量子コンピューティング

井元信之

近年，量子力学の不思議な性質を直接情報処理に利用しようという研究が盛んになってきた．量子コンピューティングや量子暗号がそれであるが，これらをひとまとめに量子情報処理と呼ぼう．これらは量子力学における不確定性原理を，雑音の源とみなすのでなく，新しい情報処理を行うために積極的に利用している点に魅力がある．特に「コンピューティング」は汎用性を期待させる語感があるので，最近とみに期待をもって注目を浴びている．しかし実際のところ量子コンピューティングは現時点では素因数分解など限られた応用のみ考えられており，一方量子暗号は単なる暗号伝送にとどまらない応用の可能性も考えられるので，量子コンピューティングの名で総体的に量子情報処理について論じるのが現時点では適当と思われる．ここでは特に光の科学との関連においてその解説を試みたい．

量子情報処理と光の科学の関係は今のところ次のようにいえるであろう．量子暗号は光ファイバー通信もしくは空間伝送が念頭に置かれているが，いずれにせよ光子通信の形態をとることがほぼ確定的であるので，いわば光子情報処理そのものといってよい．一方，量子コンピューティングでは情報の担体として光が適切かどうかまだ固まっていない．むしろ後述のように電子状態やスピン状態を使う方法が有望かもしれない．しかしそうであったとしても，電子状態やスピン状態の“制御”を光で行うことになる可能性はある．さらにそれらの状態の理論的扱いは光物性におけるブロッホベクトルの取り扱いや光カー効果による量子非破壊測定の概念で直観的に理解できるため，量子情報処理は量子光学とのなじみが良い．これらの理由によって，この分野には量子エレクトロニクスの研究者も多く参入している．

NTT 物性科学基礎研究所（〒228-0198 厚木市森の里若宮 3-1）
E-mail: nobu@will.brl.ntt.co.jp
現在： 総合研究大学院大学先導科学研究科（〒240-0193 神奈川県三浦郡葉山町湘南国際村）

1. 量子暗号

1.1 非公開鍵暗号

暗号技術は最も単純な非公開鍵暗号と整数論に基づく公開鍵暗号とに大別される[1]．現在普及しているのは公開鍵暗号であるが，量子暗号と関係があるのは非公開鍵暗号である．これは送信者と受信者があらかじめ鍵すなわち乱数表を共有しておき，送信者はメッセージをその鍵で暗号文に変換して送り，受信者が同じ鍵で元のメッセージに戻す方法である．非公開鍵暗号の中でも，一度使った鍵を使い捨てとする one-time-pad 法は完全な安全性を有していることが知られている．

たとえば送信者のメッセージを二進数で表し，それに二進乱数鍵と排他的 OR と呼ばれる演算を施す．排他的 OR は表 1 にしたがって 2 つの bit 入力に対し 1 つの bit を出力する演算である．排他的 OR の逆演算はそれ自身なので，受信者は暗号文と鍵の排他的 OR をとると元のメッセージを再現できる．

この方法の問題点は同一の鍵をいかにして安全にあらかじめ配っておくかにある．完全に信頼できるメッセンジャーボーイを仮定しなければ，古典的方法では真に安全な鍵配送法はない．この「真に安全な鍵配送」の方法として提起されたアイデアが量子暗号である．

1.2 単一光子通信による鍵配送

図 1(a)のように，1 つのビットに対応する光パルスに光子をきっかり 1 個載せることができたとし，その偏光を変調することにより，たとえば水平偏光をビット“0”とし，垂直偏光をビット“1”として鍵を送るとする．この取り決め自体は公開され，盗聴者も知り得るとする．送信者は元

表1　排他的ORの入出力規則．

入力1	入力2	→	出力
0	0	→	0
0	1	→	1
1	0	→	1
1	1	→	0

になる乱数表を見ながら光子を1つずつ受信者に向けて送り出す．送受信系中の光損失は避けられないので，図の光子伝送路以外にも古典的通信路を設け，どの光子が受信者に届いたかを確認する．到達しなかったビットについては送信者は元の乱数表から落とす．これにより元の乱数表より小さくなるが，共通の乱数表が構築できることには変わりがない．伝送路としては光ファイバーでも空間ビームでもよい．ここで，図中点線によって区分けられた“送信者側”は送信者によって，“受信者側”は受信者によって管理されており，盗聴者は“伝送路”の部分だけにアクセスすることができると仮定する．

まず盗聴者がビームスプリッターにより盗聴を試みた場合を考える（図1(b)）．光ファイバー系の場合，これはファイバーを曲げて漏洩光を検知するとかファイバーカップラーを挿入してタッピングすることに相当する．しかしこの方法では盗聴できないことは次のようにしてわかる．光子はビームスプリッターによって分割されることはなく，個々の光子は透過率の確率で通過するか反射率の確率で盗聴されるかのどちらかであるので，盗聴された光子は受信者に到達せず乱数表の構築に寄与しない．同様に乱数表の構築に寄与した光子は盗聴されていないことが明らかである．したがって，きっかり1個の光子/ビットの通信ができれば，ビームスプリッターによる盗聴は成立しないことがわかる．

しかしこれはビームスプリッターによる盗聴攻撃に対してだけ安全ということであり，他のいかなる盗聴手段に対しても安全ということではない．実際，図1(c)のように受信者と同じ装置で受信し情報を得てから送信者と同じ装置でにせの光子を受信者に送るという，いわゆるstop-and-resendという盗聴法が原理的に可能である．これはいわば量子識別再生器（quantum repeater）による盗聴である．さらに図1(d)のような量子非破壊測定[2]により盗聴することも原理的にはできる．原理的と断っているのは，現在満足のいくそのような技術が開発されていないというまでであり，未知の第三者の技術を含めあらゆる盗聴手段に対処できるためには原理段階で安全性が保証されなければならない．

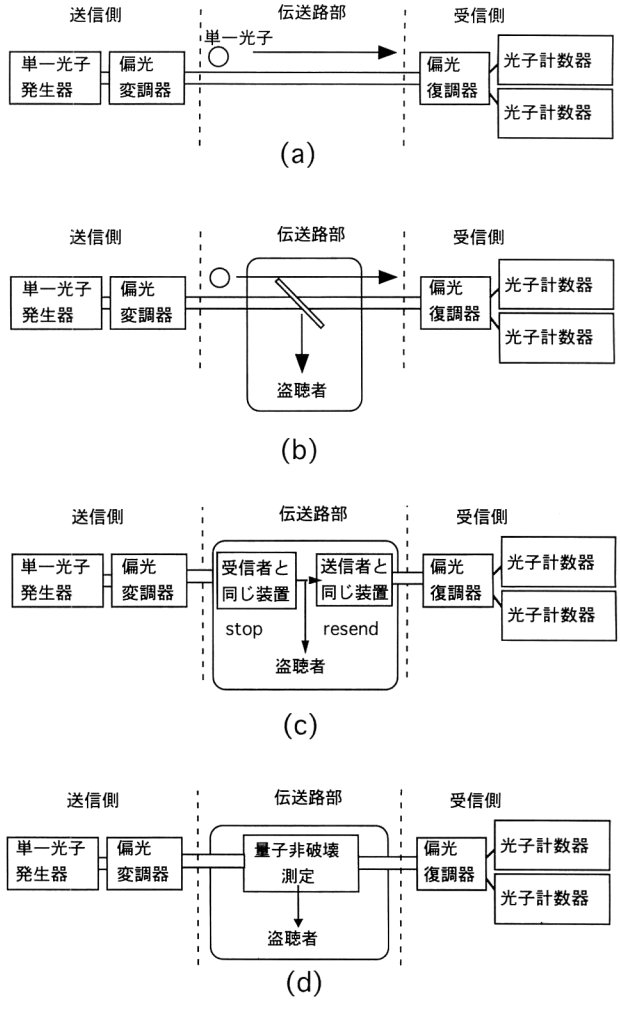

図1　単一光子通信系．(a) 送受信者のみ，(b) ビームスプリッターによる盗聴（成立しない），(c) 量子識別再生による盗聴（成立），(d) 量子非破壊測定による盗聴（成立）．

1.3　四偏光量子暗号（BB84）

前節の単一光子通信においては，その変復調法は決定論的であり，装置が完全で盗聴者もいないとすれば受信者が間違う余地はなかった．したがって受信者と同様な立場にいる盗聴者も誤りを犯すことなくstop-and-resendを行うことができた．これを阻むためにはなんらかの曖昧さが送受信系に必要である．しかし普通の意味での古典的曖昧さでは，盗聴者が常に信号のコピーを作ることができるので，受信者と盗聴者に対して同等である．両者を差別化するためにはコピーのとれない[3]量子力学的不確定性が必要である．これにより，発覚しないためにはコピーをとらなければならない盗聴者と，単なる破壊測定で受信すればよい受信者を差別化することができる．

初めて提案された量子暗号はBB84と呼ばれるが[4]，そこではビットを表すのに縦横偏光と±45°偏光の2つの変復調法を送信者が1ビットずつランダムに選択して送信する．この2つの1ビット変数—直線偏光が「縦横か？」あ

るいは「±45°か？」—の間には不確定性原理があり，1つの光子に対してこの2つを同時に測定することはできない．そこでBB84の具体的プロトコルは次のようになる．系は図1(a)と同じで，偏光変調法として縦横変調と±45°変調を使う．

Step 1： 元になる乱数表を見ながら送信者は1ビットごとにランダムに縦横変調か±45°変調を選び，光子を送信する．ただし光子送信のタイミング以外の情報は公表しない．

Step 2： 受信者も独立に縦横復調か±45°復調を選び，光子を受信する．

Step 3： 事後に送信者と受信者は古典的別回線でそれぞれの選択を公開し，両者の選択が一致した約半数の測定結果をそれぞれ保管し，一致しなかった残りのビットは捨てる．盗聴者がいなければこれだけで同一乱数表の発生が可能である．

Step 4： 盗聴痕跡を検出するため，保管しているビットの中から適当数のビットを合議の上ランダムに選んでテストビットとし，その測定値まで確認する．盗聴があれば1つのテストビットにつき0.25の確率で測定値の不一致が発見される．言い換えると，0.75の確率で盗聴者を逃す．そこで，危険率εに対し，$N \equiv \log(\varepsilon)/\log(0.75)$個をテストビットとすることにより，設定した任意の危険率でしか盗聴者を逃さないようにできる．

Step 5： テストの結果測定不一致のなかった乱数表は危険率ε以下で「盗聴痕跡のない鍵」として採用する．

1.4 量子暗号理論の発展

量子暗号は前節のBB84だけでなくいろいろな種類が考案されている．その動機はいろいろあろうが，中でも重要な動機としては，① 各デバイス・伝送路が完全でないとき（通常必ずそうである）原理的に量子暗号は成立するか？成立させるにはどのような構成にすればよいか？，② 量子暗号の本質は何か? あらゆる盗聴攻撃に対処できることの証明の本質はどこにあるか？，③ 量子情報処理を鍵配送以外のプロトコルに応用することはできないか？，の3つを挙げたい．これらについて詳述はしないが，筆者のグループの研究を中心に文献を挙げておく．上記①に関しては5)，6)を，②に関しては7)〜9)を，③に関しては10)〜13)およびそれぞれの末尾参考文献を参照されたい．

2. 古典コンピューティングの能力

現在すでに公開鍵暗号が普及している状況のもとで，量子暗号を研究する意義は何であろうか．それに答えるためには公開鍵暗号および量子コンピューティングに触れないわけにはいかない．

現在使われているコンピューターでは情報をすべて実数特に“0”と“1”の2値で表し，それらの演算で処理する．これを古典コンピューティングと呼ぶことにすると，これでは解くのに非常に時間がかかるある種の(しかも重要な)問題がいくつかあることが知られている．たとえば次の2つの問題を比べてみよう．

問題1： □×□=408034873

問題2： 14593×27961=□

これらは同一の掛け算問題とその逆問題つまり素因数分解問題であるが，問題2が単純に計算できるのに対し，問題1を解くのには大変手間がかかる．したがって問題1のほうが解くのに要する計算の複雑さの度合いが大きい．計算量理論においてはこの複雑さを次のように分類する．

- やさしい問題： 問題のサイズをn倍したとき解くためのステップ数がたかだかnの多項式で増える問題
- 難しい問題： 問題のサイズをn倍したとき解くためのステップ数が，nの多項式で書けないほど急速に増える問題

多項式（polynomial）のpをとって，前者をP型問題という．素因数分解の場合，問題のサイズとは桁数のことである．かけ算が試行錯誤を含まない一方向の計算であるのに対し，素因数分解は基本的に小さい素数から順に割り切れるか確認していくしか方法がなく，数字が大きくなった場合の素数分布の減り方がlogという非常に緩慢な減り方のため，素因数分解するために必要な計算ステップ数は桁数Nに対し$e^{\sqrt{N}}$程度で急激に増える．具体的には整数の桁数が200桁を超えると，現在のコンピューターでも宇宙的時間がかかる．

現在普及している公開鍵暗号方式は素因数分解が「難しい」問題であることに根拠を置いている．公開鍵暗号とは次のような手順に基づく暗号である．

1. まず受信者がエンコード鍵eとデコード鍵dを生成：
   (a) 2つの大きな素数pとqを選択，$(p-1)$と$(q-1)$の最小公倍数Lを計算．
   (b) Lと互いに素でLより小さい整数eを選択．
   (c) $ed=1 \pmod{L}$によりdを求める．
2. 受信者はdを取っておきeと$N \equiv pq$を公開．公開された2整数から第三者がpとqを(したがってdを)求めることは「難しい」問題．
3. 送信者は二進数で表現されたメッセージ(plain text)

P から暗号文（cipher）C へ，式 $C=P^e \bmod N$ により変換．暗号文 C を公開し受信者が受信．

4．受信者は逆演算 $P=C^d \bmod N$ により平叙文 P を得る．

上記手順からわかるように「非公開鍵の配送」のプロセスがないのでこの方式に「盗聴」の概念はないが，素因数分解が「難しい」問題であるかぎり第三者が解読に成功することは事実上ない．

素因数分解のほかに難しい問題すなわちP型に属しない問題の例としては離散対数や巡回セールスマン問題がある．ただしこれらがP型に属しないというのは証明されておらず，そう信じられているだけである．

3. 量子コンピューティングによる素因数分解

3.1 背　　景

1985年イギリスのDavid Deutschは，演算の種類を古典コンピューティングに限らず量子コンピューティングまで広げることを提唱し，それを許せば，ある種の非P型問題がP型問題に帰着することを示した[14,15]．ここで量子コンピューティングとは入力情報を物質または光の量子状態に載せ，(1) 波動関数の並列処理，(2) 2つの系の量子力学的絡み合い，(3) 観測による波動関数の収縮を利用した情報処理を行うことにより解答を出力するような演算を意味する．Deutschの問題は重要な問題とはいえなかったので当初はあまり注目されなかったが，1994年ベル研究所のPeter Shorが，素因数分解も量子コンピューティングによりP型問題に帰着することを証明した[16]．これは現在社会に普及しているセキュリティー通信の原理的安全性が脅かされることを意味するため大きな衝撃を与え，量子コンピューティングは非常に注目される分野となった．

3.2 確率的アルゴリズム

素因数分解の量子アルゴリズムの前に，まず素因数分解の確率的アルゴリズムを紹介する．もちろん確率的アルゴリズムによって素因数分解がP型問題になるわけではないが，量子アルゴリズムの説明に必要となる．いま，N を与えられた大きな（たとえば200桁の）整数，m をランダムに選ばれた小さな（たとえば2桁以下程度の）整数とし，n を0，1，2,…と動く整数変数とする．このとき，

1．数列 $F_n \equiv m^n \pmod N$ を作れ．ただし mod N とは，N で割り算した余りを求めることを意味する．

2．数列 F_n の周期 r を求めよ．$[F_{n+r}=F_n]$

3．N と $m^{r/2}\pm 1$ の最大公約数 d を求めよ．ここまでの手順で d を求めると，高い確率で d は N の約数になっている．そこで最後に確認のステップとして，

4．N が d で割れるか確認し，割れない場合は別の m を選び1．からやり直す．

とすることにより素因数分解ができる．このアルゴリズムの有効性は簡単な例，たとえば $N=15$，$m=2$ などで簡単に確認することができるので，各自試みることを勧める（ちなみにこのとき周期 r は4となり，$m^{r/2}\pm 1$ はそのまま $N=15$ の約数として見いだされる）．上記手順のうち1．と3．と4．はP型問題であるが，2．はそうではない．Shorのアルゴリズムはこの2．を量子コンピューティングにより効率的に行おうというものである．

3.3 量子論理素子

通常のコンピューターにはbitと呼ばれる二値論理素子が使われるが，量子コンピューティングではqubitと呼ばれる二準位系が単位系として使われる．その1つの状態を $|0>$ で，他方の状態を $|1>$ で表すと，これら2つの重ね合わせ状態 $\alpha|0>+\beta|1>$（ただし $|\alpha$，β は複素数で $|\alpha|^2+|\beta|^2=1$）もまたこの系の別の状態として許される．この点が古典的bitにはないqubitの特徴である．この意味で量子論理はデジタルではなく，アナログである．

また，通常のコンピューターではAND, OR, NOTなどの少数の演算の組み合わせであらゆる計算が可能であることが知られているが，量子コンピューティングではアダマール変換と制御NOTの2つが基本論理となる．この2つで古典論理を包含する量子論理をすべて構築できることが知られている．

アダマール変換とは，物理的には二準位系に $\pi/2$ の光パルスを照射する作用と同等の変換である．たとえば $|0>$ は $\frac{1}{\sqrt{2}}(|0>-|1>)$ に，$|1>$ は $\frac{1}{\sqrt{2}}(|0>+|1>)$ に変換される．この変換は，南極を $|0>$，北極を $|1>$ とする球上で90°回転させることを意味する．上記 $\frac{1}{\sqrt{2}}(|0>-|1>)$ や $\frac{1}{\sqrt{2}}(|0>+|1>)$ は赤道上相対する点となる．この変換は2回続けると準位反転の効果をもたらすので $\sqrt{\mathrm{NOT}}$ ともいわれる．

一方，制御NOTとは2つのqubitが相互作用する演算で，入力1が0のとき出力は入力2と同じで，入力1が1のとき出力は入力2を反転させたものになる．この意味で，入力1を制御ビットあるいはcontrol bit，入力2を被制御ビットあるいはtarget bitと呼ぶ．これは表1の入出力関係と全く同じである．物理的には光カー効果を用いた光子数の量子非破壊測定[2]の作用と同等である．光子数の量子非破壊測定系の「被測定光」がここでの「制御光」に相当し，「プローブ光」が「被制御光」に相当する．アダマール変換が一入力一出力であるのに対し，制御NOTは二入力二出力の素子である．

以上の2つの素子を「多項式個」組み合わせることによ

り，有限個の二準位系（＝量子演算レジスター）上のフーリエ変換を行うことや，2つの量子演算レジスターを絡ませる（entangle させる）ことができることが知られている[17]．

3.4 量子計算による素因数分解

Shor のアルゴリズムはいくつかの解説に記載されているが，ここでは数式を使わず，言葉だけで説明を試みる．これはかなり無茶な試みであるが，数式つきの他の解説[17-23]を読む前に次のあらすじに目を通しておくことは無駄ではないと思われる．

3.1節の確率的アルゴリズムを現在の（つまり古典的）計算レジスターで行おうとすると，まず n を0から N へ向けて掃引するためのレジスター1と，数列 F_n を格納するレジスター2が要る．これらのレジスターが含むべきビット数 M はおよそ $\log N$ のオーダーである．古典的計算では3.1節の Step 1でレジスター1が n のとき F_n を計算してレジスター2に格納し，しかる後 Step 2で n を掃引する．

ところが，量子コンピューティングでは以上のことを一瞬に行うことができる．まず，レジスター1のすべての qubit に $\pi/2$ パルスを照射する．これによりすべての qubit は基底準位と励起準位の重ね合わせ状態となるが，これは実はレジスター1全体がとり得る0から 2^M-1 までのすべての状態を全部重ね合わせた状態になっている．次にすべきことは，「レジスター1が n と判定されたときレジスター2が F_n となる」ように条件つき演算を量子ゲートを使って行う．これは両レジスターを「絡ませる」作業である．証明は略するが，この作業も多項式ステップ数以内で行える．

このようにして n の掃引をまともに行わず，周期関数 F_n をレジスター1（引数）とレジスター2（関数）にビルトインする作業が一度に並列処理できた．しかしこのままではまだ周期 r を求めたことにならない．周期関数から周期を引き出すにはフーリエ変換が必要である．量子レジスター2のフーリエ変換をレジスター1に書き込むプロセスも実は量子ゲートの多項式個の組み合わせで実現する回路が見いだされている．このフーリエ変換を実行すれば，レジスター1の波動関数は番号 r 番目の状態の確率だけデルタ関数的に存在し他の確率はゼロとなる．もちろん実際は有限サンプリングのフーリエ変換であるしアナログ計算に基づく誤差もあるので，デルタ関数よりはなまった関数になっている．最後にレジスター1の観測を行えば，高い確率で周期 r が求まる．確率的アルゴリズムなので答えが違っている可能性があるが，そのときは違う m を選択してすべての計算をやり直す．このようにして何回目かに（exponential 的には大きくない回数で）解が求まる．

以上が量子コンピューティングによる素因数分解の概要であるが，ここで，ペンディングしていた量子暗号の存在意義について触れておこう．もし量子コンピューティングが実現し数百桁の整数の素因数分解が短時間にできたとすると，公開鍵暗号の安全性は全く根拠を失う．しかしそれでも量子暗号は残る．もちろん量子コンピューティング実現以前に古典コンピューティングで公開鍵暗号が破られる可能性もあるのだが，いずれにせよ量子コンピューティング研究の進展は量子暗号の存在意義を高める結果をもたらす．

4. 実験研究

4.1 量子暗号

量子暗号の提案者の一人である Bennett は He-Ne レーザーを使い空間30 cm を伝送する実験を行ったが，これは全くの予備実験で，本格的実験は光ファイバー通信に近い形態で British Telecom のグループが1992年ごろから始めた．この実験では波長1.3 μm 半導体レーザー，単一モード光ファイバー，光ファイバー方向性結合器，光ファイバー偏光整合器，APD フォトンカウンターを用い，オール光ファイバー系による量子暗号の可能性を追求している．一方，光ファイバーでなく空間光ビームによる実験も検討されている．これは衛星通信を念頭に置いたものである．空間伝送では大気の吸収が小さい0.7 μm の波長が用いられる．実験については文献24)～27）を参照されたい．光子通信であるので光損失によるビット欠落が避けられず，伝送速度はせいぜい 10^3 bit/sec 程度で遅い．これはまだ実験途上なので速くなるであろうが，鍵配送は一日中バックグラウンドジョブとして行えるので，通常通信ほどの大容量高速通信は必要ない．

4.2 量子コンピューティング

量子コンピューティングで使う二準位系としてはいろいろなものが検討されているが，実験的にはイオントラップ[28]，共振器量子電気力学[29]，有機液体の NMR（核磁気共鳴）[30]で基礎実験が行われている．イオントラップではクーロン反発力で整列トラップされたベリリウムイオンの電子準位を使って二準位系とし，全体を伝わるフォノンを媒介として，任意の2つのイオン間の相互作用を可能にしている．共振器量子電気力学では，Q 値の高いファブリー・ペロー光共振器に入射する波長の異なる2つの光子それぞれが，円偏光が右回りか左回りかによって二準位系の役割を果たす．二準位系同士の相互作用は，同時に入射するセ

シウム原子によりもたらされる．有機液体のNMRでは，クロロホルムの炭素原子と水素原子の核スピンが＋か－かで二準位系としている．それぞれの原子に個別にアクセスする空間分解能は現在のところできないが，幸いなことに配位の違いからそれぞれの原子の共鳴周波数が若干ことなり，そのため，当てるラジオ波の周波数により個別原子にアクセスすることができる．二準位系間の相互作用はスピン-スピン相互作用を使う．

いずれの実験でも，扱われたビットの数は2ないし3程度で，まだまだ量子コンピューティングを行っているとはいいがたい．しかしこれからの研究進展に欠かせない通過点である．特に実験が進んでいるのはNMRである．この系の特徴は，1つのクロロホルム分子が1つの量子コンピューターの役目を負っている．このため，最終段階で1つの量子コンピューターの観測による波動関数の収縮（これは難しい）を見る必要はなく，およそアボガドロ数個存在する光子の統計的状態測定ですむ．逆に分子1個が量子コンピューターなので，扱えるビット数がおのずと制限される．しかし量子コンピューティングの問題点を調べるには今のところ最適な系である．

量子暗号はすでに原理確認実験の域を出て伝送実験の域に進んでいるが，量子コンピューティングは原理確認実験の域を出るのは当分先のことと考えられる．前者はビットごとに独立に扱うことができ，かつ演算ステップも多くないので，理論を実現するのは比較的困難でないと予想される．後者は現在のコンピューターを凌駕するためには数百の量子ビットが絡む何千という多くの演算ステップを行う必要がある．この計算のあいだじゅう誰も中を覗いてはならず，人でなくとも環境からの接触があってはならない．そしてデジタルでなくアナログなのでアダマール変換や制御NOTには誤差が伴い，その積み重ねの影響も解明されてはいない．通常の情報理論にはたかだか10^{-9}以下の誤り率できちんと動作するデバイスが現実に対応しているが，量子情報理論には今のところそれはなく，理想理論のもくろみどおり量子コンピューティングが行われるか否か，その方面からも検討する必要がある．

しかし量子情報処理はこれまでの情報処理に革命をもたらすものである点で魅力に満ちており，その実現のために障害をひとつずつ取り除いていく研究はきわめて重要と考えられる．ことに量子効率が高くダークカウンティングが少ないフォトンカウンターや大きな光非線形を有する材料の開発，それに望むモードとタイミングで光子をきっかり1個発生する技術や物質の量子状態の光制御の研究など，光科学が関連するテクノロジーの発展もこの分野の発展に欠かせない．これらの材料や素子の研究に従事されている方々が，従来技術から要求されるスペックだけでなく，量子コンピューティングや量子情報処理に要求されるスペックをも念頭に置いて研究を進めてもらえれば幸いと考える．

文　献

1) 岡本龍明，太田和夫：暗号・ゼロ知識証明・数論（共立出版，1995）．
2) 井元信之：光学，**19**（1990）762.
3) W. K. Wootters and W. H. Zurek: Nature, **299**（1982）802.
4) C. H. Bennett and G. Brassard: *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India（IEEE, New York, 1984）p. 175.
5) B. Huttner, N. Imoto, N. Gisin and T. Mor: Phys. Rev. A, **51**（1995）1863.
6) M. Koashi and N. Imoto: Phys. Rev. Lett., **77**（1996）2137.
7) L. Goldenberg and L. Vaidman: Phys. Rev. Lett., **75**（1995）1239.
8) M. Koashi and N. Imoto: Phys. Rev. Lett., **79**（1997）2383.
9) M. Koashi and N. Imoto: Phys. Rev. Lett., **81**（1998）4264.
10) B. Huttner, N. Imoto and S. Barnett: J. Nonlinear Opt. Phys. Mater., **5**（1996）823.
11) K. Shimizu, N. Imoto and T. Mukai: Phys. Rev. A.
12) A. Karlsson, M. Koashi and N. Imoto: Phys. Rev. A, **59**（1999）162.
13) K. Shimizu and N. Imoto: Phys. Rev. A.（in press）
14) D. Deutsch: Proc. R. Soc. London A, **400**（1985）97.
15) D. Deutsch: Proc. R. Soc. London A, **425**（1985）73.
16) P. W. Shor: *Proc. of the 35th Annual IEEE Symposium on Foundations of Computer Science*（1994）p. 124.
17) A. Ekert and R. Jozsa: Rev. Mod. Phys., **68**（1996）733.
18) C. P. Williams and S. H. Clearwater: *Explosions in Quantum Computing*, TELOS（The Electric Library of Science）（Springer, 1997）.
19) 西野哲朗：量子コンピュータ入門（東京電機大学出版局，1997）.
20) 細谷暁夫：パリティ，**11**, No.12（1996）50.
21) 細谷暁夫：日本物理学会誌，**52**（1997）748.
22) 北川勝浩：応用物理学会スクール「光と物質の量子状態の制御と応用」（1998）p. 71.
23) 井元信之：物理学会セミナーテキスト「アインシュタインとボーア」（1998）p. 22.
24) C. Marand and P. Townsend: Opt. Lett., **20**（1995）1695.
25) A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden and N: Gisin: Appl. Phys. Lett., **70**（1997）793.
26) B. C. Jacobs and J. D. Franson: Opt. Lett., **21**（1996）1854.
27) R. J. Hughes, E. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan and M. Schauer: Contemp. Phys., **36**（1995）149.
28) C. Monroe, D. Meekhof, B. King, W. Itano and D. Wineland: Phys. Rev. Lett., **75**（1995）4714.
29) Q. Turchette, C. Hood, W. Lange, H. Mabuchi and H. J. Kimble: Phys. Rev. Lett., **75**（1995）4710.
30) I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Lenng and S. Lloyd: Nature, **393**（1998）143.

（1999年2月12日受理）