【Grant-in-Aid for Scientific Research (S)】

Broad Section C

Title of Project : Information communication technology ensuring the long term security over a century

Akihisa Tomita
(Hokkaido University, Graduate School of Information Science and Technology, Professor)

Research Project Number : 18H05237 Researcher Number : 60501434
Keyword : Information theory, network, cryptography

【Purpose and Background of the Research】

Recently, our society is getting to rely on the electronic data that should be kept secret for a long period. For example, genome information, should be stored securely for more than human lifetime, *i.e.*, a hundred years. However, modern cryptographic protocols have been periodically updated to keep security. The present cryptographic technology can hardly guarantee the secrecy over a century.

This project therefore is aimed to develop an information theoretically secure storage, the security of which will never compromised by any technological progress. We combine secret sharing and quantum cryptography to achieve the information theoretical security.

【Research Methods】

Figure 1 depicts the network scheme developed in this project. Secret-sharing servers provide network functions such as multi-user management, synchronization and secret computing. Short distance high speed quantum key distribution (QKD) links provide secure communication between a server and a user and between servers. Even distant users can access the data securely through the user authentication with a password shared with a long distance (loss tolerant) QKD link.

The project contains four subjects: network construction and control, long distance QKD, high speed QKD, and theories on security certification and efficient key generation. The first half of the project will devote to examine candidates to achieve the project goal. Then, in the second half, we develop the devices and software to integrate the secure storage network.

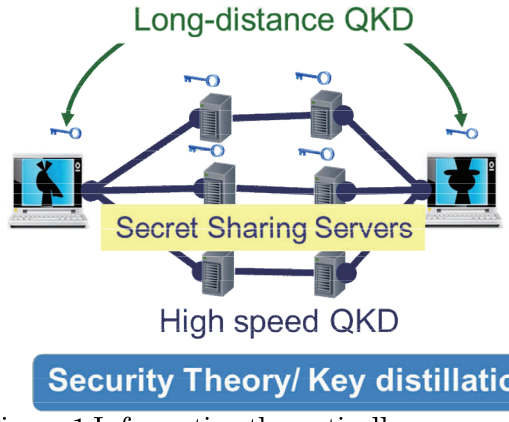

Figure 1 Information theoretically secure storage network

【Expected Research Achievements and Scientific Significance】

The project will realize an information communication and storage network secure against any possible attacks for over a century. This goal will be achieved by our newly developing technology combining the information theoretical secure modern cryptography and QKD. We will establish the technological frame work to construct practically useful combination.

The technological elements developed in the project, such as the optical pulses synchronization and precise control of the phase and frequency, will also advance the coherent optical communication.

【Publications Relevant to the Project】

K. Nakata, A. Tomita, M. Fujiwara, K. Yoshino, A. Tajima, A. Okamoto, and K. Ogawa," Intensity fluctuation of a gain-switched semiconductor laser for quantum key distribution system," Optics Express, **25**, 622-634 (2017)

M. Fujiwara, A. Waseda, R. Nojima, S. Moriai, O. Wakaha, and M. Sasaki, "Unbreakable distributed storage with quantum key distribution network and password authenticated secret sharing," Scientific Reports, 6: 29988 (2016).

【Term of Project】 FY2018-2022

【Budget Allocation】 148,200 Thousand Yen

【Homepage Address and Other Contact Information】

http://www.eng.hokudai.ac.jp/labo/hikari/index.htm