（ 続紙 １ ）

京都大学	博士（　　工　　学）	氏名	佐野　裕一
論文題目	Extension of Blind Quantum Computation (ブラインド量子計算の拡張)		

（論文内容の要旨）

量子論に従うコンピュータである量子コンピュータ（量子計算機）の概念が１９８０年代に提案された。その後、Shor のアルゴリズム（素因数分解の多項式時間解法）や、Grover の探索アルゴリズムなどの発見により従来のコンピュータ（古典計算機）よりも本質的に速い計算ができる可能性が示され、現在では実装に向けた研究も盛んに行われている。一方、将来有用な量子コンピュータが実装された場合においても、量子コンピュータを各ユーザーが所有するということはコスト面などから現実的ではない。むしろ、ユーザーは量子コンピュータを持つ企業に量子計算を委託するという現在のクラウドコンピュータのような用いられ方をすると考えられているが、その場合、問題となるのがユーザーの委託する計算に関わる情報の秘匿性である。本論文の主結果は、この秘匿性を保つ委託計算手法であるブラインド量子計算について、既存の手法をセキュリティ等の面において改良したプロトコルの提案と、セキュリティの理論的限界に関する考察からなっている。

第一章は本論文の導入にあたり、量子コンピュータと量子暗号の歴史を概観し、本研究の動機の説明を行った後、本論文の主結果について簡単に説明している。

第二章では、本論文を読み進めるにあたり必要な基礎概念が詳述されている。まず、量子情報理論において必須である状態、物理量、時間発展など量子論の一般的枠組みを紹介した後、量子コンピュータで基本単位となる量子ビットについて視覚的表現であるブロッホ球を用いて説明している。その後、委託計算において大きな役割を果たす量子ワンタイムパッドとコピー不可能性定理について触れ、量子計算の一般論について解説を行っている。最後に、本論文の先行研究となるブラインド量子計算の手法である Childs のプロトコル、BFK プロトコル、MF プロトコルの紹介を行い、また既存のマルチパーティプロトコルについても説明を行っている。

第三章では単一の量子サーバーを使ったブラインド量子計算プロトコルの拡張を行っている。１つのサーバーを利用するブラインド量子計算の場合、ユーザーは量子系を操作できる一定の能力が必要であると考えられている。先行研究では量子メモリを持たない（具体的には「量子状態の準備」あるいは「量子測定」のいずれかができる）ユーザーが実行できるプロトコルが測定型量子計算を用いて提案されているが、より基本的な計算モデルである回路型量子計算を用いたプロトコルはこれまで知られていなかった。これに対し、本章ではゲートテレポーテーションを利用した新しい暗号化法を開発することで、量子メモリを持たないユーザーが実行できる回路型量子計算を用いたプロトコルを提案している。さらに、提案されたプロトコルにおいてサーバーに対して要求される能力は先行研究で要求された能力より真に弱いものとなっており、これは提案プロトコルの長所となっている。

京都大学	博士（　　工　　学）	氏名	佐野　裕一

第四章では複数の量子サーバーを用いたブラインド量子計算プロトコルの拡張を行っている。先行研究によれば２つのサーバーを用いるマルチサーバープロトコルではユーザーは古典的な能力のみで計算を委託できることが知られている。ただし、そのプロトコルにはサーバーどうしは計算についての通信が禁止されるという強い制約が存在した。この制約は、計算が終わった後もサーバーどうしの通信を禁じており、プロトコルを現実的でないものにしている。本章ではこの制限を緩和することを目指し、N サーバー中 N-1 サーバーが計算終了後に通信を行っても安全なブラインド量子計算プロトコルを提案している。具体的には既存の 2 サーバーを使ったプロトコルを任意サーバー数 N で実行できるように拡張した後、新たな暗号化手法を適用することによりサーバー中 N-1 サーバーが計算についての情報を取得しても、計算の情報を取得できないようにしている。

第五章では複数の量子サーバーを用いたブラインド量子計算プロトコルの理論的限界を論じている。第四章では複数サーバーを用いたプロトコルの通信に関する制限を緩和したが、さらに計算中や計算後に全てのサーバーが通信可能でも利用できるプロトコルが存在すれば、ユーザーにとってはより利用しやすいプロトコルだといえる。本章では、この全てのサーバーが通信可能なプロトコルが存在することと、古典計算能力のみを持つユーザーが実行できる単一サーバープロトコルが存在することが等価であることを示している。後者の古典計算能力のみを持つユーザーが実行できる単一サーバープロトコルは存在しない可能性が高いとされているため、この等価性より全てのサーバーが通信可能なプロトコルも存在しない可能性が高いことが帰結できる。

第六章は全体のまとめと今後の展望が記されている。

（続紙 ２ ）

氏 名	佐 野　裕 一

（論文審査の結果の要旨）

近年、量子計算機の研究は理論・実験ともに盛んにおこなわれている。将来、有用な量子計算機が実装された場合においても、ユーザーは量子計算機を持つ企業に量子計算を委託するという用いられ方をすると考えられているが、その際、ユーザーの委託する計算に関わる情報の秘匿性が問題となる。本論文の主結果は、この秘匿性を保つ委託計算手法であるブラインド量子計算について、既存の手法をセキュリティ等の面において改良したプロトコルの提案と、セキュリティの理論的限界に関する考察からなっている。その主な内容と成果は以下の通りである。

（１）シングルサーバー型のブラインド量子計算について新しいプロトコルを提案している。本論文で扱っているプロトコルは、測定型量子計算に基づく既存のものとは異なり、より基本的な回路型量子計算を用いている。このプロトコルでは、ユーザーは長期間量子状態を保持できる量子メモリを保有する必要はなく、またサーバー側に要求される能力も既存のものより小さいものとなっている。

（2）マルチサーバー型のブラインド量子計算プロトコルの拡張を行っている。既存のプロトコルには、サーバー同士が通信をしてしまうとユーザーの委託した計算内容がサーバーに漏れてしまうという欠点が存在した。本論文では、この制限を緩和し、N サーバー中、N-1 サーバーが計算終了後に通信を行ってもセキュリティが保たれるようなブラインド量子計算プロトコルを提案している。

（3）マルチサーバー型のブラインド量子計算プロトコルの通信に関する制限について理論的限界を論じている。通信について制限のないマルチサーバー型ブライド量子計算プロトコルの存在が、ユーザーが量子状態を扱うことができない場合の単一サーバー型ブラインド量子計算プロトコルの存在と等価であることを示している。その結果として、前者のプロトコルが存在しない可能性が高いことを帰結している。

以上のように本論文はブラインド量子計算について、種々の理論的研究を行ったものである。各章ともに、発想が独創的であり、また結果は将来量子計算機が実装されたときに有用性の高いものとなっている。よって本論文は博士（工学）の学位論文として価値あるものと認める。また、令和６年１月１９日に論文内容とそれに関する試問を行い、申請者が博士後期課程学位取得基準を満たしていることを確認し、合格と認めた。