JST, NEC Realize Secure Quantum Key Distribution with Quantitative Assurance

March 6 2007

Japan Science and Technology Agency and NEC Corporation today announced joint development of the world's first quantum key distribution (QKD) system that guarantees security under actual operating environments.

A new formula to estimate information subject to eavesdropping on transmitted keys has been developed and enables measurement of the maximum amount of information that could be leaked on the final cryptographic key distilled from the transmitted key.

Quantum cryptography systems such as the QKD system have been attracting increasing attention worldwide as they guarantee unconditional security against future advances in eavesdropping technology. However, security of the current QKD protocol is dependent on ideal conditions, including the use of a genuine single photon source and/or unlimited computational resources. Therefore, there has been increasing desire to develop a QKD protocol that could guarantee security even without these ideal conditions.

The JST/NEC team has succeeded in constructing a theory to estimate how much information could be leaked on a transmitted key under practical conditions. Based on this, the team developed a QKD system equipped with software for secure key distillation, which erases information subject to eavesdropping from the transmitted key, thereby making the final key immune to eavesdropping.

The new QKD system generates the final key at a rate of 2000 bits/second with an optical fiber transmission of 20km. When the maximum amount of information that could be leaked to an eavesdropper on the final key is 1/128 (whereby an eavesdropper could only guess the code of a 128 bit with a probability of less than 10^{-33}), it would be practically impossible to decipher the code if a message is encrypted with the final key obtained.

This is the first time that a secure key has been successfully generated with quantitative assurance of the maximum amount of information that could be leaked to any potential eavesdropper. This research result is expected to contribute to the realization of a highly secure metropolitan optical communication network that guarantees unconditional security as it proves practical acquisition of a secure key.

This research has been carried out under the JST ERATO-SORST's "Quantum Computation and Information" project (headed by Prof. Hiroshi Imai, University of Tokyo) in cooperation with NEC. The JST team developed the software for implementation in the QKD hardware, which was developed by NEC based on research carried out under the National Institute of Communication Technology's (NICT) project "Research and Development of Quantum Cryptography."

Source: NEC Corporation