1994-TS-J-Tokyo-Tech-EEIC-Engrg

TSUJII Shigeo

"Construction of Integrated Security for Establishing Infrastructure of Digital Transformation"

1. Biography

Born on 13th September, 1933.

Graduated from Tokyo Institute of Technology, 1958. Doctor of Engineering,

1979, Professor, Tokyo Institute of Technology, 1994, Professor, Chuo University

1996, President, The Institute of Electronics, Information and Communication Engineers (IEICE)

1999, Director, Research and Development Initiative, Chuo University

2003, Member, Science Council of Japan

2004, The first Principal of Institute of Information Security (IISec)

2004, Professor, Research and Development Initiative, Chuo University

2007, Member, Japan P.E.N. Club

2010, Chairman, Foundation for Multimedia Communication

2013, Chairman, Secure Broadcasting Authorization and Research Center

2017, Chairman, Secure IoT Platform Consortium

Awards Received (excerpts)

The Order of the Sacred Treasure, Gold Rays with Neck Ribbon (2009), NHK Broadcast Cultural Award (2004), C&C Prize (2014), Memorial Award, "Takayanagi Kinen-shou" (2006), Distinguished Achievement and Contributions Award, IEICE (1996), IEEE Third Millennium Medal (2000), Invention Prize, etc.

2. Summary

Shigeo Tsujii has been continuing academic research, human resource development, and social activities for more than 60 years since he was 25 years old (1933) to now, 88 years old (2021).

(1) Research Activities, Conceptual Studies

The research activities while he was between 25 and 50 years old: he was engaged in study of analog transmission system, digital transmission system, and digital signal processing in NEC Corp., Yamanashi University, and Tokyo Institute of Technology (Tokyo Tech).

Patent: Invention of Code Modulation System for Color Television (1978), (Kanto Area Best Invention Prize)

From the age of 50 up to now: While proposing post-quantum cryptographies, he has been suggesting to integrate information security science including cryptography into a comprehensive science to endeavor to achieve the highest possible equilibrium of the three principles: "expansion of freedom, improvement of public safety, and securing individual right and privacy," which are apt to contradict

each other, with the methodology integrating Management, Ethics, Law and Technology (MELT-UP).

(2) Human Resource Development

He has been involved in various kinds of human resource development activities as an assistant professor of Yamanashi University, professor of Tokyo Tech, and professor of Chuo University. In cryptography, Dr. Kaoru Kurosawa and Dr. Jinhui Chao, both of whom have achieved outstanding results.

In 2004, taking up an appointment as the first Principal of IISec at the age of 70, he held up an idea of "Information Security as a Comprehensive Science" to train numerous people with broad expertise.

(3) Activities in the Academic Word and Contribution to the Society

Along with the duty as the chairman of IEICE, which is closely related to his special field, he worked for Japan Society of Security Management and NPO Institute of Digital Forensics, etc. as a chairman. Additionally, he has worked as the leader of Radio Wave Supervision Council and Committees about establishing legal systems about digital signature and Residential Basic Book, etc. Currently he serves as the director of Secure IoT Platform Consortium with the idea of "Authentication is the core of the principle under all layers from the physical to society." Then he has built Koukikai to support research activity of senior and female researchers and currently hold symposiums frequently.

(4) Publishing Activities

Technical Book: "Cryptography: Information Security Technology and History" (2012), Kodansha Ltd., the book which won Okawa Publishing Prize

"Elliptic Curve and Cryptographic Theory" (Morikita Publishing Co. Ltd., 2008)

Interdisciplinary Book: "Information Society / Security / Ethics" (2012), edited by Institute of Electronics, Information and Communication Engineers (IEICE) and published by Corona Publishing Co., Ltd., etc. (This book has attracted the notice of, Dr. Hisatake Kato, the philosopher, and was introduced in Homo Contribuens Colloquium. The concept in this book had the honor of winning the name of "Tsujii Information Philosophy.")

"Battle against Fakes—Idea and Reality which an Information Scientist/Cryptologist has Witnessed: from Pacific War to COVID-19" (Kotonisha, 2021）

3. Background of the Academic Achievement

DX (Digital Transformation), which has recently become the topic of conversation, began as early as around 1958, when he entered NEC Corp. He has developed Japan's first digital transmission system (PCM24CH system) and obtained the patent about digitalization for suppressing noise, foreseeing the period of color TV, and was awarded Prize for the invention. After moving to the academic field, he has also led the study of digital signal processing which was expected to take the place of analogs.

Major purpose of public key cryptographies is authentication and signature, or authenticity assurance of both people and things. When he introduced Japanese "Seal Registration Certification" system in a Japan-Germany International Conference, participants were surprised. However, in terms

of digitization of authentication / signature, we seem to be far behind other countries.

He began the study of cryptography in 1979, fascinated by the beauty of the theory and feeling the necessity of public key cryptography as the infrastructure of DX society. Then he has proposed MPKC, one of post-quantum cryptography.

Although the recognition of information security as cryptography was prevailing during 1990s, he did not think that information security could be achieved solely with cryptography and claimed the necessity of comprehensive science of information security in an invited paper of the Institute of Television Engineers (Currently The Institute of Image Information and Television Engineers).

Afterwards, around the year 2000, he has emphasized policies utilizing Management, Ethics, Law, and Technology in both domestic and overseas conferences (see Fig. 1)

When he retired from Chuo University and became the first Principal of IISec in 2004, he has held up the idea of Drei Aufheben, and MELT-UP, inviting first-class teaching staffs from various fields including technology, law, and management, etc. IISec, with lots of adult students, contributes to the human resource development, with numerous cases where technical students learn legal system, etc. Additionally, he has endeavored to implement Ethics Study Group in IEICE.

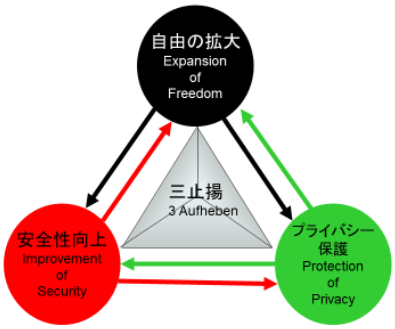

Figure 1: Drei Aufheben

Research and Development Initiative, a new organization operated exclusively with external fund, was established in Chuo University in 1999. Then he was assigned the first Director of the R & D Initiative, for which he continues working as a professor obtaining project fund after retirement as a professor of the university. During that, our group has accepted about ten well-motivated researchers, who are actively producing results in information security, blockchain, and quantum stream cryptography Y00, etc.

Outline of the Academic Achievements

I. 1958-1965, NEC Corporation

① **Development of Japan's First Digital Transmission System (PCM 24-Channel System)**
② **Development of the World's First Digital System for Television Signals**

Acquisition of Patent and Commendation for the Digitalization of Color TV

Description:

Color TV was not in use yet at that time. While he was experimenting digitization with monochrome TV, he imagined that large noise would be generated if the signal is of color TV on the digitized screen. So, he has proposed the digitization system with the sampling frequency 3 times as much as that of NTSC signals. It was later reputed that "it was owing to that patent that the Broadcasting Division still exists."

II. 1965-2004, Yamanashi University, Tokyo Tech, Chuo University

③ **Study of Digital Network Using Graph Theory, Awarded Best Paper Prize, IEICE**
④ **Start of the Leading Study of Digital Signal Processing. Two papers were awarded Best Paper Prize, IEICE.**

He began the study of modern cryptography in 1979.

⑤ Proposal of Multivariate Public-Key Cryptography (MPKC) based on Sequential Solution Method in 1985

Multi-variate Public-Key Cryptography (MPKC) , which was originated in Japan, is currently one of the candidates for post-quantum cryptography in NIST. Following Matsumoto-Imai Cryptography, he has proposed sequential solution method, inspired from structure of circuitry in 1985. It was only in Japan that the MPKC had been studied during 1980s. After it was theoretically proved in 1994 that, if quantum computer was in practical use, currently used RSA or ECC would be solved, post-quantum cryptographies including MPKC are actively studied worldwide.

⑥ Perfect Agreement between Idea and Reality in ECC — Confirmation in Neoplatonistic Way

Thales, the Ancient Greek philosopher, proposed the idea of a line with zero-width around 2600 years ago. Kitaro Nishida, a philosopher, has claimed around 1907 that "there is no such thing like a line with zero-width or a surface with zero-thickness in the real world." RSA, which is most widespread, corresponds to circle. ECC, which was proposed after RSA in 1985, corresponds to ellipse. ECC as secure as RSA with the key length 2048 bit can be constituted with 200-bit key. Then how about an ECC corresponding to an ellipse infinitely close to circle (such as the one as large as the planet earth with the width enlarged by 1 millimeter)? Theoretically it should still be an ellipse, which was confirmed with about 10,000 experiments. In a Neoplatonistic description, this is a rare case where a theory comes from the Idea World to the Reality without deterioration and enter devices. Dr. Kato (philosopher) was quite interested in this concept. This is because modern cryptography is constructed on finite fields, without continuity or size (Fig. 2).

III. As the First Principal of IISec and a Leader of Various Government-run Organizations

⑦ Structuring Digital Security Comprehensive Science and Drei Aufheben—MELT-UP

Digital Security is a wide-range science ranging from mathematical theory like cryptography to management, ethics, and law, etc., which are directly related to our life and society. As described in (1), he keenly felt the necessity of digital security comprehensive science constituted by management, ethics, law and technology in 1993 (Ref. (9)) and discussing its construction from both the standpoint of principle and realization (Ref. (3), etc.). What are the principles which create habitable society and make people happy?

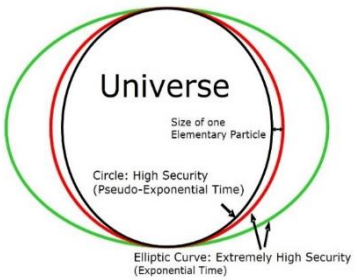

Figure 2: Security of Elliptic Curve

The solution, which is influenced by values of the period, etc., cannot be uniquely determined. Multiple principles would be combined. For example, Freedom, impartiality, and Philanthropy were proposed during French Revolution. Recently, M. Sandel has listed Liberalism, Communitarianism, and utilitarianism. Tsujii has been emphasizing 3 principles of Freedom, publicness (safety, etc.)

Individual Right (privacy, etc.) in infosec. I have proposed the Drei Aufheben to achieve equilibrium of the three principles, which often contradict with each other, at as high level as possible. Based on that principle, IISec was built and I was engaged in human resource management. Additionally, he held lots of symposiums to contribute to the reform of DX society. Recent achievements include their concrete examples about My Number, digital currency, etc.

⑧ **3-Layer Public-Key Cryptography for the Ultimate Personal Identification**

While public key cryptography has two-layer structure, with the private key embedded in the public key, the failure of personal identification may endanger our life or property in the future DX society. So Tsujii, et al. proposed 3-Layer public key cryptography, which has Short Tandem Repeat, and My Number embedded within [Figure3, Ref. (1)]

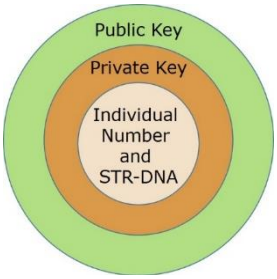

Figure 3: 3-Layer Public-Key Cryptography

References

(1) Tsujii et al., “3 Layers Public Key Cryptosystem with a Short Tandem Repeat DNA for Ultimate Personal Identification - Introduction of Short Tandem Repeat Coupled with Mai Nanbaa and its Application- part 2,” Jan. 2020, SCIS2020 (in Japanese)

(2) Tsujii, Fujita, Gotaishi, “Proposal of Multivariate Public Key Cryptosystem Based on Modulus of Numerous Prime Numbers and CRT with Security of IND-CPA,” Nov. 2019, IEICE Technical Report (in Japanese)

(3) Tsujii, Saisho, Yamasawa, Sato, “3-Aufheben・MELT-UP Sociological Study of Digital Forensic Activities,” Oct. 2017, CSS 2017 (in Japanese)

(4) S. Tsujii, “MELT-up Aufheben in Preparation for Cyberattacks and Information Leaks - I Expect Tokyo Tech to Develop Human Resources with Comprehensive Aufheben Power,” Oct. 2015, Journal of Tokyo Tech Alumni Association: Kuramae Journal (in Japanese)

(5) S. Tsujii, “4 Types of Broadcasting / Communication and Organizational Communication / Organizational Cryptography - Toward the Sophistication of the Concept of Information Security,” Nov. 2013, Column 287, NPO Institute of Digital Forensics (in Japanese)

(6) Hisatake Kato (editor), “Introduction to Information Philosophy by Shigeo Tsujii,” 2013, Homo Contribuens Colloquium (in Japanese)

(7) S. TSUJII, “Information Society, Security and Ethics,” Aug. 2011, 2011 IEEE International Conference on Peer-to-Peer Computing (IEEE P2P 2011)

(8) S. Tsujii, “New Trends in the Information Society and Information Security,” 2008, Japan Society for Information and Management (JSIM) (in Japanese)

(9) S. TSUJII, “For Establishment of Comprehensive and Structural Information Security Science,” 1993, The Journal of the Institute of Television Engineers of Japan, Vol.47 No.2 (in Japanese)

(Presented by TSUJII Shigeo on 24 July 2021)