2 量子情報処理と光による研究

井元 信之〔大阪大学〕

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をキーワードとする量子情報処理の研究は揺籃期を過ぎて成長期にある．当初よりずっと進んだ課題もあればブレイクスルーが待たれる課題も明確になってきた．ハード的実現のアイディアも多々出ている．これらを概観するとともに，光による研究について触れる．

はじめに

話の導入にあたって個人的目線から客観的目線へ視点を移すやり方も無駄ではないと思う．1990 年 4 月，イギリスに住んで間もない私はある小さなシンポジウムに参加した．それは非線形光学や光の量子雑音を扱う会議であったが，そこで私は 1 人の若い男が誰かれ捕まえては熱心に議論して回っているのを見た．やがて彼と会話を交わすことになり，彼が量子暗号や量子チューリングマシンの研究の面白さを説き回っていたのが分かった．その人はアルトゥール・エカート (Artur Ekert)．エンタングルメント (遠隔量子相関) を用いた量子暗号方式である E91 や E92 を彼が出版する直前のことであった．

同じ年の 5 月，私はデイヴィッド・ドイチュ (David Deutsch)，デイヴィッド・ボーム (David Bohm)，ルドルフ・パイエルス (Rudolf Peierls) という 3 巨星にインタビューした．ドイチュこそ「量子チューリングマシン」の概念を 1985 年に提唱した人物であるが，私が彼に会ったのは，量子力学の解釈の 1 つである「多世界解釈」(多重宇宙理論などと呼ばれることもある) についての議論のためであった．ボームは日立の外村氏が実証実験したアハロノフ・ボーム効果のボームで，やはり量子力学の解釈の 1 つで彼の提唱になる「非局所隠れた変数の理論」について議論した．パイエルスは固体物理の権威で，やはり量子力学の根源的問題について議論した．このときの議論は文献 1) にまとめたので参照されたい．この訪問でも──特にドイチュと──量子チューリングマシンや量子暗号の話をした．

それまで私は光ファイバー通信や量子雑音制御の研究を行っていたし，ランダウアーからベネットの流れをくむ「計算機のエネルギー消費の極小化」というコンテクストで可逆ゲートであるフレドキン・ゲートやトフォリ・ゲートのことも知っていたが，量子暗号や量子チューリングマシンはさらに「量子論の特質を積極的に使うと古典的情報処理を上回るか？」をまともに問う分野である点に新鮮味を覚えた．光ファイバー通信の研究経験から量子暗号は実験室レベルでは実現できそうだが量子チューリングマシンの実現は簡単でないことはすぐ分かった．この分野はすぐ消える一過性のものか，発展する分野か？　私は後者に賭け 1991 年帰国した．

翌 1992 年，量子暗号に関するエカートの解説を翻訳 [2] することから量子暗号の分野に入った．エカートのこの記事はベネット (Bennett) とブラサール (Brassard) が 1984 年に提案した量子暗号 BB84 を中心に解説したものだが，今でも恰好の入門記事と思う．そのころ電子情報通信学会情報セキュリティ研究会のアンテナは高く，早くも同年，招待講演を依頼された [3] のには驚いた．1993 年英国で「量子暗号・量子情報」に特化した初めての国際シンポジウムが開かれ，参加したが，まだ勉強の時期は続いた．最初の成果である量子暗号の新方式提案が Physical Review 誌に掲載されたのは 1995 年であった．

その直前，この分野に劇的進展があった．1993 年，英国の British Telecom で光ファイバーを使った B92 の実験を発表，1994 年にはベル研究所のピーター・ショア（Peter Shor）が素因数分解と離散対数の量子アルゴリズムを示した．これが物理的に実現されると公開鍵暗号が破られることになるため大センセーションを巻き起こした．

公開鍵暗号が量子コンピュータで破られるとしても，量子暗号はどうか？　この問には1997年，メイヤーズ(Dominic Mayers)が「量子暗号は安全である」ことを証明することで応えた．その理論は難解でかつ現実性の仮定が限定的なものであったが，現実の装置を用いる量子暗号の安全の保証に確信をもたらし，研究の方向付けに影響を与えた．こうして欧米では，量子暗号と量子コンピューティングの研究が一過性のものでなく発展していく研究であるという認識が根をおろし，日本でも着目されることになった．現代用語の百科事典であるimidasでここ数年筆者が担当している特集も2007年版からようやく「量子情報処理」の名が付けられた[4]．

複製禁止定理と量子暗号

普通の──我々が古典的と称する──信号や情報はいくらでもコピーをとれるが，量子力学的信号や量子情報はそうではない．たとえば1個の光子は波長（あるいは振動数），偏光，進行方向(より一般的には空間モード)，などの属性を持つ．いま振動数と空間モードは決まっていて，偏光だけが自在に変えられるものとする．どの偏光状態にあるか分からない光子が1つ与えられたとすると，それと同じ偏光を持つ光子をもう1つ作ることはできない．これが複製禁止定理(No-cloning theorem)である．

複製禁止定理の上記の表現は多分に一般的すぎるのであって，議論をより定量化する有用な場面設定の方向がいくつかある．代表的な2つの方向の1つは「多少不完全なコピーでもよいから，その不完全の度合いと可能なコピー数の関係は？」という方向であり，もう1つは「もらったものが皆目分からないわけでなく少しは情報を得ている場合」という方向である．量子暗号ではいくつかの偏光を用いるという取り決めでプロトコルが成立しているので後者の場面設定である．ただし安全性証明のためには任意の盗聴行為も考えなければならないため「盗聴のため強引にコピーを作ったらどの程度信号に傷がつくか」という議論となるので，前者も関係はある．

暗号の最も初歩的なものは「秘密鍵暗号」と呼ばれる．これは秘密鍵と呼ばれる0と1の乱数表を共有し，送信者はメール文のコードを乱数でかき混ぜて送り，受信者はその逆操作で文を再現するものである．この方法は同じ鍵を二度と使わないこと(one-time-pad)にすれば究極のプライバシーが保たれることが分かっているが，使い捨てするためいかにして次々と秘密鍵を送るかが問題である．秘密鍵を第三者に読まれずに共有することを鍵配送(key distribution)というが，これを行うのが量子暗号であり，量子的鍵配送の頭文字をとってQKDと呼ばれる．

量子論を忘れ古典的な世界の話として，いま送信者(慣例に従ってアリスと呼ぶ)から受信者（ボブ）に鍵を通信で送るにあたって，鍵を構成するビットの何割かは第三者(イヴ)に見られていることが分かっているとする．このときアリスとボブは独立な手順で元の鍵を縮め，イヴの知り得ない秘密鍵を共有することができる．これは秘匿性増強(privacy amplification)と呼ばれ，その具体的アルゴリズムも分かっている．だからもし「高々何割しか見られていない」という漏洩情報量の見積もりができるならば，究極のプライバシー通信が可能となる．

この漏洩情報量を見積もることは，盗聴者イヴの科学力を限定的に仮定──たとえば現在の我々と同じレベルのテクノロジーを持つなど──するならば，量子力学を持ち出さなくても可能な場合もある．しかし盗聴者イヴが物理的に許されるあらゆる手段をテクノロジーとして持っていると仮定するならば，古典的信号は見られているなら全部見られていると仮定しなければならない．

ここに複製禁止定理の定量化版が登場する．この定理によりイヴが強引に鍵情報を引き出そうとしたときアリスとボブの鍵の間にエラーを発生させてしまう．アリスとボブがそのエラー量を測ることは，工夫を要するが，可能である．エラー量から漏洩情報量の上限を求めることができ，それを元に誤り訂正符号(古典的)と秘匿性増強によりイヴの知り得ない秘密鍵を共有することができる．そのあとは実際のメッセージを鍵でランドマイズして送れば，メッセージ本体の漏洩はゼロとなる．

量子暗号の目的は仮想盗聴者であるイヴがどんなことをしてもアリスとボブの安全な通信を保証することにある．そこで上記漏洩情報量の上限の見積もり方がヘタで真の最大値より大きな上限値を出してしまうと，本当は安全な装置でも「不合格」とはねてしまうことになる．このことは「安全性見積もりの理論の進展」の重要性を示しており，後でまた触れる．

エンタングルメントとパラレル処理

問題のサイズがn倍になると解くのに要する演算ステップ数がnに関し指数関数的に増えてしまう問題の代表は素因数分解である．現在主流の公開鍵暗号は素因数分解がそのような問題であることに安全性の根拠をおいている．量子干渉を上手く使うためには，計算問題を何らかの周期性を持つ問題に転化しておくことが有用である．たとえば素因数分解は次のように周期性に関係した問題に転化できる．巨大な整数の素因数分解を目的としているが，説明のため小さい数$N = 15$を素因数分解したい

としよう．ここで乱数を振って m（たとえば $m = 2$ としてみる）のベキの数列 1, 2, 4, 8, 16, 32, … を作り，N で割り算した剰りを求めると，新たに 1, 2, 4, 8, 1, 2, … ができる．この数列は 4 つごとに同じ値をとる周期数列であり，その周期 $r(= 4)$ を使って $m^{(r/2)} \pm 1$ を作ってみると 3 と 5 が得られ，手品のように 15 の約数が求まっている．

上記は $N = 15$ だから問題ないが，N が何百桁くらいもの大きな数になると，途端に r を求める計算が実行不可能となる．しかし周期を求める問題は，波が周期の整数倍で重なるとき強め合うことを利用してパラレル処理をうまく使うことができる．このようにして素因数分解を行うのがショアのアルゴリズムである．

パラレル処理の最も簡単な例として**図 -1** にヤングの 2 重スリット実験の概念図を示す．入射光の強度を非常に弱めたとき，1 つ 1 つの光子は「スリット A を通って地点 P に行く場合の波」と「スリット B を通って地点 P に行く場合の波」の両方をあらゆる地点 P について計算し，両波の重ね合わせの絶対値の二乗を出現確率として適当な地点に出現する．つまり光子は 2 つの可能な場合をパラレル処理し，その結果生ずる確率で行動している．このようなヤングの干渉実験の粒子版は光子だけでなく，電子，中性子，原子，分子でも実際に観測されている．

2 重スリットを n 重スリットにしても同じことである．すなわち最終状態に至る可能な道筋がいくつもあれば，1 つの粒子はそのどれをも仮想的に試行し，複数の波の重ね合わせの絶対値の二乗を出現確率として適当な地点に出現する．干渉計を適切に設計することにより，たとえば上記の数列の発生をパラレルに行うことができるようになる．

しかしこれは時間的に膨大なステップ数が必要だったのを，干渉計のスリットの数に置き換えたにすぎない．解きたい問題の複雑さが n 倍になったとき，準備すべき干渉計の複雑さも n 倍にしなければならないなら，現代のコンピュータで「集積度あるいは CPU 速度を n 倍にしなさい」というのと事情は変わらない．これがもし $\log(n)$ の程度の複雑さでいいと言うなら，質的にまったく異なったコンピューティングの手法を提供したことになる．量子力学を使うと，この $\log(n)$ は次のようにして可能となる．**図 -2（a）**は 32 重スリット干渉計である．1 つの粒子は 32 通りの違ったルートを試行する．一方，**図 -2（b）**は 5 つの 2 重スリット干渉計である．5 つの粒子がそれぞれ 2 通りの違ったルートを試行するが，その組合せは $2^5 = 32$ 通りある．したがって (b) は「5 つの粒子全体として可能な場合が 32 通りあり，それをパラレル試行」している．2 重スリット系を 5 つでなく n 個とすれば，準備の努力は n 倍にして可能な場合は 2^n 倍にすることができる．基本的にはこの原理により素因数分解をはじめとするいくつかの重要な問題が，装置の空間的複雑さも時間的ステップ数も指数的増大以下に抑えて解くことができるようになる．これが量子コンピューティングである．

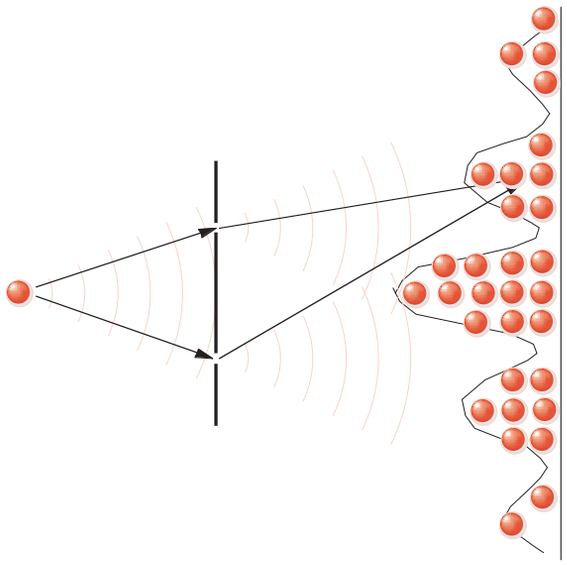

図 -1　ヤングの 2 重スリット実験：最も簡単な量子パラレル処理

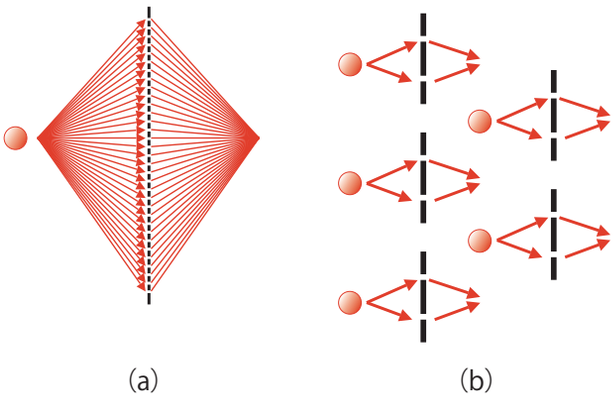

図 -2　エンタングルメントによる系の簡単化．$2^5 = 32$ により (a) の 32 個のスリット系と (b) の 5 つの 2 重スリット系は同等．ただし (a) の重ね合わせ状態は (b) ではエンタングルメントとなる．数が多い場合たとえば (a) で 2^{300} 状態の重ね合わせは不可能だが，(b) ではたった 300 個の量子ビットで済む．

このような離ればなれの複数の系全体を 1 つの系としたとき，その系の可能な状態の重ね合わせは量子力学では「エンタングルメント」と呼ぶ．これは古典物理あるいは日常生活の常識的推論の結果を覆すような現象（ベル不等式の破れ）を引き起こす．この「エンタングルメント」は量子情報処理実現のリソースとして本質的役割を果たす．

エンタングルメントの純化

前章で見たようにエンタングルメントは量子コンピューティングの最中に現れる重要な概念であるが，量子テレポーテーションでは始めから必要なもので，送信者と受信者の間に配っておく必要がある．量子暗号の中にもアリスとボブの間でエンタングルメントを配っておくもの（E91，E92 など）はその必要がないものより優れた量子暗号であるが，アリスとボブがエンタングルメントを必要としない量子暗号においても，盗聴者イヴがエンタングルメントを使うかもしれず，その安全性証明において欠かせない．要するに量子情報処理においてエンタングルメントは本質的概念である．

エンタングルメントは光では制御性良く発生することが容易である．振動数 ω，波数 k の光子 1 つをある非線形光学結晶に入れると，$\omega = \omega_s + \omega_i, k = k_s + k_i$ を満たす振動数と波数を持つ光子 s と i に分かれる「パラメトリック下方変換」という現象を用いる．これは飛んでいる石（光子）が何らかの撹乱（非線形光学）によって 2 つに割れたとき，エネルギーと運動量を保存する速さと方向に分かれることに相当する．

このようにしてアリスとボブに「エンタングルした 2 つの光子を 1 つずつ配布する」ことが可能であるが，現実に光ファイバーや空間ビームでこれを行うと，ファイバーや大気の屈折率の時間的ゆらぎによりエンタングルメントが破壊される．もしそれを回復する手段がないとすれば，エンタングルメント配布は非現実的となり，量子情報処理の多くは絵に描いた餅に終わる．

このようなエンタングルメント消失回復の手段はいくつか考えられる．1 つは，ある光子が受けるファイバーや大気のゆらぎをリアルタイムで別の方法で測定し，逆変調をかけて戻す「アクティヴ補正」である．これはテクノロジー的に困難である．2 つ目はこのようなゆらぎに敏感でない変数にエンタングルメントを載せる．たとえば光子の有無だけを使うもので，研究途上である．3 つ目は量子誤り訂正を使うもので，これも研究途上である．4 つ目は「エンタングルメントの純化」を用いるもので，これは概念的にも実用上も重要なものである．

4 つ目の「エンタングルメントの純化」の概念を簡単に説明する．**図 -3** のようにアリスとボブは弱くエンタングルしたペアを多くシェアしているとする．アリスとボブは以下に述べるような LOCC (Local Operation and Classical Communication) と呼ばれる操作が許されている．すなわちアリスは自分の持つ光子群だけに物理操作ができ，ボブもそうである．アリスとボブは古典通信手段を

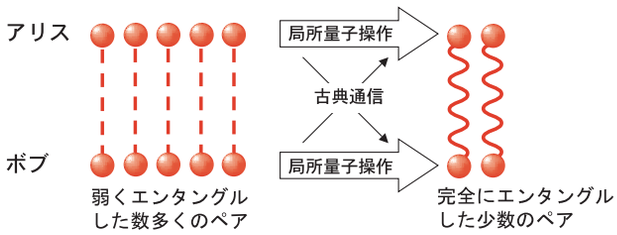

図 -3　エンタングルメントの純化の概念．アリスとボブは弱くエンタングルした数多くのペアから完全にエンタングルした少数のペアを抽出する．ただし LOCC（本文参照）の制限のもとに行う．

持ち，自分がどんな操作をしたかや，量子測定をしたならばその結果を伝え合うことはできる．LOCC でできないのはアリスが持つ光子とボブが持つ光子を直接反応させるような操作である．

LOCC の範囲でアリスとボブがシェアしているいくつかのペアのエンタングルメントを完全（純粋）なものにする手段があるとすれば，それを「エンタングルメントの純化」という．純化の代わりに蒸留とか濃縮とか抽出と呼ばれることもある．このようなことができれば，光ファイバーや大気に多少のゆらぎがあってもアリスとボブは完全なエンタングルメントを共有することができるので，実用的に重要であることは論を待たないが，理論上の重要性もある．これらについては後で触れる．

量子暗号の安全性研究の進展

量子暗号はさまざまな方式で実験が行われており，簡単な製品まで欧米のベンチャー企業から出されている．実験研究の重要性は分かりやすいが，一方理論の進展も著しく，こちらは何がどう重要なのか解説する必要があると思われるので，この章では以下それを解説する．

1984 年の BB84 から B92，E91 その他筆者の研究室を含めたいろいろな研究グループから量子暗号のさまざまなアイディアが提案されてきたが，実はそれらの方式が本当に安全であることの理論的証明は後になってなされるようになってきた．たとえば BB84 の安全性証明は 1997 年に初めてなされたが，それは理想的単一光子発生器を仮定するなど，前提条件にまだ非現実性があった．この非現実性を 1 つずつ取り払うことや，BB84 以外のさまざまな量子暗号を対象としていくことで，「量子暗号の安全性証明」という理論分野は持続的に発展している．

同じ方式の同じ現実的条件であっても，前述の「漏洩情報量の上限の見積もり」の巧拙により，安全な鍵の単位時間当たりの生成率（鍵生成レート）にケタが違うほど

の大きな差ができる．こうなると，より真の最大値に近い上限の見積もりを与えることが，同じ量子暗号の実験装置の性能を大きく進歩させることになる．すでに存在している装置の性能が理論の進展により上がるという現象が起こるのは，盗聴者によるあらゆる攻撃を実験してみることができない以上理論で見積もるしかない，というセキュリティ証明理論の特徴である．

1998 年から最近まで主流であった量子暗号の安全性証明理論の手法は，エンタングルメント純化の理論を使うものであった．これはまず，検討の対象となっている量子暗号方式をその中に包含するようなエンタングルメント純化プロトコルを見いだすことに始まる．そのようなプロトコルが見つかったならば，その純化プロトコルの成立条件を求めてやればよいのである．なぜならば，ひとたびエンタングルメント純化ができてしまえば，アリスとボブが手にした 1 つずつの粒子が他のどんな系ともエンタングルメントはおろか古典相関もないという定理(エンタングルメントの一夫一婦制と呼ばれる)があるからである．かくして，仮想したエンタングルメント純化プロトコルの成立条件は，元の量子暗号成立の十分条件となる [5]．

最近，エンタングルメント純化を用いる上記の方法とは別に，不確定性原理を直接用いる安全性証明の手法も開発され，これにより量子暗号の安全性の理論の適用範囲が拡大した．この辺の事情については文献 5）を参照されたい．基本的に単一光子発生器を必要とする BB84 以外に通常のレーザー光を用いる方法が数多く発案されてきたが，それらの安全性が従来考えられてきたよりずっと良く，単一光子を必要とする量子暗号に肉薄することも分かってきた [5]．しかしまだ未解決の課題も多いので，量子暗号の安全性証明の理論研究はまだしばらく続く研究分野である．

量子計算ハード研究の進展

量子暗号に比べると量子コンピューティングの研究は実用までにより時間がかかりそうである．現在 8 ビットの計算のデモンストレーションまできているが，これから現存のコンピュータと競争して勝つためには非常に多くの課題を克服しなければならない．その筆頭はデコヒーレンスである．極短時間あるいは極短距離でデコヒーレンスが起きないようなハードウェアを探すことがまず必須である．それを次の 5 つの条件の下で探さなければならない．

(1)素子として接続していけること (scalability)
(2)基準状態へのリセットが物理的に容易なこと
(3)デコヒーレンス時間の長いこと
(4)汎用ゲートが構成できること
(5)量子状態の読み出しが効率よくできること

そのため現在種々のハードウェアが提案されている．以下に進歩の大きい順に紹介するが，必ずしも将来有望な順序とは関係ない．まず演算にあずかる量子ビットの数が 8 個と一番大きいことからイオントラップを挙げる．これは電荷を持ったイオンが整列しやすいことと，それらを伝わる音波で情報の読み書きができる特徴を利用している．これも 100 ビットを超えることはきわめて困難と目されるが，それまでの知見の蓄積には適したハードウェアと考えられる．

有機溶媒分子 1 つを量子コンピュータとし NMR（核磁気共鳴)で量子情報の入出力を行う方法が進んでいる．量子ビットの数はイオントラップの方が多いが，こちらは 15 ＝ 3 × 5 の素因数分解に成功している．分子の中にある炭素原子が配位の違いから区別できる量子素子として使えることを利用している．しかしこの方法は膨大な数（アヴォガドロ数）の分子のうちリセットされたと見なせる（絶対零度に近い）分子のみを使うという方法をとっているため，真のリソース節約を達成するにはブレイクスルーが必要である．最も進んだ方法ではあるが，10 ビットを超えることは困難と予想されている．一方 NMR 量子コンピューティングは固体の方向にも新たな展開を見せている．

光子を用いた演算は現在のところ 5 ビットであるが，それは本質的限界でなく現在の技術的問題であること，デコヒーレンスが本質的に小さいこと，制御性が良いこと，線形素子を用いた確率的演算が可能なことから，将来有望と筆者は考え，研究を進めている．光ファイバー通信との相性も良い．問題は光子はメモリには適さないことであり，このため，物質系量子メモリとの間で量子情報をやりとりする研究も必須と考えられる．超伝導を用いた量子演算素子は現在 2 ビットが実現され，固体素子ゆえの集積化や scalability の期待がある．一方これはビット数を増やしたときの任意ゲートの構成に課題が出てくるであろう．半導体は量子ドットを用いるが，現在のところ 2 ビットに手を伸ばそうというところの 1 ビットである．しかし電子スピンと核スピンの間の情報のやりとりという新しい現象が報告され，今後の進展が大変興味深い．問題はデコヒーレンスが大きい（デコヒーレンス時間が短い）ことと，前述の現象もまだ統計力学的なもので 1 つ 1 つのスピン間の制御・観測までは行っていない点である．

比較的ダークホース的なのが原子である．これは数年前および昨年ノーベル賞がもたらされた「原子のレーザ

ー捕獲および冷却」の研究に端を発しているが，最近「光で作った光波長程度の周期的電磁場に原子を捕獲する」技術が発達している．このような系は物質的には密度が低いので，あたかも2つのレーザービームをぶつけても反発することなく通り抜けるように自在に接近させたり制御したりできる．まだ2ビットまで行かないが，今後面白い展開になる可能性がある．ほかにも分子や固体の光物性を利用するものなど種々の提案があり，今後しばらく百花繚乱の様相は続くと思われる．現在まだ本命を決める段階にはない．

多者間量子コンピューティングへ

量子暗号と素因数分解以外へのより汎用的応用の必要性があるが，多者間コンピューティングはその1つの有望なものと筆者は考えている．たとえば選挙や入札は基本的に「各人のデータを開示せず最大値やマジョリティは何かを計算すること」である．このような多者間で行う秘匿コンピューティングは種々の応用がある．「量子」の付かない情報理論にも「秘密分散」や「ゼロ知識証明」などの概念があるが，これを量子力学を使って，なるべく「信頼できる第三者」の役割を減らし，物理的に行う方向を考えることは意義があり，かつ近未来の量子暗号と遠未来の量子コンピューティングの間を埋めるマイルストーンになると考えられる．

多者間にしても二者間にしてもデコヒーレンスによる誤りをなくすことが重要であるが，前述のエンタングルメントの純化は重要である．いったんピュアなエンタングルペアを配布しておけば，あとは量子テレポーテーションが使えるので，これはきわめて有用な方法である．比較的簡単な光回路でそれが実現できることを筆者の研究室でも実証実験を行った[6]．

おわりに

量子情報処理研究への出資は現在きわめて活発で，いわゆるナノやバイオサイエンスにひけをとらない．例を挙げると，EUは5年前後で20億円のプロジェクトを走らせているほか，10年で総額100億円の案も出ている．アメリカはNFSがやはり約5年で40億円，その他国防省，国家安全保障局，標準技術局などが大きなプロジェクトプログラムを持っている．オーストラリアでは数年単位で7億円，シンガポールも3.5億円のプロジェクトがある．中国も最近力を入れている．

日本は科学技術振興機構がERATO，CREST，PRESTOなどのプロジェクトを持っている．総務省もプロジェクトを走らせているほか，経産省も検討を進めているようである．出資というのとは違うが，この分野は母体となる学会がない，言い換えるとさまざまな学会の人が研究している．筆者もかかわっている量子情報研究会は一応電子情報通信学会の第二種研究会の形をとっているが，実質的には来る者は拒まず，去る者は追わずという様で，政治色の薄い実質的討議のできる場を提供している．資金ではなく，これはいわば「場」の出資である．

従来は物性物理屋はモノのことだけ，デバイス屋はデバイスだけ考え，情報処理屋がどう使うかまで考える必要はなかった．いわゆる分業が成り立っていた．しかし量子情報処理はそれでは済まない．最終段階には必ず方式屋がシステム的発想で全体設計する必要があるが，現在は物性物理からの貢献も多大なフェーズにある．従来は物性物理の研究者や学生はシステム的発想がないと思われていたかもしれないが，今後はそうではないであろう．むしろ基礎がしっかりしているだけに，量子情報を修めた学生は非常に適応力があるように見える．私も30年前は物性物理の学生であったが，大学で物性物理分野の教育研究に携わるようになって，その辺が昔と大きく違う点であると感ずる．

最後に，筆者の研究室の同僚・スタッフ・学生ならびに研究室の研究を支えてくださる科学技術振興機構，大阪大学21世紀COEプロジェクト，日本学術振興会に感謝の念を表したい．

参考文献

1) 別冊・数理科学 2006年4月号「量子の新世紀」，pp.46-55 (2006).
2) A．エカート，井元信之訳：パリティ，Vol.7, No.2, p.26 (1992).
3) 井元信之：量子暗号の原理と課題，電子情報通信学会情報セキュリティ研究会 (1992年7月13日)，ISEC92-5.
4)「量子情報処理」，集英社「imidas 2007」pp.787-791.
5) 小芦雅斗：数理科学，Vol.42, No.10, pp.50-55 (2004).
Koashi, M. : Phys. Rev. Lett. 93, 120501 (Sep. 15 2004).
Koashi, M. : e-print quant-ph/0609180 (2006).
6) Yamamoto, T. et al. : Nature, 421 (2003), 343.
山本　俊他：応用物理，Vol.75, No.11, pp.1359-1363 (2006).

（平成18年11月6日受付）

井元　信之
imoto@mp.es.osaka-u.ac.jp
1977年日本電信電話公社入社，広帯域光ファイバー通信研究に従事．1985年光の量子非破壊測定系提案．1992年より量子情報処理研究を拡大．1999年より総合研究大学院大学教授，2004年より現職．
http://www.qi.mp.es.osaka-u.ac.jp/index-j.html