Three Leading Japanese Firms Jointly Develop a New Encryption Technology—Elliptic Curve Cryptosystem (ECDSA Signature)

Hitachi, Ltd., Mitsubishi Electric Corporation, and NTT announced on July 28, 2003 their success in jointly researching and developing a secure and efficient implementation for an elliptic curve cryptosystem (ECDSA signature)[*1], which they have called CRESERC. This is the world's first case of well-established leaders in the field of cryptography collaborating in the development of implementation technology by integrating their advanced skills and technologies.

Background to the joint R&D

To achieve e-governance[*2] and the ubiquitous[*3] environment mentioned in the "e-Japan Priority Policy Program", there is a pressing need to establish a fundamental technology to provide a truly secure communication environment and to support the advanced information sharing society. Encryption and electronic authentication[*4] are central to this technology. Secure and efficient implementation is a vital R&D goal for achieving practical use, but there has been a trade-off between security and efficiency. Hitachi, Mitsubishi Electric and NTT launched a joint project and have succeeded in developing an implementation technology with the world's strongest security level while matching the efficiency of the existing products on the market.

In March 2003, the EU (European Union) approved NESSIE[*5], a project to select the next-generation cryptographic algorithms. They selected Camellia[*6] jointly developed by Mitsubishi Electric and NTT, MISTY1[*7] by Mitsubishi Electric, and PSEC-KEM[*8] by NTT as recommended algorithms. Meanwhile, ISO (International Organization for Standardization) has been promoting the standardization of encryption goals by the Spring of 2004 at the earliest. In their deliberations, they have nominated not only Camellia, MISTY1, and PSEC-KEM, but also MULTI-S01[*9] and MUGI[*10] by Hitachi for international encryption standards. In addition, as recommended cryptographic algorithms, they also selected ones by

*1 Elliptic curve cryptosystems: Public key cryptosystems utilizing mathematical operations over elliptic curves. They can encrypt data using short key lengths at high efficiency while maintaining a high level of security, so they are receiving attention as new-generation public key cryptosystems that can replace RSA schemes (named after Rivest, Shamir, and Adleman). ECDSA (Elliptic Curve Digital Signature Algorithm) is a digital signature algorithm based on elliptic curve cryptosystems. It has been selected by NESSIE and CRYPTREC as one of the recommended signature schemes.

*2 e-governance: A governance support tool that allow various tasks including administration to be executed electronically by utilizing computer systems and Internet technology. Not to be confused with the more-commonly used term e-government, which refers to government agencies working together to use technology so that they can better provide individuals and businesses with government services and information.

*3 Ubiquitous: Existing everywhere at the same time (derived from the Latin *ubique* meaning everywhere). It is a popular term these days to describe an environment where a user can access information networks like the Internet at any time from anywhere.

*4 Electronic authentication: A technology for providing electronic (digital) signatures and public key certificates (electronic certificates).

*5 NESSIE (New European Schemes for Signatures, Integrity, and Encryption): An EU-approved project to select next-generation cryptographic schemes started in 2000 and completed at the beginning of 2003.

*6 Camellia: A 128-bit block encryption algorithm jointly developed by Mitsubishi Electric and NTT. Specifications have been disclosed and published.

*7 MISTY1: A 64-bit block encryption algorithm developed by Mitsubishi Electric. Specifications have already been disclosed and published.

*8 PSEC-KEM: A public key encryption algorithm developed by NTT. Specifications have already been disclosed and published.

*9 MULTI-S01: A 256-bit key length stream encryption algorithm developed by Hitachi. Specifications have already been disclosed and published.

*10 MUGI: A 128-bit key length stream encryption algorithm developed by Hitachi. Specifications have already been disclosed and published.

CRYPTREC: the cryptography evaluation project for e-governance by MPHPT (Ministry of Public Management, Home Affairs, Posts and Telecommunications) and METI (Ministry of Economy, Trade and Industry).

Since the late 1990's, the U.S. and Japanese governments, the EU, and ISO have actively promoted these encryption algorithm validation, selection, and standardization activities. They are now almost reaching completion, and the cryptographic algorithms that will be widely used in the first half of the 21st century are being chosen. The above Japanese cryptographic algorithms were highly regarded throughout these activities for their excellent efficiency and high commercial viability (LSI implementation), and it is likely that one or more of them will be widely used. Currently, ISO and CRYPTREC recognize that they need to emphasize secure implementation, and they plan to establish the corresponding validation criteria and validation standards.

As concern over secure implementation of cryptosystems increases, CRESERC is expected to be applied in various situations that require information security (for example, e-governance and ubiquitous communication systems) as the world's leading implementation technology in the field.

Roles of the three companies

In this joint R&D, Hitachi provided secure implementation technology for elliptic curve operations, Mitsubishi Electric provided efficient implementation technology for elliptic curve operations, and NTT provided efficient and secure implementation technology for the basic arithmetic.

Future plans

All three companies plan to launch products incorporating each others' technology in e-governance systems and ubiquitous-related security products based on their joint R&D results, namely CRESERC.

For further information, please contact
NTT Information Sharing Laboratory Group
Musashino-shi, 180-8585, Japan
E-mail: koho@mail.rdc.ntt.co.jp

Most Advanced Wireless Technology in Scotland Launched at EICC

An exhibition of the most advanced wireless technology ever to be seen in Scotland was launched at the Edinburgh International Conference Centre (EICC) on August 5, 2003 and will run until March 2004. Scottish Enterprise has been instrumental in bringing this technology to Scotland with assistance from NTT in partnership with the EICC and BT. The exhibition will give visitors to the EICC the opportunity to experience data-transfer and connection speeds of more than 50 times faster than normal dial-up speeds—without the need for wires.

Users who have a wireless-enabled laptop or PDA (personal digital assistant) will be able to send and receive e-mail, browse the web, and securely access their own company intranet sites if available—demonstrating the benefits of broadband and wireless technology.

EICC visitors will have the opportunity to experience the most widely used wireless technologies (802.11b*1), provided and installed by BT. This will be contrasted with the wireless technology of the

*1 802.11 standards: 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of IEEE. There are currently four specifications in the family: 802.11, 802.11a, 802.11b, and 802.11g. All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.