❖*This article has been translated from the original release in Japanese for your convenience*❖

HIME (R) developed by Hitachi adopted as an ISO standard

- Hitachi's public-key encryption scheme becomes an international standard -

Tokyo, 16th March 2006 --- Hitachi, Ltd. (NYSE:HIT / TSE:6501) today announced that that *HIME (R)* (pronounced heim-are), a highly-secure low-power public-key encryption scheme[(*1)] developed by the Systems Development Laboratory of Hitachi, Ltd., has been adopted as an international standard by the International Standardization Organization (ISO) / International Electrotechnical Commission (IEC). *HIME (R)*, short for **Hi**gh performance **M**odular-squaring-based public-key **E**ncryption **(R**evised version**)**, was accepted by vote of the ISO/IEC 18033 "Cryptographic Algorithms" standardization project,[(*2)] and is the third standard proposed by Hitachi to be accepted by ISO. Hitachi's symmetric key stream ciphers,[(*3)] *MUGI* [(*4)] and *MULTI-S01,* [(*5)] were adopted as standards in 2005.

The ubiquitous information society is beginning to provide various forms of convenience to the ordinary user by enabling applications, shopping and other data exchange to be conducted by PC or cellular phones. At the same time, the incidences of Internet crimes and other illegal activity based on information leaks during transmission; unauthorized access to information, falsification of data, spoofing or masquerading as another, etc., are also increasing. To ensure secure and authorized data exchange, the ability to verify identification, preserve confidentiality, authorize access and ensure accuracy, are becoming increasingly indispensable to society. Review of legal frameworks to prevent information leaks and increase information reliability has already begun such as the full enforcement of Personal Information Protection Law (Japan), and discussions on the adoption of a Japanese version of the U.S. Sarbanes-Oxley (SOX) act. Encryption technology has been developed for PCs in order to maintain confidentiality and evidence, and prevent unauthorized view or alteration of information, in response to such needs. To provide even greater security, however, encryption technology operable on small portable information terminals, i.e. with low-power requirements and high-speed encryption, is also needed.

In 1988, Hitachi developed the symmetric-key encryption scheme *MULTI2* as a high-speed encryption scheme for multimedia. This was adopted as a standard encryption scheme for digital satellite broadcasting in Japan, in 1994, by the electric wave council of the Ministry of Posts and Telecommunications (currently, Radio Regulatory Council, Ministry of Internal Affairs and Communications). This was followed by the development of high-speed stream encryption, *MUGI*, and encryption mode, *MULTI-S01*, which were also adopted as electronic government recommendation ciphers in April 2003 by the Japanese government. *MUGI* and *MULTI-S01* were submitted to the JTC1/SC27 technical committee of ISO for standardization, and both were adopted as the first stream cipher standard, ISO/IEC 18033 Part 4, in July 2005. Therefore, Hitachi has the largest number of encryption schemes that were adopted as the ISO International Standard.

Features of the public key encryption scheme *HIME (R)* providing high-speed high-security with low power requirements, are as follows:.

(1) **Encryption method with provable security:** *HIME (R)* has the highest security level defined by the security theory of the public-key encryption scheme. For this reason, even under heavy attack, it would be difficult to extract even a part of the original data (plain text) from the encrypted data (cipher text). Further, through it standardization activities, *HIME (R)* has undergone many security evaluations and verifications, and the validity of the proof of security has been objectively guaranteed.

(2) **High-speed encryption/decryption with low power consumption:** Encryption with *HIME (R)* uses the OAEP method (*6) for message padding, followed by a single modular squaring. (*7) These operations are very concise and efficient.

Moreover, the form of the modulus (composite number) (8) in modular multiplication was devised in order to attain high-speed processing of decryption. Compared with an RSA encryption scheme (using OAEP) for the same key length, *HIME (R)* encryption processing is about ten times faster and decryption processing is about two to three times faster. High-speed performance is directly linked to curbing power consumption, and therefore is operable in ubiquitous or portable information terminals.

In the ubiquitous information society, the amount of data handled by a terminal will continue to increase. On the other hand, even more compact terminals with low power requirements are important technical issues. Hitachi’s stream encryption schemes, *MUGI*, *MULTI-S01* have overcome these issues, and enabled large amounts of data to be securely sent between compact information terminals. *HIME (R)* which joins the ranks of international standards, allows high speed processing with low power requirements, and may be used in a hybrid-type along with *MUGI* and *MULTI-S01* in compact information terminals.

Hitachi will pursue research in low power encryption technology and incorporate the technology in Hitachi and Hitachi Group products to provide a secure ubiquitous information society

More information on Hitachi's encryption schemes, *HIME (R)*, *MUGI*, and *MULTI-S01*, are available at the following website.
http://www.sdl.hitachi.co.jp/crypto/index.html

■ **Notes:**

(*1) Encryption schemes: Encryption schemes are classified into symmetric-key encryption schemes and public key encryption schemes. In the symmetric-key encryption scheme, the data is encrypted using a "key", and encryption key and decryption key are the same. A secure system, therefore, is required between the sender and recipient of encrypted data for the shared key.

The public-key encryption scheme overcomes the issues related to secure key-sharing, as the encryption key and decryption key are different. The recipient provides his/her encryption key via the Internet, the sender encrypts the data with this encryption key and sends the data to the recipient, who then decrypts the data with his/her decryption key. Even if the encryption key were to be made available on the Internet, as long as the decryption key was secure, the data would be secure. The receiver exhibits his encryption key on the Internet, a sender encrypts data using the receiver's encryption key, and the receiver decrypts the encrypted data with his decryption key. However, in public-key encryption scheme, since the encryption key differ from the corresponding decryption key, its encryption and decryption processes are complicated, and has less efficient compared with symmetric-key encryption scheme. Therefore, it is common to use symmetric-key encryption scheme to encrypt bulk data and to use public-key encryption scheme to encrypt the encryption key which was used for bulk data encryption.

(*2) ISO/IEC 18033 Cryptographic Algorithms International Standardization Project: A project of Subcommittee 27 of the Joint Technical Committee 1 of ISO/IEC. The standard document for ISO/IEC 18033 "Cryptographic Algorithms" consists of four parts: Part 1 General; Part 2 Asymmetric ciphers; Part 3 Block ciphers, and Part 4 Stream ciphers. Standardization activity commenced in 1999, and the various cryptographic algorithms submitted in response to a public call for participation were evaluated by a committee of specialists. Part 1 was published on 1st March 2005, followed by Part 3 and 4 on 15th July 2005. The final vote on Part 2 was conducted in February 2006, and is expected to be published within the year.

(*3) Stream ciphers: Symmetric-key encryption schemes to encrypt bulk data using a pseudorandom number generator which generates a random data stream. Since stream ciphers have the advantage of being able to implement the algorithm on a smaller scale compared to block ciphers, i.e. data can be encrypted by the bit, etc., it is adopted in radio-communication ciphers, such as in cellular phones and Bluetooth™. Stream ciphers are also superior to block ciphers in terms of efficiency of encryption/decryption processing, and are therefore expected to be used widely in an advanced information networked society.

(*4) **Mu**lti **Gi**ga (*MUGI*™) cipher is Hitachi's pseudorandom number generator for a stream cipher. In addition to the security, it is possible to realize high-speed processing of bulk data at low cost and light load by implementing *MUGI* on 64-bit processor, 32-bit processor and LSI. For example, in the case of encryption or decryption of image data for a single DVD (4.7GB) using a software of a personal computer (Intel® Pentium® 4.2GHz processor), the processing time (except for disk access time) is about 36 seconds. Moreover, when we use a proprietary chip, the processing time is about 3 seconds and high-speed scrambling are attained in the small-scale circuit (46K gate). *MUGI*™ is a registered trademark of Hitachi, Ltd. in Japan.

(*5) **Multi**media encryption algorithm and **S**tream cipher No. **01** (*MULTI-S01*): is Hitachi's encryption mode of operation for a stream cipher. While conventional stream ciphers preserve only data confidentiality, *MULTI-S01* also preserves data integrity as it is able to detect changes to the data, even on one bit level. *MULTI-S01* may be used in conjunction with *MUGI*™.

(*6) **O**ptimal **A**symmetric **E**ncryption **P**adding (OAEP) method is a data-processing method which increases the security of a public-key encryption scheme by concatenating different data to a message after input, prior to encryption. With *HIME (R)*, the input message is processed firstly by 'OAEP padding' and secondly by a single 'modular squaring'. These operations are extremely brief and efficient.

(*7) Modular squaring : For an integer n, we write the integer remainder after squaring of an integer x divided by n "x2 mod n". Such operation is called modular squaring and the integer n is called the modulus.

(*8) Modulus used for modular multiplication (composite number) : We write the integer remainder of the multiplication x*y divided by n "x*y mod n". Such operation is called modular multiplication and the integer n is called the modulus. In calculation of RSA or HIME (R), n is a composite number, i.e., two or more prime numbers is used for composite number.

■ Trademarks

Bluetooth (TM) is a trademark or registered trademark of Bluetooth-SIG Inc. in the United States of America.

Intel® and Pentium® are trademarks or registered trademarks of Intel Corporation and its subsidiaries, in the United States of America and other countries.

RSA is a registered trademark of RSA Security Inc..

■ About Hitachi, Ltd.

Hitachi, Ltd., (NYSE: HIT), headquartered in Tokyo, Japan, is a leading global electronics company with approximately 347,000 employees worldwide. Fiscal 2004 (ended March 31, 2005) consolidated sales totaled 9,027.0 billion yen ($84.4 billion). 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 website at http://www.hitachi.com

* * *

Information contained in this news release is current as of the date of the press announcement, but may be subject to change without prior notice.

# # #

Information contained in this news release is current as of the date of the press announcement, but may be subject to change without prior notice.