Ralph Merkle

From Wikipedia, the free encyclopedia

Ralph C. Merkle (born February 2, 1952) is a computer scientist. He is one of the inventors of public key cryptography, the inventor of cryptographic hashing, and more recently a researcher and speaker of cryonics.

Contents

Contributions

Merkle devised a scheme for communication over an insecure channel: Merkle's puzzles as part of a class project while an undergraduate.[3] The scheme is now recognized to be an early example of public key cryptography. He co-invented the Merkle–Hellman knapsack cryptosystem, invented cryptographic hashing (now called the Merkle–Damgård construction based on a pair of articles published 10 years later that established the security of the scheme), and invented Merkle trees. While at Xerox PARC, Merkle designed the Khufu and Khafre block ciphers, and the Snefru hash function.

Career

Ralph Merkle

Merkle at the Singularity Summit 2007

Born	February 2, 1952 Berkeley, California
Nationality	American
Citizenship	American
Alma mater	UC Berkeley (B.A., 1974; M.S., 1977) Stanford University (Ph.D., 1979)
Known for	Co-inventor of public key cryptography Merkle tree[1] Merkle's puzzles Merkle–Hellman knapsack cryptosystem Merkle–Damgård construction
Spouse(s)	Carol Shaw
Awards	IEEE Richard W. Hamming Medal (2010) Computer History Museum Fellow (2011)[2]

Merkle was the manager of compiler development at Elxsi from 1980. In 1988, he became a research scientist at Xerox PARC. In 1999 he became a nanotechnology theorist for Zyvex. In 2003 he became a Distinguished Professor at Georgia Tech, where he led the Georgia Tech Information Security Center.[4] In 2006 he returned to the San Francisco Bay Area, where he has been a senior research fellow at IMM, a faculty member at Singularity University, and a board member of the Alcor Life Extension Foundation. He was awarded the IEEE Richard W. Hamming Medal in 2010.[5]

Website	www.merkle.com (http://www.merkle.com)
Scientific career	
Fields	Public key cryptography, cryonics
Institutions	Singularity University Alcor Life Extension Foundation Institute for Molecular Manufacturing Elxsi Georgia Institute of Technology
Thesis	*Secrecy, authentication and public key systems* (http://www.merkle.com/papers/Thesis1979.pdf)
Doctoral advisor	Martin Hellman

Personal life

Ralph Merkle is the grandnephew of baseball star Fred Merkle, the son of Theodore Charles Merkle, director of Project Pluto and the brother of Judith Merkle Riley, a historical writer.[6] Merkle is married to Carol Shaw,[6] the video game designer best known for her game, *River Raid*.

Merkle is on the Board of Directors of the cryonics organization Alcor Life Extension Foundation.[7]

Merkle appears in the science fiction novel *The Diamond Age*, involving nanotechnology.

Awards

- 1996 Paris Kanellakis Award
- 1996 ACM Award for the Invention of Public Key Cryptography.[8]
- 1998 Feynman Prize in Nanotechnology for computational modeling of molecular tools for atomically-precise chemical reactions[9]
- 1999 IEEE Koji Kobayashi Computers and Communications Award[10]
- 2000 RSA award for the invention of public key cryptography.[11]
- 2008 International Association for Cryptographic Research (IACR) fellow for the invention of public key cryptography.[12]
- 2010 IEEE Hamming Medal for the invention of public key cryptography[13]
- 2011 Computer History Museum Fellow "for his work, with Whitfield Diffie and Martin Hellman, on public key cryptography."[14]
- 2011 National Inventors Hall of Fame, for the invention of public key cryptography[15]
- 2012 National Cyber Security Hall of Fame inductee

See also

- blockchain (the most popular use of Merkle tree)

References

1. Merkle, R. C. (1988). "A Digital Signature Based on a Conventional Encryption Function". *Advances in Cryptology — CRYPTO '87*. Lecture Notes in Computer Science. **293**. p. 369. doi:10.1007/3-540-48184-2_32 (https://doi.org/10.1007%2F3-540-48184-2_32). ISBN 978-3-540-18796-7.
2. Ralph Merkle 2011 Fellow (http://www.computerhistory.org/fellowawards/hall/bios/Ralph,Merkle/)
3. Garfinkel, Simson (1994). *Pretty Good Privacy*. O'Reilly and Associates.
4. "Cybersecurity Pioneer Selected to Lead Information Security Center at Georgia Tech" (http://www.gatech.edu/news-room/release.php?id=164) (Press release). Georgia Institute of Technology. 2003-07-15. Retrieved 2007-03-17.
5. "IEEE Richard W. Hamming Medal Recipients" (http://www.ieee.org/documents/hamming_rl.pdf) (PDF). IEEE. Retrieved 2011-05-29.
6. "Ralph C. Merkle" (http://www.merkle.com/). merkle.com. Retrieved 2013-11-25. "My wife is Carol Shaw. My sister, Judith Merkle Riley, wrote historical novels. My father, Theodore Charles Merkle, ran Project Pluto. My great uncle was Fred Merkle, of baseball fame."
7. "Alcor Board of Directors" (http://www.alcor.org/AboutAlcor/meetdirectors.html#merkle). Alcor Life Extension Foundation. 2012-09-01. Retrieved 2013-10-24.
8. "Ralph Merkle - Award Winner" (http://awards.acm.org/citation.cfm?id=4605383&srt=all&aw=147&ao=KANELLAK&yr=1996). ACM. Retrieved 2013-11-25.
9. "1998 Feynman Prize in Nanotechnology" (http://www.foresight.org/FI/1998Feynman.html). Foresight.org. 1998-09-04. Retrieved 2013-11-25.
10. "Koji Kobayashi Computers and Communications Award" (http://www.ieee.org/about/awards/tfas/kobayashi.html). IEEE. Retrieved 2013-11-25.
11. "Information Security, Governance, Risk, and Compliance - EMC" (http://www.rsa.com/press_release.aspx?id=343). RSA. Retrieved 2013-11-25.
12. "Ralph Merkle, IACR Fellow" (https://www.iacr.org/fellows/2008/Merkle.html). Iacr.org. 2008. Retrieved 2013-11-25.
13. "CISAC's scholars awarded for invention of public key cryptography" (http://cisac.stanford.edu/news/cisacs_scholars_awarded_for_invention_of_public_key_cryptography_20091209/). Stanford University. 2009-12-09. Retrieved 2013-11-25.
14. "Computer History Museum | Fellow Awards - Ralph Merkle" (http://www.computerhistory.org/fellowawards/hall/bios/Ralph,Merkle/). Computerhistory.org. Retrieved 2013-11-25.
15. "Invent Now | Hall of Fame | Induction | 2011 Inductees" (http://www.invent.org/2011induction/1_3_11_induction_merkle.asp). Invent.org. 1952-02-02. Retrieved 2013-11-25.

Other references:

- Ralph C. Merkle, *Secrecy, authentication, and public key systems* (Computer science), UMI Research Press, 1982, ISBN 0-8357-1384-9.
- Robert A. Freitas Jr., Ralph C. Merkle, *Kinematic Self-Replicating Machines*, Landes Bioscience, 2004, ISBN 1-57059-690-5.
- Paul Kantor (Ed), Gheorghe Mureşan (Ed), Fred Roberts (Ed), Daniel Zeng (Ed), Frei-Yue Wang (Ed), Hsinchun Chen (Ed), Ralph Merkle (Ed), "Intelligence and Security Informatics" : *IEEE International Conference on Intelligence and Security Informatics*, ISI 2005, Atlanta, GA, US, May 19–20, ... (Lecture

Notes in Computer Science), Springer, 2005, ISBN 3-540-25999-6.
- Interview (https://web.archive.org/web/20111228061915/http://video.google.com/videoplay?docid=1598612092045110436) at Google Videos in the Death in the Deep Freeze documentary (August 2, 2006)
- Nova Southeastern University, Nanotechnology Expert Ralph Merkle to Speak on "Life and Death" (http://www.fcas.nova.edu/arts/distinguished_speakers_series/ralph_merkle/index.cfm) (August 2008)

External links

- Ralph Merkle's personal website (http://www.merkle.com/)
- Oral history interview with Martin Hellman (http://purl.umn.edu/107353) – from 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 system) and others.