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

Foundations of Secure Distributed Quantum Computing on Medium-Scale Quantum Computers

Principal Investigator	Nagoya University, Graduate School of Mathematics, Professor LE GALL François　　Researcher Number : 50584299
Project Information	Project Number : 24H00071　　Project Period (FY) : 2024-2028 Keywords : quantum distributed computing, secure protocols, complexity

Purpose and Background of the Research

●Outline of the Research

As a result of dramatic advances in the development of quantum devices, medium-scale quantum computers are expected to soon become available. In this research, we will establish the foundations of secure distributed quantum computing on medium-scale quantum computers: by designing quantum-secure protocols that can be implemented on medium-scale quantum computers and by rigorously establishing their quantum advantage, we will pioneer the development of quantum algorithms realizable in the next 10 to 15 years.

●Background

Quantum computing was first proposed in the early 1980s. Recently significant progress has been made towards realizing quantum computers, with major IT companies and startups already building small-scale quantum computers. The size of quantum computers (measured by the number of qubits) is increasing according to a "quantum version of Moore's law".

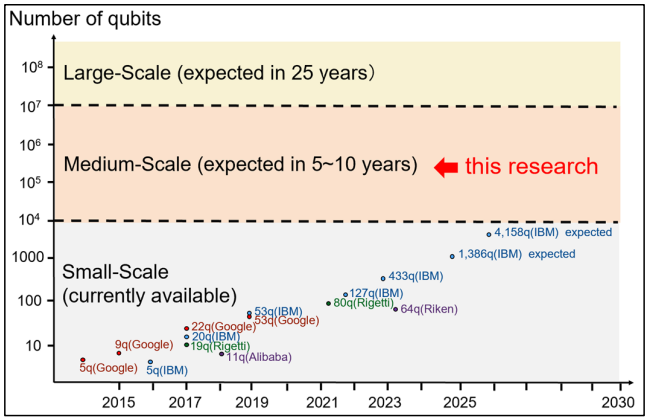

Figure 1. Progress in constructing quantum computers

It is expected that medium-scale quantum computers with 10,000 to 1 million qubits will be built in the next 5 to 10 years, and available for use in the next 10 to 15 years. To be ahead of the world both industrially and academically, it is necessary to explore their potential and start developing ways to exploit their computational power.

Scale	Nb of qubits	Availability	Noise tolerance	Usage	Quantum advantage
Large-Scale	10 millions ~ 100 millions	In 25 years	◯	Advantage with one quantum computer	Established (e.g., Shor algorithm)
Medium-Scale (this research)	10,000 ~ 1 million	In 5~10 years	◯	Multiple quantum computers needed	Not yet established
Small-Scale	100 ~ 1000	Currently available	X	Limited applications due to noise	Experimentally established (2019), then refuted (2021)

Figure 2. Comparison of small, medium, and large-scale quantum computers

●Goal of the Research

The purpose of this research is to investigate the computational power and applications of medium-scale quantum computers. Because their computational resources (such as the number of qubits) are limited, it is necessary to combine them with classical computers, or connect multiple medium-scale quantum computers together (distributed quantum computing). By establishing the foundations of distributed quantum computing on medium-scale quantum computers, we aim to develop fast quantum algorithms with guaranteed advantage over classical computers.

●Ideas Leading to this Research

In our predecessor project (Scientific Research (A), 21H04879, PI: Takeshi Koshiba), we focused on designing protocols and algorithms for small-scale and large-scale quantum computers. As the development of quantum computers accelerates, it has become an urgent issue to investigate the computational capabilities and applications of medium-scale quantum computers, which led to this research.

Expected Research Achievements

●Quantum Advantage for Medium-Scale Quantum Computers

We will rigorously show quantum advantage for medium-scale quantum computers (either one medium-scale quantum computer assisted by classical computers, or several medium-scale quantum computers connected as a network). To achieve this goal, we will first examine the results of existing research on quantum superiority and explore the possibility of achieving superiority even with 10,000 to 1 million qubits. Next, we will provide new examples of quantum advantage using techniques from computational complexity theory.

●Secure Protocols for Medium-Scale Quantum Computers

We will develop methods for designing quantum secure protocols (first with classical communication, and then with quantum communication) for networks composed of medium-scale quantum computers. We will focus on systems in which a single quantum computer is assisted by classical computers, and distributed systems in which multiple quantum computers are connected.

● Development of Fast Algorithms for Medium-Scale Quantum Computers

We will construct quantum algorithms that can be implemented on medium-scale quantum computers and whose quantum advantage is theoretically guaranteed. We will focus on applications where exponential speed-up is known (e.g., quantum system simulation, quantum machine learning), and work on settings where the data is distributed.

Figure 3. Two quantum computers assisted by a classical computer

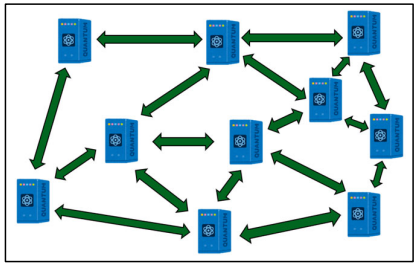

Figure 4. Quantum distributed computing

Homepage Address, etc.	http://www.francoislegall.com/