Citation

For Outstanding Contributions to the Creation of the RSA Public-Key Encryption System, and the Production of a Number of Cryptographically Important Advances

Dr. Adi Shamir

Position and Organization :

The Paul and Marlene Borman Professor of Applied Mathematics, The Weizmann Institute of Science

Doctorate:

Ph.D. in Computer Science (The Weizmann Institute of Science, 1977)

Date of Birth: July 6, 1952.

Brief Biography :

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 Asst. Prof., Dept. of Mathematics, MIT, USA
1980 Assoc. Prof., Dept. of Applied Mathematics, The Weizmann Institute of Science, Israel
1984 Prof., Dept. of Applied Mathematics, The Weizmann Institute of Science, Israel
Incumbent of the Borman Professorial Chair of Computer Science

Main 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 Erdös 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
1997 Kanellakis Prize, Association for Computing Machinery, USA
1998 Elected to the Israeli Academy of Science
2000 Kobayashi Prize, IEEE, USA
2002 Turing Award, Association for Computing Machinery, USA
2003 Docteur Honoris Causa, Ecole Normale 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

Main Achievements :

Dr. Adi Shamir has made numerous fundamental research achievements in the area of cryptography at the foundation of information security technology, devising and further developing modern cryptography, and making major contributions to its practical implementation. Especially noteworthy is his proposal in 1977, with Ronald Rivest and Leonard Adleman, of the first practical public-key cryptography system, known as RSA. Nearly all such cryptography systems in use today-for the Internet, in smartcards and in other applications-adopt this algorithm. For their contribution, the three men were jointly awarded the A. M. Turing Award.

Dr. Shamir then went on to propose in 1979 the secret sharing scheme that is a basic part of encryption technology. He proposed the Fiat-Shamir scheme and the Feige-Fiat-Shamir scheme in 1986 and 1988, respectively. Both schemes are zero-knowledge identification and signature protocols for authenticating and signing without leaking confidential information. Applying these schemes to broadcast encryption, he contributed to the commercial implementation of paid broadcasting. In 1985 he put forth the concept of an identity-based cryptosystem as a promising candidate for next-generation encryption. These are a few examples of his many achievements in cryptographic technology and its applications. His more recent proposals include the ring signature scheme applicable to privacy protection, and the visual cryptography scheme (1994), a promising approach to electronic voting and other applications, as he continues to exert a major influence on the further development of modern cryptography. In addition, his many other contributions to technology with practical applications in areas such as digital cash, a convenient means of making small payments, are too numerous to list here.

At the same time, Dr. Shamir has contributed in a major way to improving the security of encryption, by proposing cryptanalytic attacks against various kinds of encryption schemes. Specific examples are the differential attack (1989), which had a large impact in breaking shared key encryption such as DES used by the United States government as standard encryption, as well as his breaking of the basic Merkle-Hellman cryptosystem in 1982, his 2003 study of RSA encryption security based on the proposal of dedicated hardware called the TWIRL device, and his devising of a practical cryptanalytic attack on the European standard encryption SFLASH in 2006.

Another area where Dr. Shamir has made important contributions is computational complexity theory. Here he clarified the relation between traditional computational complexity models and one based on interactive proof (IP), the foundation of identification and signature theory, demonstrating that a language class IP having interactive proofs consisting of polynomial order interactions is equivalent to a language class PSPACE acceptable on a Turing machine having a polynomial order of spatial complexity (1992).

Information security technology based on modern cryptography is an essential infrastructure for achieving a secure information society, today and in the future. Dr. Shamir has played a pioneering and guiding role in the creation, development and application of modern cryptography, through his many groundbreaking inventions and technological developments enabling their implementation, and by inspiring other outstanding researchers under his tutelage, over a long and illustrious career in the cryptography field. His contributions to technologies for realizing a secure information society allow us to use information services with peace of mind. In this important effort, he is rightly regarded as a researcher without peer.

In honor of these and many achievements, Dr. Shamir was elected a member of multiple academic societies, including the Academia Europaea, the US National Academy of Sciences (NAS), the Israeli Academy of Science, etc. His many awards include the Turing Award (ACM, USA), Israel Prize, PIUS XI Gold Medal (the Vatican's Pontifical Academy) and so on.

For outstanding contributions to the creation of the RSA public-key encryption system and the production of a number of cryptographically important advances, Dr. Adi Shamir is hereby awarded the Okawa Prize.