Mitsubishi, NEC, Tokyo University Realize Successful Interconnection of Quantum Encryption Networks

12 May 2006

Mitsubishi Electric Corporation, NEC Corp., and Institute of Industrial Science, University of Tokyo have successfully interconnected quantum cryptography systems developed by Mitsubishi Electric and NEC, the first time such an experiment has been successful in Japan. The Institute of Industrial Science at University of Tokyo evaluated the system's security. Quantum cryptography guarantees absolute security, underwritten by the laws of quantum physics.

This achievement was the result of modifying different quantum encryption systems developed by NEC and Mitsubishi Electric, which were researched and developed under a quantum encryption technology project sponsored by the National Institute of Information and Communication (NICT), Research and Development on Quantum Cryptography, from 2001 to 2005.

Security of most modern cryptography is based on computational complexity, and the extraordinary time necessary for cryptanalysis. It has been pointed out that modern cryptography may be threatened by the increasing speed and ability of computers in the future.

To that end, many are suggesting a shift to using quantum encryption. This type of optical cryptography uses quantum-state photons to carry data, and has the advantage of being able to detect eavesdropping. This results in a physically unbreakable, ultimate code. However, since there has been no standardization in the details of the encryption algorithms or the construction of optical devices necessary in communication, it has not been possible to interconnect different systems or build a communication network between different users. We have now developed a technology that can interconnect Mitsubishi Electric and NEC's cryptography systems. This was done on a NICT-developed JGN2 test bed network at the Akihabara access point. Results verify the potential for our system to be the foundation for the next generation of secure networks.

Main Features

1. Confirmed experiment of interconnection between differing quantum encryption systems

We developed a new interface and shared encryption key, and confirmed mutual communication between the differing quantum cryptography systems developed by Mitsubishi Electric and NEC. This is a key technology in standardization of quantum cryptography systems, and will allow for a highly confidential communication network in the future.

2. Verified safety of interconnected quantum cryptography systems

Previously it was necessary to receive objective third party safety certification for the various systems that Mitsubishi Electric and NEC developed separately. Hideki Imai (The Institute of Industrial Science, University of Tokyo, currently Chuo University and National Institute of Advanced Industrial Science and Technology) and his team conducted an observation experiment of information leaked by eavesdropping as well as weaknesses born from implementation, and both verified and confirmed the security of the interconnected quantum cryptography system.

Future Developments

It is hoped that using this technology it will be possible to realize quantum cryptographic networks within 5 years.

The chart below represents an interconnected quantum encryption network made of Mitsubishi Electric (Device A, B) and NEC (Device C, D) quantum encryption systems. In the past, each system was constructed independently, and communication was done in a closed system. A way of relaying information was necessary in order to network the different systems. With this experiment, we were able to successfully interconnect a quantum encryption network without any affects on the different systems by developing a new relay method. The security of the network underwent a theoretical observation study at Tokyo University's Institute of Industrial Science.

Source: NEC

Process for a shared key in a quantum encryption network:

First set and apply an appropriate key to the various communications between devices A,B,C and D. Devices A and B will share the key K1, and devices C and D will share the key K2. Next, the key that should eventually be shared by Devices A and D should be produced at the center, and should be sent to Devices A and D passing through Devices B and C. Key K1 encrypted Key K3 will be sent to Device A from Device B, and key K2 encrypted key K3 will be sent to Device D from Device C. Devices A and D will decipher those and get key K3.

Using the above procedure, devices A and D can, based on quantum encryption theory, safely share key K3.Using key K3 as an encryption key, Device A and Device D can safely share data.