単一光子による量子暗号鍵配付システム

富　田　章　久

Single Photon Quantum Key Distribution System

Akihisa TOMITA

A structure and components of single-photon quantum key distribution (QKD) system are described. Recent reports have demonstrated QKD transmission over 100 km at GHz clock frequencies. Progress in security studies shows that secure key can be generated under practical conditions. Availability of QKD systems can be improved by being combined with photonic networks as a quantum network composed of optical switching and key relays. The quantum network will improve security of the photonic network.

Key words: quantum, cryptography, key distribution, secure network

インターネットをはじめとする情報通信技術の普及によってますます多くの情報が電子的に伝送されるようになっている．この中には，外交・防衛など国家の安全にかかわる情報や巨額の資金がかかわる経済活動の情報など重要度の高いものが含まれる．これらの情報を守るため，安全性が証明可能で将来も陳腐化しない暗号法の実現が望まれる．本稿では，情報理論的安全な（無条件安全＝解読時間に関する条件がない＝無限に時間をかけても解読できない）鍵配付を可能にする量子暗号鍵配付を考える．鍵配付は離れた二者間（暗号の世界では Alice と Bob のカップルが登場する）で秘匿通信を行うための乱数（鍵）を安全に共有する技術である．無条件というと常に安全性が成立するようにみえるが，実際にはさまざまな仮定を用いる（無条件でも無仮定ではない！）．盗聴者（Eve）の記憶容量が有限であるとか，伝送路を制御できないといった強い仮定をすると，古典的な通信だけでも情報理論的に安全な鍵配付ができる[1,2]．このような仮定は技術の進歩によって成り立たなくなる可能性があるので情報理論的安全が証明された鍵配付プロトコルがいつまでも安全であるということは一般的には正しくない．これに対し，QKD（quantum key distribution；量子鍵配付）では盗聴者の能力に関する一般的な仮定のもとで盗聴者が得る暗号鍵についての情報量の上限が計算できる[3]．このため QKD では，個々の盗聴法に対してではなく，現実的な設定のもとで可能なすべての盗聴法に対しての安全性が保証可能である．さらに，暗号鍵についての情報量の上限は，非直交な量子状態の測定に関する物理法則に基づいているため，技術の進歩があっても安全性は変わらない．また，QKD で作られた暗号鍵を構成要素とする暗号システム全体を考えても，暗号鍵の安全性に影響を与えない性質（composability）をもつことも証明されている．このような意味で，QKD の安全性は他の方法とは質的に異なっているといえる．

いかに安全性が高くとも実現できなければ意味がないが，単一光子の QKD は1光子が干渉性を保ったまま伝送できればよく，光通信技術を応用することで比較的容易に QKD 装置を作ることができる．安全性への期待と実現可能性から研究開発が進展し，最近では原理実証の段階を過ぎて実用化を意識した研究が進められている．すでに欧米では量子暗号鍵配付装置を市販するベンチャー企業が現れ[*1]，日本においても長時間安定に鍵生成を行う装置の試作が報告されている[4]．本稿では，理論的な解析と実験が最も進んでいる BB84 プロトコル[5]を中心に単一光子を用

(独)科学技術振興機構 ERATO-SORST 量子情報システムアーキテクチャ；日本電気(株)ナノエレクトロニクス研究所（〒305–8501 つくば市御幸が丘 34）　E-mail: tomita@qci.jst.go.jp

[*1] http://www.idquantique.com, http://www.magiq.com

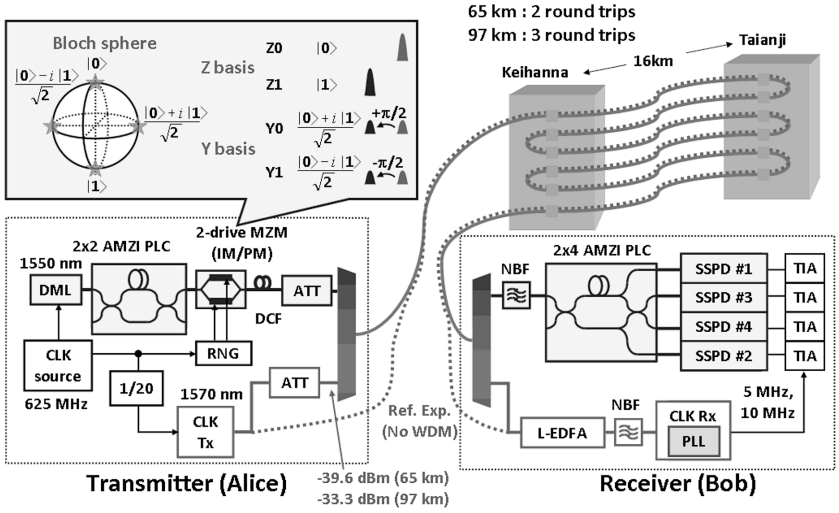

図1　単一光子量子暗号システムの構成.

いたQKDシステムを解説する．システムの構成，実験的な進展，量子暗号ネットワークなどに関する最近の成果を報告する．

1.　単一光子量子暗号鍵配付システムの構成

量子暗号で暗号鍵を共有する過程は，物理的なプロセスである量子通信と論理的なプロセスである鍵蒸留の2つに分けられる．量子通信によって鍵のもとになる乱数が送られ，シフト鍵とよばれる乱数列がAlice，Bobで生成される．伝送に伴う擾乱によってAliceのシフト鍵とBobのシフト鍵は完全には一致しない．鍵蒸留によって，シフト鍵から，安全性が保証された（Eveのもつ情報量の最大値が規定された）暗号鍵（最終鍵）を抽出する．鍵蒸留は，状態の乱れを訂正する過程（誤り訂正）とEveが送られた量子状態についてもちうる情報を消去する過程（秘匿性増強）からなる．鍵蒸留の過程は量子計算の一種なのだが，等価な処理が古典的に行えることが示されている[3]．秘匿性増強はkビットの乱数についてEveがもつ情報量がtビット以下であるとき，安全パラメーターをsとして，kビットの乱数からランダムに$t+s$ビットを捨てることにより，残った乱数（最終鍵）の1ビットについてEveがもつ平均相互情報量が$2^s/\ln 2$以下にできるということに基づいている[6]．任意の量子状態から情報を得たとき，得られた情報量の上限は状態に与える擾乱の大きさで決まる．盗聴がないときでも雑音や装置の不完全性のため誤りが生じるが，QKDでは安全サイドに考えてすべての誤りが盗聴に起因するとみなす．このため，QKDを行うためにはできるだけ量子通信装置の誤り率を小さくする必要がある．

量子通信を行う装置構成の一例を図1に示す．量子通信装置は光源とエンコーダーからなる送信器，通信路，デコーダーと光子検出器からなる受信器で構成される．このほかにビット同期とフレーム同期の機構が必要である．ビット同期は送受信されるパルスのタイミングを合わせるものであり，フレーム同期は受信したパルスを送信パルスに対応づけるものである．光子通信では通信路の損失のために送信したパルスのごく一部しか検出されないため，同期をとるためには特別な工夫が必要になる[4]．

光源は，もともとのBB84プロトコルの安全性証明では単一光子を放出することが仮定されていた．実際のQKD装置では，パルス動作する半導体レーザー光を0.1〜0.6光子/パルス程度まで減衰させたもの（弱コヒーレント光）を近似的な単一光子光源として用いるのが一般的である．減衰させたレーザー光であっても光子数はポアソン分布するため，2光子が同時に放出される可能性がある．これを利用した盗聴法（光子数分岐攻撃）が提案され，安全な鍵配付可能な距離が著しく制限されることが指摘された[7]．これに対し，デコイ法が提案され，弱コヒーレント光でも単一光子とほとんど同程度の距離を伝送できることが示された[8–11]．デコイ法を前提とすれば半導体レーザーを光源とすることができる．

光子検出器に必要な性能は高い検出効率と低いダークカウントをもち，アフターパルスの影響が小さく，さらに検出タイミングのジッターが小さいことである．このうち，アフターパルスは，光子検出後光子が来ていないにもかかわらず誤検出する現象である．アフターパルスの影響が大きいと検出後一定時間（数μs）光子検出をとめる必要があり，光子検出レートが低下する．光ファイバー通信に用いる1.55 μm帯では光通信用のInGaAs APDが用いられる

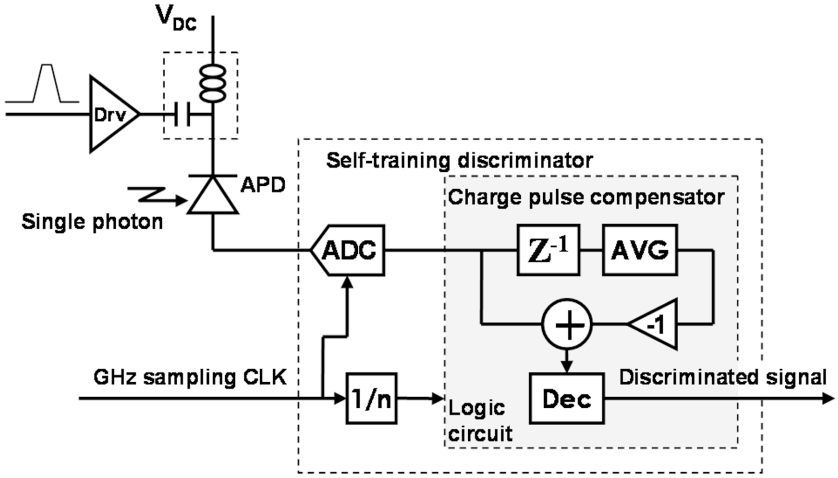

図2　A/D コンバーター（ADC）とディジタル信号処理によるセルフトレーニング型識別回路.

が，バンドギャップが小さいためにダークカウントが多く，−100 〜−40℃ に冷却してもゲートモードで用いる必要がある[12]．ゲートモードでは，直流バイアス電圧にゲートパルスを重畳して光子が到達する時間帯でのみ高い増倍利得で光子検出を行う．これによって高検出効率と低ダークカウントを両立させるものである．ところが，ゲートパルスの APD での充放電に伴うパルス波形が出力に現れるため，光子検出にはこのチャージパルスを消去することが必要である．最近，ゲート信号を正弦波にしてフィルターで不要な信号を落とす方法と 1 ビット遅延後の波形を差し引く方法が提案され，それぞれ 1 GHz を超えるクロック周波数での動作が報告されている[13,14]．われわれは，APD 素子の個体差や実装のばらつきに対する高精度な調整の問題を解決するために，図 2 に示す A/D コンバーター（ADC）とディジタル信号処理によるセルフトレーニング型識別回路を提案した[15]．

光子検出器を QKD 装置に組み込むためには，冷却性能とゲートモードに対応した高周波性能を両立させた小型 InGaAs-APD モジュールが必要である．APD のボンディングワイヤーは熱流路となるが，高周波特性はワイヤーの接続数に依存するため，断熱性と広帯域性の要求は相反する．APD モジュールを，熱シミュレーションと高周波シミュレーションにより最適設計した．図 3 に示すモジュール本体のサイズは 23.3×21.7×15.0 mm^3 である．試作したモジュールは−73℃（200K）の冷却能力，1.02〜1.05 A/W の受光感度，測定限界以下のクロストーク特性，3 GHz のゲート帯域を示した[15]．この小型 APD モジュールとセルフトレーニング型識別回路を組み合わせ光子検出特性を評価し，ダークカウント確率 2×10^{-4} において光子検出効率 $\eta=30\%$ を得た[16]．

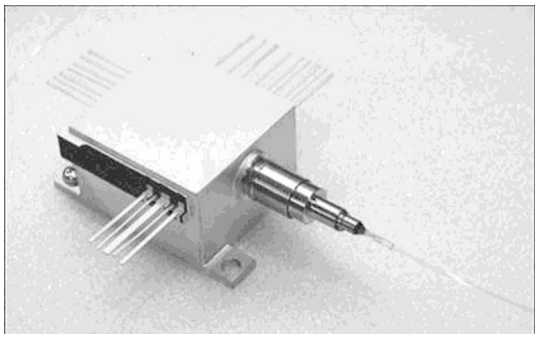

図3　試作した小型 APD モジュールの外観.

さらにクロック周波数を上げるため，超伝導光子検出器（SSPD）も検討されている．SSPD にはアフターパルスがほとんどなく，ダークカウントも小さいため，高速性・低雑音性にすぐれている[17]．

BB84 プロトコルを実装するためには，4 通りの量子状態 $Q_+=\{|0\rangle, |1\rangle\}$; $Q_\times=\{|+\rangle, |-\rangle\}$ が必要である．ただし，$|\pm\rangle=(\{|0\rangle\pm|1\rangle\})/\sqrt{2}$．$Q_+$，$Q_\times$ をそれぞれ＋（プラス）基底，×（クロス）基底という．光子の直交状態 $|0\rangle$ $|1\rangle$ としては，水平偏光と垂直偏光（偏光コーディング）や時間的に分割された光子振幅（時間–位相コーディング）がよく選ばれる．偏光コーディングはおもに空間伝送で用いられ，時間–位相コーディングはファイバー伝送で用いられる．時間–位相コーディングではエンコードとデコードに，光路差がある非対称な干渉計が必要で，誤りのない量子通信を行うためには送信器と受信器の干渉計の光路差を等しく保たなければならない．このため，われわれは平面光回路（PLC: planar lightwave circuit）技術を用いた非対称マッハ・ツェンダー（MZ）干渉計を採用した[18]．PLC 技術により精度よく同一の光回路を量産することが可能で，温度調

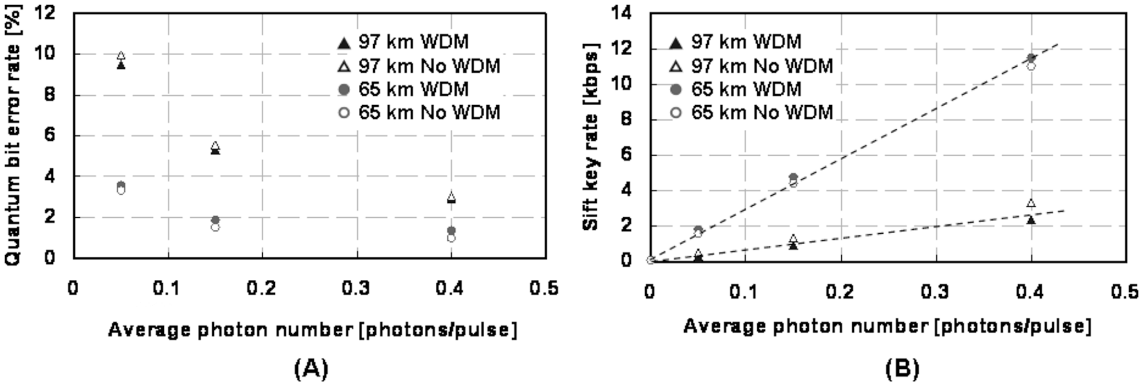

図4　QKD システムの伝送特性．(A) 誤り率，(B) シフト鍵レート．

節のみにより数時間にわたって干渉計の安定な動作が実現可能である．

時間–位相コーディングは，同強度で 90° ずつ位相の異なる 4 状態による四値位相（*XY*）コーディングと，*Y* 基底に対応する強度 1/2，位相差 90° の 2 状態と *Z* 基底に対応する強度 0, 1 の 2 状態二値位相＋時間（*YZ*）コーディングが考えられる．後者は 2×4 PLC を用いることで受信側に変調器が不要となるため，損失の減少分だけ伝送速度が向上する．上記両方式に対応できる汎用性の高い量子暗号送信器は，2×2 干渉計と二電極 MZ 変調器を使用することで実現できる[19]．二電極 MZ 変調器は，各アームに印加する電圧によってそれぞれの経路で与えられる位相を独立に制御できる．二電極 MZ 変調器の入出力関係は，MZ 各経路における位相シフト ϕ_1 および ϕ_2 を用いて次式で表すことができる．

$$E_{\mathrm{out}} = E_{\mathrm{in}} \cos\left[\frac{\phi_1 - \phi_2}{2}\right] \exp\left[\mathrm{i}\frac{\phi_1 + \phi_2}{2}\right] \qquad (1)$$

XY コーディングでは，MZ 変調器の片経路を 0° と 180° の変調位相で，他方を 90° と 270° の変調位相で駆動することで強度項である $\cos[(\phi_1 - \phi_2)/2]$ は常に一定となり，位相項である $\exp[\mathrm{i}(\phi_1 + \phi_2)/2]$ に従って 4 状態を準備できる．また，*YZ* コーディングでは MZ 変調器の片経路を 90°，他方を 0° と 180° の変調位相で駆動することで強度 1/2, 位相差 90° の 2 状態が，片経路を 0°，他方を 0° と 180° で駆動することで強度 0，1 の 2 状態が得られる．

2.　単一光子量子暗号鍵配付システムの性能

図 1 の QKD 装置を用いて行った QKD 信号の伝送実験の結果[20] を紹介する．ここでは，クロック周波数を 625 MHz とし，光子検出器として高速特性にすぐれた超伝導光子検出器（SSPD）を用いた．同期に必要な信号は，波長分割多重（WDM）技術を用いて量子信号と同じファイバー芯線で伝送した．信号の分離のため狭帯域フィルターを用い，受信側で光アンプで同期信号を増幅することでファイバー中の同期信号強度を最小限に抑えた．敷設済みのファイバー 65 km と 97 km 伝送後における鍵生成の結果を図 4 に示す．強度差が 60 dB 以上あるにもかかわらず，同期信号を WDM 伝送したことによる誤り率の増加はみられなかった．同期信号を同一のファイバー芯線で送ることにより，6 時間以上にわたって安定な QKD 伝送が行えた．平均光子数 0.4 で, 97 km ファイバー伝送後にシフト鍵生成レート 2.4 kbps，誤り率 2.8% を得た．デコイ法を用いて安全性が保証できる鍵のレートは 0.78〜0.82 kbps と見積もられる．

QKD の伝送距離としては，現在のところファイバー長 202 km の伝送が報告されている[21]．平均光子数で補正した実効的なファイバー長は，148.7 km（平均光子数 0.1），184.6 km（平均光子数 0.5）である．この実験では，低雑音高効率の超伝導ボロメーター（TES）を光子検出器として用いている．一方，自由空間伝送では，ヨーロッパのグループによって，カナリア諸島内のパルマ島標高 2400 m 地点とテネリフェ島標高 2400 m にある optical ground station（OGS）間 144 km を隔てて光子を伝送する実験が行われた．デコイ法を用いた単一光子 QKD 伝送およびエンタングルした光子の伝送に成功している[22,23]．波長は 710 nm が用いられた．最近，COW プロトコルによる 250 km 伝送が報告された[24]．

QKD 装置の動作速度はクロック周波数で表せるが，BB84 プロトコルを実装した装置でも光子検出レートが大きくない場合には InGaAs-APD によっても GHz クロックでの動作が報告されている[25]．DPS（差動位相シフト）-QKD を用いてさらに高速の QKD 伝送実験が行われている[26,27]．DPS-QKD や COW-QKD は現在のところ一般的な盗聴のサブセットに対する安全性しか証明されていないが，BB84 プロトコルより装置構成が簡単になり，DPS-

QKD では同クロック周波数で 4 倍シフト鍵生成レートを高めることができる．

QKD の伝送距離は伝送路の損失で決まり，光ファイバーでは 200 km 程度が限界となる．これより長い距離については，鍵リレー方式，衛星中継，量子中継のどれかが必要になる．技術的な難易度はこの順番で高くなる．鍵の生成レートはクロック周波数を上げることで高くすることができるが，伝送距離が大きくなると，光子が到達する割合が小さくなるため減少する．SSPD などの高速な光子検出器を用いると，10 GHz クロックも可能だが，量子通信の場合，時間同期の安定性や信号処理の速度などエレクトロニクスが追いつかなくなる．現状では，1〜2 GHz 程度以下が実用的であると考えられる．鍵の生成率は最終的に得られる安全鍵についてみるのが正しいが，プロトコルや保証する安全性の基準によっても異なる．たとえ検出される鍵のレートが高くても，盗聴者に漏洩する可能性のある情報量が大きい場合には多くの鍵を秘匿性増強で捨てなければならないので，最終鍵が少なくなる．逆に，安全性の基準を甘くすれば最終鍵の生成率を高くすることができるが，その場合にはどのような安全性基準を採用しているかを明記するべきだろう．将来的には，鍵の安全性表示の正しさを保証する機関が必要となろう．

3. 量子暗号鍵ネットワーク

QKD システムの伝送距離の増大や多対多の暗号鍵共有を実現するには，量子暗号のネットワーク化が必要である．効率的で安定なネットワークを実現するには，単に装置を多数つなぐだけではないネットワーク特有の問題がある．既存のネットワークとのインターフェースを含むネットワークトポロジーの設計が必要である．特に QKD は通信路での擾乱に敏感であるため，DoS（denial of service）攻撃を受けやすい．このため，ネットワーク管理―伝送パフォーマンスの監視と問題が生じたときの経路切り換え機能―が重要な役割をする．経路の切り換えは光スイッチで行えるが，QKD 伝送の場合，別に送られる同期信号によって同期の設定が必要になる．光スイッチによって鍵共有の相手をシームレスに切り換えることにより，暗号通信による鍵の消費量に合わせてダイナミックに鍵の生成量を調整することも可能になる．

鍵リレーを用いると，直接接続されていないノード間で鍵の共有ができる．ここで，QKD で生成される鍵（量子鍵）と暗号通信に用いる鍵（論理鍵）を区別する．QKD のリンクと論理鍵のリンクのトポロジーを独立に設計することができる．鍵リレーではリレーノードとターミナルノードの 2 種類のノードを考える．ノード N_1 と N_2 は量子鍵 K-Q12 $\equiv K_1$ を共有し，ノード N_2 と N_3 は量子鍵 K-Q23 $\equiv K_2$ を共有しているとき，直接接続されていないノード N_1 と N_3 の間で論理鍵を共有したい．この例ではノード N_1 と N_3 はターミナルノードであり，ノード N_2 はリレーノードになる．量子鍵 K_2 を論理鍵として共有するために，リレーノード N_2 は K_2 を鍵 K_1 で $K_1 \oplus K_2$ のようにビットごとに排他的論理和をとることで暗号化したのち，通常の通信路を通じてノード N_1 に送る．ノード N_1 は自身のもっている鍵 K_1 を使って $K_2 = K_1 \oplus K_2 \oplus K_1$ によって K_2 を再生でき，ノード N_1 と N_3 は論理鍵 K-L13 $\equiv K_2$ を共有することができる．これは論理鍵 K-L13 を K_2 で暗号化したワンタイムパッド通信にほかならないので，鍵の情報が漏洩することはない．もちろん，リレーノードはすべての鍵（古典情報）を知っているので外部に情報が漏れないような対策が必要である．しかし，ネットワークに参加しているノードが信頼できるということは，比較的無理のない仮定であるように思われる．秘密分散を使うことでいくつかのノードが信頼できない場合の論理鍵の共有も可能であると考えられるが，これは今後の課題である．

量子ネットワークでは，鍵管理が重要である．量子鍵の一部が論理鍵となり，残りの一部は鍵リレーで暗号化のために使われる．量子鍵は鍵リレーで使われるまでバッファーに保存され，使われたのち直ちにバッファーから消去される．量子鍵と論理鍵の量はデータ通信からの要求によって変化するので，鍵管理エージェントをおいて各ノードでの鍵の残量をモニターし，ノードで保持する鍵の残量が一定になるように量子鍵の生成を制御する．鍵リレーを使うことにより装置間の仕様の違いを吸収することができ，上のような鍵の細かい管理も可能であるので，現実的な解として，近い将来の量子鍵ネットワークには必須の要素になるものと思われる．

QKD プレーンが光通信ネットワークに統合されたアーキテクチャーの一例を図 5 (a) に示す．図 5 (b) には，鍵生成（key generation），相互接続（connection），鍵管理（key management）の層からなる QKD プレーンの構成を示す．このようなネットワークのプロトタイプが EU のプロジェクト SECOQC[*2] で開発され，2008 年に公開された．日本でも，より高速な QKD 装置を，より高度な鍵管理機能をもつ QKD プレーンで統合したネットワーク実

[*2] http://www.secoqc.net/

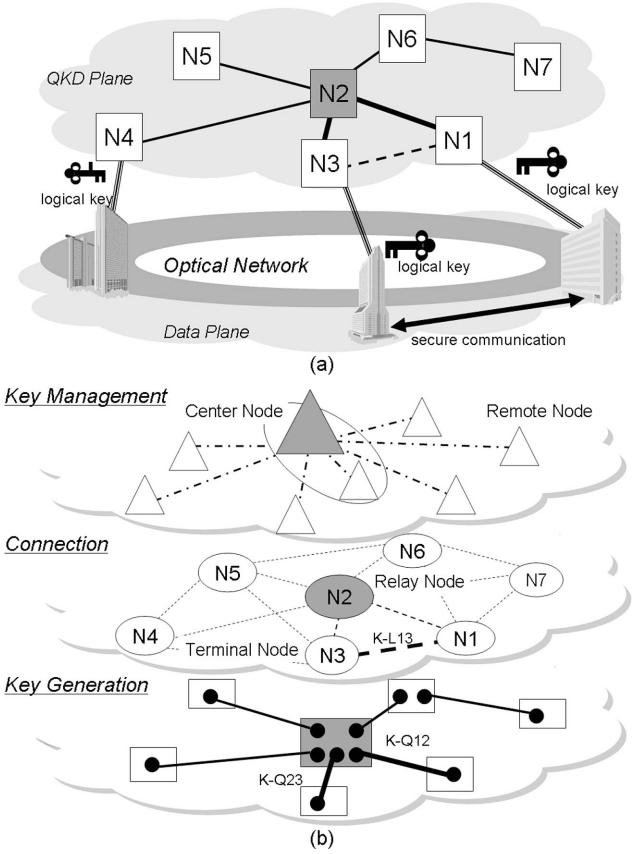

図5 (a) 光通信と量子暗号が統合されたネットワークアーキテクチャー，(b) QKD プレーンの層モデル．

験を（独)情報通信研究機構の委託研究に参加しているNEC，三菱電機，NTT の 3 社を中心に行う予定である．

単一光子を用いた QKD システムの構成と現在の実験の進展について述べた．QKD システムは，すでに原理実証を過ぎて実用化に向けた技術課題を整理し，解決していく段階にある．QKD システムの利便性を高めるため，光通信ネットワークと統合した量子ネットワークについても概説した．今後，量子ネットワークの実現に向けた研究開発が盛んになっていくものと考えられる．

本稿で紹介した研究成果は NEC ナノエレクトロニクス研究所 南部芳弘・吉野健一郎，システムプラットホーム研究所 田島章雄・田中聡寛・前田和佳子・高橋成五，JST ERATO-SORST 量子情報システムアーキテクチャ 林正人（現東北大）・廣嶋透也・長谷川淳（現東大）の各氏との共同研究によるものである．研究の一部は，（独)情報通信研究機構（NiCT）の委託研究「量子暗号技術の研究開発」の成果である．

文　献

1) U. M. Maurer: “Conditionally-perfect secrecy and a provably-secure randomized cipher,” J. Cryptol., **5** (1992) 53–66.
2) U. M. Maurer: “Secret key agreement by public discussion from common information,” IEEE Trans. Inf. Theory, **IT-39** (1993) 733–742.
3) P. W. Shor and J. Preskill: “Simple proof of security of the BB84 protocol,” Phys. Rev. Lett., **85** (2000) 441–444.
4) A. Tajima, A. Tanaka, W. Maeda, S. Takahashi and A. Tomita: “Practical quantum cryptosystem for metro area applications,” IEEE J. Sel. Top. Quantum Electron., **13** (2007) 1031–1038.
5) C. H. Bennett and G. Brassard: “Quantum cryptography: Public key distribution and coin tossing,” *Proc. IEEE International Conf. on Computers, Systems and Signal Processing* (Bangalore, India, 1984) pp. 175–179.
6) C. H. Bennett, G. Brassard, C. Crepeau and U. Maurer: “Generalized privacy amplification,” IEEE Trans. Inf. Theory, **IT-41** (1995) 1915–1923.
7) G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders: “Limitations on practical quantum cryptography,” Phys. Rev. Lett., **85** (2000) 1330–1333.
8) D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill: “Security of quantum key distribution with imperfect devices,” Quant. Inf. Comput., **5** (2004) 325–360.
9) W.-Y. Hwang: “Quantum key distribution with high loss: Toward global secure communication,” Phys. Rev. Lett., **91** (2003) 057901.
10) X.-B. Wang: “Beating the PNS attack in practical quantum cryptography,” Phys. Rev. Lett., **94** (2005) 230503.
11) H.-K. Lo, X.-F. Ma and K. Chen: “Decoy state quantum key distribution,” Phys. Rev. Lett., **94** (2005) 230504.
12) A. Tomita and K. Nakamura: “Balanced, gated-mode photon detector for quantum-bit discrimination at 1550 nm,” Opt. Lett., **27** (2002) 1827–1829.
13) N. Namekata, S. Adachi and S. Inoue: “1.5 GHz single-photon detection at telecommunication wavelengths using sinusoidally gated InGaAs/InP avalanche photodiode,” Opt. Express, **17** (2009) 6275–6282.
14) Z. L. Yuan, B. E. Kardynal, A. W. Sharpe and A. J. Shields: “High speed single photon detection in the near infrared,” Appl. Phys. Lett., **91** (2007) 041114.
15) S. Takahashi, A. Tajima and A. Tomita: “High-efficiency single photon detector combined with an ultra-small APD module and a self-training discriminator for high-speed quantum cryptosystems,” *The 13th Microoptics Conference*, PD-1 (Takamatsu, Japan, 2007) pp. 2–3.
16) 高橋成五，江口明大，浜本貴一，田島章雄，富田章久 : 第 55 回応用物理学会学術講演会 (2008) 27pZE-8.
17) S. Miki, M. Fujiwara, M. Sasaki and Z. Wang: “NbN superconducting single-photon detectors prepared on single-crystal MgO substrates,” IEEE Trans. Appl. Supercond., **17** (2007) 285.
18) Y. Nambu, K. Yoshino and A. Tomita: “Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit,” J. Mod. Opt., **55** (2008) 1953–1970.
19) K. Yoshino, A. Tanaka, Y. Nambu, A. Tajima and A. Tomita: “Dual-mode time-bin coding for quantum key distribution using dual-drive Mach-Zehnder modulator,” *Technical Digest of ECOC 2007* (IEEE, Berlin, 2007) paper 9.4.7.
20) A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki and A. Tomita: “Ultra fast quantum key distribution

over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization," Opt. Express, **16** (2008) 11354–11360.
21) D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam and J. E. Nordholt: "Long-distance decoy-state quantum key distribution in optical fiber," Phys. Rev. Lett., **98** (2007) 010503.
22) T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger and H. Weinfurter: "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett., **98** (2007) 010504.
23) R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter and A. Zeilinger: "Entanglement-based quantum communication over 144 km," Nat. Phys., **3** (2007) 481–486.
24) D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery and S. Ten: "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," New J. Phys., **11** (2009) 075003.
25) Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe and A. J. Shields: "Gigahertz quantum key distribution with InGaAs avalanche photodiodes," Appl. Phys. Lett., **92** (2008) 201104.
26) T. Honjo, H. Takesue, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe and K. Inoue: "Long-distance distribution of time-bin entangled photon pairs over 100 km using frequency up-conversion detectors," Opt. Express, **15** (2007) 13957–13964.
27) 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," Nat. Photonics, **1** (2007) 343.

(2009 年 9 月 12 日受理)