Genome analysis data transmission using quantum cryptography

Akira Murakami[1], Ririka Takahashi[1], Yoshimichi Tanizawa[1], Hideaki Sato[1], Tomoaki Chiba[2], Masao Nagasaki[2]

[1]Network System Laboratory, Corporate Research and Development Center, Toshiba Corporation
[2]Department of Integrative Genomics, Tohoku Medical Megabank Organization, Tohoku University
E-mail: akira4.murakami @toshiba.co.jp

***Abstract*—This paper reports the first field trial of genome analysis data transmission encrypted with quantum keys generated by a Quantum Key Distribution (QKD) system in Japan. We transmitted 31.6 GB of genome analysis data. Other results were an averaged quantum bit error rate (QBER) of 4.19%, an average secure key rate of 290 kbps, 537 days of operation and 1.47 TB of generated quantum keys.**

Introduction—It is important to transmit confidential and personal information securely because the importance of cyber security are recognized recently. Especially, personal health records such as electronic health record and genomic data are quintessential personal information that needs to be made permanently secure. Quantum cryptographic communication is unique highly secure communication because its security is based on quantum physical principles. Toshiba started a field trial of cryptographic communication using quantum keys generated by a Quantum Key Distribution (QKD) for genome analysis data with Tohoku University Tohoku Medical Megabank Organization (ToMMo) in Sendai, Japan [1]. We transmitted genome analysis data of Japonica Array (Human Whole Genome Genotyping Array) with the quantum cryptographic communication between Toshiba Life Science Analysis Center and ToMMo.

Method—Schematic diagram of the quantum cryptographic communication system is shown in Figure 1. Quantum keys are generated by the QKD system which consists of a transmitter, a receiver, a detector, control servers and two standard optical fibers of 7 km length (one is used for quantum channel with loss of 2.3 dB, the other is for classical channel). The transmitter, receiver and detector are designed by Toshiba Research Europe Ltd., Cambridge Research Laboratory [2] and manufactured in Japan. The protocol of the QKD system is efficient decoy BB84 protocol with phase encoding [3]. The control servers have key distillation functions, namely sifting, error correction based on Cascade algorithm [4] and privacy amplification [5], and a function delivering quantum keys to application servers with REST-based API [6]. The application servers transmit genome analysis data bi-directionally with one time pad or AES. The alarm function and the auto-tuning function of timing alignment are implemented in order to recover the QKD system quickly.

The quantum cryptographic communication system is built and operated according to several ministry's guidelines and policies of personal information and medical information protection in order to handle genome analysis data.

Results—We transmitted 31.6 GB of genome analysis data with one time pad encryption. Other results were an average QBER of 4.19%, an average secure key rate of 290 kbps, 537 days of operation, rate of operation of 93.3%, and 1.47 TB of generated quantum keys (shown in Table 1). We kept enough quantum keys to transmit genome analysis data.

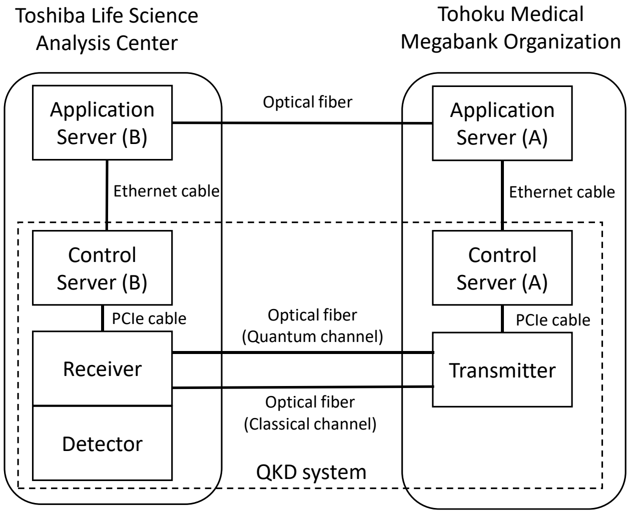

Figure 1. Schematic diagram of the quantum cryptographic communication system

Table 1. Operation results of the quantum cryptographic communication system with two optical fibers, each of which 7 km in length (quantum channel loss is 2.3 dB)

Parameter	Value
Average QBER (standard deviation)	4.19% (0.59%)
Average secure key rate (standard deviation)	290 kbps (138 kbps)
Amount of generated quantum keys	1.47 TB
Operating time	537 days
Rate of operation	93.3%
Amount of transmitted genome analysis data (one time pad)	31.6 GB

Conclusion—We achieved the first field trial of the quantum cryptographic communication for genome analysis data in Japan. We transmitted 31.6GB of genome analysis data and operated the quantum cryptographic communication system for 537 days according to ministry's guidelines and policies. As a next, we plan to introduce faster QKD system in order to transmit full genome analysis data.

References

[1] http://www.tqccs.com/cl/tech/qccs/en/case/index.html
[2] A. R. Dixon, et al, Appl. Phys. Lett. **96**, 161102 (2010)
[3] M. Lucamarini et al., Opt. Expr. **21**, 24550-24565 (2013).
[4] G. Brassard, vol. 765 of Lecture Notes in Computer Science, pp. 410–423, Springer Berlin / Heidelberg, 1994
[5] C. H. Bennett et al, SIAM Journal on Computing, Vol. 17, no. 2, April 1988, pp.210-229
[6] http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm