

Martin E. Hellman
Professor Emeritus
of Electrical Engineering
and
Affiliate of the
Center for International Security and Cooperation
Stanford University

730 Alvarado Court
Stanford, CA 94305

tel: (650) 857-1377
hellman@stanford.edu

Martin E. Hellman was born in New York, NY, in 1945. He received his B.E. from New York University in 1966, and his M.S. and Ph.D. from Stanford University in 1967 and 1969, all in Electrical Engineering. Prof. Hellman was a researcher at IBM's Watson Research Center from 1968-69 and an Assistant Professor of Electrical Engineering at MIT from 1969-71. He was on Stanford's EE faculty from 1971-1996, after which he went Emeritus. He served as Associate Chair of the EE Department, Chairman of EE Graduate Admissions, and as Associate Dean of Graduate Studies for minority student affairs. He has authored over 80 technical papers, 12 US patents, and a number of corresponding foreign patents.

Prof. Hellman is best known for his invention, with Diffie and Merkle, of public key cryptography. In addition to many other uses, this technology forms the basis for secure transactions on the Internet, and currently protects trillions of dollars in financial transactions every day. He has also been a long-time contributor to the computer security debate, starting with the issue of DES's key size in 1975, serving (1994-96) on the National Research Council's Committee to Study National Cryptographic Policy, and currently serving on Verified Voting's Board of Directors.

His work has been recognized by a number of awards, including the million-dollar ACM Turing Award (2015) — often likened to “a Nobel Prize for computer science.” Other awards include the 1978 IEEE Information Theory Group's Best Paper Award, election as a Fellow of the IEEE (1980), the IEEE's 1981 Donald G. Fink award (best tutorial or survey paper), the Electronic Frontier Foundation 1994 Pioneer Award, the Franklin Institute's 1997 Levy Medal, selection as a Marconi International Fellow (2000), election to the National Academy of Engineering (2002), the IEEE Hamming Medal (2010), induction into the National Inventors Hall of Fame (2011), induction into the Cyber Security Hall of Fame (2012), induction as a Stanford “Engineering Hero” (2012), and induction into the Silicon Valley Hall of Fame (2013).

Prof. Hellman's professional activities have included service as a member of the Board of Governors of the IEEE Information Theory Group, chairman of the 1978 IEEE Information Theory Workshop, Associate Editor of the *IEEE Transactions on Communications*, and an editor of the *Journal of Cryptology*. He serves on the Federation of American Scientists' Board of Experts and the Scientific Advisory Board of the “Nuclear Knowledges” program at Sciences Po, France's top political science institution.

He also has a deep interest in the ethics of technological development. With Prof. Anatoly Gromyko of Moscow, he co-edited *Breakthrough: Emerging New Thinking*, a book published simultaneously in Russian and English in 1988 during the rapid change in Soviet-American relations. His efforts include an address delivered to the 2019 annual meeting of Nobel Laureates (tinyurl.com/HellmanNobelTalk), “Rethinking National Security” (tinyurl.com/RNSweb), and *A New Map for Relationships: Creating True Love at Home & Peace on the Planet* (joint with his wife). His earlier work to develop an environment in which students of diverse backgrounds can function to the best of their ability has been recognized by three teaching awards from minority student organizations.

In his spare time, he enjoys people and finding where conventional wisdom is wrong. Before age intervened, he enjoyed soaring, hiking, and speed skating. He and his wife Dorothie have been married since 1967 and reside on the Stanford campus.

Education

Bronx High School of Science, June 1962.

New York University, B.E. Electrical Engineering, June 1966.

Stanford University, M.S. Electrical Engineering, June 1967.

Stanford University, Ph.D. Electrical Engineering, March 1969.

Technical Experience

Stanford University

Professor Emeritus of Electrical Engineering, 9/96-present.

Professor of Electrical Engineering, 6/79-9/96.

Acting Associate Dean of Graduate Studies, 8/89-6/90.

Associate Department Chairman for Graduate Admissions, 5/89-6/90.

Director, Information Systems Laboratory, 1/88-5/89.

Associate Department Chairman, 9/78-8/80.

Associate Professor of Electrical Engineering 6/75-6/79.

Assistant Professor of Electrical Engineering 9/71-6/75.

Research Assistant, 9/67-9/68.

Teaching and research in the area of information systems.

Massachusetts Institute of Technology

Assistant Professor of Electrical Engineering, 9/69-9/71.

Teaching and research in the area of information theory.

IBM Watson Research Center

Staff Member, Yorktown Heights, New York, 9/68-9/69.

Research and development in pattern recognition methodology.

Consultant

Independent consultant, 9/69-present.

Consultant to industry in the areas of cryptography, information theory, communications, and general engineering.

Hellman Associates, Inc.

President, 4/81-2/83 and 4/84-3/88.

Chairman, 2/83-3/84.

Continuing education, research, development and consulting in cryptography, electronic communications and computing.

The Binary Corporation

Vice President 4/75-4/76. Research, development and consulting in electronic communications and computing.

TRW Systems

Member of Technical Staff, Redondo Beach, CA 6/67-9/67 (summer).

Analysis and simulation of ballistic missile systems.

Aerospace Corporation

Member of Technical Staff, El Segundo, CA, 6/66-8/66 (summer).

Research and Development of GaAs Schottky barrier diodes.

Wheeler Laboratories

Engineer, Great Neck, New York, 6/65-9/65 (summer).

Development of microwave components for phased array radar systems.

Service to Professional and Civic Organizations

World Laureate Association, 2018-present.

Member of the Scientific Advisory Board of the “Nuclear Knowledges” program at Sciences Po, France’s top political science institution, 2017-present.

Federation of American Scientists, Board of Experts, 2015-present, Nuclear Security Advisory Board, 2011-present.

Verified Voting, Board of Directors 2021-present, Board of Advisors, 2013-2021.

Marconi Society, Board of Directors, 2011-2015.

Keddem Congregation, Adult Education Chair, 2008-2010.

Member, National Research Council Committee on National Cryptographic Policy, 1994-1996; advising Congress on national encryption policies.

Member of Editorial Board, *Journal of Cryptology*, 1992-1995.

IEEE Committee on Communications and Information Policy, Subcommittee on Privacy, 1986-1991: advising IEEE and U.S. government on information privacy and encryption policies.

Beyond War Foundation, National Staff, 1984-85: Senior Editor and Director of International Scientific Initiative. Western Editor-in-Chief, *Breakthrough: Emerging New Thinking*.

IEEE Awards Board, 1982.

Board of Governors, IEEE Professional Group on Information Theory, 1975-80.

Associate Editor for Communication Theory, IEEE Transactions on Communications, 1974-75.

Chairman, 1978 IEEE Information Theory Workshop

National Research Council Panel for Selection of NSF Fellows.

Editorial Committee and Publications Chairman, 1972 IEEE International Symposium on Information Theory.

Communication Theory Committee of the IEEE Communications Society.

San Francisco Section, IEEE Information Theory Group:

President, 1974-75.

Vice-President, 1973-74.

Secretary-Treasurer, 1972-73.

Honors and Awards

President of Estonia Cross of Terra Mariana (3rd class), 2019.

The ACM 2015 Turing Award

Silicon Valley Hall of Fame, inducted 2013.

Information Systems Security Association Hall of Fame, inducted 2013.

Stanford Engineering Hero, 2012. (The Stanford Engineering Heroes program recognizes the achievements of Stanford engineers who have profoundly advanced the course of human, social and economic progress through engineering. Hellman was among the first 23 Stanford engineering alumni or faculty given this honor.)

National Cyber Security Hall of Fame, inducted 2012.

National Academy of Inventors Hall of Fame, inducted 2012.

RSA Lifetime Achievement Award, 2012.

National Inventors Hall of Fame, inducted 2011.

Fellow of the Computer History Museum, 2011.

IEEE Hamming Medal, "For the invention of public key cryptography and its application to secure communications," 2010.

Elected a Fellow of the International Association for Cryptologic Research (2006) "For the invention of public-key cryptography and for pioneering open research in cryptology."

Elected to the National Academy of Engineering "for contributions to the theory and practice of cryptography," 2002.

Marconi International Fellow Award, 2000.

IEEE Koji Kobayashi Computers and Communications Award, 1999.

IEEE Information Theory Society Golden Jubilee Award, 1998.

Association for Computing Machinery, Kanellakis Award, 1997.

The Franklin Institute, Levy Medal, 1997.

National Computer Systems Security Award, 1996.

Electronic Frontier Foundation Pioneer Award, 1994.

Stanford Society of Black Scientists and Engineers, Outstanding Professor Awards, June 1987 and June 1989.

Stanford Society of Chicano and Latino Engineers and Scientists, Outstanding Professor Award, June 1989.

Tau Beta Pi Award for Undergraduate Teaching, Stanford University, June 1987.

IEEE Donald G. Fink Award (1981) for the outstanding tutorial or survey paper of 1979 ("Privacy and Authentication: An Introduction to Cryptography" joint with Diffie).

Elected a Fellow of the IEEE, "for contributions to cryptography", 1980.

1978 IEEE Information Theory Group Award for Best Paper Published in the Preceding Two Years ("New Directions in Cryptography", joint with Diffie).

California State Psychological Association Award for Distinguished Contributions to Consumer Protection (1978).

Honorable Mention (one of three) in Eta Kappa Nu's 1966 competition to name "The Most Outstanding Electrical Engineering Student in the United States."

IEEE 1966 Student Paper Contest: First prize for New York Section; Second prize for Region 1.

National Science Foundation Graduate Fellow 1966-68.

Tau Beta Pi (National Engineering Society).

Eta Kappa Nu (National Electrical Engineering Honor Society).

Sigma Xi (The Scientific Research Society of North America).

Arnold Award (NYU, Electrical Engineering Dept., 1966).

Outstanding Sophomore Cadet (NYU, Army ROTC, 1964).

Chemistry Award (NYU, 1963).

Publications

Most publications are available as PDFs online at tinyurl.com/HellmanPubs.

1. M. E. Hellman, *Learning with Finite Memory*, Ph.D. Thesis, Stanford University, Department of Electrical Engineering, 1969.
2. M. E. Hellman and I. Palocz, "The Effect of Neighboring Conductors on the Currents and Fields in Plane Parallel Transmission Lines," *IEEE Trans. on Microwave Theory and Technique*, Vol. MTT-17, May 1969, pp. 254-259.
3. T. M. Cover and M. E. Hellman, "The Two-Armed Bandit Problem with Time-Invariant Finite Memory," *IEEE Trans. on Info. Theory*, Vol. IT-16, March 1970, pp. 185-195.
4. M. E. Hellman and T. M. Cover, "Learning with Finite Memory," *Ann. of Math. Stat.*, Vol. 41, June 1970, pp. 765-782.
5. M. E. Hellman and T. M. Cover, "Finite Memory Decision Schemes," *Problmy Peredachi Informatsii*, Vol. 6, 1970, pp. 21-30, (In Russian).
6. T. M. Cover and M. E. Hellman, "Finite Memory Hypothesis Testing: Comments on a Critique," *IEEE Trans. on Info. Theory*, Vol. IT-16, July 1970, pp. 496-497, (Correspondence).
7. M. E. Hellman and J. Raviv, "Probability of Error, Equivocation, and the Chernoff Bound," *IEEE Trans. on Info. Theory*, Vol. IT-16, July 1970, pp. 368-372.
8. M. E. Hellman, "The Nearest Neighbor Classification Rule with a Reject Option," *IEEE Trans. on Sys. Sci. and Cybernetics*, Vol. SSC-6, July 1970, pp. 179-185.
9. M. E. Hellman and T. M. Cover, "On Memory Saved by Randomization," *Ann. Math Stat.*, Vol. 42, 1971, pp. 1075-1078.
10. R. A. Flower and M. E. Hellman, "Hypothesis Testing with Finite Memory in Finite Time," *IEEE Trans. on Info. Theory*, Vol. IT-18, May 1972, pp. 429-431, (Correspondence).
11. M. E. Hellman, "The Effects of Randomization Finite Memory Decision Schemes," *IEEE Trans. on Info. Theory*, Vol. IT-18, July 1972, pp. 499-502.
12. J. A. Horos and M. E. Hellman, "A Confidence Model for Finite-Memory Learning Systems," *IEEE Trans. on Info. Theory*, Vol. IT-18, Nov. 1972, pp. 811-813, (Correspondence).
13. M. E. Hellman and T. M. Cover, "A Review of Recent Results on Learning with Finite Memory," Special Volume of *Problems of Control and Info. Theory* containing selected papers from the Second International Symposium on Info. Theory, Publishing House of the Hungarian Academy of Sciences, Budapest, 1973.

14. M. E. Hellman and T. M. Cover, "Obucheniye c Konechnoy Pamyaty," *MATEMATIKA*, Vol. 17, No. 3, 1973, pp. 137-156. (This is a Russian translation of #4 above).
15. M. E. Hellman and T. M. Cover, "Ekonomia Pamyati c Pomoshchyu Randomizatsii," *MATEMATIKA*, Vol. 17, No. 4, 1973, pp. 125-128. (This is a Russian translation of #9 above.)
16. M. E. Hellman, "Finite Memory Algorithms for Estimating the Mean of a Gaussian Distribution," *IEEE Trans. on Info. Theory*, Vol. IT-20, May 1974, pp. 382-384 (Correspondence).
17. M. E. Hellman, "On Using Natural Redundancy for Error Detection," *IEEE Trans. on Comm.*, Vol. COM-22, Oct. 1974, pp. 1690-1693 (Correspondence).
18. A. B. Carleial and M. E. Hellman, "Bistable Behavior of ALOHA-Type Systems," *IEEE Trans. on Comm.*, Vol. COM-23, April 1975, pp. 401-410.
19. M. E. Hellman, "Error Detection in the Presence of Synchronization Loss," *IEEE Trans. on Comm.*, Vol. COM-23, May 1975, pp. 538-539.
20. C. R. Davis and M. E. Hellman, "On Tree Coding with a Fidelity Criterion," *IEEE Trans. on Info. Theory*, Vol. IT-21, July 1975, pp. 373-378.
21. M. E. Hellman, "Convolutional Source Encoding," *IEEE Trans. on Info. Theory*, Vol. IT-21, Nov. 1975, pp. 651-656.
22. T. M. Cover, M. A. Freedman and M. E. Hellman, "Optimal Finite Memory Learning Algorithms for the Finite Sample Problem," *Information and Control*, Vol. 30, January 1976, pp. 49-85.
23. S.K. Leung-Yan-Cheong and M. E. Hellman, "Concerning a Bound on Undetected Error Rate," *IEEE Trans. on Info. Theory*, Vol. IT-22, March 1976, pp. 235-237 (Correspondence).
24. W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. on Info. Theory*, Vol. IT-22, No. 6, Nov. 1976, pp. 644-654 (Invited Paper).
25. M. E. Hellman, "An Extension of the Shannon Theory Approach to Cryptography," *IEEE Trans. on Info. Theory*, Vol. IT-23, May 1977, pp. 289-294.
26. A. B. Carleial and M. E. Hellman, "A Note on Wyner's Wiretap Channel," *IEEE Trans. on Info. Theory*, Vol. IT-23, May 1977, pp. 387-390 (Correspondence).
27. W. Diffie and M. E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," *Computer*, June 1977, Vol. 10, No. 6, pp. 74-84.

28. S. C. Pohlig and M. E. Hellman, "An Improved Algorithm for Computing Logarithms Over $GF(p)$ and its Cryptographic Significance," *IEEE Trans. on Info. Theory*, Vol. IT-24, January 1978, pp. 106-110.
29. S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Trans. on Info. Theory*, Vol. IT-24, July 1978, pp. 451-456.
30. R. C. Merkle and M. E. Hellman, "Hiding Information and Signatures in Trap Door Knapsacks," *IEEE Trans. on Info. Theory*, Vol. IT-24, September 1978, pp. 525-536.
31. M. E. Hellman, "An Overview of Public Key Cryptography," *IEEE Communications Society Magazine*, Vol. 16, Nov. 1978, pp.24-32 (Invited Paper).
32. W. Diffie and M. E. Hellman, "Privacy and Authentication: An Introduction to Cryptography," *Proceedings of the IEEE*, Vol. 67, March 1979, pp. 397-427 (Invited Paper).
33. E. Verriest and M. E. Hellman, "Convolutional Encoding for Wyner's Wiretap Channel," *IEEE Trans. on Info. Theory*, Vol. IT-25, March 1979, pp. 234-236.
34. M. E. Hellman, "On Foiling Computer Crime," *IEEE Spectrum*, July 1979, pp. 31-41 (see pp. 32-39 for Hellman's portion).
35. M. E. Hellman, "The Mathematics of Public Key Cryptography," *Scientific American*, Vol. 241, No. 2, August 1979, pp. 146-157.
36. M. E. Hellman, "A Cryptanalytic Time-Memory Tradeoff," *IEEE Trans. on Info. Theory*, Vol. 26, July 1980, pp. 401-406.
37. R. C. Merkle and M. E. Hellman, "On the Security of Multiple Encryption," *Comm. of the ACM*, Vol. 24, No. 7, July 1981, pp. 465-467.
38. M. E. Hellman, "Another Cryptanalytic Attack on 'A Cryptosystem for Multiple Communication'," *Information Processing Letters*, Vol. 12, #4, August 13, 1981, pp. 182-183.
39. W. Diffie and M. E. Hellman, "Privacy & Authentication: An Introduction to Cryptography," *The Security of Data in Networks*, Donald W. Davies, ed., IEEE Computer Society Publications, 1981. (This is a reprint of #32 above.)
40. W. Diffie and M. E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," *The Security of Data in Networks*, Donald W. Davies, ed. IEEE Computer Society Publications, 1981. (This is a reprint of #27 above.)
41. W. Diffie and M. E. Hellman, "New Directions in Cryptography," *The Security of Data in Networks*, Donald W. Davies, ed. IEEE Computer Society Publications, 1981. (This is a reprint of #24 above.)

42. R. C. Merkle and M. E. Hellman, "Hiding Information and Signatures in Trap Door Knapsacks," *The Security of Data in Networks*, Donald W. Davies, ed. IEEE Computer Society Publications, 1981. (This is a reprint of #30 above.)
43. S. C. Pohlig and M. E. Hellman, "An Improved Algorithm for Computing Logarithms Over $GF(p)$ and its Cryptographic Significance," *The Security of Data in Networks*, Donald W. Davies, ed. IEEE Computer Society Publications, 1981. (This is a reprint of #28 above.)
44. W. Diffie and M. E. Hellman, "Privacy & Authentication: An Introduction to Cryptography," *Advances in Computer System Security*, pp. 217-247, Rein Turn, editor, Artech House, Dedham, MA, 1981. (This is a reprint of #32 above.)
45. E. Karnin, J. Greene and M. Hellman, "On Secret Sharing Systems," *IEEE Trans. on Info. Theory*, Vol. IT-29, January 1983, pp. 35-41.
46. M. E. Hellman, "An Overview of Public Key Cryptography," *Advances in Data Communications Management*, Heyden & Son, 1983. (This is a reprint of #31 above.)
47. M. E. Hellman and W. Diffie, "An Introduction to Cryptography," *Advances in Data Communications Management*, Heyden & Son, 1983. (This is a reprint of paper #32 above.)
48. M. E. Hellman and E.D. Karnin, "The Largest Super-Increasing Subset of a Random Set," *IEEE Trans. on Inform. Theory*, Vol. IT-29, January 1983, pp. 146-148.
49. M. E. Hellman and J. M. Reyneri, "Fast Computation of Discrete Logarithms in $GF(q)$," *Advances in Cryptology: Proceedings of CRYPTO 82*, Chaum et al, ed., Plenum Press, New York, 1983, pp. 3-13.
50. M. E. Hellman and J. M. Reyneri, "Drainage and the DES," *Advances in Cryptology: Proceedings of CRYPTO 82*, Chaum et al, ed., Plenum Press, New York, 1983, pp. 129-131.
51. M. E. Hellman, "An Overview of Public Key Cryptography," *IEEE Communications Society's Tutorials in Modern Communications*, Computer Science Press, 1983. (This is a reprint of #31 above.)
52. M. E. Hellman, "On the Inevitability and Prevention of Nuclear War," *The Bent of Tau Beta Pi* (the magazine of the Engineering Honor Society), Vol. 76, No. 1, pp. 28-31, Winter 1985.
53. M. E. Hellman, "On the Inevitability and Prevention of Nuclear War," *The Stanford Engineer*, Vol. 8, No. 1, pp. 18-23, 1985. (This is a reprint of #52 above.)
54. M. E. Hellman, "Beyond War," *Nytt fran Foreningen Svenska Ingenjorer Mot Karnvapen*, 1985, Nr 6 pp. 16-19, 1985. (This is a reprint of #52 above.)
55. M. E. Hellman, "Encryption," *IEEE ElectroTechnology Review* 1986, pp. 87-88, 1986. (Invited paper.)

56. M. E. Hellman, "On the Inevitability and Prevention of Nuclear War," *Peace Research Reviews*, Vol. 10, No. 3, pp. 38-48, 1986. (This is a reprint of #52 above.)
57. R. Winternitz and M. E. Hellman, "Chosen-Key Attacks on a Block Cipher," *Cryptologia*, vol. 11, No. 1, pp. 16-20, January 1987.
58. M. E. Hellman, "Commercial Encryption," *IEEE Network: The Magazine of Computer Communications*, vol. 1, No. 2, pp. 6-10, April 1987. (Invited paper.)
59. Sergei P. Kapitza and Martin E. Hellman, "A Message to the Scientific Community," Preface to *Breakthrough: Emerging New Thinking*, Walker and Co., New York, 1988, pp. xi-xx.
60. Sergei P. Kapitza and Martin E. Hellman, "Nayuka i Covremenni Mir," Preface to *Proriv: Stanovleniye Novogo Mishleniya*, Progress, Moscow, 1987, pp. 7-19. (This is a Russian translation of #59 above.)
61. Martin E. Hellman, "Nuclear War: Inevitable or Preventable?" in *Breakthrough: Emerging New Thinking*, Walker and Co., New York, 1988, pp. 80-85.
62. Martin E. Hellman, "Yadernaya Voina: Neizbezhna ili Predotvratima?," in *Proriv: Stanovleniye Novogo Mishleniya*, Progress, Moscow, 1987, pp. 122-129. (This is a Russian translation of #61 above.)
63. Sergei P. Kapitza and Martin E. Hellman, "Scientists Must Help Stop the Arms Race," *The Scientist*, vol. 2, No. 2, page 22, January 25, 1988. (Adapted from publication #59 above.)
64. Martin E. Hellman, "Harnessing Technology," *IEEE Spectrum*, vol. 25, February 1988, page 24.
65. H. R. Amirazizi and M. E. Hellman, "Time-Memory-Processor Tradeoffs," *IEEE Trans. on Info. Theory*, Vol. 34, pp. 505-512, May 1988.
66. M. E. Hellman, "The Mathematics of Public Key Cryptography," *Scientific American: Trends in Computing*, vol. 1, pp. 78-87, 1988. (Updated version of publication #35 above.)
67. M. E. Hellman, "The Nearest Neighbor Classification Rule with a Reject Option," in *Nearest Neighbor (NN) Norms: Pattern Classification Techniques*, Belur V. Dasarathy, Editor, IEEE Computer Society Press, 1991. (This is a reprint of #8 above.)
68. A. B. Carleial and M. E. Hellman, "Bistable Behavior of ALOHA-Type Systems," in *Multiple Access Communications*, Norman Abramson, Editor, IEEE Press, 1993. (This is a reprint of #18 above.)
69. M. E. Hellman, "Responses to NIST's Proposal," *Communications of the ACM*, vol. 35, No. 7, pp. 47-49, July 1992.

70. S. K. Langford and M. E. Hellman, "Linear-Differential Cryptanalysis," in *Advances in Cryptology: Proceedings of Crypto 94*, Yvo G. Desmedt, Editor, Springer-Verlag, Berlin, Lecture Notes in Computer Science #839, pp. 17-25, 1994.
71. M. E. Hellman "Resist Not Evil," *World Without Violence*, Arun Gandhi, Editor, 1994.
72. M. E. Hellman, "Sending Secret Messages," in *Scientific American: Triumph of Discovery*, Holt, New York, pp. 56-59, 1995.
73. M. E. Hellman, "An Overview of Public Key Cryptography," *IEEE Communications Magazine 50th Anniversary Issue: Landmark 10 Papers*, May 2002, pp. 42-49 (Invited Paper. This is a reprint of #31 above, with additional material added.)
74. M. E. Hellman, "Risk Analysis of Nuclear Deterrence," *The Bent of Tau Beta Pi* (the magazine of the Engineering Honor Society), Vol. 99, No. 2, pp. 14-22, Spring 2008.
75. M. E. Hellman, "How risky is nuclear optimism?" *Bulletin of the Atomic Scientists*, Vol. 67, No. 2, pp. 47-56, March 2011.
76. M. E. Hellman, "Fifty Years After the Cuban Missile Crisis: Time to Stop Bluffing at Nuclear Poker," A briefing paper of *The Federation of American Scientists* and *The Nuclear Age Peace Foundation*, October 2012.
77. M. E. Hellman, "Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic," *Communications of the ACM*, Vol. 60, No. 12, pp. 52-59, December 2017.
78. M. E. Hellman, "Rethinking National Security," a Special Report of The Federation of American Scientists, April 2019. Accessible online at tinyurl.com/hellmanRNS.
79. M. E. Hellman, "The Technological Imperative for Ethical Evolution," Lindau Nobel Laureates Meeting, Lindau, Germany, July 3, 2019. Accessible online both in [written form](#) and as a [video](#).
80. M. E. Hellman, "[Comments on NRC Study Mandated by Section 1674 of the FY2020 NDAA](#)," September 1, 2020. These comments were submitted to the National Research Council regarding the "Congressionally Mandated Study of Nuclear Risk" [described here](#).
81. Vinton G. Cerf and Martin E. Hellman, "[An existential discussion: What is the probability of nuclear war?](#)", *Bulletin of the Atomic Scientists*, March 18, 2021.
82. M. E. Hellman, "[Briefing for the National Research Council Study on Risk Analysis Methods for Nuclear War and Nuclear Terrorism](#)," April 21, 2021. This briefing was for the "Congressionally Mandated Study of Nuclear Risk" [described here](#).

83. M. E. Hellman, "[Probabilistic Risk Assessment](#)," Chapter 4 in *On Assessing the Risk of Nuclear War*, James Scouras, Editor, The Johns Hopkins University Applied Physics Laboratory, Laurel, MD, 2021. (The entire book is also available as [a free PDF](#).)
84. M. E. Hellman, "[Sixty Years After the Cuban Missile Crisis: Time to Stop Playing Russian Roulette](#)," October 14, 2022.
85. M. E. Hellman, "[Daniel Ellsberg's message to us, and to future generations](#)," *Bulletin of the Atomic Scientists*, June 16, 2023.
86. M. E. Hellman, "Federal Funding of Public Key Cryptography," *CACM*, Vol. 69, No. 8, pp. 48-52, 2026.

Books:

1. Anatoly A. Gromyko and Martin E. Hellman (Editors), *Breakthrough: Emerging New Thinking*, Walker and Co., New York, 1988. (Free PDF available at tinyurl.com/GromykoHellman.)
2. Anatoly A. Gromyko and Martin E. Hellman (Editors), *Proriv: Stanovleniye Novogo Mishleniya*, Progress, Moscow, 1987. (This is the Russian language version of #1 above.)
3. Dorothe Hellman and Martin Hellman, *A New Map for Relationships: Creating True Love at Home & Peace on the Planet*, New Map Publishing, Stanford, CA, 2016. (Free PDF available at tinyurl.com/HellmanBook.)

Newspaper Opinion Editorials:

1. M. E. Hellman, "A World Beyond War: The New Manner of Thinking," *The Stanford Daily*, February 13, 1984.
2. M. E. Hellman, "Nuclear War 100 Percent Certain, Unless ...," *San Mateo Times*, March 20, 1985.
3. M. E. Hellman, "Arms Race Can Only Lead to One End," *The Houston Post*, Page 3B, April 4, 1985.
4. M. E. Hellman, "The Nazi Within," *Boston Province Newsletter* (Sisters of Notre Dame), page 9, May 1985.
5. M. E. Hellman, "Psychology of War Can Lead to Atrocities," *San Mateo Times*, May 4, 1985.
6. M. E. Hellman, "Bitburg is Not as Important as Where We Go From Here," *The Houston Post*, Page 3B, May 5, 1985.

7. M. E. Hellman, "Avoiding Extinction," *Bridgeport Post*, May 26, 1985
8. M. E. Hellman, "Setting the Stage for Genocide?" *Palo Alto Weekly*, Vol. VI, No. 41, Page 27, July 17, 1985.
9. M. E. Hellman, "Military Secrecy Threatens the Peace in This Nuclear Age," *Newsday*, page 58, July 23, 1985.
10. M. E. Hellman, "Let's Share Star Wars With Soviets Right Now," *Newsday*, July 6, 1986.
11. M. E. Hellman, "Many Nations Caused World War II - so who should apologize to whom?," *San Jose Mercury News*, December 7, 1991.
12. Rep. Jerry McNerney, Rep. Bill Foster, Ronald Rivest and Martin Hellman, "Paris, San Bernardino, law enforcement and encryption," *The Hill*, December 14, 2015.
13. M. E. Hellman, "Rethinking National Security," [Scientific American online](#), June 6 2019.

Conference Presentations

1. M. E. Hellman and T. M. Cover, "Learning with Finite Memory," 1969 International Symposium on Information Theory, Ellenville, N.Y., January 28-31, 1969.
2. M. E. Hellman and J. Raviv, "Improved Bhattacharyya Bounds Including a Reject Criterion," IEEE International Conference on Communications, Boulder, Colorado, June 9-11, 1969.
3. M. E. Hellman and T. M. Cover, "Optimal Automata in Random Media; The Two-Armed Bandit Problem," First International Symposium on Information Theory (Soviet), Dubna, U.S.S.R., June 19-25, 1969.
4. M. E. Hellman and T. M. Cover, "The Two-Armed Bandit with Time-Invariant Finite Memory," Joint Statistical Meeting of A.S.A., B.S. and I. M.S., New York, N.Y., August 19-22, 1969.
5. M. E. Hellman, "The Nearest Neighbor Classification Rule with a Reject Option," 1970 International Symposium on Information Theory, Noordwijk, The Netherlands, June 15-19, 1970.
6. M. E. Hellman, "The Effects of Randomization on Finite Memory Decision Algorithms," 1970 IEEE Symposium on Adaptive Processes, Austin, TX, December 7-9, 1970 (Invited Paper).
7. M. E. Hellman and T. M. Cover, "On Memory Saved by Randomization," Hawaii International Conference on System Sciences, Honolulu, HI, January 12-15, 1971.
8. M. E. Hellman and T. M. Cover, "A Review of Recent Results on Learning with Finite Memory," Second International Symposium on Information Theory (Soviet), Tsahkadsor, Armenia, U.S.S.R., September 2-8, 1971.
9. M. A. Freedman and M. E. Hellman, "A Finite Memory, Finite Time, Gaussian Hypothesis Testing Problem," 1972 IEEE International Symposium on Information Theory, Asilomar, CA, January 31-February 3, 1972.
10. M. E. Hellman, "Finite Memory Algorithms for Estimating the Mean of a Gaussian Distribution," Third International Symposium on Information Theory (Soviet), Tallinn, Estonian U.S.S.R., June 18-23, 1973 (Invited Paper).
11. M. E. Hellman, "Finite Memory Decision Theory," 1973 IEEE International Symposium on Information Theory, Ashkelon, Israel, June 25-29, 1973 (Invited Paper).
12. F. L. Vermeulen and M. E. Hellman, "A Slightly Suboptimal Algorithm for Decoding PAM Signals with Intersymbol Interference in the Presence of Gaussian Noise," 1973 IEEE International Symposium on Information Theory, Ashkelon, Israel, June 25-29, 1973.
13. M. E. Hellman, "Anomalous Behavior in Finite Memory Learning Systems," 1973 IEEE International Symposium on Information Theory, Ashkelon, Israel, June 25-29, 1973.

14. M. E. Hellman, "Low Complexity Finite Memory Decision Rules," 1973 IEEE Conference on Decision and Control, San Diego, CA, December 5-7, 1973.
15. M. E. Hellman, "Joint Source and Channel Encoding," Seventh Hawaii International Conference on System Sciences, Honolulu, HI, January 8-10, 1974.
16. M. E. Hellman, "Complexity Issues in Coding," 1974 Communication Theory Workshop, Duck Key, FL, April 22-24, 1974.
17. M. E. Hellman and F. L. Vermeulen, "Reduced State Viterbi Decoders for Channels with Intersymbol Interference," 1974 IEEE International Conference on Communications, Minneapolis, MN, June 17-19, 1974 (invited paper).
18. M. E. Hellman, "Error Detection Made Simple," 1974 IEEE International Conference on Communications, Minneapolis, MN, June 17-19, 1974.
19. M. E. Hellman, "The Mathematical Theory of Secrecy Systems," 1974 IEEE International Conference on Communications, Minneapolis, MN, June 17-19, 1974.
20. M. E. Hellman, "The Information Theoretic Approach to Cryptography," 1974 IEEE International Symposium on Information Theory, Notre Dame, IN, October 27-31, 1974.
21. C. R. Davis and M. E. Hellman, "On Tree Coding with a Fidelity Criterion," Eighth Hawaii International Conference on Systems Science, Honolulu, HI, January 7-9, 1975.
22. M. E. Hellman, "Secure Protocols for Communication Networks," IEEE Information Theory Workshop, Lennox, MA, June 23-25, 1975.
23. M. E. Hellman and W. Diffie, "Cryptography for Data Base Security," Second Joint USA-Japan Computer Conference, Tokyo, Japan, August 26-28, 1975.
24. M. E. Hellman, "Cryptography and logs Modulo p ," IEEE Communication Theory Workshop, Captiva Island, FL, April 25-28, 1976.
25. W. Diffie and M. E. Hellman, "Multiuser Cryptographic Techniques," National Computer Conference, New York, NY, June 7-10, 1976.
26. M. E. Hellman and A. Carleial, "A Note on Wyner's Wiretap Channel," Fourth (Soviet) International Symposium on Information Theory, Leningrad, Russia, U.S.S.R., June 15-19, 1976.
27. W. Diffie and M. E. Hellman, "Public Key Cryptography," 1976 IEEE International Symposium on Information Theory, Ronneby, Sweden, June 21-24, 1976.

28. M. E. Hellman, "Low Cost Data Compression," 1976 International Telemetering Conference, Los Angeles, CA, September 28-30, 1976.
29. S. Pohlig and M. E. Hellman, "An Improved Algorithm for Computing Logarithms Over $GF(p)$ and its Cryptographic Significance," 1977 IEEE International Symposium on Information Theory, Ithaca, NY, October 10-14, 1977.
30. R. Merkle and M. E. Hellman, "Hiding Information and Receipts in Trap Door Knapsacks," 1977 IEEE International Symposium on Information Theory, Ithaca, NY, October 10-14, 1977.
31. S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian Wiretap Channel," 1977 IEEE International Symposium on Information Theory, Ithaca, NY, October 10-14, 1977.
32. M. E. Hellman, "Cryptographic Protection of Information in Communication Networks," Eleventh Annual Asilomar Conference on Circuits, Systems, and Computers, Pacific Grove, CA, November 7-9, 1977.
33. M. E. Hellman, "Cryptography: A Security Blanket for Computers," Council for the Advancement of Science Writing, NY, NY, November 14, 1977.
34. M. E. Hellman (member of panel) "Developing Countermeasures for Threats to Privacy," Western Psychological Association Convention, San Francisco, CA, April 17-22, 1978.
35. M. E. Hellman, "Security in Communication Networks," National Computer Conference, Anaheim, CA, June 5-8, 1978.
36. M. E. Hellman, "Resolving Some Myths Concerning the Data Encryption Standard," SHARE 52, San Francisco, CA, March 18-23, 1979.
37. M. E. Hellman, "New Directions in Cryptography," AFCEA Symposium, San Jose, CA, March 28, 1979.
38. M. E. Hellman, "A Cryptanalytic Time-Memory Tradeoff," 1979 IEEE International Symposium on Information Theory, Udine, Italy, June 25-29, 1979.
39. M. E. Hellman and R. Merkle, "Public Key Cryptography," Wescon/79, San Francisco, CA, September 18-20, 1979.
40. M. E. Hellman, "How Secure Should Commercial Encryption Be?" COMPCON Spring '80, San Francisco, CA, February 27, 1980.
41. M. E. Hellman, "On the Difficulty of Computing Logarithms Over $GF(qm)$," 1980 Symposium on Security and Privacy, Oakland, CA, April 14-16, 1980.
42. H. Amirazizi and M. E. Hellman, "Time-Memory-Processor Tradeoffs," CRYPTO 81, IEEE Conference in Cryptography, Santa Barbara, CA, August 24-26, 1981.

43. M. E. Hellman, E. Karnin and J. M. Reyneri, "On the Necessity of Cryptanalytic Exhaustive Search in Cryptanalysis," CRYPTO 81, IEEE Conference in Cryptography, Santa Barbara, CA, August 24-26, 1981.
44. M. E. Hellman, "Cryptographic Key Size Issues," COMPCON Spring '82, San Francisco, CA, February 22-25, 1982.
45. H. Amirazizi and M. E. Hellman, "Time-Memory-Processor Tradeoffs," 1982 International Symposium on Information Theory, Les Arcs, France, June 21-25, 1982.
46. E. Karnin and M. E. Hellman, "The Largest Super-Increasing Subset of a Random Set," 1982 International Symposium on Information Theory, Les Arcs, France, June 21-25, 1982.
47. J. M. Reyneri and M. E. Hellman, "Fast Computation of Discrete Logarithms in $GF(p^2)$," CRYPTO 82, IEEE Conference on Cryptography, Santa Barbara, CA, August 23-25, 1982.
48. J. M. Reyneri and M. E. Hellman, "The Distribution of Drainage and the DES," CRYPTO 82, IEEE Conference on Cryptography, Santa Barbara, CA, August 23-25, 1982.
49. M. E. Hellman, "Beyond War: Implications for Computer Security and Encryption," International Congress on Computer Security, Toronto, Canada, September 10-12, 1984. (Invited talk)
50. J. M. Reyneri and M. E. Hellman, "On the Distribution of Drainage and the Data Encryption Standard," Sixth International Symposium on Information Theory (Soviet), Tashkent, Uzbekistan, USSR, September 18-22, 1984.
51. M. E. Hellman, "Nuclear War: Inevitable or Preventable?," Conference on Accidental Nuclear War, University of British Columbia, Vancouver, BC, Canada, May 26-30, 1986.
52. M. E. Hellman, "DES and NSA's Commercial Comsec Endorsement Program," CRYPTO 86, IEEE Conference on Cryptography, Santa Barbara, CA, August 11-15, 1986.
53. M. E. Hellman, "Cryptanalyzing DES," Special Problems on Communication and Computation, Palo Alto, CA, September 3-5, 1986. (Invited talk)
54. M. E. Hellman, "NIST's Proposed Digital Signature Standard," 1992 RSA Data Security Conference, Redwood City, CA, November 4, 1991. (Invited talk)
55. M. E. Hellman, "An Introduction to Cryptography," Computer Professionals for Social Responsibility Conference on Cryptography, Washington, DC, June 1, 1992. (Invited talk)
56. M. E. Hellman "DES Revisited," 1993 RSA Data Security Conference, Redwood City, CA, January 14-15, 1993. (Invited talk)

57. M. E. Hellman, "Encryption," System & Network Security Audio Teleconference Series, April 7, 1993.
58. M. E. Hellman, "The Evolution of Public-Key Cryptography," CRYPTO 99, Santa Barbara, CA, August 15-19, 1999. (Invited talk)
59. M. E. Hellman, "Communications: Interconnecting the Glove," Marconi Society Symposium, SRI International, Menlo Park, CA, September 28, 2007. (Invited talk)
60. M. E. Hellman, "The Wisdom of Foolishness," Certicom ECC Conference, Toronto, Ontario, Canada, November 13-15, 2007. (Invited talk)
61. M. E. Hellman, "Inventing Public Key Cryptography: The Wisdom of Foolishness," DISI 2007, Information Security International Day, Madrid, Spain, December 3, 2007. [Video available online](#). (Invited talk)
62. M. E. Hellman, "Soaring, Cryptography, and Nuclear Weapons," RSA Conference, San Francisco, CA, April 8, 2007. (Invited talk)
63. M. E. Hellman, "Defusing the Nuclear Threat," United Nations Office for Disarmament Affairs, New York, NY, May 6, 2008.
64. M. E. Hellman, "Soaring, Cryptography, and Nuclear Weapons," Siddhartha Maitra Memorial Lecture, University of Santa Cruz, Santa Cruz, CA, October 18, 2008. (Invited talk)
65. M. E. Hellman, "The Wisdom of Foolishness," Marconi Society Symposium, SRI International, Menlo Park, CA, October 15, 2010. (Invited talk)
66. M. E. Hellman, "Academia's Role in DES: The Early Days," RSA Conference, San Francisco, CA, February 17, 2011. (Invited talk)
67. M. E. Hellman, "The Wisdom of Foolishness," Stanford Engineering Hero Induction, Stanford, CA, January 29, 2013. Video available online at tinyurl.com/SUhero. (Invited talk)
68. M. E. Hellman, "Assessing and Reducing Nuclear Risk," Federation of American Scientists Briefing, Cannon House Office Building, Washington, DC.
69. M. E. Hellman, "Improving Cyber Security by Paying Attention to History," Georgia Tech Cyber Security Summit, Atlanta, GA, November 6, 2013. (Invited keynote address)
70. M. E. Hellman, "Risk Analysis of Nuclear Deterrence," UCLA IPAM Workshop on Mathematics of Politics, Los Angeles, CA, April 22, 2014.
71. M. E. Hellman, "Improving Cyber Security by Paying Attention to History," Lonestar Security Conference, Austin, TX, October 23, 2014. (Invited keynote address)

72. M. E. Hellman, "Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic," ACM Conference on Computer and Communications Security, Vienna, Austria, October 25, 2016. Video accessible online at tinyurl.com/MHTuringLecture. (Invited talk)
73. M. E. Hellman, "Government Regulation of Cybersecurity: Pros and Cons," IEEE GLOBECOM, December 5, 2016. (Invited keynote address)
74. M. E. Hellman and D. L. Hellman, "Creating True Love at Home & Peace on the Planet," TEDx Tysons, Tysons Corner, VA, June 10, 2017. Video accessible online at tinyurl.com/HellmanTEDx. (Invited talk)
75. M. E. Hellman, "The Evolution of Public Key Cryptography," Heidelberg Laureate Forum, Heidelberg, Germany, September 25, 2017. (Invited talk)
76. M. E. Hellman, "The Evolution of Public Key Cryptography," ACM India Annual Meeting, Nagpur, India, February 17, 2018. (Invited talk)
77. M. E. Hellman, "Challenges in Making Ethical Decisions: A Personal Perspective," ACM Germany Annual Meeting, Heidelberg, Germany, September 20, 2018. (Invited keynote address)
78. M. E. Hellman, "Ingredients for Successful Research," Heidelberg Laureate Forum, Heidelberg, Germany, September 23, 2018. (Invited talk)
79. M. E. Hellman, "The Technological Imperative for Ethical Evolution," Lindau Nobel Laureates Meeting, Lindau, Germany, July 3, 2019. Accessible online both in [written form](#) and as a [video](#). (Invited talk)

Patents

1. U.S. Patent #4,200,770, CRYPTOGRAPHIC APPARATUS AND METHOD, M. Hellman, W. Diffie and R. Merkle. Issued April 29, 1980.

Canadian Patent #1121480, Issued April 6, 1978.

French Patent #2405532, Issued September 19, 1979.

Spanish Patent #474539, Issued October 6, 1978.

Swedish Patent #7810478-3, Issued September 12, 1985.

2. U.S. Patent #4,218,582, PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD, M. Hellman and R. Merkle. Issued August 19, 1980.

Australian Patent #40418/78 (519184), Issued October 4, 1978.

Belgian Patent #871.039, Issued October 5, 1978.

British Patent #GB 2006580B, Issued October 3, 1978.

Canadian Patent #1,128,159, Issued July 20, 1982.

German Patent #DE 28 43 583.c2, Issued October 5, 1978.

Italian Patent #1099780, Issued October 6, 1978 (granted September 28, 1985).

Japanese Patent #1,270,888, Issued October 6, 1978.

Spanish Patent #474.539, Issued April 16, 1980.

Swedish Patent #78 10478-3, Issued October 6, 1978.

Swiss Patent #634161, Issued October 5, 1978.

French Patent #86678 (application#839939, filed October 6, 1977).

3. U.S. Patent #4,424,414, EXPONENTIATION CRYPTOGRAPHIC APPARATUS AND METHOD, M. Hellman and S. Pohlig. Issued January 3, 1984.

Canadian Patent #1,152,592, Issued August 23, 1983.

4. U.S. Patent #4,633,036, METHOD AND APPARATUS FOR USE IN PUBLIC-KEY DATA ENCRYPTION SYSTEM, M. Hellman and C. E. Bach. Issued December 30, 1986.

5. U.S. Patent #4,658,093, SOFTWARE DISTRIBUTION SYSTEM, M. Hellman. Issued April 14, 1987.

6. U.S. Patent #5,872,917, AUTHENTICATION USING RANDOM CHALLENGES, M. Hellman. Issued February 16, 1999.

7. U.S. Patent #7,840,178, FM BROADCAST SYSTEM COMPETITIVE WITH SATELLITE RADIO, issued November 23, 2010.

8. U.S. Patent #7,865,917, SECURITY ENHANCED TIERED SUBSCRIPTION BROADCAST SYSTEM, issued January 4, 2011.

9. U.S. Patent #8,270,901, DROPOUT-RESISTANT MEDIA BROADCAST SYSTEM, issued September 18, 2012.

10. U.S. Patent #8,401,462, FM BROADCAST SYSTEM COMPETITIVE WITH SATELLITE RADIO, issued March 19, 2013.

11. U.S. Patent #8,627,354, TIERED SUBSCRIPTION BROADCAST SYSTEM, issued January 7, 2014.

12. U.S. Patent #9,124,375, TIERED SUBSCRIPTION BROADCAST SYSTEM, issued September 1, 2015.