量子暗号技術

量子暗号は量子力学の原理を用いて，通信路における最高度に安全な秘匿通信を実現する技術です．本稿では量子暗号技術全般に関して最近までの世界の研究動向とNTTでの研究の位置付けと現状を簡単に解説します．また本稿以降の記事では，ここで概観した技術の詳細を紹介します．

都倉 康弘（とくら やすひろ）

NTT物性科学基礎研究所

量子情報通信技術

20世紀初頭に生まれた量子力学は，トランジスタをはじめとするエレクトロニクスや，分子から生体に至るさまざまな物質のナノスケールを支配する法則としてその地位を確立しています．同じく20世紀に大きく進展した技術に情報通信分野があります．近年この一見関係が薄く思える2つの分野にまたがった新しい科学技術として，量子情報通信が注目を集めています．この量子情報通信は，量子力学からは新しい側面で原理検証を行うことでより深い理解が可能になり，情報通信からは従来の古典通信では実現ができなかった新しい機能が提供できるという点で意義があります．例えば非常に難解な問題を処理できる計算機として量子計算機が，また個人のプライバシが保護される通信技術として量子暗号や量子認証が提案されています．量子の情報を担う媒体としてはあらゆる素粒子や超伝導体のような巨視的な量子状態が利用できますが，通信の観点からは光の量子，つまり光子を利用します．もっとも基本的な量子情報通信は，たった1つの光子に情報を載せ，暗号通信のための鍵を送る量子暗号です．量子暗号は，従来の通信では困難であった盗聴の検知を確実に行うことができるのが特長です．

量子暗号小史

現在インターネットを用いてやり取りされているデジタル情報が，経路の途中で盗み見られている可能性は拭えません．そのためパスワードやクレジットカードの番号等をやり取りする場合には暗号技術が利用されています．現在実用技術として利用されている公開鍵暗号方式の安全性は，コンピュータの性能やアルゴリズムの能率に根拠を置いています．一方盗聴されても絶対に解読されることのない暗号として，ワンタイムパッド方式が広く知られています．しかしこの方式を用いるためには全くランダムで，メッセージと同じ長さの，たった一度きりしか使わない秘密鍵を，暗号通信する2者（送信者をアリス，受信者をボブと呼称します）が共有する必要があります．この問題を解決するために，必要な秘密鍵を安全に送受信者に配送する技術として量子暗号は提案されました．そのためこの技術は量子鍵配送（QKD: Quantum Key Distribution）とも呼ばれます．

まず簡単にQKDの原理を説明します．**図1**に示したように，アリスは0と1からなる全くランダムな長いビット列を準備します．アリスはこの0/1に応じて異なる量子状態にある光子を準備しボブに光ファイバ等の経路を用いて順次送ります．ボブは受け取った光子を1つずつ測定し，その結果に応じて0と1の論理値を得ます．ここまでは従来のデジタル通信と何ら異なる点がないようにみえます．仮にこの経路の途中で盗聴者が情報を盗もうとしたとします．古典通信では途中で経路をわずかに分岐させることにより情報を盗み出せます．しかし素粒子である光子はそれ以上分割できないため，やり過ごすか，取り出すかのどちらかしかできません．盗聴者が取り出したビットはボブに届かないので，途中に損失があるのと同じ結果ではありますが，ランダムな0，1列の一部が欠けてもランダム列なので鍵として使えます．ボブは後でどのビットが届かなかったかをアリスに伝えることにより2者は同じ秘密鍵を共有します．スマートな盗聴者は盗み出した光子を測定した後，送信者になりすまして光子を送る戦略を採るかもしれません．しかし測定により光子の状態が意図しない量

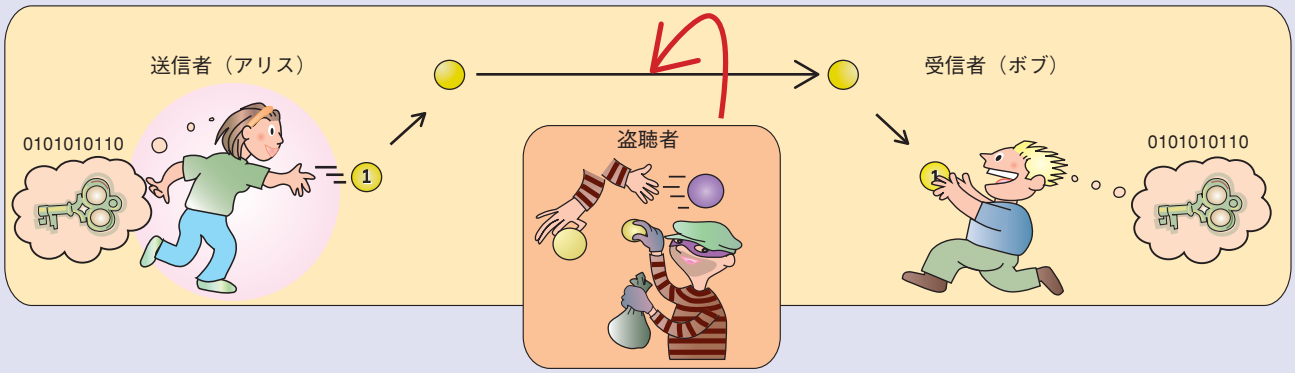


図１　量子鍵配送の原理

子状態に遷移してしまうこと（測定の反作用）があり，その結果に基づいたなりすましは必然的にエラーを引き起こします．盗聴者は測定前に光子を複製してそのコピーのみを測定することもできません．なぜなら未知の量子状態は複製できないという非クローニング定理があるからです．このように盗聴者はビットエラーを発生させずには鍵の情報を得ることができません．逆にアリスとボブはビットエラーから盗聴者の有無を判定できます．

1984年に提案された最初のQKDプロトコルは，提案者C. H. BennettとG. Brassardの頭文字を取りBB84プロトコルと呼ばれ，単一光子の２つの偏光基底，例えば円偏光（右・左回り）と直線偏光（水平・垂直）をランダムに選択し，各基底で論理値０，１を割り当てて送ります．ボブも測定基底をランダムに選んで各光子を測定しますが，アリスが選んだ基底と一致したときは必ず正しい答えを得ます．したがって，アリスとボブは後で自分が選んだ基底を開示し，それが一致したときだけその結果をシフト（ふるい）鍵とします．盗聴者を検知するためにアリスとボブは一定の割合で得られた鍵の値を比較して，エラー率を評価します．得られた量子ビットエラー率が一定値以下であれば盗聴者からの攻撃はないと判断できます．さらに後処理としてシフト鍵に対しエラー訂正とそれまでの過程で盗聴者に漏れた可能性のある情報をなくす操作（プライバシ増幅）を行い，最終的に暗号通信に用いる安全鍵を生成します．

後述するように一度に単一光子を放出する理想的な単一光子光源の場合には，盗聴者が伝送路において量子力学の許すあらゆる手段を駆使しても秘密鍵を安全に配送できることが証明されています（無条件安全性）．また最近では単一光子光源でなく，コヒーレント（レーザ）光源を極端に減衰させたものを用いても安全であることが示されています．またBB84のほかにもさまざまな量子暗号プロトコルが提案され，その安全性が検討されています．本特集では量子暗号の安全性に関して詳しく解説しています．

伝送路としては光ファイバがよく利用されます．最初BB84は光子の偏光状態を基底として利用するように提案されましたが，光ファイバで伝送する際には偏光状態を保持することは困難です．そこでその代わりに**図２**に示すように二連パルスを準備し，その第１パルスに光子がいるか，第２パルスにいるかの基底（時間位置基底），あるいは２つのパルスに広がった状態でそのパルス間の位相差が０か，πかの基底（位相基底）を利用します．あるいは，位相差が$\{0, \pi\}$と$\{\pi/2, 3\pi/2\}$の２基底が利用されることもあります．

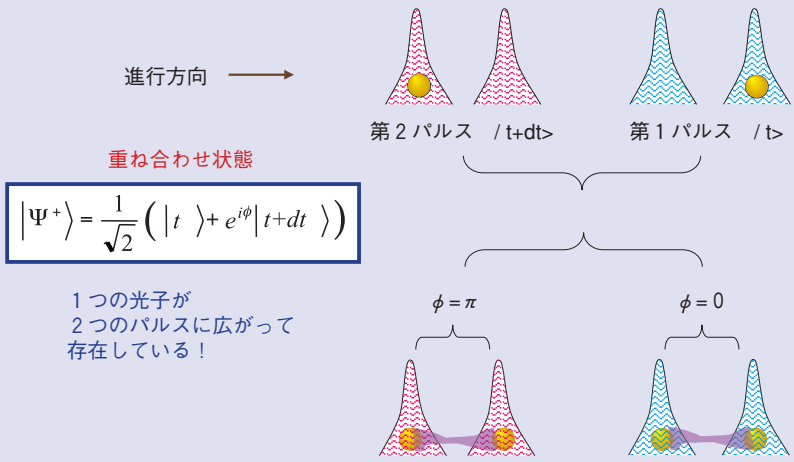


図２　時間位置基底と位相基底

実際のシステムでは単一光子検出器の感度，暗計数（光子が来なくても検出してしまうレート）や伝送路の損失によって安全鍵の生成率と伝送可能な距離の上限が制限されます．ではどれくらいまで遠くに安全に秘密鍵を配送できるでしょうか[(1)]？　実用的な光の伝送路として利用されている光ファイバの場合，もっとも損失が小さい波長である1.5 μm帯の光子を用いる必要がありますが，この遠赤外の単一光子の持つエネルギーは小さく，それを検出できる良い単一光子検出器がないことが技術的な課題でした．ここ数年で安全鍵の生成率と伝送距離が急激に伸びており，50 km 以下であれば毎秒 1 Mbit/s[(2)]，また鍵生成率は小さいですが200 km程度まで[(3), (4)]は送ることが可能となっていますが，これは主に単一光子検出器の性能の向上によります．この距離を今後飛躍的に延ばすのは困難ではありますが，この課題を解決するために３つの方法が考えられています．

１つは信頼できる中継地点を50～100 kmごとに準備し，中継地点で一度得られた秘密鍵を交換することにより長距離２地点間で秘密鍵を共有するというもので，欧州では2008年にSECOQCプロジェクト[(5)]で，2010年にはNTTも参加した東京QKDネットワークと呼ばれるテストベッドネットワーク[(6)]で実証実験が行われました．２番目は地上基地と衛星間で空間レーザ光を利用した量子通信で鍵を生成し，後に別の遠隔地の地上基地と衛星で鍵を交換するというものです．実際EUと日本で実験の準備が進められています[(7)]．

最後はまだ将来の技術ですが，途中で古典的なビットに変換することなしに，量子状態そのものを中継して遠隔地に送る量子中継技術があります．これは量子鍵配送に限らず，量子情報通信の中核となる技術と位置付けられ，現在世界的に活発に研究が始められています．

NTTの研究の位置付け

NTT研究所は量子通信技術の基礎分野である量子光学の研究で長い歴史を持っています．量子暗号に関してまず主に理論的側面の研究を進め，2000年ごろから実験的研究にも着手しました．スタンフォード大学の山本喜久教授のグループとの共同研究を通じて，量子ドットを用いた単一光子光源（波長は0.8 μm）を利用したBB84QKD実験を行いました[(8)]．**図３**左の走査型電子顕微鏡写真に示すピラー型の構造の中程に埋め込まれた量子ドットから一度に１つずつ出てくる光子に２基底×２論理値＝４値の偏光状態を設定してボブに送ります．ボブは偏光ビームスプリッタと４つの単一光子検出器を用いてランダムに基底を選んで測定します．

2003年には新しいQKDプロトコルであるDPS（Differential Phase Shift：差動位相シフト）-QKDをスタンフォード大学と共同で提案しました．これは，光通信で使用されているデジタル変調方式の１つであるDPSK（Differential Phase Shift Keying）[*1]

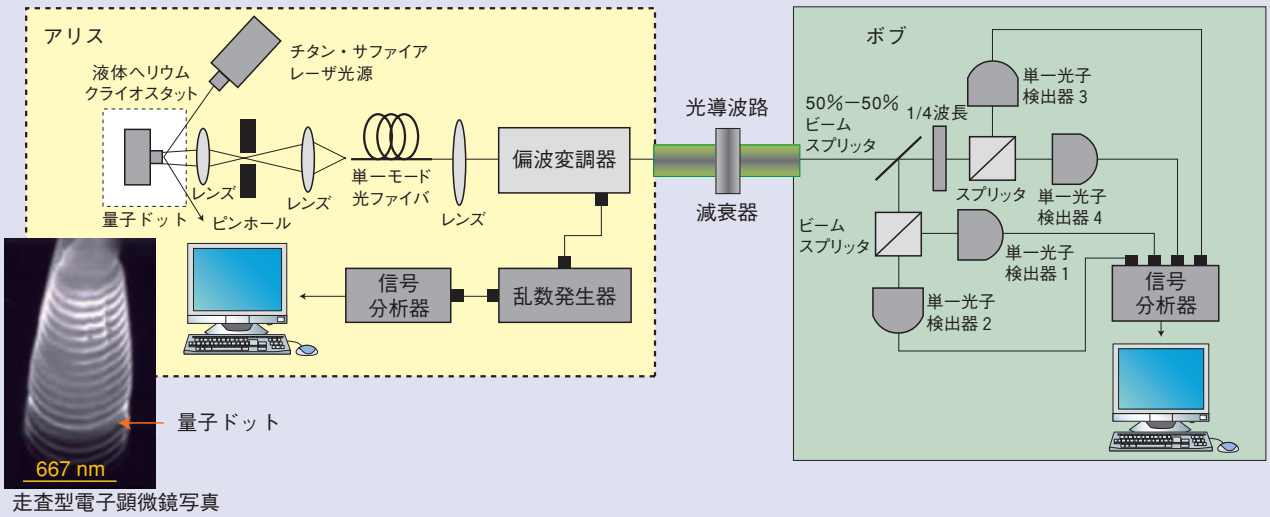


図 3　単一光子光源を用いたBB84QKD実験系

を量子力学の領域に適用したもので，図 2 の下に示したように単一光子が多数のパルスにわたり広がった状態を利用します．それまで提案されたQKDプロトコルが単一光子自体の量子状態を利用するため単一光子光源を想定していたのに比べ，DPS-QKDでは最初から微弱コヒーレント光源が利用でき，また光子数を数えて一部の情報を盗み取る光子分離攻撃に耐性があるという特長を持っています．さらに，BB84では基底が一致しなかった測定結果は棄却するのに比べ，DPS-QKDでは到達した光子の情報はすべて利用できること，またシステムが簡単で高速化に適用可能である等の特長を持っています．関連するプロトコルとしてCoherent One-Way（COW）方式が知られています[4]．NTT物性科学基礎研究所ではこのDPS-QKD方式を採用して繰り返しレート 1 GHz から10 GHzのシステム実験を報告しています[3]．本特集では，このDPS-QKD方式のシステム実験に関して解説します．

また，NTTでは高機能単一光子検出器の開発も進めています．通信波長帯の単一光子の検出のために従来用いられてきたInGaAs（インジウムガリウム ヒ 素 ）-APD（ Avalanche Photo Diode）*2は量子効率が低い，暗計数率が高い，また光子を検出した後に残留電荷によるノイズ信号（After pulse）が観測されるため，低繰り返し周波数のゲートモードでの動作が必要になる，などの問題がありました．これに対してSi（シリコン）-APDは高効率，低暗計数，ゲート動作が必要でない等の特長を持ちますが，通信波長帯の光子には感度が低いため，光子の周波数をPPLN非線形結晶*3とポンプ光を用いて高く（波長を短く）し，Si-APDで検出する周波数上方変換型単一光子検出システムの有効性を実証しました．本特集でこの技術を解説しています．さらに，Si-APDよりも高速に動作するHPD（Hybrid single Photon Detector）を用いて，高い鍵生成率のQKD実験を行っています[9]．最近では，InGaAs-APDの光子信号解析回路を工夫することにより，1 GHzを超える高繰り返し動作も実現

＊1　DPSK：差動位相偏位変調．位相のずれた複数の波の組み合わせで情報を表現するデジタル変調方式PSKの 1 つ．
＊2　APD：高速光通信用の光信号検出器．
＊3　PPLN非線形結晶：周期分極反転ニオブ酸リチウム結晶の略称で，大きな光非線形性を持つため高い効率で波長変換などを行うことができます．

しています．一方非常に低い暗計数と高速動作により注目されているのは超伝導を用いた単一光子検出器（SSPD: Superconducting Single Photon Detector）です．このデバイスは最近特にその性能の向上が著しいです．本特集でもSSPDの最近の開発状況について解説します．

ここまでは単一光子もしくは微弱コヒーレント光を用いたQKDについて述べてきましたが，量子力学では複数の量子の間に量子もつれ状態と呼ばれる不思議な状態が実現できることが知られています．2つの光子によるもつれ光子対の生成技術は近年成熟しつつあり，特に通信波長帯のもつれ光子対生成ではNTTは先導的な成果を上げてきています．本特集ではこの通信波長帯量子もつれ光子対の生成とそれを用いたQKD実験に関しても解説します．今後は量子中継などを実現することにより，遠隔地の量子計算機や量子標準システムを結び，高度に発達した量子ネットワーキングの実現を目指し研究開発を進めていきます．

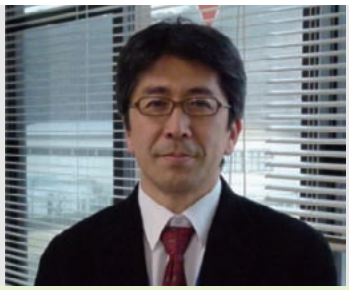
まとめ

近年の高度情報化社会でますますプライバシ保護の重要性が認識されてきている中，量子暗号の無条件安全は非常に魅力的にみえます．しかしシステム全体の安全は，それぞれの要素の持つ安全性の総和ではなく，かけ算で与えられます．例えば量子鍵配送で送った秘密鍵の取り扱いがずさんであれば，全体の安全性はゼロとなります．その意味で量子暗号の研究開発は究極の安全性に対するチャレンジと位置付けられると思います．また，これまではハード技術指向のシーズ的な研究開発が進められてきましたが，今後はこれをどう使うかという適用システム，ソフトウェアの比重が高くなると考えられます．量子暗号は実用的な面や量子力学の適用分野としてのサイエンス上の興味も尽きない魅力的なテーマです．

なお，本研究の一部はNICT，JST-CRESTの支援を受けて行われました．

■参考文献

(1) 石井：“実験室の外に飛び出した「絶対安全」な暗号，”日経コンピュータ2006年3月6日号，No.647，pp.196-201，2006.
(2) A. R. Dixon，Z. L. Yuan，J. F. Dynes，A. W. Sharp，and A. J. Shields: “Continuous operation of high bit rate quantum key distribution，”Appl. Phys. Lett., Vol.96, No.16, pp.161102- 161102-3，2010.
(3) H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto: “Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors,” Nature Photonics 1, pp.343-348, 2007.
(4) D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Grey, C. R. Towery, and S. Ten: “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,” New J. Phys., Vol.11, 2009.
(5) M. Peev, C. Pacher, R. Alleaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legre, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger: “The SECOQC quantum key distribution network in Vienna,” New J. Phys., Vol.11, 2009.
(6) http://arxiv.org/abs/1103.3566
(7) http://www.quantum.at/quest
(8) E.Waks, K.Inoue, C.Santori, D.Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto: “Secure communication: Quantum cryptography with a photon turnstile,” Nature, Vol. 420, No.6917, p.762, 2002.
(9) Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, and Y. Yamamoto: “Megabits secure key rate quantum key distribution,” New J. Phys., Vol. 11, 2009.



都倉 康弘

量子情報処理は高速な情報処理，低エネルギー，新機能などの特長があります．この新しい分野は，数学，情報科学，化学，物理，材料科学などの分野をまたいだ学際的な視点が欠かせません．相対性理論がグローバル・ポジショニング・システム（GPS）の基礎として普通に使われているように，いつか量子情報が日常に使われる日が来るかもしれません．

◆問い合わせ先
NTT物性科学基礎研究所
量子光物性研究部
TEL 046-240-3340
FAX 046-270-2360
E-mail tokura.yasuhiro@lab.ntt.co.jp