Citation

For Outstanding Contributions to Research in Coding Theory, Cryptography, and Their Applications

Dr. Hideki Imai

Positions and Organizations :

Professor, Faculty of Science and Engineering, Chuo University
Professor Emeritus, The University of Tokyo
Director, Research Center for Information Security, National Institute of Advanced Industrial Science and Technology

Doctorate: Ph.D. in Electrical Engineering (The University of Tokyo, 1971)

Date of Birth: May 31, 1943

Brief Biography :

1966 B.E., Electrical Engineering, The Univ. of Tokyo
1968 M.E., Electrical Engineering, The Univ. of Tokyo
1971 Ph.D., Electrical Engineering, The Univ. of Tokyo
1971 Lecturer, Yokohama National Univ.
1972 Assoc. Prof., Yokohama National Univ.
1984 Prof., Yokohama National Univ.
1992 Prof., The Univ. of Tokyo
2005 Director, Research Center for Information Security, National Institute of Advanced Industrial Science and Technology
2005 Member, Science Council of Japan
2006 Prof., Chuo Univ.
2006 Prof. Emeritus, The Univ. of Tokyo

Main Awards and Honors :

1976, 1991, 1992, 2003, 2004, 2008
Best Book Awards and Best Paper Awards from the Institute of Electronics, Information and Communication Engineers (IEICE)
1992 IEEE Fellow
1992, 2003
Yonezawa Memorial Paper Award and Inose Award from IEICE
1998 Golden Jubilee Paper Award from IEEE Information Theory Society
2002 Official Commendations from the Minister of Internal Affairs and Communications and from the Minister of Economy, Trade and Industry
2007 IACR Fellow
2007 The Wilkes Award (British Computer Society)

Main Achievements :

Dr. Imai has addressed numerous issues related to optimization of communication systems and information protection, and created new fundamental theories in these fields, applying his keen insight and originality. A number of application technologies based on these theories have been implemented, and are now essential technologies in various fields for the improvement of communication quality and information security. In addition, he has made major contributions to cryptography and information security measures by drawing up the e-Government Recommended Ciphers List, bringing together researchers in the cryptography field in Japan and overseas to conduct a multifaceted assessment of encryption technologies.

Dr. Imai received B.E., M.E., and Ph.D. at the Faculty of Engineering of the University of Tokyo in 1966, 1968, and 1971 respectively. Dr. Imai was hired immediately after the completion of his Ph.D. as lecturer at Yokohama National University, where he became Associate Professor in 1972 and Full Professor in 1984. In 1992 he became Professor at the University of Tokyo, and in 2005 he also took a position concurrently as Director of the Research Center for Information Security in the National Institute of Advanced Industrial Science and Technology. In 2006 he was made Professor Emeritus at the University of Tokyo, and in the same year, he became Professor at Chuo University. Throughout this time, he has carried on research and educational activities in the information and communication fields, achieving outstanding research results as well as sending numerous researchers and engineers to the academic and industrial worlds.

On the research front, he took up coding theory starting in 1971, conducting trailblazing studies on two-dimensional arrays and two-dimensional cyclic codes, and making major contributions as a pioneer in this field. From the mid-1970s, he proposed multistage decoding and multilevel coding techniques, path-breaking achievements in coded modulation that have had a major impact in both academia and industry. The research field of coded modulation, which crosses over the fields of coding theory and modulation theory, has since grown into a large field, while finding practical application in such areas as UHF communication and satellite broadcasting and showing promise also for use in optical communication. From the 1970s into the 1980s, he conducted pioneering research on interference cancelation in CDMA (code division multiple access) systems, where he contributed greatly to opening up a new research field with some of the world's first papers in this area. Interference canceling technology is used today in the W-CDMA technology adopted for third-generation mobile phone systems, and in terrestrial digital broadcasting, becoming an essential component technology for enhancing communication quality.

Starting in the late 1970s, he began research on cryptography, where he broke new ground in developing cryptographic techniques that no longer depend on computation quantity for security. They include public key encryption based on multivariate polynomials and linear coding, unconditionally secure digital signature schemes, and quantum key sharing, among others. Through these efforts, he built new cryptographic theories necessary for achieving long-term security. His theories have had a major influence on researchers in the cryptography field worldwide, and have contributed importantly to the formation of new research fields, such as in the area of encryption secure from the standpoint of information theory, and encryption that can be used securely even after the appearance of quantum computers. Dr. Imai has also taken up cryptographic research from some unique perspectives, proposing the highly original research field of human cryptography, which incorporates human elements in cryptography. Some examples are an authentication scheme that takes advantage of human sight characteristics to protect against snooping, an authentication key sharing protocol for secure use of short passwords, and privacy protection techniques. In addition, he has contributed importantly to the establishment of basic technologies for enhancing information security, through his researches in such areas as KPS (key predistribution system) for secure private key sharing using a peer ID without the need for prior communication, ID-based encryption, digital watermarks, and copyright protection schemes. Some of these technologies have been adopted in consumer products such as information appliances, and are used in systems for exchanging audio, video and other content between devices while complying with the digital rights management policy.

As described above, a succession of the results of Dr. Imai's world-pioneering research from a broad perspective in coding theory and cryptography have contributed greatly to the advancement of information and communication research in each area of study. For his accomplishments, the Institute of Electronics, Information and Communication Engineers (IEICE) has conferred on him the Yonezawa Memorial Paper Award, Achievement Award, Inose Award, and Distinguished Achievement and Contributions Award, as well as making him a Fellow. He was also made a Fellow of the Institute of Electrical and Electronics Engineers (IEEE), received the Golden Jubilee Paper Award from the IEEE Information Theory Society. Moreover, he was made a Fellow of the International Association for Cryptologic Research (IACR), received the Wilkes Award from the British Computer Society, and has won many other awards.

In addition to his scientific endeavors, he is a member of the Information Security Committee of the government's IT Strategic Headquarters, chairs both the Cryptography Research and Evaluation Committees (CRYPTREC) and the CRYPTREC Advisory Committee established jointly by the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI), and has served in many other important posts, contributing to the promotion of science policy as well as scientific knowledge in the field of information and communication technology in Japan. As CRYPTREC Chairperson, he was instrumental in drawing up the e-Government Recommended Ciphers List (a list of ciphers that should be recommended for use in the procurement of "e-Government"), engaging cryptography researchers from Japan and overseas for a multifaceted assessment of encryption technologies. In honor of his major contributions to information security policy in Japan, he received Official Commendations from the Minister of Internal Affairs and Communications and from the Minister of Economy, Trade and Industry.

For outstanding contributions to research in coding theory, cryptography and their applications, and to society as a whole through encryption and information security measures, Dr. Imai is hereby awarded the Okawa Prize.