World's First Success! Three Leading Japanese Firms Jointly Develop A New Encryption Technology

--Elliptic Curve Cryptosystem (ECDSA Signature)--

TOKYO, July 28, 2003 - Hitachi, Ltd. (President: Etsuhiko Shoyama), Mitsubishi Electric Corporation (President and CEO: Tamotsu Nomakuchi) and Nippon Telegraph and Telephone Corporation (President: Norio Wada) hereafter, Hitachi, Mitsubishi Electric and NTT, respectively, announced their success in mutually researching and developing an implementation technology of an elliptic curve cryptosystem (ECDSA signature) [1]. They named the technology "CRESERC". To establish this technology, Hitachi, Mitsubishi Electric and NTT founded a project team to research and develop a secure and efficient implementation for elliptic curve cryptosystem (ECDSA signature). 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 realize e-governance [2] and the ubiquitous [3] environment listed in "e-Japan Priority Policy Program", there is a pressing need to establish a fundamental technology to realize 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 technology" is a vital R&D goal for achieving practical use. However, R&D has been faced with a trade-off between "security" and "efficiency". Therefore, Hitachi, Mitsubishi Electric and NTT launched the joint project and now they have succeeded in developing an implementation technology with the world's strongest security level while matching the efficiency of the existing products in the market.

In March 2003, 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", "PSEC-KEM" but also "MULTI-S01" [9] and "MUGI" [10] by Hitachi for international encryption standards. In addition, they have also been selected as recommended cryptographic algorithms by 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, EU and ISO, have actively promoted these encryption algorithm validation, selection, and standardization activities. They are now being almost completed, and the cryptographic algorithms that will be widely used in the first half of the 21st century are being listed up. The above Japanese cryptographic algorithm's excellent efficiency and their high commercial viability (LSI implementation) are highly regarded throughout these activities and it is likely that one or more of these Japanese company's algorithms 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 set into various application areas 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 3 Companies
Hitachi, Mitsubishi Electric and NTT mutually carried out this joint R&D by sharing their preeminent technology on the basis of their shared advantage: the mathematical theory of elliptic curve cryptosystems. Their roles are as follows:
Hitachi: secure implementation technology of elliptic curve operations
Mitsubishi Electric: efficient implementation technology of elliptic curve operations
NTT: efficient and secure implementation technology of basic arithmetic

Future Plan
These three companies plan to launch products incorporating each company's preeminent technology in e-governance system and ubiquitous-related security products based on their joint R&D results, namely "CRESERC".

Terminology

1. Elliptic curve cryptosystem: Public key cryptosystems utilizing the mathematical operations over elliptic curves. They can encrypt the data using short key lengths at high efficiency while maintaining the high level of security, thus it is receiving attention as the new generation public key cryptosystems that can replace RSA schemes. 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 electrically by utilizing computer systems and Internet technology.

3. Ubiquitous: Derived from Latin meaning "exists everywhere". It means the environment where user can access information network like the Internet at any time from everywhere.

4. Electronic authentication: A technology to realize seals and seal certificates in the electronic world by utilizing electronic signatures and public key certificates (electronic certificates).

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

6. Camellia: 128 bit block encryption algorithm jointly developed by Mitsubishi Electric and NTT. Specifications are already disclosed and published.

7. MISTY1: 64 bit block encryption algorithm developed by Mitsubishi Electric. Specifications are already disclosed and published.

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

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

10. MUGI: 128 bit key length stream encryption algorithm developed by Hitachi. Specifications are already disclosed and published.

About HITACHI
Hitachi, Ltd. (NYSE: HIT), headquartered in Tokyo, Japan, is a leading global electronics company, with approximately 340,000 employees worldwide. Fiscal 2002 (ended March 31, 2003) consolidated sales totaled 8,191.7 billion yen (68.3 billion dollars). The company offers a wide range of systems, products and services in market sectors, including information systems, electronic devices, power and industrial systems, consumer products, materials and financial services. For more information on Hitachi, please visit the company's Web site at http://global.hitachi.com.

About Mitsubishi Electric
With over 80 years of experience in providing reliable, high-quality products to both corporate clients and general consumers all over the world, Mitsubishi Electric Corporation (TSE: 6503) is a recognized world leader in the manufacture, marketing and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, energy, transportation and building equipment. The company has operations in 35 countries and recorded consolidated group sales of 3,639 billion yen (30.3 billion US dollars*) in the year ended March 31, 2003. For more information, visit http://global.mitsubishielectric.com

*At an exchange rate of 120 yen to the US dollar, the rate given by the Tokyo Foreign Exchange Market on March 31, 2003.

About NTT
NTT is a holding company of the Global Information Sharing Enterprise Group and NTT group, which consists more than 430 companies.
One of the important missions of NTT group is to contribute the achievement of a Ubiquitous Broadband society. NTT group concentrates on integrating the group on expanding Broadband Service on Photonic Access, Third Generation Cellular Phone, Wireless LAN, are provided for Access means, promoting the structure of distributing the contents of Movies and music, and enhance the providing contents.
In November 2002, the Vision for a new optical generation is announced.
For more information, please visit http://www.ntt.co.jp/index_e.html

For media inquiries only:
Hitachi, Ltd.
Public Relations of Corporate Communications Division ; Konno
Tel: +81-3-3258-2056 atsushi_konno@hdq.hitachi.co.jp

Mitsubishi Electric Corporation
Robert Barz, Public Relations Department
Tel: +81-3-3218-2346 Robert.Barz@hq.melco.co.jp

NTT Information Sharing Laboratory Group

Planning Department, Public Relations Group; Iizuka, Sano, Chizuka
Tel: +81-422-59-3663 koho@mail.rdc.ntt.co.jp