WIKIPEDIA

Martin Hellman

Martin Edward Hellman (born October 2, 1945) is an American cryptologist, best known for his invention of public key cryptography in cooperation with Whitfield Diffie and Ralph Merkle.[2][3] Hellman is a longtime contributor to the computer privacy debate, has applied risk analysis to a potential failure of nuclear deterrence, and in 2016 wrote a book with his wife, Dorothie Hellman, that links creating love at home to bringing peace to the planet (*A New Map for Relationships: Creating True Love at Home and Peace on the Planet*).

Contents

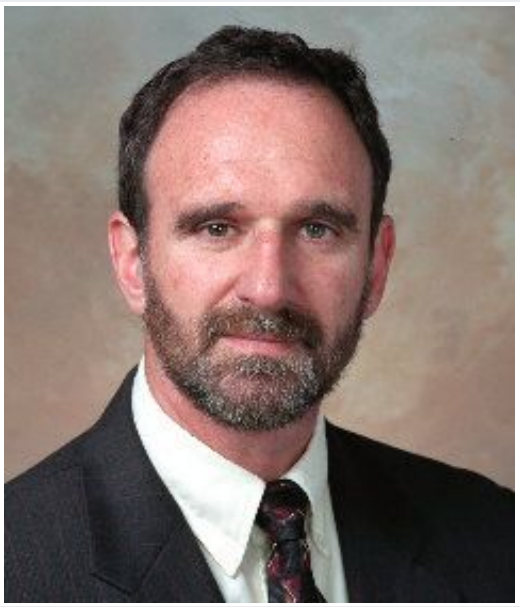
Early life

Born to a Jewish family,[4] Hellman graduated from the Bronx High School of Science. He went on to take his bachelor's degree in electrical engineering from New York University in 1966, and at Stanford University he received a master's degree and a Ph.D. in the discipline in 1967 and 1969.[5]

Career

From 1968 to 1969 he worked at IBM's Thomas J. Watson Research Center in Yorktown Heights, New York, where he encountered Horst Feistel. From 1969 to 1971, he was an assistant professor of electrical engineering at the Massachusetts Institute of Technology. He joined Stanford University electrical engineering department in 1971 as an assistant professor and served on the full-time faculty for twenty-five years before taking emeritus status as a full professor in 1996.[6]

Martin Hellman



Born	Martin Edward Hellman October 2, 1945 New York City, United States
Nationality	American
Alma mater	New York University (BE, 1966) Stanford University (MS, 1967; PhD, 1969)
Known for	Diffie–Hellman key exchange
Awards	IEEE Centennial Medal (1984) EFF Pioneer Award (1994) Louis E. Levy Medal(1997) Golden Jubilee Awards for Technological Innovation (http://www.itsoc.org/honors/golden-jubilee-awards-for-technological-innovation) (1998) Marconi Prize (2000) National Academy of Engineering Member

Public key cryptography

Hellman and Whitfield Diffie's paper *New Directions in Cryptography* was published in 1976. It introduced a radically new method of distributing cryptographic keys, which went far toward solving one of the fundamental problems of cryptography, key distribution.[7][8] It has become known as Diffie–Hellman key exchange, although Hellman has argued that it ought to be called Diffie-Hellman-Merkle key exchange because of Merkle's separate contribution. The article stimulated the development of a new class of encryption algorithms, known variously as public key encryption and asymmetric encryption. Hellman and Diffie were awarded the Marconi Fellowship and accompanying prize in 2000 for work on public-key cryptography and for helping make cryptography a legitimate area of academic research,[9] and they were awarded the 2015 Turing Award for the same work.[7]

	(2002) Hamming Medal (2010) Computer History Museum Fellow (2011) [1] ACM Turing Award (2015)
Scientific career	
Fields	Cryptography Computer science Electrical engineering
Institutions	Stanford University MIT IBM Research
Thesis	*Learning with Finite Memory* (http://www-ee.stanford.edu/%7Ehellman/publications/01.pdf) (1969)
Doctoral advisor	Thomas Cover
Doctoral students	Ralph Merkle Taher Elgamal
Website	ee.stanford.edu/~hellman (http://ee.stanford.edu/~hellman)

Computer privacy debate

Hellman has been a longtime contributor to the computer privacy debate. He and Diffie were the most prominent critics of the short key size of the Data Encryption Standard (DES) in 1975. An audio recording survives of their review of DES at Stanford in 1976 with Dennis Branstad of NBS and representatives of the National Security Agency.[10] Their concern was well-founded: subsequent history has shown not only that NSA actively intervened with IBM and NBS to shorten the key size, but also that the short key size enabled exactly the kind of massively parallel key crackers that Hellman and Diffie sketched out. In response to RSA Security's DES Challenges starting in 1997, brute force crackers were built that could break DES, making it clear that DES was insecure and obsolete. As of 2012, a $10,000 commercially available machine could recover a DES key in days.

Hellman also served (1994–96) on the National Research Council's Committee to Study National Cryptographic Policy, whose main recommendations have since been implemented.

International security

Hellman has been active in researching international security since 1985.

Beyond War

Hellman was involved in the original Beyond War movement, serving as the principal editor for the "BEYOND WAR: A New Way of Thinking" booklet.[11]

Breakthrough

In 1987 more than 30 scholars came together to produce Russian and English editions of the book *Breakthrough: Emerging New Thinking, Soviet and Western Scholars Issue a Challenge to Build a World Beyond War*. Anatoly Gromyko and Martin Hellman served as the chief editors. The authors of the book examine questions such as: How can we

overcome the inexorable forces leading toward a clash between the United States and the Soviet Union? How do we build a common vision for the future? How can we restructure our thinking to synchronize with the imperative of our modern world?[12][13]

Defusing the nuclear threat

Hellman's current project in international security is to defuse the nuclear threat. In particular, he is studying the probabilities and risks associated with nuclear weapons and encouraging further international research in this area. His website NuclearRisk.org (http://NuclearRisk.org) has been endorsed by a number of prominent individuals, including a former Director of the National Security Agency, Stanford's President Emeritus, and two Nobel Laureates.

Hellman is a member of the Board of Directors for Daisy Alliance, a non-governmental organization based in Atlanta, Georgia, seeking global security through nuclear nonproliferation and disarmament.

Awards and honors

In 1997 he was awarded The Franklin Institute's Louis E. Levy Medal,[14] in 1981 the IEEE Donald G. Fink Prize Paper Award (together with Whitfield Diffie),[15] in 2000, he won the Marconi Prize for his invention of public-key cryptography to protect privacy on the Internet, also together with Whit Diffie.[16] In 1998, Hellman was a Golden Jubilee Award for Technological Innovation from the IEEE Information Theory Society,[17] and in 2010 the IEEE Richard W. Hamming Medal.[18]

In 2011, he was inducted into the National Inventors Hall of Fame.[19]

Also in 2011, Hellman was made a Fellow of the Computer History Museum for his work, with Whitfield Diffie and Ralph Merkle, on public key cryptography.[20]

Hellman won the Turing Award for 2015 together with Whitfield Diffie. The Turing award is widely considered the most prestigious award in the field of computer science. The citation for the award was: "*For fundamental contributions to modern cryptography. Diffie and Hellman's groundbreaking 1976 paper, "New Directions in Cryptography," introduced the ideas of public-key cryptography and digital signatures, which are the foundation for most regularly-used security protocols on the internet today*."[7]

References

1. Martin Hellman 2011 Fellow (http://www.computerhistory.org/fellowawards/hall/bios/Martin,Hellman/) Archived (https://web.archive.org/web/20130509235730/http://www.computerhistory.org/fellowawards/hall/bios/Martin,Hellman/) 2013-05-09 at the Wayback Machine
2. "Martin E. Hellman, Professor Emeritus of Electrical Engineering" (https://ee.stanford.edu/~hellman/). *Stanford*. Retrieved 2016-03-05.
3. "Martin E. Hellman" (http://dblp.org/pid/h/MartinEHellman). *DBLP*. Retrieved 2016-11-04.
4. *Universities should restore spiritual side, says Professor Martin Hellman*, NEWS RELEASE, 11/28/95
5. Hellman, Martin (1969). *Learning with Finite Memory* (http://search.proquest.com/docview/302464730) (PhD thesis). Stanford University.
6. Martin Hellman's webpage at Stanford University http://www-ee.stanford.edu/~hellman
7. "Cryptography Pioneers Receive 2015 ACM A.M. Turing Award" (http://amturing.acm.org/award_winners/diffie_8371646.cfm). ACM.

8. Diffie, Whitfield; Hellman, Martin (1976-11-01). "New directions in cryptography" (https://www-ee.stanford.edu/~hellman/publications/24.pdf) (PDF). *IEEE Transactions on Information Theory*. **22** (6): 644–654. CiteSeerX 10.1.1.37.9720 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.37.9720). doi:10.1109/TIT.1976.1055638 (https://doi.org/10.1109%2FTIT.1976.1055638). ISSN 0018-9448 (https://www.worldcat.org/issn/0018-9448).
9. Columbia University press release regarding Marconi Fellowship (http://www.columbia.edu/cu/record/archives/vol26/vol26_iss4/2604_Marconi_Honors_Investors.html)
10. "DES (Data Encryption Standard) Review at Stanford University" (http://www.toad.com/des-stanford-meeting.html). 1976. Retrieved 2012-03-20.
11. Richard Rathbun, Rick Roney, Louise Smith, Donna Richeson, Don Fitton, Craig Ritchey, "BEYOND WAR: A New Way of Thinking", (Editors: Martin Hellman, Craig Barnes, Al Braun, Pat Chandler, Jack Li, Mac Lawrence, Tom Lindsay, Tom Osborne, Chris Rich, Nancy Ritchey, Karen Stevens and Judie Swope.) PDF available free online (http://traubman.igc.org/bwthinking.pdf)
12. Breakthrough website page (http://www-ee.stanford.edu/~hellman/Breakthrough/)
13. Anatoly Gromyko, Martin Hellman, Craig Barnes, Alexander Nikitin, Donald Fitton, Sergei Kapitza, Elena Loshchenkova, William McGlashan, Andrei Melville, Harold Sandler, Olivia Simantob, "Breakthrough: Emerging New Thinking", Walker and Company, ISBN 0-8027-1026-3, ISBN 0-8027-1015-8 and published simultaneously in the Soviet Union by Progress Publishing Company, Moscow. Martin Hellman's Stanford website page (http://www-ee.stanford.edu/~hellman/), PDF online free (http://www-ee.stanford.edu/~hellman/Breakthrough/book/pdfs/breakthrough.pdf)
14. "Franklin Laureate Database – Louis E. Levy Medal Laureates" (https://web.archive.org/web/20110629195033/http://www.fi.edu/winners/show_results.faw?gs=&ln=&fn=&keyword=&subject=&award=LEVY+&sy=1923&ey=1999&name=Submit). Franklin Institute. Archived from the original (http://www.fi.edu/winners/show_results.faw?gs=&ln=&fn=&keyword=&subject=&award=LEVY+&sy=1923&ey=1999&name=Submit) on June 29, 2011. Retrieved January 22, 2011.
15. "IEEE Donald G. Fink Prize Paper Award Recipients" (https://www.ieee.org/documents/fink_rl.pdf) (PDF). IEEE. Retrieved January 2, 2011.
16. "Martin E. Hellman – Awarded the Marconi Prize in 2000" (http://marconisociety.org/fellows/martin-e-hellman/). *Marconi Society*.
17. "Golden Jubilee Awards for Technological Innovation" (http://www.itsoc.org/honors/golden-jubilee-awards-for-technological-innovation). IEEE Information Theory Society. Retrieved July 14, 2011.
18. "IEEE Richard W. Hamming Medal Recipients" (https://www.ieee.org/documents/hamming_rl.pdf) (PDF). IEEE. Retrieved January 22, 2011.
19. "Meet the 2011 National Inventors Hall of Fame Inductees – Martin Hellman" (https://archive.is/20120904082305/http://www.invent.org/2011induction/1_3_11_induction_hellman.asp). National Inventors Hall of Fame. Archived from the original (http://www.invent.org/2011induction/1_3_11_induction_hellman.asp) on September 4, 2012. Retrieved May 5, 2011.
20. "Martin Hellman" (https://web.archive.org/web/20130509235730/http://www.computerhistory.org/fellowawards/hall/bios/Martin,Hellman/). Computer History Museum. Archived from the original (http://www.computerhistory.org/fellowawards/hall/bios/Martin,Hellman/) on 2013-05-09. Retrieved 2013-05-23.

External links

- Oral history interview with Martin Hellman (http://purl.umn.edu/107353) Oral history interview 2004, Palo Alto, California. Charles Babbage Institute, University of Minnesota, Minneapolis. Hellman describes his invention of public key cryptography with collaborators Whitfield Diffie and Ralph Merkle at Stanford University in the mid-1970s. He also relates his subsequent work in cryptography with Steve Pohlig (the Pohlig–Hellman algorithm) and others. Hellman addresses the National Security Agency's (NSA) early efforts to contain and discourage academic work in the field, the Department of Commerce's encryption export restrictions (under the International Traffic of Arms Regulation, or ITAR), and key escrow (the so-called Clipper chip). He also touches on the commercialization of cryptography with RSA Data Security and VeriSign.
- Martin Hellman's website on the risk of nuclear threat from nuclear war or nuclear terrorism (http://nuclearrisk.org/)
- "Defusing the nuclear threat and making the world safer" (http://www.soe.ucsc.edu/news/event?ID=1512) Announcement of Hellman presentation at U.C. Santa Cruz; Oct. 2008

- Hellman at the 2009 RSA conference (https://web.archive.org/web/20090428195928/http://media.omediaweb.com/rsa2009/preview/webcast.htm?id=1_5), video with Hellman participating on the Cryptographer's Panel, April 21, 2009, Moscone Center, San Francisco
- Soaring, Cryptography and Nuclear Weapons (https://www.youtube.com/watch?v=D1xnM3bbkCg) on YouTube

---