A-40

Statistical Machine Learning

N. Ueda constructed a learning algorithm based on the mathematical approach to the basic study and actual application of statistical machine learning, thereby, making a significant contribution to scientific development in this field. Specifically, research included the selection-type competitive learning method for vector quantizer design, the DAEM method and the SMEM method which were problem solving methods for local optimization of the EM algorithm, the optimal model search method with the variational Bayesian method and the application of the hidden Markov model for sound recognition to optimal model design. These research findings were highly appreciated globally.

A-41～A-44

Ciphers and Information Security

Cryptographic Theory/Methods

Cryptanalysis/Security

International Data Encryption Standards

Comprehensive Measures for Information Security

In terms of methods, modern ciphers are classified into symmetric-key cryptography and public-key cryptography. In terms of applications, they have two functions, concealment and authentication/signature.

Symmetric-key cryptography, which has been used for military affairs/foreign diplomacy from old times, is the method where the sender and the receiver use a common key, and its application is mainly for concealment. In the information society, because the importance of concealment has become a social need, the algorithm is opened to the public while the key alone is kept secret. On this point, the modern cipher is different from the classical cipher, and consequently, since the 1970s, the sophistication of this method has been promoted internationally. Security analysis is crucially important. The linear analysis by Mitsuru Matsui is a world-class Japanese achievement deserving special mention.

On the other hand, public-key cryptography, unlike symmetric-key cryptography, consists of two types of keys, secret keys and public keys. The secret key is kept by the persons concerned alone, while the public key is opened to the public. Its essential functions are authentication (confirmation of identity/authenticity) and the signature, which are indispensable for the information society/IoT. The invention of public-key cryptography was an epoch-making event—equal to the invention of gunpowder—as described in some science

technology books. Because of its difficulty, however, it is not well recognized socially. However, the bitcoin/blockchain which is expected to bring in significant changes in economic infrastructure in the days to come is based on public-key cryptography (elliptic cipher) and the authentication/signature with the Huck function as its technology platform, and accordingly its importance is increasing more and more.

Globally many research papers have been published, and their world rankings have been announced. In Japan, Tatsuaki Okamoto and Kaoru Kurosawa are sometimes placed in the top ten in world rankings.

In addition, around 2000, parings were conceptualized by R. Sakai and M. Kasahara and now cover a large part of the fields discussed at international conferences.

Currently, RSA and the ellipse cipher are widely used as public-key cryptography, however, in the days ahead, when quantum computers are put to practical use, the security of these ciphers may not be assured, and accordingly, alternatives are now being searched for. One of these is multivariable public-key cryptography. T. Matsumoto and H. Imai followed by S. Tsujii, et al., proposed this method before the rest of the world in the 1980s.

Cryptographic technology is the basis of information security technology; however, information security measures area part of social infrastructure consisting of four-way integrated cooperation—control/management, information ethics/psychology/code of conduct, legal system, and technology. Many results have also been published in this field. For example, digital forensics, integrated systems for evidence, consists of technology, auditing, and regulations. Incidentally, the pioneering achievement in this field by Ryoichi Sasaki was significant indeed.