研 究 報 告 書

量子鍵を用いた次世代量子暗号プロトコル

（研究領域:「量子と情報」）

研究者氏名: 村尾 美緒

（研究期間: 2003 年 10 月 1 日～ 2007 年 3 月 31 日）

研究報告書

1．研究課題名　量子鍵を用いた次世代量子暗号プロトコル

2．氏名　村尾　美緒

3．研究のねらい

量子鍵配布に代表される従来の量子暗号のプロトコルは、量子状態を用いることで古典情報の安全な通信を可能とするものであった。一方、量子情報科学技術が進めば、量子情報そのものの安全な通信のために「量子情報のための暗号」が必要となる。そこで、量子情報を主体とした次世代の量子情報処理への手がかりとして、量子力学特有の性質である量子もつれの性質を解明し、その性質を量子情報のための暗号鍵（量子鍵）へと応用した、次世代の量子暗号プロトコルを探索する。

本研究は暗号プロトコルの提案という量子情報処理の応用研究的な側面を持つと共に、量子もつれを中心とした、量子力学的な非局所性と情報処理との関連の解明という基礎研究的な側面も持つ。基礎研究と応用研究との相互的発展によって、量子情報を用いることで何ができ何はできないのか、量子情報の優位性を保つためには何が必要なのか、という理論的基盤の構築に貢献を目指すものである。

4．研究成果①

4．1　基礎研究の成果

遠隔操作量子情報抽出と遠隔操作量子情報破壊

多量子ビット量子もつれを用いて2量子ビットに符号化した1量子ビットの量子情報が、LOCCのみで量子情報の抽出が可能であるための必要十分条件を、作用素代数的な方法を用いて求めた。この条件を用いて、どちらか一方には LOCC のみで量子情報を抽出することができるが他方には抽出できない、というような量子情報の二者間での非対称な共有方法（遠隔操作量子情報集約）を見出すことに成功した。

量子情報の共有には、量子もつれを持つ純粋状態を符号化の基底として用いており、どのような性質の量子もつれ状態を基底として用いるか、ということが、量子状態の共有の性質を決める。純粋状態の場合、2者間の量子もつれ自体は2者間に対称的に存在することが知られており、この類推から、量子情報の共有についての非対称性を分析した研究はこれまでにほとんどなかったため、本研究における非対称性の発見は重要な意義を持つものと考える。

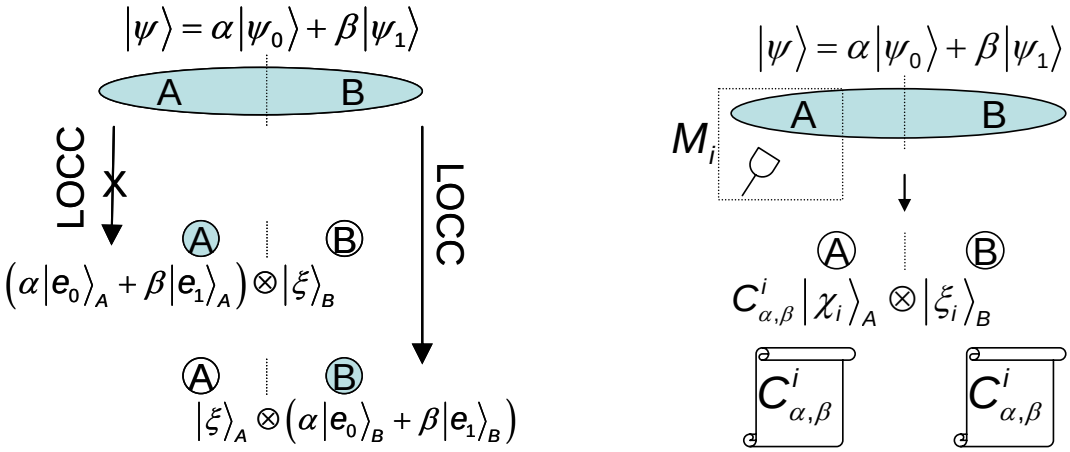
更に、遠隔操作量子情報抽出とは逆のタスクとも考えられる、遠隔操作量子情報破壊が可能であるための必要十分条件を求めた。これは、2者間で共有する量子情報を、どちらか一方の局所的操作のみによって、測定後の状態には量子情報が存在しないように破壊するタスクである。その結果、量子もつれを持つ状態を符号化基底として用いる場合、遠隔操作量子情報破壊が可能であるためには、量子情報を2者間で対称的に共有しなければならないこと示した。

非対称遠隔量子もつれ操作

純粋状態を用いて量子情報を2者間で共有する場合には、遠隔操作量子情報破壊の条件の制約により、遠隔操作量子情報抽出と遠隔操作量子情報破壊のどちらも非対称にすることは不可能となる。そこで、混合状態を用いた量子情報の共有を行うことによって、局所的操作の選択に応じて、非対称な遠隔操作量子情報抽出と遠隔操作量子情報破壊を選ぶことができる方法を見出した。

さらに、LOCCによる量子情報の変換と、拡張された系におけるLOCCの下での量子もつれの変換を結びつけることによって、A と B と C の3者間で共有する量子もつれから、B が局所操作を選び実行し、C が古典通信による回復量子操作を行なうことで、A と C との間で遠隔操作によっ

て量子もつれを抽出したり、量子もつれを破壊したりすることが可能である条件を得た。そして、混合状態の作用により、A と B の間では、量子もつれを抽出することが不可能であるが、A と C との間では量子もつれを抽出することが可能であるような、非対称遠隔量子もつれ操作を考案した。



遠隔操作量子情報集約（左）と遠隔量子情報破壊(右)の概念図

無限準位系に特有な量子もつれの性質の発見

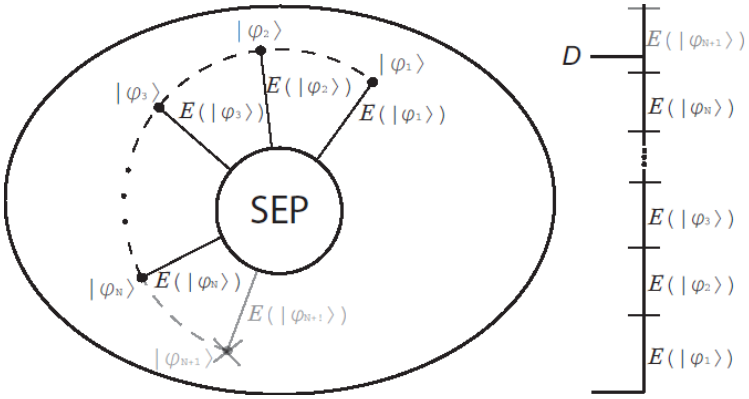
従来、エネルギーが有限で有限情報のやりとりしか含まないような物理的に可能な条件下においては、無限準位系においても有限準位系の量子もつれと性質には大きな違いがないと考えられていた。我々は、有限・無限の次元性の違いによる量子物理の基盤的な量子もつれ構造（全順序・半順序構造の違い）に相違が生じることを示した。更に、無限準位系においては、物理的に可能な状況下においても相互に変換不可能な状態が無限に存在することを示した。この予想外の性質は、数学的性質の違いによる量子物理の基盤的な構造の違いを示し、量子情報処理への応用も期待されるものである。

LOCC 状態識別と量子もつれ量の関係

量子計算や量子通信は量子情報の演算や操作を扱うものであるが、情報処理の最終段階（出力過程）においては、我々が扱うことのできる古典情報に変換する必要がある。出力過程は、量子情報から古典情報への変換過程となっており、量子状態に符号化された古典情報をいかにうまく引き出すか、すなわち、異なる古典情報が符号化された量子状態をいかに識別するか、という問題が非常に重要となる。

そこで、LOCC 変換よりひとつ大きな量子操作の集合である Separable 変換に着目し、状態の量子もつれの量のみで定まる識別性の限界を求めた。そして、一般的な多粒子状態の空間において、大局的量子もつれ頑強性、相対エントロピーを用いた量子もつれ測度や幾何学的量子もつれ測度などの幾何学的に定義される量子もつれの量が、LOCC で識別可能な状態の数に上限を与えることを証明した（図）。また、N 粒子の W 状態が N 粒子の GHZ 状態よりも LOCC 状態識別の視点では非局所性が高いことを示した。

この研究成果は、これまでにほとんど知られていなかった、操作的な観点からの多粒子量子もつれの定量化を与えるものであり、量子暗号等への応用が期待される。一方、量子もつれの距離的測度の大きい状態を探索することで、量子秘密共有などの量子暗号プロトコルへの応用研究へと発展する可能性がある。



LOCC 識別可能な状態と量子もつれの距離的測度および状態の次元との関係（量子もつれの距離的測度の和が次元数以下でないと LOCC 識別が不可能となる。）

量子もつれ頑強性と低階数ノイズ

量子もつれ頑強性(Robustness of entanglement)は、ノイズに対する量子状態の量子もつれ保持性を表す測度である。ノイズが量子状態に及ぼす効果は、その量子状態を表す密度演算子に別の密度行列を混合することでモデル化できる。混合する密度行列の階数は、ノイズによって引き起こされる可能性のあるユニタリ変換の数を示すものである。低階数の密度行列で表されるノイズにによる影響を考察することによって、多者間量子もつれの一つの指標である、シュミット数から1を引いた階数を持つようなノイズは、量子状態の多者間量子もつれを完全には破壊することができないことを示した。

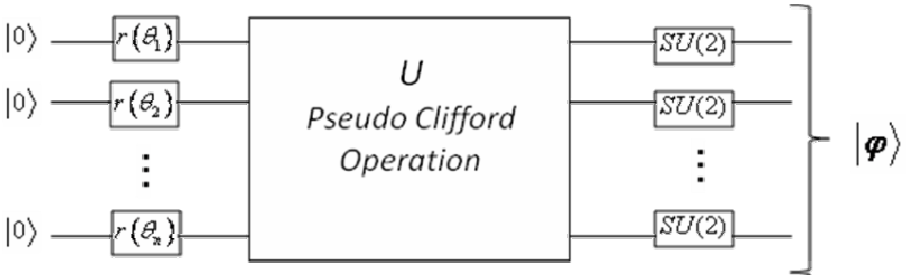
熱平衡状態における多者間量子もつれ

ここ数年、量子情報科学のみならず、物理の様々な分野で量子もつれの存在とその役割を理解するための多大なる努力がなされてきた。例えば、凝縮系物理の臨界現象や高エネルギー物理での対称性の破れ、ホーキング放射などにも量子もつれの存在が関連づけられてきており、マクロな系でも量子もつれが絶対零度以外で存在し得ることが証明された。

そこで我々は、マクロな系における多者間量子もつれの性質をよりよく理解するために、有限温度の熱平衡状態における多者間量子もつれ保持性を、量子もつれの距離的測度を用いて解析した。その結果、量子もつれの距離的測度である量子もつれ頑強性の大きな基底状態を持つ熱平衡状態において、量子もつれの存在を保証する臨界温度を導出することに成功した。マクロスコピック熱平衡状態における量子もつれの見積りは、ノイズの影響を受ける現実的な系における量子情報処理の研究に欠かせないものであり、量子もつれ頑強性による解析は、広い分野へ応用可能であると考える。

局所演算による量子状態への古典情報符号化

量子もつれを持つ量子状態に対して、その量子状態の次元と同じ数の古典情報を、局所演算のみによって符号化する方法および、そのような符号化が可能である量子もつれを持つ量子状態の条件を求めた。その結果、クリッフォード群に属する演算によってゼロ状態（量子ビットがすべてゼロからなる積状態）から作られる量子もつれをもつ状態は、局所演算による量子状態への古典情報符号化が可能であることを示した。また、クリッフォード群には属さないが、局所演算による量子状態への古典情報符号化が可能であるような擬クリッフォード集合の存在を提示し、W状態などの非クリッフォード群状態での局所演算による古典情報符号化の方法を示した。（図）



局所量子演算のみで古典情報符号化が可能となる状態$|\varphi\rangle$を作る量子回路。$r(\theta_i)$はx軸に関する回転、Uは多量子ビットの擬クリッフォード集合に属するユニタリ演算、$SU(2)$は1量子ビットの任意のユニタリ演算である。

4．2　応用研究

量子情報のための量子鍵プロトコル・遠隔量子情報スイッチプロトコル

2 者間非量子情報分配の研究出られた成果を用いて、二者のうち一方が持つ量子情報は、他方への量子情報復元のための鍵（量子鍵）としかなり得ない、というような量子情報の「不公平」分配のプロトコルを提案した。

更に、純粋状態のみならず混合状態の量子鍵を考察することにより、さらに安全性を高めた量子鍵プロトコルである遠隔量子情報スイッチプロトコルを提案した。このプロトコルは、送信者・受信者・情報通信の是認者(approver)の三者からなるプロトコルであり、この当事者以外の信頼できる第三者の存在を不要としながらも、情報通信の是認者が承認した時のみ送信者から受信者への量子通信が可能となる一方、是認者が承認しない場合には、古典的限界を超えて量子情報を送信者から受信者に送ることが不可能となるもので、是認者が量子情報の伝達を「遠隔スイッチ」で制御することができるプロトコルとなっている。

量子錠プロトコル

量子情報における暗号的応用分野では、量子状態を用いて古典情報である乱数共有を行うBB84 プロトコルなどの量子鍵配送が成功している。我々は、量子情報そのものを用いた暗号プロトコルの可能性を模索し、群論的アプローチによる一方向性量子計算の暗号的応用の一例として、認証者を通じて証明者と確認者の間で認証を行うための量子錠プロトコルを提案した。このプロトコルでは、全行程を通してクローン禁止原理を持つ量子情報を用いることで、複製による情報漏洩の可能性が非常に低くなっていることが特色である。

プロトコルは、証明者に配布される量子状態である量子鍵、確認者が持つ量子状態である量子確認鍵、認証者によって作成される最大エンタングル状態である量子錠からなる。そして、証明者が提出した量子鍵が量子確認鍵と同一の状態であることが確認者によって確認されれば、認証が成功することになる。ここで、量子鍵は認証者の行うパウリ群の演算によって暗号化されており、同じパウリ群の演算が組み込まれた量子錠によってのみ復号化することができる。一方、量子錠は、確認者の行うクリッフォード群の演算によって暗号化されており、認証者の知識のみでは、量子鍵と量子確認鍵を一致させることは不可能となっている。

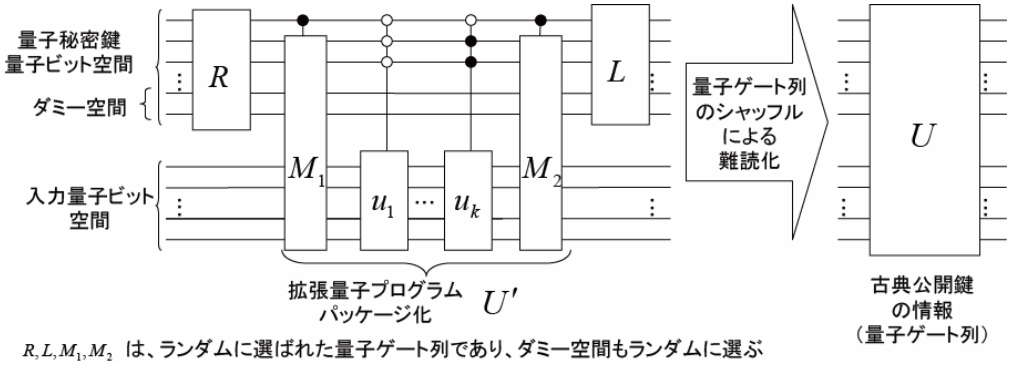
計算量的秘匿量子演算

公開通信路を通じて古典情報を安全に送るために現在広く用いられている公開鍵暗号は、古典計算機による計算量によって安全が保障されているものであり、量子計算機が実現されると安全ではなくなる。そこで、量子系を用いて秘密鍵の共有を行う量子鍵分配が提案された。量子鍵分配では、認証が正しく行われていれば無条件安全性が保障される。しかしながら、現在用いられている認証プロトコルは公開鍵暗号と同様の性質を用いており、量子計算機が実現されると安全性が保障されない。量子計算機が実現しても安全性が保障されるような量子系を用いた公

開鍵暗号プロトコルについては、河内らによる先駆的な研究(A. Kawachi et al, Proc. EUROCRYPT 2005, LNCS 3494, 268, 2005)があるが、量子状態を公開鍵として用いているため、認証プロトコルとして用いるには困難があった。一方、量子計算機が実現された場合には、量子情報の保全だけではなく、量子計算を行うためのソースプログラム(量子ゲート列)の暗号化も必要となる。このような課題に対処する方法も知られていなかった。

そこで、量子計算機が実現されても計算量的に安全性が保障される可能性が高い量子暗号要素技術(暗号プリミティブ)を考察するために、秘匿量子計算の概念を提唱した。秘匿量子演算は、ユニタリ演算を複数組み込み、さらに暗号化を行った拡張量子プログラムの量子ゲート列に難読化(obfuscation)を施すことによって得られた量子ゲート列を古典情報からなる公開鍵とし、量子状態からなる量子秘密鍵と組み合わせることによって、量子秘密鍵が指定するユニタリ演算で表される量子計算を任意の入力量子情報に対して実行するものである。

量子計算の実行者は、難読化の効果により、量子計算機を用いても古典公開鍵の情報から多項式時間でユニタリ演算を特定することができず、また、量子秘密鍵の量子状態の特定も、多項式時間の量子計算によっては不可能となる。この秘匿量子計算を用いると、量子秘密鍵を用いずに多項式時間で量子計算を実行することが可能であるのは、古典公開鍵の作成者だけとなる。そのため、量子計算機が実現されても計算量的に安全性が保障される可能性が高い量子暗号要素技術(暗号プリミティブ)となり得る。

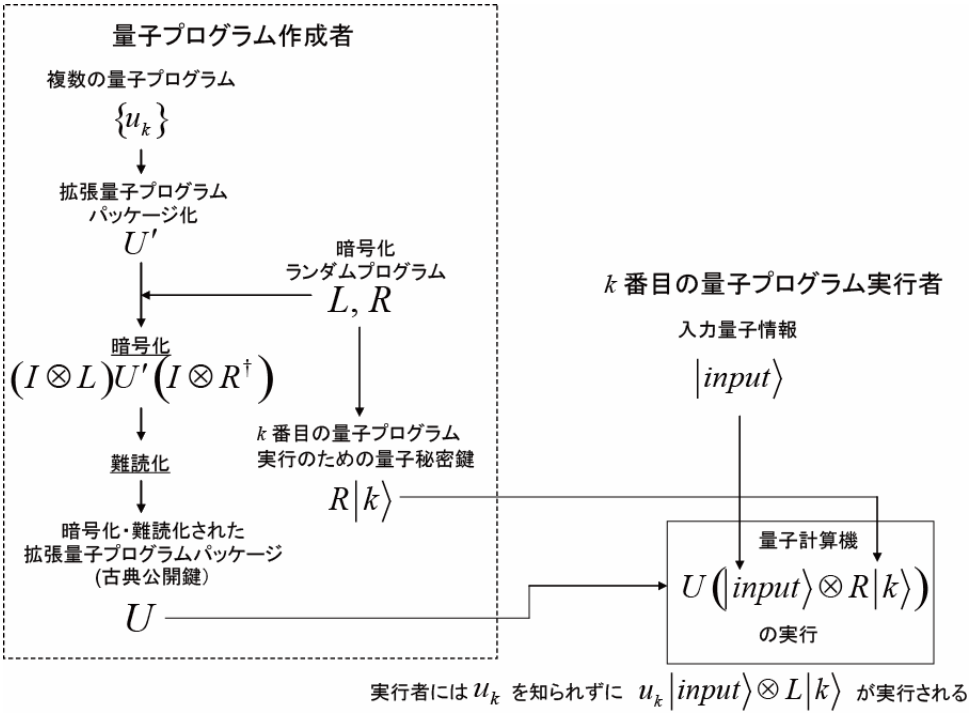


古典公開鍵の作成方法

計算量的秘匿量子演算を利用した量子公開鍵暗号システム

計算量的秘匿量子演算は、暗号要素技術(暗号プリミティブ)として、3種類の量子公開鍵暗号システム(量子計算機が実現してもなお計算量的に安全が保障される認証プロトコル、量子情報を安全に通信するための暗号システム、量子計算のソースプログラム暗号化方法)を構築することが可能となることを示した。これらの量子公開鍵暗号システムの特徴は、量子秘密鍵が再利用可能であり、量子メモリーが完全であるならば、秘密量子鍵配送のための量子通信を繰り返す必要がないという点である。また、量子プログラムから拡張量子プログラムを作る際に、複数の量子プログラムをまとめた量子プログラムパッケージを作成することも可能となる。このため、A と B の2者間のみならず、A と C、A と D など A に対して多者間で秘匿量子計算を行うことができる。

更に、本研究は量子プログラム(量子ゲート列)の難読化(obfuscation)という新たな研究課題を提起するものであり、効率よく難読化を行うためのアルゴリズムなど、今後の量子情報の研究発展の新たな方向性を提供する。



多者間での計算量的秘匿量子計算

6. 今後の展開

本研究の開始後に、量子もつれを資源として、LOCC のみを用いて量子計算を行なう、測定ベース量子計算についての研究が世界的に進んだ。そこで、本研究で得られた量子情報符号化とそれに必要な量子もつれ資源との関連をさらに拡張し、複数の量子情報が量子計算によってヒルベルト空間内を複雑にからみ合う状況を量子情報の流れとして定義することによって解析し、量子情報処理の優位性の根源を知る手がかりを得たいと考えている。また、本研究を通じて得られた量子もつれ頑強性の性質をさらに解析することで、量子計算のみならず物性物理の問題に関しても、量子もつれの解析を通して量子効果の根源を明らかにするための道具立ての整備を行う予定である。一方、計算量的秘匿量子演算の実用化可能性を探るためには、量子プログラムの難読化のアルゴリズム開発やその評価の研究をさらに進める必要があり、情報理論、計算機科学、そして物理的考察の3つの側面から研究を継続する。

7. 研究成果リスト

（1）論文（原著論文）発表

1. Owari Masaki, Keiji Matsumoto and Mio Murao, Entanglement convertibility for infinite dimensional pure bipartite states, Phys. Rev. A 70, 050301 (2004)
2. M. Hayashi, D. Markham, M. Murao, M. Owari and S. Virmani, Bounds on Multipartite Entangled Orthogonal State Discrimination Using Local Operations and Classical Communication, Phys. Rev. Lett. 96, 040501 (2006)
3. D. Markham, J. Anders, V. Vedral, M. Murao, Survival of entanglement in thermal states, quant-ph/0606103
4. Masaki Owari, Samuel L. Braunstein, Kae Nemoto, Mio Murao, ε -convertibility of entangled states and extension of Schmidt rank in infinite-dimensional systems, quant-ph/0609167

5. Yu Tanaka, Damian Markham, Mio Murao, Local encoding of classical information onto quantum states, quant-ph/ 0702190

（2）特許出願

研究期間累積件数：1件(特許出願準備中)
発 明 者： 村尾美緒 田中雄
発明の名称： 古典公開鍵と量子秘密鍵を用いた計算量的秘匿量子計算
出 願 人： 独立行政法人科学技術振興機構
出 願 日：

（3）その他の成果

- Yu Tanaka, Masaki Owari, Mio Murao, A quantum lock protocol, The Ninth Workshop on Quantum Information Processing (QIP2006), 2006
- Mio Murao, Yoshiko Ogata, Mixed state asymmetric qubit information sharing, The Ninth Workshop on Quantum Information Processing (QIP2006), 2006
- M. Hayashi, D. Markham, M. Murao, M. Owari, S. Virmani, Local Discrimination and Multipartite Entanglement Measures, ERATO conference on Quantum Information Science 2005
- Yoshiko Ogata, Ryu Ebisawa and Mio Murao, Asymmetric quantum information sharing between two parties, Gordon Research Conference on Quantum Information Science 2004
- Masaki Owari, Kenji Matsumoto and Mio Murao, Entanglement convertibility for infinite-dimensional pure bipartite states, ERATO conference on Quantum Information Science 2004.