量子暗号と光通信

清　水　　薫

急速に展開していくコンピューターネットワーク社会において，電子商取引に関するメッセージなどの盗聴や書き換えを防ぎ情報通信のセキュリティーを保護することは非常に重要な課題となっている．数論を駆使して構築された公開鍵暗号方式などの現代暗号は，まさにこの要請に応えるものとしてすでに広く認知され，現在も活発に研究開発と商用化がすすめられている．

一方で近年，全地球規模でリンクされた多数のコンピューターを総動員した結果これらの現代暗号の鍵が解読されてしまった事例が何件か報告されている．このように現代暗号といえども鍵の安全性は暫定的な確信であるにとどまり，しかも鍵の複雑さと解読に利用できる計算処理能力の増大との間にはいたちごっこの関係が続いている．また大幅に計算時間を短縮できる効率的な解読アルゴリズムが将来発見されないとは限らない．実際に，ショアによる素因数分解量子計算アルゴリズムの発見は（その実現はきわめて困難と予想されているとはいえ）現代暗号の安全性に対して深刻な脅威を与えている．

こうした背景のもとで最近関心を集めているのが量子暗号である[1-6]．量子暗号では秘密通信用の暗号鍵を生成するにあたって，光の強さを少数光子のレベルにまで弱めていったときに顔を出し始める不思議な現象―量子効果―を巧みに利用することにより，離れた二者間での原理的に安全な鍵の共有を可能にしている．こうして得られた鍵を1回だけ使用する限り何人もいかなる計算機も暗号文を解読できない．本稿では，量子暗号による遠隔鍵生成を光ファイバー通信技術を利用して実現しようとするいくつかの試みを紹介し，現状での課題と将来への期待を展望する．

NTT 物性科学基礎研究所（〒243-0198 厚木市森の里若宮 3-1）

1.　光の干渉計による量子暗号

量子暗号の基本原理を説明するとき，光子の偏光自由度を題材にすることが多いが[4,5]，ここでは光ファイバー通信による実現を念頭におき光の二経路干渉を題材にした説明を行おう．

1.1　微弱なレーザー光による量子暗号[7]

まず最初に図1のような普通のマッハ・ツェンダー干渉計を用意しレーザー光（コヒーレント状態の光）のパルスを入力したとしよう．干渉計の入力側には送信者アリスがいて上側の経路における位相シフト量 ϕ_A を操作し，出力側には受信者ボブがいて2つの出力ポートCおよびDから出てくる光の強度を測定する．もし $\phi_A=0$ および π の場合にそれぞれCおよびDだけから光が出力されるように調整してあるとすると，ϕ_A の値が0か π かをそれぞれ符号値の0と1に対応させておけばアリスからボブへの1ビットの情報伝達ができる．これが古典的な場合である．

次にレーザー光の強度をきわめて弱くしてパルスに含まれる平均光子数を0.5個程度にした場合を考えてみる．このときの光の量子状態は記号 $|\alpha>$ によって表され[8]，それは光子数が確定した量子状態（$|0>$，$|1>$，$|2>\cdots$）の重ね合わせ

$$|\alpha>=0.778|0>+0.550|1>+0.275|2>+\cdots$$

として展開できる．ここで各項の振幅の自乗は光子数を測定した場合それぞれ光子数0個，1個，2個である結果が得られる確率を与える．さてボブがCにおいて光子を検出したら符号値は0に確定しDにおいて光子を検出したら符号値は1に確定するという点では，古典的な場合となんら変わるところはない．ところがどちらのポートでも光子が検出されない場合（むろん検出器の効率は1とする）つまり光子数0の量子状態$|0>$に確定する場合が半分近くあり，このときボブは符号値については何も知りようがな

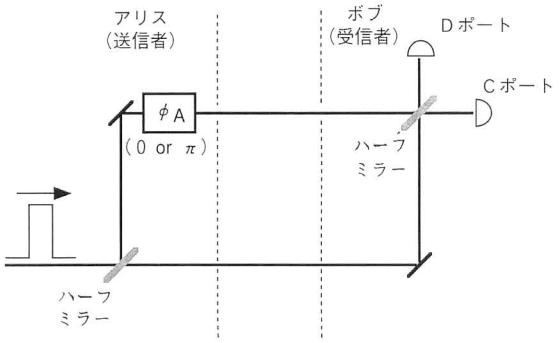

図1　量子暗号の原理説明のための干渉計1.

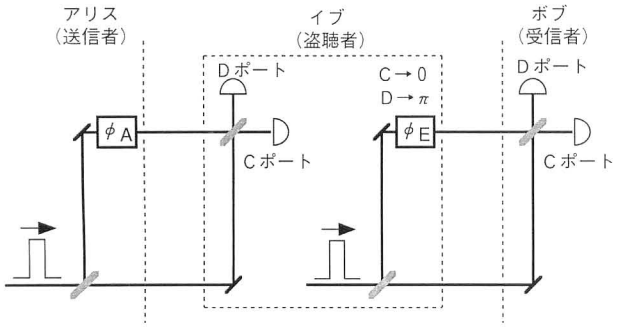

図2　量子暗号の原理説明のための干渉計2（盗聴者イブがいる場合).

い．以後，こうしたビットを不達ビットと呼ぶことにする．

(1) このようにして0，1の乱数ビット列を送信し，(2) 2人で不達ビットを除去した後で，(3) テスト用に抽出した何十個かのビットについて伝送エラーがないことを確認できれば，残りのビット列は暗号鍵として使用できるといったら読者は驚くであろうか．しかしこれが非直交二状態量子暗号と呼ばれる方法の基本手順なのである[1,2,7]．

なぜこれで暗号鍵の秘匿性が保証されるのか，このままでは見当がつかないが，図2のように途中で鍵を覗き見しようと試みる盗聴者イブの存在を想定すれば仕掛けはみえてくる．ここでイブは干渉計の途中に自分用の受信装置と送信装置とを挿入し，アリスから送られた符号値を記録した後で同じ符号値をボブに向けて送り出す．レーザー光が十分に強い古典的な場合にはイブの作戦は成功しアリスとボブは盗聴されていることには気がつかない．ところが光の量子性があらわになる微弱レーザー光の場合には以下に述べるようにイブの目論見は失敗する．

光子が検出されずに符号値が不明な場合でも，イブは「でたらめ」に0か1かを決めてボブに送らなければならない．もし何も送らないとボブに伝わるビットの数が不自然に減少するためかえって気づかれてしまうからである（イブにとって符号値が確定したビットでも首尾よくボブに伝わるのは約半数であることに注意しよう）．

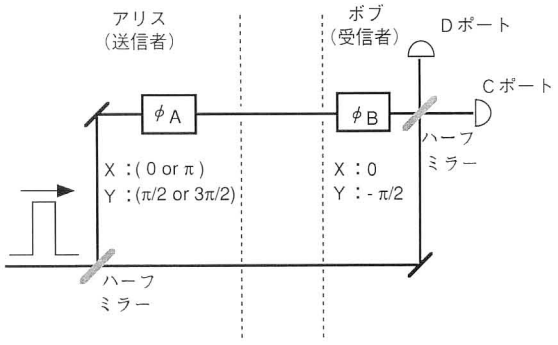

図3　量子暗号の原理説明のための干渉計3(四位相状態制御の方法).

さてこうして「でたらめ」に補完したビットのうちおよそ半数はボブにそのまま伝わることになる．そこでアリスとボブが手順に従って不達ビットを除き伝送エラーの有無を確認するとき，全テストビットのおよそ1/4に符号値の反転が生じることになる．イブが「でたらめ」に送ったビットが運よく的中する確率は1/2なので，イブが検査を逃れられる確率はテストビット数の増加に対して指数関数的に0に漸近する．逆に，十分に多くのテストビットについて符号値の一致が確認できれば，途中で覗き見されていないことが確信できるわけである．

以上が量子暗号による鍵生成の基本的な考え方である．実際にはさらにさまざまな工夫が必要になるのだが，それらについては次節で説明しよう．ここでは，鍵の乱数ビット列がアリスからボブへと伝えられたのではなく，届いたビットだけが抽出されて新たに乱数ビット列が生成されていることを強調しておく．つまり量子暗号は鍵を伝える手段ではなく鍵を生成する手段なのである．

1.2　四位相状態制御による量子暗号[9,10]

干渉計を用いた量子暗号にはこれから述べるような方法もある．前節と同様に干渉計の両側にアリスとボブがいることには変わりはないが，図3に示すようにボブも上側の経路において位相シフト量 ϕ_B を操作できる．

アリスの位相設定 ϕ_A はやや複雑で，$(0, \pi)$ をXベース，$(\pi/2, 3\pi/2)$ をYベースとして，Xベースなら0で符号値0を π で符号値1を表すとし，Yベースならば $\pi/2$ で符号値0を $3\pi/2$ で符号値1に対応させる．ボブも同様にXベースならば $\phi_B=0$ を，Yベースならば $\phi_B=-\pi/2$ を設定する．どちらのベースを選ぶかは，アリスもボブも独立にビットごとにランダムに決める．そして2人ともベース選択の情報は伏せておく．このとき干渉計の出力は位相シフト量の和 $\phi_A+\phi_B$ に依存する．

まず十分な強さのレーザー光を入力する古典的な場合から考えよう．もし2人が選んだベースが一致していれば，

位相シフト量の和は0かπになるので光はポートCかDのどちらか一方だけからしか出力されない．そこでボブはベースの一致を知り，さらにアリスが送った符号値を容易に決定できる．ベースが不一致だと位相の和は$\pi/2$の奇数倍になるため光は両方のポートから同じ強さで出力されるが，それでもボブは2つの出力光の位相差を測定することでアリスの位相設定すなわち符号値を知ることができる．このように光が古典的とみなせるほど強ければ，2つのベースX，Yを使い分けそれを秘密にすることに意味はない．

ところが，個々の光パルスが単一光子とみなせるほどに弱ければ事情は一変する．2人のベースが不一致の場合，光子はこれ以上分割できないのでどちらか一方のポートに確率1/2で出力される．残りのポートからは何も出力されないため，ボブにはベースの一致・不一致を自力で判定する術はない．結局，最後にアリスからベースを教えてもらい，さらにベースの一致がみられた場合に限り自分の光子検出結果から符号値を決めることができるのである．このようにして両者がベース情報を公開し協力して不達ビットを除去した後で，十分な数のテストビットに対して符号値の一致を確認できれば，残った乱数ビット列は安全な暗号鍵として使用できる．

鍵の秘匿性が保証されることをみるには，前と同様に盗聴者イブの存在を想定すればよい．アリスやボブのベース選択は最終段階まで明らかにされないので，イブは「でたらめ」にベースを選んで盗聴しボブに向けて再送信しなければならない．この「でたらめ」が不可避な符号値反転をもたらすことになる．誌面の都合上詳細は省くが，前節を参考にして読者が自分で考えてみてほしい．

この四位相状態の方法は，X，Yベースをそれぞれ直線偏光（水平または垂直），円偏光（左回りまたは右回り）におきかえれば，光子の偏光自由度を用いた最初に提案された量子暗号と等価になる[4]．しかし光ファイバー中を任意偏光状態を保持したまま長距離伝搬させることは通常は困難なので，その代替方法として四位相状態の方法が考案された経緯がある．

なお，ここでは単一光子の入力を想定したが，多くの場合平均光子数を0.1個程度にまで減少させた微弱レーザー光が用いられる．この場合上の説明からも示唆されるように，光子数状態$|2>$，$|3>$…の確率が0ではないことが若干の安全性の低下をもたらすことを注意しておこう．

鍵生成の過程で，アリスとボブはベースの選択情報を普通の通信回線でやりとりしている．このときベースの情報はいくらでも盗聴可能であるが，有線，無線を含めた可能な通信回線のすべてに盗聴者がアクセスして通信内容を盗聴するわけには事実上いかないであろう．このことから鍵生成過程ではベース選択情報の書き換えは不可能であることが前提とされている．実際に鍵を生成するにあたってはこの点の配慮が不可欠である．

ここでは最も単純な盗聴方法を想定したが，さらに手の込んだ方法を試みても単位ビット当たりの検査効率などに違いがでるだけで盗聴不可能なことには変わりはない[5]．より一般的には量子力学のno-cloning定理[11]—「状態準備に関する基底（ベース）情報を知らずして未知の量子状態を複製することはできない」—という物理法則によって鍵の安全性が裏づけられている．

2. 光ファイバーを利用した量子暗号の実験

図1や図3のような干渉計を長い光ファイバーを2本並べて組んで安定化するのは至難の技である．しかしながら，干渉する2つの成分を時間領域あるいは周波数領域で1本の光ファイバー中に多重化することは比較的容易と考えられる[12-21]．本章ではそのような方法による量子暗号鍵生成の実験を2つ紹介しよう[16-21]．なお，どちらの例もボビンに巻いた光ファイバーを用いた室内実験である．

2.1 時間領域光ファイバー干渉計の方法[12,13,16]

まず1章2節で説明した四位相状態制御による量子暗号を実現する時間領域光ファイバー干渉計について紹介する．この実験は1995年に英国British Telecomの研究グループにより発表されたものである[16]．

図4はその全体的な構成図である．まず送信者アリスの装置から眺めてみよう．光源は波長1.3 μm帯の半導体レーザーであり，繰り返し周期1 μsで幅80 psの光パルスを発生する．出力パルス光は垂直に直線偏光しており，さらに平均光子数μが0.1〜0.2程度になるまで大きな減衰を受ける．その後，光カップラーAにより2等分され，片方の成分は水平偏光へと変換された後に時間遅延τを受ける．τは光パルスの幅80 psよりも長くなくてはならない．もう片方の成分は垂直偏光のままアリスによる位相シフトϕ_A（0，π，$\pi/2$，$3\pi/2$のいずれか）を受ける．位相変調器としては光通信用導波路型LN変調器（PM_1）が用いられている．この光カップラーAは図3の干渉計では入口のハーフミラーに相当することに注意しよう．こうして直交する偏光をもつ2つの成分は時間差τをおいて1本の長い光ファイバー中を伝搬することになる．伝搬距離は10〜30 kmである．途中で偏光状態が変わっても2つの成分には時間差があるため両者がクロストークを起こす心配はない．

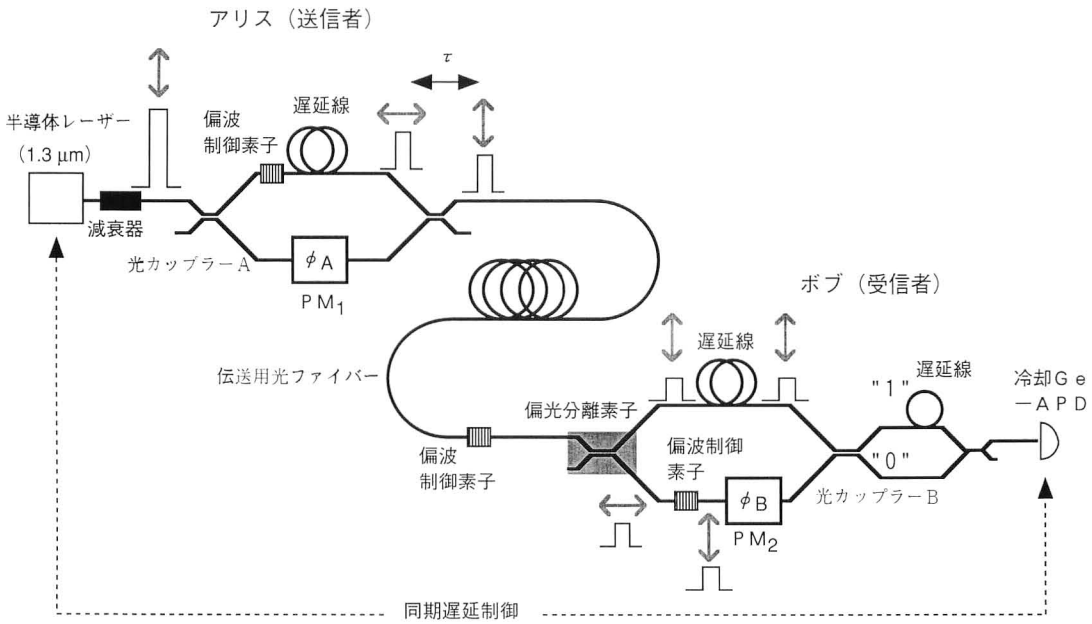

図4　量子暗号のための時間領域干渉計．

次に受信者ボブの装置をみてみよう．まず伝搬中に生じた偏光の変動は偏波補償器により元に戻される．その後，先に到着した垂直偏光成分と遅れた水平偏光成分とは偏光分離素子により空間的にも分離される．垂直偏光成分はその後時間遅延 τ を受け，こうしてまず2つの成分の間の時間差が解消される．一方，水平偏光成分は垂直偏光に戻された後で，同様の位相変調器（PM_2）によって位相シフト ϕ_B（0か$-\pi/2$のどちらか）を受ける．2つの成分は等分岐比光カップラーBにより重ね合わせられ干渉を起こすことになる．光カップラーBは図3の干渉計では出口のハーフミラーに対応していることがわかるだろう．図3の構成では2つの出力ポートの両方に光検出器をおいているが，ここでは2つの出力に時間差をつけることで光検出器の数を1つにしている．

この構成では時間領域と偏光領域を併用して2つの経路の多重化を行っている．どちらか一方の領域を使うだけでも干渉計自体は構成できるのだが，両者の併用により経路の多重化に伴う損失を減らし偏光変動や検出器の暗電流などによる背景雑音から有意な検出信号を効率的に分離することが可能になる．量子暗号では伝送エラーによって盗聴の有無を判断するので，システムに内在するエラーはできるかぎり除去しておかなければならない．この意味でこのような工夫はきわめて重要であることを強調しておく．

光子の検出にはゲルマニウムのアバランシ・フォトダイオード（APD）を使っている[22]．1.3 μm帯や1.5 μm帯などの光通信用長波長帯では，短波長帯にあるような低バックグラウンドで高量子効率をもつ光子検出装置が今のところ存在しない．そこで，APDを液体窒素を使って冷却し熱雑音を抑えた上で，光子1個の入力でも大きな電子なだれが生じるようにブレークダウン電圧以上のバイアスをかけておく．一般にはこれをGeiger modeと呼んでいる．ところがバイアスの増加に伴い光子が入っていないのに勝手になだれが生じて暗電流が起きやすくなってしまう．このように高量子効率と低暗電流との間にはトレードオフがあり，この実験では量子効率を10%前後に低く設定するかわりに暗電流カウントを1パルス当たり10^{-5}個程度に抑えることに成功している．APDは光源と同期制御され，光パルスが入る100 nsの間だけバイアスがかけられる．また光ファイバーの複屈折変動等を補償するために5秒ごとに鍵生成モードから校正モードに切り替え平均光子数 μ を2程度にした上で干渉計全体のキャリブレーションを行っている．

それでは実際のオペレーションと実験結果をみてみよう．アリスやボブの位相設定はすでに1章2節で説明してあるとおりである．入力パルスの繰り返し周波数は1 MHzであるが，パルス当たりの平均光子数 μ が0.1程度，変調器での損失，光子検出効率が10%程度であることから，光子検出の頻度はたかだか～数kb/s程度にしかならない．さらに光ファイバーの伝送損失（～4 dB/10 km），ベース不一致時に不達ビットを除去することなどの理由により，事実上のビットレートはkb/s前後まで下がってしまう．

表1に報告された実験結果をまとめておく．伝搬距離の増加とともに光損失も増えるので当然光子検出数は減少す

表1　鍵生成の実験結果（文献16）参照）．

長さ（km）	μ	ビットエラーレート（%）	伝送レート（bits/s）
10.8	0.1	1.5	700
10.8	0.2	1.2	1400
21.8	0.1	4	350
21.8	0.2	2.8	700
30	0.2	4	260

る．しかしAPDの暗電流は一定なのでエラーレートは増えることになる．30 kmをとばしてもエラーレートが4%に抑えられているのは実用性の観点から注目に値する．平均光子数μが0.2になると光子が増えた分エラーレートも減るが，最終的に得られる鍵のビット数は実はさほどに変わらない．これは，鍵を生成する過程で伝達ビットの生データを直接使うのではなく，システムエラーの影響を除去するために誤り訂正を施していることに関係している．1章2節で少しふれたようにμの増加は安全性の低下をもたらすので，より複雑な誤り訂正を行って安全性を確保する必要があるからである．

2.2　周波数領域光ファイバー干渉計の方法[17,21]

次に，外部位相変調による側帯波成分を利用した光ファイバー干渉計の方法を説明しよう．これは1章1節で述べた微弱レーザー光による量子暗号を実現する手法であり，1999年にフランスのGTL-CNRS Telecomを中心とするグループにより発表された[21]．

図5に示すように装置の構成はいたって簡単である．まずアリスの送信装置からみてみよう．1.5 μm波長帯（光の中心キャリヤー周波数ω_0）の線幅1 MHzの半導体レーザーの出力光は電気光学変調器（EOM）により繰り返し周波数1 MHz，幅50 nsの光パルスとして切り出されその後パルス当たり平均光子数が10数個になるように著しい減衰を受ける．そして光通信用LN位相変調器（PM_1）により周波数Ω＝300 MHz，初期位相Φ_1の位相変調を受ける．変調の深さmは浅く片側側帯波成分（光周波数$\omega_0 \pm \Omega$）に含まれる平均光子数μが0.1程度になる程度である．そして20 kmの伝送用光ファイバーに入力される（損失2 dB/10 km）．

次にボブの受信装置をみてみよう．送られてきた位相変調光パルスはさらに同様の位相変調器（PM_2）により位相変調を受ける．変調周波数Ωは同様に300 MHzであり初期位相はΦ_2である．ここでアリスとボブの変調信号は同期されている．その後，中心キャリヤー周波数成分ω_0と側帯波成分$\omega_0 \pm \Omega$とはファブリー・ペロー・エタロン（FPE）により分離され片側側帯波成分に含まれる光子が検出される．光子の検出には前項と同様に液体窒素で冷却したゲルマニウムのAPDをGeiger modeで使用する[22]．

この系で干渉を起こすのは，アリスによる位相変調で生じた初期位相Φ_1の側帯波成分と，中心キャリヤー周波数成分として伝搬しボブによる位相変調によって初期位相Φ_2の側帯波へと変換された成分である．伝搬中に受ける位相のゆらぎは，中心キャリヤー周波数成分も側帯波成分も同じなので干渉には影響しない．アリス側で生じる側帯

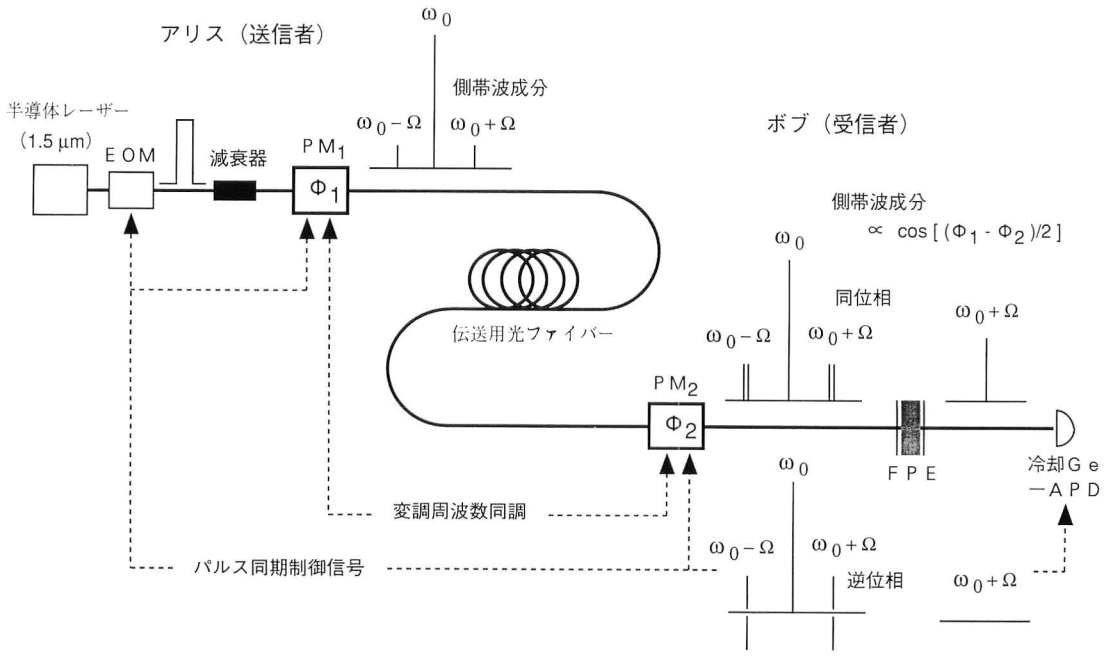

図5　量子暗号のための周波数領域干渉計．

波とボブ側で生じる側帯波の振幅が等しくなるように変調の深さを調整できれば，干渉後の側帯波の振幅は $\cos[(\Phi_1-\Phi_2)/2]$ に比例することになる．

1章1節で説明したように，Φ_1，Φ_2 の値はともに0か π なので cos 関数の値は1か0になる．図1と比べると，アリス，ボブの位相変調器がそれぞれ入口と出口のハーフミラーに対応していることがみてとれるだろう．図1との違いは片方の出力ポートしかみていない点であるが，ボブが Φ_2 を0と π との間でランダムに切り替えることでポートC，Dでの測定を1つの出力ポートで兼用している．ただし同時に測定はできないために効率は半分になる．

20 km 伝搬させたときの光検出信号と暗電流カウントの比は25:1でありエラーレートは4%と報告されている．この方式ではエラーを小さくするために光キャリヤー周波数やFPEの透過ピークの位置を安定化しておくことが必要である．なお，中心キャリヤー周波数の成分は必ず届かなければならない準古典的なパルスなので，もはや盗聴者イブはビットが不明だった場合に何も送らないという手段はとれなくなる．このことは盗聴検出を行う上で有利に作用する．

以上，完成度が高い2つの実験について簡単に紹介した．量子暗号が成立するために許容されるシステムエラーの上限は7%程度であることが知られているが，どちらの例でもすでに十分にこの条件はクリアされている．光ファイバー利用による量子暗号の実験にはこのほかにも，往路と復路とで同じ光ファイバーを利用し伝搬中の外乱の影響を相殺する往復方式（敷設光ファイバーによる実験）[18-20]，伝搬中の偏光状態の変化をモニターしてフィードバック制御により補償する方式などが知られている[14]．

3. 課題と展望

量子暗号という名前の高尚さとは裏腹に，実験のほうはわりと単純であることを意外に思われたであろう．少なくとも光源と伝送媒体に関する限り現存する技術でも対処は可能である（もちろん課題はたくさんある）．むしろ現状での最大のボトルネックは光通信波長帯で適当な光子検出素子が存在しないことであろう．冷却Ge-APDを用いる方法[22]はとうてい手軽とはいいがたいし，量子効率や暗電流特性の素子間でのばらつきを考慮すると紹介したような良好なデータはそう簡単に得られるものではないことが推察されよう．

それでもなお，光子検出に適した受光素子を素子レベルで設計・開発する可能性は十分に残されている．従来の光通信用受光素子に要求されていた特性と光子検出に求められる特性とは大きく異なるため設計段階での最適化が期待できるからである．かつて冷却しなければ発振しなかった半導体レーザーが今では大量に商用化されていることを思えば，これはあながち希望的推測とはいいきれないだろう．

また量子暗号システムの総合実験という観点からは，実際に盗聴者がいる場合のシステムの挙動を把握することが今後の課題になってくるだろう．著者の知る限り実際に盗聴シミュレーションまでやったという例はまだない．

量子暗号の基本原理が最初に提案されてからすでに15年以上が経過した．この間の物理学者と情報科学者の協力によって理論面での整備はほぼ完了したといってよい．しかし実験面での本格的な研究はようやく始まったばかりである．そろそろ量子光学のみならず光工学やフォトニクス関係の研究者・技術者もこの分野に参入して腕をふるう頃合だと思われるがいかがであろうか．

文　献

1) A. エカート（井元信之訳）："量子暗号への招待"，パリティ，**7**（1992）26-31.
2) G. コリンズ（井元信之訳）："量子暗号は史上最強の暗号"，パリティ，**5**（1993）31-35.
3) C. H. Bennett, G. Brassard, S. Breidbart and S. Wiesner: *Advances in Cryptography: Proceedings of Crypto '82*, eds. D. Chaum, R. L. Rivest and A. T. Sherman (Plenum, New York, 1983) p. 267.
4) C. H. Bennett and G. Brassard: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984) p. 175.
5) *Introduction to Quantum Computation and Information*, eds. H. K. Lo, S. Popescu and T. Spiller (World Scientific, New Jersey, 1998).
6) 特集/量子コンピュータ，数理科学，No. 424（1998）.
7) C. H. Bennett: Phys. Rev. Lett., **68** (1992) 3121.
8) たとえばR. Loudon: *The Quantum Theory of Light*, 2nd ed. (Oxford University Press, 1983)；松岡正浩：量子光学（東京大学出版会，1996）.
9) P. D. Townsend and I. M. Thompson: J. Mod. Opt., **41** (1994) 2425-2433.
10) B. Huttner, N. Imoto, N. Gisin and T. Mor: Phys. Rev. A, **51** (1995) 1863-1869.
11) W. K. Wootters and W. H. Zurek: Nature, **299** (1982) 802-803.
12) P. D. Townsend, J. G. Rarity and P. R. Tapster: Electron. Lett., **29** (1993) 634-635.
13) J. C. Rarity, P. C. M. Owens and P. R. Tapster: J. Mod. Opt., **41** (1994) 2435-2444.
14) J. D. Franson and H. Ilves: Appl. Opt., **33** (1994) 2949-2954.
15) J. Brequet, A. Muller and N. Gisin: J. Mod. Opt., **41** (1994) 2405-2412.
16) C. Marand and P. D. Townsend: Opt. Lett., **20** (1995) 1695-

1697.
17) P. C. Sun, Y. Mazurenko and Y. Fainman: Opt. Lett., **20** (1995) 1062-1064.
18) A. Muller, H. Zbinden and N. Gisin: Europhys. Lett., **33** (1996) 335-339.
19) A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden and N. Gisin: Appl. Phys. Lett., **70** (1997) 793-795.
20) H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller and W. Tottel: Electron Lett., **33** (1997) 586-588.
21) J. M. Merolla, Y. Mazurenko, J. P. Goedgebuer and W. T. Rhodes: Phys. Rev. Lett., **82** (1999) 1656-1659.
22) P. C. M. Owens, J. C. Rarity, P. R. Tapster, D. Knight and P. D. Townsend: Appl. Opt., **33** (1994) 6895-6901.

(2000年2月1日受理)