1. 量子インターネットとは

1.1. はじめに

量子情報技術の産業化が急速に進み、量子コンピュータという単語を新聞やテレビで見る機会も増えてきた。一方で、未成インフラである量子インターネットの知名度はまだまだ低い状況といえる。本稿が量子インターネットの仕組みや建設目的、量子暗号のためのトラステッドノード・ネットワークとの相違点などの理解に役立てば幸いである。

まずは古典／量子の情報システムについて整理してみよう。我々が普段利用するスマートフォンやパソコンなどの古典コンピュータはデジタルデータ＝古典情報を取り扱う。ここで**古典**とは、古さではなく**非量子**を意味している。古典情報の最小単位は古典ビットであり、0 と 1 で記述される。

量子コンピュータは重ね合わせ状態や量子もつれなどの量子状態で表される量子情報を処理し、古典コンピュータでは模倣できない量子計算の実現を目的とする。量子情報の最小単位は $|0\rangle$ と $|1\rangle$ を重ね合わせた量子ビットであり、

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

と記述される (α、β は $|\alpha|^2 + |\beta|^2 = 1$ を満たす複素数)。

古典インターネットでは古典通信路を介して古典ビットを転送する。また、トラステッドノード･ネットワーク (Sec. 3.1) では量子通信路を介して古典情報が書き込まれた量子ビットを転送する。両者の構成やプロトコルは大きく異なるが、**古典情報が送受信者間で共有される**点が共通する。

量子情報の送受信では、複製不可能定理によって量子状態のコピーを手元に残すことが禁止されているため、転送をやり直すことは出来ない。また、量子状態を光ファイバで転送すると、距離に対して成功確率が指数関数的に低下してしまうため、遠距離間での**量子情報の直接転送は難しい**。

しかし、送受信者間で**ベル状態が共有されている**ならば、量子操作と古典通信を用いて**距離に依らず量子情報を転送することができる** (量子テレポーテーション)。ベル状態とは、２量子ビットが最大までもつれた状態（エンタングルメント）であり、以下の４状態を指す：

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{2}$$

例として、A の持つ１量子ビットの量子情報 $|\psi\rangle$ を、ベル状態 $|\Phi^+\rangle$ を共有する B へ転送する。まず、A は手元の２量子ビットに対してベル測定（ベル状態を基底とする射影測定）を行い、測定結果（２古典ビット）を B へと送信する。測定後に、B の手元の量子ビットは $|\psi\rangle$ に何らかの副次的な演算子が作用した状態となっている。B はこの演算子を A から受信した測定結果によって特定できるため、対応する量子操作によって打ち消し、$|\psi\rangle$ を得ることができる。

$$|\psi\rangle_A|\Phi^+\rangle_{A,B} \xrightarrow{A\text{ のベル測定と結果に基づく }B\text{ の量子操作}} |\psi\rangle_B \tag{3}$$

ここで、ベル状態は量子通信資源として消費されている。

1.2. 量子インターネットの建設に向けて

量子インターネットは量子中継によって任意の地点に適切な量子もつれを分配可能なネットワークであり、現行のネットワークでは原理的に実装できない**量子もつれを必須とするアプリケーション**の運用を目的とする。

ノイズのある量子通信路で構成されたネットワークで高い忠実度（Fidelity、量子状態の類似性の尺度）の量子もつれの分配を行うデバイスとして、1998 年に Briegel らは**量子中継器**[1] を提案した。量子中継器は以下の機能を持つ：

1. 光ファイバで相互接続された量子中継器間に量子もつれ（主にベル状態）を生成・共有する。
2. 局所量子操作によるもつれ交換を行い、相互接続されていない量子中継器間に量子もつれを生成する。
3. 量子メモリに保持する量子もつれの忠実度を管理し、純粋化などによる忠実度の回復操作を行う。
4. 量子中継器ネットワークの状態を管理し、通信経路や必要な量子資源の確保、攻撃の検知などを行う。

ここで、3. の忠実度の回復には古典通信の待機時間などに対して十分な性能の**量子メモリ**が必要となる。そのため、量子メモリの性能が不十分な黎明期の量子中継器ネットワークでは、量子もつれの分配可能な距離や品質、量子もつれを利用するアプリケーションの選択肢に大きな制約が発生するだろう。

量子インターネットの建設は、少数の量子中継器からなるネットワークを構築し、自律運用されるネットワーク同士の相互接続により進展していくだろう。現状は、量子メモリをはじめとするハードウェアの進歩だけではなく、自律運用に必要となるさまざまな技術的仕様やルールの整備、それらの検証に必要な大規模シミュレータの開発など多くの課題が残されている。昨今は各国でテストベッド・ネットワークの計画が動き出しており、競争力維持に向けた人材確保・育成の重要性は日に日に増している。

また、需要喚起に向けたユースケース開拓も重要になる。パソコン通信の時代に今日のインターネット・アプリケーションの用途や進化を予見することが難しかったように、数十年後の量子インターネットが提供する先進的サービスの想像は困難だが、多くのキラーアプリが発見され、我々の生活に不可欠なインフラになっていくことを期待したい。

次節以降において、まず、量子中継器ネットワークの概要について解説する（Sec. 2）。次に、さまざまな段階の量子インターネットにおいて運用が想定される量子インターネット・アプリケーションを解説する（Sec. 3）。また、量子中継技術の最近の進展について、さまざまな物理系を用いた量子メモリを中心に紹介する（Sec. 4）。最後に、量子インターネット建設に向けた我々の取り組みについて紹介する（Sec. 5）。

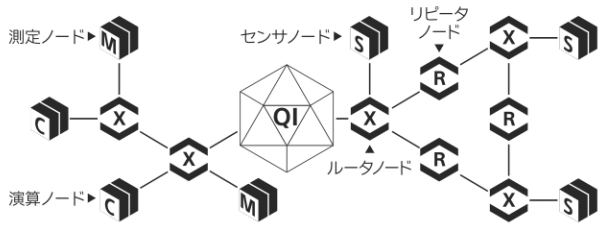

図 2　量子中継器ネットワークの構成例。量子中継器（R,X）が量子もつれの分配を担い、用途に応じたエンドノード（M,C,S）が量子もつれを必要とするアプリケーションを実行する。クラウド量子計算のためのツリー型ネットワーク（左）やセンサノードを組み込んだ循環型ネットワーク（右）のように用途や構成が異なるネットワークを相互接続することで量子インターネット（QI）が構成されていくだろう。

2. 量子中継器ネットワーク

本節では、遠隔地間で量子もつれを共有・利用する**量子中継器ネットワーク**を俯瞰する。現段階で想定されるノード構成や、隣接するノード間におけるベル状態の共有手法、隣接していないノード間でベル状態の共有を実現するプロトコルについて解説する。将来的には、大規模化した量子中継器ネットワークが相互接続されていくことで**量子インターネット**へと拡張されていくだろう。

2.1. 量子中継器ネットワークの構成

量子中継器ネットワークの概観を図 2 に示す。量子もつれを分配するため、各ノードは（量子もつれを構成する）量子ビットを転送可能な光ファイバのリンクで他ノードと接続される。量子ビットの測定情報やネットワークの制御情報などを交換するため、各ノードはインターネットなどの古典ネットワークにも接続されていることを前提とする。

量子もつれを利用するエンドノード

量子もつれを用いたアプリケーション（Sec. 3）を実行するノード。インターネットに接続された計算サーバやスマートフォンなどのように、能力の異なるさまざまな端末が想定される。将来的には、十分な量子演算能力を備えてクラウド量子計算に貢献する**演算ノード**（図 2 における C）や、簡易な構成で秘匿性の高いブラインド量子計算によって演算ノードを利用する**測定専用ノード**[2]（M）などが登場するだろう。また、広域に共有された量子もつれを用いる超長基線電波干渉計や量子時刻同期の実装を担う**センサノード**（S）も想定される。

量子もつれを分配するノード

量子中継器が相当し、後述する**もつれ交換**や**もつれ純粋化**によって、高品質な量子もつれの長距離分配を担うノード。長大な直線上リンクには一定の距離ごとに**リピータノード**（R）を設置し、量子もつれの忠実度を回復する必要がある。また、ルート分岐や他の量子中継器ネットワークとの接続を担う、インターネットのスイッチングハブ・ゲートウェイに相当する高い処理能力を持った**ルータノード**（X）も登場するだろう。

2.2. 隣接するノード間にベル状態を生成する手法

量子ビットはリンク中で確率的に消失してしまうため、量子情報の直接転送は難しい。消失確率よりも低い局所量子操作の失敗確率を前提として、ノード間で共有されたベル状態を前述の量子テレポーテーションに利用することで、実質的な量子通信路を構築することができる。ベル状態もリンク中で消失するが、量子情報が書き込まれていないため、共有が成功するまで転送を繰り返すことができる。ベル状態を生成する方法として、リンクの中間点でベル測定を行う方式や、中間点に量子もつれ光源を設置して両端のノードに配送する方式があります。これらの方式は、使用する物理系や実装方法によって異なる性能を発揮するため、適切な選択が必要です。

Sender-Receiver 方式は、ノード内で生成されたベル状態の片方の量子ビット（光子）を光ファイバのリンクで接続された他ノードに送信する方式であり、受信側のノードは、自身が生成したベル状態の片方の光子と受け取った光子に対してベル測定を行います。両端のノードに残された 2 量子ビットは、測定結果に基づいた適切な量子操作によってベル状態となります（もつれ交換）。

Meet-in-the-Middle 方式は、リンクの中間点にベル測定器を設置する方式であり、両端のノードはそれぞれ、自身が生成したベル状態の片方の光子を送信し、中間点でのベル測定によってもつれ交換を行います。古典通信に必要なラウンドトリップ時間が半分になるため、光子の転送成功確率が高い環境では高レートなもつれ生成が期待できます。

Midpoint-Source 方式は、リンクの中間点にベル状態生成器を設置し、両端のノードに配布する方式です。この方式は、ノード内の量子メモリを効率的に利用できるため、光子の転送成功確率が低い環境においてもつれ生成レートを改善することが期待できます。

これらの方式は、2 光子干渉とベル測定を用いるものが基本的ですが、中間点にベル測定器を設置する Meet-in-the-Middle 方式のように、両端のノードから送られる光子が双方とも到着する必要のない、**1 光子もつれを用いる**方式も知られている[4, 5]。様々な物理系・実装方法の長所/短所と相まって、現在は 1 つの手法が決定打となる状況には至っていない。

2.3. 隣接していないノード間にベル状態を分配する手法

次に隣接していないノード間にベル状態を共有するケースを想定する。隣接していないノード間に高忠実度なベル状態が事前に共有されていれば、前述の量子テレポーテー

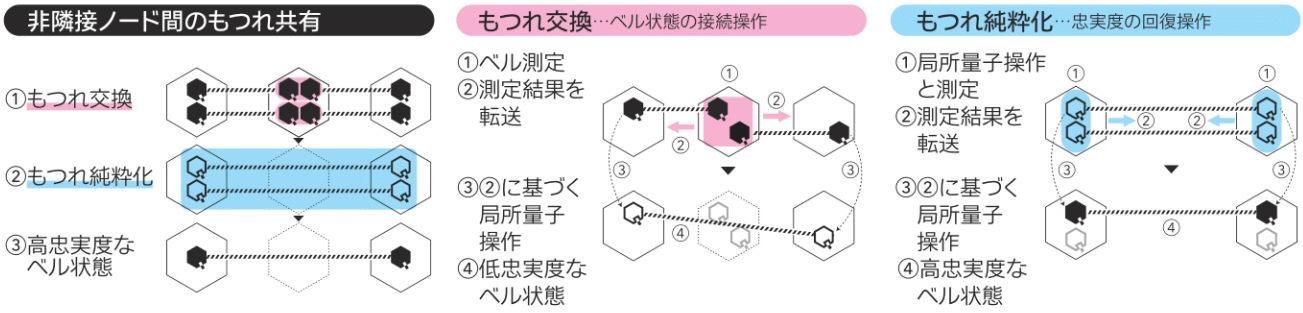

図 3　入れ子状プロトコル。もつれ交換を繰り返し、長距離もつれ共有を実現する。短距離もつれ（ベル状態）を多数用意し、忠実度が下がるともつれ純粋化により（ペア数を犠牲にすることで）忠実度を回復させる。もつれ交換ごとに忠実度が下がるので、必要なステージごとに純粋化を繰り返す。

ションによって距離に依らず高確率で量子情報を転送できる。では、前提となる高忠実度なベル状態はどのように通信相手と共有されたのだろうか？多数のベル状態を準備して、指数関数的な回数の転送を繰り返す必要があるのだろうか？また、光ファイバで直接相互接続されていないノード間ではベル状態を共有できるのだろうか？

一見すると堂々巡りになりそうなこれらの問題は**もつれ純粋化**と**もつれ交換**を組みわせることで解決できる。それぞれの操作の基本的な例 (図 3) と共に、もつれ共有に至るプロトコルを以下に紹介する。

もつれ純粋化（Entanglement Purification）

ノイズの影響を受けたベル状態の忠実度を回復するこの操作は、ノード間で転送・共有された複数の低い忠実度のベル状態から、（量子テレポーテーションに利用可能な）忠実度の高い少数のベル状態を作り出すものである（図 3 右下）。

例えば、確率 p でビット反転している忠実度 $F = 1 - p$ のベル状態を二組用いると、成功確率 $F^2 + (1-F)^2$ で一組の忠実度

$$F' = \frac{F^2}{F^2 + (1-F)^2} \tag{4}$$

のベル状態が一組得られる。ここで、他方のベル状態は補助系として用いられ、測定によって失われる。$F > 0.5$ であれば $F' > F$ となり忠実度は回復する（ここでは簡略化されたノイズモデルと完璧な量子操作・測定を仮定している）。

もつれ交換（Entanglement Swapping）

量子もつれ間にベル測定を行うことで、量子もつれ同士を接続する操作。中継ノードでもつれ交換を実行することで、隣接していないノード間にベル状態を共有することができる（図 3 中央）。この操作は（現状の線形光学にもとづくベル測定では）確率的で、また、実行後に生成されるベル状態の忠実度は初期状態よりも低下する。

もつれ共有プロトコル（Purify-and-Swap モデル）

もつれ純粋化で精製されたベル状態をもつれ交換によって接続すると忠実度は低下する。接続されたベル状態を多数用意して、もつれ純粋化によって忠実度を回復して、接続されたベル状態同士をもつれ交換して、‥と各操作を入れ子状に繰り返し実行することで、多数のノードから構成される長大な経路であっても End to End で忠実度の高いベル状態を共有し、量子通信を行うことができる (図 3)。

この Purify-and-Swap モデルの共有プロトコルは、十分な性能の量子メモリ（Sec. 4）があれば、通信距離に対して多項式的な回数のベル状態生成で実行出来ることが知られている[1)]。

我々が普段利用するインターネットは、標準化団体 IETF によって策定された TCP/IP や http などのプロトコルに従う、数万の自律システム (Autonomous System, AS) の相互接続によって構成されている。これを鑑みると、未来の量子インターネットも統一された運用ポリシーによって管理される量子中継器ネットワーク＝**量子自律システム**を相互接続しながら拡張されていくことが想定される。

3. 量子インターネット・アプリケーション

量子インターネットは、古典インターネットやトラステッドノード・ネットワークでは提供できないサービスの運用を目的とする。既に運用されている量子鍵配送から未来の量子インターネット・アプリケーションまで俯瞰してみよう。

量子インターネットの進化過程を QuTech の Wehner らは被転送情報や量子中継器の機能要件に応じて分類した[12)](表 1)。

Stage 0 (前量子ネットワーク) には、現代のトラステッドノード・ネットワークが相当する。量子ビットを介して秘密鍵を転送する QKD プロトコルが運用され、

3.1. 現行の量子鍵配送ネットワーク

量子通信の代表的な応用例に量子鍵配送（quantum key distribution, QKD）がある。QKD は離れた 2 ユーザー間

表 1　現行の量子通信ネットワークである Stage 0 は量子中継器を必要としない。Stage 3 以降は量子状態の維持・回復が可能となり高度なアプリケーションが運用可能になる。

Stage	被転送情報	量子メモリ	用途例
0	古典	なし	量子鍵配送（QKD）
1,2	量子	なし	QKD、秘匿認証
3-5	量子	あり	量子計算への応用

での、ランダムビット列からなる秘密鍵（古典情報）の効率的共有方法で、送りたい情報と同等以上の鍵ビット列を用意すれば one time pad 方式によって情報理論的安全な暗号通信ができる。代表的なプロトコルとして、BB84[13]（単一光子もしくは微弱レーザーなどを光源として、2 ユーザー間で量子状態を付加した光子を送信し、鍵生成する方式）や E91[14]（ユーザー間で共有したベル状態を使って鍵を生成する方式）などがある。プロトコルの詳細は割愛するが、QKD は基本的に重ね合わせ状態や量子もつれといった量子ビットの特徴と古典通信を組み合わせることで盗聴と改竄を防止し、安全な秘密鍵共有を実現する。

QKD を運用するトラステッドノード・ネットワークは社会実装が進んでいる。東京都心部-小金井間には**東京 QKD ネットワーク**が稼働しており、2010 年には量子鍵配送を用いたセキュアなテレビ会議を実現した。また、国際標準化 (ITU-T) にも貢献しており、現在は QKD 衛星も組み合わせた大規模・高速化を目指している。

また、中国では北京・上海を結ぶ 2000km の光ファイバー、および地上-人工衛星間通信も含め全長 4600km 以上の長距離 QKD ネットワーク**京滬幹線**が稼働している[15]。このネットワークは１００以上のノードを持ち、北京・上海・済南・合肥の 4 つの大都市を結ぶ幹線部分と、各大都市でのスター型ネットワークや量子暗号衛星**墨子号**などで構成される。

量子インターネットは、任意の地点間で量子中継器を介しながら量子もつれの共有し、もつれを用いた量子テレポーテーションによる量子状態転送を行う。QKD はあくまでもランダム古典ビット列の共有であり、量子インターネットの基本機能「量子もつれの配布、量子状態転送能力」をもちいたら当然（中継ノードを信頼しなくてよい）QKD も実装できるという一例に過ぎず、上節で述べたように量子インターネットによって様々な機能の獲得ができる。

3.2. 近未来の実装が期待されるアプリケーション

量子インターネットが稼働するともつれ交換を介した長距離もつれ共有や、それを用いた End to End での量子情報の送受信が可能となる。この前提を実現するためには、任意のノード（量子中継器）は 1 量子ビットの状態を準備・送信し、他のノードから受信した量子ビットの測定を行うことが求められる。しかし、黎明期には（主に量子メモリ開発の困難さから）もつれ純粋化の実装は困難で、通信距離や品質には大きな制限があるだろう。

十分な性能の量子メモリを持たない量子インターネットで運用可能なアプリケーションとして、信頼できないノードを介する QKD や、なりすましの可能性があるユーザと悪意のあるサーバのように**互いに信頼していない二者間**での認証プロトコル[16] やコインフリップ[17] などが提案されている。

これらのアプリケーションの運用だけでなく、経路選択などの自律運用プロトコルの整備・標準化もこの世代のネットワークにおける重要な課題となる。

3.3. 高規格なネットワークを必要とするアプリケーション

高品質な量子メモリが実現し、ノード上で量子情報を一定時間保持することが可能になると、もつれ純粋化を用いた高忠実度のもつれ共有が実現する。ネットワークが広帯域化・高品質化することで、私たちはより高度な量子インターネット・アプリケーションを利用することが出来るだろう。

たとえば**ブラインド量子計算プロトコル**を用いると、量子インターネットに接続された遠隔地の量子コンピュータを、その**所持者に計算内容・結果を知られることなく利用可能**になる。末端ユーザは簡易な量子状態送信デバイスや測定デバイスを用意すれば運用できることもあり[18]、生体情報や金融情報といった機密性の高いデータを用いる実用的量子計算での利用も期待される。

ネットワークパフォーマンスがさらに向上し、低帯域だがエラー訂正が可能な初期のフォールトトレラント量子ネットワークが実現すると、量子コンピュータ同士を接続し、計算空間の拡張を図る**分散量子計算**が運用可能になる。この技術は単体の量子コンピュータでは困難な、たとえば巨大数の素因数分解といった大量の量子ビットを必要とする計算において重要になるだろう。

3.4. ユースケースと市場開拓の必要性

ここまでに挙げた他にも、古典ネットワークの限界を超える性能の時間同期や超長基線電波望遠鏡、セキュアと不正防止を両立した量子投票などのアプリケーションに応用可能な多数のアルゴリズムが提案されている。社会実装を念頭に置くと、これらのアプリケーションが必要とするネットワークパフォーマンスや実用的ユースケースを精査する必要がある（例えば、多人数での運用を前提としたアプリケーションにおいて少数のユーザが帯域を使い切ってしまったり、投票所を必要としない量子投票が却って不正選挙を引き起こしてしまうかもしれない）。

また、量子インターネットの建設推進には社会需要が必須であり、民生用の簡易な量子デバイス・ガジェットや、ロバスト性の高い有用なアプリケーションなどの開発重要性

は年々高まっていくだろう。

4. 量子中継器実現に向けた最近の進展

次に、量子中継に関して具体的に研究開発が進んでいる物理系を見ていこう。ただし、ここでは最近提案されている全光量子中継[19]に関しては省略し、量子メモリを中継ノードに設置する方式を取り扱う。

量子中継に必要な要素として、光ファイバー伝送用通信波長量子もつれ光源、量子状態保存用量子メモリ（これら２つが一緒になったスピン-光子もつれ発生源などもある）の他に、量子メモリ波長と通信波長をつなぐ波長変換がある。また別途量子メモリ吸収線幅が 10MHz 程度以下といった狭いスペクトル領域にある場合、もつれ光源や波長変換励起レーザー、また場合によっては量子メモリ制御レーザーに周波数安定化を施さねばならない。これらの要素を用いて Sec. 2 で述べた量子もつれ交換と純粋化を行うことで、長距離高忠実度量子もつれ共有を目指す。もつれ純粋化に関して実用化は比較的遠い将来と考えられているが、もつれ交換による少数ノード間を介したある程度の高忠実度なもつれ共有は実現に近づいている。

本節では、さまざまな物理系を用いた量子メモリを中心に、量子中継器ネットワークの実現に向けた近年の進展を概観する。

4.1. 気体原子集団

2020 年に中国の J.W.Pan グループはフィールド実装された光ファイバ 22km、およびラボインストールされた光ファイバ 50km の距離で Rb 原子集団を用いた 2 量子メモリ間のもつれ生成に成功した[20]。原子集団メモリとのもつれ状態にある発生光子の波長は 795nm であり光ファイバ伝送で大きな損失を受けるため、発生直後に通信波長の 1342nm へと波長変換を施している。2 メモリの中間ステーションには超伝導単一光子検出器が設置されており、送られてきた通信波長光子を検出する (Meet-in-the-Middle 方式)。

4.2. ダイヤモンド

2020 年に米国ハーバード大の M.Lukin らのグループがダイヤモンド中シリコン空孔中心量子メモリをもちいたメモリアシスト測定器無依存量子鍵配送実験を成功させた[21]。この実験は、メモリ無使用のいわゆる Direct Transfer による鍵配送レートの上限を、量子メモリを使用することで超えた初の結果とみなすことができ、量子メモリ搭載中継ノードによる量子中継実装へ至る一つのマイルストーンとみなすことができる。ただし、この結果は量子鍵配送つまりランダム古典ビット列の共有であり、量子もつれ共有及びそれを用いた量子状態転送という量子インターネットの本来的な機能の達成とは言えない。

2021 年にオランダのデルフト工科大学の R.Hanson らのグループは、ダイヤモンド窒素空孔中心 (NV 中心) 量子メモリを用いた系で３ノード量子ネットワークを構築し、３者間もつれ生成および中央ノードでのもつれ交換に成功した[22]。ここで生成されたもつれは $|01\rangle + e^{i\phi}|10\rangle$ であり（どちらかにのみ１励起されている形式のもつれ)、位相差 ϕ は２つのノードと中間点の測定器への光路差に対応している。NV 中心からの発生光子は、電子スピンともつれた電子スピン-光子もつれであり、光ファイバ伝送の後、中央の単一光子検出器で検出される。１光子検出が起きると、左右どちらのノードにあるダイヤモンドから発生したかの重ね合わせにあるもつれが得られる。この成果は量子もつれ交換を非同期に実施した初の結果であり、もつれの生成レート（正確には heralding rate）は $1/40s^{-1}$ であった。同グループからは 2022 年に、もつれ交換を経た非隣接ノード間でのテレポーテーション実証実験も報告されている[23]。

4.3. 捕獲中性原子・イオン

2021 年にドイツの G.Rempe らのグループは、光共振器内にトラップされた 2 つの Rb 原子を用いた中継操作の実験を行った[24]。中継ノードである１つの光共振器にトラップされた 2 原子から、それぞれともつれにある光子を順に発生させ、各光子を離れた 2 基のエンドノードに送る。各光子がエンドノードに届いた後、共振器内の 2 つの Rb 原子に対してベル測定を実施し、エンドノード間でのもつれ 2 光子の生成と、その 2 光子を用いた量子鍵配送に成功した。離れたエンドノードに設置された量子メモリ間のもつれではないが、この実験では捕獲原子間のベル測定に成功しており、この系の長所といえる。彼らは既に制御 NOT ゲートの実証もしており、これは中継ノードにおけるもつれの純粋化につながる成果である[25]。

また、Sr イオンを用いた 2 者間もつれ共有が英国のグループにより達成された[26]。各エンドノード内の Sr イオンともつれにある放出光子が、中継ノードのビームスプリッタで 2 光子干渉するもつれ交換操作により、Sr イオン同士のもつれ共有に成功した。長距離伝送に不向きな 422 nm の光子波長を使用した実験室内の短距離実験ではあるが、ベル状態忠実度 94 %、もつれ生成レート 182 s^{-1} というメモリ間もつれとして高忠実度、高レートの実証である。

4.4. 希土類添加物質

2021 年に通信レートの大幅増強を見据えた 2 つの成果がスペイン（H. Riedmatten らのグループ）および中国（G. C. Guo らのグループ）から同時に発表された。[27, 28] 使われた量子メモリは希土類添加物質（前者は Pr:YSO、後者は Nd:YVO4）である。希土類添加物は、希土類 4f 軌道電子の外部からの高い遮蔽効果を利用し、固体にも関わらず高いコヒーレンスをもつ性質がある。また、吸収スペクトルの不均一幅を光制御して時分割多重・波長分割多重能力を獲得できることによって、高いもつれ生成レートを可能にし、量子中継実現への有望なデバイスと期待される。実

験室内での短距離実証ではあるが、時分割多重性を利用し高いもつれの heralding rate（中国グループはおよそ 100 Hz、スペイングループは 1.4 kHz。しかし測定されたもつれレートは中国グループの場合 1 時間に 1 程度で、メモリの非効率なもつれ測定系によって低下) を達成した。これらの実験の特徴は、吸収型量子メモリを用いた点にある。吸収型メモリは、自動で heralding 信号となる光子生成はしてくれない。それが弱点とみなされてきたが、今回の実験では、光ファイバー伝送後のベル測定出力を heralding 信号として使うことで吸収型の弱点を回避した。スペインの実験では、連続波レーザー励起による時間任意性により、ある時刻においてはどちらか片方ノードでのみ 2 光子生成される。そうして中央のベル測定器に光ファイバー伝送後届き測定された後の、量子メモリ間でのもつれは 1 励起のもつれ $|\phi\rangle = (|01\rangle + |10\rangle)$ である（0 及び 1 は各量子メモリの励起数)。一方中国の実験では、パラメトリック下方変換はパルスレーザーで励起されている。この場合、中央ステーションに届く時間が同期されれば、2 ノードで 1 励起ずつの 2 光子もつれ $|\phi^+\rangle = |HH\rangle + |VV\rangle$ が生成される。

4.5. 多種物理系を用意する意義

ここでの概観は、すべての量子メモリを網羅したものではないが、有力なものをいくつか列挙した。これらの各量子メモリには各々の長所・短所がある。例えば希土類添加物質なら、多重性に優れる一方、もつれ純粋化へと進める展望が開けていない、一方で量子論理ゲート操作が発達している捕獲イオン系においては純粋化が現実的なものである。量子インターネットの構成要素としていずれか 1 種類の量子メモリのみが使用されるよりも、各々の特徴を生かした（物理層）ネットワークの構成や機能化がなされると、より早期の構築へとつながる可能性がある。例えば比較的近距離の複数ノード間では多重性を活かし希土類添加物質量子メモリを用いてもつれ生成レートを稼ぎ、もつれ純粋化が必要になる距離において捕獲イオン量子メモリへもつれ交換で渡すといったハイブリッド系も考えうる。また様々な物理系で近年 dynamical decoupling などを使用したコヒーレンス時間（メモリ時間）の向上があり、秒を超える系も多く出ている。これは（エンドノードでの超長期保存を考えず）量子中継操作が完了するまでの時間保存という観点からは、実用に近づいていることを示している。またいずれの系でも（信号 – 雑音比の波長依存性があるとはいえ）波長変換システムを組み合わせることによるメモリ波長 – 通信波長変換が可能である。

4.6. もつれ共有の反復レート向上を目指して

量子中継の実現スキームは、量子メモリ搭載型の系に限っても一通りでは無い。たとえば上述した希土類メモリの 2 研究は（スペインは 1 光子干渉であるが）Meet-in-the-Middle 方式であり、光源が量子メモリのすぐ側にある。Midpoint-Source 方式であれば、光子準備はシステム反復レートを高くできる量子もつれ（光子対）源に任せ、比較的反復レートが遅くなりがち（初期化、励起など多数のシークエンスによって時間がかかることが多い）な量子メモリは光子が送られてくるのを待つ。これにより 2 励起ベル状態生成レートを向上させるのに有利と考えられる[3, 29]。ここで量子メモリは到達（したかもしれない）光子とのベル測定をローカルに行い、その成否がすぐわかるため、失敗した場合は即座に次の光子到来に備えたメモリ準備を行える。一方で、Meet-in-the-Middle 方式の場合には中央まで光子が到着したかどうかの heralding 信号が長い光ファイバー通信路を往復する時間を待たねばならず、時間がかかる。従来の研究[3] では、量子メモリに spin-photon もつれが仮定されていたが、量子メモリが発光型（メモリ内スピンともつれにある光子発生）の場合だけでなく[3]、吸収型メモリを用いた場合でも Midpoint-Source 方式のもつれ生成レートの方が高くなり得ることが示された[29]。しかしこの場合は、吸収型のため heralding 信号を発生しないので別途、光子到来検出システム[30] など用意する必要があり、原理的に中継のもつれ生成レートを向上させられるとはいえ、もう一つ克服すべき技術が生まれることになる。

4.7. もつれ純粋化に向けた最近の進展

2017 年にオランダの R.Hanson らによるダイヤモンド量子メモリ間のもつれ純粋化実証が報告された[31]。純粋化操作後に得られたベル状態の忠実度は 0.65 であった。実用的に十分な忠実度とは言えないが、量子メモリ間もつれにおいて得られた強い結果である。

また、2021 年には中国の G.C.Guo らによる 11km の光ファイバ伝送後のもつれ純粋化実証として、純粋化前のベル状態忠実度 0.771 から純粋化後の忠実度 0.887 を得たとの報告が出されている[32]。

4.8. 都市間ネットワークや人工衛星量子通信の進展

都市間でのオンデマンドな量子もつれ交換を目指して、オランダの QuTech はデルフト-ハーグ-ライデン-アムステルダムの 4 都市に設置されたリピータノードの循環型ネットワークの構築を進めている。また、同ネットワークをブラウザ上でシミュレートできる Quantum Network Explorer も公開されている[33]。

人工衛星量子通信も進展しており、中国の J.W.Pan らのグループが人工衛星内で発生したもつれ 2 光子を地上 1000 km 以上離れた地点に配布し、もつれ共有に成功している[34]。将来的には、複数人工衛星を量子中継でつなぐ手法も提案されており[35, 36, 37]、その際には地上の光ファイバ量子中継ネットワークに加えて、量子メモリ搭載衛星中継器を含むハイブリッド系へと量子インターネットが進展する可能性も有る。

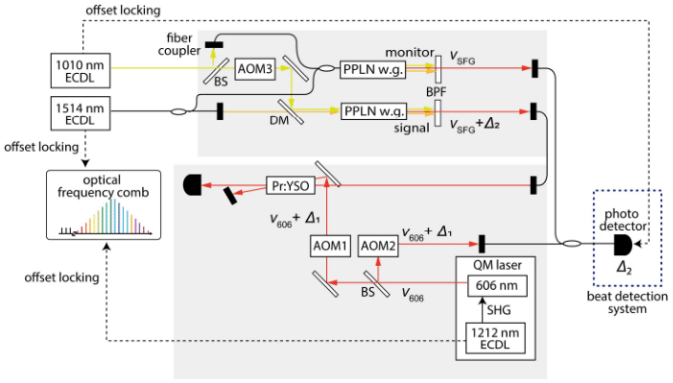

図 4　通信波長光子と希土類量子メモリ結合実験。通信波長光子が光ファイバー伝送後中継ノードにて波長変換後、量子メモリへ結合する。メモリの狭い遷移周波数と安定結合し続けるため、光周波数コムへの安定化システムを構築した。文献[40] から引用。

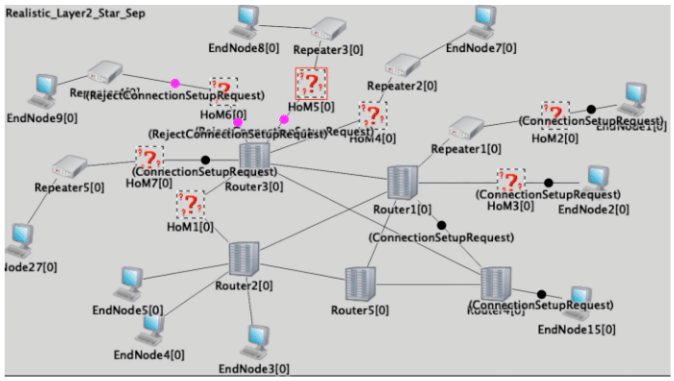

図 5　QuISP の実行画面。150 ノードを超えるネットワークのシミュレーションが実行可能。

5. 最近の著者らの取り組み

最後に、量子インターネット建設に向けた我々の取り組みを紹介する。

5.1. 長距離光ファイバーを介した光 - 物質量子結合

我々は現在、通信波長量子もつれ生成および 10km 光ファイバ伝送後の中継ノードにおける量子メモリ波長変換に成功している[38]。また、量子メモリ間もつれ生成レート向上にむけた波長分割多重度を高めるため、Pr:YSO 量子メモリ波長チャンネルを多数生成している。Pr:YSO の準位構造に起因する限界のため 1 チャンネル帯域は狭く（10MHz 以下）、関わる光の周波数安定化が必要である。そのため我々は光周波数コムを用いた通信波長 2 光子源、波長変換励起レーザー、量子メモリ制御レーザーの一括制御システムを提案実証している[39, 40](図 4)。

このシステムによって、最近我々は通信波長 2 光子源を 10km 光ファイバ伝送後、Pr:YSO 量子メモリへの結合に成功した (論文投稿中)。2 光子源は基本的に Midpoint-Source 方式対応だが、Meet-in-the-Middle に適した非縮退発生も可能であり、その場合波長変換デバイスを別途必要としないメリットが生まれる。このシステム開発を進め、多重化メモリによるもつれ通信レート向上を生かした中継実証へと進む計画である。

5.2. 大規模量子インターネットシミュレータの開発

量子インターネットを見据えたプロトコルやアーキテクチャの設計は、将来の量子自律システムを構築していく上で非常に重要である。我々の開発している QuISP[41] (a Quantum Internet Simulation Package) はそれらの挙動や有用性の検証が可能な、大規模ネットワークシミュレーションに特化した量子インターネット・シミュレータである。ユーザは設定を変えることで、アプリケーションの運用環境やルーティングといったさまざまな状況をシミュレーションすることが出来る。

QuISP は一般的な密度行列を用いたシミュレーションとは異なり、状態に関するリアルタイムな情報を持たず、エラーの伝播を適切にトラッキングすることで、表現可能なエラーの数を減らすことなく大規模な量子ネットワークシミュレーションを実現している。光子の位置や古典通信の遅延なども設定・シミュレート可能なため、提案プロトコルの検証やネットワークパフォーマンスの計測などの実験により、量子インターネットが抱えるであろう新たな問題の発見・解決や、より良いアーキテクチャへの提案に貢献していくと考えられる。

また、柔軟な拡張を目指してオープンソース開発に移行しており、エラートラッキングだけでなく、Graph State Stabilizer や Density matrix を用いたシミュレーション機能の実装も予定されている。

5.3. 量子インターネットのセキュリティ問題

量子インターネットでは、情報理論的に安全性が保証された量子暗号プロトコルやアルゴリズムの運用が想定される。しかし、第三者が管理する量子中継器や量子自律システムと相互接続されている状況でも常に安全なのだろうか?

ネットワークに悪意のある量子中継器が存在する（あるいは攻撃者に管理権限が奪われている）場合、量子情報への直接的な攻撃は不定期な量子トモグラフィなどによって検知しうる。しかし、我々はネットワークの構成によっては攻撃者の量子中継器の特定が困難であり、また、攻撃者が検知プロトコルを逆用することで、ネットワークパフォーマンスの低下や分断が発生することを示した[42]。我々は上記の乗っ取り攻撃による影響解析だけでなく、量子インターネットへの攻撃手段や対象をモデル化し、侵害されるセキュリティーの要素（可用性、機密性、完全性）と共に分類した[43]。例として、量子複製不可能定理は機密性の保持に有益だが、ネットワークへの過剰な負荷による量子情報喪失を狙った DoS 攻撃のリスクを増大させる。また、量子中継器内の古典情報を処理する部位は古典的なネットワークシステムと多くの脆弱性を共有しているだろう。

このように量子インターネットのセキュリティは量子情

報の機密性によって完全にカバーされるものではない。量子中継器やプロトコルは現行のインターネットと同様に、脅威を可能な限り洗い出した上で設計しなくてはならず、また新たな攻撃手法に随時適応させていく必要があるだろう。

5.4. 量子インターネットタスクフォースの設立

2019 年には量子インターネット設計に必要な幅広い領域の研究者が集う量子インターネットタスクフォース (QITF) が設立された。遠くない将来における量子インターネット・テストベッドの建設に向け、ハードウェアやモジュール間インターフェイスなど包括的な設計を進めている。

上で述べたような量子中継を構成する候補物理系は様々あり、量子ゲート操作に適した系、多重化通信に適した系など長所が異なる。将来的に量子インターネットにおいては、一番基層の物理レイヤにおいても、様々な物理系からなるハイブリッドシステムとなり、長距離化、高スループット、高忠実度、などの量子インターネットが満たすべき性能を獲得する方向へ進むことが期待される。そのために様々な研究者の集合によって量子インターネット・テストベッドを構築し、頑強な量子インターネットへと向けた研究開発を加速させていく必要がある。

最後になりますが、量子インターネットの研究開発プロジェクト推進に関して、日頃協働・協力いただいている QITF ボードの永山翔太氏（代表）、生田力三氏、佐々木寿彦氏、高橋優樹氏、逵本吉朗氏、山崎歴舟氏、および武岡正裕氏をはじめとするメンバーに感謝します。

参考文献

1) H. -J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
2) T. Morimae, and K. Fujii, Phys. Rev. A **87**, 5 (2013).
3) C. Jones, et al., New J. Phys. **18**, 083015 (2016).
4) L-M. Duan, et al., Nature **414**, 413 (2001).
5) Y. Wu, J. Liu, and C. Simon, Phys. Rev. A **101**, 042301 (2020).
6) A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg, Phys. Rev. Lett. **104**, 18 (2010).
7) L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, Phys. Rev. A. **79**, 032325 (2009).
8) Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, New J. Phys. **15**, 2 (2013).
9) S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Phys. Rev. Lett. **112**, 250501 (2014).
10) https://irtf.org/qirg
11) M. Pompili, et al., arXiv:2111.11332 [quant-ph](2021).
12) S. Wehner, D. Elkouss, and R. Hanson, Science **362**, 303 (2018).
13) International Conference on Computers, Systems and Signal Processing (1984)
14) A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
15) Y. -A. Chen, et al., Nature **589**, 214 (2021).
16) I. Damgaard, et al., TCS **560**, 12 (2014).
17) D. Aharonov, et al., Proc. of STOC00 (2000).
18) A. Broadbent, J. Fitzsimons, E. Kashefi, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, p.517-526 (FOCS 2009)
19) K. Azuma, K. Tamaki, and H. K. Lo, Nat. Comms. **6**, 6787 (2015).
20) Y. Yu, et al., Nature **578**, 240 (2020))
21) M. K. Bhaskar, et al., Nature **580**, 60 (2020).
22) M. Pompill, et al., Science **372**, 259 (2021)
23) S. L. N. Hermans, et al., Nature **605**, 663–668 (2022)
24) S. Langenfeld, et al., Phys. Rev. Lett. **126**, 230506 (2021).
25) S. Welte, et al., Phys. Rev. X **8**, 011018 (2018).
26) L. J. Stephenson, et al., Phys. Rev. Lett. **124**, 110501 (2020).
27) D. Lago-Rivera, et al., Nature **594**, 37 (2021).
28) X. Liu, et al, Nature **594**, 41 (2021).
29) D. Yoshida, et al., Int. J. Quant. Inf. **18**, 2050026 (2020).
30) N. Sinclair, et al., Nat. Comms. **7**, 13454 (2016).
31) N. Kalb, et al., Science **356**, 928 (2017)
32) X-M. Hu, et al., Phys. Rev. Lett. **126**, 010503 (2021)
33) `https://www.quantum-network.com/`
34) J. Yin, et al., Nature **582**, 501 (2020).
35) K. Boone, et al., Phys.Rev. A **91**, 052325 (2015).
36) M. Gündogan, et al., npj Quantum Inf **7**, 128 (2021).
37) C. Liorni, H. Kampermann, and D. Bruß, New J. Phys. **23**, 053021 (2021).
38) K. Niizeki, et al., Comms. Phys. **3** 138, (2020).
39) T. Miyashita, et al., Jpn. J. Appl. Phys. **60** 122001 (2021).
40) K. Mannami, et al., Opt. Exp.**29**, 41522 (2021).
41) `https://aqua.sfc.wide.ad.jp/quisp_website/`
42) T. Satoh, et al., IOP QST. **3** (3), 034008 (2020)
43) T. Satoh, et al., IEEE TQE. **2** 1-17 (2021)