光子を用いた量子情報通信・処理

北海道大学　電子科学研究所
竹内　繁樹
takeuchi@es.hokudai.ac.jp

1. 量子情報処理、量子情報通信とは

「科学技術の世紀」と呼ばれる２０世紀は、量子力学の発見とともに始まった。1894年のプランクの量子仮説に始まったその激動のうねりは、1904年のアインシュタインによる光量子の発見に引きつがれ、ついに1926年のシュレーディンガーとハイゼンベルクによる量子力学の確立に至る。その後の量子力学がこの 100 年たらずに及ぼした影響は計り知れない。現在の高度情報化社会の基礎を支える半導体チップや半導体レーザーは、量子論抜きには成り立つことができない。

その量子力学は、「（量子力学的な）重ねあわせ」「波束の収縮」「不確定性原理」「量子もつれ合い」といった、それ以前のニュートン力学など（いわゆる古典力学）には見られないような基本的な性質を有する（図１）。量子情報通信・処理とは、これらの量子力学の基本的な性質を直接、情報処理に応用するものである。1960年代終わりに端を発するそのようなアイデアは、その後1984年にBennettとBrasardらによって、波束の収縮と不確定性原理を利用する

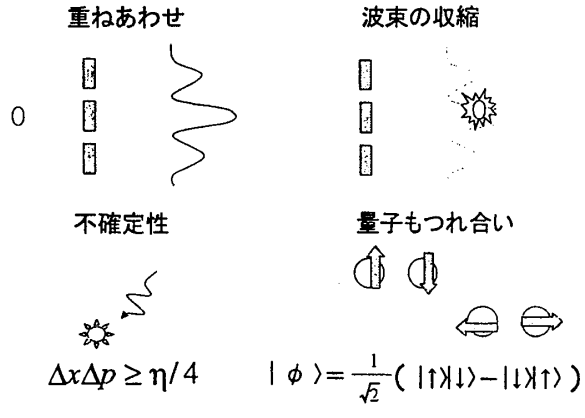

図１　量子力学の基本的な性質

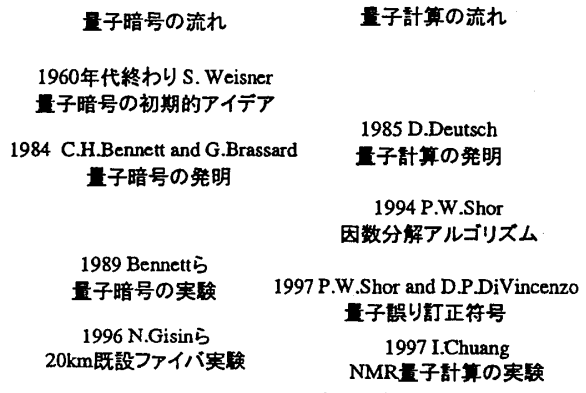

図２　研究の流れ

「量子暗号」として具体化された[1]。この方法を用いれば、他人に決して盗聴されることなく乱数鍵を遠隔地間で共有することが可能になる。ついで1985年に量子計算が提案された。これは「重ねあわせ」と「量子もつれ合い」の原理を応用して、大規模な並列計算を可能にするアイデアである[2]。当初はその能力がまだ明らかでなかったが、1994 年に Shor が因数分解を高速に処理するアルゴリズムを発見[3]し、量子計算の研究は脚光を浴びるようになった。因数分解は、対象となる数の桁数に対して、計算時間が指数関数的に増大することが知られており、200 桁の因数分解にはたとえば現在最高速の計算機を用いても数億年かかると言われている。この事実上の「計算不可能性」が、現在のインターネットで使われている RSA 暗号などの安全性を保証している。ところが、Shor は、量子計算を用いれば、桁数に比例する程度の時間で解けることを示した。100 MHz のクロックで動作するとすれば、200 桁の因数分解なら数分で解けてしまう事になる。

Shor のアルゴリズムの発見前後から、この分野の研究は理論・実験ともに急速に進んでいる。本稿では、量子暗号や量子計算

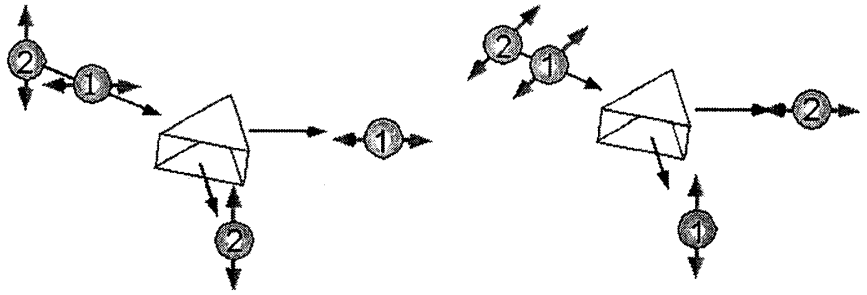

図３　光子の偏光

の原理や研究現状を解説するとともに、２１世紀に向けた分野の展開について展望してみたい。

２．量子暗号

2.1　量子暗号のしくみ

最初に、現在の通信システムにおける盗聴について考えてみよう。たとえば、光ファイバを用いた既存の通信システムの場合、光ファイバをすこし曲げてやるだけで外部に光を漏らすことができる。このとき、もれの量がわずかであれば、盗聴を探知することは困難だろう。

現在は「データは盗聴される」事を前提とし、比較的短い鍵を用いてデータを効率的に暗号化する方法が用いられている。ただ、そのような効率的な暗号化は、どうしても解読される危険性が付きまとう。もし、送りたいデータ列と同じ長さの乱数表を暗号化に用いる事ができれば、解読できないことが分かっている[4]。では、そのような乱数表を、なんとか誰にも知られずに共有できないだろうか？

光の最小単位は、光子である。盗聴者による光子の途中捕獲を完全に検出するために、ビットに対して光子一粒を対応させ、例えば０は縦偏光で、１は横偏光で表すようにするのはどうだろう？　残念ながら、この方法でも盗聴はできてしまう。この場合は、盗聴者は光子をとりだして情報を読み出した後、その情報をコピーした別の光子を送りなおせばよい。

しかし、光子一個になると、量子力学的な性質が現れるようになる。たとえば、光子一つが、単に「縦」か「横」かの２者択一でなく、「斜めの偏光」を取ることもある場合を考える。その時は、光子一粒を測定しただけでは、もともとどのような偏光が与えられているかを知ることは、不確定性原理によりできない（図3）。このしくみをうまく利用するのが、量子暗号である。

量子暗号の目的は、乱数表を盗聴されずに共有することである。まず送受信者は、ビットと偏光を対応させる２種類のコード表（図４で「＋」と「×」）を準備する。送信者は、送りたい乱数表のビットの一つ一つについて、２つのコード表を無作為に選び、その方法で決まる偏光方向を持った光子を受信者に送信する。そのとき、どちらのコード表を選んだかはこの時点ではだれにも明かさない。受信者は、同様に２つのコード表の一つをランダムに選び、それに

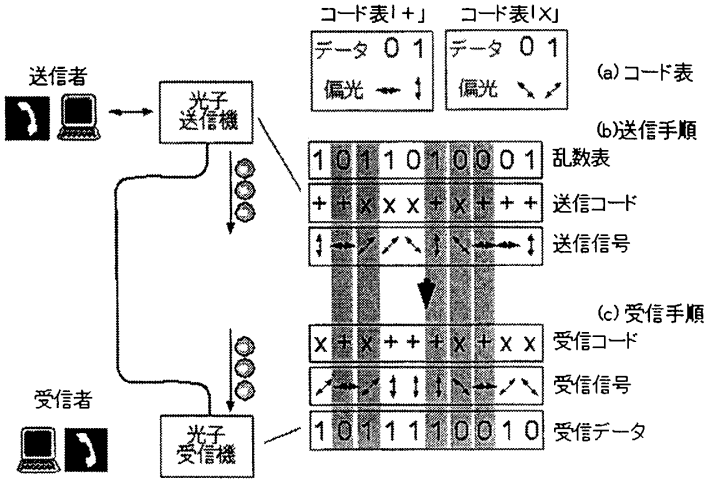

図４　量子暗号通信

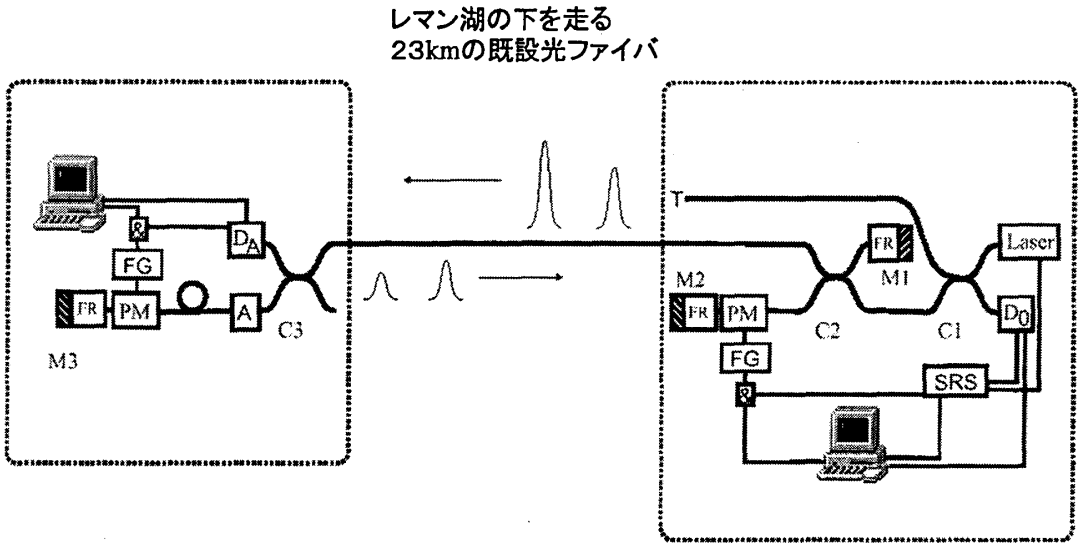

図５　量子暗号通信実験

対応した方向で光子の偏光を読み取る。この時、たまたま送受信で用いたコード表が同じ場合（図４中、緑のラインで表示）には、送信者の送ったビットと受信者の受け取ったビットは同じになるが、違った場合はでたらめになる。光子の送受信が一段落したところで、送信者と受信者は毎回どのコードで送受信したかを通常の回線を用いて照らし合わせる。そして、送受信の方法が一致した部分だけを用いれば、同じ乱数表を共有出来る事になる。

では、どのようにして盗聴者を発見できるだろうか。盗聴者は、送られている光子を盗聴しようとしても、それぞれの光子が、縦横斜めのどのような偏光を持っているのかを知ることができないため、どうしても読みだし誤りを起こしてしまう。盗聴を探知されないためには、光子を再送信する必要があるが、読み出しが誤っていた場合には、間違った情報を受信者に送る事になる。このため、本来は完全に一致するはずのデータ(図４中の影付きの領域)が、送受信者で食い違う。定期的に、お互いに共有したビット列を比較して、もし食い違いが見られるようだと、そのデータは盗聴を受けた可能性がある。以上が、量子暗号の仕組である。

2.2 量子暗号実験の現状

光子一つ一つと聞くと、実際にそのような状態を送受信したり、制御が可能かと怪しまれるかもしれないが、実際には既存の光通信技術をほぼそのまま用いる事が可能である。たとえば、平均的にパルス内に一つ以下の光子の状態を作り出す事は、単にパルス状のレーザー光を減衰フィルタで減衰するだけで容易に作成する事が出来る。光子の偏光状態の回転は、既存の電気光学素子をそのまま用いる事が出来るし、また長距離伝送については、通常の通信用光ファイバで可能である。たとえば、光ファイバで50km送信したときの光のロスが50%だとすると、これは、送信した内の半数の光子が伝送されることを意味する。現在提案されている量子暗号の光学系が、通常の光通信と本質的に違う点は、受信機に光子検出器を用いる点だろう。送られる光子の位相の扱いに注意しなければならない点は、コヒーレント光通信と共通する点が多い。実際に、1996年ジュネーブ大学のN. Gisinらによって行われた実験[5]のセットアップを図５に示す。彼らはレマン湖の下に敷設されていた長さ 23km の光ファイバを用いて実験した。この時は毎秒１ビット程度でしか安全な乱数を共有できなかったが、1998年には毎秒210ビットの共有に成功している。

2.3 量子暗号技術の課題

量子暗号の実用化にあたっては、伝送距離とビットレートが問題となる。量子暗号通信は、光子の偏光情報が複製できないこ

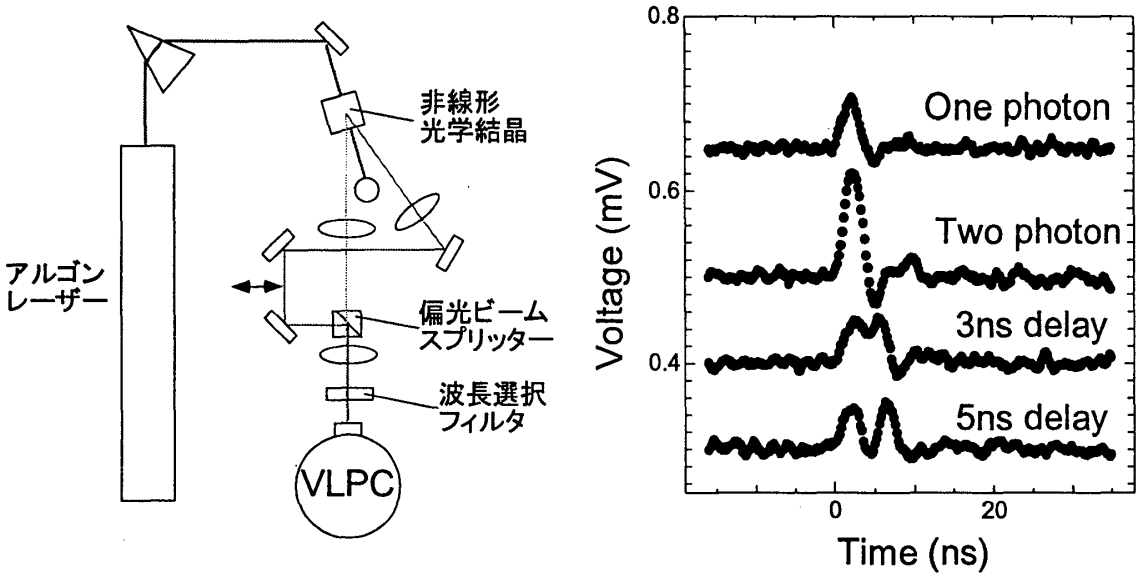

図６　光子数検出器

とを盗聴防止に利用していたが、逆に複製ができないために、増幅することもできない。このため、光ファイバー中での減衰と、検出器のダークカウント（光子の入射が無いときのカウント数）との兼ね合いで伝送距離の限界がきまり、現状技術では 100km 程度と考えられている[5]。また、ビットレートについては、パルス発信の周波数、伝送路中での光の減衰、光子検出器の量子効率などが問題となる。

もう一つの問題として、現在は微弱光を用いているために、パルスあたりの平均光子数を 0.1 程度にしている点がある。これは、パルス内に２つ以上光子が存在すれば、その分盗聴が可能になるからである。もし、一パルスあたり光子を確実に一つづつ放出する光子源が存在すれば、伝送レートを最大１０倍程度向上できる。そのような試みの一つとして、我々は、同時刻に同時に２つの光子が発生する、パラメトリック蛍光と、入射光子数を検出できる高い量子効率の光子検出器(図 6)を用いて、パルス内の光子数を制御する試みに取り組んでいる[6]。他には、ターンスタイルデバイスによる試み[7]などが報告されている。

2.4 量子暗号の展開

量子暗号のメリットは「絶対に安全な暗号」を提供できる点である。実際には、ノイズ他の原因で「完全」とは言えないが、共有した乱数列に「セキュリティ増幅」と呼ばれる処理をほどこす事で、盗聴の割合を任意に小さくすることができる[8]。今後は、さらに伝送距離の長距離化、伝送速度の高速化、および既存のセキュリティ技術との融合が行われていくだろう。１００ｋｍといわれている伝送距離の壁を破るためには、100km 毎に安全性が他の方法で保証された「中継基地」を設ける方法もあるが、量子状態をそのまま中継する「量子リピーター」の研究も始められている[9]。この技術が広く使われるかどうかの鍵は、このような高度のセキュリティを持つ新しい道具に対してどの程度のニーズがあるかだろう。

理論面でも、量子暗号はさらに展開を見せている。現在、インターネット上では、公開鍵暗号をベースにしたさまざまなセキュリティ技術が使われている[10]。たとえば、発信者が間違いなくその人自身であることを確認する「認証」や、意思決定の為の「コイン投げプロトコル」などである。これらのセキュリティ技術についても、量子力学の基本的な性質を用いて実現する研究も進められている[11]。

３．量子計算

３．１　量子計算のしくみ

量子計算は、量子力学的な重ねあわせと、量子もつれあいを用いて、天文学的な数の並列計算を可能にするアイデアである。現

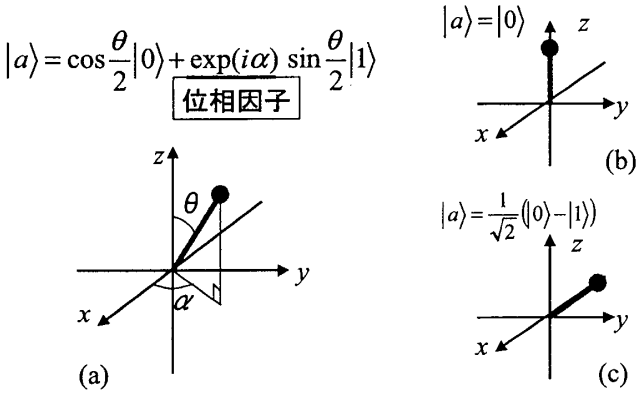

図７　量子ビット

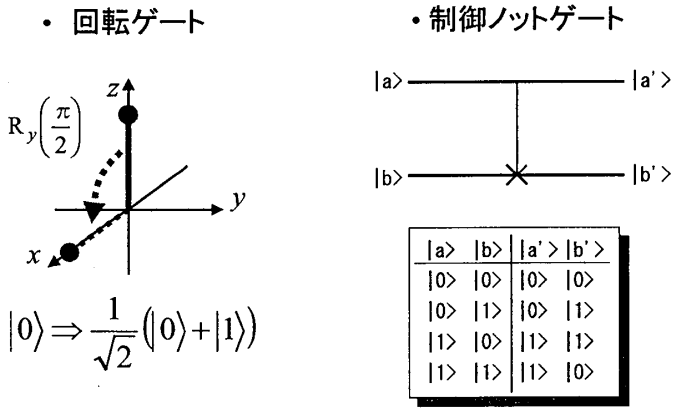

図８　基本量子ゲート

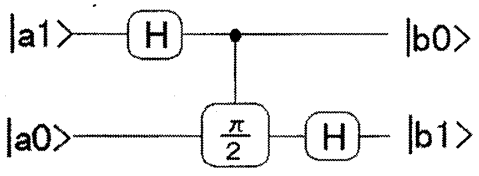

図９　量子フーリエ変換回路

在用いられている計算機では、0 または１の値を取る「ビット」とそれに対する「論理ゲート」によって回路が作られている。それに対して量子計算は、0 と１の重ねあわせ状態をもつ「量子ビット」に、量子論理ゲートを作用させて演算を行う。

図７に示すように、この重ねあわせ状態は、0 と 1 の重みづけのパラメータθと、位相パラメータαを用いて表すことができる。この量子ビットに対して、図８に示す２つの「基本量子ゲート」が実現出来れば、量子計算が可能になる。一つは、回転ゲートと呼ばれるもので、単独の量子ビットに作用して、θやαの値を一定の割合「回転」させる。もう一つは、制御ノットゲートである。これは、信号ビットと標的ビットの２つの量子ビットに働くゲートで、信号ビットが１の時のみ、標的ビットに対してノットゲートとして作用する。これらの２つの基本ゲートが実現すれば、量子計算機を作ることができる。

では、具体的に量子計算の高速性を、フーリエ変換を例として見てみよう。図９に、量子計算によるフーリエ変換の例を示した。この例では、２ビットから２ビットへの離散フーリエ変換を３回のゲート操作で実現している。同様にして、N ビット(データ点数 2^N)から N ビットへの離散フーリエ変換を、N(N+1)/2 回程度の操作で実行することができる。逐次的なフーリエ変換の場合 2^{2N} ステップ、高速フーリエ変換の場合でも N 2^N ステップ程度かかることを考えると、量子計算によるフーリエ変換が圧倒的に早いことが分かる。

Shor はこの量子フーリエ変換をうまく用いて、因数分解や離散対数問題を高速に解くアルゴリズムを発見した[3]。その後 Grover は、データーベース検索を高速に行うアルゴリズムを発見した[12]。ランダムに並んだ N 個のデーターベースから、1 つのデータを探しだすには、普通の方法だと N/2　回程度データベースを参照しなければならない。ところが量子計算を用いると、√N 回程度でできる。100 万回かかるところを 1000 回で出来ることになる。

３．２　量子計算の実現に向けた取り組み

このような量子計算機を実現するには、0 と１の重ねあわせ状態を取りうるような量子ビットとそれに対する基本量子ゲートを実現する必要がある。量子ビットとしては、核スピンや電子準位など、さまざまな物理量を用いることができる(図 10)。それぞれ

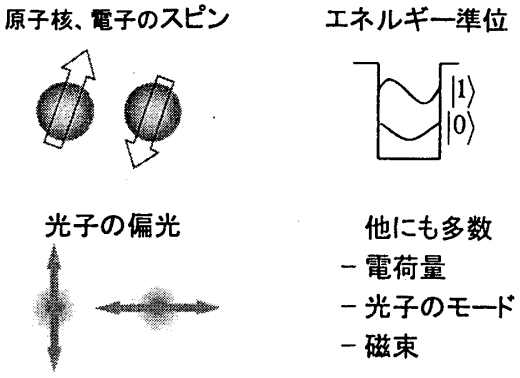

図１０　量子ビットの候補

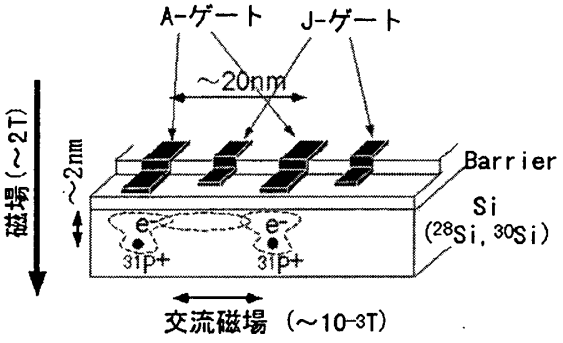

図１１　シリコン量子計算機のアイデア

の量子ビットの候補についていくつかの実現方式が提案されている[13]が、個々のアイデアの詳しい説明はここでは割愛する。

これまでに、溶液中の分子の核スピンをNMR で制御する方法[14]や、著者らの光子を線形光学素子で制御した実験[15]によって量子計算のアルゴリズムは検証されている。しかし、これらの方法は量子ビット数10 程度で限界がくると見られている。より大規模な量子計算機の実現に向けて、真空中に浮かべたイオンを量子ビットとする、イオントラップを用いたシステムの構築が、アメリカのロスアラモス国立研究所等で進められており、これまでに４量子ビット間の状態制御に成功している[16]。

一方で、固体デバイスを用いた量子計算機についてもさまざまな提案が行われている。有力な提案として、B. Kane によるシリコン半導体中に埋め込まれた核スピンを用いるものがある(図 11)[17]。日本においても、量子計算機の実現に向けた取り組みがすすめられている。NEC の中村らは、超伝導体でできた微小な「島」の中の電荷量を量子ビットとして、回転ゲートの実験に成功している[18]。固体デバイスで回転ゲートに成功したのは初めての例である。ほかに、理化学研究所の石橋、東京大学の樽茶らのグループは、結合量子ドットを素子として用いる実験に取り組んでいる[19]。また、大阪大学の北川らのグループは、NMR 量子計算の量子ビット数の増加に取り組んでいる[20]。

３．３　量子計算の実現に向けた課題

現在の計算機を凌駕するような量子計算機はいつ実現するのだろうか。筆者は、２０１０年までに、そのような量子計算機が実現しているとは思わないが、それ以降いつ頃になるかの特定は難しい。

実現にあたっては、位相緩和をどのように抑制するかが問題になる。量子計算では、計算の間は、重ねあわせ状態が保たれている必要がある。しかし、実際の量子ビットは、時間の経過とともに徐々に重ねあわせ状態が壊れてしまう。これが位相緩和である。たとえば 200 桁の因数分解を行おうとすれば、1000 個程度の量子ビットに対して 10^{10} 回程度量子ゲートの操作を行わなければならない。そのためには、最低数秒は位相緩和が生じない必要がある。

空中に量子ビットとなるイオンを浮かせて並べるイオントラップでは、緩和時間は長く取る事が出来るが、イオンを大量にならべてそれを制御しつづけることは、かなり困難そうに見える。一方、固体中の電子状態や核スピンなどを用いる方式は、一度基本ゲートができてしまえば、それを集積するのは比較的容易にみえる。しかし、固体中では、量子ビットと周囲の電子などとの相互作用を遮断し、長い緩和時間を達成することが難しい。

現在は、それぞれの提案の基礎となる物理をより詳しく調べ、提案の検証実験を積み重ねながら、ブレークスルーを模索することが重要だと感じられる。

4．　おわりに

この分野には、通信、計算機科学、数学、物理、化学など様々なバックグラウンドをもつ研究者が参加し、その一種のるつぼから様々な新しい成果が現れている。量子計算の位相緩和を解決する手段として発見された、量子誤り訂正符号[21]がよい例だろう。これは、これまで物理的な条件のみで決まっていると考えられていた位相緩和を、ソフトウェア的な手続きで阻止することができるという画期的な発見である。この発見は、もともと符号論などにもバックグラウンドをもつP. Shor と D. P. Divincenzo が、古典的な誤り訂正の考え方を量子に応用して得られた成果である。

また、これらの具体的なアプリケーションの出現によって、量子情報研究は急速に進展しているが、それとともに、量子力学の世界について、我々の理解が十分でない点が明確になってきた[22]。例えば、多粒子間の量子力学的なもつれ合いについては、定量的な指標さえ確立していない。このように、量子情報研究は豊かなサイエンスを含む領域でもある。今後も様々な分野の方の積極的な参加によって、この分野の実りある発展を願っている[23]。

参考文献

[1] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computer, Systems, and Signal Processing, Bangalore, India (IEEE, New York), p175, 1984.

[2] D. Deutsch, Proc. R. Soc. London Ser. A 400, p97, 1985.

[3] P. W. Shor, Proceedings 35th Annual Symposium on Foundation of Computer Science, IEEE Computer Soc, Los Alamitos, CA , p124 , 1994.

[4] Vernum 暗号、One time pad 暗号と呼ばれる。D. Kahn, The Codebreakers: The Story of Secret Writing, New York: Macmillan Publishing Co., 1967

[5] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, G. Ribordy, Appl. Phys. B 67, p743, 1998.

[6] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, Nature 397, p500, 1999

[7] S. Takeuchi, J. Kim, Y. Yamamoto, and H. H. Hogue, Appl. Phys. Lett. Vol. 74, p1063 , 1999;

[8] J. Kim, S. Takeuchi, Y. Yamamoto, and H. H. Hogue, Appl. Phys. Lett., Vol 74, p902, 1999.

[9] C. H. Bennett, 'Experimental Quantum Cryptography', J. Cryptology, vol. 5, p3, 1992.

[10] H. J. Briegel, W. Dur, J. I. Cirac and P. W. Zoller, ロスアラモス e-print server, http://xxx.lanl.gov/abs/quant-ph/9803056

[11] 岡本龍明, 図解 暗号と情報セキュリティ, 日経BP社 1998 など

[12] H. K. Lo and H. F. Chau, Phys. Rev. Lett. Vol. 78, p3410, 1997; D. Mayers, Phys. Rev. Lett. Vol. 78 p3414 , 1997.

[13] L. K. Grover, Phys. Rev. Lett. Vol. 79, p325, 1997

[14] 竹内繁樹, ２１世紀、量子猫は計算をするか？, 日本物理学会誌 vol. 54 no. 4 p263, 1999;竹内繁樹、井須俊郎,「量子計算の実現に向けて, 応用物理, Vol 68, No. 9 pp1038, 1999; 細谷暁夫, 量子コンピュータの基礎、サイエンス社, 1999.;西野哲朗, 量子コンピュータ入門、東京電機大学出版局, 1997.; 特集 量子情報と量子コンピュータ、数理科学 ６月号, 2001.

[15] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung and S. Lloyd, Nature, vol. 393, p143, 1998

[16] S. Takeuchi, Phys. Rev. A, vol61 052302, 2000.

[17] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe: Nature, vol. 404, p256, 2000.

[18] B. E. Kane, Nature, vol. 393, p133, 133.
[19] Y. Nakamura, Yu. A. Pashkin and J. S. Tsai, Nature vol. 398, p768, 1999.
[20] T. H. Oosterkamp, T. Fujisawa, W.G. van der Wiel, K. Ishibashi, R. V. Hiijman, S. Tarucha, L. P. Kouwenhoven, Nature, vol. 395, p873, 1998.
[21] 北川勝浩，数理科学 vol. 424, p43, 1998.
[22] D. P. Divincenzo and P. W. Shor, Phys. Rev. Lett., vol. 77, p3260, 1996.
[23] たとえば、M. Koashi and N. Imoto, Phys. Lev. Lett., vol. 81, p4264, 1998.
[28] 電子情報通信学会 量子情報技術時限研究専門委員会主催の研究会が定期的に行われている。
http://www.qc.ice.uec.ac.jp/qit4/

注）本稿は、電子情報通信学会誌 2001 年 1 月号掲載の原稿を元に著者が加筆したものであることをお断りさせていただきます。