光量子ビットを用いた量子計算機

竹　内　繁　樹

量子計算とは，「重ね合わせの原理」や「量子もつれあい」といった量子力学の原理に基づく新しい計算機の概念である．本稿では，量子計算についてその利点や原理をわかりやすく解説するとともに，量子ビットとして光子を用いた提案や実験について，光子で他の光子を制御する量子ゲートの最近の研究状況や，われわれの行った線形光学素子と光子を用いた量子計算の実験について解説する．

1.　なぜ，量子計算か

量子計算とは，「重ね合わせの原理」「量子もつれあい」といった量子力学の本質的な性質を用いる新しい計算機の仕組みである[1-4]．量子計算が注目されているのは，1994年の因数分解アルゴリズムの発見[5]によって，現在の計算機よりも本質的に計算を速く行えることが理論的に示されたからだろう．

「21＝3×7」といったように，ある数が与えられたときにその因数を発見する因数分解の問題を考えよう．この程度であれば暗算で可能だが，さらに大きな数，たとえば「3433939」が与えられたときに，それが「1993×1723」であることを発見するには，3，5，7，11と小さい素数から順に割っていって調べるしかない．このため，因数分解は与えられる数の桁数に対して指数関数的に計算時間が増大することが知られている．たとえば200桁の整数を因数分解するには，現在最高速の計算機を用いても数十億年かかり，因数分解は事実上不可能である．因数分解の面白い点は，このように因数を調べることは大変だが，もしその因数の1つを知っていれば，対になる因数は単に割り算をすることでたちどころに知ることができる点である．この性質をうまく利用しているのが，現在インターネットで用いられているRSA暗号[6]である．この暗号技術は電子マネーや電子署名をはじめとする最新のセキュリティー技術の基盤となっている．

ところが量子計算機を使えば，桁数に比例する時間でこのような計算を行えることが示された．もしも100 MHzで動作する量子計算機が実現すれば，数分で解けてしまう可能性がある．またこれまでは200桁を202桁にするだけでさらに100倍程度の時間がかかっていたものが，量子計算では1.01倍程度の時間しかかからない．

ほかには，データベースの検索を高速に行うアルゴリズムが発見されている[7]．たとえば，名前順に100万件の電話番号が載っている電話帳だけを使って，電話番号から人名を探す場合を考える．普通には，1つずつ電話番号をチェックしていくしかなく，平均してデータ数の半分，50万回程度のチェックが必要だろう．ところが，量子計算のアルゴリズムを用いると，データ数の平方根，1000回程度の試行で可能であることがわかっている．現在，ほかにどのような問題が高速に解けるか研究が進められている．

2.　量子計算の仕組み

2.1　「重ね合わせの原理」と「量子もつれあい」

量子力学の登場以前の理論（古典理論）では，電子は必ず確定した「位置」をもっていると考えられていた．たとえば，箱の中に電子が1つ存在する場合を考える．この箱を真中で左右に仕切ると，古典理論では，電子は左右のどちらか一つの状態を必ずとると考える．ところが量子力学では，条件を整えれば，電子は，箱の左側に存在する状態（波動関数）$|L\rangle$と，右側に存在する状態$|R\rangle$の「重ね合わせ」として存在することが可能になる．つまり，1つの「電子」が複数の状態を同時にとることができるようにな

科学技術振興事業団さきがけ研究，北海道大学電子科学研究所（〒060-0812 札幌市北区北12条西6丁目）
E-mail: takeuchi@es.hokudai.ac.jp

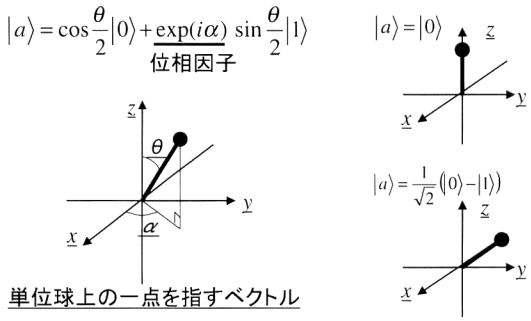


図1　量子ビットの表記方法とその例.

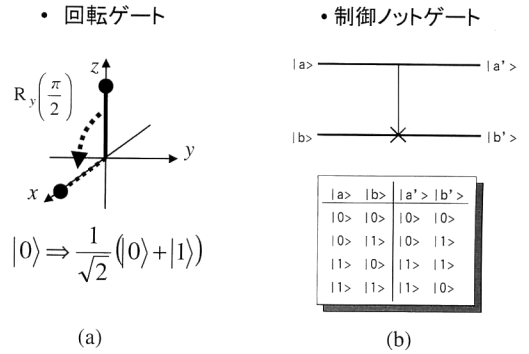


図2　基本量子ゲート．(a) 回転ゲート，(b) 制御ノットゲート．

る．ここで，“|⟩” は，量子力学的な状態を表す記号である．

これを，計算と対応させて考えよう．現在の計算機では，0 もしくは 1 の値を必ずとる「ビット」を基本単位としている．量子計算では，このビットを量子力学的な「重ね合わせ状態」をとれるように拡張された量子ビット (qubit, quantum bit の略) を基本単位として用いる．

「量子もつれあい」とは，複数の粒子の間に量子力学的な特殊な相関関係が生じることをいう．たとえば，0 と 1 の 2 つの状態をとり得る粒子のペアを考えると，それらがとり得る状態は 00，01，10，11 の 4 通りになる．量子力学では，それらの状態間で任意の重ね合わせ状態をとることができ，その重ね合わされ方によって相関関係が生まれる．たとえば，$(|00\rangle+|11\rangle)/\sqrt{2}$ という状態は，粒子 1 つだけをみると，$(|0\rangle+|1\rangle)/\sqrt{2}$ となり，これは $|0\rangle$ と $|1\rangle$ の等分な重ね合わせ状態になっている．しかし，この状態を「観測」すると，両方 $|0\rangle$ または両方 $|1\rangle$ の状態しか表れない．同様に，粒子数が N 個だと，2^N 個の状態から任意の組み合わせで重ね合わせ状態をとり得る．量子計算は，この重ね合わせを利用して一種の超並列計算を行っていると考えてよい．

2.2　量子ビットと基本ゲート

量子ビットは一般に，

$$|a\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \exp(i\alpha)\sin\left(\frac{\theta}{2}\right)|1\rangle \qquad (1)$$

と表すことができる（図 1）．ここで，i は虚数単位，θ は 0 と 1 の重み付けを決定し，また α は位相に関するパラメーターである．また，各項の計数の 2 乗がそれぞれの事象の確率を示す．このような量子力学的な重ね合わせをとることが可能な物理量であれば，量子ビットとして用いることができる．

この量子ビットに，回転ゲートと制御ノットゲートの 2 種類の基本ゲートを作用させることで，どのような量子計算アルゴリズムでも構成できることがわかっている．回転ゲートは，1 つの量子ビットに関するゲートであり，量子ビットの 0 と 1 の割合 θ や位相 α を任意の値だけ変化させる．図 2(a) に，回転ゲートの例を示す．Hadamard 変換とよばれるこのゲートは，$|0\rangle$ を $(|0\rangle+|1\rangle)/\sqrt{2}$ に，$|1\rangle$ を $(|0\rangle-|1\rangle)/\sqrt{2}$ へと変換する．

一方，制御ノットは，2 つの量子ビットに関する量子ゲートで，一方を制御量子ビット，他方を信号量子ビットとしたとき，制御量子ビットが $|1\rangle$ のときに限って，信号量子ビットの $|0\rangle$ と $|1\rangle$ を反転させる（図 2(b)）．その出力だけをみると，これは一見排他的論理和（EX-OR）と同様にみえるが，入出力として重ね合わせ状態となるところが大きく異なる．たとえば，制御量子ビットに $(|0\rangle+|1\rangle)/\sqrt{2}$，信号量子ビットに $|0\rangle$ を入れると，出力は $(|00\rangle+|11\rangle)/\sqrt{2}$ と前述のもつれあい状態になる．

2.3　緩和時間

量子計算を実現するには，量子ビットとしての物理系に対して，これらの 2 つのゲート操作を実現すればよいが，実際に実現するには，重ね合わせ状態の崩壊という問題が生じる．量子計算は，量子力学的な重ね合わせ状態を用いて計算を行う．ただし，実際の物理系では，重ね合わせ状態は指数関数的に破壊されていき，一定の時間しか保たれない．この時間を緩和時間とよぶ．緩和には，θ に関連する縦緩和と，α に関する横緩和があるが，通常横緩和時間のほうが短く，これが計算可能時間に制限を加える．この緩和時間を，1 回のゲート操作にかかる時間で割ると，計算可能回数 $N_{\max}$ が求まる．たとえば，200 桁の因数分解を行うには，10^{10} 回程度の計算可能回数が必要である[8]．もし最短のゲート時間を 100 ps 程度と仮定すると，秒のオーダーの緩和時間が必要である．

2.4　量子計算の諸提案と現状

因数分解アルゴリズムの直後，イオントラップを用いた量子計算が提案された[9]．これは，特殊なコイルで発生する磁場によって空中にイオンを浮かせ，そのイオンの電子準位を外部からレーザー光でコントロールするものであ

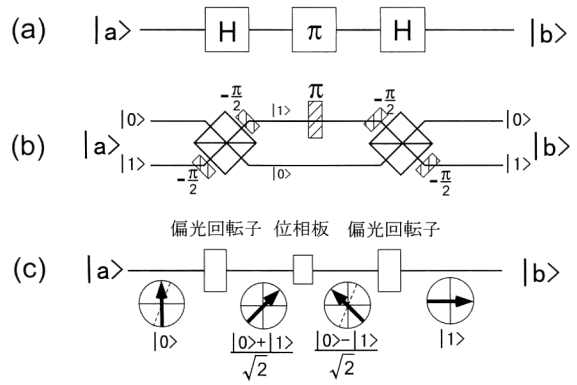


図3 (a) 量子回路の例．囲は図2のRy（$\pi/2$）と同一．(b) モードを量子ビットとして (a) の量子回路を実現した例．π などで示されている光学素子は，光子の位相を示されている値だけ変化させる．(c) 偏光を量子ビットとして (a) の量子回路を実現した例．矢印は偏光方向を表す．

る．現在，アメリカのロスアラモス研究所などで活発に研究が進められており，4つのイオン間に量子もつれあいを生じさせる実験が最近報告されている[10]．

一方，固体デバイスの研究も進められ，たとえば，シリコン中のリン原子の核スピンを量子ビットとする提案が行われている[11]．ほかにも固体デバイスとして実現する方法として，2準位原子の電子準位[12]や電子スピン[13]，超伝導素子で電荷数[14]や磁束[15]をコントロールするものなど，さまざまな提案がなされている．これらの固体デバイスの提案には，集積化が容易であり，小型化できる利点があるが，どうしても緩和時間が短くなる傾向がある．現状の技術では，単一の量子ビットに対する回転ゲートが，超伝導素子で実現している[14]程度である．

今のところ量子計算のアルゴリズムのデモンストレーションに成功しているのは，溶液中の分子の核スピンを核磁気共鳴でコントロールするNMR（nuclear magnetic resonance）量子計算[16]と，後述する線形光学素子量子計算[17]のみである．以下，光子を量子ビットとして用いた量子計算について詳しく述べる．

3. 光子を量子ビットとして用いる

3.1 量子ビットとしての物理量と回転ゲート

光子に対しては，そのモード（光路）や偏光を量子ビットとして用いることができる．モードを量子ビットとして用いる場合を，図2(a) で示したHadamard変換（H）を2つ含む量子回路（図3(a)）を用いて説明する．この回路は，図3(b) に示されるような，マッハ・ツェンダー干渉計に対応している．この光学系において，光子は2つのモードにまたがって存在し，それらのモード $|0\rangle$ と $|1\rangle$ は量子ビットの基底に対応する．それぞれのモードの波動

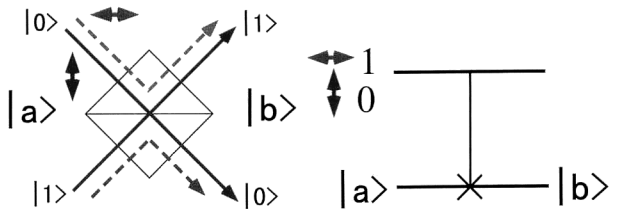


図4 偏光ビームスプリッターによる制御ノットゲート．偏光が制御量子ビット，モードが信号量子ビットに相当する．

関数に対して，分岐比50：50のビームスプリッター（$-\pi/2$ の回転ゲートが位相補正のために補われている）はHadamard変換として働く．

もちろん，偏光を量子ビットとして用いることも可能である．その場合，たとえば $|0\rangle$ は水平偏光で，$|1\rangle$ は垂直偏光で表される．この場合のHadamard変換は，ちょうど光学軸を22.5度だけ垂直軸から傾けた $\lambda/2$ 波長板によって実現可能である（図3(c)）．

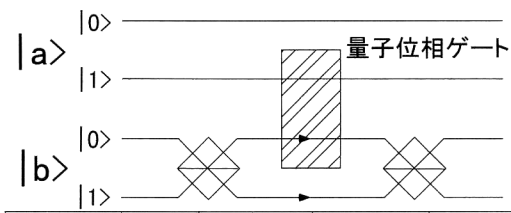
3.2 制御ノットゲート

次に，2つの量子ビットに対する制御ノットゲートについて考えよう．まず，光子1つが「モード」と「偏光」の2つの量子ビットを担っている場合を考える（図4）．「偏光」を制御ビット，「モード」を標的ビットとすると，縦偏光の光子についてはモードの入れ替えが行われず，横偏光の光子に対しては入れ替えが起こればよい．このような操作は，縦偏光を透過し横偏光を反射する，偏光ビームスプリッターを用いて実現できる．しかし，このままでは2つの量子ビットしか用意することができない．

さらに量子ビットを増やすためには，複数の光子と，それらのモードや偏光で表された量子ビット間で制御ノット操作を行う必要がある．Chuangら[18]は，光子と非線形光学素子を用いた量子計算を提案した．この方法では，光子1つの入力に応じてもう1つの光子の位相を反転するような，巨大な非線形性をもつ光学素子を用いる．図5に制御ノットを構成した例を示す．量子ビット $|b\rangle$ の部分に注目すると，2つのビームスプリッターによって構成されたマッハ・ツェンダー干渉計になっている．この干渉計は，光子が $|0\rangle$ から入射した場合に必ず $|0\rangle$ から出力されるように，光路差が設定されている．この干渉計の腕の一方に前述の非線形光学素子が図5のように組み込まれると，量子ビット $|a\rangle$ の状態が $|0\rangle$ であれば量子ビット $|b\rangle$ は影響を受けないが，量子ビット $|a\rangle$ が $|1\rangle$ のときには $|b\rangle$ が反転される．このように，図5の回路は制御ノットを実現していることがわかる．

3.3 巨大非線形光学素子

では，そのような巨大な非線形をもつ光学素子を実現す



	(I)	(II)	(III)	(IV)
$\|b\rangle$ $\|a\rangle=\|0\rangle$	$\|0\rangle$	$\|0\rangle-\|1\rangle$	$\|0\rangle-\|1\rangle$	$\|0\rangle$
$\|b\rangle$ $\|a\rangle=\|1\rangle$	$\|0\rangle$	$\|0\rangle-\|1\rangle$	$\|0\rangle+\|1\rangle$	$\|1\rangle$

図5　量子位相ゲートを用いた制御ノットゲート．

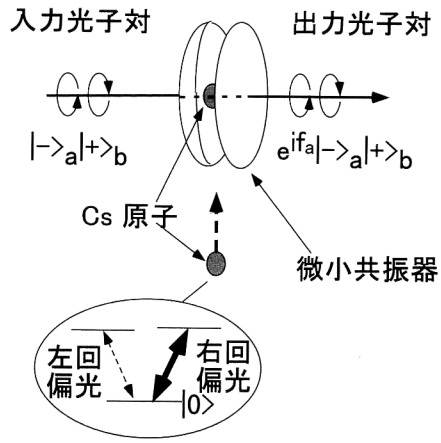


図6　微小共振器中に閉じ込めた原子による量子位相ゲート．

ることは可能だろうか．1995年にTurchetteら[19]は，図6のような装置を用いて，単一光子で別の単一光子の位相を変調することに成功している．実験では，ほぼ全反射に近い2つのミラー（透過率は10^{-4}〜10^{-6}）でマイクロキャビティーを構成し，その中にセシウム原子を1原子ずつ導入する．ミラー間で反射を繰り返しながら，光子はマイクロキャビティーの内部に長く留まることができ，結果として光子と原子は強く相互作用する．この場合，セシウム原子の微細構造準位の2状態が，補助的な量子ビットとして働く．基底状態$|0\rangle$からは，右回り偏光と左回り偏光でそれぞれ異なる状態へと遷移が可能であるが，右回り偏光に対する遷移確率のほうが十分大きい．このため，左偏光を入射した場合は光子と原子はほとんど相互作用を行わず，右回り偏光のときだけ相互作用する．右回り偏光の光子が2つ連続して入射する場合，マイクロキャビティーの効果で，最初の光子1つで吸収が飽和し，次に入射する右回り偏光の光子は，通過時に本来受ける位相シフトを受けなくなる．この実験では，この単一光子同士の相互作用による位相変化量として16度の値が得られている．この値が180度に達すれば，先に述べた方法で任意の量子回路を実現することができる．このように，一方の光子により他方の光子の位相を変調できる素子を，量子位相ゲート（quantum phase gate: QPG）とよぶ．ただ，この実験においては，原子の通過位置や時刻を制御できないため，安定したゲート操作はまだ実現していない．

4.　線形光学素子量子計算

このように，光子と非線形光学素子を用いて量子計算を実現するのは，現状では難しい．電子スピンや，イオンの準位などのほかの量子状態を用いた量子ビットについてもそれぞれ困難さを抱えている．唯一，NMR量子計算[16]が，アルゴリズムの実行可能なテストベッドとして用いられているが，この方式にも一部問題が指摘されている．溶液中の分子一つ一つが量子計算機として働くが，シグナルとしてはそれらの結果の平均値しか得られないからである．

光子を用いて，制御ノット実現の困難さを回避しながら実験的に量子計算のアルゴリズムを研究する方法として，著者らは線形光学素子を用いる方法を提案した[20]．

この方法では，モード間にもつれあいをもたせることができないため，N個の量子ビットで実行可能なアルゴリズムを実現するためには，2^Nのモードを用意しなければならない．このため大規模な量子計算を実現することはできないが，10個程度までの量子ビットで記述されたアルゴリズムを，実験的に調べるのには適している．その後，ほかのいくつかのアルゴリズムにも適用されている[21,22]．

4.1　Deutsch Jozsa 量子計算アルゴリズム

まず最初に，Deutsch Jozsaの問題[23]について紹介する．いま，$2N$個の0または1からなる数列が与えられたとしよう．この数列が，1と0をN個ずつ含むときを「等分」，またすべて1または0のみからなる場合を「均一」とよぶことにする．たとえば$N=2$のとき，等分の例は$\{1, 0, 1, 0\}$であり，均一の例は$\{1, 1, 1, 1\}$である．このとき，Deutsch Jozsaの問題とは，「与えられた数列は均一ではない」「与えられた数列は等分ではない」の2つのうち，正しいものを1つ選べ，というものである．この問題を解くのに，古典的な計算機を用いると，最悪の場合$N+1$回の試行が必要だが，彼らの量子計算アルゴリズムを用いるとLog（N）のオーダー回の試行で解くことができる．

4.2　Deutsch Jozsa アルゴリズムの実験

筆者の「線形光学素子量子計算機」は，4ビットの数列に対してこの問題を解くことができる[17]．光学系を図7に示す．数列は電気光学素子の制御信号として与えられ，光

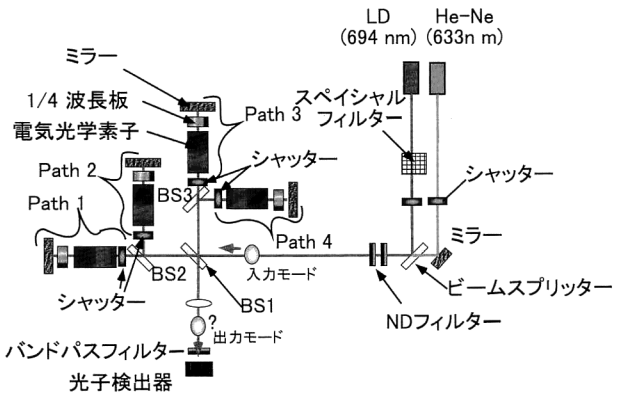


図7　線形光学素子量子計算機.

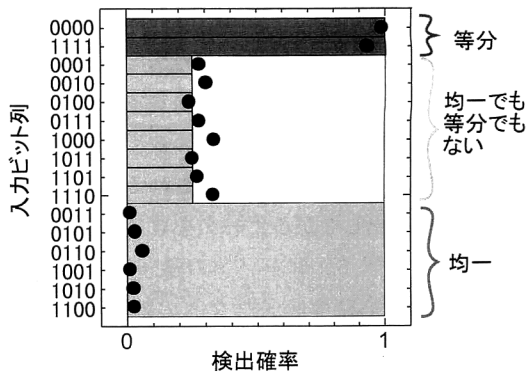


図8　4ビットDeutsch Jozsa実験の結果．黒丸が実験で得られた値を，棒グラフが理論的な予測値を表す．たとえば，この量子計算機は，光子を検出した場合は「等分でない」と答えたことになるが，実験結果をみると入力ビット列が均一の場合には検出確率が0に近く，ほぼ正しく答えを出していることがわかる．

子を1つ実験系に入射し，この光子が出力部で検出できるかどうかによって，答えを得ることができる．

この実験では，ダイオードレーザーから出力された垂直偏光をもつ694 nmの光を減衰フィルターによって減衰して光子源としている．まず光子は，3つの50：50ビームスプリッター（BS1，BS2，BS3）を透過した後，4つのモードのそれぞれに等しい確率で存在する「重ね合わせ状態」へと変化する．それぞれのモードでは，対応する入力ビットが1のとき，電気光学素子が偏光を垂直から水平へと回転するようセットされている．次の4分の1波長板では，偏光が水平のとき，垂直な場合に比べて位相が$\pi/2$ずれる．その後，光子はそれぞれのモードでミラーにより反射され，4分の1波長板では再び$\pi/2$，合計πの位相シフトを受ける．その後，電気光学素子で偏光はもとの垂直状態へと戻される．BS1～BS3で干渉した後，出力部に設置された光子検出器で検出される確率は，

$$P(f(j))=\frac{1}{16}\left|\sum_{j=1}^{4}(-1)^{f(j)}\right|^2 \qquad (2)$$

として与えられる．この確率は，等分な$\{f(j)\}$に対しては0であり，均一な$\{f(j)\}$に対しては1になっている．

この量子計算機の動作を確認するために，入力ビット列をさまざまに入れ替えながら，1つの入力ビット列に対して0.1秒間光子計数を行い，光子の検出確率を求めた．実験に先立って，上述のような干渉条件が成り立つように各光路中のシャッターを開閉しながら光路長を設定し，実験中も参照用のHe-Neレーザーを用いて光路長を能動的に制御した．

実は，微弱光を用いた場合，いつ光子が入射したのかは特定できず，出力モードだけを検出したのでは「光子を検出しなかった」場合について判断できない．その解決法として，残り3つの出力モードでも光子検出し，出力モードで検出した場合を「検出した」と，残り3つの検出器で検出した場合を「検出しなかった」と判定する方法がある．本実験では出力モードしか光子検出を行わなかったが，検出確率の導出にあたっては，ほかの3つの出力モードにも3つの同等の検出器を設置していたと想定，毎秒60万個の光子を計4つの検出器でカウントしていたと推定し，検出確率を求めた．

実験結果を図8に示す．図8からわかるように，入力ビット列が「等分」のときにはほぼ検出確率は0であり，また「均一」のときにはほぼ1であった．このことから，光子を検出すれば「等分でない」と，また光子を検出しなければ「均一でない」と，この量子計算機は正しく判断していたことがわかる．

しかし，等分の入力に対しても光子を検出してしまう確率は0ではなく，これがこの計算機のエラーとなる．この実験では，「光子を検出したが入力は実は等分であった」というエラー率が2.6%，「光子を検出しなかったが均一であった」というエラーの率が7.7%であった．このようなエラーの原因について定量的に評価した結果，現状の実験技術を用いて，11量子ビット程度の大きさの量子計算をエラー率20%以下で実行可能であることがわかっている[17]．

筆者らが線形光学素子量子計算を提案したころ，まだ量子アルゴリズムを実証した系が存在せず，量子計算を机上の空論とする見方もあった．量子計算を実験として「やってみた」ことで，自分の中では少し理解が深まったように感じている．

この方法は，量子ビットの数をNとすると2^N個の経路が必要になる．このため，200桁の素因数分解のような

大規模な量子計算を行うことはできない．しかし，小規模な量子回路が必要な場合には手軽な方法である．量子計算を含む大きな分野として，量子力学の基本原理を情報通信や処理に応用する研究が進められており[24]，それらの中には比較的小規模な量子回路が必要とされることがある．たとえば，盗聴を検出しながらデータをロスなしに送信できる4状態量子暗号[25]や，シャノンの量子限界を超えた通信を実現する量子高密度伝送[26]などの線形光学素子を用いた実現が提案され，実験も進められている．

もちろん，線形光学素子だけでは，光子間のもつれあいを生成できないなど限界がある．本稿で述べた量子位相ゲート（QPG）が実現されるかどうかは，今後，量子情報通信，量子情報処理が現実のものになるかどうかの鍵を握るだろう．

本稿で紹介した量子計算実験は，科学技術振興事業団さきがけ研究制度のもと，三菱電機先端技術総合研究所において行ったものです．井須俊郎様，小蒲哲夫様，光通信デバイスプロジェクトチームの皆様，ならびに，吉森昭夫領域統括をはじめとする事業団の皆様に感謝します．またコメントをくださいました北海道大学の笹木敬司様に感謝します．

文　献

1) 竹内繁樹："21世紀，量子猫は計算をするか？"，日本物理学会誌，**54** (1999) 263-273.
2) 竹内繁樹，井須俊郎："量子計算の実現に向けて"，応用物理，**68** (1999) 1038-1041.
3) 細谷暁夫：量子コンピュータの基礎（サイエンス社，東京，1999).
4) 西野哲朗：量子コンピュータ入門（東京電機大学出版局，東京，1997).
5) P. W. Shor: *Proceedings 35th Annual Symposium on Foundation of Computer Science* (IEEE Comput. Soc., Los Alamos, California, 1994) p. 124.
6) 岡本龍明：図解暗号と情報セキュリティ（日経BP社，東京，1998).
7) L. K. Grover: "Quantum mechanics helps in searching for a needle in a haystack," Phys. Rev. Lett., **79** (1997) 325-329.
8) R. J. Hughes, D. F. James, E. H. Knill, R. Laflamme and A. G. Petschek: "Decoherence bounds on quantum computation with trapped ions," Phys. Rev. Lett., **77** (1996) 3240-3243.
9) J. I. Cirac and P. Zoller: "Quantum computation with cold trapped ions," Phys. Rev. Lett., **74** (1995) 4091-4094.
10) 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: "Experimental entanglement of four particles," Nature, **404** (2000) 256-259.
11) B. E. Kane: "A silicon-based nuclear spin quantum computer," Nature, **393** (1998) 133-137.
12) A. Barenco, D. Deutsch and A. Ekert: "Conditional quantum dynamics and logic gates," Phys. Rev. Lett. **74** (1995) 4083-4087.
13) D. Loss and D. P. DiVincenzo: "Quantum computation with quantum dots," Phys. Rev. A, **57** (1998) 120-126.
14) Y. Nakamura, Yu. A. Pashkin and J. S. Tsai: "Coherent control of macroscopic quantum states in a single-Cooper-pair box," Nature, **398** (1999) 786-789.
15) J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Wal and S. Lloyd: "Josephson persistent-current qubit," Science, **285** (1999) 1036-1039.
16) I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung and S. Lloyd: "Experimental realization of a quantum algorithm," Nature, **393** (1998) 143-146.
17) S. Takeuchi: "Analysis of errors in linear-optics quantum computation," Phys. Rev. A, **61** (2000) article no. 052302.
18) I. Chuang and Y. Yamamoto: "Simple quantum computer," Phys. Rev. A, **52** (1995) 3489-3496.
19) Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi and H. J. Kimble: "Measurement of conditional phase shifts for quantum logic," Phys. Rev. Lett., **75** (1995) 4710-4713.
20) S. Takeuchi: "Simple quantum computer: Realization of the Deutsch Jozsa algorithm with linear optics," *Proceedings of Fourth Workshop on Physics and Computation: PhysComp96* (Boston, 1996) p. 299.
21) N. J. Cerf, C. Adami and P. G. Kwiat: "Optical simulation of quantum logic," Phys. Rev. A, **57** (1998) R1477-R1481.
22) J. C. Howell and J. A. Yeazell: "Linear optics simulations of the quantum baker's map," Phys. Rev. A, **61** (1999) 1-4.
23) D. Deutsch and R. Jozsa: "Rapid solution of problems by quantum computation," Proc. R. Soc. London, **439** (1992) 553-558.
24) 郵政省：量子力学的効果の情報通信技術への適用とその将来展望に関する研究会報告書 (2000).
25) K. Shimizu and N. Imoto: "Communication channels secured from eavesdropping via transmission of photonic Bell states," Phys. Rev. A, **60** (1999) 157-166.
26) M. Sasaki, S. M. Barnett, R. Jozsa, M. Osaki and O. Hirota: "Accessible information and optimal strategies for real symmetrical quantum sources," Phys. Rev. A, **59** (1999) 3325-3335.

(2000年8月17日受理)