レーザーを用いた量子テレポーテーション

Quantum Teleportation with a Laser

藤居　三喜夫

■FUJII Mikio

量子テレポーテーションは実現可能性を伴うもっとも重要な量子情報技術の一つと言われ，その応用範囲は，絶対に盗聴されない通信から量子ネットワークや量子計算機などを構成する基礎部品までと多岐にわたる。

ところが2000年になり，世界初と言われるレーザーを用いた量子テレポーテーションの実証実験に対して徹底した批判が現れ，その後実験の正当性をめぐり２年の長きにわたって論争が続いた。東芝ソリューション（株）は今回，量子論に基づきレーザーの測定過程の記述を与えることで，この論争を世界に先駆けて解決することができた。更に，論争解決で得られた知見に基づき，複数レーザーを用いた量子テレポーテーションのための新たな提案を行った。

Quantum teleportation is considered as one of the most important quantum information technologies with high feasibility, and its potential applications range from unconditionally secure communication to a building block for a quantum network or a quantum computer.

In the year 2000, the so-called first demonstration experiment of quantum teleportation with a laser came under severe criticism, which later developed into a controversy that lasted for more than two years. Toshiba Solutions Corp. has solved this long-standing controversy for the first time by formulating the measurement process with a laser on the basis of the quantum theory. We have also made a new proposal for quantum teleportation with plural lasers based on the knowledge obtained from the above-mentioned solution.

一般論文

1　まえがき

ここ10年，量子情報と呼ばれる新しい分野が世界的な盛り上がりを見せている。量子情報とは，現代物理学の基礎をなす量子論を支柱として，従来の情報理論の拡張と再構築を目指す分野である。そこでは，これまで不可能とされてきた革新的な情報技術の創出が試みられ，既に多くの目覚ましい成果が上げられている。かつては物理学，情報科学，暗号理論，応用数学などと細分化されてきた専門家たちは，現在，量子情報のもと一堂に会し，互いに連携を取りながら学際的な研究開発を精力的に進めている。

ここでは，量子情報における技術開発の概観と，その代表的な技術“量子テレポーテーション”に関する東芝ソリューション（株）オリジナルの研究成果について述べる。

2　量子情報技術

2.1　量子情報技術とは？

従来の伝統的な情報理論においては，プログラミングから学術研究にいたるまで，情報の実体はニュートン以来のいわゆる古典的な世界観を土台にして理解されてきた。これは例えば，1ビットデータは当然0あるいは1どちらかの値のみに確定している，といった具合である。しかし慣習を離れてよくよく考えるならば，入出力，記憶，計算，制御など，すべての情報処理は必ず物理現象を介して実行されるわけであるから，情報の実体は物理学のもっとも基本的な枠組みである量子論により初めて正しく記述されるのではないか，と考えを進めることは自然であろう。そこで量子論に従うならば，例えば1ビットデータに対応する“量子ビット”は，0と1の異なる値を同時にとる“重ね合わせの状態”にあることも可能であるし，更にそこから，量子ビットが未知のときにはそのコピーが原理的に不可能であることも示される。このように，量子論の視点から伝統的な情報科学の見慣れた風景を眺め直すとき，古典的な視点では見えなかった多くの可能性がこつ然と姿を現す。量子情報技術とは，物質において通常は眠っているこれら顕著な量子性を人為的に引き出し，制御対象として積極的に利用することで，情報処理の新たな可能性を実現する技術なのである。

2.2　量子情報と情報セキュリティ技術

当初の見込みとは大きく異なり，これまでの量子情報技術の成果には不思議と情報セキュリティ技術に深くかかわるものが多い。例えば，最近よく耳にする量子暗号では，量子論に基づいた安全性を保証しつつ送受信者間の鍵共有を行うことで，どれだけ優れた性能の計算機を用いて攻撃しても絶対に破れない暗号通信が実現される。また，別の代表的な応用例である量子計算機は，現在の情報セキュリティ技術全体に対して潜在的な脅威であることが知られている。大規模な超並列計算を可能とする量子計算機は，一つには公開

鍵暗号が安全性の根拠とする素因数分解問題と離散対数問題に対して，もう一つには共通鍵暗号などの秘密鍵の推定に有効な探索問題に対して，その驚異的な計算能力を発揮することが理論的に示されている。そしてこれは直ちに，現在の情報セキュリティ技術に使用されている暗号技術のほとんどが，量子計算機の完成とともに完全に無力化することを意味するのである。

2.3 東芝グループの取組み

これら一連の世界的な流れを受け，東芝グループも次世代技術開発の一環として量子情報技術の研究に取り組んで来た。量子暗号については東芝欧州研究所（ケンブリッジ）が，長らく実用化への試金石と言われてきた100 kmの壁を越える長距離量子暗号の実験に世界で初めて成功した[(1)]。また量子計算機については，東芝 研究開発センターがEIT（電磁波誘起透明化）と呼ばれる物理現象によって固体素子における重ね合わせの状態を生成することに成功しており，これは量子計算機の材料の有力候補の一つとされている[(2)]。更に，同じく東芝 研究開発センターから，量子ドットと呼ばれる半導体原子から成る極微小な塊を用いた，量子計算機の先駆的な理論提案もなされており，現在の微細加工技術の延長線上にあることから，これも世界的な注目を集めている[(3)]。

2.4 エンタングルメントと量子情報技術

ここで各技術の成熟度を見ると，量子暗号はもはや基礎研究の段階を終え，2004年にはいくつかの製品も市場に登場し，既に実用に耐える高品位な製品の開発を競う段階に入っている。一方，量子計算機については，おそらく当分の間は試行錯誤を伴う基礎研究の段階が続くものと思われる。というのも，意味のある量子計算を行うには少なくとも数百の量子ビットを一括して保存・制御する必要が知られているが，これを実現する決め手となる技術がいまだに見つかっていないからである。

このように量子情報技術における実用化までのタイムテーブルを思い描くとき，製品化に限りなく近い量子暗号と，製品化までの道のりがいまだ見えない量子計算機との中間に，実は“エンタングルメント”と呼ばれる量子状態の特性を利用した，一連の新しい情報技術が存在する。

ここでエンタングルメントとは，量子論で物質を記述することにより初めて現れる，空間中の離れた物質どうしを結んでいる光速を超えた不思議な相関のことである。エンタングルメントは過去多くの実験によりその存在が確認されており，しかも現在，既に効率的な生成方法がいくつか知られている。

エンタングルメントを情報資源として利用する技術は，量子暗号の次に実用化に近いものとして大きな期待を集めている。ただし技術上の難点として，エンタングルメントは環境からのノイズに非常に弱く，そのままでは瞬時に崩壊してしまうため，今のところ特殊な実験環境の中でわずかな時間しか使用することができない。そこで現在は，一般の環境下でも壊れにくく純度の高いエンタングルメントの生成技術，大量の薄いエンタングルメントをもとに少量の純度の高いエンタングルメントを生成する蒸留技術，生成されたエンタングルメントを長時間保存する技術など，エンタングルメントを実用化するための提案と実験が数多く行われている。

エンタングルメントを応用した情報技術には，量子テレポーテーション，エカートの量子暗号，量子稠密（ちょうみつ）符号化，量子リピータ，量子秘密分散法など，既に多くのものが知られている。中でもとりわけ量子テレポーテーションは，単独で機能するのみならず，高度な情報処理を行う量子ネットワークや量子計算機を構築する基礎部品としても必要であるため，特に重要な要素技術として知られている。

以下に，この量子テレポーテーションに焦点を当てて，技術の背景と当社オリジナルの研究成果について述べる。

3 量子テレポーテーション

3.1 量子テレポーテーションのプロトコル

量子テレポーテーションとは，エンタングルメントを用いて，局所的操作と古典通信路により任意の量子状態を伝送する通信プロトコルである。**図1**にプロトコルを示す。

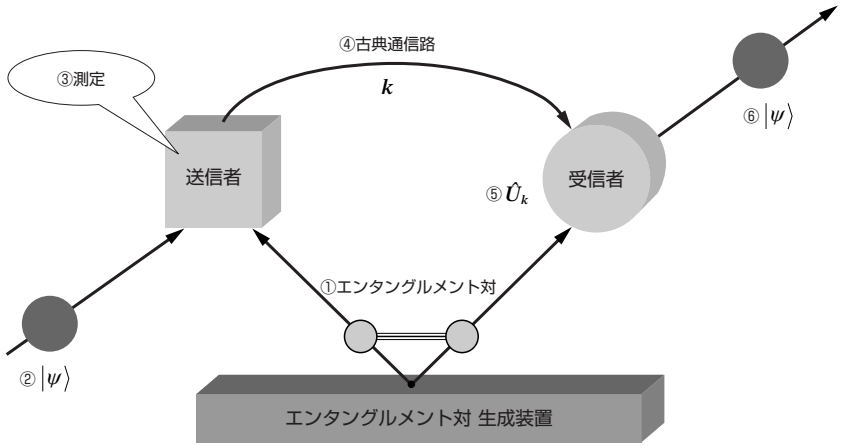
ここで図1の古典通信路を通る古典情報kは，伝送する量子状態にまったく依存しない乱数である。したがって伝送する量子状態をメッセージ情報とすると，量子テレポーテーションは，攻撃者が持つ計算機の性能と無関係に，盗聴に対して安全性が保証された通信プロトコルであることが理解される。

3.2 量子テレポーテーションの歴史

量子テレポーテーションは1993年に理論的に発見されたが[(4)]，当時は新技術というよりも，むしろ学術的に興味を引く一つの原理的な可能性にすぎなかった。しかし，ほどなく1997年にインスブルック大学のグループによって[(5)]，更にその翌年にカリフォルニア工科大学（カルテック）のグループによって[(6)]，レーザーを光源とする実証実験の成功があいついで発表されることで，量子テレポーテーションは現在の技術水準で実現可能な先端技術として一躍脚光を浴びることとなった。その後，前記両グループ間に起こった，技術の優先権をめぐる数年ものし烈な論争を経て，オリジナル提案に正しく対応した“無条件”量子テレポーテーションであるという主張に基づき，現在はカルテックの実験が最初の量子テレポーテーションとして取り上げられることが多い。

3.3 論争

ところが2000年になり，カルテックの実験に対してもその正当性に深刻な疑問が投げられることとなった。オーストリアのESIのグループにより，光源であるレーザー光の量子状



①送信者と受信者にエンタングルメント対の片方ずつを配布する。
②送信者は送りたい任意の量子状態を入手する。
③送信者は移動させる量子状態と自分のエンタングルメント対の片方を混ぜて測定する。
　測定により，送信者が持つ量子状態は壊れる。
④送信者は得られた測定値 k を古典通信路によって受信者へ送信する。
⑤受信者は測定値 k に応じたユニタリー変換 $\hat{U}_k$ を自分のエンタングルメント対の片方に施す。
⑥受信者のエンタングルメント対の片方が，送信者の送りたい量子状態へと変わる。

$|\psi\rangle$：送信される任意の量子状態

図1．量子テレポーテーションのプロトコル―古典通信路を用いるため，量子状態の伝送速度は光速を超えることができない。
Quantum teleportation protocol

態を正しく考慮すると，無条件量子テレポーテーションとしての理論提案と彼らが実際に行った実験との間に原理的なギャップが存在することが指摘され，カルテックの実験は量子テレポーテーションではないと結論づけられたのである[7]。それまで高精度の量子テレポーテーションの実験はほとんどが従来型レーザーを用いて行われていたため，この論争は単にカルテックの実験が正当か否かにとどまらず，はたして現在の技術水準で量子テレポーテーションが可能か否かを正面から問うものとして，世界的な注目を集めることとなった。

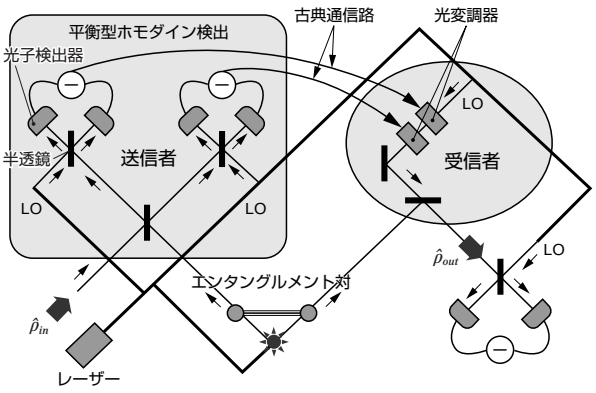
3.4　論争の焦点

2000年にESIのグループから指摘されたカルテックの実験のギャップは次のとおりである。

(1)　カルテックのグループは理論提案で，各光源に位相成分が確定したコヒーレント状態を想定していた。しかし実験では，光源として原理的に位相がランダムなレーザー光を用いていた。これを考慮すると，カルテックの実験は量子テレポーテーションではないことが示される。

(2)　理論提案と，実際に行った実験のスキームが根本的に異なる。実験では**図2**に示すように，送信者と受信者はエンタングルメント対と古典通信路のみで結ばれる独立なパーティではなく，理論にはなかった余分な光路により最初から結合された一つの系を構成していた。

これに対するカルテックのグループの反論[8]は次のとおりである。



LO：局部発振光
$\hat{\rho}_{in}$：送信者により送信される任意の量子状態
$\hat{\rho}_{out}$：受信者により復元される量子状態

図2．カルテックが実際に行った量子テレポーテーションの実験スキーム―送信者と受信者は，本来の量子テレポーテーションにはない余分な光路によってあらかじめ結合され，一つの系を成している。
Experimental scheme for quantum teleportation performed by the Caltech group

(1)　レーザー光の位相が完全にランダムなのは，レーザー共振器内にある場合だけである。実験で使われるのは共振器外のレーザー光であり，これを求めると共振器内とは異なり，レーザー光はコヒーレント状態に類似した位相特性を持つことが示される。ゆえにレーザーを用

いても，コヒーレント状態を仮定した場合と同様に量子テレポーテーションが実現される。

⑵　理論提案にはない余分な光路は位相を合わせるためだけにあるので，特に問題ではない（ただし明示的な証明はなし）。

3.5　論争解決への見極め

カルテックのグループの反論に沿って計算を追うと，彼らが求めたと主張している“共振器外のレーザー光の状態”とは一種の近似表現にすぎないもので，正確にはレーザー光は共振器の中も外も形式上同等な量子状態で表されることがわかった。つまりこれは，共振器外のレーザー光は共振器内と同様に位相不定性を持つことを示している。

それではESIのグループの指摘どおり，カルテックの量子テレポーテーションの実証実験は原理的に誤りだったのだろうか？

ESIのグループはカルテックの実験の批判を組み立てるなかで，一つの重大な見落としをしていた。彼らはレーザー光の測定過程を正しく考慮に入れていなかったのである。量子論によると，観測者がレーザー光を測定しそこから情報を得るとき，レーザー光は測定直後に“波束の収縮”によって状態が不連続に，そして場合によっては劇的に，変化を受けるはずである。したがって，特にカルテックの実験のように，プロトコルの1ステップとしてレーザーを用いた測定が必要である場合，レーザーの量子状態を考慮し測定過程を正しく記述することは避けられないと考えられる。

3.6　考察

当社は，カルテックの実験の正確な記述と論争の解決を目指し，量子論に基づいて，局部発振光にレーザーを用いる平衡型ホモダイン検出の測定過程の定式化を行った[9),(10)]。

出発点としたのは「量子効率が高い光子検出器の観測可能量（出力電流値）は，光子数演算子により精度良く表せる」という経験的知見である。これは40年以上の実験の歴史に裏打ちされており，この研究では帰納的に見いだされた“確実に真であるもの”として受け入れることとした。

この知見から出発して，平衡型ホモダイン検出の観測可能量を求め，更にその固有値と固有状態を得たところ，固有値には位相情報が含まれていないことがわかった。ここで測定に関する量子論の公理に従うならば，この数式上の事実は，この測定では測定値としてレーザー光の位相情報を得ることができないことを意味している。

これより，①位相不定性のため，レーザー装置が持つ外部パラメータからはレーザー光の位相情報をあらかじめ知ることができない，更に，②この測定を行ってもレーザー光の位相情報は得られない，という二つの事実を考慮したうえで，固有状態に基づく測定演算子を用い，**図3**に示すようにレーザー光による平衡型ホモダイン検出の定式化を行うことができた。

続いて，図3の提案公式が従来の実験結果と矛盾しないことを確かめるため，平衡型ホモダイン検出を用い，かつ20年の実験の歴史に裏打ちされたスクイーズド光の生成実験について，測定値の統計分布を提案公式に従い計算した。その結果，提案公式による計算結果は過去の実験結果と完全に一致することが示された。

次に，この提案公式をカルテックの実験に適用した。その

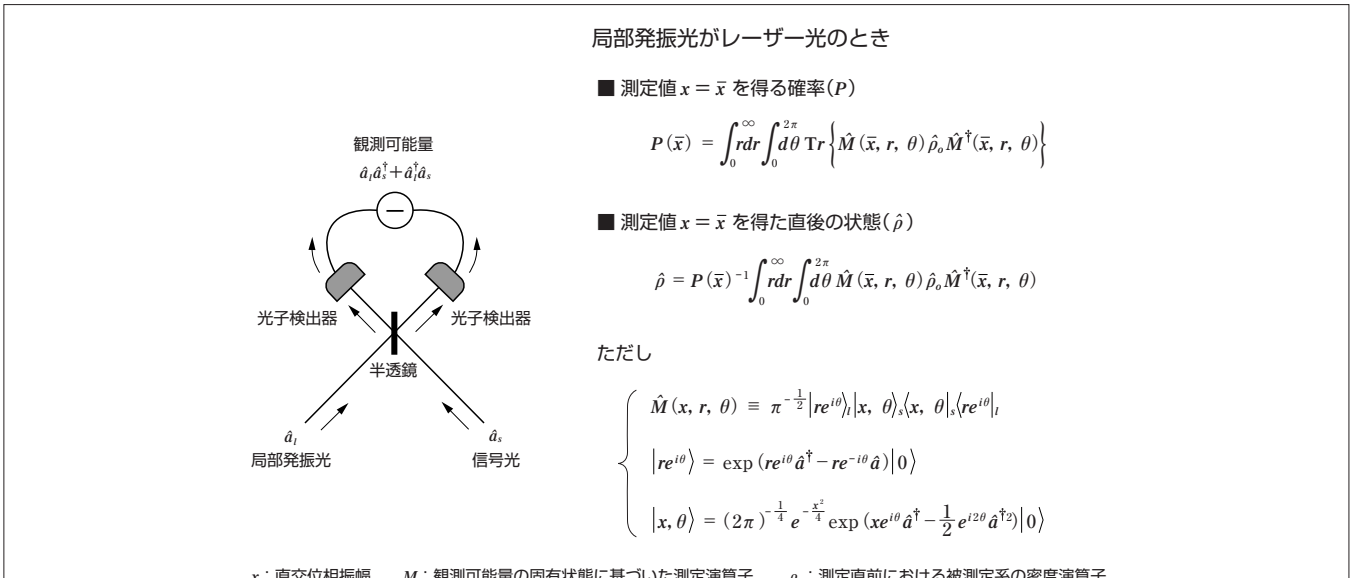


図3．平衡型ホモダイン検出― 局部発振光に高出力レーザーを用いる場合の，測定過程の定式化を行った。
Balanced homodyne detection

結果，もし送信者と受信者が何らかの手段でレーザー光の不定の位相を共有することができれば，レーザーを用いて量子テレポーテーションが成り立つことが解析的に証明された。カルテックの実験は，余分な光路によって不定の位相が共有されていたため，量子テレポーテーションとして正当であることが明らかとなった。

以上，量子論に基づきレーザーの測定過程の正確な記述を与えることによってこの論争は解決され，現在の技術水準のもと，量子テレポーテーションがレーザーを用いて実現可能であることが初めて示された。

3.7　提案実験

論争の解決により，送受信者間で不定の位相を共有すれば量子テレポーテーションが可能となることが示された。しかし，共有の仕方についてはなにも実験のように余分な光路を用いる必要はない。そこで当社は**図4**に示すように，テレポーテーションを行う前に独立した二つのレーザー間で不定の位相を共有しておく方法を提案した[(9),(10)]。提案は，1990年前後に発展した連続測定理論に基づく。この方法では位相が確率的にしか共有されないため，ある程度のトライアル＆エラーが必要である。

この提案において位相差が固定されていくメカニズムを分析すると，独立なレーザー間の相対位相を固定するには，測定に相当する操作が本質的であることを示唆している。位相の安定性は，量子情報通信を含めレーザーを用いた通信において特に重要であるため，この提案の応用範囲は意外に広いのではないかと思われる。

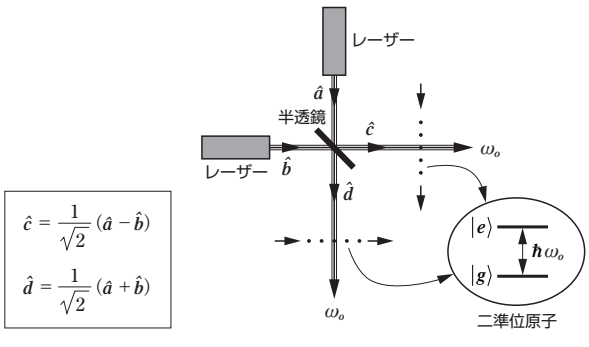


図4．レーザー光の連続測定のための提案実験 ― 独立した二つのレーザー光を半透鏡で混ぜ合わせ，そこへレーザー光に共鳴する二準位原子を基底準位にそろえたうえで1個ずつ定間隔かつ高速に交差させて，連続測定を実現する。

Proposed experimental setup for continuous measurement of laser fields

4　あとがき

ここでは，初めに量子情報技術の全般的な説明を行った。次に，盗聴不可能な通信として利用可能な量子テレポーテーションに焦点を当て，世界初とうたわれた量子テレポーテーションの実験の是非をめぐる論争について，当社の研究成果により解決へと至った経緯を述べた。これにより，現在の技術水準において，量子テレポーテーションがレーザーを用いて実現できることが初めて示された。また，解決の際得られた知見に基づき，複数レーザーを用いた量子テレポーテーションのための提案も行った。

ところで，これまで光学の教科書には，慣習として天下り的に「レーザー光は位相成分が確定したコヒーレント状態で表される」と記述されることが多かった。しかし厳密なレーザーの量子論に従う限り，定常状態でレーザー光の位相が完全にランダムであることは既に明確に示されている。今回の論争を経て，量子状態そのものを情報として扱う際には，もはやレーザーに関して従来の粗雑な理解のみで満足することは許されないと言えるであろう。

文　献

(1) シールズ A. J., ほか. 量子暗号通信で最長記録を達成. 東芝レビュー. **59**, 1, 2004, p.74－75.
(2) 市村厚一, ほか. 固体における EIT（電磁波誘起透明化）. 東芝レビュー. **54**, 5, 1999, p.67－71.
(3) Tanamoto, T.“ Quantum gates by coupled asymmetric quantum dots and controlled-NOT-gate operation ”. Phys. Rev. A 61, 2000, p.022305.
(4) Bennett, C.H., et al.“ Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels ”. Phys. Rev. Lett. **70**, 1993, p.1895.
(5) Bouwmeester, D., et al.“ Experimental quantum teleportation ”. Nature. **390**, 1997, p.575.
(6) Furusawa, A., et al.“ Unconditional Quantum Teleportation ”. Science. **282**, 1998, p.706.
(7) Rudolph, T. ; Sanders, B. C.“ Requirement of Optical Coherence for Continuous-Variable Quantum Teleportation ”. Phys. Rev. Lett. 87, 2001, p.077903.
(8) van Enk, S. J. ; Fuchs, C. A.“ Quantum State of an Ideal Propagating Laser Field ”, Phys. Rev. Lett. 88, 2002, p.027902.
(9) Fujii, M.“ Continuous-Variable Quantum Teleportation with a Conventional Laser ”, quant-ph/0304148, 2003.
＜http://arxiv.org/abs/quant-ph/0304148.＞,（accessed 2004-7-28）.
(10) Fujii, M.“ Continuous-Variable Quantum Teleportation with a Conventional Laser ”, Phys. Rev. A 68, Rapid Communications, 2003, p.050302.

藤居　三喜夫　FUJII Mikio, D.Sc.
東芝ソリューション（株）SI技術開発センター　SI技術担当，理博。情報セキュリティ技術の研究・開発に従事。
Toshiba Solutions Corp.