October 14, 2010

Press Release

Inauguration of the Tokyo QKD Network

~ Ultimate secure communication at the world's highest bit rate on a metropolitan fiber network in Tokyo ~

The National Institute of Information and Communications Technology (NICT, President Dr. Hideo Miyahara) in cooperation with its commissioned research partners NEC, Mitsubishi Electric and NTT has started with the operation of the world's fastest quantum key distribution (QKD)*[1] network using part of NICT's open fiber testbed network JGN2plus. The Tokyo QKD Network boasts key generation rates at around 100kbps allowing perfectly secure one-time pad encryption*[2] of video data in real time. In this field network operation, Toshiba Research Europe Ltd and other European organizations have also participated in an effort to promote standardization of the interconnection technology between Japanese and overseas QKD systems..

[Background]

Quantum key distribution enables two remote parties to share instantly a random secret key and at the same time provides a means of detecting any attempt of interception in the transmission. When using such a shared symmetric key in combination with one-time pad encryption, the encrypted message will be perfectly secure against any current or future form of unauthorized decipherment and tampering. So far, quantum network projects funded by the United States Department of Defense and the European Union were able to demonstrate secure voice transmission over a few tens of kilometers. NICT has been promoting research and development of QKD technologies since 2001 and started in October of this year with the operation of its "Tokyo QKD Network"(Fig.1) to demonstrate secure video transmission in the metropolitan area of Tokyo over 45 km using NICT's open testbed network JGN2plus.

[Operation Goals]

The goals of the Tokyo QKD Network are threefold: Firstly, it shall serve as a testbed with respect to various types of eavesdropping attacks and in this way promote secure operation as well as establish a security evaluation standard for QKD systems. Secondly, it shall provide a means for absolutely secure video transmission in a stress-free manner based on the latest QKD technologies. And thirdly, it shall function as a cooperation platform between Japanese and overseas research organizations to facilitate standardization of the network interface that is needed to interconnect different QKD systems developed around the world.

[Future Plans]

After sufficient tests of long-term operation stability in the Tokyo QKD Network, QKD systems are expected to be deployed first in networks of government agencies and critical infrastructures where communication security is imperative to protect state secrets and the well-being of the public.Further improvements in device compactness will then expand the application area of QKD to financial, medical and business organizations.

< Technical Contact >
Information Technology R&D Center
Mitsubishi Electric Corporation
https://global.mitsubishielectric.com/ssl/contact/company/form.html

< Media Contact >
Public Relations Division
Mitsubishi Electric Corporation
Tel: +81-3-3218-2333
E-mail：prd.gnews@nk.MitsubishiElectric.co.jp

< Terminology and Interpretations >

***1 Quantum key distribution**
Quantum key distribution (QKD) was proposed in the 1980s for the safe delivery of one-time pad. In QKD, each bit of key information is carried by a single photon, which is the elementary particle of light and cannot be divided further. Any attempt of measuring or copying a photon inevitably induces some change in the photon's state due to Heisenberg's uncertainty principle and the no cloning theorem of quantum mechanics. The ability to detect any eavesdropping attempt on the optical signal in the transmission channel constitutes the most remarkable feature of QKD.

***2 One-time pad encryption**
Among all the methods of encryption ever devised, only one-time pad encryption has been mathematically proven to be absolutely secure if used correctly. The key, consisting of a truly random sequence of bits or characters, should be as long as the message to be encrypted and used only once. The message is encrypted by a modular addition with the key, and decrypted by a modular subtraction. In case of binary messages and keys, modular addition and subtraction are equivalent to XOR operations.

< Supplementary Information >

Tokyo QKD Network
The Tokyo QKD Network, whose layout is depicted in Fig. 1, makes use of Japan's Gigabit Network dubbed JGN2plus. JGN2plus represents an open testbed network that provides a platform for new R&D activities and leading-edge experiments in the field of network technologies. Currently, over 100 research projects utilize the services of JGN2plus. The Tokyo QKD Network is configured as a star network connecting the JGN2plus operation center in Otemachi with NICT's Headquarter in Koganei as well as the Information Technology Center of the University of Tokyo in Hongo and NICT's research facility in Hakusan.

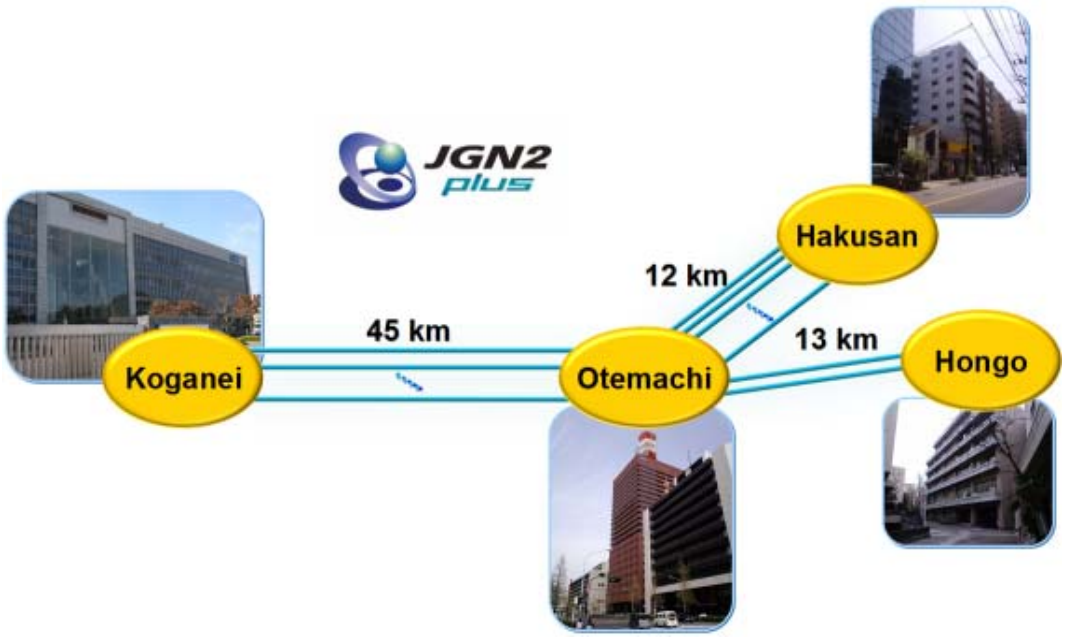

Fig.1 Network layout of the Tokyo QKD Network.

As shown in Fig. 2, the Tokyo QKD Network is structured into three layers: the quantum layer, the key management (KM) layer and the communication layer. In the quantum layer, the QKD devices generate quantum keys via a point-to-point connection. The key data is then sent to the KM layer comprising several KM agents and a central KM server. The KM agents collect and store the key data from the QKD devices. The KM server monitors the amount of key data in each agent and supervises the overall key distribution in the network. Finally, in the communication layer, secure communications is ensured by using the distributed keys for encryption and decryption of binary data produced by various applications such as a video conferencing.

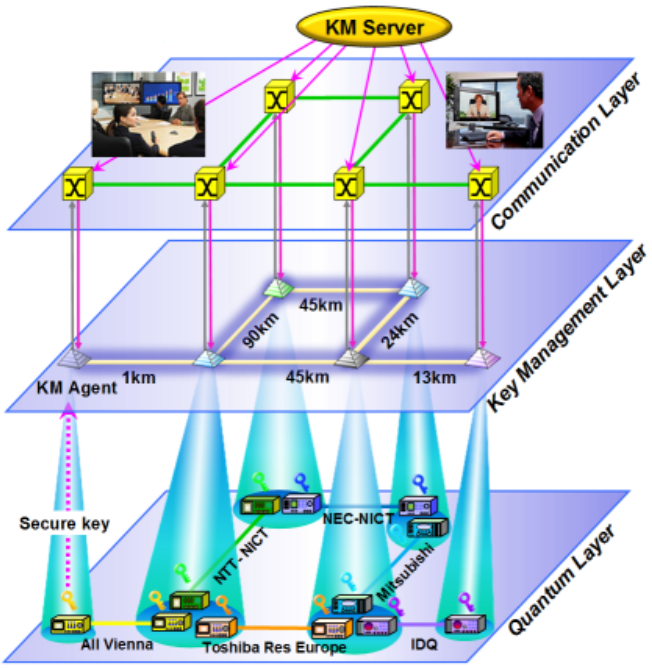

Fig 2 Network layer structure of the Tokyo QKD Network.