CC-03-03

Information theoretically secure data utilization using “Quantum Secure Cloud”

Mikio Fujiwara

NICT

Abstract

We have been developing a system that implements a secret sharing protocol on a QKD network to enable secure transmission, storage, and secondary use of data. We have developed an XOR based high-speed secret sharing and high-speed OTP encryption/decryption system for distributed data backup. The throughputs of these systems are 700 Mbps and over 2 Gbps, respectively. We named the system Quantum Secure Cloud. We named the system “Quantum Secure Cloud” and have been conducting POC in various fields. This system not only transmits and stores genome analysis data, which require long-term confidentiality, but is also expanding its functions as a platform that enables secure utilization of data. For the secondary use of secure data, we have developed a system in the Quantum Secure Cloud that uses a secure computation system based on the assumption of a trusted server, where data is restored only during computation and encrypted during input/output. The system also has a filtering function to prevent unnecessary leakage of personal information. To our knowledge, this is the first in the world to analyze whole genome data in an information-theoretically secure manner. In this presentation, we will explain the details of the system.