List of Scholarly and Creative Works

February 21, 2008

Alan Theodore Sherman

Contents

1 Overview

1.1 My Four Favorite Publications

- Kaliski, Burton S. Jr., Ronald L. Rivest, and Alan T. Sherman, "Is the Data Encryption Standard a group? (Results of cycling experiments on DES)," *Journal of Cryptology*, **1**:1 (1988), 3–36.

  Using a combination of software and special-purpose hardware, we carried out novel cycling experiments on DES to determine if DES has certain extreme algebraic weaknesses. Probabilistic analyses of our experimental results show, with overwhelming confidence, that the set of DES transformations does not form a group under functional composition. In addition, we unexpectedly discovered fixed points for each of the so-called "weak-key" transformations, and we developed new cryptanalytic attacks against group ciphers. This work is of special interest for its integration of algebra, algorithm design, probabilistic analysis, and special-purpose hardware.

  I have presented this work at Eurocrypt 85, Johns Hopkins University, and other universities. Rivest presented parts of this work at Crypto 85.

- Sherman, Alan T., *VLSI Placement and Routing: The PI Project*, Springer-Verlag (New York, 1989). 189 pages.

  The *PI (Placement and Interconnect) System* is an experimental system for laying out custom VLSI chips. It was the first system to automate completely the entire layout process. The PI System decomposes the layout process into separate subproblems and solves each subproblem using a special-purpose heuristic. The major contributions of PI are its novel problem decomposition and its new and effective component algorithms. Several ideas and component algorithms from the PI System have been used in industrial layout systems. As a key student member of this project, I designed and implemented the placement heuristics. This book describes how PI works and uncovers many of the thoughts, issues, and considerations that went into the design and implementation of PI.

  I have presented this work at several universities, including Brandeis and University of Maryland, College Park.

- Cain, Thomas, and Alan T. Sherman, "How to break Gifford's Cipher," *Cryptologia* (July 1997), **XXI**:3 (July 1997), 237–286.

  We present and implement a ciphertext-only algorithm to break Gifford's cipher, a stream cipher designed in 1984 by David Gifford of MIT and used to encrypt *New York Times* and *Associated Press* wire reports. The cipher consists of a linear feedback shift register with nonlinear output. Applying linear algebra over finite fields, we exploit a novel hashing technique to determine key segments derived from the primary rational canonical decomposition of the feedback function. Our attack runs in 2^{27} steps and 2^{18} bytes of memory, which is a significant shortcut over the 2^{64} steps required for a straightforward exhaustive search of all initial fills. Given ciphertext only from one encrypted article, our prototype implementation running on a loosely-coupled network of eight Sparcstations finds the article key within approximately four hours on average. This work, the first proposed attack on Gifford's cipher, illustrates the power of algebraic decompositions and provides a detailed instructive example of how to apply linear algebra over *GF*(2) in cryptanalysis.

  I have presented this work at AT&T Bell Labs, Crypto 94 (rump session), MIT, and other universities. Cain presented this work at the 1994 ACM Conference on Computer and Communications Security.

- McGrew, David A., and Alan T. Sherman, "Key establishment in large dynamic groups using one-way function trees" (May 20, 1998, revised June 29, 2001), *IEEE Transactions on Software Engineering*, 29:5 (May 2003), 444–58.

  We present, implement, and analyze a new scalable algorithm for establishing shared cryptographic keys in large, dynamically changing groups. Our algorithm is based on a novel application of one-way function trees. In comparison with the logical key hierarchy (LKH) method of Wallner, *et al.*, our algorithm approximately halves the numnber of bits that need to be broadcast to members in order to re-key after a member is added or evicted. The number of keys stored by group members, the number of keys broadcast to the group when new members are added or evicted, and the computational efforts of group members are logarithmic in the number of group operations. Our algorithm provides complete forward and backward security: newly admitted group members cannot read previous messages, and evicted members cannot read future messages, even with collusion by arbitrary many evicted members. In addition, and unlike LKH, our algorithm has the option of being member contributory in that members can be allowed to contribute entropy to the group key. Running on a Pentium with 400 MB of RAM, our prototype has handled groups with up to 10 million members. This algorithm offers a new scalable method for establishing group sessions keys for secure large-group applications such as broadcast encryption, electronic conferences, multicast sessions, military command and control, and broadcast satellite services. This work is especially interesting for its integration of theory and practice and for its ongoing application and adaptation in modified form in a major new worldwide system under development.

  I have presented this work at NSA, DARPA, MIT, and other universities.

1.2 Number of Research Publications

Table 1: Number of major research publications by type.

Publication Type	Published*	In Review	Total
Books authored	1	0	1
Books co-edited	1	0	1
Articles in refereed journals	10	0	10
Other works in refereed journals and magazines	3	0	3
Articles in refereed proceedings of competitively-selected conferences	11	0	11
Total:	26	0	26

*Includes papers accepted for publication but still in press.

Table 2: Number of other research works by type (selected).

Publication Type	Published*	In Review	Total
Internet Drafts for the Internet Engineering Task Force (IETF)	2	0	2
Articles in non-refereed journals	2	0	2
Workshop papers at major conferences	1	0	1
Papers in research-community periodicals	4	0	4
Computer music compositions performed in public concerts	1	0	1
Patents	3	2	5
Total:	13	2	15

*Includes papers accepted for publication but still in press.

In addition, several new works are in preparation.

1.3 Author Impact

Table 3: Sherman's ten most cited papers, as measured by Google Scholar on 2-18-08.

Citations	Title	Publisher	Year
196	Key establishment in large dynamic groups	NAI Labs - *IEEE TSE**	1998
46	Note on Bennett's time-space tradeoff	*SIAM Journal on Computing*	1990
33	Is DES a group?	*Journal of Cryptology*	1988
30	An observation on associative one-way functions	*Information Processing Letters*	1997
28	Policy-based security management - DCCM project	DARPA - *DISCEX 2000*	2000
14	Punchscan: Introduction and system definition	*WOTE 06*	2006
14	Techniques for Lang. recog.: Intro & guide	*Cryptologia*	1993
10	Techniques for Lang. recog.: Empirical study	*Cryptologia*	1994
8	Randomized encryption techniques	MIT LCS - *Crypto 82*	1983
8	Exact formula for wirelength	CSEE UMBC - *SIAM Review*	1994

*The version of this paper published in *IEEE Transactions on Software Engineering* was cited 86 times.

h-factor = 8, as computed by Harzing on 2-18-08 (Sherman published at least 8 papers each cited at least 8 times). Note that search engines fail to find many citations prior to the web and from certain publishers.

2 Books

1. Chaum, David, Ronald L. Rivest, and Alan T. Sherman, eds., *Advances in Cryptology: Proceedings of Crypto 82*, Plenum Press (New York, 1983). 331 pages.

2. Sherman, Alan T., *VLSI Placement and Routing: The PI Project*, Springer-Verlag (New York, 1989). 189 pages.

3 Major Research Papers

3.1 Articles in Refereed Journals

3. Kaliski, Burton S. Jr., Ronald L. Rivest, and Alan T. Sherman, "Is the Data Encryption Standard a group? (Results of cycling experiments on DES)," *Journal of Cryptology*, **1**:1 (1988), 3–36.

4. Levine, Robert Y., and Alan T. Sherman, "A note on Bennett's time-space tradeoff for reversible computation," *SIAM Journal on Computing*, **19**:4 (August 1990), 673–677.
   [A preliminary version appears as Technical Report 89-2, Department of Computer Science, Tufts University (May 1989), and in modified form as Technical Report UMIACS-TR-90-63/CS-TR-2467, University of Maryland, College Park (May 1990).]

5. Baldwin, Robert W., and Alan T. Sherman, "How we solved the $100,000 Decipher Puzzle (16 hours too late)," *Cryptologia*, **XXIV**:3 (July 1990), 258–284.
   [A preliminary version appears as Technical Report 89-3, Department of Computer Science, Tufts University, (July 1989), and in modified form as Technical Report UMIACS-TR-90-64/CS-TR-2468, University of Maryland, College Park (May 1990).]

6. Ganesan, Ravi, and Alan T. Sherman, "Statistical techniques for language recognition: An introduction and guide for cryptanalysts," *Cryptologia*, **XVII**:4 (October 1993), 321–366.
   [Preliminary version available as Technical Report CS-TR-3036/UMIACS-TR-93-16, University of Maryland, College Park (February 1993), and as Technical Report TR CS-93-02, University of Maryland, Baltimore County (February 28, 1993).]

7. Konstantinos Kalpakis, and Alan T. Sherman, "Probabilistic analysis of an enhanced partitioning algorithm for the Steiner tree problem in R^d," *Networks*, **24**:3 (May 1994), 147–159.
   [An early version appears as Technical Report CS-TR-2936/UMIACS-TR-92-83, University of Maryland, College Park (July 1992), and in modified form as Technical Report TR CS-93-10, University of Maryland, Baltimore County (July 29, 1992).]

8. Ravada, Sivakumar, and Alan T. Sherman, "Experimental evaluation of a partitioning algorithm for the Steiner tree problem in R^2 and R^3," *Networks*, **24**:8 (December 1994), 409–415.

   [A complete version appears as Technical Report TR CS-93-12, University of Maryland, Baltimore County (June 23, 1993).]

9. Ganesan, Ravi, and Alan T. Sherman, "Statistical techniques for language recognition: An empirical study using real and simulated English," *Cryptologia*, **XVIII**:4 (October 1994), 289–331.

   [A a complete preliminary version (with supplement) appears as Technical Report TR CS-93-03, University of Maryland, Baltimore County (September 28, 1993). 48 pages plus supplement.]

10. Cain, Thomas, and Alan T. Sherman, "How to break Gifford's Cipher" *Cryptologia* **XXI**:3 (July 1997), 237–286.[1]

    [Also appears as Technical Report CS-TR-3298/UMIACS-TR-94-72, University of Maryland, College Park (June 2, 1994), and as Technical Report TR CS-94-7, Computer Science Department, University of Maryland, Baltimore County (June 2, 1994).]

11. Rabi, Muhammad, and Alan T. Sherman, "An observation on associative one-way functions in complexity theory," *Information Processing Letters*, **64**:5 (December 1997), 239–244.

    [A preliminary version appears as "Associative one-way functions: A new paradigm for secret-key agreement and digital signatures" Technical Report CS-TR-3183/UMIACS-TR-93-124, University of Maryland, College Park (July 1993), and as Technical Report TR CS-93-18, Computer Science Department, University of Maryland, Baltimore County (November 15, 1993). 13 pages.]

12. Sherman, Alan T., and David A. McGrew, "Key establishment in large dynamic groups using one-way function trees" *IEEE Transactions on Software Engineering*, 29:5 (May 2003), 444–58.

    [A preliminary version appears as TIS Report No. 0755, TIS Labs at Network Associates, Inc., Glenwood, MD (May 1998). 13 pages.]

3.2 Additional Research Works in Refereed Journals

13. Lazoff, David M., and Alan T. Sherman, "Expected wire length between two randomly chosen terminals," Problem 95-6, *SIAM Review* (June 1995), 235.

    [Available (with solution) as "An exact formula for the expected wire length between two randomly chosen terminals," Technical Report TR CS-94-08, Computer Science Department, University of Maryland, Baltimore County (July 20, 1994). 14 pages.]

14. Kuszmaul, B. C., and A. T. Sherman, "*Socrates 2.0 beats Grandmaster Sagalchik," *International Computer Chess Association Journal* (June 1995), 124–125.

15. Chaum, David, Aleks Essex, Richard Carback, Stefan Popoveniuc, Jeremy Clark, Alan T. Sherman, and Poori Vora, "Scantegrity: Independent End-to-End Verification for Optical

[1]This paper was accepted before I became an editor of *Cryptologia*.

Scan Voting Systems," *IEEE Security & Privacy*, accepted for publication in 2009 special issue on voting (submitted October 2007).

3.3 Articles in Refereed Proceedings of Competitively-Selected Conferences

16. Rivest, Ronald L., and Alan T. Sherman, "Randomized encryption techniques" in *Advances in Cryptology: Proceedings of Crypto 82*, David Chaum, Ronald L. Rivest, and Alan T. Sherman, eds., Plenum Press (New York, 1983), 145–163.

    [Also appears as Technical Memorandum TM-234, MIT Laboratory for Computer Science (January 1983). By agreement with Plenum Press, this paper will not be published elsewhere.]

17. Kaliski, Burton S. Jr., Ronald L. Rivest, and Alan T. Sherman, "Is the Data Encryption Standard a group?" in *Advances in Cryptology: Proceedings of Eurocrypt 85*, Franz Pichler, ed., Springer-Verlag (New York, 1986), 81–95.

18. Kaliski, Burton S. Jr., Ronald L. Rivest, and Alan T. Sherman, "Is the Data Encryption Standard a pure cipher? (Results of more cycling experiments on DES)" in *Advances in Cryptology: Proceedings of Crypto 85*, H. C. Williams, ed., Springer-Verlag (New York, 1986), 212–226.

19. Kalpakis, Konstantinos, and Alan T. Sherman, "Probabilistic analysis of an enhanced partitioning algorithm for the Steiner tree problem in R^d" in *Proceedings of the 13th Annual Allerton Conference on Communication, Control, and Computing*, edited by Paul Van Dooren and Mark Spong, University of Illinois at Urbana-Champaign (1992), 553–564.

20. Cain, Thomas, and Alan T. Sherman, "How to break Gifford's Cipher (extended abstract)," *Second Annual ACM Conference on Computer and Communications Security*, ACM Press (November 2–4, 1994), 198–209.

21. Adcock, Jamison M., David M. Balenson, David W. Carman, Michael Heyman, and Alan T. Sherman, "Trading off strength and performance in network authentication: Experience with the ACSA Project," *Proceedings of the DARPA Information Survivability Conference & Exposition (DISCEX 00)*, IEEE Computer Society (January 25–27, 2000), 127–139.

22. Dinsmore, Pete, David M. Balenson, Michael Heyman, Peter S. Kruus, Caroline D. Scace, and Alan T. Sherman, "Policy-based security management for large dynamic groups: An overview of the DCCM project," *Proceedings of the DARPA Information Survivability Conference & Exposition (DISCEX 00)*, IEEE Computer Society (January 25–27, 2000), 64–73.

23. Sherman, Alan T., Brian O. Roberts, William E. Byrd, Matthew R. Baker, and John Simmons, "Developing and delivering hands-on information assurance exercises: Experiences with the Cyber Defense Lab at UMBC" in *Proceedings from the Fifth IEEE Systems, Man and Cybernetics Information Assurance Workshop*, June 10–11, 2004, West Point, New York (Piscataway, NY, 2004), 242–249.

24. Fisher, Kevin, Richard Carback, and Alan Sherman, "Punchscan: Introduction and system definition of a high-integrity election system" in *Preproceeedings of the IAVoSS Workshop on Trustworthy Elections (WOTE 2006)*, (June 29–30, 2006), Cambridge, England. 8 pages. Accessed 3/21/07 from http://www.punchscan.org/papers/fisher_punchscan_wote2006.pdf

25. Sherman, Alan T., Donald F. Norris, Andrew Sears, Aryya Gangopadhyay, Stephen H. Holden, George Karabatis, A. Gunes Koru, Chris M. Law, John Pinkston, and Dongsong Zhang, "An examination of vote verification technologies: Findings and experiences from the Maryland Study" in *Proceedings of the USENIUSENIX/Accurate Electronic Voting Technology (EVT) Workshop* (August 1, 2006). 15 pages. Accessed 2/18/07 from http://www.usenix.org/events/evt06/tech/

26. Carback, Richard, Stefan Popoveniuc, Alan Sherman, and David Chaum, "Punchscan with independent ballot sheet: Simplifying ballot printing and distribution with independently selected ballot halves," in *On-Line Proceedings of the 2007 IAVoSS Workshop on Trustworthy Elections (WOTE 2007)*, (June 20–22), Ottawa, Canada. Accessed 2-18-08 from http://research.microsoft.com/conferences/WOTE2007/program.htm

4 Research Works in the Pipeline

4.1 Works Submitted for Publication (In Review)

None at this time.

4.2 Works in Preparation (Active)

27. Fink, Russ, Alan Sherman, and Richard Carback, "Reducing the Trusted Base of Electronic Voting Machines with Trusted Platform Modules," (draft: October 2007).

28. Mark, Henry, and Alan T. Sherman, "A unifying theory of the evolution of cognition and mental disorders and a critical role for chess-based psychodiagnostics" (draft: December 9, 2004), 13 pages.

29. Sherman, Alan T., and William Byrd, "Theoretical and experimental evaluation of the Rivest-Sherman attacks on Enigma-like machines: Determining the rotors one at a time from ciphertext only" (draft: August 2003), 60 pages.

4.3 Works in Preparation (Inactive)

30. Carman, David W., and Alan T. Sherman, "KRx: A new family of primitives for fast nested MACs" (draft: March 14, 2000), 11 pages. [This paper describes work I have started at NAI Labs.]

31. Heyman, Michael, and Alan T. Sherman, "Enhancing key trees with reusable power sets" (spring 2001), in preparation. [This paper will describe work I have carried out at NAI Labs.]

32. Sherman, Alan T., and Tim Redman, "Developing a university chess program: The models of the University of Maryland, Baltimore County, and The University of Texas at Dallas," presented at *The Koltanowski Memorial Conference on Chess and Education 2001*, University of Texas at Dallas (December 13–17, 2001), (draft: May 17, 2003), 8 pages.

33. Sherman, Alan T., *Introduction to Discrete Math for Computer Scientists: Theorem-Proving, Calculation, and Counting*, textbook in preparation.

34. Falcone, Anthony J., and Alan T. Sherman, "DTEL: A digital telestrator for spectator chess," (draft: April 2, 2000), 44 pages. For possible submission to *Software Practice and Experience.*

35. Pollack, Ann, and Alan T. Sherman, "The complexity of orienting uniform modules to minimize estimated wire length" (draft: July 19, 1993), 14 pages.

36. Cain, Thomas, and Alan T. Sherman, "Cryptanalysis of filter-generators using the primary rational canonical decomposition of the feedback function," in preparation.

37. Sherman, Alan T., "A simplified approach to probabilistic polynomial-time complexity classes" (draft: August 23, 1990), 14 pages. [A brief abstract appears in *Structure's Abstracts '92.*]

38. Panesar, Kiran S., Alan T. Sherman, and Kirthivasan Venkatraman, "The vowel-count method for solving columnar transposition ciphers: Quantification, analysis, extensions, and experimental results" (draft: August 16, 1993), 21 pages.

39. Sherman, Alan T., "Decoding the radiograms of the Carpathia," in progress.

40. Sherman, Alan T., "Master Preparation: An experience in distance chess education," in progress.

41. Mcgrew, David, and Alan T. Sherman, "Key cluster search: Algorithms, Analysis, and Heuristics," in progress.

42. Abzug, Charles, James Mayfield, Pavel Pasmanik, Alan T. Sherman, and Ishan Weerakoon, "Using more information from evaluations: An experimental evaluation of an improvement to the Crafty chess program," in progress.

43. Beale, Jay, and Alan T. Sherman, "Perfect play in the board game Mühle by retrograde analysis," in progress.

44. Colangelo, Mark, Barry Herman, Alan T. Sherman, and Anocha Yimsiriwattana, "DVD system insecurity: Analysis and legal aspects" (draft: December 23, 2000), 23 pages. For possible submission to *Cryptologia.*

5 Other Research Works

5.1 Theses

45. Sherman, Alan T., "On the Enigma cryptograph and formal definitions of cryptographic strength," S.M. Thesis, Department of Electrical Engineering and Computer Science, MIT (June 1981). Thesis supervisor: Ronald L. Rivest. 45 pages.

46. Sherman, Alan T., "Cryptology and VLSI (a two-part dissertation): I. Detecting and exploiting algebraic weaknesses in cryptosystems II. Algorithms for placing modules on a custom VLSI chip," Ph.D. Thesis, Department of Electrical Engineering and Computer Science, MIT (October 1986). Thesis supervisor: Ronald L. Rivest. 221 pages.
    [Available as Technical Report TR-381, MIT Laboratory for Computer Science (October 1986), and as VLSI Memo No. 86-343, Microsystems Research Center, MIT (October 1986).]

    Note: Book [2] and article [3] (and associated conference papers [17,18]) are closely related to my dissertation research; all other of my projects proceed in new research directions.

5.2 Internet Drafts for the Internet Engineering Task Force (IETF)

47. Balenson, David M., David A. McGrew, and Alan T. Sherman, "Key management for large dynamic groups: One-Way function trees and amortized initialization," Internet Draft (work in progress), Internet Engineering Task Force, draft-irtf-smug-groupkeymgmt-oft-00.txt (July 31, 2000), 37 pages.
    [Revises draft-balenson-groupkeymgmt-oft.00.tex (February 26, 1999).]

5.3 Papers in Non-Refereed Journals

48. Balenson, David M., David A. McGrew, and Alan T. Sherman, "Key management for large dynamic groups: One-Way funtion trees and amortized initialization," *Advanced security Research Journal—NAI Labs*, Vol. 1, No. 1 (fall 1998), 29–46.

49. Adcock, Jamison M., David M. Balenson, David W. Carman, Michael Heyman, and Alan T. Sherman, "Trading off strength and performance in network authentication: Experience with the ACSA Project," *Advanced security Research Journal—NAI Labs*, Vol. 2, No. 1 (winter 2000), 1–14.

5.4 Workshop Papers at Major Conferences

50. Sherman, Alan T., "Workshop: Applying cryptography in electronic commerce" in Proceedings of the 1996 ACM Computer Science Conference, (Philadelphia, PA, February 17, 1996), 148.

5.5 Papers in Research-Community Periodicals

51. Sherman, Alan T., "On superpolylogarithmic subexponential functions (Part I)," *SIGACT News*, **22**:1 (winter 1991), Whole Number 78, 65–73.

[A preliminary version of the entire paper is available as Technical Report UMIACS-TR-90-97/CS-TR-2506, University of Maryland, College Park (July 1990), and in modified form as Technical Report TR CS-91-17, University of Maryland, Baltimore County (April 1991). This work was performed at the University of Maryland, College Park on December 11, 1991.]

52. Sherman, Alan T., "On superpolylogarithmic subexponential functions (Part II)," *SIGACT News*, **22**:2 (spring 1991), Whole Number 79, 51–56.

53. Chang, Richard, and Alan T. Sherman, "Report on the 8th Maryland Theory Day," *SIGACT News*, **24**:2 (April 29, 1993), Whole Number 87, 81–82.

54. Chang, Richard, Konstantinos Kalpakis, and Alan T. Sherman, "Report on the 16th Maryland Theory Day," *SIGACT News*, **28**:2 (June 1997), Whole Number 103, 56–58.

5.6 Technical Reports

5.6.1 Technical Reports not Superseded by Other Works

55. Sherman, Alan T., "A proof of security for the OFC and LKH centralized group keying algorithms," NA Labs Technical Report TR 02-043D (November 7, 2002). 22 pages. [Based in part on a talk given by Sherman at NSA on October 13, 2000.]

5.6.2 Technical Reports Superseded by Other Works

Most technical reports have been superseded by other works (see in-line listings throughout this document). These technical reports include ones in the following series:
Technical Reports/Memorandums, MIT Laboratory for Computer Science
VLSI Memos, Microsystems Research Center, MIT
Department of Computer Science, Tufts University
Computer Science Department, UMBC
UMIACS/CS, University of Maryland, College Park
TIS Labs at Network Associates, Inc., Glenwood, MD NA Labs at Network Associates, Inc., Rockville, MD

5.7 Reports for Major Research Contracts

I have contributed significantly to several lengthy reports for research contracts from DARPA and other clients through my consulting work at NAI Labs. These reports, which contain more details than do the associated publications, are for the DARPA-sponsored DCCM and ACSA projects and for other government-sponsored projects. Some of these reports and projects are described at the NAI Labs web site http://www.pgp.com/research/nailabs/cryptographic.asp

5.8 Consultancy Reports

I have written numerous consultancy reports connected with my consulting work for NAI Labs, Maryland State Board of Elections, 2factor, LuxSAT, Phoenix Technologies, SAIC, Mattel

Toys, and for other clients who wish not to be named. These reports are not listed at the request of the clients.

5.9 Patents

I am a co-inventor on five cryptographic patent applications owned by Network Associates, Inc., connected with my consulting work at NAI Labs. Three of these patent applications grew from the DARPA-sponsored ACSA project; two from another government-sponsored project.

56. Carman, David W., Michael D. Heyman, and Alan T. Sherman, inventors, United States Patent Number 6,845,449, "System and method for fast nested message authentication codes and error correction codes" (January 18, 2005). Assignee: Networks Associates Technology, Inc. (Santa Clara, CA).

57. Carman, David W., Michael D. Heyman, and Alan T. Sherman, inventors, United States Patent Number 6,915,426, "System and method for enabling authentication at different authentication strength-performance levels" (July 5, 2005). Assignee: Networks Associates Technology, Inc. (Santa Clara, CA).

58. Dinsmore, Peter T., David W. Carman, Michael D. Heyman, Peter Kruus, and Alan T. Sherman, United States Patent Number 7,043,024, "System and method for key distribution in a hierarchical tree" (May 9, 2006). Assignee: McAfee, Inc. (Santa Clara, CA).

6 Other Writings

6.1 Public Speeches

59. Sherman, Alan T., “The importance of mathematics,” salutatory address, Lafayette High School First Commencement Exercises, William and Mary Hall, Williamsburg, Virginia (June 16, 1974). 4 pages.

6.2 Memoranda, Guidelines, and How-To's

60. Sherman, Alan T., “How to solve and write up homework problems,” Computer Science Department, UMBC (February 4, 1990), unpublished document. 9 pages.

61. Sherman, Alan T., “How to give an oral presentation,” Computer Science Department, UMBC (spring 1990), unpublished document. 6 pages.

62. Sherman, Alan T., “A proposal for basic-skills ‘gateway courses’ in discrete mathematics and computer systems software,” Computer Science Department, UMBC (August 20, 1991), unpublished document. 6 pages.

63. Sherman, Alan T., “CMSC-693 guidelines,” Computer Science Department, UMBC (November 18, 1991), unpublished document. 9 pages.

64. Sherman, Alan T., “Nurturing and evaluating effective teaching at UMBC,” individual report by member of SCEQ Committee (February 12, 1994). 15 pages.

65. Sherman, Alan T., “Reflections on teaching computer science at UMBC,” essay (November 28, 1998). http://www.cs.umbc.edu/~sherman/Papers/misc/umbc [A version also appears in *The Retriever* (fall 1998).]

66. Sherman, Alan T., “A proposal for a departmental honors program in computer Science” (April 4, 1999). 10 pages.

6.3 Articles in Magazines, Newspapers, and Newsletters (Selected)

67. Sherman, Alan T., “It's mating season kids! At the UMBC Chess Club,” *The Retriever*, **XXVII**: 8 (October 22, 1991), 10. [My title was: “Mating season opens at chess club.”]

68. Sherman, Alan T., “Kimani Stancil, UMBC Chess Club Prez speaks of chess and life,” *The Retriever*, **XXVII**: 8 (October 22, 1991), 11. [My title was: “Kimani Stancil, chess club president.”]

69. Sherman, Alan T., “Of kings, queens, and honor: The genesis of a faculty-student chess rivalry,” *The Retriever*, **XXVII**: 9 (October 29, 1991), 10. [My title was: “Students checkmate professors.”]

70. Sherman, Alan T., “In chess, it's all in the notation,” *The Retriever*, **XXVII**: 9 (October 29, 1991), 11. [My title was: “How to read algebraic chess notation.”]

71. Sherman, Alan T., "1993 Pan-Am Tournament," *Maryland Chess Newsletter* (spring 1994), 9–10. [My title was: "UMBC ties for third place at 1993 Pan-American Chess Tournament."]

72. Sherman, Alan T., "UMBC scores at 1994 Pan-Am Chess Championship," *Maryland Chess Newsletter* (spring 1995), 5–6.

73. Sherman, Alan T., "Grandmaster Sagalchik goes 25-3-5 at simultaneous exhibition," *Maryland Chess Newsletter* (spring 1995), 16–17.

74. Sherman, Alan T., "Star-Socrates beats Grandmaster Sagalchik in Man vs. Machine Chess Match at UMBC, *Maryland Chess Newsletter* (summer 1995), 23.

75. Sherman, Alan T., "Sagalchik wins UMBC Open," *Maryland Chess Newsletter* (summer 1995), 24–25.

76. Sherman, Alan T., ed., "Smirin victorious at 1995 National Chess Congress," *Maryland Chess Newsletter* (spring 1996), 11.

77. Sherman, Alan T., "UMBC Checkmates MIT," *Maryland Chess Newsletter* (winter 1996), 14. [Appears also as: "MIT just pawns in the Hand of UMBC Chess Team," *Retriever* (November 28, 1995), 15.]

78. Sherman, Alan T., UMBC places fourth at 1995 Pan-American Chess Championship," *Maryland Chess Newsletter* (spring 1996), 24–25. [Appears also as "UMBC places fourth at Pan-American Intercollegiate Chess Championship," *Retriever* (February 6, 1996).]

79. Sherman, Alan T., "Cooper collection," *Chess Life*, (March 1996), letter to the editor, p. 222.

80. Sherman, Alan T., "Yes, chess deserves sporting treatment," *Baltimore Sun* (June 16, 1996), op-ed essay, 8F. [My title was "Chess as sport." Reprinted as "Give chess a sporting chance," *Retriever* (May 6, 1997), 8.]

81. Sherman, Alan T., "College chess and the 1996 Pan-Am," *Chess Life*, **15**:11 (November 1996), 6.

82. Sherman, Alan T., "UMBC wins 1996 Pan-Am," *Chess Life*, **16**:5 (May 1997), 34, 36.

83. Sherman, Alan T., "Chess at UMBC," *Chess Life*, **53**:2 (February 1998), 14–16. Abbreviated version of the full 10,000-word essay.

84. Sherman, Alan T., "How to select a college chess team," *Chess Life* **54**:12 (December 1999), 34.

85. Alan T. Sherman, "UMBC's William 'The Exterminator' Morrison," *Chess Life* **55**:3 (March 2000), 31.

86. Alan T. Sherman, "College chess eligibility requirements," letter to the editor, *Chess Life* (get date and page).

87. Alan T. Sherman, "My game from the Pan-Am," *Maryland Chess Newsletter* (get date and page).

88. Sherman, Alan T. , "UMBC's speed chess spectacular—A sporting smash," *Chess Life* **58**:9 (September 2003), 50–51.

89. Sherman, Alan T., and Craig Jones, "Pan Am showcases top collegians," *Chess Life* (March 2007), 34–36.

6.4 WWW Publications

90. Sherman, Alan T., "The story of chess at UMBC: 1990–1997," hypertext, http://www.umbc.edu/chess (February 1, 1998). WWW-rendered by Derrick Longo. An abbreviated version appears in *Chess Life* (February 1998).

7 Musical Compositions, Recordings, Videotapes, and Performances

7.1 Computer Music Compositions Performed in Public Concerts

91. Sherman, Alan T., "Fantasy for computer" in *Music for Computer and Instruments: A Program of Student Works from the Course 21 Seminar in Music Composition*, MIT (May 13, 1982). 3.5 minutes. [Synthesized in the MIT Experimental Music Studio using the Music 11 System. Concert organizer and seminar instructor: Barry L. Vercoe.]

7.2 LP Recordings

92. Played flute in *1973 V.M.E.A. (Virginia Music Educators Association) District VIII Regional Band*, Frederick C. Ebbs, conductor, Recorded Publications Company (Camden, NJ, 1973).

93. Played fife in *The Fifes & Drums of Williamsburg*, WS101, Colonial Williamsburg Foundation (Williamsburg, VA, 1975). Musick Master: John C. Moon.

7.3 Videotapes

94. *UMBC Exhibition Chess Match* (June 21–22, 1996). Chess match between International Grandmaster Ilya J. Smirin and Senior Master William "The Exterminator" Morrison. Concept, event organizer, script writer, and assistant video editor: Alan T. Sherman. Video, editing, and voice over: Robert Kuhlman. Commentators: Senior Master Craig Jones and Lifetime Master Igor Epshteyn. Produced and available through UMBC Instructional Technology. 51 minutes.

95. *Master Preparation: An Advanced Course in Chess* Concept, course organizer, and developer: Alan T. Sherman. Video: William Shewbridge and assistants. Produced and available through UMBC Instructional Technology. Some tapes are also available through

WWW Chess Superstore (www.smartchess.com). Complete list of 83 tape titles available from www.umbc.edu/chess and by request.

- Fall 1995–12 tapes: Middlegame Strategy (Instructors: GM Ilya J. Smirin and Igor Epshteyn).
- Spring 1996–13 tapes: Middlegame Strategy (Instructors: Igor Epshteyn, GM Ilya J. Smirin, and William Morrison).
- Fall 1997–10 tapes: Middlegame Strategy (Instructors: GM Alexander Shabalov and Igor Epshteyn).
- Fall 1998–12 tapes: Middlegame Strategy (Instructors: Igor Epshteyn and William Morrison).
- Spring 1999–12 tapes: Pawn Endings (Instructors: Igor Epshteyn, GM Ron Henley, and William Morrison)
- Fall 1999–12 tapes: Art of Attack (Instructors: IM Larry Kaufman, IM Eugene Perelshteyn, Igor Epshteyn, and Tom Brownscombe).
- Spring 2000–12 tapes: World Champions (Instructors: IM Larry Kaufman, IM Eugene Perelshteyn, Igor Epshteyn, William Morrison, Victor Sherman, Tom Brownscombe). Also includes a lecture by David Pelletier on the rules of tournament chess.

96. *Chess at UMBC* (December 1999), trailer for *Master Preparation* series. Concept and script writer: Alan T. Sherman. Video, editing, and voice over: Robert Kuhlman. Produced and available through UMBC Instructional Technology. $\sim$5 mins.

7.4 Musical Performances (Selected)

97. Principal flute, *Bye Bye Birdie* by Michael Stewart (music by Charles Strouse), James Blair High School (Williamsburg, VA, spring 1972). Orchestra Director: Warren King.

98. Principal flute, *A Thurber Carnival* by James Thurber (music by Don Elliott), James Blair High School (Williamsburg, VA, May 10–12, 1973). Orchestra Director: D. Keith Miller.

99. Principal flute (and piccolo), *The Music Man* by Meredith Wilson, Lafayette High School (Williamsburg, VA, spring 1974). Orchestra Director: D. Keith Miller.

100. John Byam (spoons, etc.), Duffy Elliott (banjo), Bruce Hornsby (mandolin), Jonathan Hornsby (bass), John King (guitar), William Leonard (wash board), Hilary Selby (fiddle), Winston Sheppard (guitar), and Alan Sherman (ocarina) as The No Name Grit Band, "I saw the light" by The Nitty Gritty Dirt Band in the *Annual AFS (American Field Service Organization) Talent Show*, Lafayette High School (Williamsburg, VA, May 3–4, 1974). Artistic director: Bruce Hornsby.

101. Bob Barsky (violin), Eleanor Feingold (viola), Cynthia Forbes ('cello), and Alan Sherman (piano), *Piano Quartet No. 2 in E♭ Major, K. 493* by Wolfgang Amadeus Mozart, The MIT Chamber Music Society (February 24, 1984), MIT. Coach: Marcus A. Thompson.