Field Test of QKD Secured Video Conference System for Clinical Use

Ririka Takahashi1, Yoshimichi Tanizawa1, Alexander R. Dixon1, Akira Murakami1, Kazuaki Doi1, Mamiko Kujiraoka1, Hideaki Sato1, Muneaki Shimada3, Inaho Danjoh2, Fumiki Katsuoka2,4, Yasunobu Okamura2,4, Fuji Nagami2,4

1Corporate Research and Development Center, Toshiba Corporation, 2Tohoku Medical Megabank Organization, Tohoku University, 3Tohoku University Hospital, Tohoku University, 4Advanced Research Center for Innovations in Next-Generation Medicine, Tohoku University

E-mail: ririka.takahashi@toshiba.co.jp

Introduction
Medical histories is considered as special care-required personal information that should be protected. Genomic data is one example of data related to medical histories. Sequencers analyze genomic data and the results are used to determine the optimal targeted therapy. An expert panel of medical experts
• examines the genomic analysis reports to determine the expected effect of the therapeutic drug,
• discusses information on patient cases to determine diagnosis and treatment,
• can be convened remotely as a video conference.

We introduce a system for video conferencing using QKD and show the result of the field test demonstration by medical experts between Tohoku University Tohoku Medical Megabank Organization (ToMMo) and Tohoku University Hospital (TUH) in Sendai, Japan.

Methods
QKD transmitter/receiver pair
• is linked by optical fibers.
• provides the QKD keys for each site.

QKD-VPN (Virtual Private Network) servers
• encrypt/decrypt with one-time pad using the QKD keys.
• provide the QKD encrypted link as a QKD-VPN [1].
• have a packet routing function to forward packets to the encrypted link.

Video conference application
• One video server
• is installed on a server at ToMMo.
• One or more video clients
• are deployed at each site.
• Local client uses a unencrypted link.
• Remote client uses an encrypted link via QKD-VPN servers.

Contents discussed by the expert panel
• are based on the analysis result reports on genomic data.
• are not only video and audio but also the analytical reports.
• should be protected by high security.

Results
Demonstration overview
• TUH explained a simulated document of a patient case by using an application screen sharing function.
• ToMMo provided the simulated genomic analysis report generated by sequencers of that patient case.
• the contents were transmitted via an encrypted link.
• The simulated conference was held for 39 minutes.

Size of the key used
• Total sizes / average rates
  - TUH (client) to ToMMo (server): 270 MB (avg. 923 kb/s)
  - ToMMo (server) to TUH (client): 457 MB (avg. 1.56 Mb/s)
• Our QKD system [2] having a 10 Mb/s secure key rate is sufficient to provide the QKD keys for point-to-point expert panel in real time.

Conclusion
We applied QKD to a video conference system in a field environment. Our system provided the environment for medical experts to discuss the contents remotely with high security with information theoretic security by one-time pad encryption/decryption. The results showed that our high-speed QKD system has a sufficient secure key rate to support a point-to-point video conference by providing the QKD keys in real time.

Acknowledgment
A part of this work was supported by Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), “Photonics and Quantum Technology for Society 5.0” (Funding agency: QST).

Reference

© 2020 Toshiba Corporation