Alan T. Sherman

Office: Dept. of CSEE, UMBC, 1000 Hilltop Circle, Baltimore, MD 21250. Tele: 410-455-2666, fax: 410-455-3969, sherman@umbc.edu, www.csee.umbc.edu/~sherman. ***Home:*** 3618 Ordway St., NW, Washington, DC, 20016. Tele: 202-966-7204, fax: 202-362-4838, alantsherman@gmail.com. US citizen (born in Cambridge, MA). Married with two children under fifteen years old.

Research Interests. Security of voting systems, information assurance, cryptology, discrete algorithms.

Education. PhD, computer science, MIT, 1987 (dissertation advisor: Ronald L. Rivest). SM, electrical engineering and computer science, MIT, 1982. ScB, mathematics, *magna cum laude*, Brown University, 1978.

Experience in Higher Education. Associate Professor of Computer Science (with tenure), University of Maryland, Baltimore County (UMBC), July 1, 95–present. Assistant Professor, UMBC, August 89–June 95. Assistant Professor of Computer Science, Tufts, September 86–August 89. Instructor, Tufts, September 85–August 86.

Research Affiliations. Member, National Center for the Study of Elections at UMBC, 06-09. Joint Appointment, University of Maryland Institute for Advanced Computer Studies (UMIACS), University of Maryland College Park, Maryland, August 89–August 95. Research Affiliate (in Theory of Computation Research Group), MIT Laboratory for Computer Science, Massachusetts Institute of Technology, September 85–August 88.

Consulting (selected). Expert witness for Fish & Richardson, Maryland State Board of Elections (05, 06-07), and WilmerHale representing RSA (06-07). Performed DARPA- and other government-sponsored research through Cryptographic Technologies Group, NAI Labs, Network Associates, Inc., Rockville, MD, Aug. 97–04 (including my 97–98 sabbatical year). Security review of products for ID2P, 2factor (05), LuxSAT (02), Infoscape, Corp., Redmond, WA (02), and Phoenix Technologies, San Jose, CA (01).

Honors and Awards (selected). Member, *Phi Beta Kappa* and *Sigma Xi*. *Who's Who in America, Who's Who in the East*, *Who's Who in Science and Engineering*, *Who's Who in American Education*, *Who's Who in the Media*, Marquis. Senior Class Award—awarded primarily for teaching cryptology (fall 85, Tufts). Meritorious Service Award–US Chess federation (97).

External Funding (selected).

(1) Principal Investigator, Information assurance scholarships at UMBC, funded by DoD for $85,537 in 2011-2012 to develop security education game at Meade high School.
(2) Principal Investigator (PI), SGER: CT-ISG: The VoComp University Voting System Competition, funded by NSF for $29,940 in 06–07.
(3) Investigator at NAI Labs on four government contracts (over $1 million total) to design a key-management security architecture for a world-wide satellite broadcast system.
(4) Investigator at NAI Labs on three DARPA cryptography research contracts, each funded for over $1 million. These contracts dealt with key establishment in large dynamic groups (DCCM), fast data stream authentication (ACSA), and cryptography for limited-resource sensor networks (SENSEIT).
(5) Co-Investigator (with Tim Finin) at UMBC, A security architecture for intelligent software agents, funded by NSA for $49,984, April 1997–April 1998.

Publications (summary). 2 books, 17 refereed journal articles, 22 refereed conference papers, numerous other publications, confidential consultancy reports, and 4 cryptographic patents issued (Co-Inventor).

Recent Publications (selected).

(1) Sherman, Alan T., Dhananjay Phatak, Vivek G. Relan, and Bhushan Sonawane, ``Location authentication, tracking, and emergency signaling through power line communication: Designs and protocols for new out-of-band strategies," *Cryptologia* (accepted May 2011), 12 pages, in press.

(2) Sherman, Alan T., Russell A. Fink, Richard Carback, and David Chaum, ``Scantegrity III: Automatic trustworthy receipts, highlighting over/under votes, and full voter verifiability" in *online Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE '11)*, (August 2011). 16 pages. Accessed 11-24-11 from http://www.usenix.org/event/evtwote11/tech/final_files/Sherman.pdf

(3) Carback, Richard T., David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc, Ronald L. Rivest, Emily Shen, Alan T. Sherman, and Poorvi L. Vora, ``Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy" in online *Proceedings of USENIX Security 2010*, (Washington, DC, August 2010). 16 pages. Accessed 11-24-11 from http://www.usenix.org/events/sec10/tech/full_papers/Carback.pdf

(4) Chaum, David, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y.A. Ryan, Emily Shen, Alan T. Sherman, and Poorvi Vora, "Scantegrity II: End-to-End verifiability by voters of optical scan elections through confirmation codes," *IEEE Transaction on Information, Forensics, and Security---special issue on voting*, Vol. 4, No. 4 (December 2009), 611--627.

(5) Fink, Russ, Alan Sherman, and Richard Carback, ``TPM meets DRE: Reducing the trust base of electronic voting using Trusted Platform Modules," *IEEE Transaction on Information, Forensics, and Security---special issue on voting*, Vol. 4, No. 4 (December 2009), 628--637.

(6) Sherman, Alan T. and David Mcgrew, David, "Key establishment in large dynamic groups using one-way function trees," *IEEE Transactions on Software Engineering*, 29:5 (May 2003), 444–458.

Professional Activities (selected). Member, Editorial Board, *Cryptologia*, Dec. 94–Dec. 00; July 05–date. Member, Program Committee, Crypto 95. Grant panelist for National Science Foundation, *Journal of Cryptology*, and other journals.

Recent Teaching Activities at UMBC. Information Assurance (644/444), Electronic Voting Systems (691/491), Cryptology (CMSC-652, 443), Algorithms (641, 441), Discrete Math (603, 203). As thesis advisor, graduated four PhD students (three more in progress) and twenty MS students (one more in progress).

Service to UMBC (selected). Director, Center for Information Security and Assurance (CISA), 01–date. Under my leadership, UMBC became a Center of Academic Excellence in Information Assurance Education (CAE), as designated by DoD/DHS. Director, Graduate Program, February 95–June 96. Member of Undergraduate, Graduate, Hiring, Lecture Series, and Chair Search Committees. Created and organized annual CSEE Research Review (06-to date).

UMBC Chess. Director, UMBC Chess Program, 91–date. Under my leadership, the UMBC Chess Team won nine international titles at the Pan-American Intercollegiate Team Chess Championships (96,98–02,05,08-09), and six national titles at the President's Cup "Final Four of College Chess" (03-06,09-10). Appeared on *CNN Headline News*, *NBC Today Show, ABC Good Morning America, NPR Morning Edition,* and *BBC Radio.* Member, US Chess Federation College Chess Committee. Raised over $182,000 for UMBC Chess and organized four national events (2000 US Junior, 96 and 06 Pan-Am, and 08 President's Cup).

Personal Interests. Piano, flute, tennis, golf, cycling, ballroom dancing. *Shodan* (first-degree black-belt) in Japanese martial art of Tomiki Aikido. Five-time top faculty chess player at Pan-American Open (93–4, 98–9, 01). My Erdös number is 3 (one path to coauthorship with Paul Erdös is via A. Odlyzko, R. Rivest).

November 24, 2011