

量子インターネットに向けて

量子インターネットは地球上の任意のクライアント間での量子通信を可能にするだけでなく、量子計算や量子計測、さらには量子多体系のシミュレーションまでもを包含するパラダイムで、その構築は分野の長期的課題であり、究極的挑戦といえます。本稿では、量子インターネットとは何か、実現には何が必要か、また最近の分野での取り組みについて解説します。

あすま
東

こうじ
浩司

NTT 物性科学基礎研究所

はじめに

現代物理学において、素粒子レベルから宇宙に至るまでのさまざまな自然現象を、もっとも精巧に記述するのは量子力学であるとされています。量子力学は、起こり得る事象が生じる確率を言い当てるだけで古典力学が与えてきた決定論的世界観を包含する、より一般性が高いものとなっています。事実、決定論的世界観で構築された理論があったとしても、それを量子化することは、現代物理学における基本的な取り組みの1つであり続けています。前世紀末からは、そのような量子力学の枠組みで許される情報処理、すなわち量子情報処理の可能性が考察され始め、今となっては量子情報処理が、従来の情報処理の枠組みを包含するのみならず、その枠組みでは困難とされる情報処理タスクまでもを可能にすることが分かっています。

例えば、量子コンピュータは、現在のコンピュータでは難しいとされる大きな整数の素因数分解を効率的に行うことができます。そのため、量子コンピュータが実現され、もしそれが盗聴

者の手に渡れば、日常生活でもっとも利用されているRSA暗号の安全性を脅かします。他方、量子鍵配送 (QKD) は、たとえ盗聴者が量子力学で許される任意の盗聴行為を行ったとしても (つまり、任意のサイズの量子コンピュータに基づく盗聴行為に対しても) 情報理論的に安全な暗号通信を提供します。つまり、量子力学が自然界の正しい記述である限り、そのような量子力学で許される量子情報処理が、実現可能な情報処理の究極形であると考えられます。

では、そのような量子情報処理の究極形とはなんでしょう。現在のインターネットが地球上の最大の情報処理ネットワークであると考えられるならば、

その量子版である「量子インターネット⁽¹⁾」は、究極の情報処理ネットワークとなるはずですが、本稿では、量子インターネットとは何か、実現には何が必要か、また最近の分野での取り組みについて解説します (詳細は包括的総説論文⁽²⁾を参照)。

量子インターネットとは

量子インターネットは、(量子コンピュータや量子メモリなどの) 量子情報処理ノードを、(光ファイバや自由空間などの) 量子通信路で結びつけた地球規模の量子情報処理ネットワークで (図1)、地球上の任意のクライアントの、さまざまな量子情報処理タスクの実行を可能にします。このような

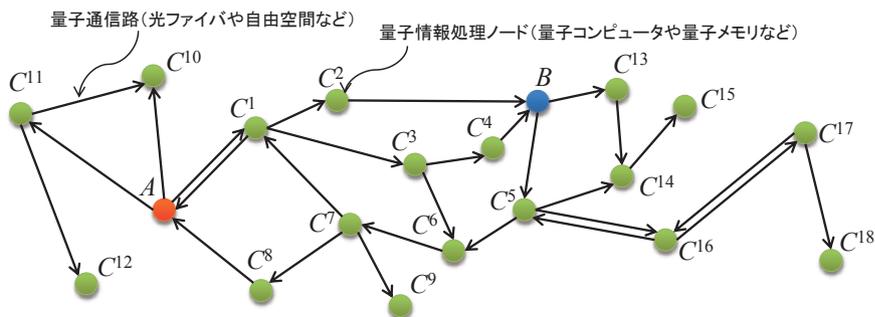


図1 量子ネットワークの模式図

量子インターネットは、現在のインターネットの枠を超えたさまざまな応用を持っています⁽³⁾。例えば、それはネットワーク上の任意のユーザ間での量子鍵配送を可能にします。そのため、国民投票や首脳会談、金融取引、遺伝情報や生体情報のやり取りが可能になります。また、量子インターネットは、量子テレポーテーションによって未知の量子系の情報を遠く離れた地点に光速で忠実に転送することも可能にします。これは、分散型量子計算、クラウド量子計算、あるいは量子コンピュータネットワーク構築の基礎となります。さらに量子インターネットは、現存するもっとも高い精度の時計である原子時計を正確かつ秘密裏に同期することにも利用でき、安定で正確で安全な世界時計の共有を可能にし、高精度のナビゲーションシステムへの応用も期待できます。ほかにも、望遠鏡アレイの長基線化を可能にするため、天文学の発展にも貢献します。

量子インターネットを構築するには

では、どのように量子インターネットを構築すればよいのでしょうか。量子インターネットの役割は、クライアントに対し、「量子もつれ」を効率的に配布することです。量子もつれは、原子や光子などの量子系でしか持つことができず、古典力学や従来の情報理論の枠組みでは説明がつかない奇妙な相関です。この量子もつれは元々、アインシュタイン、ポドルスキー、ローゼンによって、量子力学が局所实在論と相容れない予想を含むことを指摘する際に利用された状態で、ある意味、量子力学の正当性を批判するために引き合いに出されました⁽⁴⁾。しかし、皮肉なことに、結果的には量子もつれの存在は実験で再三確認されてきまし

た。2022年には、この実証実験を行ってきたアスペ、クラウザー、ザイリンガーの3名にノーベル物理学賞が授与されました⁽⁵⁾。さらに現在では、その量子もつれは量子通信だけでなく、量子計算の実行をも可能にする万能リソースであることが明らかにされています。したがって、そのようなリソースとしての量子もつれを効率的に配る役割を担うことで、量子インターネットはクライアントにさまざまな機能を提供することをめざすこととなります。

実際には、欧州のSECOQCネットワーク、日本の東京QKDネットワーク、中国の2000 kmに及び上海・北京ネットワークのように、量子鍵配送を目的とする量子ネットワーク自体は世界各地で構築されてきました。しかし、これらのネットワーク中のノードは、量子情報処理ノードではなく、たとえ量子的な信号を入力として受け取ったとしても、それを古典的な信号に落としてから処理する能力しかない「古典的」な情報処理ノードです。そのため、それらのネットワークは、ネットワーク中の任意のノード間に量子もつれを配ることはできず、たとえ量子鍵配送だけを行うことに特化しても、すべてのノードが信頼できる状況でない限り、安全な秘密鍵の配送はできません。この意味で、それら既存のネットワークはトラステッドノードネットワークと分類され、量子インターネットと区別されます。

他方、クライアント間を量子通信路で全結合する、すなわちすべてのクライアントがポイント・ツー・ポイントで量子通信を行うのであれば、安全な量子鍵配送ネットワークになります。しかし、このようなネットワークを地球規模に拡大するのはコストや効率という観点から現実的ではありません。例えば、量子通信路として光ファイバ

を用いた場合、その透過率はその長さに対して指数関数的に減少します。具体的には、送信者が発した、量子情報が埋め込まれた単一光子レベルの光が、受信者に検出される確率は、標準的な光ファイバの透過率を考慮するだけで、50 kmで約10%、100 kmで約1%、150 kmで約0.1%というように、50 kmごとに約0.1倍となっていくます。したがって、たとえ1 GHzクロックで動作するシステムであったとしても、1000 kmの光ファイバを通じてポイント・ツー・ポイントの量子通信を行う場合、送受信者が1対の量子もつれを得るのに必要な時間の期待値は100年オーダーとなり、これは現実的ではありません。したがって、ポイント・ツー・ポイント量子通信だけでは、量子インターネットは実現できず、それを実現するためには、量子中継⁽⁶⁾、⁽⁷⁾が必要とされます。

量子中継とは

従来の通信においても、送信者と受信者の距離が離れている場合は、送受信者はポイント・ツー・ポイントで結ばれているわけではなく、送受信者間に設置された中継器を利用しています。ここでの中継器の役割は、弱まった受信信号を増強し、次の中継器（あるいは受信者）に向け、信号を再発信することにあります。しかし、この原理は量子の世界では通用しません。なぜなら、量子複製不可能定理⁽⁸⁾により、量子的な信号の複製や増幅が原理的にも禁止されているからです。ゆえに量子中継は、そのような信号増幅に基づきません。

量子中継では、中継器を利用して、主に「量子もつれ生成」と「量子もつれスワッピング」という操作を行います。量子メモリ方式⁽⁶⁾では(図2)、物質量子メモリと量子インタフェース

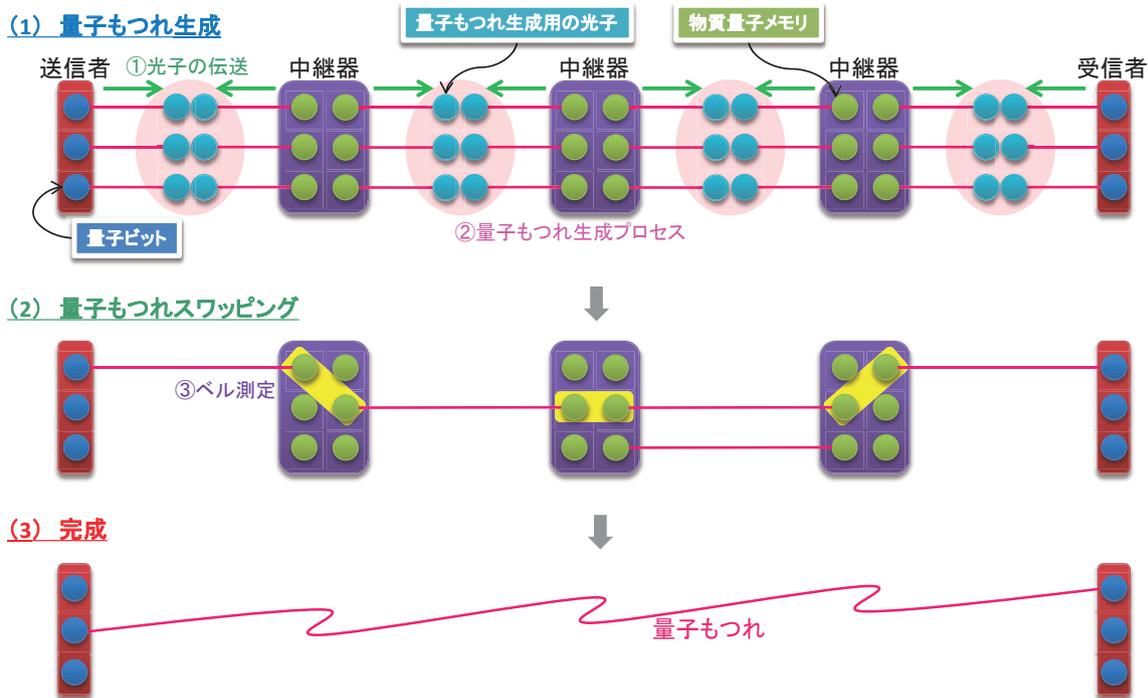


図2 量子メモリに基づく量子中継

を内蔵した量子中継器を光ファイバで結び、最近接中継器間で光子をやり取りすることで、最近接中継地点を結び量子もつれの生成を試み、生成に成功したら、その量子もつれを物質量子メモリに保存しておきます（量子もつれ生成）。この量子もつれ生成を成功するまで繰り返すことで、すべての最近接中継地点間が量子もつれで結ばれたら、中継器内の量子もつれの片割れの対にベル測定を施すことで、最近接中継地点を結んでいた量子もつれを、送受信者を直接結ぶ量子もつれへと変換します（量子もつれスワッピング）。このように、量子メモリ方式では量子もつれ生成を行い、その後量子もつれスワッピングを行います。

他方、全光方式⁽⁷⁾は（図3）、量子もつれスワッピングに対応する操作を最初に行い、その後量子もつれ生成を行うという時間反転方式に基づきます。具体的には、全光方式では各中継地点において、量子もつれスワッピングを実装するために、「グラフ状態」

と呼ばれる量子もつれ状態にある光子を準備します。ここで準備されたグラフ状態にある光子は、光ファイバを通じて最近接中継地点に分配され、それを受け取った中継器は、量子もつれ生成操作を施し、成功・失敗に応じて残りの光子を測定すると、高い確率で送受信者間に量子もつれが供給されます。全光方式における中継器は、量子メモリ方式とは異なり、物質量子メモリや量子インターフェースを必要とせず、光デバイス（単一光子源、線型光学素子、アクティブフィードフォワード技術、光子検出器）だけで機能し、方式の繰り返しレートは通信距離によらず、光デバイスの動作速度だけで決まります。そのため、従来の通信分野における全光アプローチとも親和性が高く、量子もつれの供給速度も極めて速くなります。

おわりに

量子ネットワークに関する理論研究の近年の進展（詳細は総説論文⁽⁹⁾を参

照）により、透過率 η の光ファイバが持つ量子通信容量 [= (伝送可能な量子ビット数)/(使用モード数)] や秘匿通信容量 [= (秘匿伝送可能なビット数)/(使用モード数)] が、 $-\log_2(1-\eta)$ となることが明らかにされました。これは、光ファイバを用いたポイント・ツー・ポイントの量子通信の限界を表し、（透過率 η がファイバの長さ l と定数 l_{att} に対して $\eta = e^{-l/l_{att}}$ となることを考慮に入れると）量子中継がなければ、効率的な長距離量子通信、ひいては量子インターネットは実現できないことを示します。また、任意の光ファイバネットワーク中の2者間通信に対する量子/秘匿通信容量が導出され、この容量が量子中継を並列化することで達成可能であることが示されました。これは量子中継が、原理限界の効率を持つ、あるいはそれに近いハイパフォーマンスの量子インターネットを構築する際においても、基本的な役割を担うことを示しています。

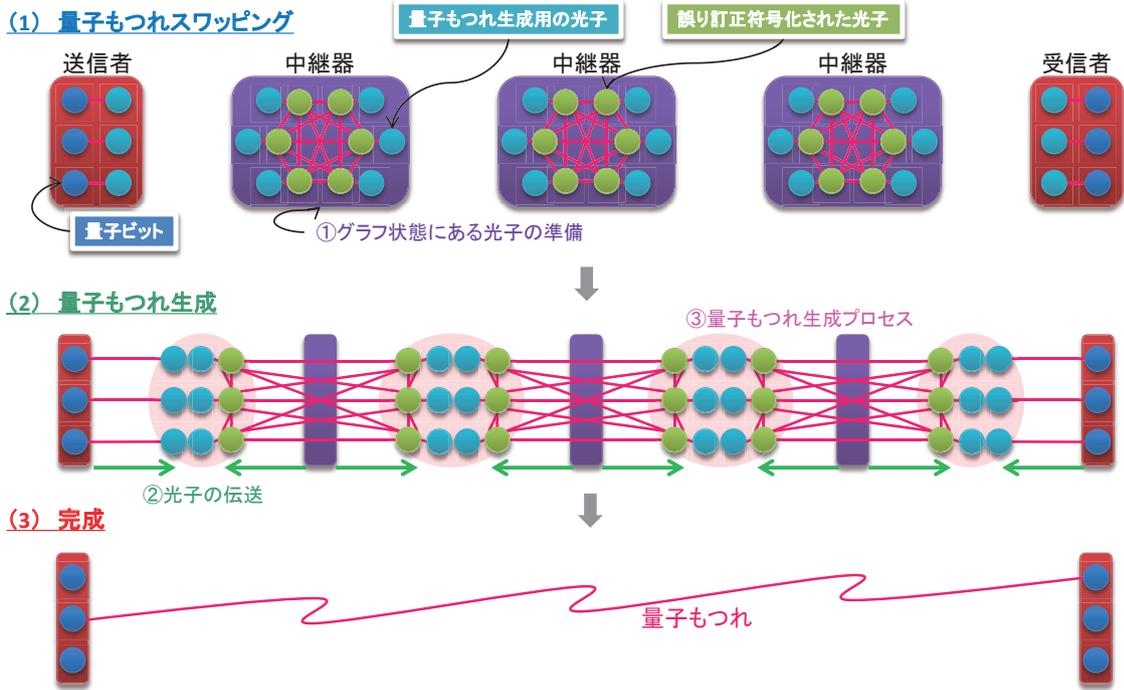


図3 全光量子中継

他方で、現状で実用化段階にあるポイント・ツー・ポイント量子鍵配送と、量子インターネット実現に不可欠な量子中継には技術的、概念的な間隙が存在します。この間隙を埋める方式の探索と実装は、量子鍵配送分野の大きなトレンドとなっています⁽¹⁰⁾。例えば、適応型測定装置無依存QKDやツイン・フィールドQKDなどはこれに分類されます。また、量子中継の原理検証実験についても、メモリ方式、全光方式ともに近年さかに行われています⁽²⁾。量子メモリ方式について、オランダのデルフト工科大学ではダイヤモンド中のNV中心を用いて、米国のハーバード大学・MITではシリコン中の空孔を用いて、中国の清華大学ではRb原子集団を用い、量子メモリを利用した量子もつれスワッピングの原理検証実験が行われています。また、全光方式については、パラメトリック下方変換と線形光学素子を通じて生成されたGHZ状態と呼ばれるグラフ状態に基づき、日本の大阪大学、NTT、

富山大学、カナダのトロント大学の研究チームと、中国の中国科学技術大学の研究チームが独立に、時間反転型の量子もつれスワッピングの原理検証実験を報告しています。

■参考文献

- (1) H. J. Kimble : “The quantum internet,” Nature, Vol.453, pp.1023-1030, 2008.
- (2) K. Azuma, S. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin: “Quantum repeaters: From quantum networks to the quantum internet,” arXiv:2212.10820, 2022.
- (3) S. Wehner, D. Elkouss, and R. Hanson: “Quantum internet: A vision for the road ahead,” Science, Vol.362, No.6412, 2018.
- (4) A. Einstein, B. Podolsky, and N. Rosen: “Can quantum-mechanical description of physical reality be considered complete?,” Phys. Rev., Vol.47, pp.777-780, 1935.
- (5) <https://www.nobelprize.org/prizes/physics/2022/press-release/>
- (6) H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller: “Quantum repeater: The role of imperfect local operations in quantum communication,” Phys. Rev. Lett., Vol. 81, No.26, pp. 5932-5935, 1998.
- (7) K. Azuma, K. Tamaki, and H.-K. Lo: “All-photonic quantum repeaters,” Nat. Commun., Vol.6, No.6787, 2015.
- (8) W. K. Wootters and W. H. Zurek: “A single quantum cannot be cloned,” Nature, Vol.299, pp.802-803, 1982.
- (9) K. Azuma, S. Bäuml, T. Coopmans, D. Elkouss, and B. Li: “Tools for quantum

network design,” AVS Quantum Sci., Vol.3, 014101, 2021.

(10) M. Curty, K. Azuma, and H.-K. Lo: “A quantum leap in security,” Phys. Today, Vol.74, No.3, pp.36-41, 2021.



東 浩司

量子インターネットについての理論的理解は近年急速に進み、その結果、量子中継の研究開発の重要性が再認識されました。実際、欧州をはじめ、中国、米国と大型の研究プロジェクトが走っています。日本においても追従すべく、量子インターネット研究への注目が高まっています。

◆問い合わせ先

NTT物性科学基礎研究所
 量子科学イノベーション研究部
 TEL 046-240-3440
 FAX 046-240-4722
 E-mail koji.azuma.ez@hco.ntt.co.jp