光を用いた量子情報処理の理論および実験的研究

研究室紹介

井元信之*，小芦雅斗**，山本　俊***

Quantum Information and Quantum Optics

Key Words： Quantum Information, Quantum Cryptography, Quantum Computing

1　はじめに

量子暗号、量子コンピューティング、量子テレポーテーション等をキーワードとする「量子情報処理」の研究が生まれ、育ちつつある。我々の研究室は理論と実験の両方にわたってこの分野の研究を行っている。その基盤となる量子光学の研究では、新しい量子状態の発生制御、エンタングルメント（量子相関）の発生制御、量子力学的に許される操作の特長や限界の解明、物質と光の間の量子情報転送に関する研究を行っている。スタッフである著者３名のほか、共同研究者であるワシントン大学（セントルイス）のオズデミル研究員ならびにNTT情報流通プラットフォーム研究所徳永裕己研究員と研究を進めている。

もともと井元はNTTにて光ファイバー通信の標準量子限界打破を目的とする量子ゆらぎ制御の研究を行っていた。その限りにおいて量子ゆらぎは「除くべき邪魔者」であった。しかし1990～93年にかけて数回の英国出張中に、量子コンピューティングを提案したDeutschとJozsaそれに量子暗号の発案者であるBennettとEkert等に会い、彼らの「量子ゆらぎの不思議な性質をプラスに利用する」スタンスに共鳴、帰国後その方向へ研究を広げることにした。

一方小芦は東大物性研究所で博士研究として、現在光の量子情報研究の標準テクノロジーとなっている「パラメトリック下方変換」を利用した量子ゆらぎ制御の研究を行っていた。1999年に総合研究大学院大学にて二人で量子情報・量子光学の研究室を発足させると同時に、博士課程学生として入学した山本と３人で研究室を立ち上げ、以後参加したPDの一人であるオズデミル氏や院生の一人である徳永氏とともに研究を軌道に乗せることに成功、2004年から現体制で研究を進めている。

2　量子情報処理とは

量子情報処理の研究には、量子暗号や量子コンピューティングのように実用目的のはっきりしたものと、そのための要素技術となる量子テレポーテーション、量子誤り訂正、それに多様な様相を呈する量子操作の本質構造解明といった基礎研究がある。

現在実用化されている現代暗号は、通信が盗聴されることを前提とし、漏れた信号列から本来のメッセージが復元されないことを目的としている。もち

*Nobuyuki IMOTO

1952年10月生
東京大学大学院工学系研究科物理工学修士課程修了（1977年）
現在，大阪大学大学院　基礎工学研究科物質創成専攻・物性物理工学領域，教授，博士（工学），量子情報・量子エレクトロニクス
TEL：06-6850-6445
FAX：06-6850-6445
E-mail：imoto@mp.es.osaka-u.ac.jp

**Masato KOASHI

1969年12月生
東京大学大学院理学系研究科物理学専攻博士課程修了（1995年）
現在，大阪大学大学院　基礎工学研究科物質創成専攻・物性物理工学領域，准教授，博士（理学），量子光学・量子情報
TEL：06-6850-6446
FAX：06-6850-6446
E-mail：koashi@mp.es.osaka-u.ac.jp

***Takashi YAMAMOTO

1975年1月生
総合研究大学院大学　先導科学研究科光科学専攻博士課程修了（2003年）
現在，大阪大学大学院　基礎工学研究科物質創成専攻・物性物理工学領域，助教，博士（理学），量子光学・量子情報
TEL：06-6850-6446
FAX：06-6850-6446
E-mail：yamamoto@mp.es.osaka-u.ac.jp

ろん正統な受信者だけは復元できなければならない。これを実現する最も安全な方法は、復元するための鍵を別途盗聴されないように受信者に送ることである。これを秘密鍵方式と呼ぶが、結局盗聴されない通信チャンネルが必要である。もう一つは現代暗号として主流である「公開鍵暗号」と呼ばれる方法があるが、これは「巨大整数の素因数分解は事実上できない」という数論の経験則を前提としている。ところが量子コンピューターが実現すれば簡単にできてしまうことがわかっており、量子コンピューターができる前に解かれる可能性も否定されていない。

図1

そこで、秘密鍵方式において「鍵を別途盗聴されないように送る」ことを量子力学の不確定性原理に基づいて行う。これを量子鍵配送と呼ぶが、これを含め一般にデータの安全を保証しつつ演算または通信を行うのが量子暗号である。現在までに様々な方式が提案され、大きく分類すると、光の粒子性に情報を載せるか波動性に載せるかという軸と、量子もつれ（エンタングルメント）と呼ばれる特有の量子相関を使うか使わないかという軸があり、たとえば粒子性を使い量子もつれは使わない方法など、組み合わせで種々の提案がある。しかしどの方法でも、図1に示すように、光の量子性を壊さず運ぶ量子チャンネルと送受信者間打合せのための古典チャンネル（被盗聴と非改ざんを前提）を併用する点は共通している。もちろん物理的には一本の光ファイバーのチャンネル多重化で両方を併用することも考えられる。

量子コンピューティングは素因数分解のような有名な難問題を解くことを目的としている。素因数分解したい整数の大きさが千桁程度になると、現在実現されているコンピュータープログラムを走らせると10の100乗ほどのステップを踏まなければならず、これは宇宙の年齢をプランク時間で割ったものよりはるかに大きいので、この宇宙では解けないことになる。しかし量子力学には複数の状態を重ね合わせた状態があるので（重ね合わせの原理）、複数の計算を同時進行させることができる。10の100乗もの大量のパラレル処理も量子もつれを使うと数百個の光子でできることが数学的には示されているので、これは十分現実的である。量子コンピューターや量子暗号を組み合わせた情報通信の将来イメージを図2に示す。

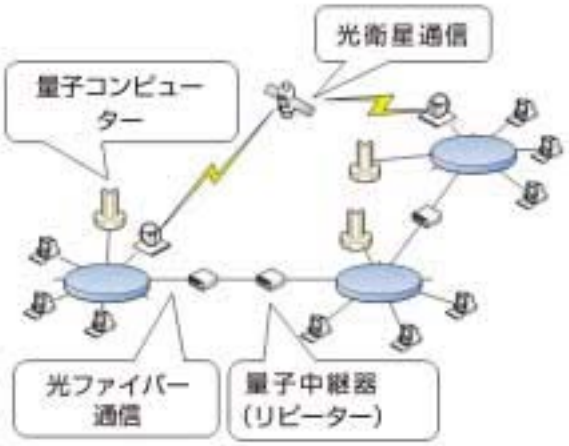

図2

3　研究室の最近の成果

量子暗号

量子暗号は様々な方法が提案され実験も行われている。ところが、本当に盗聴不可能かという証明は意外と難しい。まず、考えられるあらゆる盗聴を実験することはできない。しかし理論的には、どんな物理的手段をもってしても盗聴されないことを証明することは可能である。それを「安全性の理論」と呼び、量子暗号理論の分野では新方式の提案とともに大きな部分を占める。

ところが、安全性理論には優劣がある。たとえば過剰に安全マージンを取らないと成立しない理論か、あるいは必要十分条件に近い条件を提示できる理論かという優劣。劣った理論は実用上低速度過ぎたり短距離過ぎたりする使用制限を装置に課してしまう。へたをすると安全を保証する伝送速度や距離はないと結論づけ、本当は安全な装置を不合格と宣言してしまう。一方優れた理論は装置の能力を最大限発揮させる。このように、同じ装置であっても劣った理

論は性能を下げさせ、優れた理論は性能をアップさせる。理論がハードの性能を上げ下げするのは一見不思議だが、安全を保証する技術特有のことである。当研究室では適用範囲が広く必要十分条件に近い条件を提示する理論を構築している。最近はデコイ量子暗号なる進展がある。これはおとり（デコイ）信号を混入させるとより性能が上がるというものである。方式の多様化に伴い、安全理論も進化が要求されている。当研究室では従来方式をハード的には変えずデータ処理上の改変だけで速度を1万倍にしても安全な方法を提案した。これは2007年Physical Review Letters誌に発表し、同年11月26日の日本経済新聞にとりあげられた。

量子情報保護

量子情報処理における実用上の大きな問題は、環境からの雑音に非常に脆弱であることである。通常の情報処理や通信でも雑音による誤りはあるので、そのために誤り訂正符号が使われる。量子情報処理ではこれがもっと必要である。そのために量子誤り訂正符号が考えられたが、一般に1量子ビット情報に5個以上の物理的量子ビットでコーディングする必要があり、かつ、誤りが1回起こった場合にしか適用できない。従って2回以上の誤りが起きないような短い時間間隔で誤り訂正を繰り返す必要がある。

量子情報処理の誤りは一般にビット誤り、位相誤り、その両方、の3種がある。そのどれもが同じ頻度で起こるならば量子誤り訂正符号が必要となるが、光ファイバー伝送の場合は実は位相誤りが重要である。光ファイバー特有の誤りだけ訂正したい場合は、実は1量子ビット情報に5個の物理的量子ビットは要らず、2個だけで済む。我々はその方法を2005年に提案し、光ファイバー伝送実験で実証した。この実験結果は2008年Nature Photonics誌に発表し、同年7月12日の日刊工業新聞など4紙にとりあげられたほか、同年「子供の科学」10月号でも紹介された。

量子コンピューティング

我々が日常使うコンピューターの演算は、ANDとORとNOTという基本演算ゲートに分解できるという話を聞いたことがあるであろう。量子コンピューティングも同様に、回転ゲートと制御NOTゲートという基本ゲートに分解できる。このためスタンダードな研究はこれらのゲート素子を実現することに向けられて来た。ところが今世紀に入って全く別の構成法が提案された。それは「クラスターステートを用いる一方向量子計算」というものである。我々は光子でクラスターステートを発生し、それを使って上記二つのゲートを実現し、しかもそれが古典的素子では達成できないレベルを超えたことを実験的に証明した。この実験結果は2008年Physical Review Letters誌に発表し、同年9月8日の読売新聞など4紙にとりあげられた。

「弱い量子測定」の実証実験

量子力学で最も特異な事象の一つに、初期状態から終状態に至る途中を覗くことは許されず、その遷移確率だけが意味があるということがある。ところが最近の量子力学の進展によれば「弱い量子測定」という概念があり、これを使うと、一回ごとには正確ではないが平均値としては十分正確に「途中を覗ける」ことがわかって来た。我々はこれを量子もつれを用いた量子光学実験で実証した。この実験結果はNew Journal of Physics誌に発表し、2009年3月23日の日本経済新聞にとりあげられたほか、同年イギリスの経済誌The Economist誌3月号でも紹介された。

4　終わりに

先に当研究室は理論と実験の両方を扱っていると書いた。理論は光に限らず、それこそ量子ドット、イオン、原子その他何でも扱うが、実験は当研究室は量子光学を基軸としている。もちろん量子情報処理の全面実用化の暁に、その全てが光だけで行われているとは考えにくいが、最終的にも光が重要な役目を負うことは論を待たない。光はそのままの形ではメモリーにならないが、演算や通信や制御性の良さは他の追随を許さない。実用導入が近いと目される量子暗号からいつ売り物になるかわからない量子コンピューターまで、研究は基礎も開発も持続的に続くであろう。そして社会的に使用されるようになったときには光が多方面で活躍していることであろう。