

1

量子コンピュータ
—その本質と、最近の研究展開

竹内 繁樹 [北海道大学電子科学研究所]

量子コンピュータの本質は、重ね合わせ状態をとることのできる量子ビットをその基本単位とすることにある。本稿ではまず、その重ね合わせ状態の物理的な意味を、光子と干渉計を用いた仮想実験を通じて明らかにする。さらに、通常の物理系では重ね合わせ状態が位相緩和によって有限時間しか維持できないことを述べる。後半では、2000年以降のさまざまな研究展開のうち、特に実装に関連した2つの流れについて取り上げる。1つは、位相緩和の問題を解決する、量子誤り訂正符号を組み込んだエラー耐性のある量子計算に関する研究、もう1つは、小規模量子回路の量子通信への応用を目指した研究について取り上げる。

はじめに—本稿の執筆にあたって考えたこと

1985年にD. Deutschの発案した量子コンピュータが実質的に世にでたのは、1994年にP. Shorが因数分解のアルゴリズムを発表したときだろう。今年はそのから12年にあたる。実は、私は1999年に本誌からの依頼で、『量子計算機』の現状と今後」と題した解説¹⁾を書かせていただいている。その頃はようやく関心を持たれた頃で、まだ量子コンピュータという言葉は一般的でなかった。

そこで現在はどうかだろうと、Googleで検索してみた。すると、「量子計算」で85万3千件、「量子コンピュータ」でのヒット数は23万7千件に上ることが分かった。ちなみに「スーパーコンピュータ」のヒット数が85万5千件である。以前は「量子計算」で検索した場合、その上位は分子軌道を量子力学的に計算する方法(量子化学計算)などが現れたように思う。しかし今回は、19件目まですべて本稿が対象とする「量子計算」だった。正直、これらの結果には筆者自身驚かされた。「量子計算」「量子コンピュータ」が、ここわずか7年の間に、いかに急激にポピュラーになったかが分かる。

実は、編集部からいただいた仮題は「量子コンピュータ入門」というものだった。しかし一般的な(教科書的な)量子コンピュータの入門という意味ではすでに前の解説があり、またその後この7年の間にも、拙著²⁾を含

めた入門的な啓蒙書が出版されている。そこで、本稿では一般的な(教科書的な)量子コンピュータの入門を目指すのではなく、次の2つのポイントに的を絞って、解説することにしたい。

- 量子コンピュータでいうところの「重ね合わせ状態」とは何か。
- この7年間で、研究はどのような方向に発展したのか。私は、量子コンピュータの研究は歴史の必然的な流れの中で行われていると思っている。単に「量子コンピュータがあれば、巨大な数の因数分解が高速になる」という理由だけではない。本稿では、物理屋を駆り立てる「理由」にも触れたいと思う。それをふまえた上で、量子コンピュータ研究のいくつかの流れについて紹介したい。

量子コンピュータでいうところの「重ね合わせ状態」とはなにか

□ 光子と半透鏡

ここでは、光子(こうし, photon)による仮想的な実験を通じて、「重ね合わせ状態」について解説する。光子とは、光のエネルギーの最小単位で、そのエネルギーは振動数に比例(波長に反比例)する。光子のエネルギーは非常に小さく、一般に目にする光はこの光子が莫大に集まったものである。最小単位であるとは、それ以上分割できない、という意味である。お金の単位が1円であり、それ以下には分割できないのと同様に、「半分の光子」と

いうものを検出することはできない。

この光子を用いた実験では、4つの装置が登場する。「鏡」、「半透鏡」、「単一光子源」および「光子検出器」である。鏡は、光を反射し、向きを変える働きをする。普段目にされている通常の鏡である。半透鏡は、光を一部だけ反射する。あまり目にされないかもしれないが、マジックミラーなどとして使われている。本稿では、光を50%透過、50%反射するような半透鏡を想定する。

単一光子源とは、ある決められた波長の光子を、1つだけ射出する装置である。以前は仮想的な存在だったが、ここ数年でさまざまな単一光子源が実現されてきている。最後の光子検出器は、光子が入射すると、それに応じて電気パルスを発生する装置である。

まず、半透鏡が光子に対してどのように振る舞うかを検討しよう。さきほど述べたように、半透鏡は光を50%反射しあるいは透過する。では、光子1つを入射した場合には、半透鏡はどのように振る舞うのだろうか。それを調べるために、**図-1**に示すような実験を考えよう。単一光子源から射出された光子を半透鏡に入射したのち、その反射側、透過側に設置した2つの光子検出器で検出する、というものである。この実験をした場合、それぞれの検出器はどのように応答するのだろうか？読者には、次の段落の「答え」に進む前に、ここで少し考えてもらいたい。

では、答えである。この実験をした場合、光子は透過側、あるいは反射側のいずれかでのみ検出される。透過側、反射側のどちらの検出器で検出されるかは、光子を入射することによってでたらめであり（確率は50%）、一度ごとどちらで検出されるかは、一切予言することができない。現在では、物理乱数発生にも用いられている。

□ 光子と干渉計

この実験結果からは、「光子を透過するか反射するかを半透鏡がでたらめに決めている」ように見える。では、はたしてこの考えが正しいのかどうか、**図-2**に示す次の実験をみてみよう。経路aから入射された光子は、最初の半透鏡1で透過（経路c）あるいは反射（経路d）された後、鏡で方向を変えられ、2つ目の半透鏡2に入射される。その2つ目の半透鏡の出口（経路e、経路f）に光子検出器（検出器E、F）を設置して、どちらから出力されるかを測定する、という実験である。ちなみに、**図-2**のように2つの半透鏡を組み合わせた装置は干渉計と呼ばれる。

まず、「光子を透過するか反射するかを半透鏡がでたらめに決めている」という考え方で実験結果を予測して

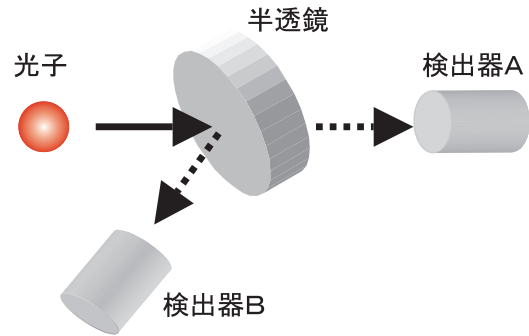


図-1 半透鏡に入射された光子

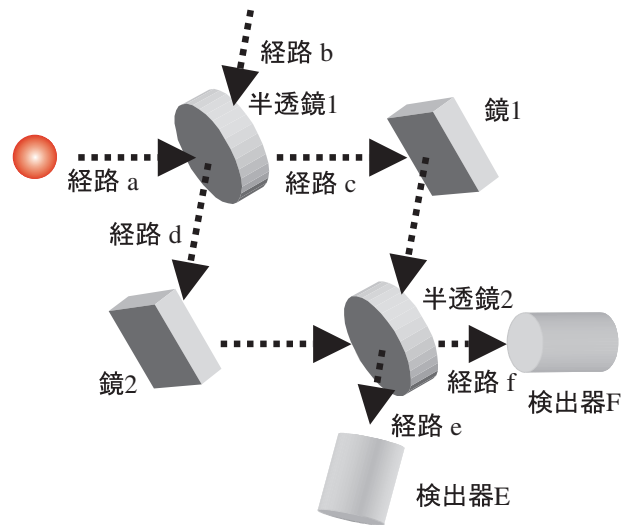


図-2 光子を干渉計に入射する実験模式図。経路c、経路dのそれぞれは、半透鏡1から半透鏡2までを鏡を経由してつないでいる。

みよう。その場合、検出器Eで検出されるのは、「両方の半透鏡で反射される場合（経路dを通った場合）」ならびに「両方の半透鏡を透過する場合（経路cを通った場合）」の2通りである。前者、後者ともに、確率は、25%。つまり、検出器Aで検出される確率は、この確率の和で50%となる。検出器Fで検出される確率も、同様に考えて50%になる。つまり、入力された光子は、最初の実験と同様に検出器E、あるいは検出器Fでデタラメに検出されるはずだ。

ところが、実際に実験を行うと、この予想とはまったく異なる結果が得られる。しかも、その結果は、2つの経路の長さ（経路長）の差に敏感に応答するのだ。経路cと経路dの長さがまったく同じ長さの場合、入力された光子は、かならず検出器Fで検出される。経路長の差を変化させると、次第に検出器Fで検出される確率が減り、それによって検出器Eで検出される確率が増える。そして、上側の経路と下側の経路長の差がちょうど

光子の波長の半分になったとき、今度は入力された光子は100%検出器Eで検出されることになる。

ここで、注意してほしいのが、2つの経路長差に結果が依存していることだ。経路c、経路d、いずれの経路長を変化させても、経路長差は変わる。この経路長差を知るには、光子は経路c、経路dの両方を「経験」しなければならない。その一方で、図-1の実験のように半透鏡の直後(経路cまたは経路d)で光子を検出すると、そのいずれかでしか光子は検出されない。この2つともが、実験の結果である。つまり、この2つの実験結果を無矛盾に説明できる「なにか」を、半透鏡の直後の光子の状態として考えなければならない。それが、重ね合わせ状態である。

□ 光子と重ね合わせ状態

量子力学では、光子の状態を長さ1のベクトルとして表す。その表す際に用いる基底ベクトルが、「経路cに存在する状態」や「経路dに存在する状態」に対応している。そして、それぞれの基底状態として観測される確率は、基底ベクトルの係数の絶対値の2乗で与えられると考える。また、量子力学では慣習として、そのベクトルを、 \vec{a} といった表記ではなく、「 $|a\rangle$ (ケット)」を用いて「 $|a\rangle$ (ケットa)」と表す。この表現に対して、違和感を持たれる方がいらっしゃるかもしれないが、慣れの問題なので、我慢しておつきあいをお願いしたい。

たとえば、図-2で最初経路aに存在する光子の状態は、 $|a\rangle$ (1) と表される。半透鏡は、式(1)から式(2)への基底変換(2×2行列)に対応するが、ここでは詳細を省略しよう。その行列を式(1)に作用させると、半透鏡1を通過したあとの状態は、

$$\frac{1}{\sqrt{2}}|c\rangle + \frac{1}{\sqrt{2}}\exp(i(\alpha + \delta))|d\rangle \quad (2)$$

と表される。ここで、 i は虚数単位、 α は光路長差を d 、波長を λ として、 $\alpha = 2\pi d/\lambda$ として表される位相差である。ちなみにこの状態が $|c\rangle, |d\rangle$ で検出される確率は、それぞれの係数の2乗、つまり0.5と計算できる。これは、図-1を用いて行った最初の実験結果と一致する。そして、半透鏡2を通過した後の状態は、同様に式(2)に半透鏡に対応する行列を作用させることで、次のように求めることができる。

$$\sin\left(\frac{\alpha}{2}\right)|e\rangle - \cos\left(\frac{\alpha}{2}\right)|f\rangle \quad (3)$$

$|e\rangle, |f\rangle$ 共通に掛かる位相項は省略している。 $|e\rangle, |f\rangle$ の係数の2乗を計算して得られる検出器E、Fでの検出確

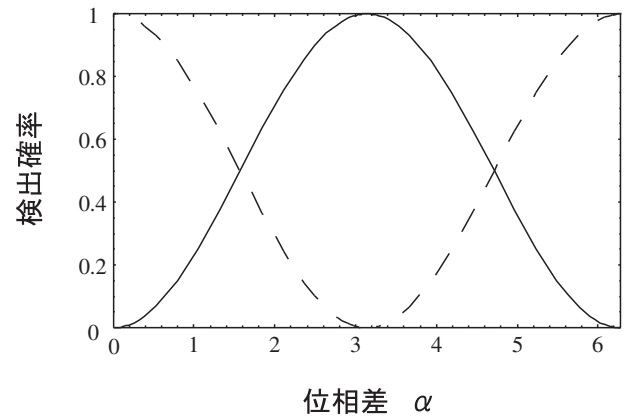


図-3 重ね合わせ状態を仮定して得られる検出確率。実線が検出器E、破線が検出器Fでの検出確率に対応する。また、位相差 α は、光路長差を d 、波長を λ として、 $\alpha=2\pi d/\lambda$ で与えられる。

率を図-3に示した。検出器Eでの検出確率(実線)に注意すると、位相差 α が0、すなわち経路長差が0のときには検出器Eでの検出確率は0であるが、経路長差を変化させると次第に確率が増え、ちょうど α が π 、つまり経路長差が波長の半分になったところで確率は1となる。これは、先に図-2について述べた実験結果と一致する。

式(2)や式(3)で表された「光子の状態」が、いわゆる「重ね合わせ状態」である。実は、光子や電子などのあらゆる素粒子の状態は、このような「重ね合わせ状態」で表される。その実験結果(=現象)は、状態をこのようなベクトルで表現し、その状態変化を、ベクトルの基底変換として演算することで、計算、予測することができる。ちょうど、ニュートン力学が実験結果を予測できたように、その新しい方法論が、量子論である。

□ 「計算規則をきめるもの」—量子ビットの誕生

情報処理の読者には釈迦に説法であることを恐れるが、通常のコンピュータにおける計算では、0または1の値をとる「ビット」と、それに対する論理演算(ANDやORなど)が基本になっている。では、なぜこのようなビットと論理演算が「基本」なのだろうか。ほかに、もっといくらでも「基本」を考えてもよいのではないかと?

こういう疑問を持ったのが、量子計算の発案者、D. Deutschである。Deutschは、自然法則こそがその基本を決めることに気がつく。では、その自然を動かしている根本法則とは? それは、量子論である。そのようにして、Deutschはビットに代わる概念として、状態 $|0\rangle$ と状態 $|1\rangle$ の任意の重ね合わせをとることができる「量子ビット」を発案した。Deutschが量子ビットとそれに基

づく量子計算を提案する事情については、文献3) に詳しいので関心のある方はぜひご覧になってほしい。

ところで、量子コンピュータの特徴は、巨大な数の並列処理が可能なことだといわれる。この点について少し解説したい。先ほどは干渉計に光子を1つだけ入射した場合を考えた。ここでは、干渉計に入射する光子の数を増やした場合について考えてみよう。まず、光子2つを干渉計に入射した場合。この場合、最初の光子が上側、下側の経路を通る場合に加えて、2個目の光子が上側、下側の経路を通る場合がある。それぞれは独立なので、全体の可能な状態数は、 $2 \times 2 = 4$ 、となる(図-4)。

同様に、光子を3つ干渉計に入射した場合には、可能な状態数は $2 \times 2 \times 2$ で8。そして、 N 個の光子を入射した場合には、可能な状態数は 2^N となる。つまり、 N 個の光子は、 2^N 個の状態の重ね合わせ状態を取り得ることになる。たとえば、光子の数がたった100個でも、 2^{100} 、つまり約 10^{30} 個の状態を並列に処理でき得る。1テラ = 10^{12} であり、これがいかに莫大か分かっていただけだと思う。

ちなみに、量子論の1つの解釈の方法として、並行宇宙論というものがある。並行宇宙論的な解釈をすれば(Deutsch自身、並行宇宙論者である)、その莫大な数の宇宙にあるコンピュータがそれぞれ計算を行い、その計算結果を宇宙間の干渉により集約することで、高速計算が可能になる、ということになる。

□ 重ね合わせ状態は壊れる—位相緩和—

前節で紹介した量子重ね合わせ状態は、実はあまり安定した状態ではない。たとえば、図-2の干渉計の一方の経路の長さが、他方に対して揺らいでしまった場合を考えよう。これは、一方の経路の気流が安定していない場合や、鏡が振動してしまっている場合に相当する。このとき、経路長差 d 、つまり位相差 α をたとえ変化させたとしても、干渉計からの出力はこの揺らぎのために、図-5に示すように位相差 α とはかかわりなく、1/2の確率で検出器Eまたは検出器Fで検出されることになる。これは、式(2)の位相差 α がもはや一定の値で確定しないため、このような光子の状態は、式(2)の重ね合わせ状態としては表せないことに対応している。むしろ、光子の状態は経路c、経路dを確率1/2で選択しているような状態になっている。このように、重ね合わせ状態が単なる確率的な状態へと変化することを、位相緩和と呼ぶ。

一般に、物理的に実現される重ね合わせ状態は、時間とともに位相緩和によって、単なる確率的な状態に変化

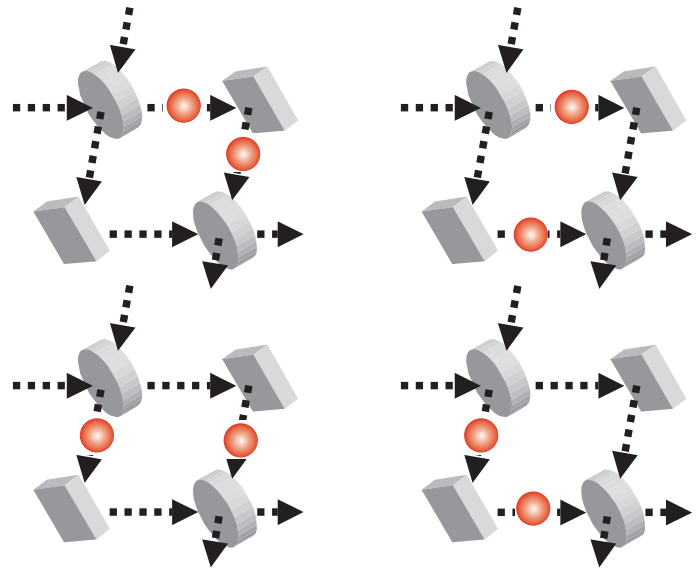


図-4 光子2つを干渉計に入射した場合、これら4つの状態の重ね合わせ状態となる。

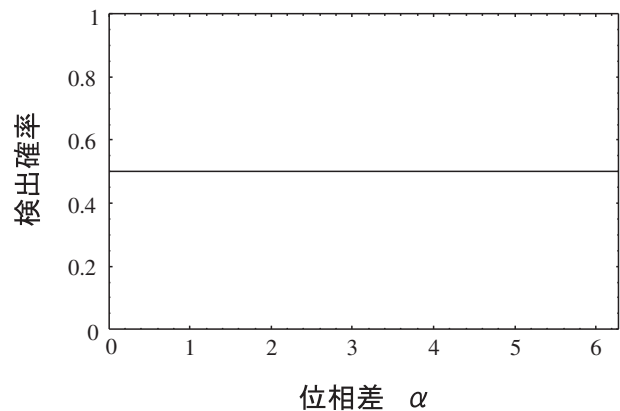


図-5 位相緩和が生じた場合の検出確率、位相差 α によらず、検出確率は一定となる。

してしまう。その時間のことを位相緩和時間と呼ぶ。位相緩和時間は、その重ね合わせ状態をとっている物理量(光子の偏光、電子スピン、原子核スピンなど)やその置かれた環境によって異なるが、せいぜい長くても数分、短いものでは数ピコ秒(10^{-12} 秒)しかない。この問題を何とかしない限りは、この位相緩和時間の間しか計算ができないことになる。

私たちがこの量子重ね合わせ状態にまつわる現象を、日常ほとんど経験することがないのは、この位相緩和が原因と考えられている。しかし、実際のさまざまな物理系の中で、どのようにこの位相緩和が発生しているのかは、まだよく分かっていない。それは、これまでそのような単一量子の状態を検出、制御する技術が発達していなかったからである。また、この位相緩和の仕組みは、量子力学の基礎の問題(観測過程)とも密接に関連してい

る。このように、位相緩和に打ち勝って量子ビットを実現し、制御することは、物理屋からみて非常に興味深い課題である。

この7年間で、研究はどのような方向に発展したのか

1999年以降の7年間で、特に物理、デバイス側から一言で振り返ると、「予想以上に進展したが、予想通り、実現への路はまだまだ長い」というものだろう。ここでは、特に物理的(実装的)な視点から、「エラー耐性のある量子コンピュータの実現に向けた研究」と、「小規模量子回路の実現に向けた研究」について紹介しよう。

□ エラー耐性のある量子コンピュータを目指して

さきほどの章で、物理的に実現される重ね合わせ状態は、時間とともに位相緩和によって、単なる確率的な状態に変化してしまうと述べた。では、量子コンピュータとは、「あっという間に状態が破壊されてしまうので、その破壊される前に計算を終わらさなければならない」というような代物なのだろうか？ 量子コンピュータの発案当初は、この問題は重大な問題であったが、現在の答えは「ノー」である。理論的には、量子誤り訂正符号と呼ばれる方法によって解決できる。

量子誤り訂正符号の考え方を簡単に説明しよう。通常の(古典的な)誤り訂正符号と同様、複数の量子ビットを用いて、1つの論理量子ビットを構成する。そして、1つの量子ビットに何か「誤り」(ビット反転や、位相反転など)が生じた場合それを検出し、訂正しようとするものである。位相緩和は、位相反転エラーの一種と見なすことができる。よって、量子誤り訂正符号を用いれば、位相緩和を打ち消すことが可能になる。つまり、量子計算を、エラー訂正の組み込まれた「論理量子ビット」によって行えば、もはや位相緩和は問題ではない。同時に、量子計算中に発生する、ゲート操作エラーも自動的に修正されることになる。このような方式は、エラー耐性のある量子計算(fault-tolerant quantum computation)と呼ばれる。

しかし、量子誤り訂正を行うには、実際の個々の量子ビットに生じるエラー(位相緩和やゲート操作エラー)が十分小さい必要がある。では、いったいどの程度のエラーが許されるのだろうか？ それを、いわゆる「エラー閾値」だ。以前は、量子誤り訂正符号を入れ子状に多重に行った場合の、 10^{-6} が閾値と考えられていた。しかし、この方法は、大量の量子ビットや操作が必要になる。たとえば、6量子ビットを用いる訂正符号を4重

に用いた場合、1論理量子ビットを表現するだけで $6^4 = 1296$ の量子ビットが必要だ。また、 10^{-6} というエラー率も、なかなか実現が困難な数字であった。

しかし、ここ数年、理論的な研究が活発に行われた結果、敷居値はよりエラーが許される方向に推移してきた。特殊な状況を仮定した場合や、ある種のエラーを重点的に考慮した理論では、 $10^{-2} \sim 10^{-3}$ という敷居値も報告されている⁴⁾。また、同時に、ハードウェアとして誤り訂正に適したシステムや、物理系自体が誤り訂正機能を持ったようなハードウェアに関する研究も始まっている。

□ 小規模量子回路の使い道—量子暗号通信との融合を目指して

別の方向性として研究が進められているのが、小規模量子回路に関するものだ。特に、光子を用いた小規模量子回路は、量子計算(量子回路)が実際の役に立つ最初のアプリケーションとなる可能性が高い。

たとえば、量子暗号を長距離化するには、良質のもつれ合った光子対を遠隔地間で共有する必要がある。それには、量子もつれ合いの純化(purification)という操作が必要になるが、その操作を小規模の量子回路で実現できる可能性がある。また、最近多くの光子が互いにもつれあった状態(多光子間もつれ合い状態)を用いて、古典的には実現できないさまざまなプロトコルが提案されている。そのような多光子間もつれ合い状態の生成や操作には、小規模量子回路が利用できる。

我々のグループでは、最近、複数光子間の量子ゲート操作が可能な素子の開発に成功した⁵⁾。それまでに提案された方法では、図-2に示したような経路間の干渉計が、多重に複雑に組み合わせられ、さらに内部に単一光子源や光子数検出器を内蔵しなければならなかった。しかしその場合、それぞれの経路の長さを、光の波長の100分の1(数ナノメートル、 10^{-9} m、原子数十個分)という精度で制御、安定化する必要がある、実現にあたっての壁となっていた。今回我々は、そのような経路干渉を必要としないゲート素子を発案、実現した(図-6)。我々は、偏光干渉計が2つ結合した簡便な構成の量子ゲートを2002年に理論提案していた。今回、偏光ごとに反射率の異なる「部分偏光ビームスプリッター」という光学部品を特別に作成することで、干渉計を一切不要にした形でその提案を実現することができた。たとえばこの素子を多段に連結するだけで、多光子もつれ合い状態(専門的には、N光子GHZ状態)を実現することが可能である。今後、小型量子回路の実現や、それを用いた新しいプロトコルの提案が期待される。

まとめ

以上、重ね合わせ状態の物理的な意味、実現に向けた問題点、また実装の観点から、エラー耐性のある量子コンピュータの研究、光量子通信内で用いられる小型量子回路の実現に向けた研究を紹介した。量子情報理論面、コンピュータサイエンス面での展開については、本特集内の各記事をご参照いただきたい。

なお、本稿で紹介した私たちの研究に対する、科学技術振興機構 CREST「量子情報処理」、総務省 SCOPE、日本学術振興会科学研究費、21世紀 COE プロジェクトの支援に対してこの場をお借りして感謝したい。

参考文献

- 1) 竹内繁樹：「量子計算機」の現状と今後、情報処理, Vol.40, No.12, pp.1192-1197 (1999).
- 2) 竹内繁樹：量子コンピュータ、講談社ブルーバックス、東京 (2005).
- 3) 古田 彩：二人の悪魔と多数の宇宙-量子コンピュータの起源-, 物理学会誌, Vol.59, No.8 (2005)
- 4) Steane, A. M. : Phys. Rev. A 68, 042322 (2003).
- 5) Okamoto, R., Hofmann, H. F., Takeuchi, S. and Sasaki, K. : Phys. Rev. Lett. Vol.95, 210506 (2005).

(平成 18 年 10 月 7 日受付)

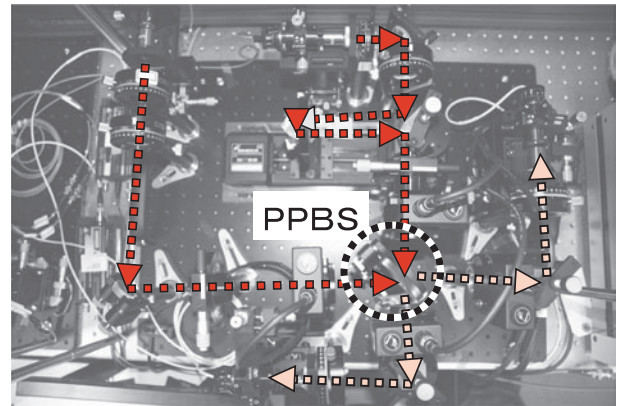


図-6 光子制御NOTゲートの実験装置写真。パラメトリック下方変換過程で発生させた2つの光子のそれぞれの偏光状態を、量子ビットとして用いた。適当な入力状態（偏光状態）を準備した後、制御NOTゲートに相当する、部分偏光ビームスプリッタ（PPBS）に入射させ、その結果として得られる2つの光子の偏光状態を解析した。その結果、量子プロセス忠実度約80%程度で制御NOTゲート操作に成功していることが明らかになった。写真からも分かるように、いっさい経路干渉計が必要ない点が利点である。

竹内 繁樹

takeuchi@es.hokudai.ac.jp

京大博士（理学）、1993年京都大学大学院理学研究科修士課程修了。三菱電機中央研究所を経て、1999年現所属講師、2000年同助教授、現在に至る。光子を用いた量子情報通信・処理の研究に従事。