Nippon Telegraph and Telephone Corporation
Mitsubishi Electric Corporation

# NTT and Mitsubishi Electric Develop Advanced Encryption Scheme to Increase Cloud Computing Security

**Tokyo, July 28, 2010** – Nippon Telegraph and Telephone Corporation (NYSE: NTT, "NTT") and Mitsubishi Electric Corporation (TOKYO: 6503, "Mitsubishi Electric") today announced that they have developed a new advanced encryption (fine-grained encryption) scheme expected to become a potential solution to the security risks in cloud computing. This new encryption scheme achieves the most advanced logic in the encryption-decryption mechanism, which enables sophisticated and fine-grained data transmission/access control.

The rapid development of information and communication technology has led to the recent spread of cloud computing and other advanced network systems. These networks, however, transmit private or confidential information to the server to process, which demands higher security than current systems that use symmetric [*1] and public [*2] key encryption to maintain network security. These advanced network systems therefore require a more sophisticated encryption scheme.

NTT and Mitsubishi Electric have successfully developed a new fine-grained encryption scheme with the most advanced logic as an encryption-decryption mechanism. This scheme, developed using a mathematical approach called the "dual pairing vector spaces," [*3] will allow network users to maintain highly confidential information encrypted even in cloud computing environments. This achievement will help expand cloud computing applications to fields where they could previously not be applied.

The details of this scheme will be presented at "CRYPTO 2010," the 30th International Cryptology Conference, which is scheduled to be held in Santa Barbara, California, USA from August 15 to 19, 2010.

## Main features of the new fine-grained encryption scheme

### 1. Achieving the most general logic

For the past few years, fine-grained encryption has attracted many researchers in the field of cryptography. The new, fine-grained encryption scheme by the two companies achieves the most advanced logic that comprehends those of the existing fine-grained encryption schemes. This logic can be realized by comprising AND, OR, NOT and threshold gates.

One of the most significant achievements is that the NOT gate is now available, allowing cloud computing systems to manage databases easily and flexibly in cases of change in user attributes and other information.

### 2. Available to a variety of applications

In fine-grained encryption, a variety of parameters are added to the ciphertext and decryption key in the encryption-decryption logic. In this logic, attributes and predicates on them become the parameter of the ciphertext or decryption key. The newly developed encryption scheme is available to a variety of applications because it is capable of being used in either of the following forms: (1) attributes as the parameter of the decryption key, predicates as that of the ciphertext, and (2) attributes as the parameter of the ciphertext, predicates as that of the decryption key.

In case (1), various access conditions will be set in detail for each encrypted data in a cloud computing database, and a user will be able to decrypt and access the data by using the decryption key when the attributes of the decryption key satisfy the pre-set predicates in the ciphertext. Applications include confidential document management systems in firms, as well as personal information database management by public organizations. For confidential document management systems in firms, for example, each document will be set by a predicate that describes the attributes of users allowed to decrypt the encrypted document. The document and its predicate as a set will then be encrypted and placed in a cloud computing database. The encrypted document will only be able to be decrypted and accessed by an employee who has a decryption key associated with some attributes, when the decryption key's attributes satisfy the predicate pre-set in the encrypted document.

Meanwhile, in case (2), data and attributes will be encrypted as a set when it is managed by the cloud computing system, and each user can only decrypt and read the data if the attributes of the encrypted data satisfy the predicate in the decryption key. Applications include content distribution as well as database management in finance or medical fields. In the content distribution, for example, content providers will encrypt contents like animation, films and others with its attributes and place the encrypted contents in a cloud computing database. The audience will then view the contents by decrypting it using the decryption key when the contents' attributes satisfy the decryption key's predicates.

## Future plans

The new encryption scheme developed by NTT and Mitsubishi Electric is expected to play an important role in achieving secure environments for cloud computing and other advanced network services. The two companies now plan to study how to efficiently implement and utilize this scheme for various applications.

*Notes:*

**1: Symmetric key encryption*

*It is a cryptosystem using the same key for both encryption and decryption. It is widely used for transferring data in large volumes, encrypting files at high speed, authenticating mobile handsets and other applications due to its fast processing capabilities. Representative symmetric key encryptions are: the Advanced Encryption Standard (AES), the 64-bit block cipher "MISTY" developed by Mitsubishi Electric and the 128-bit block cipher "Camellia" which was jointly developed by NTT and Mitsubishi Electric in 2000.*

**2: Public key encryption*

*Proposed by Diffie and Hellman in 1976, it is a cryptosystem where the encryption key and decryption key are different and the encryption key can be published. It is suitable for cryptographic communication in networks available to the general public. Today, it is mainly used to transfer and share the secret key used in the symmetric key encryption system. Representative examples are: the RSA encryption and the "PSEC-KEM," which was developed by NTT.*

**3: Dual pairing vector space*

*The field of cryptography has recently seen wide use of "bilinear groups" on an elliptic curve, in applications such as ID based encryption, fine-grained encryption and others. By using a direct product of bilinear groups, it is possible to construct "dual pairing vector spaces" with a richer algebraic structure than that of a bilinear group itself. Because of this property, rich cryptographic "trapdoors" can now be realized. In 2009, NTT and Mitsubishi Electric introduced the concept of "Dual pairing vector spaces." This new encryption scheme has been constructed by using the vector spaces.*

**PRESS CONTACT**

**Nippon Telegraph and Telephone Corporation**
Planning Dept. Public Relations
NTT Information Sharing Laboratory Group
Tel:+81-422-59-3663
E-mail:islg-koho@lab.ntt.co.jp

**Mitsubishi Electric Corporation**
Public Relations Division
Tel: +81-3-3218-2346
E-mail:prd.gnews@nk.MitsubishiElectric.co.jp