ATTACHMENT 1: Profile of the Group A Recipients of the 2014 C&C Prize

Prof. Shigeo Tsujii

Current Positions

Professor, Research and Development Initiatives, Chuo University
Professor Emeritus, Tokyo Institute of Technology
Professor Emeritus, Institute of Information Security

Personal History (born in 1933)

1958	BE, Tokyo Institute of Technology
1958	Entered NEC
1965	Associate Professor, Yamanashi University
1970	Ph.D., Tokyo Institute of Technology
1971	Associate Professor, Tokyo Institute of Technology
1977	Overseas Researcher, City University London
1978	Professor, Tokyo Institute of Technology
1994	Professor, Chuo University
1996	Chair, Institute of Electronics, Information and Communication Engineers (IEICE)
1999	President, Research and Development Initiatives, Chuo University
2003	Member, Science Council of Japan
2004	President, Institute of Information Security
2007~	Member, Japan P.E.N. Club
2010~	President, Multimedia Promotion Center
	President, Secure Broadcasting Authorization and Research Center

Major Awards

1978	Commendation for Invention (Kanto Region)
1981, 89, 91	IEICE Best Paper Award
1985	IEICE Achievement Award
1990	IEEE Fellow
1993	ITU Association of Japan Award
1996	IEICE Distinguished Achievement and Contributions Award
1996	Okawa Publication Prize
1999	Ericsson Telecommunication Award
2000	IEEE Millennium Medal
2003	Official Commendation from MIC
2004	NHK Broadcasting Culture Award
2006	Takayanagi Memorial Award
2007	Official Commendation from Chief Cabinet Secretary
2009	Order of the Sacred Treasure, Gold Rays with Neck Ribbon

2014	SPECIAL AWARD for the contribution to CULTURE of SECURITY

Dr. Hideki Imai

Current Position

Professor Emeritus, The University of Tokyo

Personal History (born in 1943)

1966	BE, The University of Tokyo
1971	Ph.D., The University of Tokyo
1971	Lecturer, Yokohama National University
1972	Associate Professor, Yokohama National University
1984	Professor, Yokohama National University
1992	Professor, Institute of Industrial Science, The University of Tokyo
2004	President, IEEE Information Theory Society
2005	Director of Research Center for Information Security, AIST
2005	Member, Science Council of Japan
2006	Professor Emeritus, The University of Tokyo
2006	Professor, Chuo University
2011	Director of Institute of Science and Engineering, Chuo University
2012	Emeritus Researcher, AIST

Major Awards

1976, 91	IEICE Best Book Award
1992	IEEE Fellow
1992	IEICE Yonezawa Memorial Paper Award
1992, 03, 04, 08	IEICE Best Paper Award
1995	IEICE Achievement Award
1998	IEEE, Golden Jubilee Paper Award
1999	Honorary Doctorate, Soonchunhyang University
2002	Official Commendation from MIC
2002	Official Commendation from METI
2002	Docteur Honoris Causa, Toulon University
2003	IEICE Inose Award
2004	IEICE Distinguished Achievement and Contributions Award
2005	Ericsson Telecommunication Award
2007	IACR Fellow
2008	Okawa Prize
2008	AsiaJCIS LifeTime Achievement Award
2008	Wilkes Award, British Computer Society
2009	Official Commendation from Chief Cabinet Secretary

2009	IEICE Honorary Member
2010	NHK Broadcasting Culture Award

–Achievements–

People obtain a variety of conveniences from the rapid development of information systems and the Internet. However, the risks that lurk in the background have been a social problem in recent years. “Information security” refers to the protection of information assets from various threats based on confidentiality, integrity, and availability. Therefore, the importance of information security has been increasing very rapidly. However, such security will not be achieved only with the evolution and advances of related technology. Instead, a comprehensive approach is essential, including sophisticated application and use by people who have a good understanding of information security.

Prof. Shigeo Tsujii proposed the world’s first multivariable public-key encryption method based on a sequential solution method in the 1980s. Currently, research on this method is continuing internationally as a candidate for public-key encryption that will be able to withstand even a future ultra-high-speed quantum computer. In addition, Prof. Tsujii is promoting research on elliptic-curve encryption systems. And he is presently testing these approaches in government-research projects for the purpose of later introducing secure systems for e-government in Japan.

Prof. Tsujii is well known for being the first person in Japan to focus on security-related research, especially on encryption. And he has been promoting the start of research workshops on information ethics due to the development of related research fields.

In addition, in the 1990s, he soon recognized that, to improve information security, close integration among aspects related to management, operations, information ethics, legal systems, and technology is required. Therefore, in 1993, he proposed including information security in scientific studies and research. Later, he became the first president of the Institute of Information Security. The institute was established in 2004 based on the philosophy that such an organization is essential in order to avoid information technology risks and constraints while enabling the freedom necessary for the evolution of that technology. Through the institute, he fostered the development of lots of people who are supporting today’s technological prosperity in the information-security field.

In the area of public administration, Prof. Tsujii participated in OECD conferences on cryptography policy in the 1990s. After that, through his outstanding leadership on a lot of research committees organized by the Ministry of Economy, Trade and Industry (METI), the Ministry of Internal Affairs and Communications (MIC), and the Cabinet Secretariat, he made numerous and varied contributions to society.

In addition, with his outstanding leadership and extensive and positive influence on academia, industry, and government, Prof. Tsujii laid the foundation for the development of a wide-ranging field of information security in Japan. Moreover, he played a leading role in both establishing a well-balanced information society and fostering a culture of information security. Even now, he is developing new research areas, such as ones covering the sophistication of information-security concepts and encryption theory based on logic. In addition, he is continuing innovative research with his colleagues at the forefront of information security.

Dr. Hideki Imai started the theoretical study of cryptography in the field of information security in the late 1970s. He proposed public-key encryption with high-speed encryption and decryption characteristics in 1983. Also, he was the global pioneer in the research field of cryptography based on multivariate polynomials. Digital signatures based on this theory were standardized through a university-industry collaboration project in Europe called the New European Schemes for Signature, Integrity, and Encryption (NESSIE). The project ran from 2000 to 2003.

Dr. Imai has also been working on innovative technology such as quantum-key cryptography that is completely different from conventional cryptography, which depends on a very large number of computations. As a result, he proposed novel forms of cryptography that are necessary to ensure long-term safety. A typical example is the Key Pre-distribution System (KPS). It allows the secure sharing of a secret key by using a counterpart’s ID without any prior communication. KPS is practical as an information security system for IC cards as well as a promising approach for system development for the future Internet of Things (IoT).

Dr. Imai’s achievements are not limited to academic research areas. He became the chairperson of a committee that was established in 2000 to evaluate encryption suitable for the e-government of Japan. He oversaw a lot of researchers as the leader of the committee and selected the encryption that was designated as the standard for Japan’s e-government.

In addition, Dr. Imai founded the Symposium on Cryptography and Information Security (SCIS) in Japan 30 years ago and has been leading the information-security research communities. Moreover, as an international contribution to that kind of community, he established Asia's first international conference on the theory and application of cryptography and information security with Prof. Tsujii and others in 1990. It is called ASIACRYPT. Subsequently, he fostered the growth of this conference until it became one of the three major cryptography conferences in the world. In addition, he played a major role in the foundation of the International Conference on Practice and Theory of Public-Key Cryptography (PKC), which is well known in this field. He was also instrumental in the promotion of encryption research in the information theory community as the president of the IEEE Information Theory Society.

Through these activities, Dr. Imai’s contributions to spreading the applicable areas of encryption have been quite remarkable. And he has been raising the talent of many information-security researchers. Based on those achievements, the International Association for Cryptologic Research (IACR) made him the first Fellow in the East-Asia Region.

As described above, the contributions that both of these men have made in the field of information security have been remarkable and were key factors in the creation of today's prosperous information society. Both recipients noticed the importance of the field from the initial research stage, and their subsequent advances and leadership have been excellent. Therefore, they are known as pioneers of numerous applications of cryptographic research and work aimed at post-quantum computers. Moreover, they contributed significantly to the development of human resources and research areas through the promotion of information security for science through community-building activities and standardization work for the ISO. Thus, they are quite worthy of the 2014 C&C Prize.