【基盤研究（S）】

中規模量子コンピュータによるセキュアな分散型量子計算の基盤創出

研究代表者	名古屋大学・多元数理科学研究科・教授 ルガル　フランソワ（るがる　ふらんそわ）　研究者番号：50584299
研究課題情報	課題番号：24H00071　研究期間：2024年度～2028年度 キーワード：分散型量子計算、セキュア量子プロトコル、計算量理論、量子多体複雑性

なぜこの研究を行おうと思ったのか（研究の背景・目的）

●研究の全体像

近年の量子デバイスの開発における劇的な進歩の結果として、中規模量子コンピュータは次の10～15年で利用可能になると期待される。計算資源（量子ビット数など）が限られているため、量子コンピュータを通常のコンピュータで補助するシステム、あるいは複数台の量子コンピュータを接続した分散型システムの導入が不可欠となるが、その構築方法と活用方法はほとんど未開拓である。本研究では、中規模量子コンピュータの潜在的能力を最大限に活かすため、中規模量子コンピュータによる分散型量子計算の基盤を創出する。中規模量子コンピュータで実現可能な、量子的にセキュアなプロトコルを設計し、量子優位性（すなわち、量子コンピュータがスーパーコンピュータよりも速く問題を解決できること）を厳密に裏付けることにより、中規模量子コンピュータの活用方法を開拓し、10～15年後で利用可能な量子アルゴリズムの開発を先駆する。

●研究の背景

量子計算は、1980年代に初めて提案された量子力学の原理に基づく計算パラダイムである。初期の結果では、量子コンピュータが特定の計算問題（例：素因数分解）を、従来のコンピュータとは比較にならない効率の良さで解くことが示された。過去10年間で量子コンピュータの実現に向けて大きな進歩が達成され、主要なIT企業やスタートアップ企業はすでに小規模な量子コンピュータを構築しており、量子ビットの数で測定される量子コンピュータのサイズは、「量子版ムーアの法則」に従って増加している。

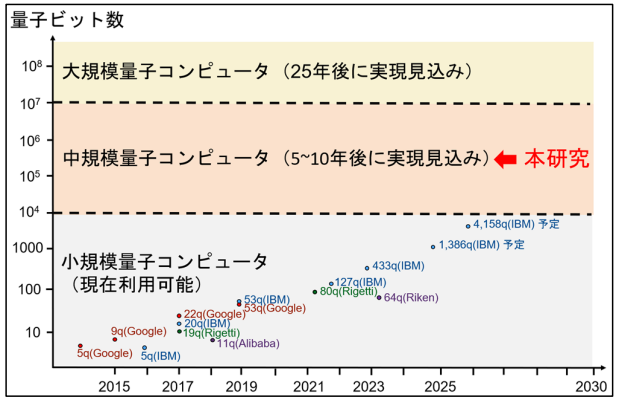

図1　量子コンピュータ開発の加速

次の10年～15年では、1万～100万量子ビット程度の中規模量子コンピュータが利用可能となる見込みである。産業的にも学術的にも世界に先駆けるためには、大規模量子コンピュータの実現を待たず、中規模量子コンピュータの潜在能力を究明し、活用方法を開拓する必要がある。

量子コンピュータの規模	量子ビット数	実現可能な時期（見込み）	ノイズ耐性	利用状況	量子計算の優位性
大規模	1000万~1億 程度	25年後	○	1台であっても古典計算に対し優位	理論的優位性が確立（素因数分解アルゴリズム等）
中規模（本研究）	1万~100万 程度	5~10年後に実現 10~15年後に利用	○	古典計算の補助・複数台接続が必要	未確立
小規模	100~1000 程度	現在利用可能	X	ノイズの影響により応用が限定的	実験的優位性 (2019) が報告されるも後に否定 (2021, 2023)

図2　小･中･大規模量子コンピュータの比較

●研究の目的

本研究の目的は、次の10年～15年で利用可能となる中規模量子コンピュータの計算能力の究明と応用の開拓である。計算資源（量子ビット数など）が限られているため、古典計算による補助や複数台の中規模量子コンピュータを接続すること（分散型量子計算）が必要となり、従来の量子計算システムと異なり、学術的課題が山積している。これらの課題を解決し、中規模量子コンピュータの活用に指向した分散型量子計算の基盤を創出することにより、優位性が理論的に裏付けられている高速量子アルゴリズムの開発を目指す。

●研究実績に基づく着想

前身課題「量子情報化社会に向けた量子計算基盤の構築」（基盤研究(A)、21H04879、研究代表者：小柴健史）において、現在の小規模量子コンピュータおよび2050年頃の大規模量子コンピュータを中心に、量子プロトコルの設計方法と量子アルゴリズムの開発を部分的に推進していた。量子コンピュータの開発の加速により、中規模量子コンピュータの計算能力の究明と応用の開拓が喫緊な課題となり、本研究の着想に至った。

この研究によって何をどこまで明らかにしようとしているのか

●中規模量子コンピュータによる量子優位性の理論研究

量子ビット数などが限られている量子コンピュータ（1台、あるいは接続された数台）の量子優位性を理論的に裏付ける。方法としては、まず量子優位性の既存研究の成果を精査し、1万～100万量子ビットでも優位性が達成できる可能性を探究する。次に、計算量理論の手法を用いて、新しい量子優位性の例を与える。

具体的な目標：10万量子ビット規模の量子コンピュータ２～10台程度で、量子優位性を厳密に証明

●中規模量子コンピュータによるセキュアなプロトコルの設計

計算資源が限られている量子コンピュータで構成されているネットワークのための量子的にセキュアなプロトコル（古典通信・量子通信の各状況を想定）の設計方法を与える。特に量子コンピュータ1台を通常のコンピュータで補助するシステム、あるいは複数台の量子コンピュータを接続した分散型システムに着目する。

具体的な目標：10万量子ビット規模の量子コンピュータ2～10台における量子的にセキュアなプロトコル（例：量子公開鍵暗号、量子秘匿計算）を設計

●中規模量子コンピュータのための高速量子アルゴリズム開発

上記のアプローチで創出された分散型量子計算の基盤を活かし、中規模量子コンピュータで実現可能な、量子優位性が理論的に裏付けられている量子アルゴリズムを開発する。指数関数的なスピードアップが知られている量子コンピュータの応用分野（例：量子系のシミュレーション、量子機械学習）を中心に量子アルゴリズムを開発する。データが分散されている設定にも取り組む。

具体的な目標１：10万量子ビット規模の量子コンピュータ2～3台程度で実現可能な、100量子ビット程度の量子系のシミュレーションのための量子アルゴリズムの開発

具体的な目標２：10万量子ビット規模の量子コンピュータ10台程度で実現可能な、分散されたデータのための量子機械学習アルゴリズム（例：特異値分解の計算）の開発

図3　量子コンピュータ（2台）を通常のコンピュータで補助するシステム

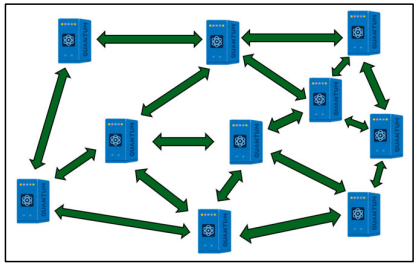

図4　量子コンピュータ（１０台）による分散型量子計算

ホームページ等	http://www.francoislegall.com/