposium on Foundations of Computer Science (FOCS)*, 1992, pp. 703–713.

19. M. Kao, J. H. Reif, and S. R. Tate. "Searching in an Unknown Environment: An Optimal Randomized Algorithm for the Cow-Path Problem", *Proceedings of the Fourth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 1993, pp. 441–447.
20. J. H. Reif and S. R. Tate. "The Complexity N -body Simulation", *20th Annual International Conference on Automata, Languages, and Programming (ICALP)*, 1993, pp. 162–176.
21. J. H. Reif and S. R. Tate. "Dynamic Algebraic Algorithms", *Proceedings of the Fifth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 1994, pp. 290–301.
22. S. R. Tate. "Band Ordering in Lossless Compression of Multispectral Images", *Proceedings of the Data Compression Conference (DCC)*, 1994, pp. 311–320.
23. J. H. Reif and S. R. Tate. "Dynamic Parallel Tree Contraction", *Proceedings of the Symposium on Parallel Algorithms and Architecture (SPAA)*, 1994, pp. 114–121.
24. M.-Y. Kao and S. R. Tate. "On-Line Difference Maximization", *Proceedings of the Eighth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 1997, pp. 175–182.
25. B. Chapin and S. R. Tate. "Higher Compression from the Burrows-Wheeler Transform by Modified Sorting", *Proceedings of the Data Compression Conference (DCC)*, 1998, p. 532.
26. M.-Y. Kao and S. R. Tate. "Designing Proxies for Stock Market Indices is Computationally Hard", *Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 1999, pp. 933–934.
27. S. R. Tate and K. Xu. "General-Purpose Spatial Decomposition Algorithms: Experimental Results", *Proceedings of the 2nd Workshop on Algorithm Engineering and Experimentation (ALENEX)*, 2000, pp. 197–216.
28. M.-Y. Kao, A. Nolte, and S. R. Tate. "The Risk Profile Problem for Stock Portfolio Optimization," *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC)*, 2000, pp. 228-234.
29. S. R. Tate and K. Xu. "Mobile Code Security Through Multi-Agent Cryptographic Protocols," *Proceedings of the 4th International Conference on Internet Computing*, 2003, pp. 462–468.
30. S. P. Joglekar and S. R. Tate. "ProtoMon: Embedded Monitors for Cryptographic Protocol Intrusion Detection and Prevention," *Proceedings of the 2004 IEEE Conference on Information Technology: Coding and Computing (ITCC), Information Assurance and Security Track*, 2004, pp. 81–88.
31. V. Gunupudi and S. R. Tate. "Performance Evaluation of Data Integrity Mechanisms for Mobile Agents," *Proceedings of the 2004 IEEE Conference on Information Technology: Coding and Computing (ITCC), Information Assurance and Security Track*, 2004, pp. 62–69.
32. K. Xu and S. R. Tate. "Universally Composable Secure Mobile Agent Computation," *Proceedings of the 7th International Conference on Information Security (ISC)*, 2004, pp. 304–317.

33. V. Gunupudi and S. R. Tate. "SAgent: A Security Framework for JADE," *Proceedings of the 5th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, 2006, pp. 1116–1118.
34. H. Ge and S. R. Tate. "Efficient Authenticated Key-Exchange for Devices with a Trusted Manager," *Proceedings of the 3rd IEEE International Conference on Information Technology (ITNG) – Embedded Cryptographic Systems track*, 2006, pp. 198–203.
35. H. Ge and S. R. Tate. "A Group Signature Scheme with Signature Claiming and Variable Linkability," *Proceedings of the 25th IEEE International Performance, Computing, and Communications Conference (IPCCC)*, 2006, pp. 497–504.
36. H. Ge and S. R. Tate. "Traceable Signature: Better Efficiency and Beyond," *Proceedings of Applied Cryptography and Information Security (ACIS)*, 2006, pp. 327–337.
37. V. Gunupudi, S. R. Tate, and K. Xu. "Experimental Evaluation of Security Protocols in SAgent," *Proceedings of the International Workshop on Privacy and Security in Agent-based Collaborative Environments (PSACE)*, 2006, pp. 60–74.
38. V. Gunupudi and S. R. Tate. "Exploring Data Integrity Protection in SAgent," *Proceedings of the International Workshop on Privacy and Security in Agent-based Collaborative Environments (PSACE)*, 2006, pp. 35–49.
39. V. Gunupudi and S. R. Tate. "Design of the SAgent Security Framework for JADE," *Proceedings of the 18th Annual IASTED International Conference on Parallel and Distributed Computing and Systems (PDCS)*, 2006, pp. 90–95.
40. H. Ge and S. R. Tate. "A Direct Anonymous Attestation Scheme for Embedded Devices," *Proceedings of the 10th International Conference on Theory and Practice of Public-Key Cryptography (PKC)*, 2007, to appear.

Thesis:

41. S. R. Tate. "Arithmetic Circuit Complexity and Motion Planning", Ph. D. Dissertation, Duke University, 1991.

Technical reports, manuscripts:

42. S. R. Tate. "Lossless Compression of Region Edge Maps," Duke University Computer Science Technical Report CS-1992-09.
43. S. R. Tate. "Report on the Workshop on Data and Image Compression Needs and Uses in the Scientific Community," CESDIS Technical Report TR-93-99.
44. J. H. Reif and S. R. Tate. "*N*-body Simulation I: Fast Algorithms for Potential Field Evaluation and Trummer's Problem," University of North Texas Technical Report N-96-002, 1996.
45. J. H. Reif and S. R. Tate. "*N*-body Simulation II: Simulation of Moving Particles," University of North Texas Technical Report N-96-003, 1996.

46. S. R. Tate and K. Xu. "On Garbled Circuits and Constant Round Secure Function Evaluation," CoPS Lab Technical Report 2003-02, 2003.

Book reviews:

47. S. R. Tate. Review of *Polynomial and Matrix Computations; Volume 1: Fundamental Algorithms* by Dario Bini and Victor Pan. Appeared in *SIGACT News*, Vol. 26, No. 2, June 1995.

Other recent presentations and non-peer reviewed publications:

- "Mobile Agent Security Through Multi-Agent Protocols," poster presentation at the NSF Cyber Trust Point Meeting, Baltimore, MD, August 2003.
- S. R. Tate and K. Xu. "Some Security Issues in a Garbled Circuit Construction," CRYPTO '03 Rump Session Presentation, 2003.
- V. Gunupudi and S. R. Tate. "A Flexible Object-Oriented Approach to Data Integrity in Mobile Agents," *South Central Information Security Symposium*, April 2003.
- K. Xu and S. R. Tate. "Privacy of Mobile Agent Data on Malicious Hosts Using Multi-Agent Protocols," *South Central Information Security Symposium*, April 2003.
- Invited presentation: "Mobile Agent Computation with Secret Data," the University of Texas at Arlington, April 2003.
- S. R. Tate and K. Xu. "On Garbled Circuits and Constant Round Secure Function Evaluation," CoPS Lab Technical Report 2003-02.
- K. Xu and S. R. Tate. "Universally Composable Secure Mobile Agent Computation," *South Central Information Security Symposium*, April 2004.
- Invited presentation: "Security Protections for Mobile Agents," Southern Methodist University, August 2004.
- V. Gunupudi and S. R. Tate. "A Security Framework for the JADE Mobile Agent Platform," *South Central Information Security Symposium*, April 2005.
- F. Chang, G. White, and S. Tate. "How to Build Lab Exercises and Capture the Flag Activities", panel at the *9th Colloquium for Information Systems Security Education*, June 2005. (Our panel received the highest evaluation of any presentation or panel at this 4-day colloquium.)

REFEREE WORK

Refereed many papers for journals and conferences, including *SIAM Journal on Computing*, *Journal of Algorithms*, *Algorithmica*, *Information and Computation*, *Journal of Combinatorial Optimization*, *Journal of Systems and Software*, *Journal of Universal Computer Science*, the *ACM-SIAM Symposium on Discrete Algorithms*, *Computers and Mathematics with Applications*, *IEEE*

Trans. on Information Theory, IEEE Trans. on Parallel and Distributed Processing, IEEE Trans. on Image Processing, IEEE Trans. on Computers, Parallel Processing Letters, Information Processing Letters, the Internet Encyclopedia, The Handbook of Information Security, the Symposium on Theoretical Aspects of Computer Science, the Workshop on Wireless Mobile Multimedia, the Journal of Visual Communication and Image Representation, the IEEE International Conference on Information Reuse and Integration, the IEEE International Conference on Information Technology: Coding and Computing (ITCC), the International Parallel Processing Symposium, and the ACM Computer Science Conference.

Served on NSF Review Panel for the Experimental Partnership Program, Washington, DC (June 2000).

Served on NSF Review Panel for Cybertrust CAREER Awards, Washington, DC (November 2003).

Served on NSF Review Panel for Cybertrust Program, Washington, DC (June 2006).

Reviewed books and book chapters for *Introduction to Data Compression* by Khalid Sayood, *Cryptography and Network Security: Principles and Practice* by William Stallings, and others.

TEACHING

- Experience teaching a wide range of courses, including introductory undergraduate courses, assembly language, data structures, file structures, cryptography, computer security and secure electronic commerce courses (both undergraduate and graduate), undergraduate and graduate algorithms, and several advanced graduate seminars (topics: data compression, on-line algorithms, randomized algorithms, Java and network security, and cryptography and security).
- Participated in teaching workshops on secure electronic commerce and network security (Washington D.C., March 2003; Tulsa, OK, July 2003).
- Designed and established a multi-course sequence in computer security at both undergraduate and graduate levels. Applied for and received two federal certifications, showing a mapping of our computer security courses to two the Committee for National Security Systems (CNSS) training standards 4011 (for Information Security Professionals) and 4013 (for Secure System Administration).
- Organized and supervised a group of three graduate students in the *Honeynet Reverse Engineering Challenge*, placing second in this international competition (May–June 2002).
- Organized and coached a team of 8 students (including 2 from the Department of Information Technology and Decision Sciences) for participation in the *1st Texas Collegiate Cyber Defense Contest*, San Antonio, April 2005 (travel funding from Microsoft).
- Organized and supervised a group of 6 directed study students who performed a formal security audit of the Department of Computer Science systems and network (Fall 2005).
- Three graduated Ph.D. students (Brent Chapin, 2001; Ke Xu, 2004; He Ge, 2006), and two current Ph.D. students.

- Served or currently serving on 18 Ph.D. committees and 7 Master's committee at UNT (other than my own students).
- External reviewer and Ph.D. committee member for a student (Elliott Landowne) at the City University of New York.
- Supervised students (both at undergraduate and graduate levels) in directed study and independent projects.

SOFTWARE

Major port of PPP (Point-to-Point Protocol) software to DEC OSF/1, including kernel drivers and user-level support software. This software has been widely distributed, being obtained by users from many other states and foreign countries, and was subsequently included with the official distribution of Digital UNIX (beginning with version 4.0). Last version released by me November, 1996.

Graphical policy browser/analyzer for Security-Enhanced Linux. Last version released March, 2002. Available at <http://cops.csci.unt.edu/projects/selinux/main.html>

SAgent security framework for the JADE mobile agent platform (over 10,000 lines of code). Available at <http://cops.csci.unt.edu/sagent>.