Martin Hellman
Professor of Electrical Engineering, Emeritus

Bio

BIO
Martin E. Hellman is Professor Emeritus of Electrical Engineering at Stanford University and is affiliated with the university’s Center for International Security and Cooperation (CISAC). His recent technical work has focused on bringing a risk informed framework to a potential failure of nuclear deterrence and then using that approach to find surprising ways to reduce the risk. His earlier work included co-inventing public key cryptography, the technology that underlies the secure portion of the Internet. His many honors include election to the National Academy of Engineering and receiving (jointly with his colleague Whit Diffie) the million dollar ACM Turing Award, the top prize in computer science. His most recent project is a book, jointly written with his wife of fifty years, “A New Map for Relationships: Creating True Love at Home & Peace on the Planet,” that provides a “unified field theory” of peace by illuminating the connections between nuclear war, conventional war, interpersonal war, and war within our own psyches.

ACADEMIC APPOINTMENTS
- Emeritus Faculty, Acad Council, Electrical Engineering
- Affiliate, Stanford Woods Institute for the Environment

PROGRAM AFFILIATIONS
- Science, Technology and Society

Publications

PUBLICATIONS
- Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic. *Communications of the ACM*
  Hellman, M. E.
  2017; 60 (12): 52–59
- Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic
  Hellman, M. E., ACM
  ASSOC COMPUTING MACHINERY 2016: 1–2
- How risky is nuclear optimism? *Bulletin of the Atomic Scientists*
  Hellman, M. E.
  2011; 67 (2): 47–56
- RESPONSES TO NISTS PROPOSAL. *Communications of the ACM*
  1992; 35 (7): 41-54
- TIME MEMORY PROCESSOR TRADE-OFFS *IEEE Transactions on Information Theory*
AMIRAZIZI, H. R., HELLMAN, M. E.
1988; 34 (3): 505-512

• SCIENTISTS MUST HELP STOP THE ARMS-RACE (REPRINTED FROM BREAKTHROUGH EMERGING NEW THINKING, 1988) SCIENTIST
Kapitza, S. P., HELLMAN, M. E.
1988; 2 (2): 22-22

• ON SECRET SHARING SYSTEMS IEEE TRANSACTIONS ON INFORMATION THEORY
KARNIN, E. D., Greene, J. W., HELLMAN, M. E.
1983; 29 (1): 35-41

• THE LARGEST SUPER-INCREASING SUBSET OF A RANDOM SET IEEE TRANSACTIONS ON INFORMATION THEORY
KARNIN, E. D., HELLMAN, M. E.
1983; 29 (1): 146-148

• ANOTHER CRYPTANALYTIC ATTACK ON A CRYPTOSYSTEM FOR MULTIPLE COMMUNICATION INFORMATION PROCESSING LETTERS
HELLMAN, M. E.

• ON THE SECURITY OF MULTIPLE ENCRYPTION COMMUNICATIONS OF THE ACM
Merkle, R. C., HELLMAN, M. E.
1981; 24 (7): 465-467

• ON MULTIPLE ENCRYPTION SECURITY - REPLY COMMUNICATIONS OF THE ACM
Merkle, R. C., HELLMAN, M. E.
1981; 24 (11): 776-776

• REPORT OF THE PUBLIC CRYPTOGRAPHY STUDY-GROUP ACADEMIE-BULLETIN OF THE AAUP
Baum, W. A., Heyman, I. M., BRANDIN, D. H., Buck, R. C., DAVIDA, G. I., Handelman, G., HELLMAN, M. E., Kaplan, W., Schwartz, D. C.
1981; 67 (6): 372-379

• A CRYPTANALYTIC TIME-MEMORY TRADE-OFF IEEE TRANSACTIONS ON INFORMATION THEORY
HELLMAN, M. E.
1980; 26 (4): 401-406

• PRIVACY AND AUTHENTICATION - INTRODUCTION TO CRYPTOGRAPHY PROCEEDINGS OF THE IEEE
Diffie, W., HELLMAN, M. E.
1979; 67 (3): 397-427

• CONVOLUTIONAL ENCODING FOR WYNER WIRETAP CHANNEL IEEE TRANSACTIONS ON INFORMATION THEORY
Verriest, E., HELLMAN, M. E.
1979; 25 (2): 234-236

• FOILING COMPUTER CRIME .1. DES WILL BE TOTALLY INSECURE WITHIN 10 YEARS IEEE SPECTRUM
HELLMAN, M. E.
1979; 16 (7): 32-39

• MATHEMATICS OF PUBLIC-KEY CRYPTOGRAPHY SCIENTIFIC AMERICAN
HELLMAN, M. E.
1979; 241 (2): 146-?

• HIDING INFORMATION AND SIGNATURES IN TRAPDOOR KNAPSACKS IEEE TRANSACTIONS ON INFORMATION THEORY
Merkle, R. C., HELLMAN, M. E.
1978; 24 (5): 525-530

• IMPROVED ALGORITHM FOR COMPUTING LOGARITHMS OVER GF(P) AND ITS CRYPTOGRAPHIC SIGNIFICANCE IEEE TRANSACTIONS ON INFORMATION THEORY
POHLIG, S. C., HELLMAN, M. E.
1978; 24 (1): 106-110
• **GAUSSIAN WIRE-TAP CHANNEL** *IEEE TRANSACTIONS ON INFORMATION THEORY*
  LEUNG YAN CHEONG, S. K., HELLMAN, M. E.
  1978; 24 (4): 451-456

• **EXHAUSTIVE CRYPT-ANALYSIS OF NBS DATA ENCRYPTION STANDARD** *COMPUTER*
  Diffie, W., HELLMAN, M. E.
  1977; 10 (6): 74-84

• **COMPUTER ENCRYPTION - KEY SIZE** *SCIENCE*
  HELLMAN, M. E.
  1977; 198 (4312): 8-8

• **NOTE ON WYNER'S WIRETAP CHANNEL** *IEEE TRANSACTIONS ON INFORMATION THEORY*
  CARLEIAL, A. B., HELLMAN, M. E.
  1977; 23 (3): 387-390

• **EXTENSION OF SHANNON THEORY APPROACH TO CRYPTOGRAPHY** *IEEE TRANSACTIONS ON INFORMATION THEORY*
  HELLMAN, M. E.
  1977; 23 (3): 289-294

• **CONCERNING A BOUND ON UNDETECTED ERROR PROBABILITY** *IEEE TRANSACTIONS ON INFORMATION THEORY*
  LEUNG YAN CHEONG, S. K., HELLMAN, M. E.
  1976; 22 (2): 235-237

• **OPTIMAL FINITE MEMORY LEARNING ALGORITHMS FOR FINITE SAMPLE PROBLEM** *INFORMATION AND CONTROL*
  COVER, T. M., Freedman, M. A., HELLMAN, M. E.
  1976; 30 (1): 49-85

• **NEW DIRECTIONS IN CRYPTOGRAPHY** *IEEE TRANSACTIONS ON INFORMATION THEORY*
  Diffie, W., HELLMAN, M. E.
  1976; 22 (6): 644-654

• **TREE CODING WITH A FIDELITY CRITERION** *IEEE TRANSACTIONS ON INFORMATION THEORY*
  DAVIS, C. R., HELLMAN, M. E.
  1975; 21 (4): 373-378

• **ERROR DETECTION IN PRESENCE OF SYNCHRONIZATION LOSS** *IEEE TRANSACTIONS ON COMMUNICATIONS*
  HELLMAN, M. E.
  1975; CO23 (5): 538-539

• **BISTABLE BEHAVIOR OF ALOHA-TYPE SYSTEMS** *IEEE TRANSACTIONS ON COMMUNICATIONS*
  CARLEIAL, A. B., HELLMAN, M. E.
  1975; CO23 (4): 401-410

• **CONVOLUTIONAL SOURCE ENCODING** *IEEE TRANSACTIONS ON INFORMATION THEORY*
  HELLMAN, M. E.
  1975; 21 (6): 651-656

• **FINITE-MEMORY ALGORITHMS FOR ESTIMATING MEAN OF A GAUSSIAN DISTRIBUTION** *IEEE TRANSACTIONS ON INFORMATION THEORY*
  HELLMAN, M. E.
  1974; 20 (3): 382-384

• **USING NATURAL REDUNDANCY FOR ERROR DETECTION** *IEEE TRANSACTIONS ON COMMUNICATIONS*
  HELLMAN, M. E.
  1974; CO22 (10): 1690-1693