WIKIPEDIA

Ron Rivest

Ronald Linn Rivest (/rɪˈvɛst/;[5][6] born May 6, 1947) is a cryptographer and an Institute Professor at MIT.[2] He is a member of MIT's Department of Electrical Engineering and Computer Science (EECS) and a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL). He was a member of the Election Assistance Commission's Technical Guidelines Development Committee, tasked with assisting the EAC in drafting the Voluntary Voting System Guidelines.[7]

Rivest is one of the inventors of the RSA algorithm (along with Adi Shamir and Len Adleman).[1] He is the inventor of the symmetric key encryption algorithms RC2, RC4, RC5, and co-inventor of RC6. The "RC" stands for "Rivest Cipher", or alternatively, "Ron's Code". (RC3 was broken at RSA Security during development; similarly, RC1 was never published.) He also authored the MD2, MD4, MD5 and MD6 cryptographic hash functions. In 2006, he published his invention of the ThreeBallot voting system, a voting system that incorporates the ability for the voter to discern that their vote was counted while still protecting their voter privacy. Most importantly, this system does not rely on cryptography at all. Stating "Our democracy is too important", he simultaneously placed ThreeBallot in the public domain.

Rivest frequently collaborates with other researchers in combinatorics, for example working with David A. Klarner to find an upper bound on the number of polyominoes of a given order[8] and working with Jean Vuillemin to prove the deterministic form of the Aanderaa–Rosenberg conjecture.[9]

Contents

Education

Rivest earned a Bachelor's degree in Mathematics from Yale University in 1969, and a Ph.D. degree in Computer Science from Stanford University in 1974 for research supervised by Robert W. Floyd.[3]

Ron Rivest	
Ronald Rivest in 2012	
Born	Ronald Linn Rivest May 6, 1947 Schenectady, New York
Residence	United States
Nationality	American
Alma mater	Stanford University (PhD) Yale University
Known for	Public-key[1] RSA, RC2, RC4, RC5, RC6 MD2, MD4, MD5, MD6, Ring signature
Awards	Paris Kanellakis Award (1996) Turing Award (2002) Marconi Prize (2007)
Scientific career	
Fields	Algorithms[2] Cryptography[2] Voting[2]
Institutions	Massachusetts Institute of Technology
Thesis	*Analysis of associative*

	retrieval algorithms (http://worldcat.org/oclc/897011820) (1974)
Doctoral advisor	Robert W. Floyd
Doctoral students	Avrim Blum[3] Burt Kaliski[3] Anna Lysyanskaya[3] Ron Pinter[3] Robert Schapire[3] Alan Sherman[3] Mona Singh[4]

Career and research

Rivest is a co-author of *Introduction to Algorithms* (also known as *CLRS*), a standard textbook on algorithms, with Thomas H. Cormen, Charles E. Leiserson and Clifford Stein. He is a member of the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) in the Theory of Computation Group, and a founder of its Cryptography and Information Security Group. He was also a founder of RSA Data Security (now merged with Security Dynamics to form RSA Security), Verisign, and of Peppercoin. Rivest has research interests in algorithms, cryptography and voting.[2] His former doctoral students include Avrim Blum,[3] Burt Kaliski,[3] Ron Pinter,[3] Robert Schapire,[3] Alan Sherman,[3] and Mona Singh.[4]

Publications

His publications[2] include:

- Cormen, Thomas H.; Leiserson, Charles; Rivest, Ronald (1990). *Introduction to Algorithms* (first ed.). MIT Press and McGraw-Hill. ISBN 978-0-262-03141-7.
- Cormen, Thomas H.; Leiserson, Charles; Rivest, Ronald; Stein, Clifford (2001). *Introduction to Algorithms* (second ed.). MIT Press and McGraw-Hill. ISBN 978-0-262-53196-2.
- Cormen, Thomas H.; Leiserson, Charles; Rivest, Ronald; Stein, Clifford (2009). *Introduction to Algorithms* (third ed.). MIT Press. ISBN 978-0-262-03384-8.

Rivest (right) in March 1999.

Honors and awards

Rivest is a member of the National Academy of Engineering, the National Academy of Sciences, and is a Fellow of the Association for Computing Machinery, the International Association for Cryptologic Research, and the American Academy of Arts and Sciences. Together with Adi Shamir and Len Adleman, he has been awarded the 2000 IEEE Koji Kobayashi Computers and Communications Award and the Secure Computing Lifetime Achievement Award. He also shared with them the Turing Award. Rivest has received an honorary degree (the "laurea honoris causa") from the Sapienza University of Rome.[10] In 2005, he received the MITX Lifetime Achievement Award. Rivest was named the 2007 the Marconi Fellow, and on May 29, 2008 he also gave the Chesley lecture at Carleton College. He was named an Institute Professor at MIT in June 2015.[11]

References

1. Rivest, R. L.; Shamir, A.; Adleman, L. (1978). "A method for obtaining digital signatures and public-key cryptosystems". *Communications of the ACM*. **21** (2): 120–126. CiteSeerX 10.1.1.607.2677 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.607.2677). doi:10.1145/359340.359342 (https://doi.org/10.1145%2F359340.359342). ISSN 0001-0782 (https://www.worldcat.org/issn/0001-0782).
2. Ron Rivest (https://scholar.google.com/citations?user=6qE0tdAAAAAJ) publications indexed by Google Scholar
3. Ron Rivest (https://www.genealogy.math.ndsu.nodak.edu/id.php?id=50081) at the Mathematics Genealogy Project

4. Singh, Mona (1996). *Learning algorithms with applications to robot navigation and protein folding* (https://dspace.mit.edu/handle/1721.1/40579). *dspace.mit.edu* (PhD thesis). Massachusetts Institute of Technology. hdl:1721.1/40579 (https://hdl.handle.net/1721.1%2F40579). OCLC 680493381 (https://www.worldcat.org/oclc/680493381).
5. RSA Conference (25 February 2014). "The Cryptographers' Panel" (https://www.youtube.com/watch?v=gMc9fHvc78Y&t=1m7s) – via YouTube.
6. https://www.youtube.com/watch?v=WDGh3-1itPw&t=1m The second syllable is stressed
7. "TGDC members" (https://web.archive.org/web/20070608071658/http://vote.nist.gov/tgdcmem.htm). National Institute of Standards and Technology. 2009-05-06. Archived from the original (http://vote.nist.gov/tgdcmem.htm) on 2007-06-08.
8. A procedure for improving the upper bound for the number of n-ominoes (https://people.csail.mit.edu/rivest/pubs/KR73.pdf), by D. A. Klarner and R. L. Rivest, Canadian Journal of Mathematics, Vol. XXV, No. 3, 1973, pp. 5
9. A Generalization and Proof of the Aanderaa-Rosenberg Conjecture (http://dblp.uni-trier.de/db/conf/stoc/stoc75.html) by Ronald L. Rivest and Jean Vuillemin
10. Biography (https://www.webcitation.org/63jGW7VaO?url=http://people.csail.mit.edu/rivest/bio.html). Archived from the original (http://people.csail.mit.edu/rivest/bio.html) on 2011-12-06.
11. "Chisholm, Rivest, and Thompson appointed as new Institute Professors" (http://newsoffice.mit.edu/2015/chisholm-rivest-thompson-institute-professors-0629).

External links

- List of Ron Rivest's patents on IPEXL (http://www.ipexl.com/share/fecba62ecb1bfc4a861cfb31ea1373d1)
- Home page of Ronald L. Rivest (http://people.csail.mit.edu/rivest/)
- Official site of RSA Security Inc. (http://www.rsasecurity.com/)
- Ron Rivest election research papers (https://web.archive.org/web/20071213115534/http://www.electiontechnology.com/who.php?id=17)
- The ThreeBallot Voting System (PDF) (http://theory.csail.mit.edu/%7Erivest/Rivest-TheThreeBallotVotingSystem.pdf)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Ron_Rivest&oldid=887571731"

This page was last edited on 2019-03-13, at 21:46:42.