Overview

The Current State of Encryption Technology

*by Kotaro Katsuyama**

With advances in the Internet, progress in mobile phones and other mobile communications devices, and with similar developments taking place in digital electrical equipment for the home and in sensors, we are entering the era of the ubiquitous network. While this offers society the prospect of great convenience, enabling the almost instantaneous exchange of large volumes of electronic data, the facts that everything will be connected to the same network and communications will be possible from any one point to any other within the network pose new threats of eavesdropping, tampering, impersonation and breaches of security. These threats are making the technology for ensuring the security of information, particularly encryption technology, increasingly important. Mitsubishi Electric possesses world-class technologies in this area: our MISTY encryption technology is used in the KASUMI algorithm adopted for third-generation mobile phone systems and for GSM. The corporation also provides a number of advanced security solutions that make major contributions to the safety and security of the social infrastructure.

This issue of *Advance* introduces the corporation's MISTY, Camellia and KASUMI encryption algorithms, along with the technologies for evaluating the degree of security provided, and for implementing these algorithms. The tamper-proof TURBOMISTY secure boards are also introduced. Finally, there is an article that outlines the corporation's work directed at future applications of quantum cryptography. ❑

**Kotaro Katsuyama is with the Information Technology R&D Center*