CC-06-03

A case: cybersecurity of financial institutions in quantum computer Era

Yuto Takahashi

The Japan Research Institute, Limited

Abstract

The rapid growth of quantum computer technology has led to research into its applications across various fields. In the financial sector, it has already been proposed for option trading and arbitrage, and its future applications are highly expected.
However, the immense computational power of quantum computers poses a significant threat to traditional encryption algorithms. For instance, the authentication and encryption mechanisms used in Internet banking and cash cards could become vulnerable. To ensure the provision of safe and stable financial services in this new era, we need encryption methods that can withstand quantum computing.
Although we eagerly anticipate the advancements in quantum computing, we must also prepare countermeasures. Currently, Post-Quantum Cryptography and Quantum Key Distribution are emerging as potential solutions. Quantum Key Distribution is promising due to its theoretical security, but it faces the challenge of requiring specialized equipment.
To implement more flexible countermeasures, it is important to consider Post-Quantum Cryptography that can be implemented as software. Global academic research on Post-Quantum Cryptography is advancing, and the National Institute of Standards and Technology is leading a project to standardize these algorithms.
We have been closely monitoring global trends, evaluating to these algorithms, and deepening our understanding of Post-Quantum Cryptography. We would like to share an example of our efforts to ensure secure communication in the era of quantum computing from a banking corporation's perspective.