科学技術・学術審議会　先端研究基盤部会
量子科学技術委員会

量子情報処理・通信（うち量子通信・暗号）に係る議論(H28.6.20、第4回)の骨子案

H28.8.25

研究動向

○　量子通信は、量子力学的な効果を通信に応用したもので、通信の大容量化・低電力化が可能になると期待されている。量子暗号も、量子力学的な効果を用いてセキュリティの高い通信を行う技術であり、現在、私たちが日常的に行っているネットショッピング等において情報を守っている暗号と比べ、より安全性の高い通信が実現できるようになると期待されている。

○　量子通信は1960年代のレーザーの発明とほぼ同時にコンセプトが生まれ、量子暗号は1980年代に最初のプロトコルが発表された。1994年に米国の研究者であるピーター・ショアが、量子コンピュータが実現すると主な暗号はすべて破られてしまう、という理論を発表したことで、量子通信・暗号は各国で国家戦略として進められ、近年においても、欧米政府や企業、中国等が大規模ネットワーク形成や中長期的観点からの投資に積極的に取り組んでいる。

○　現在のデジタル通信が電気や電波、光による「0」か「1」の符号で送られる信号を受信し、誤り訂正処理をすることで必要な情報を伝送しているのに対し、量子通信では、受信側で複数パルスを重ね合わせ状態に変換しながら量子コンピューティングによる処理を行うことで大容量・低電力通信を可能とする。

○　量子通信において、通信距離を伸ばすためには量子中継が必須である。これには、量子テレポーテーションや量子メモリといった従来とは全く異なる新たな技術も含まれており、それを実現するための素子として、ダイヤモンドＮＶセンタが、現時点で研究が進んでいる代表例として挙げられる。

○　現在一般的に使われている暗号は、素因数分解などの活用により、解読に膨大な時間がかかるようにして安全性を高めている一方、量子暗号は、「量子状態は観察されると壊れてしまう」という不確定性原理と呼ばれる性質を利用しているため、盗聴が確実に検知でき、理論上いかなる技術でも破れない高度な安全性の実現が可能となる。

○　量子暗号を実現する方法の一つとして研究開発が主に進められているのが量子鍵配送

（QKD）技術で、伝送したい情報を暗号化・復号するための鍵を、量子力学的な効果により情報の送信者と受信者だけが共有できるように配送するものである。BB84 と呼ばれるプロトコルが、現時点で研究が進んでいる代表例として挙げられる。

（量子通信）

○　量子通信における受信過程での重ね合わせの原理を用いた信号識別性の向上には、量子コンピューティングによる超並列計算が必要であり、量子コンピューティングに必要な要素技術の進展とともに今後も発展が期待される。

○　量子中継は量子通信の長距離化に必須の技術であり、通信の中継を絶対的に安全なものにできる。量子中継を実現する基盤技術は量子もつれスワッピングであるが、実現化が進められている物質系の中でも、情報を数秒以上保持できる量子メモリであって、かつ極低温を必要としないダイヤモンドＮＶセンタが圧倒的に優位である。

○　量子中継の実現には量子もつれの活用が必須であるため、量子もつれの活用を実現化する素子の開発と小規模集積化（注６）が次のマイルストーンと考えられる。また、量子通信は量子暗号を含め、ワイヤレスネットワーク技術等との融合が今後の方向性であると考えられる。

（量子暗号）

○　量子暗号技術の一つである BB84 方式は、光子１個で１ビットの情報を送ることにより盗聴困難性を保障するものであり、現時点で最も研究が進んでいる。現在の性能としては、通信距離は光子が届く距離に制限を受けるため約 100km、その際の通信容量は約 1kbps である。

○　我が国においては 2001 年以降、産学官連携プロジェクトや ImPACT を通じて、量子暗号方式の実用レベルの技術開発やテストベッドを用いたネットワーク上における安全性実証試験、新しいネットワークアプリケーションの開発を進め、世界をリードしてきた。現在は6～8ノードの都市間ネットワークでの暗号プロトコルの安全性保証が堅実に進められているところであるが、市場開拓までには至っていない。

○　欧米ではベンチャー企業が QKD 装置を販売しており、性能の面では我が国に及ばないが、研究機関を対象として販売するビジネスモデルを構築している。一方で、大型国家プロジェクトでは基礎研究に軸足を置いていると考えられ、実用化への具体的戦略はあまり読み取れない。中国は総距離 2000km の QKD ネットワークを現在構築中であり、この大規模量子暗号ネットワークを基にした標準化戦略を推進されるおそれがある一方で、大規模ネットワークにおける暗号プロトコルの安全性保証の手法は不透明である。

○　量子暗号は通信距離と通信容量に原理的な限界があることが分かってきており、大規模ネットワーク化には現在、50km 程度で中継する方法がとられている。その中継点には盗聴者を物理的に侵入させないという古典的手法がとられており、理論上安全な量子中継技術の確立が今後のマイルストーンと考えられる。

（各アプローチの概観）

○　量子通信は量子暗号を一部含むような研究に進展してきているが、現在のインターネットを支えている暗号技術である公開鍵暗号が１対千万規模での電子署名を実行しているのに対し、量子通信、量子暗号、量子中継は現在１対１のプロトコルであるなど、実現できている機能はまだ限られている。今後は情報理論や暗号理論、光ネットワーク技術、ワイヤレスネットワーク技術と融合させ、新しい技術体系に移行する方向性と、量子中継を核とした技術の確立が重要である。

○　QKD は非常に高い安全性を実現するが、利便性や速度、距離、コストの面を犠牲にせざるを得ない。そのため、衛星と地上間のレーザー光通信のように伝送速度を優先する必要がある場合には、セキュリティはある程度犠牲にし、電波通信で取り扱われつつある物理レイヤ暗号と量子暗号を融合するなどの新分野の技術が期待されている。

○　量子中継のための量子テレポーテーションに成功している物質系は、ダイヤモンドＮＶセンタの他、トラップイオン、半導体量子ドット、超伝導量子回路等があるが、いずれも低温での動作が必要な点が不利である。ダイヤモンドＮＶセンタは、室温でも量子性が確認できるほど量子性に優れ、将来的には集積化も期待できるため、世界的に注目されている。

○　量子テレポーテーションは、半導体量子ドットによる物質系では初めて 2013 年に 5m の距離で実証され、ダイヤモンドＮＶセンタは 2014 年に 3m の距離で実証された。現在は実験室内の数 m での実証試験の時代から、km 単位での実証試験に移りつつある。国内では、発光と吸収のメカニズムを組み合わせて、距離が伸びても伝送レートが低下しない方式なども実証されており、今後も新しいアイデアの開拓が期待されている。

<u>日本の強み・課題</u>

○　量子通信・暗号において我が国は、理論研究、基礎研究、ネットワーク技術実験で世界を牽引してきた。これは、光工学を含めた物理学、情報工学の強みがある上で、長年に亘る連綿とした基礎研究や産官学連携の取組があってこその成果と考えられる。

○　情報理論や暗号理論、光ネットワーク技術、ワイヤレスネットワーク技術といった異分野との融合についての理論研究や基礎研究が我が国で開始されており、我が国の強みとなる期待や可能性がある。しかしながら、斬新なアイデアが重視されにくいこと、異

分野融合を率先するとともに基礎理論や実証実験、アーキテクチャを連携してシステムとしての方向性を組み上げる人材の欠如が課題である。

○　量子中継に必要なデバイスの集積化については、半導体技術や、ダイヤモンドの結晶成長技術など、これまで我が国で培われてきたものづくりの技術とデバイス・アーキテクチャなどの理論との融合による量子デバイス技術の活用・開発が鍵であり、我が国の強みとなる期待や可能性がある。しかしながら、国内で生産されたダイヤモンドのサンプルは国内では入手しづらい状況である。量子中継の研究は近年、海外で活発である一方、我が国では研究の短期的な成果が求められる傾向から活発とは言えないなど、我が国では画期的なアイデアが軽視される傾向にあるため、新しいアイデアは海外へ流れる傾向にある。また、光子検出器については海外製が国産技術よりも優れているため購入せざるを得ず、ボトルネックとなっている。

推進方策の検討にあたって考慮すべき点

○　現在の量子通信・暗号の技術体系に、情報理論や光ネットワーク技術、ワイヤレスネットワーク技術といった異なる分野を融合した技術体系に移行することで普及を促すことが必要（注７）。その際、量子暗号と数理暗号といったライバル分野や、周辺分野との連携関係も構築することが、短期的なニーズに応えながら、我が国の強みである理論研究や基礎研究を長期的に継続できる基盤となると考えられる。将来の潜在的ユーザーと対話しながら、段階的に、着実に量子技術を向上させる取組が効果的。

○　基礎理論や基礎研究における斬新なアイデアを重視し、それを国内で実証しやすい環境にすることも、想像をはるかに超えた量子科学技術の進化に対応するための取組として必要ではないか。

○　研究や実験など、各分野のレベルが高度化している中において、分野間の協力や融合努力を積極的に評価する視点や、基礎物理からシステム開発まで見通せる人材の育成が必要ではないか。

○　量子通信・暗号の分野に限るものではないが、欧州では研究者が国境なく往来して共同研究を実施しており、一国当たりの研究者数は限られていても、欧州全体として見ると多くの研究者が存在している。我が国の研究環境を改善することで、欧米との研究協力や共同研究を促進し、相乗的に技術を向上させるような国際化への対応が重要ではないか。また近年、中国やシンガポールといったアジアの研究グループも急速に力を付けてきている。アジアの研究グループとの積極的な研究協力や共同研究を含む研究ネットワークの構築についても考える時期に来ているのではないか。

以上

注記

（注６）

将来展望として、量子もつれを利用したネットワークにより、量子中継による量子通信速度の向上が期待される。

（注７）

例えば、超長期安全性を持つデジタルアーカイブシステムはニーズが高いが、現代暗号のみでは解決できない課題があり、それを量子技術と従来技術の融合により解決できる可能性がある。また、進展する移動体への成果展開や技術の取り込みを必要とする「空の産業革命」を支えるセキュア通信技術においては、いかに接続性の高いネットワークを構築するかが重要であり、情報理論、暗号、量子の新しい境界領域である物理レイヤ暗号が期待される。

物理レイヤ暗号

・正規通信路と盗聴通信路の性質が推定できる場合に、適切な符号化を行うことで安全かつ高効率にメッセージの伝送や鍵交換を行う暗号通信技術。

・通常、電波や光のワイヤレス通信（特に視野通信）を想定。

・どんな計算機でも解読できないことが証明できる（情報理論的安全性）。

用語解説

QKD　量子鍵配送(Quantum Key Distribution, QKD)

量子暗号技術の一つの手法。通信を行う二者間でのセキュア通信を保証するために、量子力学を用いてランダムな秘密鍵を共有し、それをもとに情報を暗号化・復号する。

テストベッド

大規模なシステム開発で用いられる、実際の運用環境に近づけた試験用プラットフォームの総称。

量子もつれスワッピング

二つのもつれ合った量子のペアがあるとき、それぞれのペアから一つずつ量子を選んでこの二つの量子の合同測定を行うと、残りの２つの量子がもつれ合う。

ダイヤモンドＮＶセンタ

ダイヤモンド格子中の炭素原子の置換位置に入った窒素（N）と、それに隣接する炭素原子が抜けてできた空孔（Vacancy）からなる複合不純物欠陥で、中心に電子スピンを持つ。ＮＶセンタに光を照射して返ってくる光の強度からスピンの状態を読み出すことができ、量子センサや量子ビットなどに応用する研究が進められている。