

ATTACHMENT 2: Profile of Group B Recipients

Professor Ronald L. Rivest

Current Position:

Andrew and Erna Viterbi Professor of Electrical Engineering and
Computer Science
Massachusetts Institute of Technology

Career History:

1947 Born in Schenectady, New York, USA
1965 B.A. Mathematics, Yale University, New Haven, Connecticut, USA
1973 Ph.D. Computer Science, Stanford University, Stanford, California, USA
1973 Post-doc, INRIA, Rocquencourt, France
1974 Assistant Professor, EECS, Massachusetts Institute of Technology
1977 Associate Professor, EECS, Massachusetts Institute of Technology
1979 Associate Professor with tenure, EECS, Massachusetts Institute of
Technology
1983 Professor, EECS, Massachusetts Institute of Technology
1983 Founder, RSA Data Security
1995 Founder, Verisign
2001 Founder, Peppercoin

Professor Rivest's research career has been devoted primarily to the theoretical aspects of computer science, with an emphasis on computer algorithms, cryptography, computer and network security, machine learning, and the security of voting systems.

In 1977, inspired by the work of Diffie, Hellman, and Merkle, Professor Rivest, together with Professors Adi Shamir and Leonard Adleman, invented the first practical proposal for a public-key cryptosystem, known now as the “RSA” public-key cryptosystem, after the initials of its inventors.

Professor Rivest has developed other cryptographic algorithms that have found widespread use in practice, such as the stream cipher RC4 and the hash algorithm MD5. He has also worked on the theoretical foundations of cryptography; his paper (with Goldwasser and Micali) on the notion of security for digital signatures is widely cited, and his work on the SPKI/SDSI public-key infrastructure has had significant theoretical (and practical) impact. More recently, he has worked on various aspects of the security of cryptographic hash functions, and has led a team that submitted the “MD6” hash function algorithm to the U.S. NIST SHA-3 hash function competition.

He has worked extensively on applying cryptographic methods to problems of practical importance, such as electronic payments (and in particular, micropayments), and voting systems. He is a co-developer of the PayWord, MicroMint, and Peppercoin micro-payment methods; the latter method (with Silvio Micali) was the basis for the formation of the Peppercoin micro-payment company.

Since 2001, Professor Rivest has been actively interested in the security of voting systems, from both a practical and a theoretical point of view. He is a lead member of the CalTech/MIT Voting Technology Project, and has served on the Technical Guidelines Development Committee, advisory to the U.S. Election Assistance Commission, regarding security standards for federal voting system certification. He has designed and developed a number of new voting system proposals, such as ThreeBallot and Twin. One voting system he has worked on, Scantegrity II, is the first such “end-to-end” voting system to be used in a binding political election.

Professor Rivest has strong interests in individual privacy, has served on a National Academy committee that studied privacy in a digital age, and is an advisor to the Electronic Privacy Information Center.

He is a co-author of the best-selling text on computer algorithms, “Introduction to Algorithms” (with Cormen, Leiserson, and Stein), now in its third edition. He has also developed numerous algorithms for machine learning.

Professor Rivest also enjoys travelling and photography, Boston sports teams (Red Sox and Patriots) and has a strong interest in solar energy.

Major Awards:

- 1990 Member, U.S. National Academy of Engineering
- 1991 Fellow, American Academy of Arts and Sciences
- 1993 Fellow, Association for Computing Machinery
- 1996 National Computer Systems Security Award
- 1996 ACM Paris Kanellakis Theory and Practice Award
- 2000 Secure Computing Lifetime Achievement Award
- 2000 IEEE Koji Kobayashi Computers and Communications Award
- 2002 Laurea Honoris Causa, University of Rome La Sapienza, Italy
- 2002 ACM Turing Award
- 2004 Fellow, International Association for Cryptologic Research
- 2004 Member, U.S. National Academy of Sciences
- 2004 Ceremonial Opening Pitch, Red-Sox Yankees baseball game
- 2005 MITX Lifetime Achievement Award
- 2007 Computers, Freedom, and Privacy “Distinguished Innovators Award”
- 2007 Marconi Prize

- 2008 Burgess and Elizabeth Jamieson Award (MIT EECS)
- 2008 Doctorat Honoris Causa, Universite Catholique Louvain

Professional Contributions:

- Co-author of “Introduction to Algorithms (with Cormen, Leiserson, and Stein)
- Author of approximately 150 technical publications; holds 8 patents.
- Served as Director of International Association of Cryptologic Research, and of the Financial Cryptography Association
- Served on National Research Council committee on Privacy
- Served on the Technical Guidelines Development Committee, advisory to the U.S. Election Assistance Commission.
- Serves on Advisory Board to Electronic Privacy Information Center

Professor Adi Shamir

Current Position:

The Paul and Marlene Borman Professorial Chair of Applied Mathematics
The Weizmann Institute of Science

Career History:

- 1952 Born in Tel Aviv, Israel
- 1973 B.Sc. (summa cum laude). Mathematics, Tel Aviv Univ., Israel
- 1975 M.Sc.. Computer Science, The Weizmann Institute of Science, Israel
- 1976 Postdoc, Dept. of Computer Science. Univ. of Warwick, England
- 1977 Ph.D., Computer Science, The Weizmann Institute of Science, Israel
- 1977 Instructor, Dept. of Mathematics, MIT, USA
- 1978 Assistant Professor, Dept. of Mathematics, MIT, USA
- 1980 Associate Professor, Dept. of Applied Mathematics, The Weizmann Institute of Science, Israel
- 1984 Professor, Dept. of Applied Mathematics, The Weizmann Institute of Science, Israel

Professor Adi Shamir was born in Tel Aviv, Israel. He received his BS degree in Mathematics from Tel Aviv University, his MSc and PhD degrees in Computer Science from the Weizmann Institute in 1973, 1975 and 1977, respectively. After a year postdoc at University of Warwick, he did research at MIT from 1977–1980, where he developed the idea of a public-key cryptosystem along with Professor Rivest and Professor Adleman.

After returning to the Weizmann Institute, he continued to lead the advancement of cryptography with new and unique ideas such as the Shamir secret sharing scheme in 1979,

identity-based cryptosystems and signature schemes in 1984, Feige-Fiat-Shamir identification scheme in 1988 and visual cryptography in 1994 (with Naor).

He has also contributed in a major way to improving the security of cryptographic primitives by indicating the weaknesses of well-known schemes like the Merkle-Hellman knapsack cryptosystem in 1982, NTRU in 1997 (with Coppersmith), A5/1 in 2000 (with Biryukov and Wager), WEP in 2001 (with Fluhrer and Mantin) and SFLASH in 2007 (with Dubois, Fouque and Stern). He has created new methods of analyzing schemes, for example, the differential cryptanalysis and the differential fault analysis in 1997 (with Biham), acoustic cryptanalysis in 2004 (with Tromer) and cub attacks in 2009 (with Dinur). Professor Shamir also challenged the factorization of long integers by developing specialized devices such as TWINKLE in 1999 and TWIRL in 2003 (with Tromer).

Another area where Professor Shamir has made important contributions is computational complexity theory. He proved that a language class IP (a class that is verifiable using Interactive Proofs) is equivalent to the conventional typical language class PSPACE, acceptable on a Turing machine having a polynomial order of spatial complexity. Outside of theoretical results, Professor Shamir has also designed many secure and practical protocols such as the Payword and Micromint payment systems in 1996 (with Professor Rivest), the Secureclick web payment system in 2001 and the SQUASH mac algorithm for RFIDs in 2008.

Living in Tel Aviv with his family, he has also been an invited professor at École Normale Supérieure in Paris since 2006.

Major Awards and Honors:

- 1975 Kennedy Prize, The Feinberg Graduate School
- 1978 Best Paper Award, IEEE Information Theory Group, USA
- 1982 Special Award, Israeli Information Processing Society
- 1983 Lubell Prize, The Weizmann Institute of Science, Israel
- 1983 Erdős Prize, The Israeli Mathematical Society
- 1986 Baker Prize, IEEE, USA
- 1990 UAP Scientific Prize, UAP, France
- 1992 PIUS XI Gold Medal, the Vatican's Pontifical Academy
- 1994 Rothschild Prize, Israel
- 1996 Kanellakis Prize, Association for Computing Machinery, USA
- 1998 Elected to the Israeli Academy of Science
- 2000 Koji Kobayashi Computers and Communications Award, IEEE, USA
- 2002 Turing Award, Association for Computing Machinery, USA
- 2003 Docteur Honoris Causa, Ecole Nonnale Superieure, France
- 2004 Elected Fellow, International Association of Cryptographic Research
- 2005 Elected to the US National Academy of Sciences

- 2007 Elected to the Academia Europaea
- 2008 Israel Prize in Computer Science
- 2008 Okawa Prize, The Okawa Foundation for Information and Telecommunications, Japan

Professor Leonard M. Adleman

Current position:

Henry Salvatori Chair in Computer Science and
Distinguished Professor of Computer Science and Biological Sciences
University of Southern California

Career History:

- 1945: Born in San Francisco, USA
- 1968: B.S. in Mathematics, University of California, Berkeley
- 1976: Ph.D. in Computer Science, University of California, Berkeley
- 1976: Instructor, Department of Mathematics, Massachusetts Institute of Technology
- 1977: Assistant Professor, Department of Mathematics, Massachusetts Institute of Technology
- 1979: Associate Professor, Department of Mathematics, Massachusetts Institute of Technology
- 1980: Associate Professor, Department of Computer Science, University of Southern California
- 1983: Professor, Department of Computer Science, University of Southern California
- 1985: Henry Salvatori Professor, Department of Computer Science, University of Southern California

Professor Adleman is best known for his co-discovery with Professor Ronald L. Rivest and Professor Adi Shamir of the RSA public-key cryptosystem. In addition he is the creator of the field of DNA computation, wherein computation takes place in aqueous solution via the interactions of biological molecules such as DNA and proteins. He is also credited with having coined the term “computer virus”. Though he has worked in many areas including theoretical computer science, virology, physics and chemistry, his primary area of interest and affection is number theory.

Major Awards and Honors:

- 1996 Elected to the National Academy of Engineering.
- 1996 ACM Paris Kanallakis Award for Theory and Practice (joint with Diffie, Hellman, Merkle, Rivest and Shamir).

- 2000 IEEE Kobayashi Award for Computers and Communications (Joint with Rivest and Shamir).
- 2002 ACM Turing Award (Joint with Rivest and Shamir).
- 2006 Elected to the National Academy of Sciences.
- 2006 Elected to the American Academy of Arts and Sciences.