

October 21, 2002

Curriculum Vitae

Neal R. Wagner

Work Address: Division of Computer Science, The University of Texas at San Antonio, San Antonio, Texas 78249, (210)458-5550.

Personal: Married to Deborah L. Callanan.

Education:

Ph.D., University of Illinois at Urbana-Champaign, 1970. Major: mathematics, minor: German.

M.A., University of Illinois at Urbana-Champaign, 1964. Major: mathematics.

Fulbright grant, Universität Hamburg, Germany, 1962-63.

B.A., University of Kansas, 1962. Majors: mathematics and English.

Employment:

1987-present: *Associate Professor*, Division of Computer Science; and Division of Mathematics, Computer Science, and Statistics, The University of Texas at San Antonio. (Acted as Chairman of the Search Committee for hiring new faculty, Graduate Advisor for Computer Science, Chairman of the Computer Science Graduate Studies Committee, member of the University Council on Graduate Education. Took care of extensive revisions and additions to the Undergraduate and Graduate Bulletins. Served in various roles in the Computer Science Information Security Laboratory.)

1981-1987: *Associate Professor of Computer Science*, Department of Mathematics and Computer Science, Drexel University. (As Chairman of the Computer Science Curriculum Committee, completely redesigned the undergraduate CS curriculum. Coordinated design of the proposed Ph.D. in Computer Science. Acted as coordinator for the evaluation of the Computer Science Program by the Computer Science Accreditation Commission. Did most of the work associated with filling out the evaluation questionnaire. Served as Chairman of the Search Committee for a department head.)

1979-1981: *Visiting Associate Professor*, Computer Science Department, University of Houston. (Developed undergraduate curricula.)

1976-1979: *Associate Professor*, Mathematical Sciences Department, University of Texas at El Paso. (Helped create an interdisciplinary degree in computer science. Served as Computer Science Advisor. Acted as Local Arrangements Chairman for ACM regional meeting.)

1975-1976: *Applications Programming Group Leader*, Singer/Link, Simulation Products Division, Johnson Space Center, Houston. (In charge of all applications programming for two real-time Space Shuttle simulations.)

1974-1975: *Programmer/Analyst*, Singer/Link. (Real-time simulation of the Space Shuttle.)

1969-1974: *Assistant and Associate Professor*, Mathematics Department, University of Texas at El Paso. (Served as Graduate Advisor.)

Research Grants:

1. Grant from the National Science Foundation, 1990-1991 (with K. Robbins (PI), and S. Robbins (CO-PI)). Title: *Concurrency Experiments in a UNIX Environment*. (Partly an equipment grant an advanced workstation laboratory.) Amount: \$91,000.
2. Grant from the Advanced Research Program off the State of Texas, 1988-1990. Title: *Non-linear Dynamics in Random Number Generation and Cryptography*. (An investigation of encryption methods and random number generation methods based on chaotic phenomena.) Amount: \$17,621.00.
3. Research Scholar award from Drexel University, 1985. Title: *New Approaches to Public Key Cryptosystems*. (Looking at the use of problems harder than NP-complete as the basis for a public key cryptosystem.) Amount: \$5000.00 plus a research assistant and release time.
4. National Science Foundation Grant DCR-8403350, 1984-1987. Title: *Database Security*. (The study of several approaches to database security, including the use of cryptography in a fundamental way and the use of fingerprinting.) Amount: \$54,100.00.
5. Grant from Siemens Corporation of New Jersey for research in cryptography and data security, 1981-1982. Title: *A Cryptography-based Secure Office System*. (Construction of a prototype secure office system using a hybrid of DES and RSA cryptography.) Amount: \$10,000.00. (Because of patent difficulties with Drexel University, this was converted to a straight fee.)
6. Faculty research grant from Drexel Univ., 1982-1983. Title: *Secure Personal Workstations*. Amount: \$2,500.00.
7. Faculty summer research grant from Univ. of Texas at El Paso, 1972.
8. NSF Undergraduate Research Grant, 1961.

Membership in Professional Societies:

Association for Computing Machinery

IEEE Computer Society

Mathematical Association of America

Honors:

Acted as referee for various research journals: *American Journal of Mathematics*, *Illinois Journal of Mathematics*, *Pacific Journal of Mathematics*, *ACM Transactions on Computer Systems*, *ACM Transactions on Database Systems*, *Information Processing Letters*, *The Journal of Cryptology*, *IEEE Computer*.

Served as reviewer for *Mathematical Reviews*, *Computing Reviews*.

Served as reviewer for NSF grant proposals.

Received NSF Fellowship and NSF Research Assistantship.

SUPERVISION OF STUDENTS:

Ms. Marianne R. Cain, supported by grant money as a Graduate Research Assistant for 2 years. Work carried out includes Publications 18, 20, 21 and 22.

Plus numerous undergraduate Senior Projects and graduate research projects.

Invited Presentations and Lectures:

1982 National Computer Conference, Houston, Texas.

1982 Symposium on Security and Privacy, Berkeley, California.

Crypto 82 Workshop in Cryptography, Santa Barbara, California.

1983 Symposium on Security and Privacy, Berkeley, California.

1984 Symposium on Security and Privacy, Berkeley, California.

Crypto 84 Workshop in Cryptography, Santa Barbara, California.

Eurocrypt 85 Workshop in Cryptography, Linz, Austria.

Crypto 86 Workshop in Cryptography, Santa Barbara, California.

Sixth International Conf. on Data Engineering, Los Angeles, California (February, 1990).

Second Annual IEEE Symposium on Parallel & Distributed Processing, Dallas, Texas (December, 1990).

Business Ethics Symposium III, San Antonio, Texas (February, 1992).

Thirtieth Annual Allerton Conference on Communications, Control, and Computing, Monticello, Illinois (September, 1992).

Plus four mathematics talks at meetings of the American Mathematical Society.

Plus numerous invited colloquium talks at universities (at least 9 universities and 14 talks).

Graduate Courses Taught:

Topology (1 semester)
Real Analysis (2 semesters)
Theory of Algorithms (3 quarters and 1 semester)
Cryptography and Data Security (2 quarters)
Compiler Construction (2 quarters)
Data Base Management Systems (2 semesters)
Network Security (1 semester)

Undergraduate Courses Taught:

Programming courses in Pascal, PL/I, Fortran, Basic, Lisp, C, Java
Second courses in programming.
Data Structures.
Assembler Language.
Computer Systems Architecture (2 quarters, emphasizing PDP-11).
Programming Languages.
Operating Systems (several versions, including one based on UNIX, C, and MINIX).
Software Engineering (1 semester and 2 quarter courses).
Compiler Theory (mainly language theory and parsing).
Compiler Workshop (project oriented).
Theory of Algorithms.
Cryptography.
Information Theory.
Ethical and Social Issues in Computer Science (see book project below).
Data Base Management Systems.
Plus numerous undergraduate mathematics courses.

Book Projects:

1. *The Laws of Cryptography, with Java Code*. An unusual book on cryptography emphasizing mathematics for the uninitiated and covering information theory.
2. *Walden Three: What if Crime Were Impossible? The Use of Computer Technology*. This is intended as a popular book for the educated public.
3. *Ethical and Social Issues in Computer Science* (with Dr. Myles McNally). This was to be an innovative college textbook with technically oriented material suitable for

computer science majors. The book is on hold at present.

Publications:

1. Wagner, N.R. "The space of retractions of the 2-sphere and the annulus," *Transactions of the American Mathematical Society*, Vol. 158 (1971), No. 2, pp. 319–329.
2. Wagner, N.R. "The space of retractions of a 2-manifold," *Proceedings of the American Mathematical Society*, Vol. 34 (1972), No. 2, pp. 609–614.
3. Wagner, N.R. "Constructions with pentacubes," *Journal of Recreational Mathematics*, Vol. 5 (1972), No. 4, pp. 266–268.
4. Wagner, N.R. "Constructions with pentacubes II," *Journal of Recreational Mathematics*, Vol. 6 (1973), No. 3, pp. 211–214.
5. Wagner, N.R. "A continuity property and surface topology," *Bulletin of the American Mathematical Society*, Vol. 79 (1973), No. 6, pp. 1308–1311.
6. Wagner, N.R. "A continuity property with applications to the topology of 2-manifolds," *Transactions of the American Mathematical Society*, Vol. 200 (1975), pp. 369–393.
7. Deter, R.L. and Wagner, N.R. "Mathematical modeling of early pre-implantation embryogenesis in mice," *Journal of Cell Biology*, Vol. 67 (1975), p. 93a. (Abstract)
8. Wagner, N.R. "The sofa problem," *American Mathematical Monthly*, Vol. 83 (1976), No. 3, pp. 188–189.
9. Wagner, N.R. "A computer search for integer values of 2^{*c} and 3^{*c} ." (Unpublished manuscript. Results announced in the *American Mathematical Monthly*, Vol. 84 (1977), No. 10, p. 811.)
10. Wagner, N.R. "The faceless clock," *Mathematics Teacher*, Vol. 70 (1977), No. 9, p. 765. (Short note.)
11. Coyne, R.A. and Wagner, N.R. *User's Guide to UTEP's IBM 360*, University of Texas at El Paso, 1979. (60-page user manual.)
12. Wagner, N.R. "A Fortran preprocessor for the large program environment," *SIGPLAN Notices*, Vol. 15 (1980), No. 12, pp. 92–103.
13. Müller-Schloer, C. and Wagner, N.R. "The implementation of a cryptography-based secure office system," *AFIPS Conference Proceedings: 1982 National Computer Conference* (Houston, Texas), AFIPS Press, pp. 487–492.

14. Wagner, N.R. "Shared database access using composed encryption functions," *Proceedings of the 1982 Symposium on Security and Privacy*, IEEE Computer Society, pp. 104–110.
15. Müller-Schloer, C. and Wagner, N.R. "Cryptographic protection of personal data cards," *Advances in Cryptology: Proceedings of Crypto 82*, ed. by D. Chaum et al., Plenum Press, 1983, pp. 219–229.
16. Wagner, N.R. "Fingerprinting," *Proceedings of the 1983 Symposium on Security and Privacy*, IEEE Computer Society, pp. 18–22.
17. Wagner, N.R. "Searching for public-key cryptosystems," *Proceedings of the 1984 Symposium on Security and Privacy*, IEEE Computer Society, pp. 91–98.
18. Wagner, N.R. and Magyarik, M.R., "A public-key cryptosystem based on the word problem," *Advances in Cryptology: Proceedings of Crypto 84, Lecture Notes in Computer Science No. 196*, ed. by G.R. Blakley and D. Chaum, Springer Verlag, pp. 19–36.
19. Putter, P.S., and Wagner, N.R. "Technical Correspondence" (related to the article "Pass Algorithms"), *Communications of the ACM*, Vol. 28 (1985), No. 7, p. 750.
20. Wagner, N.R., Putter, P.S., and Cain, M.R., "Using algorithms as keys in cryptosystems," *Proceedings of Eurocrypt 85, Lecture Notes in Computer Science No. 219*, ed. by F. Pichler, Springer Verlag, pp. 149–155.
21. Wagner, N.R., Putter, P.S., and Cain, M.R., "Encrypted database design: Specialized approaches," *Proceedings of the 1986 Symposium on Security and Privacy*, IEEE Computer Society, pp. 148–153.
22. Wagner, N.R., Putter, P.S., and Cain, M.R., "Large scale randomization techniques in cryptography," *Advances in Cryptology—Crypto 86, Lecture Notes in Computer Science No. 263*, Springer Verlag, 1986, pp. 393–404.
23. Wagner, N.R., "Technical Correspondence" (related to the article "Novel Security Techniques for On-line Systems"), *Communications of the ACM*, Vol. 29 (1986), No. 12, pp. 1240–1241.
24. Wagner, N.R., and Putter, P.S., "Error detecting decimal digits," *Communications of the ACM*, Vol. 32, No. 1 (Jan., 1989), pp. 106–110.
25. Robbins, K.A., Wagner, N.R., and Wenzel, D.J., "Virtual rings: an introduction to concurrency," *SIGCSE Bulletin*, Vol. 21, No. 2 (June, 1989), pp. 23–28.

26. Wagner, N.R., and Putter, P.S., “Authors’ Response” to “Technical Correspondence” (related to the article “Error detecting decimal digits”), *Communications of the ACM*, Vol. 32 (1986), No. 9, pp. 1132.
27. Wagner, N.R., Fountain, R. L., and Hazy, R.J., “The fingerprinted database,” *Sixth International Conference on Data Engineering: Proceedings*, IEEE Computer Society Press, 1990, pp. 330–336.
28. Wagner, N.R., “Randomized fault-detecting leader election in a bi-directional ring,” *Proceedings of the Second Annual IEEE Symposium on Parallel & Distributed Processing*, IEEE Computer Society Press, 1990, pp. 506–510.
29. Wagner, N.R., “The logistic lattice in random number generation,” *Proceedings of the Thirtieth Annual Allerton Conference on Communications, Control, and Computing*, Coordinated Science Lab and Department of Electrical and Computer Engineering, University of Illinois at Urbahn-Champaign, 1993, pp. 922–931.