非局所相関と量子情報

小　芦　雅　斗

Nonlocal Correlations and Quantum Information

Masato KOASHI

Seventy years ago, Einstein, with Podolsky and Rosen, pointed out that the quantum theory predicts abnormally strong correlations between the measurement outcomes of two distant observers. Later it was confirmed by Bell that these correlations violate so-called Bell's inequalities for the local hidden-variable theories, and hence they cannot be explained by any theory assuming the local realism. Now these nonlocal correlations, which are easily produced in the experiments, are being considered to be a useful resource in the communication problems. One of such applications is quantum cryptography, where the quantum mechanics guarantees that communication using quantum states cannot be monitored by any eavesdropping strategies.

Key words: nonlocality, Bell's inequality, quantum cryptography, quantum key distribution

1935年，アインシュタイン（Einstein）は，ポドルスキー（Podolsky）およびローゼン（Rosen）とともに，量子力学のもつ特異な性質を指摘する重要な論文を発表した[1]．その性質とは，ある量子力学的に許された状態に準備された2つの量子系を遠く離れた場所に引き離し，おのおのの場所で測定を行うと，その測定値が異常に強い相関を示すというものである．著者3人の名前から，今日でもこのような状態や相関をEPR状態，EPR相関などとよぶことがある．この特異な性質は，長いこと単なる学術的な興味にとどまっていたが，EPR論文から半世紀あまりを経て，この性質を通信の問題に応用できる可能性が浮上してきた．本稿では，まず，この量子相関が，いったいどのような意味で特異なのかを，光子対の偏光測定を例にとりながら，EPRの指摘とその後のベル（Bell）による発見という流れに沿って解説する．続いて，最近になって発達してきた量子情報科学という分野の中で，この性質を暗号通信などに利用する可能性が開けてきていることを紹介する．

1.　非局所的な相関

1.1　EPR光子対

EPRの論文では，仮想的な2粒子の位置と運動量の測定を例として取り上げているが，ここでは光子対の偏光を測定する実験に基づいて解説を試みたい．二次の光非線形性をもつ結晶に，波長λのパルスレーザー光を励起光として照射すると，光パラメトリック過程とよばれる相互作用によって，波長2λをもつ光が発生する．ここで，波長λの光子は波長2λの光子の2倍のエネルギーをもつことを考慮すると，励起光子が1個変換されるたびに波長2λの光子は2個生成されるはずである．つまり，波長2λの光子は常に2個が対となって放出される．ここで，励起光の入射方向に対して結晶軸の方向をうまく選ぶと，例えば，H偏光（直線偏光で偏光方向が地面に平行）の光子がある方向に放出され，それと対をなす光子はやはりH偏光をもって別の方向に放出されるようになる．この光子対を方向で選別し，前者の光子は観測者Aliceのもとへ，後者は観測者Bobのもとへ届けることにしよう．このときの2光子の量子状態を$|H\rangle_A|H\rangle_B$と書く．

大阪大学基礎工学研究科（〒560-8531 豊中市待兼山町1-3）　E-mail: koashi@mp.es.osaka-u.ac.jp

さて，EPR の議論にのせるためにはもう一捻りが必要である．結晶軸の向きや励起光の偏光を調整すれば，Alice と Bob に届く光子の偏光がともに V 偏光（直線偏光で偏光方向が地面に垂直）になるようにもできる．ここで，単一の励起レーザーを用いて 2 種類の生成方法を同時に注意深く行い，Alice や Bob に届いた光子がどちらの生成方法で得られた光子なのかが，偏光を見るまでは決してわからないようにできたとしよう．これは，例えば 2 枚の薄い非線形結晶を貼り合わせて使うなどの方法[2] によって可能である．この場合，2 光子の量子状態は 2 つの可能性の重ね合わせ状態 $(|H\rangle_A|H\rangle_B+e^{i\phi}|V\rangle_A|V\rangle_B)/\sqrt{2}$ となる．ここで，重ね合わせの位相 ϕ は複屈折性媒質を用いて調整が可能なので，$\phi=0$ ととることにしよう．このあとわかるように，この状態の 2 光子に対する測定結果は特異な相関を示し，このような光子対は EPR 光子対とよばれることもある．

Alice と Bob のおのおのは，偏光子を用いて届いた光子の偏光方向を測定する．H 偏光の光は透過し，V 偏光の光は 90° 進行方向を曲げる偏光子（偏光ビームスプリッター）の後ろに光子検出器を 2 個置けば，どちらが光子を検出したかによって偏光が H なのか V なのかを識別できる．H 偏光だった場合の測定値を 1，V 偏光だった場合の測定値を -1 とすれば，この測定は演算子 $\hat{Q}(0)\equiv|H\rangle\langle H|-|V\rangle\langle V|$ で表される物理量を測定していると考えてもよい．さらに，この偏光子を含む測定装置は，そっくりそのまま好きな角度 θ 回転できるとしよう．その場合，H 偏光と角度 θ をなす直線偏光の光子が測定値 1 を与え，角度 $\theta+90°$ をなす光子は測定値 -1 を与えることになる．角度 θ の偏光方向をもつ光子の状態を $|\theta\rangle=\cos\theta|H\rangle+\sin\theta|V\rangle$ と書くと，この場合に測定される物理量は $\hat{Q}(\theta)\equiv|\theta\rangle\langle\theta|-|\theta+90°\rangle\langle\theta+90°|$ となる．

さて，Alice と Bob はおのおのの測定装置の角度を θ_A，θ_B に選び，状態

$$|\Phi\rangle\equiv(|H\rangle_A|H\rangle_B+|V\rangle_A|V\rangle_B)/\sqrt{2} \qquad (1)$$

の 2 光子の偏光を測定するとしよう．このとき，測定値の相関，すなわち 2 人の測定値の積の期待値 $E(\theta_A, \theta_B)$ は，簡単な計算から，

$$E(\theta_A, \theta_B)=\langle\Phi|\hat{Q}_A(\theta_A)\hat{Q}_B(\theta_B)|\Phi\rangle=\cos 2(\theta_A-\theta_B) \qquad (2)$$

となる．特に，$\theta_A=\theta_B$ の場合，つまり，2 人が測定装置を同じ角度だけ回した場合には，$E(\theta_A, \theta_B)=1$ となる．すなわち，どんな角度に設定しても，測定結果は完全な相関をもち，Alice の測定結果と Bob の測定結果は一致する．

以上の結果は，EPR の時代には思考実験に対する量子力学の予言という位置づけであったが，今日では多数の実験が行われており，式（2）にかなり近い相関が実際に観測されている．すなわち，この相関は，量子力学の予言であると同時に，量子力学とは無関係に実験的に観測できる相関でもある．

1.2 EPR の議論

EPR の議論は，まず，自然を記述する理論が理想として備えていてほしいある条件を明示することから始まる．そのために，彼らは「物理的実在の要素（elements of physical reality）」とよばれる概念を定義した．これは，測定を行って得られるデータは何を意味するのか，というやや哲学的な疑問と関連している．素朴に考えれば，測定とは対象とする系のもつ定量的な性質（物理量）を知ろうとする行為であり，測定によってある値が得られるということは，測定するしないにかかわらず系はその（物理量がその値をとるという）性質をもって実在していると考えたくなるかもしれない．しかし，測定といってもいろいろな場合があり，例えば測定装置が不完全なために本来の正しい値を返さない場合や，測定装置が系に影響を与えてしまう場合などを考えると，上記の考えをすべての測定の場合に当てはめてしまうのは素朴すぎるであろう．そこで，そういった怪しい場合を排除して，誰もが同意できる範囲に絞ったのが次の定義である： もし，ある系にまったく影響を与えることなしに，その系のもつある物理量（すなわちある測定を行ったときの測定値）を 100% 予言できるとき，この物理量に対応する物理的実在の要素が存在する．このようにして，少なくとも実在していると考えられる一連の要素が定義される．すると，当然ながら，系の状態を完全に記述できたと胸を張っていえるには，少なくともこの一連の実在の要素に対応する物理量の値がその記述からすべて決定できるということが必要だろう．もし，ある理論における系の状態の記述から，実在の要素に対応している物理量の値をどうしても決められないならば，その記述は不完全であるといわねばならない．

ここで，前節の EPR 光子対に関する量子力学の予言について考える．Alice と Bob が遠く離れていて，光が Alice の場所から Bob の場所まで到達するのにかかる時間よりも短い時間の間に両者はそれぞれ $\hat{Q}_A(\theta)$ と $\hat{Q}_B(\theta)$ の測定を行ったとしよう．アインシュタインの相対性理論によれば，Alice の測定の影響が Bob のもとにある光子に及ぶことはありえない．この性質は局所性（locality）とよばれる．一方，Alice の $\hat{Q}_A(\theta)$ の測定結果と，Bob が $\hat{Q}_B(\theta)$ を

測定した結果は式（2）のように必ず一致するのであるから，Alice は $\hat{Q}_B(\theta)$ の測定結果を 100% 予言できることになる．すなわち，Bob の偏光測定によって測定される物理量 $\hat{Q}_B(\theta)$ は，対応する物理的実在の要素をもつことになる．

それでは，量子力学における状態の記述から，すべての実在の要素 $\hat{Q}_B(\theta)$ を決定できるだろうか．これは，量子力学の基本的な定理である不確定性関係によってあっさりと否定されてしまう．例えば，$\theta=0$ と $\theta=45^\circ$ の 2 つの演算子は可換ではなく，両方の演算子の同時固有状態は存在しない．$\hat{Q}_B(0)$ の値が確実に 1 となる状態は $|H\rangle_B$ のみであり，この状態に対する $\theta=45^\circ$ の測定結果はまったくランダムになる．このように，量子力学における状態の記述では，すべての実在の要素を把握しきれていないため，この記述は不完全といわねばならない．これが EPR の議論の結論である．この結論が気に入らないとしたら，議論の途中で当然のように導入した仮定である局所性を疑ってかかるしかない．

1.3　ベルの不等式の破れ

EPR の議論は，局所性を捨てない限り，量子力学の記述は実在の記述としては不完全なものであるということであった．当然ながら，この不満足な結果は単に量子力学の欠陥，力不足であって，自然そのものはまともなはずだと期待したくなるのが人情であろう．つまり，量子力学を超えた未知の理論があって，その理論においては実在の要素の完全な記述が与えられるはずだ，という期待である．そのような理論では，実在の要素に対応する物理量をすべて決定するのに十分なパラメーター，変数によって状態が指定される．もちろん，われわれが測定によってその変数を完全に決定できるかどうかは別問題であって，原理的にそんなことは不可能だということであっても一向に差し支えない．その意味で，この変数は隠れた変数（hidden variable）とよばれる．この考え方と局所性を同時に満たすような理論を，局所隠れた変数理論（local hidden-variable theory）とよぶ．すなわち，この種の理論においては，ある場所における測定結果は，測定方法と隠れた変数によって決定され，遠く離れた場所で何が起こっても測定結果には影響しない．

局所隠れた変数理論に属する未知の理論が将来発見されて，量子力学はその地位を譲り，八方まるく収まるという淡い期待は，1964 年，ベルによって脆くも否定されてしまう．彼は，局所隠れた変数理論の詳細とは関係なく，局所性と実在性の要請だけから，あらゆる局所隠れた変数理論の予言が満たさなければならない不等式を導いた[3]（この不等式や，その後導かれた同様の不等式をまとめてベルの不等式とよぶ）．しかも，量子力学の予言は，その不等式を満たさないのである．その後の実験は，確かに量子力学の予言を支持し，ベルの不等式が確かに破れていることが確認された．すなわち，EPR が指摘したように，単に暫定的な一理論である量子力学が不完全だということではなくて，そもそも自然を局所隠れた変数理論で記述することが不可能であるという不思議な事実が浮かび上がったのである．

ここでは，ベル自身が導いた不等式のかわりに，直感的にわかりやすい例を 1 つと，現在最もよく使われている不等式を紹介する．最初の例では，遠く離れた Alice と Bob は，3 種類の測定方法 a，b，c の中から，それぞれ 1 つを無作為に選んで自分の粒子に対して測定を行い，測定値 1 または -1 を得るものとする．前提条件として，両者が同じ測定法を選択した場合，測定結果は常に一致するとしよう．つまり，隠れた変数の値が何であったとしても，Alice の測定 a の結果 μ_a と Bob の測定 a の結果 ν_a は等しく，同様に $\mu_b=\nu_b$，$\mu_c=\nu_c$ が成り立つ．さて，両者が異なる測定方法を選択した場合，両者の結果が異なる確率はどのくらい大きくできるだろうか．$(\mu_a, \mu_b, \mu_c)=(\nu_a, \nu_b, \nu_c)=(1, -1, 1)$ の場合，Alice と Bob の測定の組み合わせが a と b，あるいは b と c なら測定結果が異なるが，a と c なら測定結果は同じになってしまうので，測定結果が異なる確率は 2/3 となる．$(\mu_a, \mu_b, \mu_c)=(\nu_a, \nu_b, \nu_c)$ のパターンは 8 種類あるが，どれについてもこの確率は 2/3 または 0 となることが容易にわかる．したがって，隠れた変数の確率分布をどう工夫しようが，測定結果が異なる確率を 2/3 より大きくすることはできない．

ここで，EPR 光子対の例に戻ろう．上の議論における測定 a，b，c が，それぞれ角度 $\theta_a=0$，$\theta_b=60^\circ$，$\theta_c=120^\circ$ の偏光測定であるケースを考える．式（2）の相関 $E(\theta_A, \theta_B)$ は，定義から，測定結果が同じ確率と異なる確率の差に等しいことに注意しよう．$E(\theta, \theta)=1$ であるから，両者が同じ測定を選べば測定結果は常に一致し，上記の前提条件は満たされている．ところが，$E(\theta, \theta\pm60^\circ)=E(\theta, \theta\pm120^\circ)=-1/2$ であるから，両者が異なる測定を選んだときに結果が食い違う確率は 3/4 であり，これは局所隠れた変数理論で導ける限界の 2/3 よりも大きい．つまり，この量子力学の予言を局所隠れた変数理論によって説明することは不可能なのである．

上の例では，同じ測定をしたときの結果が 100% 一致するという前提条件を置いたが，エラーを完全には排除できない実際の実験でこの条件を満足させることはできない．

そこで，実験では，ベル不等式の中でも検証がより容易なCHSH不等式[4]が用いられることが多い．この場合，Aliceは2種類の測定から選択する．その選択を$\alpha=0, 1$で表そう．Bobは別の2種類の測定$\beta=0, 1$のいずれかを選択する．Aliceの測定値$\mu=1, -1$はAliceの測定方法αと隠れた変数λだけで決まり，Bobの測定方法にはよらない．Bobの測定値$\nu=1, -1$も同様である．したがって，測定法α，βが選択されたときの両者の測定値の相関$E_{\alpha,\beta}$は，隠れた変数の確率分布を$P(\lambda)$として，

$$E_{\alpha,\beta}=\int \mathrm{d}\lambda P(\lambda)\mu(\alpha,\lambda)\nu(\beta,\lambda)$$

と書ける．ここで，±1の値しかとらない2変数の和と差は，和がゼロなら差が±2になり，和が±2なら差がゼロとなるので，

$$[\mu(0,\lambda)+\mu(1,\lambda)]\nu(0,\lambda)+[\mu(0,\lambda)-\mu(1,\lambda)]\nu(1,\lambda)=\pm2$$

が成り立つ．したがって，$P(\lambda)$で平均をとれば，

$$S\equiv E_{0,0}+E_{1,0}+E_{0,1}-E_{1,1}$$

として

$$|S|\leq 2 \qquad (3)$$

が常に成立することがわかる．局所隠れた変数理論が必ず満足するこの不等式を，CHSH不等式とよぶ．

EPR光子対を用いてこの不等式を検証する場合，Aliceの測定角を$\theta_{A\alpha}$，Bobの測定角を$\theta_{B\beta}$に選ぶ．ただし，$\theta_{A0}=0$，$\theta_{A1}=45^\circ$，$\theta_{B0}=22.5^\circ$，$\theta_{B1}=-22.5^\circ$である．すると，式(2)より，$E_{0,0}=E_{1,0}=E_{0,1}=\cos(\pm45^\circ)=1/\sqrt{2}$，$E_{1,1}=\cos 135^\circ=-1/\sqrt{2}$となるので，$S=2\sqrt{2}$となり，量子力学の予言はCHSH不等式を破ることがわかる．この場合では，実験にいろいろな不完全性があってSの値がちょうど$2\sqrt{2}$にならないとしても，実験誤差に比べて大きく2を超えてさえいれば，CHSH不等式は満たされないと結論づけられる．実際，現在までには数多くの実験で破れが確認されており，自然が局所隠れた変数理論では記述できない現象を示すことはほとんど疑いがない*1．この事実は，きわめて常識的な概念である局所性と実在性のどちらかを捨て去らない限り，われわれの住む世界を説明することは不可能であることを意味している．

2. 情報理論とのかかわり

2.1 量子暗号

これまでみてきたように，EPR光子対のような状態を作って各光子を測定すると，常識とは相容れないような強い相関が観測される．最近では，このような相関をはじめとする量子力学の特異な性質を積極的に利用して，通信などの情報科学の問題に役立てようという試みが盛んになってきている．そのひとつが量子暗号である．量子暗号の目的は，離れた場所にいるAliceとBobが量子状態を用いた通信を行うことで，秘密鍵とよばれるランダムなビット列を盗聴者（Eveとよぶことが多い）に知られないように共有することであり，量子鍵配送ともよばれる．秘密鍵がいったん確保されれば，同じ長さのメッセージとビットごとに排他的論理和（2を法とする足し算）をとったものを公開すれば，同じ秘密鍵をもつBobはもとのメッセージを復元できて，一方Eveにとってはまったくランダムなビット列にしかみえないため，確実に安全な通信が保証される．

それでは，量子状態を用いて秘密鍵を作ると，いったいどのようなからくりでEveへ情報が漏洩していないことが保証されるのだろうか．このからくりについては，いろいろな角度からみた説明が可能である．最もポピュラーな説明は，AliceがBobに送る量子状態に対してEveが測定を行って情報を取り出そうとすると，測定の反作用によって状態が変化し，AliceとBobはその変化を追跡することで盗聴行為の程度を確認できるというものである．ここでは，前節までにみてきた非局所的な相関に深くかかわった説明をいくつか紹介しよう．

一つ目は，ベルの不等式の破れの議論をほぼそのまま用いる定性的な説明である[5]．Aliceが自分でEPR光子対を作り，その1光子をBobに送信するとしよう．Eveはその送信された光子に対して途中でいろいろと細工することが可能である．Bobが光子を受け取ったあとで，AliceとBobは，適当に角度を切り替えて測定を行う．この測定は，先ほどのCHSH不等式の破れの検証に使った2種類の角度に加えて，Aliceは$\theta_{A2}=22.5^\circ$，Bobは$\theta_{B2}=0^\circ$も測定の候補に入れるとしよう．そうすると，AliceとBobが同じ角度で測定する場合があり，その場合の測定結果は一致するので，それを秘密鍵とする（測定値1をビット値0に，-1を1に読み替える）．異なる角度で測定したデータは，2人とも公開してしまい，Sの値を計算する．$|S|$が

*1「ほとんど」というのは，実験の解釈にあたっていくつかの自明と思われる仮定を置いているためである．例えば，検出器の効率が低い場合，実際に得られるデータは一部の光子からのものになるが，それはすべての光子からのデータから偏りなく抽出されたものだという仮定を置く．

確かに $2\sqrt{2}$ になっていたら，作った秘密鍵を採用し，そうでなければ捨てる．さて，Eve が途中の光子に細工して，秘密鍵すなわち Alice と Bob の測定結果があらかじめ予想できるようにしたと仮定しよう．これは，ちょうど前節の議論において隠れた変数を導入し，しかもその隠れた変数の値を Eve が知っているという状況にほかならない．しかし，不等式の破れはまさにそのような隠れた変数の存在を否定しており，したがって Eve は秘密鍵がわかるような細工をする余地はないことになる．この議論は，自然を記述する理論はどんな形をしているか，という問題と，暗号通信の問題が深くかかわっていることを示すもので，非常に興味深いといえる．また，量子力学の正しさを仮定しなくても，局所性だけから安全性の証明ができるという可能性も示唆している．一方，$|S|$ が $2\sqrt{2}$ より小さかったらどうなるかといった定量的な議論は困難であり，実際の量子暗号の安全性の評価に使うことは難しい．

量子暗号の安全性は，その名前が示す通り，量子力学の正しさに基づいて証明がなされている．最もよく使われる証明法は，次のような議論である[6]．前と同じように光子対を分配したうえで，Alice と Bob はそれぞれ $\theta=0^\circ$ と $\theta=45^\circ$ で測定を行う．ここで，ランダムに光子対を選んでその測定結果をテストのために公開する．もし両者が同じ角度で測定した結果がすべて一致しているようならば，残りの光子対の測定結果から作った秘密鍵は以下の理由で安全となる．実は，$\hat{Q}_A(0)\hat{Q}_B(0)$ と $\hat{Q}_A(45^\circ)\hat{Q}_B(45^\circ)$ の期待値がともに 1 となる状態は，式（1）の状態のみであることが示せる．この状態は純粋状態であるから，それに対して測定を行って作った秘密鍵の値を Eve が知る方法はないのである．この議論はさらに拡張[7]できて，テストの結果が一致しない値を含む場合でも，秘密鍵の長さを短くすれば安全になることが示せるので，現実的な状況での量子暗号の安全性の証明として広く使われている．また，Alice がわざわざ光子対を作らずに，単純に 1 光子の偏光を何種類か選んで送るような手法の安全性証明も，この議論に帰着することができる[7,8]．

この広く使われている証明法は，一見すると非局所的な相関とはあまり関係がないようにみえるが，実は，EPR の議論で指摘された量子力学の奇妙な性質を使っても，ほぼ同じ安全性の証明を与えることが可能である*2．EPR の議論をもう一度復習すると，Alice は $\hat{Q}_A(0)$ を測定することで $\hat{Q}_B(0)$ の値を知ることができるし，$\hat{Q}_A(45^\circ)$ を測定することで $\hat{Q}_B(45^\circ)$ の値を知ることもできる．にもかかわらず，量子力学は $\hat{Q}_B(0)$ と $\hat{Q}_B(45^\circ)$ の両方の値が指定された状態は作れない．この時点で，EPR は量子力学の完全性を疑うことになるわけであるが，いまわれわれは量子力学が正しいという立場で量子暗号の安全性を示したいわけである．つまり，$\hat{Q}_B(0)$ と $\hat{Q}_B(45^\circ)$ の両方の値が指定された状態は，本当に誰も作れないという立場にたつ．すると，Alice がどちらの値を知るかの選択権をもっていることが重要な意味をもってくる．仮に，Eve が $\hat{Q}_B(0)$ の値を知っているとしよう．すると，Alice が $\hat{Q}_B(45^\circ)$ の値を知ることを選択すれば，2 人合わせて $\hat{Q}_B(0)$ と $\hat{Q}_B(45^\circ)$ 両方の値を指定できることになり，量子力学と矛盾する．すなわち，非可換な 2 つの物理量の値を知る選択権は 1 人にしか与えられず，誰かが選択権をもてばその他の人はどちらの物理量の値も知ることができないのである．

2.2 通信コスト

ベルの不等式を破るような相関が，直接利点となる場面があることも最近指摘されている[9]．Alice と Bob がもつそれぞれのデータ D_A, D_B から決まるあるビット値 $k=f(D_A, D_B)$ を計算したいとき，2 人の間で何ビットの情報をやりとりする必要があるかという問題を考える．関数 f を，D_A のみから計算できるビット値 $a_1, a_2, \cdots$ と，D_B のみから計算できるビット値 $b_1, b_2, \cdots$ を用いて $f=\sum_{j=1}^{n} a_j b_j$（和は排他的論理和）という形に書ければ，明らかに n ビットの通信で f が計算できる．ここで，次のような機械を考える．Alice と Bob のおのおのの場所に機械があって，これらは非局所的な相関をもっている．2 人がビット値 α と β を入力すると，それぞれビット値 μ と ν が機械から出力される．仮想的に，次のルールで出力が決まるとしよう： 入力にかかわらず，μ の値はランダムに決まり，ν の値は，$\alpha\beta=0$ なら $\nu=\mu$，$\alpha\beta=1$ なら $\nu=1-\mu$ となる．つまり，入出力の間には，$\mu+\nu=\alpha\beta$ が常に成立している．Alice は，出力 μ をみても，Bob の入力 β の値についての情報は得られないので，この機械を用いて通信を行うことはできない．ところが，Alice と Bob がこの機械を使って，α_j と β_j から μ_j と ν_j を作れば，$f=\sum_j(\mu_j+\nu_j)=(\sum_j\mu_j)+(\sum_j\nu_j)$ となり，どんな関数 f に対しても，Alice はたったの 1 ビット，$\sum_j\mu_j$ の値を Bob に伝えるだけで，計算ができてしまう．残念ながら，このような都合のいい機械は存在しない．この機械を CHSH 不等式のときの議論に当てはめると，$E_{0,0}=E_{1,0}=E_{0,1}=1$，$E_{1,1}=-1$ となるので，$S=4$ となるが，量子力学が許す S の値は，最大で $2\sqrt{2}$ であることが証明されている[10]ためである．

*2 M. Koashi: quant-ph/0505108.

しかし，それでも非局所的な相関がないときの値 $S=2$ よりは大きいため，EPR 光子対の示すような非局所的な相関を用いると，f の計算にかかるコストを 1 ビットまでとはいわないまでも，節約ができるのである．

70 年前にアインシュタインらによって指摘された，量子系の示す非局所的な相関は，最近になって情報理論とのかかわりの中で新しい局面を迎えている．非局所的相関を実際に応用できるという可能性に加えて，現象の定量的な理解が急速に進んでいることも見逃せない．秘密鍵の生成率や通信コストなど，意味のはっきりした数値を通して非局所的な相関を眺めてみると，新しい謎がいくつも浮かび上がってくる．今回取り上げた例に関連していえば，秘密鍵の最大生成率と非局所相関の大きさとの関係はどうなっているのか，CHSH 不等式の破れは $S=4$ ではなくなぜ $S=2\sqrt{2}$ という中途半端な値までなのか，など，まだよくわからないことも多い．今後，われわれの理解が進み，この不思議な相関が当たり前の相関だと感じられる日が来ることを期待したい．

文　　献

1) A. Einstein, B. Podolsky and N. Rosen: “Can quantum-mechanical description of physical reality be considered complete?” Phys. Rev., **47** (1935) 777–780.
2) P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum and P. H. Eberhard: “Ultrabright source of polarization-entangled photons,” Phys. Rev. A, **60** (1999) R773–R776.
3) J. S. Bell: “On the Einstein Podolsky Rosen paradox,” Physics, **1** (1964) 195–200.
4) J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt: “Proposed experiment to test local hidden-variable theories,” Phys. Rev. Lett., **23** (1969) 880–884.
5) A. K. Ekert: “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett., **67** (1991) 661–663.
6) C. H. Bennett, G. Brassard and N. D. Mermin: “Quantum cryptography without Bell’s theorem,” Phys. Rev. Lett., **68** (1992) 557–559.
7) P. W. Shor and J. Preskill: “Simple proof of security of the BB84 quantum key distribution protocol,” Phys. Rev. Lett., **85** (2000) 441–444.
8) K. Tamaki, M. Koashi and N. Imoto: “Unconditionally secure key distribution based on two nonorthogonal states,” Phys. Rev. Lett., **90** (2003) 167904.
9) H. Buhrman, R. Cleve and W. van Dam: “Quantum entanglement and communication complexity,” SIAM J. Comput., **30** (2001) 1829–1841.
10) B. S. Cirel’son: “Quantum generalizations of Bell’s inequality,” Lett. Math. Phys., **4** (1980) 93–100.

(2005 年 7 月 11 日受理)