DAMOP07-2007-000428

Abstract for an Invited Paper
for the DAMOP07 Meeting of
the American Physical Society

Stable operation of a Secure QKD system in the real-world setting[1]

AKIHISA TOMITA, JST

Quantum Key Distribution (QKD) now steps forward from the proof of principle to the validation of the practical feasibility. Nevertheless, the QKD technology should respond to the challenges from the real-world such as stable operation against the fluctuating environment, and security proof under the practical setting. We report our recent progress on stable operation of a QKD system, and key generation with security assurance. A QKD system should robust to temperature fluctuation in a common office environment. We developed a loop-mirror, a substitution of a Faraday mirror, to allow easy compensation for the temperature dependence of the device. Phase locking technique was also employed to synchronize the system clock to the quantum signals. This technique is indispensable for the transmission system based on the installed fiber cables, which stretch and shrink due to the temperature change. The security proof of QKD, however, has assumed the ideal conditions, such as the use of a genuine single photon source and/or unlimited computational resources. It has been highly desirable to give an assurance of security for practical systems, where the ideal conditions are no longer satisfied. We have constructed a theory to estimate the leakage information on the transmitted key under the practically attainable conditions, and have developed a QKD system equipped with software for secure key distillation. The QKD system generates the final key at the rate of 2000 bps after 20 km fiber transmission. Eavesdropper's information on the final key is guaranteed to be less than 2^{-7} per bit. This is the first successful generation of the secure key with quantitative assurance of the upper bound of the leakage information. It will put forth the realization of highly secure metropolitan optical communication network against any types of eavesdropping.

[1]This work was partly supported by NiCT.