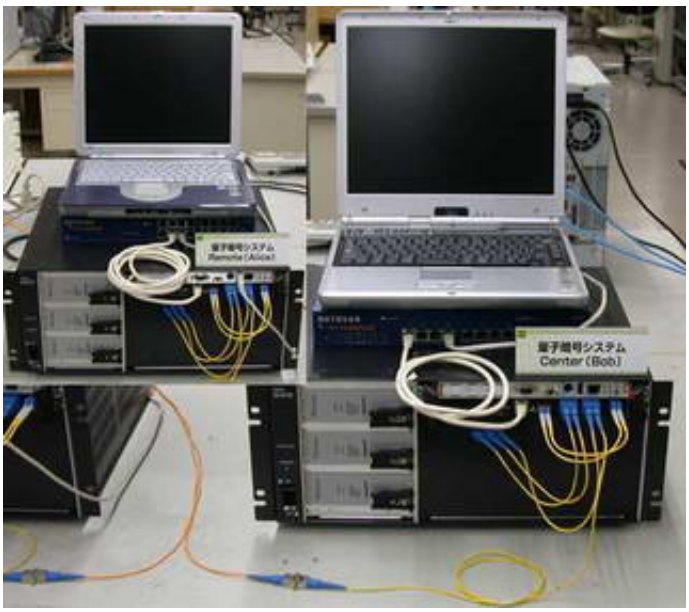
# NEC Succeeds in World's Fastest Continuous Quantum Cryptography Key Generation over Fortnight Period

May 31 2005




***Realized on network employing commercial optical fiber***

NEC Corporation, National Institute of Information and Communications Technology, POWEREDCOM, Inc., and Japan Science and Technology Agency have jointly succeeded in realizing fortnight-long, continuous quantum cryptography final-key (note 1) generation at an average rate of 13 kbps over a 16-km-long commercial

optical network.

*Image of verification experiment of quantum cryptography system*

*These results have been achieved by NEC under the NICT project "Research and Development on Quantum Cryptographic Technology" through employment of a low-noise photon receiver, in addition to an alternative-shift phase modulation method (note 2), which was developed by NEC and the Imai Quantum Computation Information Project (Exploratory Research for Advanced Technology ("ERATO"), JST.)*

*The main features of this research are as follows:*

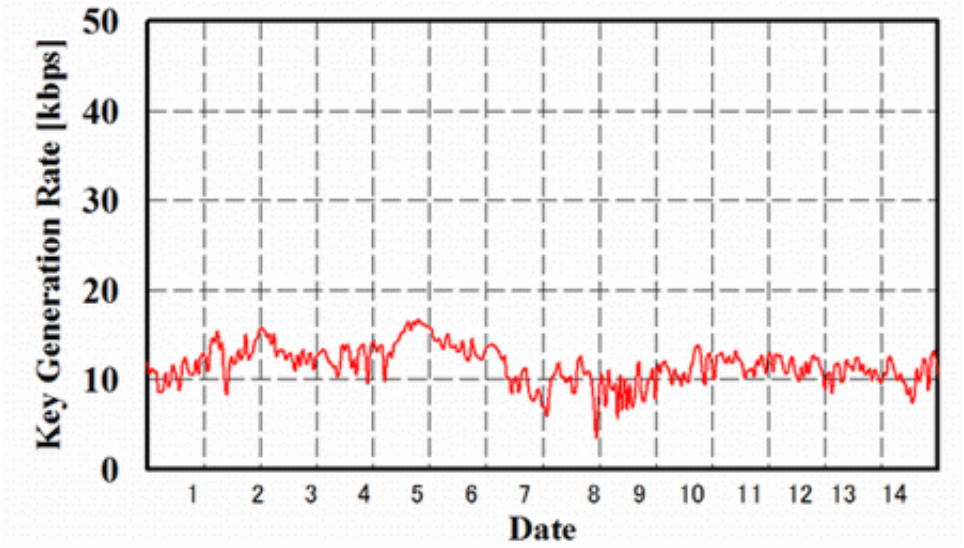
*1. This experiment is carried out under general environment conditions by using optical fiber commercially settled on the outside and quantum cryptosystems in an office environment.*

*2. Continuous generation of the final-key, which is used in encryption and decryption and ensures unconditional safety, from the raw-key (note 1.) over a 14 day period is enabled in parallel with single photon transmission, realizing the world's longest continuous final-key generation period.*

*3. Over 16.3-km-long access optical fiber, the average quantum error rate is 7.5 % and the average final-key generation rate is 13.0 kbps. Previous quantum cryptography systems have not been able to achieve long-time continuous key generation due to fiber delay variations, reflection and scattering in fiber. In order to solve these problems, the following novel technologies have been newly developed and their validity has been confirmed through continuous key generation experiments employing POWERDCOM's optical fiber.*

*(a) Wavelength division multiplexing ("WDM") technologies enable transmission of synchronizing signals and quantum signals in the same*

*optical fiber. Crosstalk (note 3) from synchronizing signals is suppressed by filters. Use of an automatic phase-alignment mechanism realizes compensation of group velocity dispersion (note 4) between the synchronizing signals and quantum signals. Consequently, stable phase modulation and photon detection is achieved despite fiber delay being varied.*
*(b) Burst mode (note 5), using NEC's proprietary alternative-shift phase modulation method, achieves avoidance of the scattering of light in fiber and reflection light from the connection point, leading to stable key generation.*




*Final-key generation rate transition*

*Achieved through a newly developed quantum cryptography system adopting a novel method, this continuous key generation enables secure network communication supported by the principles of quantum mechanical physics. As this system continuously generates final-keys under general conditions, it enables quantum cryptography transmissions in*

*commercial optical networks, and is expected to contribute to the realization of an optical fiber network system requiring advanced safety levels to prevent against code-breaking in the future.*

*Present cryptography systems do not guarantee unconditional safety as their security is based on the limited calculation abilities of present computers, however, quantum cryptography provides unconditionally secure network communication and safety, even when these capabilities are infinite. This is because quantum cryptography is not reliant on calculation capability but on the principle of physics. Therefore, its development is now attracting considerable attention on a global scale.*

*NEC's quantum cryptography research is accelerating with each new achievement putting us ahead of the competition, thus allowing us to contribute to overall development in the field of quantum cryptography.*

## *Notes:*

*(1) Final-key / Raw-key: The final-key is generated from the raw-key by eliminating bits that have possibilities of errors and eavesdropping. The raw-key is a set of random bits generated by single-photon transmission and detection. The final-key is essential for transmitting coded information.*
*(2) Alternative-shift phase modulation method: This is an NEC proprietary method used in place of the conventional Faraday-Mirror. It uses polarization rotation and loop back in the fiber-loop and phase-modulation.*
*(3) Crosstalk: In ordinary power signals and single-photon signal WDM, spontaneous emission from the ordinary power signals of the light source and nonlinear effects, for example Spontaneous Raman Scattering, influence single-photon signal as crosstalk. This crosstalk is neglected in ordinary optical communication systems; however, it degrades the performance in quantum cryptography systems.*

*(4) Group velocity dispersion: Optical signal speed in fiber depends on its wavelength due to wavelength dispersion in fiber. Therefore, transmission delay difference between different wavelength signals depends on fiber length.*
*(5) Burst mode: Optical signals are launched intermittently enabling signal and noise to be isolated.*