論文審査の結果の要旨および担当者

報告番号	※　　第　　号

氏　　名　SONG Seunghoan

論　文　題　目

Information-Theoretic Aspects of Quantum Private Information Retrieval

(量子プライベート情報検索の情報理論的側面)

論文審査担当者

主　査　名古屋大学大学院多元数理科学研究科　教授　博士（情報科学）
ガリグ　ジャック

委　員　名古屋大学大学院多元数理科学研究科　准教授　博士(情報理工学)
ルガル　フランソワ

委　員　名古屋大学大学院多元数理科学研究科　教授　博士（理学）
永　尾　太　郎

協　力　委　員　名古屋大学大学院情報学研究科　教授　Ph.D.
ブシェーミ　フランチェスコ

論 文 審 査 の 結 果 の 要 旨

情報検索がインターネットで頻繁に行われる中、情報のやりとりの第三者からの秘匿性を始めとして、様々な秘匿性質が求められている。その中で、プライベート情報検索 (PIR) は第三者からの秘匿性ではなく、当事者 (検索を要請するユーザと情報を提供するサーバ) が相手の情報をみだりに得られなくすることを目的としている。インターネットの普及を起爆剤に、1990 年代から盛んに研究され、複数のサーバを同時に利用することで、各サーバがどの情報が求められたかを独自に判断できないようなプロトコルが発明され、様々な条件での理論的な性質も研究された。2000 年代から、量子情報理論の原理が解明されるとともに、量子情報理論に基づいたプライベート情報検索 (量子 PIR) も研究され、特に量子情報理論を使わない古典的なプライベート情報検索に対する優位性が興味の対象になっている。

本論文は、量子 PIR に対する情報理論的な側面 (すなわち、検索データのサイズが十分大きい設定における議論) を初めて追究するものである。

PIR のためのプロトコルの基本的なアイデアは、それぞれのサーバに検索したい情報ではなく、それを含む (あるいは意図的に含まない) ランダムな項目の集合を求め、それらの項目から計算された情報を送ってもらい、最終的にそれぞれのサーバが送った情報を元に欲しかった情報を再構築することである。各サーバとやりとりする情報から欲しい情報が特定されなければ、ユーザの秘匿性が守られている。また、サーバが送る情報の計算を巧妙に定めることで、ユーザが本来求めていた情報以外の情報を得られないことをサーバ秘匿性という。さらに、t 個のサーバ (全体のサーバ数を n として $t < n$) が結託しても、ユーザの情報が漏れないという t 結託秘匿性も考えられる。本論文では、それぞれの性質を保証するプロトコルが提案され、その情報理論的な効率 (f 個ある m ビットの検索情報を一つ得るために実際に何ビットがやりとりされるか) も解析されている。多くの場合では従来のもの (古典的な PIR プロトコルあるいは既に知られている量子 PIR プロトコル) より効率のよいものが提案されている。なお、本論文で提案される各量子 PIR プロトコルではサーバとユーザがある量子もつれを共有していると仮定するが、量子的な通信路の使用がサーバの返答のみに限定されている。ユーザからの照会には通常の通信路が使われる。

本論文は序文と結論を含む 7 章からなる。第 2 章では、量子計算および量子情報理論の基礎についての解説があり、次にその後に必要となる、様々な量子情報理論の概念（量子相対 Renyi エントロピーなど）および不等式が導入される。

第 3 章では量子 PIR の定義と評価が行われる。まず量子 PIR 容量の定義が与えられる。サーバ数 n やデータ数 f を固定し、データサイズ m を任意に動かした際の、全ての量子 PIR プロトコルに対する量子 PIR レートの上限が量子 PIR 容量である。続いて、漏れるユーザ情報を 0 にしても、量子 PIR 容量が 1 であるという、本論文の最も主要な結果が証明される。 そのために、完全なユーザ秘匿性を持ち、誤りがなく、容量を達成する巧妙な量子 PIR プロトコルが与えられている。高く評価できる貢献である。なお、従来の情報通信技術では実現できない優れた点が 2 つあげられる。1 つ目は、サーバ数 n が有限のとき、量子 PIR 容量は常に古典 PIR 容量より大きいことである。2 つ目は、提案した量子 PIR プロトコルは古典 PIR プロトコルと違い、必要な情報以外がユーザに漏れない（すなわち、ユーザの秘匿性だけでなく、サーバの秘匿性も保証される）ことである。

第 4 章では複数回のやりとりを使った量子 PIR が検討されるが、結果的には 1 回のや

論 文 審 査 の 結 果 の 要 旨

りとりより量子 PIR 容量が増えないという証明に至る。第 3 章と併せて、林正人氏と共著で IEEE Transactions on Information Theory に掲載予定である。

第 5 章はサーバが結託する場合の量子 PIR 容量を対象とする。第 4 章までは、全てのサーバが互いに通信しない仮定のもとに議論されたが、第 5 章はより現実的な設定として、ユーザが知らない t 個のサーバの間の通信を許し、 他のサーバは互いに通信しない設定に着目する。そして、量子計算のスタビライザー形式に基づく巧妙な量子プロトコルを構築することにより、量子 PIR 容量を厳密に求めることに成功する。特に、結託するサーバ数が $n/2$ 以下の場合、量子 PIR 容量が 1 であることが証明される。この結果は量子計算に対する相当な寄与になっており、高く評価できる。

第 6 章では結託するサーバが $(n-1)$ 個の場合の解析を行う。この章の最も主要な結果は、量子 PIR 容量 が $2/n$ であることの証明である。古典 PIR 容量はデータ数 f が無限大のときに $1/n$ となるため、量子 PIR は古典 PIR の 2 倍以上の容量を持つことが明らかになる。なお、この章で構成される量子 PIR プロトコルでもサーバ秘匿性が保証される。

SONG 氏は 2020 年 12 月 4 日に行われた公開学位審査セミナーにおいて、背景を含めた主結果の詳細な発表を行った。古典的な場合との比較も効果的に使い、プロトコルの仕組みと証明方法が理解できる明快な発表であった。委員会の質問にも適切に回答し、研究内容に関して十分な知識・理解と見識を持っていることが伺え、外部審査員からも高評価を得た。

上記の評価に鑑み、本学位審査委員会は、申請者には博士 (数理学) の学位が授与される資格があるものと判断する。