量子鍵を用いた次世代量子暗号プロトコル
Next generation quantum cryptographic protocols using quantum keys

村尾美緒
Mio Murao
東京大学大学院理学系研究科
The University of Tokyo

概要： 本研究では、多粒子間の量子もつれを用いて符号化した量子情報に注目し、多粒子間量子もつれと量子情報保全との関連の解析を行ないました。そして、量子もつれを暗号の資源（暗号鍵）として用いることによって量子情報の安全な通信を目指す、量子鍵を用いた次世代量子暗号プロトコルを探索しました。その結果、量子もつれと量子情報保全に関しては、遠隔操作量子情報抽出・遠隔操作量子情報破壊・非対称遠隔量子もつれ操作の条件を導出するとともに、無限次元系特有の量子もつれの性質を発見し、多粒子間量子もつれの距離的指標と局所量子状態判別との関連を見出しました。また、量子鍵プロトコル、遠隔量子情報制御スイッチプロトコル等の提案を行いました。

【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した。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」が必要となります。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、量子暗号の新しい方向性として量子もつれを量子情報のための暗号鍵として用いる「量子鍵」の概念を提唱し、量子情報保全のための新たな量子暗号プロトコルの探索を行ないます。

量子情報保全のための暗号プロトコルとしては、古典鍵を用いる提案が既にありましたが、古典鍵を用いた場合には不正な複製の危険が常に存在します。そこで本研究では、量子もつれを持つような量子状態を量子鍵として利用することにより、暗号鍵の不正な複製を不可能とする量子暗号プロトコルの提案を目指しました。

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ちます。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す。

【研究方法】 量子もつれ理論を中心とした基礎研究により量子もつれの新たな性質を発見し評価する基礎研究と、基礎研究で得られた研究成果を量子暗号プロトコルへと応用する応用研究を同時に進めるという手法をとりました。

量子もつれは非局所的量子相関であり、量子もつれの本質を明らかにするためには、量子状態の持つ古典的な相関と量子相関を明確に区別する必要があります。その一つの方法として、古典相関を増やすことはあっても量

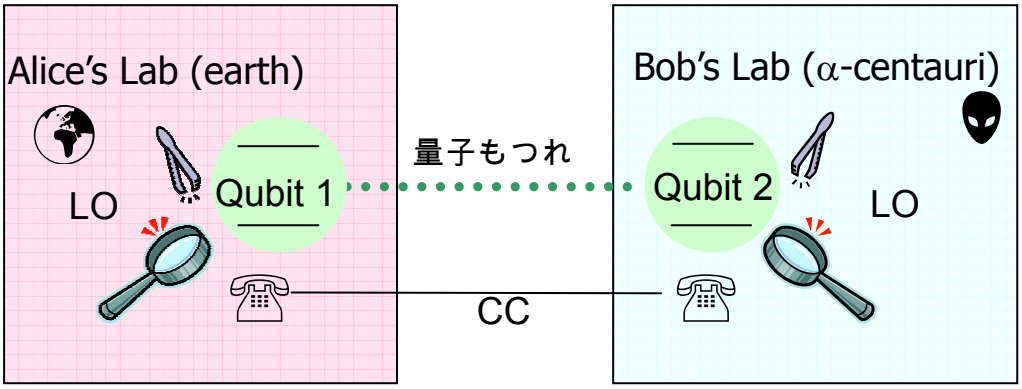

図１　　LOCC の概念図

Alice と Bob はそれぞれ離れた場所にある量子もつれを持つ量子ビット状態を共有しているが、それぞれ自分の量子ビットに対してのみ測定や操作を行なうことができる。測定結果は古典通信で相手に伝えることが可能である。

子相関を平均としては増やさないような操作のもとで、量子状態がどのように変化し、量子状態や量子情報を用いたタスクを行うことができるか、ということを解析する方法があります。この操作は、局所操作と古典的通信（LOCC）と呼ばれる操作であり、一般化された測定を含むような局所的な演算とその測定結果を伝える古典情報の通信、そして測定結果に基づく更なる条件付測定が含まれます。

そこで、さまざまな量子情報処理タスクを設定し、各タスクに LOCC の制限を加えた状況における量子状態の解析を行なうことによって、量子情報処理タスクにおける量子もつれの存在による非局所性の影響を解明すると同時に量子暗号プロトコルへの応用研究を探索する、という手法をとりました。

【研究成果】　基礎研究・応用研究の成果に大別して記述いたします。

基礎研究

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ました。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ました。

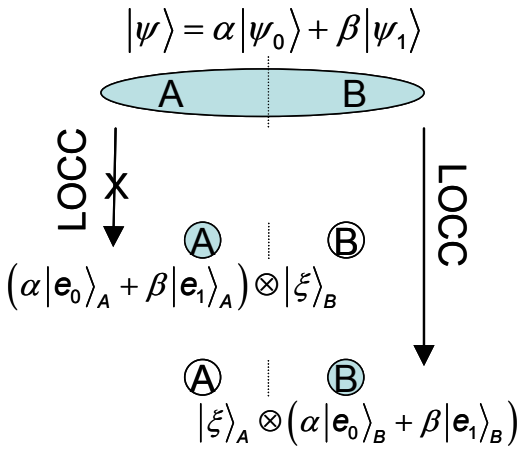

図２　遠隔操作量子情報集約

２者間の量子もつれは本質的に２者間に対称的に存在するものですが、量子情報の共有を行なう場合には、２者間で非対称性を導入することができる、ということを見出したことによって、量子暗号への応用可能性が大きく広がりました。この結果、量子鍵プロトコルへの応用研究へと発展いたしました。

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ました。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ものです。また、このタスクを行なうためには、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を示しました。

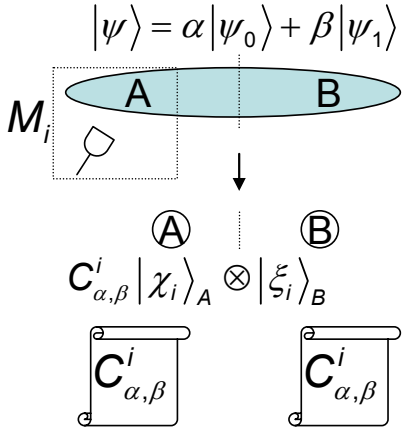

図３　遠隔操作量子情報破壊

非対称遠隔量子もつれ操作：局所的操作の選択を変えることによって、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のどちらも行なうことが可能となるように量子情報を２者間で共有する符号化方法を見出すことができますが、純粋状態を用いた符号化を用いる場合には、遠隔操作量子情報破壊の条件の制約により、２者間に非対称性を導入することはできませんでした。

しかし、混合状態を用いた量子情報の共有を行なうことによって、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すことに成功いたしました。

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ることができました。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いたしました。この結果は、混合状態を用い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へと応用されました。

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ました。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ました。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ました。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す。

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すが、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ります。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ります。この状態識別のタスクを LOCC で行うことができる場合はどのような場合であるかを解析する LOCC 状態識別可能性の研究は、近年盛んに行われてきましたが、多くの研究が特殊な場合にしか成り立たないプロトコルの発見に拘泥して、一般的な識別可能性の限界が得られていませんでした。

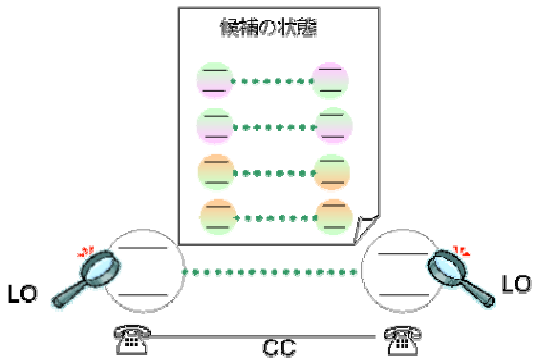

図４　LOCC 量子状態識別

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ました。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ました。

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ものです。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り、現在研究を続けております。

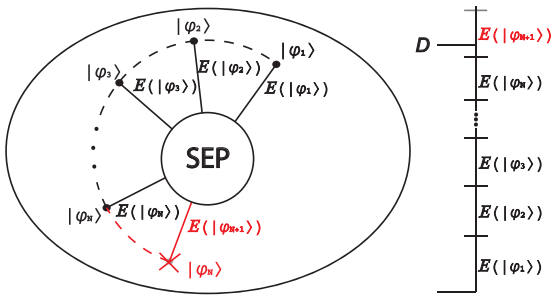

図５ LOCC 識別可能な状態と量子もつれの距離的測度および状態の次元との関係（量子もつれの距離的測度の和が次元数以下でないと LOCC 識別が不可能となる。）

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す。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されます。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異なるユニタリ変換の数を示すものです。低階数の密度行列で表されるノイズの多者間量子もつれを持つ量子状態に対す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ました。

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ました。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ました。

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ました。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ました。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もりは、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ます。

応用研究

量子情報のための量子鍵プロトコル：2 者間非量子情報分配の研究から得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」分配を提案しました。

遠隔量子情報スイッチプロトコル：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ました。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ます。

【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みました。そこで基礎研究としては、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ます。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す。

一方、応用研究については、複数のプロトコルが提案中で、現在それらプロトコルの安全性の解析を行なっているところであり、これらの研究を継続する予定です。

【結言】 本研究は、基礎研究で得られた知見を応用研究に生かし、さらに基礎研究にフィードバックを行なうという研究方法をとって行いました。量子情報のための暗号プロトコルを考察するために、量子もつれを持つような量子状態に量子情報や量子操作を符号化し、量子情報のいわばダイナミックスを探ることを手がかりに研究を進めました。その結果、

量子もつれの性質および、量子情報の非局所的な性質について多くの知見を得ることができ、今後の発展につながる成果を得ることができました。

一方、応用研究である、実際の量子暗号プロトコルについては、量子鍵プロトコル、遠隔量子情報スイッチプロトコルをはじめとして、様々なプロトコルを提案いたしました。量子暗号プロトコルとして確立するには、より詳細な安全性の評価を含めた今後の発展が必要となりますが、次世代量子暗号のプロトタイプ・プリミティブとして今後の発展可能性が期待されていると考えます。

参考文献

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) Yoshiko Ogata and Mio Murao, Remote extraction and destruction of spread qubit information, in preparation.

6) Mio Murao and Yoshiko Ogata, *Mixed state asymmetric quantum information sharing*, in preparation.