情報処理最前線 Frontier

量子暗号技術とその将来展望

長谷川俊夫（三菱電機（株）情報技術総合研究所）
toshio@iss.isl.melco.co.jp
西岡　毅（三菱電機（株）情報技術総合研究所）
nishioka@iss.isl.melco.co.jp

はじめに

近年，通信インフラの整備が進み，またインターネットなどのオープンなネットワーク上で現代暗号技術を応用した情報セキュリティシステムの構築が進んでいる．また一方，それらの技術とは別に，量子力学を情報処理技術に応用した量子情報処理技術が最近注目されている．量子情報処理技術とは，電子や光子といった量子が主役となる新しい情報処理技術である[1),2),4)]．

量子情報処理の理論研究は1970年代頃から行われ，近年の実験技術の向上に伴い，理論での予言が実験的に検証されつつある段階である．量子情報処理技術には，大きく分けて量子暗号，量子通信，量子計算の3つの技術がある．このうち暗号・情報セキュリティと関連するものに量子暗号と量子計算が挙げられる．

量子計算では，1994年に素因数分解の多項式時間アルゴリズム，1996年にデータベース高速検索アルゴリズムという理論的な大きな発見があり，物理的な実験なども少しずつであるが着実に進んでいる．ところで，現在利用されている暗号技術の多くは，計算量理論に基づいてその安全性が評価されている．すなわち解読するためには膨大な計算量が必要であるということを安全性の根拠にしている．このため，現代暗号は将来量子計算機のようなある種の超高速計算機が実用化されると解読されてしまうという問題点があるし，また盗聴されても検知できないという課題もある．

一方，量子暗号は，物理の基本原理をうまく利用しているため，物理法則で安全性が保証され，前述の問題を克服することができて，絶対解読されない究極の暗号技術として期待されている．量子暗号は，量子情報処理技術の中で一番素朴に量子力学的効果を利用したものであり，実験やそのシステム化も多くの研究者が行っている実用化に一番近い技術である．

本稿は，情報処理系の技術者にも分かりやすく量子暗号技術の概要と実用化および将来展望を解説する．まず最初に量子暗号の基本原理について説明し，次に実際の実現方法について簡単な例を交え紹介する．さらに現実の環境では生じてしまうノイズなどを安全に取り除くようなデータ処理（これはまったく情報理論的なもの）についても記述する．そして国内外の研究開発動向について紹介する．最後に暗号，量子情報，通信分野からみた量子暗号技術の位置付け，将来展望について考察する．

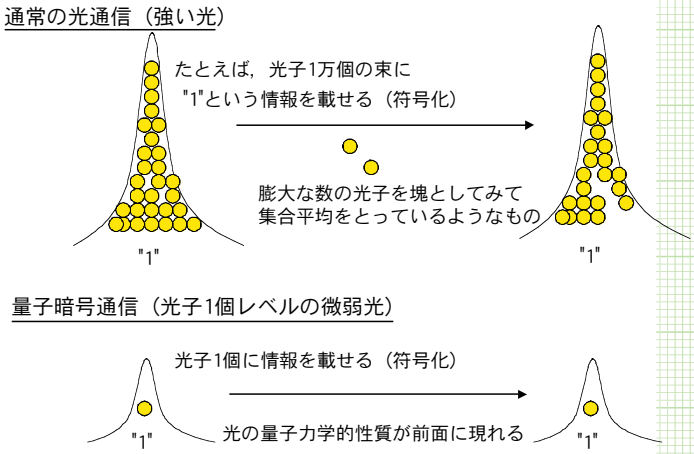

図-1　量子暗号通信と通常の光通信の簡略イメージ

量子暗号の基本原理

量子暗号とは一言でいうと，「量子力学の基本的性質を利用した絶対解読が不可能な暗号技術」といえる．その特徴は，物理法則により安全性が保証され解読されることがない，また通信路上で不正なデータの盗聴があっても即座に検知可能という2点である．

まず最初に量子暗号の大雑把なイメージを通常の光通信と比べて図-1で説明しよう．通常の光通信では，強い

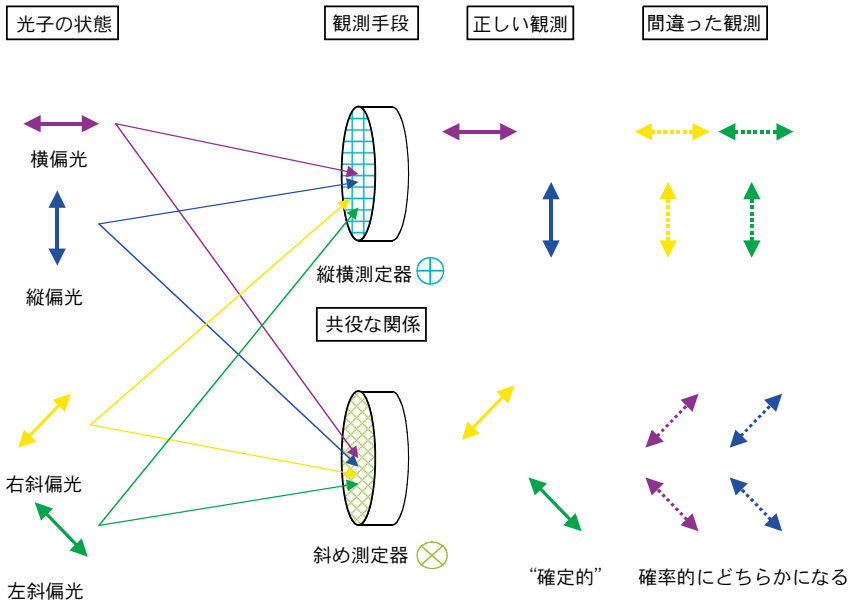

図-2　光子の偏光状態と観測手段の関係

光を用いて膨大な数の光子に情報を載せている．このため光子（量子）を用いてはいるが，それらを集合として扱っているため，その量子力学的効果は前面に出てこない．一方，量子暗号は簡単にいうと，非常に微弱な光による通信であり，情報を伝送媒体である光子１個に対して１個の情報を載せて通信をする．このため光子の量子力学的性質が前面に現れてくる．それでは通常の光通信で単純に光を弱くすれば量子暗号かという疑問が湧いてくると思うが，そう単純ではない．実際は情報が載った量子状態を正規の受信者のみは正しく観測できるが，それ以外の者には正しい観測ができないような“仕組み（プロトコル）”を構築して初めて絶対安全な暗号通信が実現する．

ではその仕組みを説明する前に，準備としてこれらを可能にする物理の基本原理を説明しよう．量子暗号において，情報は量子状態に変調されて伝送される．量子状態には，「重ね合わせの原理」が成り立ち，相異なる状態，たとえば，“0”を表す状態 $|0\rangle$ と“1”を表す状態 $|1\rangle$ を合わせたようなミラクルな状態 $\alpha|0\rangle+\beta|1\rangle$ を伝送することも可能となる．このため，量子伝送のプロセスにおいては量子力学の法則に従って奇妙な現象が起こる．これを暗号に応用したものが量子暗号である．その安全性を保証する物理の基本原理は，大きく２つの柱から成り立っている．１つは，複製不可能定理（no-cloning theorem）．もう１つは，Heisenbergの不確定性原理（uncertainty principle）である．

複製不可能定理とは，“未知の”量子状態があったとき，その完全な複製である量子状態を作成し，この量子状態を２つ持つことができないという定理である．この定理によれば，盗聴者Eveが通信路上にある量子状態をかすめ取って，コピーをつくり，１つは自分が情報を傍聴するのに使い，もう１つは通信路に戻して盗聴の痕跡を消すという攻撃が不可能であることが保証される．ちなみに，量子テレポーテーションでは，量子状態が別の場所で再生されるが，オリジナルの状態を壊してしまうので，複製不可能定理には抵触しない．

それでは，Eveが通信路上でかすめ取った未知の量子状態を観測して，既知の量子状態にしたら，検知されない盗聴が可能であろうか．これに対する保証がHeisenbergの不確定性原理で与えられている．Heisenbergの不確定性原理によると，観測対象となる物理量がいくつかあるうちで，同時に正確に測定できない物理量の組が存在する．よく知られたものでは，位置と運動量であり，光子では，縦・横偏光と右斜・左斜偏光がある．これらの物理量は共役な関係にあるといわれる．

そこで，伝送に用いる量子状態への符号化ルールとして，共役な物理量を使い，２つの符号化ルールをランダムに選択して用いるのである．たとえば，光子の場合，(0,1) の符号化として（横，縦），（右斜，左斜）の偏光状態を用いることができる（図-2）．このとき，Eveに限らず任意の観測者は１回の観測では，どちらか一方の組しか正確に観測できない．量子状態に対して，正しい観測を行えば正しい結果が得られるが，間違った観測を行うと，その結果からは何も判断できない．このため，Eveが観測した量子状態のほぼ半数は間違って観測したことになり，その分不確かな状態を伝送せざるを得ないので，盗聴の痕跡を残さざるを得なくなる．

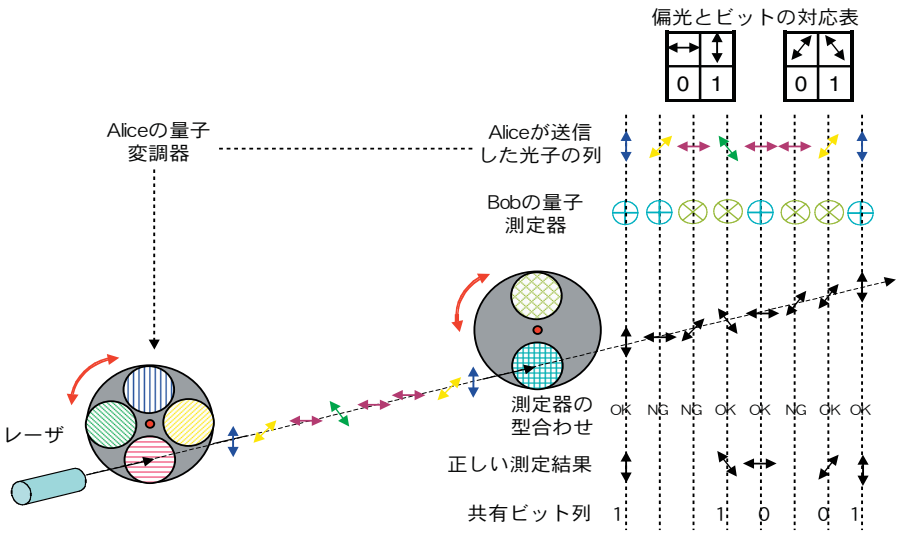

図-3　偏光状態を用いたBB84プロトコルの仕組み

具体的実現方法

前章で述べた原理を利用して見事な成功を収めた量子暗号として，遠く離れた2者間AliceとBobの間で共通鍵の共有を実現する量子鍵配布プロトコルがある．ここでは，その代表的なプロトコルであり，BennettとBrassardにより1984年に提案されたBB84プロトコルを説明する．狭義のBB84プロトコルは，量子状態として光子の4つの偏光状態を用いて実現する方式である（偏光変調方式）．一方，光子の位相状態を用いて実現する位相変調方式も存在する．光ファイバーを用いた実現方式では主に位相変調方式が用いられている．いずれにせよ，その数学的構造は同じである．

Aliceは横偏光，縦偏光，右斜（45度）偏光，左斜（135度）偏光に対応する4つの量子状態を準備する．これに応じて，Bobは縦横測定器⊕と斜め測定器⊗の2つの観測手段を用意しておく．縦横測定器⊕は横偏光，縦偏光を正しく測定できる．斜め測定器⊗は右斜偏光，左斜偏光を正しく測定できる．いずれも間違った測定器を選択すると，まったく量子状態の手がかりが得られない．では秘密鍵を共有するまでのプロトコルを図-3を用いて説明しよう．

(1) AliceとBobは独立に乱数を用意する．Aliceはこの乱数に従って光子1個ごとに4つの状態（↔, ↕, ↗, ↖）の1つをランダムに選択し（すなわち符号化し），Bobに伝送する．Bobは独立に生成した自分の乱数に従い，2つの測定器（⊕，⊗）から1つをランダムに選択し，伝送された光子を測定する．測定結果は秘密に記録しておく．

(2) 光子の伝送が済んだら，Bobはどの測定器（⊕か⊗）を用いたかをAliceに連絡し，Aliceはその中からどれが正しい測定器を用いていたかを回答する．これは，（盗聴される危険のある）公開通信路で行ってよい．

(3) 次に，AliceとBobは正しい測定が行われた光子の測定結果のみを抽出すると，2者間で秘密に乱数ビット（この例ではビット列"11001"）が共有されたことになる．これが秘密共通ビット列となる．

前章での“仕組み”とは，要は光の伝送後，観測基底を交換し基底が合致した観測結果のみを使用するというものである．

ただし，現実の系ではこの共有ビット列中には，若干のエラーや盗聴者による擾乱（じょうらん）も含まれているため，直接の暗号の鍵として用いることができない．そこで量子暗号の実用的システムでは，次章で述べるような量子暗号特有のデータ処理が必要となる．このデータ処理では，ほぼ同じランダムデータ2つを互いに開示することなく，かつ，公開通信路において相互参照しあう情報量はなるべく小さくしつつ，ビットエラーの誤り訂正（除去）処理を行う．さらに，これまでの過程で盗聴者に漏洩されたとみられる情報をできるだけ小さくするためのプライバシー増幅処理も実行される．この処理の過程において，量子通信におけるビットレートおよび量子ビットエラーレート（QBER）も算出する．この推定されたビットレートとQBERの値を基に量子暗号通信において盗聴者の有無が決定される．一般に，正常の通信時より大きなQBERが算出される，もしくは，ビットレートがより低い値を示すと盗聴行為があったと検知される．

実用システムのためのデータ処理

理想的な環境下での量子暗号（鍵配布プロトコル）では，通信2者間で絶対安全に鍵共有を実現することがで

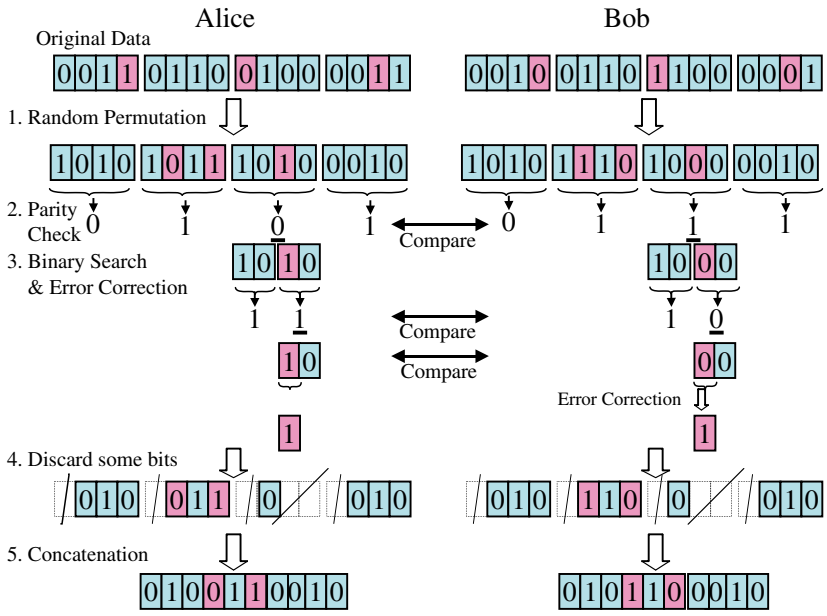

図-4　量子暗号における誤り訂正処理イメージ

きることが理論的に示されている．この鍵を用いて，絶対安全な暗号通信が実現することになる．しかし，実際の環境下では，通信路上での擾乱（じょうらん）や物理的な計測機器の不完全さによる影響（たとえば，光子検出器などの暗計数など）が存在する．このため，鍵配布プロトコルで共有した鍵データにわずかではあるが不一致ビットが存在する場合がある．

というわけで現実の系では，量子暗号のプロトコルを実施して鍵を共有した後に，さらに量子力学の世界から離れて情報理論的なデータ処理を行う必要がある．このデータ処理は，誤り訂正処理とプライバシー増幅からなるが，簡単にこの2つを説明しよう．

誤り訂正処理

誤り訂正処理は，共有した鍵データ中の不一致ビットを訂正（除去）する処理で，量子暗号とはまったく関係なく情報理論的な仕組みに基づいて行うものである．

ただ注意すべき点は，通常の通信等で用いられる誤り訂正処理とは異なり，安全性を保ったまま誤りを訂正（除去）する必要があるということである．ここでは代表的なBBBSSプロトコルを示す（**図-4** では共有したデータが16ビット，不一致ビットが3ビットの簡単な例）．

[BBBSSプロトコル]

鍵共有プロトコルで不一致ビットを含む乱数系列を通信2者間（Alice，Bob）で共有する．

(1) 乱数列の全ブロックでパリティ一致する事象が，ある設定回数続くまで，次の（a）～（c）の処理を実行する．

（a）乱数系列全体をランダム置換する

（b）得られた乱数系列をブロック（図-4では4ビットごとの簡単な例）に分割する

（c）次の操作を各ブロックごとに実行する

i. ブロックごとにパリティ値を計算し，公開通信路を通じて送信し比較する．

ii. パリティが一致なら，1ビット削除してそのブロックを残す．パリティ不一致なら2分探索法により不一致ビットを訂正する．ただしこの場合，公開通信路で比較したビット数分は削除する．なぜなら，鍵データの中でこのビット数分だけの情報量は，第三者（盗聴者）に対して漏れてしまっているからである．

(2) 得られた系列を精製されたデータ（corrected key）として出力する．

というわけで，量子暗号における誤り訂正処理では，公開通信路を通じて比較したパリティのビット数分だけは削除するため，最初の訂正前のデータより訂正後のデータはビットサイズ的に少なくなる．もちろん誤り率が大きい場合ほど最終的に訂正後の鍵サイズが小さくなってしまうことになる．また(1)の(b)でのブロックサイズの設定も（推定される）誤り率に従って適した値が考えられ可変にすると効率がよい．ちなみに情報理論的に考えると，共有ビット列（ビット数N）の不一致ビットを訂正するために公開通信路を通じて交換するのに必要なビットの下限N_{pub}は，いまエラー率をeとするとShannonの定理より次式で与えられる．

$$N_{pub} = N\,(-e\log e - (1-e)\log(1-e))$$

	波長帯（nm）	伝送距離（km）	QBER（%）	鍵共有速度（bps）
Geneva	1300	22.8（fiber）	1.4	0.5
BT	1300	21.8（fiber）	4.0	350
		10.8（fiber）	1.5	700
Geneva	1310	4.9（fiber）	4.0	1630
		22.8（fiber）	5.4	486
IBM	1300	10.0（fiber）	5.0	1000
三菱電機&北大	830	0.2（fiber）	1.7	1100
		1.0（fiber）	5.0	762

表-1　量子暗号のシステムとしての実現例（光ファイバー通信路）

プライバシー増幅

プライバシー増幅機能は，同じビット列を共有しているときに，その共有ビットの一部が盗聴者に漏れてしまっていても，この処理を施すことでまったく盗聴者に最終的な共有ビット列に関する情報を分からないようにするものである．具体的には，訂正された共有ビット列（corrected key）中にある盗聴者にわずかに知られている可能性のある情報をなくすために，たとえば適当な行列を用いて線形和を生成しビットサイズをセキュリティパラメータs分だけ少なくしたり，ハッシュ関数を用いてより短いビット列として情報を落とし完全な鍵データ（final key）にする．

たとえば前者の簡単な例を挙げると，k_f，k_cをcorrected key（nビット），final keyの縦ベクトル表示，Kを0,1からなる（n-s）行n列の行列とすると，

$$k_f = K\, k_c (\mathrm{mod}\ 2)$$

なる処理でk_fが導出される．

実際のシステムでは，誤り訂正（除去）処理の際にエラー率を評価（推定）し，これをもとに盗聴者にどれくらい情報が漏れているかの上限を見積もり，プライバシー増幅の際にどのくらい鍵の圧縮をすればよいかに反映させるというステップがとられる．この値はRényiエントロピーが目安となる．詳細はここでは省略する．

研究開発動向

量子暗号の基本原理やその実現方式に関してこれまでの章で説明した．ここでは，量子暗号の研究・実験がどのような研究機関で行われており，実用化に向けた動きはどうなっているのか紹介しよう．

理論研究は，当初IBM，Oxford大学等で進められ，現在では各研究機関で実施されている．国内ではNTTが早くから研究に着手し，その他，日本電気，通信総合研究所，三菱電機，各大学などで行っている．

実際の実験に関しては，IBM，ロスアラモス国立研究所（LANL），John Hopkins大学（JH），ブリティッシュテレコム（BT），Geneva大学，Oxford大学など，また国内では，産業技術総合研究所，三菱電機，日本電気，学習院大学，北海道大学，日本大学などで行われている．さらにデータ処理まで含めた量子暗号のシステム化まで行っているのは，Geneva大学，IBM，BT，三菱電機&北海道大学などの研究機関である．特にGeneva大学では，レマン湖の下の既設光ファイバー23kmを用いて実験済みで，さらにシステム化も実施しており，かなり進んでいる．参考までに，量子暗号システムの実現例を**表-1**にまとめた．現在，伝送距離は数十Km，鍵共有速度は1Kbps程度の性能が達成されている．速度的には通常の光通信と比較すると非常に遅いが，暗号通信での秘密鍵（たとえば128ビット程度）としての使用用途を考えれば，ある意味この値でも実用的ともいえる．

実現方法としては，符号化の方式として位相変調方式を用いて，伝送路として光ファイバーを用いて実現するのが最近の実験例の主流である．具体的な実験の詳細はここでは省略するが，参考までに，Faraday Mirrorを用いた光学的に高い系の安定性を持ち，タイミング同期等の機能も含んだ洗練された実験系例を**図-5**に示す．

図-5で，APDは光子検出器，PMは位相変調器，FMはFaraday Mirror，Cは光カプラ，PBSは偏光ビームスプリッタ，D_Aは光検出器を表す．制御系で光子がPMを通過したときタイミングよく位相変調制御を行う．この位相変調方式では，2つの光路長が同じpathで，位相差（AliceとBob）による干渉効果を利用して量子暗号（鍵配布）を実現する．

技術課題

それでは，ここで量子暗号の実用化の技術課題について考えてみよう．技術課題は大きく分けて単一光子生成技術，単一光子検出技術，量子中継技術の3つ挙げることができる．

単一光子生成技術

量子暗号では，光子1個に対して情報を載せて通信を行っている．重要なのは，光子1個ということである．しかし実際は，光子1個を確実に生成し送信することは，いまだ困難な技術である．光源としてレーザーを用いる

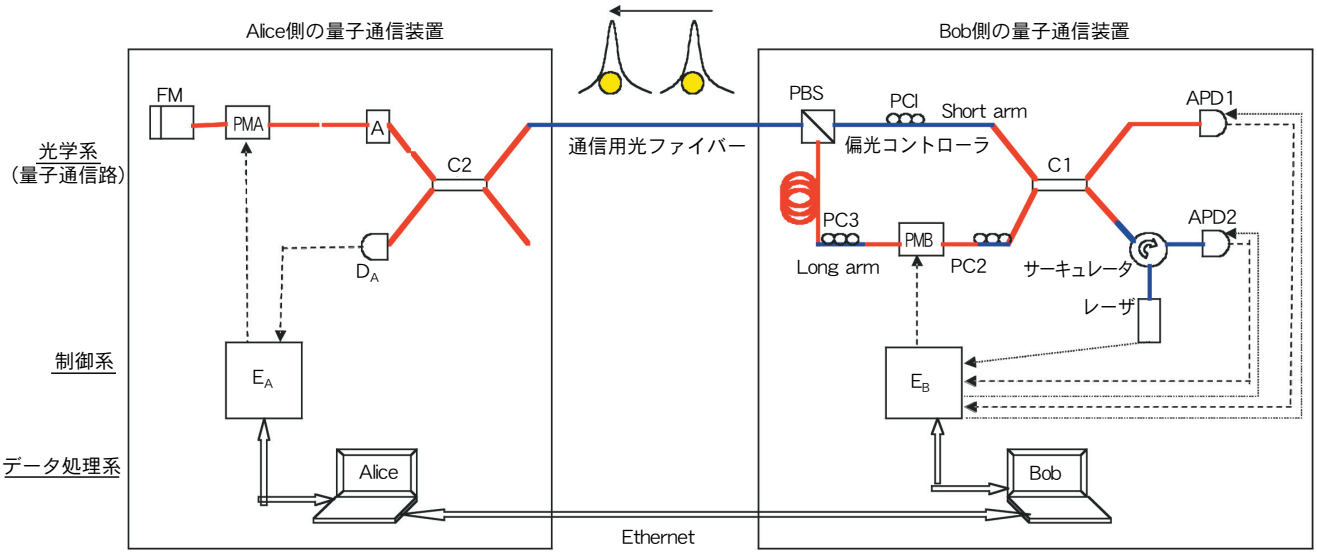

図-5　光ファイバーを用いた量子暗号の実験系列（代表的なGeneva大学のplug&play方式）

検出デバイス材料	波長帯（nm）	温度（K）	量子効率（%）
Si	800	室温	50
Ge	1300	77	10
InGaAs	1300	77	20
InGaAs	1300	173	10
InGaAs	1550	173	2
InGaAs	1550	238	24

表-2　光子検出器の性能例[3), 5)]

と，パルス当たりの平均光子数を確率分布的にしか設定できない．たとえばパルス平均光子数を1個と設定しても，パルス当たり2個光子を含む場合や0個だったりする確率もわずかだが存在する．このため通常の実験システムでは，レーザー光を減衰させてパルス当たりの平均光子数を0.1個（平均10パルスに1個光子が含まれるよう）にして，2個以上含む確率を十分無視できるほどに小さくして近似的に単一光子源として使用している．2個以上の光子を含む場合の影響は後に施すデータ処理で十分落とせるが，平均光子数を0.1にすると鍵生成速度が1/10遅くなるという問題がある．

単一光子生成技術は，安全性という観点からも，また量子暗号のシステム性能向上という点でも重要な技術課題である．ただし，双子の光子対を用いて片方をモニタ制御に，他方を光子発生として使用する方法や，また近年東芝欧州研でLDを用いた単一光子発生素子の研究等の報告もあり，着実に研究は進んでいる．

単一光子検出技術

量子暗号は，通常の光通信と異なり光検出部分で単一光子検出（または微弱光検出）を行っている．このため単一光子検出技術が必要である．使用する光の波長帯で短波長帯（700～900nm）と長波長帯（1300nm, 1550nm）に分けられる．**表-2**に示した通り，短波長帯での光検出器は市販され，室温で動作し検出効率が50%程度のものが存在するが，長波長帯ではこのようなものは存在せず，まだ解決すべき課題が残っている．このため，長距離通信に適した長波長帯で量子暗号の実現を図る場合，この検出効率の低さが，鍵共有速度の低さや通信距離の限界にも関係してくる．

しかし，今までは市販のAPD（avalanche photo diode）素子を非常に低温（たとえば173K）に冷却してある特殊な動作モードで動作させ，ようやく10%程度の検出効率の検出実験がなされていたが，近年，産業技術総合研究所での実験報告で238Kと高温で（ペルチェ電子冷却可能温度）30%程度の検出効率が達成されている[5)]．市販のAPD素子を使って通信波長帯で光子検出器を開発する方向では，比較的洗練された結果が得られている．ただし，単一光子デバイスからの研究という面ではまだまだ研究段階である．

量子中継技術

量子暗号通信では，通信距離の限界は100km程度ではないかといわれている．ちなみにこれは光子検出器の暗計数などによって決まる限界である．さらなる長距離での量子暗号の実現には，この量子中継技術が必要となっ

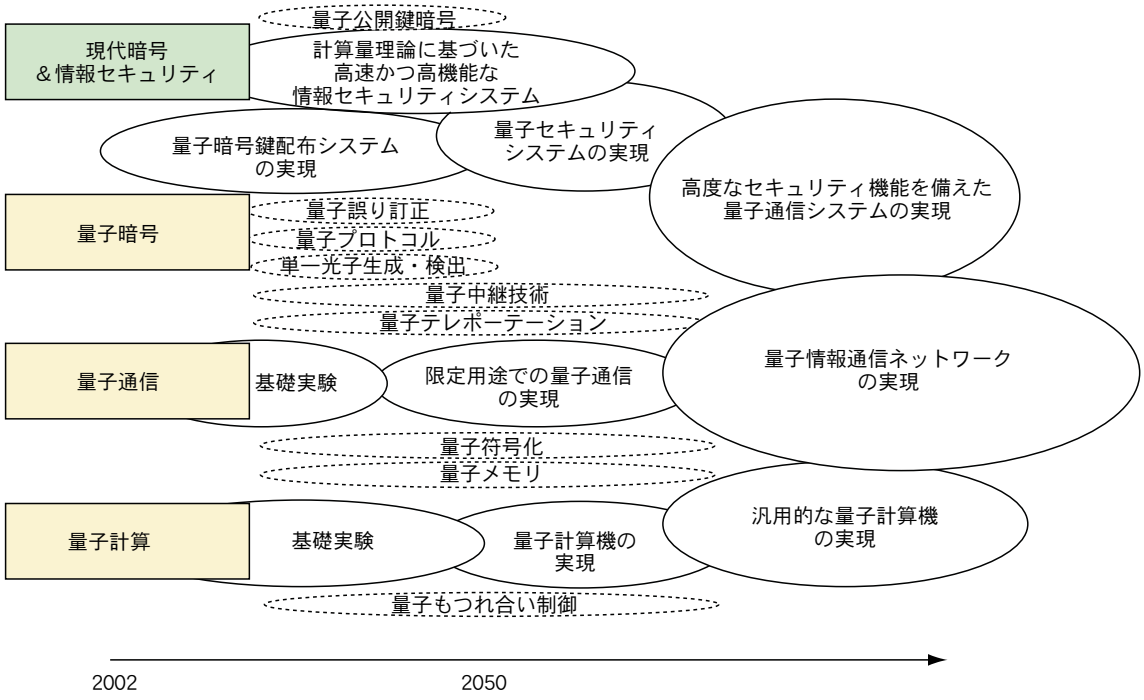

図-6　現代暗号，量子暗号，量子通信，量子計算などの将来展望

てくる．こちらは量子もつれ合いなどを利用する技術で，まだ研究段階で今後の発展を期待したい．

将来展望

以上本稿では量子暗号の基本原理や具体的実現方法，データ処理について説明した後，研究開発動向や技術課題について概観した．ここでも分かるように，量子暗号はすでに実験室レベルではなく，技術課題はあるものの，プロトタイプ販売など実用化に向けて着実に進んでいる．最後に現代暗号・情報セキュリティ，量子暗号の将来展望や位置付けについて考えてみよう（**図-6**）．

暗号・情報セキュリティ分野において量子暗号の位置付けを考えてみると，理論的には量子計算の出現で公開鍵暗号は解読されるというセンセーショナルな理論結果があり，それに対する１つのパラダイムとして量子暗号が存在する．すなわち量子暗号は，量子計算機が実現されても絶対的な安全性は揺らぐことがない．では既存の現代暗号がすぐに量子暗号にとって替わるかというと，実際は現代暗号と量子暗号の共存した世界がしばらく続き，その後，量子情報技術の研究進捗に合わせ徐々に移行していくのが自然な考え方だろう．

また，光通信や量子通信という観点から量子暗号を考えてみると，当然のことながら光通信と密接に関係した分野であり，原理は量子通信より簡単であるが，将来の量子通信への実現の着実な第一歩となり得る重要な要素技術を含んでいる．

量子情報技術の中では量子暗号は，量子計算や量子通信と比べてある意味地味な印象があるかもしれない．しかし，一番実現が近い技術であり，実際は実証実験やその研究成果がその他の分野にフィードバック可能であり非常に魅力的な分野であることは間違いない．また，理論的には大枠はできてはいるが，実際の実験・実装的観点からの研究要素も豊富であり，さらなる発展が期待できるだろう．

謝辞　最後に本稿を執筆するにあたり貴重なコメントをいただいた北海道大学 電子科学研究所 竹内繁樹助教授に，また有意義な議論をいただいた三菱電機（株）情報技術総合研究所の松井充チームリーダ，石塚裕一氏，安部淳一氏，鶴丸豊広氏に感謝いたします．

参考文献

1）Lo, H.-K. et al.: Introduction to Quantum Computation and Information, World Scientific (1998).
2）Bouwmeester, D. et al.: The Physics of Quantum Information, Springer (2000).
3）Zbinden, H. et al.: Quantum Cryptography, Appl. Phys. B67 (1998) 743.
4）Gisin, N. et al.: Quantum Cryptography, Rev. Mod. Phys. 74 (2002) 145, quant-ph/0101098.
5）Yoshizawa, A. et al.: A 1550nm Single-Photon Detector using a Thermoelectrically Cooled InGaAs Avalanche photodiode, Jpn. J. Appl. Phys. Vol.40 (2001) 200.
6）Hasegawa, T. et al.: An Experimental Realization of Quantum Cryptosystem, IEICE Trans. Fundamentals, Vol.E85-A, No.1, 149 (2002).

（平成 14 年 6 月 12 日受付）