Curriculum Vitae

August 3, 2014

Alan Theodore Sherman

Personal Data

Date of birth: February 26, 1957
Place of birth: Cambridge, Massachusetts
Citizenship: USA
Marital status: married, children born 1996 and 2003

Research Areas

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

Education

Ph.D.	Feb. 1987	MIT, computer science
S.M.	June 1981	MIT, electrical engineering and computer science
Sc.B.	June 1978	Brown University, mathematics, *magna cum laude*
H.S. Diploma	June 1974	Lafayette High School, *salutatorian*, Williamsburg, Va.

Experience in Higher Education

July 2014–present. University of Maryland, Baltimore County (UMBC), Baltimore, Maryland. Professor of Computer Science (with tenure), Department of Computer Science and Electrical Engineering.

July 1995–June 2014. University of Maryland, Baltimore County (UMBC), Baltimore, Maryland. Associate Professor of Computer Science (with tenure), Department of Computer Science and Electrical Engineering.

August 1989–July 1995. University of Maryland, Baltimore County (UMBC), Baltimore, Maryland. Assistant Professor of Computer Science, Computer Science Department.

September 1986–August 1989. Tufts University, Medford, Massachusetts. Assistant Professor of Computer Science, Department of Computer Science.

September 1985–August 1986. Tufts University, Medford, Massachusetts. Instructor of Computer Science, Department of Computer Science.

January 1979–January 1982. Massachusetts Institute of Technology (MIT), Cambridge, Massachusetts. Teaching Assistant, Department of Electrical Engineering and Computer Science.

Experience Outside of Higher Education

A. Consulting and Contracting

July 2014–date. Blank Rome, Washington, DC. Serving as cryptologic expert witness for Strike Force in *Strike Force vs. Phone Factor* in patent litigation involving multi-channel authentication.

May 2013–date. Sidley Austin, Washington, DC. Serving as cryptologic expert witness on invalidity for Apple in *Content Guard vs. Apple* in patent litigation involving digital rights management.

May 2013–March 2014. Kirkland & Ellis, Chicago, IL. Served as a cryptologic expert witness on invalidity for Apple in *Intertrust vs. Apple* in patent litigation involving digital rights management.

May 2013–May 2014. Perkins Coie, Seattle, WA. Served as a cryptologic expert witness on non-infringement for McAfee in *Uniloc vs. McAfee* in patent litigation involving product activation (via Rubin Anders).

April 2013–June 2013. Quinn Emanuel, Redwood Shores, CA. Researched prior art as expert cryptologic witness for IBM in *Softvault vs. IBM* in a patent litigation matter involving embedded controllers(via Thomson Reuters).

June 2012–date. Kirkland & Ellis, Chicago, IL. Analyzed the validity of two cryptographic patents dealing with streaming media for Wowza Media Systems in *Adobe vs. Wowza.* Wrote invalidity and security reports and was deposed as expert witness.

April 2012–date. Morgan, Lewis & Brockius, Houston, TX. Provided technical advice on prior art for Rite Aid in *TQP Development vs. DirectTV, et al.* (via Thomson Reuters, Rockville, MD).

October 2011–March 2012. Fish & Richardson, Boston, MA. Devised a technical work-around for Microsoft in the second damages phase of *Uniloc vs. Microsoft* concerning a patent for product activation, helping to reduce damages from $388 million to an amount reported to be about $80 million. Wrote report and was deposed as expert witness.

July 2008–May 2010. ID2P Technologies, Inc., Lake Forest, CA. Evaluated the security of the SafeIDKey Authentication Device.

July 2008–July 2009. Kenyon & Kenyon, New York City, Provided technical advice as expert witness for Sony in *Certicom vs. Sony.*

August–September 2007; July 2008–January 2009. Kirkland & Ellis, New York City. Provided technical advice as expert witness concerning a cryptographic patent.

July 2006–April 2007. WilmerHale, Boston, Massachusetts and Washington, DC (via Silicon Valley Expert Witness Group, Inc., Washington, DC). Provided technical advice as expert witness for RSA in *PRISM vs. RSA Security, Inc., et al.*, in which PRISM alleged patent infringement.

July 2006–April 2007. State of Maryland, Attorney General's Office, Baltimore, Maryland. Wrote report and provided technical advice as expert witness in *Shade vs. State of Maryland State Board of Elections, et al.*, in which Shade sought to decertify the Diebold AccuvoteTS electronic voting system on the basis of poor security.

July 2005. State of Maryland, Attorney General's Office, Baltimore, Maryland. Testified as an expert witness in *Fox vs. State of Maryland Department of Budget and Management*, in which Fox sought access under FOIA to the unredacted SAIC report on the security of the Diebold AccuvoteTS electronic voting system.

May 2005. 2factor, L.L.C, Centreville, Virginia. Evaluated the security of the 2factor Authentication and Key-Management System.

August 4, 1997–April 2003. Cryptologic Consultant, NAI Labs at Network Associates, Inc., Rockville, Maryland—formerly Advanced Research and Engineering Division of Trusted Information Systems (TIS), Inc. Analyzed the security of the TIS RecoverKey product and performed cryptographic research in support of DARPA and other government contracts on key management for large dynamic groups, ultra-fast network authentication, and distributed sensor networks. Contractual arrangements last made through TAC Worldwide Companies. Supervisors: Dennis K. Branstad, David Balenson, Pete Dinsmore, Michael St. Johns.

July–August 2002. LuxSAT, Inc., Luxenburg, Netherlands. Evaluated security of a multimedia-on-demand broadcast system. Via Plus Five Consulting, Palo Alto, CA. Point of Contact: Robert W. Baldwin.

January 2002. InfoScape Corporation, Redmond, WA. Evaluated the security of protocols in InfoScape Technologies. Via Plus Five Consulting, Palo Alto, CA. Point of Contact: Robert W. Baldwin.

September 2001. Phoenix Technologies, San Jose, CA. Evaluated the security of the FirstAuthority StrongROM and StrongClient products. Point of contact: Sameer Mathur.

March 27, 1997. Science Applications International Corporation (SAIC), McLean, Virginia. Science & Technology Assessment Division. Advised government agencies on the impact of technology advances on cryptography and signals intelligence for the year 2010.

March 28, 1991. Synchronetics, Baltimore, Maryland. Suggested improvements to text-retrieval algorithms used in an automatic system that converts linear text to hypertext. Coordinated through the Technology Extension Service, University of Maryland.

October 5 and 23, 1990. Digital Systems Corporation, Walkersville, Maryland. Outlined a cryptographic scheme to authenticate control signals for electronically-operated vault doors. Coordinated through the Technology Extension Service, University of Maryland.

July 10–12, 1982. Mattel Inc., Hawthorne, California. Consultant, Mattel Toys. Devised a cryptographic method to authenticate electronic game scores on a 4-bit microprocessor.

B. Research Appointments

2006–2009. Member, National Center for the Study of Elections, UMBC.

August 1995–August 1998; August 1989–October 1992. Joint appointment, University of Maryland Institute for Advanced Computer Studies (UMIACS), University of Maryland College Park, College Park, Maryland.

September 1985–August 1988. MIT Laboratory for Computer Science, 545 Technology Square, Cambridge, Massachusetts. Research Affiliate, Theory of Computation Research Group.

June 1979–August 1985. MIT Laboratory for Computer Science, 545 Technology Square, Cambridge, Massachusetts. Research Assistant. Performed research in cryptology and VLSI layout algorithms under the supervision of Professor Ronald L. Rivest.

C. Other Employment

Summer 1977. Computer Sciences Corporation, NASA Langley Research Center, Hampton, Virginia. Programming Aide. Helped maintain and improve navigation, guidance, and flight control software for computers aboard NASA's Boeing 737 experimental research airplane.

Summers 1974–1976. Colonial Williamsburg Foundation, Williamsburg, Virginia. Interpreter at Magazine. Guided tours through historic powder magazine and demonstrated firing the Brown Bess musket while dressed in eighteenth-century apparel.

Summer 1974. NASA Langley Research Center, Hampton, Virginia. Participant, Career Exploration Program. Analyzed three algorithms used to compute trigonometric functions on a navigation flight computer aboard NASA's 737 experimental research airplane. Supervisor: Dr. Terry A. Straeter.

October 1965–September 1974. Colonial Williamsburg Foundation, Williamsburg, Virginia. Member, Colonial Williamsburg Fife and Drum Corps (Fife Sergeant, November 1972–September 1974). Played fife in hundreds of parades and ceremonies. Duties as Fife Sergeant included supervising and rehearsing the senior corps's fife section and helping oversee fife instruction for the junior corps.

Honors Received

Awards for Scholarship

- Outstanding Case Study Award for 2012 by the American Academy of Forensic Sciences, based on a paper by Josiah Dykstra and Alan T. Sherman published in the *Journal of Network Forensics*.
- Listed in the following *Who's Who* publications by Marquis:
  Who's Who in America
  Who's Who in the East, 25–26th+ editions (94–96+)
  Who's Who in Science and Engineering, 2nd edition (94+)
  Who's Who in American Education, 3rd–5th+ editions editions (92–95+)
  Who's Who in the Media
- Member, *Sigma Xi*, MIT (April 1981).
- Fellowship, German Academic Exchange Office (June 1978). To attend a Goethe Institute Summer Language Program.
- Member, *Phi Beta Kappa*, Brown University (April 1978).
- Member, *Sigma Xi*, Brown University (March 1978).

Teaching Awards

- Senior Class Award, Tufts University (May 1986). Awarded primarily for teaching CSC–150c Cryptology, fall 1985.
- Forgivable Loan, General Electric Foundation/Ford Foundation, MIT (November 1983). Awarded primarily for excellence in teaching at MIT.

Other Awards and Accomplishments

- Meritorious Service Award, United States Chess Federation (August 1997). For contributions to college chess.
- Promoted to the rank of shodan (first-degree black belt) in the Japanese martial art of Tomiki Aikido, as certified by the Japan Aikido Association (February 1995).
- Top Faculty Chess Player, Pan-American Open (1993, 1994, 1998, 1999[tie], 2001).
- Erdös Number 3: One path of coauthorships to Paul Erdös is via Andrew Odlyzko and Ronald Rivest.

Funding

External — Research

- *August 2013–August 2014,* $271,435 (amount for research: $271,435). National Science Foundation. Principal Investigator, "Supplement to UMBC Cybersecurity Scholarship for Service Program and Innovations in Cybersecurity Education Workshop Series" (Richard Forno CoPI). Supports two research projects, each with GRA: SecurityEmpire educational multiplayer computer game, and verifiable randomness. At UMBC.
- *August 2013–July 2015,* $44,206 (non-participant cost amount for research: $28,574). National Science Foundation. Co-Principal Investigator, "INSuRE EAGER" (Melissa Dark, Purdue, PI). At UMBC (subcontract from Purdue).
- *August 2012–August 2017,* $2,542,169 (non-participant cost amount for research: $293,864). National Science Foundation. Principal Investigator, "UMBC Cybersecurity Scholarship for Service Program and Innovations in Cybersecurity Education Workshop Series" (Richard Forno CoPI). At UMBC.
- *August 2012–December 2013,* $83,280 (amount for research: $83,280). National Security Agency. Principal Investigator, "University of Maryland, Baltimore County (UMBC) Information Assurance Scholarship Program 2012-2013" (Richard Forno Co-PI). Research funds are for the project, "Teaching information assurance concepts to high school students through our new social media game SecurityEmpire: Outreach to academia" (Marc Olano and Linda Oliva, Co-Investigators). At UMBC.
- *August 2011–December 2012,* $85,537 (amount for research: $85,463). National Security Agency. Principal Investigator, "University of Maryland, Baltimore County (UMBC) Information Assurance Scholarship Program 2011-2012" (Richard Forno Co-PI). At UMBC. Research funds are for the project, "Teaching information assurance concepts to high school students through a new social media game: Outreach to academia" (Marc Olano and Linda Oliva, Co-Investigators). At UMBC.
- *August 2010–December 2011,* $74 (amount for research: $0). National Security Agency. Principal Investigator, "University of Maryland, Baltimore County (UMBC) Information Assurance Scholarship Program 2010-2011" (John Pinkston Co-PI). At UMBC.
- *September 2009–December 2010,* $19,205 (amount for research: $0). National Security Agency. Principal Investigator, "DoD IASP Scholarships at UMBC" (John Pinkston Co-PI). At UMBC.

- *September 2008–September 2013,* ∼$7,500,000 (my portion: ∼$25,000–50,000). Multi-Disciplinary University Research Initiative (MURI), AFOSR. Investigator (Tim Finin, PI), "A framework for managing the assured information sharing lifecycle." At UMBC.
- *September 2008–September 2009,* $66,346 (amount for research: $0) National Security Agency. Principal Investigator, "DoD IASP Scholarships at UMBC," (John Pinkston Co-PI). At UMBC.
- *September 13, 2007–September 12, 2008,* $36,300 (amount for research: $30,583) National Security Agency. Principal Investigator, "DoD IASP Scholarships at UMBC," (John Pinkston Co-PI). At UMBC.
- *October 1, 2006–September 30, 2007,* $29,940. National Science Foundation, Principal Investigator, "SGER: CT-ISG: The VoComp University Voting Systems Competition." At UMBC.
- *September 15, 2006–January 30, 2008* $65,646 (amount for research: $11,760). National Security Agency. Principal Investigator, "DoD IASP Scholarships at UMBC," (John Pinkston Co-PI). At UMBC.
- *August 29, 2005–August 29, 2007,* $63,833 (with extension), (amount for research: $21,014). National Security Agency. Principal Investigator, "DoD IASP Scholarships at UMBC," (John Pinkston Co-PI). At UMBC.
- *September 14, 2004–September 14, 2006,* $ 143,999 (with extension), (amount for research: $0). National Security Agency. Principal Investigator, "DoD IASP Scholarships at UMBC," (John Pinkston Co-PI). At UMBC.
- *August 2003–August 2004,* $57,021 (amount for research: $53,449). National Security Agency. Principal Investigator, "DoD IASP Scholarship Grant, with NDU/IRMC Partnership" (John Pinkston Co-PI). At UMBC.
- *August 2002–August 2003,* $120,384 (amount for research: $110,000). National Security Agency. Principal Investigator, "DoD IASP Scholarship Grant, with NDU/IRMC Partnership" (John Pinkston Co-PI). At UMBC.
- Fall 2001–Summer 2002, $37,000 (amount for research: $37,000). Department of Defense. Principal Investigator (Peng Liu and John Pinkston Co-PIs), "Program Initiation Award," for UMBC Center for Information Security and Assurance. At UMBC.
- *April 1997–April 1998,* $43,735. National Security Agency. Investigator, "A security architecture for intelligent software agents: Adding security to KQML" (Tim Finin Co-Investigator). At UMBC (via subcontract from UMCP under Principal Investigator Joseph JaJa).
- *December 1, 1995–June 30, 1996,* $35,597. IBM, Thomas J. Watson Research Center. Principal Investigator, "Efficient implementation of cryptographic algorithms for electronic commerce." At UMBC.

- *Summer 1995,* $6,283 (my portion). National Science Foundation (via subcontract from UMCP). Member, Maryland Collaborative for Teacher Preparation (MCTP). At UMBC.
- *March 1–September 1, 1995,* $5,328. National Security Agency. Principal Investigator, "Maryland Theory Day at UMBC" (Co-Principal Investigator: Richard Chang). Mathematical Sciences Program. At UMBC.
- *March 1–June 1, 1993,* $3,860. National Science Foundation. Principal Investigator, "Maryland Theory Day at UMBC" (Co-Principal Investigator: Richard Chang). Division of Computer and Computation Research, CCR-93-08170. At UMBC.
- *August 1989–August 1992,* ∼$20,000 (50% Joint Appointment). University of Maryland Institute for Advanced Computer Studies (UMIACS), Collegel Park. At UMBC.
- *March 15, 1988–August 31, 1989,* $15,000. National Science Foundation. Investigator, "VLSI algorithms" in "Research instrumentation award for memory increase to Ncube parallel processor" (Co-Principal Investigators: James G. Schmolze and Beth Adelson). Computer and Information Science and Engineering, CCR-87-16916. At Tufts University.

Internal — Research

- *Summer 1990,* $4,000. UMBC. Principal Investigator, "Relationships among algebraic and security properties of cryptographic functions." Summer Faculty Fellowship. At UMBC.

External — Research through Consulting

Note: I helped write these grant proposals, which could not have been coordinated through UMBC in part because portions have a sensitive nature or because of other restrictions by the sponsor.

- *May 2011-November 2012,* $25,000, U.S. Election Assistance Commission. Consultant (Richard Carback, PI), "Post-election auditing with voter-verified privacy preserving receipts." At City of Takoma Park, MD.
- *September 2000–April 2001,* $200,000, Contractor, extension to previous contract. [Project title and funding source withheld at request of client.] Through Maryland Procurement Office. At NAI Labs at Network Associates, Inc., Glenwood, MD.
- *Spring 2000,* $200,000, Contractor. [Project title and funding source withheld at request of client.] Through Maryland Procurement Office. At NAI Labs.
- *July 1999–December 2001,* ∼$1,500,000 (exact amount NAI sensitive). Defense Advanced Project Agency (DARPA). Contractor, "A communications security architecture and cryptographic mechanisms for distributed sensor networks (SENSIT)" (David W. Carman, Principal Investigator). At NAI Labs.
- *September 1998–August 2000,* ∼$1,500,000 (exact amount NAI sensitive). Defense Advanced Project Agency (DARPA). Contractor, "Adaptive cryptographically synchronized authentication (ACSA)" (Dennis Branstad, then David Balenson, then David Carman, Co-Principal and Principal Investigators). At NAI Labs.
- *September 1997–December 2000,* ∼$1,500,000 (exact amount NAI sensitive). Defense Advanced Project Agency (DARPA). Contractor, "Dynamic Cryptographically Context Management (DCCM)" (Dennis Branstad, then David Balenson, then Peter Dinsmore, Principal Investigators). At NAI Labs.

External — Chess

- As Director of the UMBC Chess Program, I raised over $218,957 for UMBC Chess in over 38 grants, gifts, and awards from over 14 sponsors (1995–present). Sponsors included The Abell Foundation, US Chess Federation, Connections Academy, and Maryland State Department of Education.

Note: I was instrumental in gaining favorable publicity for UMBC with feature stories and appearances on the following national TV and radio shows about UMBC chess (selected):
CNN Headline News (December ∼28, 1996—2.5 mins),
NPR's *Morning Edition* (May 9, 1997)—∼3 mins),
ABC's *Good Morning America* (March 3, 1999—3.5 mins),
NBC's *Today Show* (March 5, 2001—4.5 mins), and
CNN's *Next* (February 2002—3 mins),
BBC World Radio (circa 2001)
NPR's "Maryland Morning with Sheilah Kast" (December 27, 2006).
NPR's "Tell Me More" (April 12, 2010–5.5 mins).
I estimate that the cash value to UMBC (based on the cost of a comparable duration and type of national TV advertising) of this publicity **exceeds five million dollars.**

Student Projects Supervised

A. Ph.D. Dissertations—As Advisor (5)

Farid Javani, "Security of wearable computers," UMBC, in progress (expected May 2018). Thesis advisor.

Christopher Nguyen, "Verifiable randomness with applications to voting," UMBC, in progress (expected May 2017). Thesis co-advisor (with D. Phatak). [I am fully supporting Nguyen under my 2013 NSF grant.]

Edward J. Birrane, "Virtual circuit provisioning in challenged sensor internetworks: With application to the Solar System Internet," Department of CSEE, UMBC, in progress (expected August 2014). Thesis co-advisor (with M. Younis).

Josiah Dykstra, "Digital forensics for cloud computing: Framework, tools, and legal analysis for Infrastructure-as-a-Service cloud computing," Department of CSEE, UMBC (May 2013). Thesis advisor. [In May 2012, Dykstra won the Dept.'s CSEE Research Review award for best research by a PhD student.]

Russell A. Fink, "Applying trustworthy computing to End-to-End electronic voting," Department of CSEE, UMBC (December 2010). Thesis advisor. [In May 2008, Fink won the Dept.'s CSEE Research Review award for best research by a PhD student.]

Richard T. Carback, "Engineering practical end-to-end election systems," Department of CSEE, UMBC (December 2010). Thesis advisor. [In May 2011, Carback won the Dept.'s CSEE Research Review award for best research by a PhD student.]

F. John Krautheim, "Building trust into utility cloud computing," Department of CSEE, UMBC (May 2010). Thesis co-advisor (with D. Phatak). [I fully supported Krautheim under my DoD IASP grants.]

Muhammad Rabi, "Relationships among algebraic and security properties of cryptographic functions, and a security architecture for intelligent agents" Computer Science Department, UMBC (August 1998). Thesis co-advisor (with T. Finin).

B. Ph.D. Dissertations—As Reader

Michael Oehler "Private packet filtering: Searching for sensitive indicators without revealing the indicators in collaborative environments," Department of CSEE, UMBC (December 2013). Reader (Advisor: Phatak).

Xiaonong Gu, "A new classification algorithm," Math Department, UMBC (October 1999). Reader (Advisor: Rukhin).

David M. Lazoff, "Network reliability and optimal resource allocation in distributed database systems," Department of Computer Science and Electrical Engineering, UMBC (August 1996). Reader (Advisor: Stephens).

Zhi-Ming Lin, "DAVE: An automatic layout compiler for mixed analog/digital integrated circuits," Ph.D. Thesis, Department of Electrical Engineering, University of Maryland College Park (1991). Reader.

C. M.S. Theses and Projects[1]—As Advisor (22)

Chirag Shah "A usability study of the PICO authentication device: User reactions to Pico implemented on an Android phone," MS Thesis, UMBC, in progress (expected August 2014). Thesis advisor.

Nathan Price "How to generate repeatable keys using Physical Unclonable Functions: Correcting PUF errors with iteratively broadening and prioritized search," MS Thesis, UMBC (May 2014). Thesis advisor. [I fully supported Price under my NSF SFS grant.]

Christopher Nguyen, "Fast modular exponentiation using residue domain representation: A hardware implementation and analysis," MS Thesis, UMBC (December 2013). Thesis co-advisor (with D. Phatak).

Nikhil Joshi, "Experimental evaluation and implementation of the Spread Identity Framework," MS Thesis, UMBC (December 2011). Thesis co-advisor (with D. Phatak).

William Newton, "Chaum's protocol for detecting man-in-the-middle: Explanation, implementation, and analysis," MS Thesis, UMBC (December 2010). Thesis advisor.

Bhushan Sonawane, "Spread Identity: A new dynamic address translation mechanism for anonymity and DDoS defense," MS Thesis, UMBC (December 2010). Thesis co-advisor (with D. Phatak).

Vivek Relan, "Location authentication through powerline communication: Design, protocol, and analysis of a new out-of-band strategy," MS Thesis, UMBC (December 2010). Thesis co-advisor (with D. Phatak).

Richard Carback, "Security enhancements to the Punchscan voting system," MS Thesis, UMBC (May 2008). Thesis advisor.

Allen Stone, "OBID: An ontology-based intrusion-detection system," MS Thesis, UMBC (May 2007). Thesis advisor.

[1]Prior to the merger of the CS and EE Departments at UMBC circa 1996, there was no thesis option for MS students in CS.

Kevin Fisher, "Security analysis of the Punchscan high-integrity voting system," MS Thesis, UMBC (December 2006). Thesis advisor.

Nicholas Dickerson, "Arpdefender: Detecting and recovering from ARP cache poisoning attacks," MS Thesis, UMBC (fall 2004). Thesis advisor.

Anthony Falcone, "DTEL: A digital telestrator for spectator chess," MS Thesis, UMBC (April 2000). Thesis advisor.

Pavel Pasmanik, "Using more information from evaluation functions: An improvement to the Crafty chess program," UMBC (December 1997). Chairperson, Advisory Committee.

Ali Selcuk, "Linear cryptanalysis of RC-5," MS Thesis, UMBC (December 1997). Thesis advisor.

Qi He, "A new electronic cash scheme with flexible denominations," MS Thesis, UMBC (May 1997). Thesis advisor.

Bryan Olson, CMSC-693 Project, "A new radix sort," Computer Science Department, UMBC (August 1995). Chairperson, Advisory Committee.

Ravada Sivakumar, "Experimental analysis of a partitioning algorithm for the Steiner minimum tree problem in R^2 and R^3," CMSC-693 Project, Computer Science Department, UMBC (August 1993), Chairperson, Advisory Committee.

Thomas R. Cain, "How to break Gifford's cipher," CMSC-693 Project, Computer Science Department, UMBC (April 1993), Chairperson, Advisory Committee.

Katherine A. South, "Solving recurrences with generating functions: A tutorial," CMSC-693 Project, Computer Science Department, UMBC (June 1993), Chairperson, Advisory Committee.

Kirthivasan Venkatraman, "The vowel-count method in solving single columnar transposition ciphers: Its effectiveness and improvement," CMSC-693 Project, Computer Science Department, UMBC (January 5, 1992). Chairperson, Advisory Committee.

Konstantinos Kalpakis, "Refinements of a partitioning algorithm for the Steiner tree problem in d-dimensional Euclidean space," CMSC-693 Project, Computer Science Department, UMBC (December 19, 1991). Chairperson, Advisory Committee.

Kiran S. Panesar, "The vowel-count for solving single columnar transposition ciphers: Quantification, analysis, and improved tests," CMSC-693 Project, Computer Science Department, UMBC (August 21, 1991). Chairperson, Advisory Committee.

Virginia Schneeman, "Simulated annealing and iterative improvement: An experimental comparison," CMSC-693 Project, Computer Science Department, UMBC (August 18, 1991). Chairperson, Advisory Committee.

D. MS Theses—As Reader

Jason Dowd "Identifying malware using N-Gram clustering metrics," MS Thesis, UMBC (August 2014). Reader (Advisor: Nicholas).

Fahad Zafar, "Tiny encryption algorithm for cryptographic gradient noise," MS Thesis, UMBC (December 2009). Reader (Advisor: Olano).

Wei-cheng Lin, "Weak keys of the Data Encryption Standard: Regularities and cycle properties," CMSC-693 Project, Computer Science Department, UMBC (May 15, 1990). Reader (Advisor: Sidhu).

E. Undergraduate Theses

Horace H. Dediu, "The design and implementation of a multiprocessor simulator," honors thesis, Department of Electrical Engineering, Tufts University (fall 1988). Reader.

F. Independent Study Projects (selected)

Travis Mayberry, "Implementation improvements to the Scantegrity II voting system," CMSC-699: Independent study in computer science, Dept. of CSEE (spring 2010), UMBC.

John Conway, "Implementation improvements to the Scantegrity II voting system," CMSC-499: Independent study in computer science, Dept. of CSEE (spring 2010), UMBC.

Michael Rushanan, "Range voting in practice," CMSC-690: Independent study in computer science, Dept. of CSEE (spring 2009), UMBC.

Brian Roberts, William Byrd, Matthew Baker, John Simmons, "Cyber Defense Exercises at UMBC" (summer 2003). Supervisor of summer lab assistants.

Anthony Falcone, "Design and implementation of a digital telestrator for exhibition chess matches," CMSC-699: Independent Study in Computer Science, Dept. of CSEE (spring 98), UMBC.

Michael D. Miller, "Course tools for CMSC-443: Cryptology," independent study project (spring and summer 1995), UMBC.

Brian E. Brzezicki and Uriel Nordenberg, "Hypermedia tools for teaching discrete mathematics," non-credit independent study project (summer 94, fall 94), UMBC.

Ann Pollack, "On the complexity of module orientation problems in VLSI layout," CMSC-699: Independent Study in Computer Science, Computer Science Department, UMBC (spring 1994).

David M. Lazoff, "An exact formula for the expected wire length between two randomly chosen terminals," CMSC-699: Independent Study in Computer Science, Computer Science Department, UMBC (spring 1994).

Predag Tosic, "Discrete mathematics for computer science," Independent study and credit by examination for CMSC-203, UMBC (summer 1993).

Thomas R. Cain, "Cryptanalysis of filter generators," CMSC-699: Independent Study in Computer Science, Computer Science Department, UMBC (fall 1992, spring 1993).

Muhammad A. Rabi, "Introduction to cryptology," CMSC-699: Independent Study in Computer Science, Computer Science Department, UMBC (spring 1992).

Ellen F. Rakatansky, "A relaxation method for breaking transposition ciphers," CSC-194: directed study, Department of Computer Science, Tufts University (spring 1987). [In addition to our work on transposition ciphers, Ratakansky and I solved the 1986 Cryptogift $50,000 Puzzle Game sponsored by the The Swiss Colony.]

Margaret A. Konner, "Implementing a new cryptographically secure pseudorandom number generator based on the elliptic logarithm problem," CSC-194: directed study, Department of Computer Science, Tufts University (spring 1986).

David Hunt, Margaret A. Konner, Sarah B. Levine, Stanley N. Marshall III, Ellen F. Rakatansky, and Andriés E. Sadler, "Cryptanalysis of the $100,000 Decipher II Puzzle," extracurricular group project, Department of Computer Science, Tufts University, (fall 1985).

Robert Baldwin, Ravi Bopanna, John Chang, Joseph Marshall, and David Saslow, "Solving the $100,000 Decipher Puzzle," IAP (Independent Activities Period) Course 4505, MIT, (January 1984). [In March 1985, Baldwin and I eventually solved the puzzle. The work carried out during this mini-course laid the foundation for our solution.]

Scholarly and Creative Works[2]

A. Books (2)

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

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

B. Research Articles in Refereed Journals (19)

3. Michael Oehler, Dhananjay S. Phatak, and Alan T. Sherman, "A conjunction, language, and system facets for private packet filtering," *Journal of ASE Science*, Vol. 1, No. 2 (August 15, 2013), 103120.

4. Dykstra, Josiah, and Alan T. Sherman, "Design and Implementation of FROST: Digital Forensic Tools for the OpenStack Cloud Computing Platform," *Digital Investigation*, Vol. 10 (2013), S87–S95.

5. Phatak, Dhananjay, Alan T. Sherman, Nikhil Joshi, Bhushan Sonawane, Vivek G. Relan, and Amol Dawalbhakta, "Spread Identity: A new address remapping mechanism for anonymity and DDoS defense," *Journal of Computer Security*, vol. 21 (2013), 233–281.

6. Dykstra, Josiah, and Alan T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques," *Digital Investigation* Vol. 9 (2012), S90–S98.

7. 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*, Vol. 36, No. 2 (2012), 129–148.

8. Dykstra, Josiah, and Alan T. Sherman, "Understanding issues in cloud forensics: Two hypothetical case studies," *Journal of Network Forensics*, Vol. 3, Issue 1 (Autumn 2011), 19–31. [This paper won the Outstanding Case Study Award for 2012 by the The American Academy of Forensic Sciences.]

[2]For a more complete and detailed list of my earlier works, see the separate document *Scholarly and Creative Works*. Until 2003, I always listed authors in alphabetical order.

9. 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 Transactions on Information, Forensics, and Security—special issue on voting,* Vol. 4, No. 4 (December 2009), 611–627.

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

11. Chaum, David, Aleks Essex, Richard Carback, Alan T. Sherman, Jeremy Clark, Stefan Popoveniuc, and Poori Vora, "Scantegrity: End-to-End voter-verifiable optical-scan voting," *IEEE Security & Privacy*, vol. 6, no. 3 (May/June 2008), 40–46. Special issue on e-voting, David R. Jefferson and Aviel D. Rubin, eds.

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), 444–458.

13. 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.

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

15. 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.

16. 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.

17. 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.

18. Ganesan, Ravi, and Alan T. Sherman, "Statistical techniques for language recognition: An introduction and guide for cryptanalysts," *Cryptologia*, **XVII**:4 (October 1993), 321–366.

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

19. 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.

20. 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.

21. 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.

C. Other Research Publications in Refereed Journals (2)

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

    [This refereed journal article reports on a chess match (March 24, 1995) that I organized, one of the first in which a computer defeated a human grandmaster under certified tournament conditions. http://www.cs.umbc.edu/conferences/mtd95/mm_match/]

23. Lazoff, David M., and Alan T. Sherman, "Expected wire length between two randomly chosen terminals," Problem 95-6, *SIAM Review*, vol. 37 (June 1995), 235.

    Lazoff, David M., and Alan T. Sherman; together with W. Boehm, "Expected wire length between two randomly chosen terminals," Problem 95-6 and solution, *SIAM Review*, vol. 38 (June 1996), 321–324.

    [This refereed problem&solution reports on a useful problem and its solution. In 1996, *SIAM Review* published an elegant solution by Boehm, including a passaage from my 1994 technical report in which Lazoff and I had independently described and analyzed our own solution in more detail. See: "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, revised August 2, 1994). 14 pages.]

D. Works Submitted for Publication (In Review) (3)

24. Price, Nathan, and Alan T. Sherman, "How to generate repeatable keys using Physical Unclonable Functions: Correcting PUF errors with iteratively broadening and prioritized search," submitted to the *Journal of Cryptographic Engineering* (June 29, 2014), 9 pages.

25. Nguyen, Christopher, Dhananjay S. Phatak, Steven D. Houston, and Alan T. Sherman, "A preliminary FPGA implementation and analysis of Phataks quotient-first scaling algorithm in the reduced-precision residue number system," submitted to the *Journal of Cryptographic Engineering* (June 29, 2014). 6 pages.

26. Dhananjay S. Phatak, Q. Tang, Alan T. Sherman, Warren D. Smith, Peter Ryan, and Kostas Kalpakis, "SingleMod and DoubleMod: Simple randomized secret-key encryption with field," with bounded homomorphicity (February 6, 2014), 24 pages, submitted to *Journal of Cryptography and Communications*.

E. Articles in Refereed Proceedings of Competitively-Selected Conferences (28)

27. Olano, Marc, Alan T. Sherman, Linda Oliva, Ryan Cox, Deborah Firestone, Oliver Kubic, Milind Patil, John Seymour, and Isaac Sohn, and Donna Thomas, "SecurityEmpire: Development and evalaution of a digital game to promote cybersecurity education" in *Proceedings of 3GSE '14: 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education*, (San Diego, August 18, 2014), 10 pages.

28. Michael Oehler, Dhananjay S. Phatak, and Alan T. Sherman, "A private packet filtering language for cyber defense," *Proceedings of the Annual Symposium on Information Assurance (ASIA'13)*, (June 4–5, 2013, Albany, NY), 46–55.

29. Dykstra, Josiah, Alan T. Sherman, "Design and implementation of FROST: digital forensic tools for the OpenStack cloud computing platform" in *Proceedings of the 2013 Digital Forensics Research Workshop (DFRWS 2013)*, (Monteray, CA, August 4–7), 10 pages.

30. Leschke, Timothy R., and Alan T. Sherman, "Change-Link: A digital forensic tool for visualizing changes to directory trees" in *Proceedings of VizSec '12* (Seattle, WA, October 15, 2012), 8 pages.

31. Dykstra, Josiah, Alan T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques" in *Proceedings of the 2012 Digital Forensics Research Workshop (DFRWS 2012)*, (Washington, DC, August 6–8), 9 pages.

32. 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

33. Leschke, Timothy, Alan T. Shermanm, and Penny Rheingans, "Using a fisheye view to visualize change-over-time in support of digital forensic examinations," 2011 Government Forum of Incident Response and Security Teams (GFIRST), (Nashville, TN, August 8-12, 2011), 12 pages. Accessed 4-20-12 from

http://www.us-cert.gov/GFIRST/presentations/2011/Visualizing_Change_Over_Time.pdf

34. Phatak, Dhananjay S., Alan T. Sherman, and J. Pinkston, "A new paradigm to approximate oblivious data processing (ODP) for data confidentiality in cloud computing," *IEEE Services 2011*, paper 4065 (Washington, DC, July 2011), 391–398.

35. Fink, Russell A., Alan T. Sherman, Alexander O. Mitchell, and David C. Challener, "Catching the cuckoo: Verifying TPM proximity using a quote timing side-channel (short paper)" in *Proceedings of 4th International Conference on Trust and Trustworthy Computing*, LNCS 6740, McCune, *et al.*, eds., Springer (Berlin, Germany, June 2011), 294–301.

36. Dykstra, Josiah, and Alan T. Sherman, "Understanding issues in cloud forensics: Two hypothetical case studies" in *Proceedings of the 2011 ADFSL Conference on Digital Forensics Security and Law* (May 2011), 191-206.

37. 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 *Proceedings of USENIX Security 2010*, (Washington, DC, August 2010). Accessed 11-24-11 from http://www.usenix.org/events/sec10/tech/full_papers/Carback.pdf

38. Sherman, Alan T., Richard Carback, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc, Ronald L. Rivest, Anne Sergeant, Emily Shen, Bimal Sinha, and Poorvi Vora, "Scantegrity mock election at Takoma Park" in *Proceedings of the 4th International Conference on Electronic Voting 2010 (e-vote.cc 2010)*, (Lochau, Austria, July 2010).

39. Krautheim, F., Dhananjay S. Phatak, and Alan T. Sherman, Introducing the Trusted Virtual Environment Module: A new mechanism for routing trust in cloud computing in *Proceedings of 3rd International Conference on Trust and Trustworthy Computing*, LNCS 6101, Acquisti, Smith, and Sadeghi, eds., Springer (Berlin, Germany, June 2010), 211–227.

40. Sherman, Alan T., Dhananjay Phatak, Bhushan Sonawane, Vivek G. Relan, "Location authentication through power line communication: Design, protocol, and analysis of a new out-of-band strategy" in *Proceedings of 14th IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*, (Rio de Janeiro, Brazil, March 2010), six pages. To be available on IEEE Explore.

41. Sherman, Alan T., Richard Carback, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc, Ronald L. Rivest, Anne Sergeant, Emily Shen, Bimal Sinha, Poorvi Vora "Scantegrity mock election at Takoma Park (summary)" in *Proceedings of the NIST Workshop on End-to-End Voting Systems* (Washington, DC, October 2009), 3pages.

42. Fink, Russell A., and Alan T. Sherman, "Combining end-to-end voting with trustworthy computing for greater privacy, trust, accessibility, and usability (summary)" in *Proceedings of the NIST Workshop on End-to-End Voting Systems* (Washington, DC, October 2009), 3pages.

43. Chaum, David, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y.A. Ryan, Emily Shen, Alan T. Sherman, "Scantegrity II: End-to-End verifiability for optical scan election systems using invisible ink confirmation codes" in *Online Proceedings of USENIX/ACCURATE Electronic Voting Technology Workshop (EVT/WOTE '08),* (July 28–29, 2008). 13 pages. Accessed 9-1-08 from http://www.usenix.org/events/evt08/tech/full_papers/chaum/chaum.pdf

44. Carback, Richard, Stefan Popoveniuc, Alan Sherman, and David Chaum, "Punchscan with independent ballot sheets: 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. 8 pages. Accessed 2-18-08 from http://research.microsoft.com/conferences/WOTE2007/program.htm

45. 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 *Online Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '06)* (August 1, 2006). 14 pages. Accessed 9-1-08 from http://www.usenix.org/events/evt06/tech/full_papers/sherman/sherman.pdf

46. 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

47. 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.

48. 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.

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," *Proceedings of the DARPA Information Survivability Conference & Exposition (DISCEX 00)*, IEEE Computer Society (January 25–27, 2000), 127–139.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.
    [By agreement with Plenum Press, this paper will not be published elsewhere.]

F. Patents (4)

55. Dinsmore, Peter T. Michael Heyman, Peter Kruus, and Alan T. Sherman, United States Patent Number 7,590,247, "System and method for reusable efficient key distribution" (Sept. 15, 2009). Assignee: McAfee, Inc. (Santa Clara, CA). Filed: April 18, 2001.

56. 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). Filed April 18, 2001.

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). Filed July 21, 2000.

58. 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). Filed June 21, 2000.

G. Other Publications (13)

59. Sherman, Alan T., Warren D. Smith, and Richard T. Carback III, "Scoring the candidates: Range voting would prevent third-party spoilers—and give voters more say," *MIT News* in *Technology Review*, vol. 111, no. 5 (September/October 2008), M16–M17. Also available on-line: accessed 9-1-08 from http://technologyreview.com/article/21172/

60. Sherman, Alan T., Warren D. Smith, and Richard T. Carback III, "How we think range voting would have affected the 2008 U.S. presidential race," on-line sidebar, *MIT News* in *Technology Review*, vol. 111, no. 5 (September/October 2008), accessed 9-1-08 from http://www.technologyreview.com/article/21211/

61. Donald F. Norris, PI, Andrew Sears, and Charles Nicholas, CoPIs. Anne V. Roland, Ed. Aryya Gangopadhyay, Stephen H. Holden, George Karabatis, A. Gunes Koru, Chris M. Law, John Pinkston, Andrew Sears, Alan T. Sherman, and Dongsong Zhang, "A study of vote verification technologies. **Part I: Technical study appendices**," prepared for the Maryland State Board of Elections, National Center for the Study of Elections of the Maryland Institute for Policy Analysis and Research, University of Maryland, Baltimore County (February 2006). 75 pages. Accessed 6/2/06 from www.umbc.edu/mipar/documents/VoteVerificationAppendiceswebversion.pdf

62. Donald F. Norris, PI, Andrew Sears, and Charles Nicholas, CoPIs. Anne V. Roland, ed. Aryya Gangopadhyay, Stephen H. Holden, George Karabatis, A. Gunes Koru, Chris M. Law, John Pinkston, Andrew Sears, Alan T. Sherman, and Dongsong Zhang, "A study of vote verification technologies. **Part I: Technical study**," prepared for the Maryland State Board of Elections, National Center for the Study of Elections of the Maryland Institute for Policy Analysis and Research, University of Maryland, Baltimore County (February 2006). 68 pages. Accessed 6/2/06 from www.umbc.edu/mipar/documents/VoteVerificationStudyReport-FINAL_001.pdf

63. Sherman, Alan T., "A proof of security for the OFC and LKH centralized group-keying algorithms," NAI Labs TR 02-043D (November 2002). 26 pages.

64. 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.

65. 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).]

66. 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.

67. 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.

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

69. 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.

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

71. Sherman, Alan T., "On superpolylogarithmic subexponential functions (Part I)," *SIGACT News*, **22**:1 (winter 1991), Whole Number 78, 65–73. [This work was performed at the University of Maryland, College Park on December 11, 1991.]

H. Works in Preparation (selected)

72. Carback, Richard, Alan T. Sherman, and David Chaum, "A simple approach to mutually-attested threshold software: How to create, seal, and unseal a group secret with encryption and hashing," (draft: August 3, 2010), 12 pages. [I intend to submit a final version of this work to *IET Information Security Journal*.]

73. Russell A. Fink, Alan T. Sherman, and David C. Challener, "A human attestation protocol for trustworthy electronic voting: Bootstrapping trust using TPMs, smart cards, timings, and scratch-off codes" (June 2010), 17 pages.

74. Carback, Richard, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc, Ronald L. Rivest, Emily Shen, Alan T. Sherman, Bimal Sinha, and Poorvi Vora, "Exploring Reactions to Scantegrity: Analysis of survey data from Takoma Park voters and election judges" (April 2010), 19 pages. [I intend to submit to *Social Science Computer Review*.]

75. Sherman, Alan T., "A report on the VoComp 2007 international voting system design competition," (draft: April 22, 2007), 6 pages.

76. 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. [I intend to submit a final version of this work to *PLOS Biology*.]

77. 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. [I intend to submit a final version of this work (which I presented at MIT on May 12, 2006) to *Cryptologia*.]

I. Theses

78. 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).]

79. 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.

Research Presentations (Selected)

1. "SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education,"
   - 3GSE '14: 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, San Diego, CA (August 18, 2014). Invited talk.
2. "Random sample elections,"
   - Rump Session, EVT/WOTE, Washington, DC (August 13, 2013).
   - Rump Session, USENIX Security, Washington, DC (August 14, 2013).
3. "Digital forensics in the cloud,"
   - Forensics Enabled Intelligence (FEI) 2013, Alexandria, VA (April 22, 2013). Invited talk (co-speaker: Josiah Dykstra).
4. "Scantegrity: End-to-end verifiable elections using invisible ink"
   - 2013 Mid-Atlantic Collegiate Cyber Defense Competition (CCDC) Speaker Symposium, Johns Hopkins Applied Physics Laboratory (APL), Scaggsville, MD (April 10, 2013). Invited talk. [video of talk: http://www.maccdc.org/2013-symposium-video/]
5. "Scantegrity III: Automatic trustworthy receipts, highlighting over/under votes, and full voter verifiability"
   - 2011 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '11), San Francisco, CA (August 8, 2011).
6. "A new paradigm to approximate oblivious data processing (ODP) for data confidentiality in cloud computing"
   - Workshop on Privacy and Security in Cloud Computing, IEEE Services 2011 Washington, DC (July 9, 2011).
7. "Scantegrity II at Takoma Park: The first End-to-End binding governmental election with ballot privacy"
   - CSEE Research Review, UMBC (May 7, 2010).
8. "Location authentication through powerline communication: Design, protocol, and analysis of a new out-of-band strategy"
   - IEEE International Symposium on Powerline Communications and Its Applications (ISPLC), Rio de Janeiro, Brazil (March 30, 2010).
9. "Scantegrity mock election at Takoma Park"

- NIST Workshop on End-to-End Voting Systems, Washington, DC (October 13, 2009).

10. "Voting in America: Problems, past, present, possible solutions"
    - George Washington University (October 18, 2007).
11. "A study of vote verification technologies"
    - USENIX/Accurate Electronic Voting Technology (EVT) Workshop, Vancouver (August 1, 2006)
    - Threat analyses for voting system categories: A workshop on rating voting methods (VSRW 06), (invited talk), Washington, DC (June 9, 2006)
    - MIT Computer Science and Artificial Intelligence Lab (May 11, 2006)
    - CSEE Research Review, UMBC (May 5, 2006)
    - George Washington University (May 4, 2006).
12. "The Rivest-Sherman ciphertext-only attacks on Enigma-like machines"
    - MIT Computer Science and Artificial Intelligence Lab (May 12, 2006)
13. "Developing and delivering hands-on information assurance exercises: Experiences with the Cyber Defense Lab at UMBC"
    - West Point Workshop on Information Assurance, USMA, NY (June 11, 2004)
14. "Key establishment in large dynamic groups"
    - National Security Agency (NSA), MD (October 13, 2000, and fall 1997)
    - MIT Lab for Computer Science (spring 1999)
    - US Naval Academy, Annapolis, MD (March 24, 1999)
    - University of Richmond, VA (January 21, 1999)
    - DARPA, Ballston, VA (March 2, 1998)
    - Trusted Information Systems, Inc., Glenwood, MD (February 27, 1998)
15. "Electronic money"
    - Induction ceremony of the *Sigma Xi* honorary society (invited talk), Villanova University (April 19, 1996).
16. "How to break Gifford's cipher"
    - University of Arizona, Tucson (March 8, 1997). Conference of the Mathematics of Cryptography/Security (invited talk). Southwest Regional Institute in the Mathematical Sciences.
    - Crypto 94 (Rump Session), Univ. of California Santa Barbara (August 23, 1994).
    - AT&T Bell Laboratories, Murray Hill, NJ (July 17, 1994).
    - MIT Laboratory for Computer Science (May 12, 1994).
    - University of Maryland, College Park (March 24, 1994).
    - University of Delaware (March 21, 1994).
17. "Statistical techniques for language recognition: An introduction and empirical study for cryptanalysts"

- University of Pennsylvania (April 15, 1993).

18. "Probabilistic analysis of an enhanced partitioning algorithm for the Steiner tree problem in R^d"
    - 13th Annual Allerton Conference on Communication, Control, and Computing, University of Illinois at Urbana-Champaign (October 1, 1992).
19. "A simplified approach to probabilistic polynomial-time complexity classes"
    - UMBC (May 8, 1991).
20. "How we solved the $100,000 Decipher Puzzle (16 hours too late)"
    - Math Colloquium, University of Maryland, College Park (June 11, 2003).
    - Capital Area Theory Seminar, University of Maryland, College Park (April 11, 1990).
    - Eurocrypt 85 (Rump Session), University of Linz, Austria (April 10, 1985).
21. "Tight analysis of Bennett's time-space tradeoff for reversible computation"
    - UMBC (November 1989).
22. "VLSI placement and routing: The PI System"
    - University of Maryland, College Park (April 4, 1990).
    - UMBC (March 14, 1989).
    - Brandeis University (February 2, 1989).
23. "What is a zero-knowledge proof?"
    - Brandeis University (April 30, 1987).
24. "Algorithms for placing modules on a custom VLSI chip"
    - Tufts University (December 2, 1987).
    - MIT VLSI Research Review (May 19, 1986).
25. "Is the Data Encryption Standard a group?"
    - Johns Hopkins University (March 15, 1989).
    - George Mason University (February 16, 1989).
    - The American University (February 15, 1989).
    - Brandeis University (April 18, 1985).
    - Eurocrypt 85, University of Linz, Austria (April 10, 1985).
    - Tufts University (March 18, 1985).
26. "A taxonomy of randomized encryption techniques"
    - Crypto 82, University of California, Santa Barbara (August 23, 1982).

Service to Department, College, University, Community, Profession

A. Service to the Profession

Journal Editor:

Cryptologia, Member Technical Editorial Board (2005–present, December 1994–December 2000).

Grant Review Panelist:

National Science Foundation (10-07, 2-07, 3-14).

Grant Reviewer:

National Science Foundation (8/99, 8/90).

Academic Program Reviewer:

University of Maryland, University College (UMUC), (spring 2014).

Program Committee for Competitively-Selected Conferences:

IASTED International Conference on Communication, Network, and Information Security (CNIS), (spring 2006)
Crypto 95 (spring 95).

Conference Reviewer:

1998 USENIX Annual Technical Conference (October 1997)
1st ACM Conference on Computer and Communications Security (spring 93)
Fifth MIT Conference on Advanced Research in VLSI (spring 88).

Book Reviewer:

Addison-Wesley (spring 87)
Kluwer Academic Publishers (fall 87)
Prentice Hall (fall 97, spring 88)
Wiley (spring 2014).

Journal Reviewer:

Cryptologia (9/13, 3/12, 3/11, 6/10, 1/07, 12/06, spring 01, summer 93)
Discrete Applied Mathematics (fall 83)
IEEE Transactions on Computers (spring 89)
IEEE Transactions on Information, Forensics, and Security (summer 09)
IEEE Transactions on Information Theory (fall 87)
IEEE Transactions on Systems, Man, and Cybernetics (spring 85)
Information and Computation (7/94)
Information Processing Letters (12/03,3/02)
International Journal of Electronic Government Research (9-06)
Journal of Computer and Systems Sciences (fall 80)
Journal of Cryptology (6/10, 3/08, 3/96, 8/91, 3/91, 9/90, 7/90, spring 89)
SIAM Journal on Computing (spring 82, fall 80).

Conference Organizer:

- Innovations in Cybersecurity Education Workshop (June 25, 2014), UMBC.
- VoComp University Voting Systems Competition and Conference (July 16–18, 2007), Portland, Oregon.
- Informatics Maryland: The State of Informatics Success and Challenges (November 28, 2006), Linthicum, Maryland. Organized panel on information assurance.
- Maryland Theory Day at UMBC, April 11, 1997, UMBC. Co-organizer (December 1996–May 1997).
- Workshop: Applying Cryptography in Electronic Commerce, 1996 ACM Computer Science Conference, Philadelphia, PA (February 17, 1996).
- Maryland Theory Day at UMBC, March 24, 1995, UMBC. Co-organizer (August 1994–June 1995).
- Maryland Theory Day at UMBC, March 19, 1993, UMBC. Co-organizer (December 1992–June 1993).
- Crypto 82: A Workshop on the Theory and Practice of Cryptographic Techniques, August 23–25, 1982, University of California, Santa Barbara. Member, Organizing Committee (January–August 1982).

Board Member:

- Research Board, Majority Decisions (March 2013–date).
- Technical Advisory Board, Spectoccular (June 2013–date).
- Maryland Center of Academic Excellence (CAE) Collabortation Cyber Security Virtual Resource Lab (Cyber Battle Lab), Capitol College (fall 2010-date).
- Voting Systems Institute, Washington, DC (2011-date).

B. Service to the UMBC Department of CSEE

Director, Center for Information Security and Assurance (CISA). Wrote successful proposal for UMBC to be designated by DoD/DHS as a National Center of Academic Excellence in Information Assurance Education (fall 2000–date). Wrote successful applications for renewals of this designation. Wrote successful application for UMBC also to be designated as a National Center of Academic Excellence in Information Assurance Research. Recruited students to UMBC to study information assurance, and created the *Cyber Defense Lab (CDL)* for students and faculty to carry out research and educational projects.

Leader, Security Technology Research Group (STRG). Organized talks on cryptology (fall 95–fall 00).

Organizer, CSEE Research Review. Created and organized an annual meeting of the Dept. to celebrate recent research accomplishments by faculty and students (spring 06–spring 13).

Director, Graduate Program. Responsible for all aspects of the M.S. and Ph.D. graduate programs in computer science (February 1995–June 1996).

Department Committee Member:

- Graduate Admissions Committee (fall 2013-present, fall 07–August 2011, Chair February 14-date). Evaluated applications to the MS and PhD programs in CS.
- Adjunct Recruitment and Evaluation (fall 12–spring 2013).
- Colloquium/Guest Speaker Committee (Chair: fall 08-present. Member: fall 02–present). Organized special talks at UMBC.
- Graduate Committee (fall 07–August 08, fall 89–August 96). Discussed and proposed ways to improve the graduate program. Wrote guidelines for the CMSC-693 master's project. Evaluated graduate applications.
- Hiring Committee (fall 12–present, fall 99–August 02, spring 92). Read hundreds of applications and met with applicants.
- Graduate Planning Committee (fall 95–fall 96). Developed revised graduate program for newly merged Department.
- Undergraduate Planning Committee (fall 95–spring 96). Made recommendations to improve the undergraduate program in computer science.
- Space Committee (spring 93–summer 94). Organized the selection and purchase of new furniture for the Department's seminar and laboratory areas.
- Tenure and Promotion Committee (fall 96–present).
- Undergraduate Committee (fall 03–August 07, spring 98–August 02, spring 97) Wrote proposal for a departmental honors program in computer science.
- Chair Search Committee (spring 97, fall 03). Interviewed and reviewed candidates for the position of Department Chair.
- Scheduling Committee (spring 1999–spring 03, fall 90–spring 91,).
- Library Committee (spring 91–fall 91). Advised Kuhn Library on book purchases.

Classroom Observer. Observed computer science instructors (fall 89–spring 97).

Comprehensive Examinations. Wrote and graded the following comprehensive written examinations: M.S. exam in algorithms (fall 89, spring 89, fall 91, fall 92, fall 95); Ph.D. exam in algorithms (summer 90, winter 91, fall 91, winter 92, fall 92, winter 93, fall 93, winter 94, fall 94, winter 95, fall 95, winter 96, fall 96, winter 97, winter 99, summer 99, winter 00, summer 00, winter 01, fall 01, winter 04).

Advisor. Advised computer science graduate and undergraduate students (spring 1990–present). Computer Science Advisor to Meyerhoff student (spring 92).

Course Coordinator.
CMSC-203 (spring 2001–spring 03)
CMSC-441 (spring 2001, fall 03)
CMSC-443 Cryptology (fall 99–spring 2005).

Invited Speaker:

- "Cryptography and language," guest lecture, Linguistics 209, UMBC (November 24, 1997). Instructor: Thomas Field.
- "Electronic money," Honors College (April 8, 1996).
- "How to play mental poker," Undergraduate Computer Science Colloquium (October 13, 1992). Sponsored by Computer Science Department and Honors College.

C. Service to the UMBC College of Engineering and Information Technology

Department Representative, Attended receptions and luncheons for prospective engineering students (1997–date).

College Committee Member:

- Hiring committee to select new Chair of the Dept. of CSEE (spring 97).
- Space Committee (fall 96–spring 97). Analyzed current space use, and suggested policies and plans for future space use.

D. Service to the University (other than chess)

University Committee Member:

- Member, Faculty Award Review Committee (January 2003).
- Member, Executive Committee, UMBC Chapter of *Phi Beta Kappa* (fall 98–spring 2000).
- Nominating Committee (August 96–spring 97). Nominated members for all standing University Committees.
- 30th Anniversary Steering Committee (spring 96–fall 96). Helped plan UMBC's 30th anniversary celebration.
- *Ad Hoc* Task Force Committee to Study the Student Course Evaluation Questionnaire. (Spring 1992–July 1996). Proposed ways to nurture and to improve effective teaching at UMBC.

- University Subcommittee on Instruction—Information Transfer and Technology Committee (fall 93–August 94). Proposed ways for UMBC to make effective use of emerging educational technologies.
- *Ad Hoc* University Committee on Mathematical Software (spring 1992). Helped develop UMBC policy on mathematical software.

Department Representative, Orientation for parents of freshmen (July 13, 1990). President's reception for academically talented students (September 28, 1994). Computer Science transfer students (April 18, 1997). Luncheon for scholarship recipients (spring 97–date).

UMBC Representative, Career Fair, Meade High School, April 12, 2012.

Reviewer, Technology Incubator, University of Maryland, College Park (9/03).

Meyerhoff Interviewer, Interviewed candidates for Meyerhoff scholarships (spring 96, 95, 94).

Adjudicator, Oral examination of English proficiency for prospective teaching assistants (August 95, August 94, spring 94).

Judge, Twelfth Annual Graduate Research Day (May 2, 1990). Judged oral presentations of research in mathematics and computer science.

Member, Steering Committee, Fifth Annual Maryland Computer Bowl (spring 1989). Helped plan and run Computer Bowl. Served as a head judge, and gave computer demonstrations to high school teachers.

E. Service to the Community (other than chess)

Women's Self-Defense. Assisted instructors in the UMBC winter-session course PHED-129/WMST-099: Women's Self-Defense by sharing my expertise as a shodan (first-degree black belt) in the Japanese martial art of Tomiki Aikido (1/94,1/93,1/92). [Instructors: Kim Knapp and Brian Sutherland]

F. Service to the University and Community Through Chess

Chair, College Chess Committee, US Chess Federation (2001–2003). Committee Member, 1996–date. Played an important role in bringing about reforms to college chess eligibility requirements, which took effect in January 2004.

Director, UMBC Chess Program, and Faculty Advisor, UMBC Chess Club (fall 1991–date). Initiated and promoted chess activities at UMBC, including recruiting, fundraising, team competition, chess instruction, public relations, special events, and advising Chess Club Officers.

(a) Organized UMBC's participation in the Pan-American Intercollegiate Team Chess Championships (1993–present). UMBC won (or tied for first place) ten times (96,98–02,05,08-09,12)—more times than for any other college in the history of college chess. In 1990, before I became involved, UMBC placed 26th out of 27 teams.

(b) Organized UMBC's participation in the Presidents's Cup ("Final Four of College Chess") (2001–present). UMBC won six times (02–05,08-09)—no college has won more times.

(c) Arranged intercollegiate matches with other schools, with wins over MIT (95), Harvard (96), University of Pennsylvania (97), Princeton (99), and Yale (99).

(d) Raised over $218,000 in external support for chess at UMBC.

(e) Established two endowments for the UMBC Chess Program: UMBC Chess Endowment (unrestricted), UMBC Chess—Alvin S. Mintzes Endowment (restricted to support the UMBC Open—Alvin S. Mintzes Chess tournament). Was instrumental in securing (what has become) a $20,000 bequest to the restricted endowment, and helped bring the unrestricted endowment now to over $10,000.

(f) Recruited many chess-player scholars to UMBC from throughout the world, including some who turned down offers from Harvard, Yale, and MIT. A few examples: International Grandmaster (GM) Ilya J. Smirin ranked 27th in world (95, Belarus); former World Junior Champion International Grandmaster Tal Shaked (98, USA); 2000 USA Junior Champion IM Eugene Perelshteyn (98, USA), now a GM; GM Alexander Onischuk, 2006 USA Champion (02, Ukraine); GM Pawel Blehm, former Captain of World Junior Team (02, Poland); International Woman Grandmasters (WGM) Katerina Rohonyan (04, Ukraine) and Sabina Foisor (08, Romania).

(g) Hosted major chess events, including: 1994-95 Maryland Scholastic Chess Championship (March 11, 1995), Pan-American Chess Championships (December 27–30, 1996, Baltimore), 2000 US Junior Chess Championship and US Junior Chess Open (July 2000), 2006 Pan-American Chess Championships (December 27-30, 2006, Washington, DC), and 2008 President's Cup (April 5-6, 2008, UMBC).

(h) Organized spectator chess events:
Man vs. Machine Match—Sagalchik vs. *Socrates (March 1995),
Exhibition Chess Match—Smirin vs. Morrison (June 21–22, 1996),
UMBC Action Chess Playoffs (October 1998, October 1999),
UMBC Speed Chess Spectacular (May 2003), and
Connections Academy Exhibition Match (August 2008–present).

Developed and applied technology to enhance these events through Internet broadcast of moves, video projection of games from autosensory chessboard, chess telestration, and FM transmission of live sports commentary.

(i) Arranged visits to UMBC by former World Chess Champions Garry Kasparov (May 17, 2007) and Anatoly Karpov (April 6, 2005).

(j) Created, organized, and developed the *Master Preparation* chess course, taught by Grandmaster Smirin, Master Epshteyn, and others. Made this course available to people throughout the world via a variety of internet technologies, including Mbone multicasts, www pages, email, and office hours on the Internet Chess Club. Our 85 Master Preparation videotapes were sold through the WWW Chess Superstore (www.smartchess.com).

(k) Supported the chess club at Arbutus Middle School (fall 2007–present).

(l) Organized UMBC Chess Masters, Johns Hopkins Center for Talented Youth, February 19, 2012, at UMBC (a day of chess activities and instruction for 55 students and their parents).

(m) Created the Summer Chess Camp at UMBC and served as Executive Director (summers 1996–2000).

(n) Wrote articles about Club activities published in the student newspaper *The Retriever*, the *Baltimore Sun*, the *Maryland Chess Newsletter*, and *Chess Life*.

(o) Played on the Faculty Chess Team in annual student-faculty chess matches (spring 91–date).

(p) Was instrumental in UMBC being selected as *Chess College of the Year* in 2000 by the US Chess Federation.

(q) Generated significant favorable publicity for UMBC through chess, including dozens of stories in newspapers including *Baltimore Sun* and *Washington Post*, interviews on National Public Radio, and feature stories on local and national TV—see comment at end of funding section.

Professional Memberships and Conferences Attended

A. Membership in Honorary Societies

Delta Epsilon Phi
National Honor Society
Phi Beta Kappa
Sigma Xi

B. Membership in Professional Organizations

Current:
Advanced Computing Systems Organization (USENIX)
Association for Computing Machinery (ACM)
Association of American University Professors (AAUP)
Institute of Electrical and Electronics Engineers (IEEE), Senior Mmeber

Previous:
American Mathematical Society (AMS)
International Association for Cryptologic Research (IACR)
Mathematical Association of America (MAA)
Society for Industrial and Applied Mathematics (SIAM)

C. Conferences Frequently Attended

Current:
National Colloquium for Information Systems Security Education (CISSE)
USENIX/ACCURATE Electronic Voting Technology Workshop (EVT/WOTE)
USENIX Security Symposium (USENIX Security)

Previous:
International Cryptology Conference (Crypto)

Teaching Experience

A. UMBC

Requried classroom courses taught:
CMSC-203 Discrete Structures (spring 94, fall 99, spring 00, fall 00, spring 01, fall 01, spring 02, fall 02, spring 08, fall 09, spring 11)
CMSC-441 Algorithm Design and Analysis (fall 90, fall 93, spring 95, fall 96, spring 97, fall 98, spring 01, fall 03, fall 07, fall 08, spring 10, fall 10, fall 12, fall 2013)
CMSC-641 Design and Analysis of Algorithms (fall 89, fall 91, fall 92, fall 95, fall 98, fall 99, spring 00, fall 01, fall 05, spring 07, spring 09, spring 2013, fall 2013)

Elective classroom courses taught:
CMSC-443 Cryptography and Data Security (spring 91, fall 94, spring 99, spring 02, spring 11, spring 13)
CMSC-444/644 Information Assurance (fall 06, spring 08, fall 12), (as 491i/691i: fall 05), (as 791i: spring 03, spring 04).
CMSC-491v/691v Electronic Voting (spring 06, spring 07, fall 08, fall 10)
CMSC-603 Advanced Discrete Structures (spring 92–95, spring 99)
CMSC-652 Cryptography and Data Security (spring 90, fall 92, fall 94, spring 97, fall 00, fall 02, fall 03, spring 09)
CMSC-691 Cybersecurity Research Seminar (spring 14)
CMSC-691 Special Topics in Cryptology (spring 93)
CMSC-691g Internet Security (spring 96)
CMSC-691u Unix System Security Administration and Policy (spring 07). Instructor of record (Classroom instructors: Geoff Weiss, William Farrell).
CMSC-791 Computer Chess (fall 95)

Research courses taught:
CMSC-499 Independent Study in Computer Science
CMSC-693 Research and Writing Skills for Computer Scientists
CMSC-699 Independent Study in Computer Science
CMSC-799 Master's Thesis Research
CMSC-898 PhD Research (pre-candidacy)
CMSC-899 Doctoral Dissertation Research.

Non-credit chess courses organized:
Master Preparation (fall 95*, spring 96*, fall 97, fall 98, spring 99, fall 99, spring 00).
(* Coordinated through Continuing Education and delivered over the internet.)

B. Tufts

Courses taught:
CSC-11 Introduction to Computer Science (spring 86)
CSC-71 Data Structures (spring 87)
CSC-60 Algorithms (fall 87, fall 88)
CSC-150c Cryptology (fall 85, spring 87)
CSC-150v VLSI Algorithms (spring 86)
CSC-163 Algorithms (fall 86)
CSC-260 Algorithms (spring 88, spring 89)
CSC-270 Theory of Computation (fall 87, fall 88).

Courses assisted:
CSC-11 Introduction to Computer Science (fall 85)
CSC-71 Data Structures (fall 86).

C. MIT

Sections taught as Recitation Instructor:
6.030 Introduction to Computation (fall 79, spring 81: Professor J. C. R. Licklider in charge)
6.001 Structure and Interpretation of Computer Programs (spring 82: Professors Abelson and Sussman in charge).

Courses assisted as Teaching Assistant:
6.031 Structure and Interpretation of Computer Programs (spring 79: Professors Abelson, Fano, and Sussman in charge)
6.046 Introduction to Algorithms (fall 82: Professor Ronald Rivest in charge).

Hobbies

Piano, Tomiki Aikido, chess, tennis, hiking, cycling, jogging, downhill skiing, flute, ballroom dancing.

Foreign Languages

Some knowledge of German and Japanese.

My Coordinates

A. Mailing Addresses

Office:
Dept. of CSEE
UMBC, 1000 Hilltop Circle
Baltimore, MD 21250 USA

Home:
3618 Ordway St., NW Washington, DC 20016

B. Telephone Numbers

Office:
(410) 455-2666 [Direct. Voice messages may be left 24 hrs. a day.]
(410) 455-3500 [Department Secretary]

Home:
(202) 966-7204 [There is an answering machine on this numbers.]

Cell:
(410) 963-4779 [There is an answering machine on this number.]

C. Fax Numbers

UMBC: (410) 455-3969 [Be sure to write my name of the fax cover page.]
Home: (202) 362-4838

D. Email Addresses

UMBC: sherman@umbc.edu
Consulting: alantsherman@gmail.com

E. URL to WWW Home Page

www.csee.umbc.edu/∼sherman