サイバースペースの限界に挑戦する量子情報科学

研究室紹介

山　本　　俊*

Quantum information science: A challenge toward a forefront of Cyberspace

Key Words：Quantum information, Quantum computer, Quantum network, Quantum Cyberspace

はじめに

2025年には大阪・関西万博が開催される。この原稿の執筆時点では、パビリオン建設の遅れや建設費用の高騰により開催が危ぶまれているが、最終的には予定通りに開催されると信じる一人である。約50年前に大阪で開催された日本万国博覧会（1970年）は、アジア初の万博であった。4年前の1966年に開催が決定され、政府からの総事業費は6500億円にのぼり[1]、大成功であった。当時は、世界第2位の経済大国である。現在の大阪大学吹田キャンパスも、この万博と並行して整備され、大きく発展している。当時の多くの関係者の努力によって作り上げられたレガシーを再認識し、改めて深く感謝したい。さて、2025年は、量子情報科学にとっても重要な節目の年であり、国連が宣言する国際量子科学技術年（International Year of Quantum Science and Technology）となる予定である。これは、その100年前にあたる1925年に、ハイゼンベルグによって発見された量子力学の数学的な記述法（行列形式）により、量子的な現象が予測可能になったことを記念するとともに、その後に、現代の様々なテクノロジーを生み出した量子科学技術の発展を祝うものである。この量子力学によって生み出されたテクノロジーを挙げるときりがない。トランジスタが生み出され、現代のコンピュータが実現し、それを動作させるプログラミング言語も発明された。メーザーが発明され、レーザーが生み出された。1970年の万博で披露されたテレビ電話や携帯電話は、これらの発展のおかげである。アメリカでは前年の1969年に、世界初のインターネットであるARPANETの実証実験が行われ、アポロ11号を月面着陸させている。このとき持ち帰られた「月の石」が万博で披露されている。これらはコンピュータなしでは実現していないし、量子力学の発展が大きく寄与している。

このようにまとめてみると、現代のテクノロジーの根源は、私が生まれる前にはすでに生み出されている。私が生きている現代社会は、それらが発展し、世界中で利用されることで、形作られている。情報技術が発達し、コンピュータとインターネットの融合により、サイバースペースの利用が急速に進展した時代である。現在、これらの元になっている量子技術は「量子1.0」と位置づけられるようになってきている。それは、これまで利用されていなかった「量子2.0」と位置づけられる量子技術が誕生し、第二次量子革命が始まっているからである。「量子2.0」では、量子力学に固有の性質である「重ね合わせ」や「量子もつれ」が利用され、量子コンピュータ、量子通信・ネットワーク、量子センシングなどの情報科学と融合した量子情報科学が発展してきている[2]。

量子コンピュータの発端は1981年に開催された「Physics of Computation」と題された国際会議におけるファインマンの講演とされている。それ以前には、1970年のウィーズナーの量子マネーがあり、その後の1984年にベネットとブラサードの量子鍵配送の提案（BB84）がある。これにより量子通信・ネットワークの研究が始まる。1994年には有名なショアのアルゴリズムが提案され、素因数分解が量子コンピュータによって効率的に解かれることが明らかにされた。量子コンピュータの研究が一気に加速する契機となる。私が研究を始めたのは、そのよ

* Takashi YAMAMOTO
1975年1月生まれ
総合研究大学院大学　先導科学研究科
光科学専攻博士後期課程（2003年）
現在、大阪大学　大学院基礎工学研究科
物質創成専攻　教授　博士（理学）
大阪大学　量子情報・量子生命研究センター（QIQB）　副センター長（兼任）
TEL：06-6850-6445
E-mail：yamamto.takashi.es@osaka-u.ac.jp

うな時期であった。1993年に提案された量子テレポーテーションの実現方法を当時の指導教員と議論をし、実験の準備を始めていた。その矢先、1997年のNature誌に量子テレポーテーション実現の論文が掲載されたことを強く記憶している。Nature誌を初めて読んだのもこのときであった。その後、博士後期課程に進学し、「量子もつれ」による量子ネットワークによって、量子コンピュータを実現する提案や「量子もつれ」の蒸留の提案を行い、幸運にも在学中にその実現をNature誌に掲載することができた。

現在は、内閣府・JSTのムーンショット型研究開発事業ムーンショット目標6「2050年までに、経済・産業・安全保障を飛躍的に発展させる誤り耐性型汎用量子コンピュータを実現」（PD：北川 勝浩）[3]の下で、「ネットワーク型量子コンピュータによる量子サイバースペース」プロジェクトのPM（プロジェクトマネージャー）を務めている[4]。量子コンピュータをネットワーク化し、現在のスーパーコンピュータのように大規模化し、任意の量子アルゴリズムを動作させるための要素技術開発を行っている。量子コンピュータと言っても、超伝導、光、イオン、原子や半導体などの様々なハードウェアによって研究開発が行われ、どれが最も有望かを現状で見極めるのは難しい。また、先にゴールに辿り着いても、その優位はいつまで続くかわからない。すべてのハードウェアで実現し、適材適所で使われるシナリオも十分にありえるのである。そのため、すべてのハードウェアに対して、ネットワーク化するための様々なタイプの要素技術開発を行っている。各ハードウェアに特化した技術もあれば、共通の技術もある。それらのベストミックスを探りながら研究を進めており、挑戦的かつ面白い。プロジェクト全体の詳細は、別の機会にするとして、ここでは我々の研究室での活動に限定して、紹介したい。

原子量子コンピュータ

我々の研究室では、中性原子を量子ビットとした、原子量子コンピュータに注目して研究開発を行っている。中性原子を一つ一つ真空中にトラップするために、レーザーを使った光ピンセットのアレイを使う。量子ビット間の演算は原子の高い励起状態（リドベルグ状態）を用いるため、その励起のためにもレーザーを用いる。原子量子コンピュータと言っても、制御の殆どはレーザーであり、一部、マイクロ波による制御がある。原子量子コンピュータの特徴は、約10000個程度の原子を2次元アレイ状に整列できる可能性が示唆されており、ムーンショット目標に掲げている100万量子ビット規模に最も近いことである。ただし、その他のハードウェアと同様に課題も山積しており、十分な開発期間が必要である。我々の研究室では、最初のテストとして7×10サイトの原子トラップを作成して、整列させることに成功している。また、トラップビームアレイは任意の平面形状を作成できる。例えば、図1のように大阪大学のシンボルマークを原子で描くこともできる。ボーア模型でもよく知られているように、原子一つ一つは、励起することで、光子を発生する。それを観測することでトラップされた原子の存在がわかる[5]。適切な励起準位を選択すると、原子は励起状態から複数の基底状態に遷移することが可能になる。選ばれた基底状態により発生する光子の状態が決まるため、励起状態から基底状態に遷移する際に、「重ね合わせ」になっており、遷移した基底状態と発生した光子の間に「量子もつれ」が生じる。まさに「量子2.0」技術である。この光子との「量子もつれ」を発生する実験を現在行っているところである。

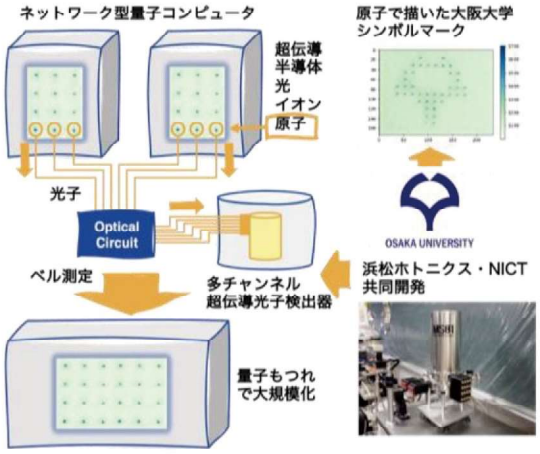

図1　ネットワーク型量子コンピュータの概念図

ネットワーク型量子コンピュータ

この原子と光子の量子もつれを利用して、量子コンピュータを繋いだネットワーク型量子コンピュータが可能になる（図1参照）。ある量子コンピュータのシステムと別の量子コンピュータのシステムを

2つ独立に利用しても量子コンピュータとしての能力は1つのシステムを利用する場合とほぼ変わらない。（量子コンピュータ内に量子ビットを一つ増やす方が遥かに量子コンピュータとしての能力が勝る。）一方、量子コンピュータ同士を「量子もつれ」によって繋ぐと大きな1つの量子コンピュータとなる。量子コンピュータの大規模化は、このようにモジュール化された量子コンピュータを「量子もつれ」によって繋ぐことによって可能になる。原子量子コンピュータのネットワーク接続は、原子と量子もつれにある光子を使って行う。それぞれの原子量子コンピュータからの光子をまとめて、ベル測定と呼ばれる測定を行う。このベル測定によって、一方の光子の状態を他方の原子量子コンピュータへ送ることができる。これは、前に述べた量子テレポーテーションである。量子テレポーテーションは、「量子もつれ」を同時に送るため、原子量子コンピュータ同士が「量子もつれ」で繋がることになる。このベル測定には、光子検出器が必要となる。原子1つ1つに対して行うために、高効率かつ多数の光子検出器が必要である。プロジェクトでは、現在、最も優れた性能をもつ超伝導光子検出器の開発をNICTおよび浜松ホトニクスが担当し、国産超伝導光子検出器の開発に成功している。

量子通信・ネットワーク

上記のように、モジュール化された量子コンピュータを繋ぐと量子ネットワーク（量子インターネットとも呼ばれる）が形成される。特に、長距離量子通信によって量子ネットワークを形成すると、セキュア通信への応用が期待できる。「ムーンショット目標6」のゴールである誤り耐性型汎用量子コンピュータが実現すると、現在、インターネット上で利用されているRSA暗号が破られることが知られている。アメリカではこれに対処する大統領令「Quantum Computing Cybersecurity Preparedness Act」が発布[6]され、耐量子暗号（PQC）への移行が示されている。PQCの候補として挙げられている暗号方式は、インターネット上で実装可能であり、量子コンピュータによって破られることが、今のところ示されていない。しかし、後々までセキュアであるかはわからない。アルゴリズムの進化や技術の進歩によって、破られる危険性も指摘されている[6]。これは、PQCがコンピュータの計算能力に依存した安全性だからである。

一方、量子ネットワークを利用することで、量子暗号と呼ばれる物理法則に基づいた暗号方式を実装することができる。前述のように、量子ネットワークは「量子もつれ」によって繋がっている。この「量子もつれ」をそれぞれの量子コンピュータ上でプロトコルにしたがって測定すると、第三者が原理的に予測できない秘密の乱数列（秘密鍵）を共有することができる。プロトコルの詳細には立ち入らないが、第三者が原理的に予測できないことは、「量子もつれ」の以下の性質によるものである。①測定結果はランダム、②双方の測定結果は同じ、③完全な相関は二者間のみで成立（モノガミー性）。これらの性質は、どんなに計算能力が高い量子コンピュータであっても破ることができない原理なので、究極のサイバーセキュリティを提供できる。完全なセキュリティを実装できることが望ましいが、一般にはリスクを適切に評価できればよいため、安全性理論によって、不完全な量子ネットワークの安全性を適切に評価している。セキュア通信に限った用途であれば、量子ネットワーク上の量子コンピュータには、誤り耐性や汎用性といった高レベルなものは求めない。例えば、1つの量子ビットを測定するようなものでもよい。1984年に提案された最初の量子暗号のプロトコル（BB84）では1つの量子ビットを一方から他方へ送信するものであり、実装の容易さから現在でもその方式が主流となっている。BB84では「量子もつれ」を利用していないが、第三者からみて、「量子もつれ」を利用したものと区別がつかないため、同様の安全性が可能となっている。一方、実際に「量子もつれ」を配るプロトコルでは、量子ネットワークを利用して、量子中継プロトコルを実装可能であり、長距離の量子暗号が可能となる。

実際に、現在の光ファイバー通信を利用して「量子もつれ」を配るために、これまで、様々な研究を行ってきた。光子と光子の「量子もつれ」を効率的かつ広い波長帯で発生させる光源の開発を行い、現在では光ファイバー通信波長帯において、1000を超える周波数モードの光源となっている。また、量子ネットワークにおいて必須の光子の周波数変換器（量子周波数変換器）を開発し、「量子もつれ」を壊さずに望みの周波数に変換できるデバイスを開発した。さらに、原子の量子メモリと光子の「量子もつれ」に対して適用し、原子量子メモリが光ファイバ

ー通信で動作可能であることを示した。現在は、この手法を原子量子コンピュータに適用して、量子ネットワーク化を目指している。

このような量子ネットワークの社会実装を進めていくためには、実験室だけではなく、敷設ファイバーを利用したフィールド実証実験が必要である。現在、JR西日本光ネットワーク株式会社と協力して、新幹線に敷設された光ファイバーを利用した「量子もつれ」配送の実証実験も行っている（図2参照）。

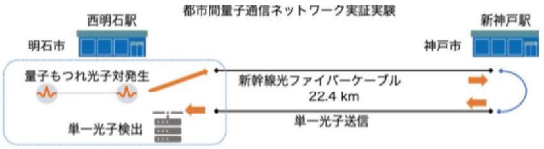

図2　新幹線光ファイバーケーブルを用いた実証実験

おわりに

1935年はアジア初のノーベル賞受賞者である湯川秀樹博士が大阪帝国大学で受賞対象となる中間子論文を執筆した年であり、2025年にはその90周年を迎える。1935年当時、湯川秀樹博士はすでに量子力学が広範な科学技術に拡がっていくことを明確に認識されていたようである[8]。量子情報科学という形の発展を予見されていたかは知る由もないが、想像の範疇を超えるものではないのではないかと推察する。量子情報科学に関するノーベル賞としては、2012年に「重ね合わせ」に関連する単一量子系の制御に対してアロシェとワインランドに物理学賞が授与され、2022年に「量子もつれ」に関連して、Bellの不等式の破れの実験にクラウザー、アスペ、ザイリンガーに物理学賞が授与されている。徐々にノーベル物理学賞の新たな構成分野となっており、さらに増加するだろう。日本からの受賞の可能性も十分に出てきている。量子情報科学の適用範囲の広さを考えると、今後は物理学賞の域を超えた受賞もあるだろう。20世紀に誕生した量子力学が21世紀の現代の発展を築いているように、量子情報科学が発展し、今後の人類の発展に大きく寄与することは確実である。我々が研究開発を行っている「ムーンショット目標6」では、2050年を目処に、誤り耐性型汎用量子コンピュータの実現を目指している。目標設定時期からの技術進歩が目覚ましく、前倒しの空気も出てきている。実現後には、量子情報科学を自在に制御できるようになっていくだろう。本稿で紹介してきたように、現在のサイバースペースに量子コンピュータや量子ネットワークが加わった量子サイバースペースが誕生していても全く不思議ではない。さらにその先に、何があるのかは、想像すらできないが、我々の子供や孫の世代まで探求し続けることができることは確実である。私の研究人生は、そこまで長いものではないが、「ムーンショット目標6」の成否を見届けられる程度にはある。長く大変な道のりのように見えるが、これまでのように好奇心をもって楽しんで挑戦していきたいと思う。

参考文献

1) 阪神高速ショートストーリー　第7話　万国博覧会の成功へ、供用延長を一挙4倍：https://www.hanshin-exp.co.jp/50th/short-story/past/story07.html
2) 山本俊，藤井啓祐，根来誠，山下眞，市川翼，野口裕信，町田尚子，松岡智代，藤田維明：量子情報技術，国立国会図書館科学技術に関する調査プロジェクト2021報告書，調査資料2021-6（2022）
3) ムーンショット目標6　2050年までに、経済・産業・安全保障を飛躍的に発展させる誤り耐性型汎用量子コンピュータを実現：https://www8.cao.go.jp/cstp/moonshot/sub6.html
4) 「ネットワーク型量子コンピュータによる量子サイバースペース」プロジェクト：https://qcnqc.jp/
5) 浜松ホトニクス アプリケーション＆事例集 量子技術：https://camera.hamamatsu.com/jp/ja/application_and_case_study/quantum_technology.html
6) H.R.7535 - Quantum Computing Cybersecurity Preparedness Act：https://www.congress.gov/bill/117th-congress/house-bill/7535/text
7) Renato Renner and Ramona Wolf: Quantum Advantage in Cryptography, AIAA Journal Vol. 61, No. 5, 1895 (2023).
8) 細谷裕，湯川秀樹博士と大阪大学―ノーベル賞はかくして生まれた，大阪大学出版会（2021）