■S2 群（ナノ・量子・バイオ）- 5 編（量子通信と量子計算）

1 章 量子通信と量子鍵配布

（執筆者：佐々木雅英）［2010 年 1 月 受領］

■概要■

通信技術の主要課題は，（1）いかに正確に多くの情報を効率よく伝送するか，（2）いかに安全に盗聴されることなく情報を伝送するかに大別される．

最初の主題は，雑音や損失の下で与えられたエネルギーと帯域を使い最大の情報量を伝送することであり，シャノンの通信理論によってその基本指針が与えられている．その原理はこれまで電磁気学と光学の法則に基づいて実装されてきた．伝送容量は信号対雑音比の改善とともにいくらでも大きくできると考えられていた．しかし，量子通信理論は，“不確定性原理” による量子雑音のために送信エネルギーが有限である限り伝送容量には原理的限界が存在すること，その限界の実現には “重ね合わせの原理” を利用した量子計算による復号が必要であることを教える．

もう一つの主題は，有史以来，軍事などで利用されながら暗号学として発展してきた．現在の暗号技術は，解読に膨大な時間がかかることで安全性を保つ．従って，コンピュータの性能が飛躍的に向上したり，数学的解法が新たに発見されれば無力化する．一方，量子暗号は不確定性原理を利用することで，将来のどんな技術でも解読できない情報安全性（無条件安全性）保証を可能にする．最も研究が進んでいるのは，秘密鍵を共有する量子鍵配布（QKD）である．それは使う検出器によって離散量 QKD と連続量 QKD の二つに分類される．前者は単一光子検出器を用いるもので，単一光子状態に基づく BB84，B92, DPS-QKD, COW（コヒーレント一方向方式）などと，量子もつれ状態を用いる E91，BBM92 などがある．BB84 や量子もつれ QKD では無条件安全性が証明されているが，DPS-QKD や COW は今のところ条件付き安全性にとどまっている．後者は，光の位相振幅変調とホモダイン検出器を用いる方式で，光通信の技術がそのまま使える．2009 年になって無条件安全性が証明された．

こういった新技術の研究には，量子もつれ光子対発生技術や光子検出技術が必須であり，これらを組み合わせることで光による量子計算を実現することも可能である．またこれらは，計測など広い科学技術分野の基盤でもある．

この分野の研究はこれまで光の離散性（粒子性）を制御する方式と光の連続性（波動性）を制御する方式が別々に行われてきたが，今後はこれらを融合し，光の両側面を統合的に制御する研究が必要である．その延長線上に，今はまだ大きなギャップがある現在の光通信技術と量子情報技術をつなぐ架け橋が見えてくるだろう．そして，いずれ人類が知りうる最高の情報通信技術の全貌が見えてくると期待する．

【本章の構成】

本章では，主題（1）に関して量子通信理論と実現に向けた課題（1-1 節），主題（2）に関して，量子鍵配布の基礎理論（1-2 節），量子鍵配布実験の到達点（離散量 QKD について 1-3 節，連続量 QKD について 1-4 節），量子光源技術の研究経緯と各種の方式（1-5 節），種々の波長帯に対する様々な光子検出器技術（1-6 節）が解説される．

■S2 群 - 5 編 - 1 章

1-1 量子通信理論

（執筆者：佐々木雅英）[2008 年 4 月 受領]

1-1-1 はじめに

量子通信は，通信理論や暗号理論を実装する原理を，従来の電磁気学と光学だけではなく，さらに量子力学まで含めて拡張した新しい通信技術である．その研究は，レーザが発明された 1960 年頃から，電磁波のエネルギーが厳密には量子化されていることを従来の通信理論（シャノン理論[1]）に取り入れて拡張することから始まった．電波による無線通信ではエネルギー量子 $h\nu$ の値が小さいため，量子効果は回路の熱雑音に埋もれてしまい通常問題とならない．一方，光ファイバ通信では，光子のエネルギー $h\nu$ の値は温度に換算して約 1 万 °C に達し，熱雑音を凌駕して量子効果が顕在化する．

通信における量子効果はまず「不確定性原理」という形で現れる．これは，粒子の位置 x と運動量 p を同時に正確に決定することはできないというもので，$\Delta x \Delta p \geq h = 10^{-34}$ J·s という不等式で表される（h はプランク定数）．光子の場合，x と p は電場成分と磁場成分（あるいは cos 成分と sin 成分）に対応する直交位相振幅である．つまり，受信過程の信号対雑音（SN）比に根本的限界が存在することになる．従来のシャノン理論では SN 比に原理的な限界はなく，通信路容量は SN 比の増加とともにいくらでも大きくできると考えられていた．これに対して，量子通信理論は信号エネルギーが有限である限り，通信システムがどんなに完全であっても通信路容量には原理的限界が存在することを教える．

不確定性原理は通信に原理的限界を与えるが，盗聴者にとっても大きな阻害要因である．この SN 比の絶対的限界を，符号化の工夫によって盗聴者のほうに積極的に課して，正規送受信者の情報安全性を確保しようというのが量子暗号である．実際，どんな盗聴戦略に対しても，符号長を十分長くすることによって漏えい情報量をいくらでも小さくできる，いわゆる「無条件安全性」がいくつかの量子鍵配布方式で証明されている．このような量子鍵配布技術は，将来的に技術が進歩しても絶対に破られることのない究極の暗号技術となる．量子鍵配布の詳細は，次節以降で詳しく解説される．

本節では，量子通信理論のなかでも究極の通信路容量に関する問題に焦点を当てる．この問題は，通信はもとより信号識別を扱う計測全般にかかわる基本問題である．特に，通信路容量は与えられたエネルギーのもとで，あらゆる変調方式や符号化方式を考慮して達成されうる通信や計測の基本的測度を与える．その究極の限界は不確定性原理によって課されるが，それを明らかにしようとする研究は，実は量子力学のもう一つの重要な原理「重ね合せの原理」を積極的に使うことによって，新しい可能性が生まれることを示すことになった．

1-1-2 シャノンの通信理論

雑音や損失があっても，誤り訂正のための冗長なビット列を付加して符号化を行うことによって，誤りのない伝送が可能となる．つまり，k ビット分のメッセージを伝送する場合でも，それより長い $n\ (>k)$ ビット分のパルス列で符号化する．伝送速度は $R = k/n$ で定義される．伝送速度は高いほどよいが，復号誤り率を十分小さくするためには雑音特性に応じたある上限値が存在し，それを通信路容量と呼ぶ．シャノンの通信理論[1, 2, 3]では，通信システムを抽象的な文字とその確率事象によってモデル化し，情報量や通信路容量を定量化する．情

報源は文字 x とその生起確率 $P(x)$ からなる確率事象 $X = \{x, P(x)\}$ としてモデル化される．雑音や損失を伴う通信路は入力文字 x と出力文字 y の間の遷移確率 $P(y|x)$ でモデル化される．通信路容量 $C^{(C)}$ は，相互情報量 $I(X:Y) \equiv \sum_x P(x) \sum_y P(y|x) \log_2 \frac{P(y|x)}{\sum_{x'} P(x')P(y|x')}$ を生起確率で最大化した量

$$C^{(C)} = \max_{P(x)} I(X:Y) \tag{1･1}$$

で与えられる（図 1･1 上）．周波数帯域 B 内にある連続信号を伝送エネルギー $\int_{-\infty}^{\infty} dx P(x)x^2 \le S$ のもとで伝送する場合には，式 (1･1) の通信路容量は $C^{(C)} = B\log\left(1 + \frac{S}{N}\right)$ となる．N は周波数帯域における雑音の平均電力である．これはシャノン理論のなかでも最も有名な公式である．

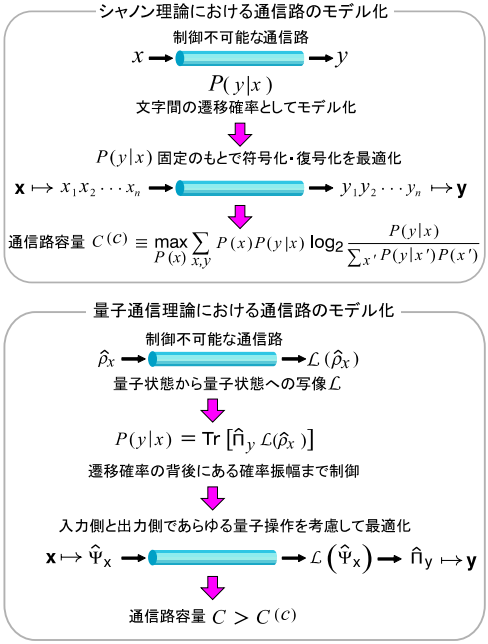

図 1･1　シャノン理論による通信路のモデル化と量子通信理論による通信路のモデル化の比較

1-1-3 量子効果を取り入れた拡張

シャノン理論に量子的離散性を取り入れて拡張する試みは，1960 年初頭からゴードン（J. P. Gordon）によって進められた．彼は光子の離散的エネルギー拘束条件 $h\nu\bar{m} = \sum_m mP(m)$ のもとでエントロピー最大化問題を解き，単一モード当たりの光子通信路の伝送容量として

$$C_{\text{photon}} = g(\bar{m}) = \log(1+\bar{m}) + \bar{m}\log\left(1 + \frac{1}{\bar{m}}\right) \tag{1･2}$$

という表現を導いた．第 2 項が量子力学特有の項で，信号エネルギーが量子レベルになってきたときに顕著になる項である．ただし，当時は量子測定を定式化する理論がまだ未完成で，式 (1･2) の導出には信号を取り出す量子測定が明らかに考慮されていない．ゴードン自身その不備を認めており，C_{photon} は通信路容量に対する上限値と捉えるべきであると考えていた．(C_{photon} が実は線形損失通信路の究極の通信路容量となっていることが証明されるのは 40 年後のことである)．

量子通信理論では，信号を運ぶ搬送波，通信路，そして信号検出過程をすべて量子力学の言語で記述する．文字 x を運ぶ搬送波の量子状態は密度行列 $\hat{\rho}_x$ によって表される．量子通信路とは，入力 $\hat{\rho}_x$ を別の量子状態 $\hat{\rho}_x^{\mathrm{out}}$ へ変換する過程（完全正値写像）である．数学的には信号状態 $\hat{\rho}_x$ と外部環境の状態 $\hat{\rho}_E$ を含めた系全体の変化を記述するユニタリ作用素 $\hat{U}$ を導入して $\hat{\rho}_x^{\mathrm{out}} = \mathrm{Tr}_E\left(\hat{U}\hat{\rho}_x \otimes \hat{\rho}_E \hat{U}^\dagger\right) \equiv \mathcal{L}(\hat{\rho}_x)$ と書かれる．Tr_E は環境系に関する部分トレースを表す．

信号検出過程は，正値作用素測度（Positive Operator-Valued Measure: POVM）という概念を用いて記述される[5, 6]．これは，$\hat{\Pi}_y = \hat{\Pi}_y^\dagger \geq 0, \sum_y \hat{\Pi}_y = \hat{I}$ という条件を満たす Hermite 作用素のセットである．はじめの条件は，確率の非負性を保証し，次の条件は検出過程における確率の保存則に対応する．$\hat{I}$ は恒等演算子（単位行列）である．入出力文字間の通信路行列は $P(y|x) = \mathrm{Tr}\left[\hat{\Pi}_y \mathcal{L}(\hat{\rho}_x)\right]$ で与えられる．

量子通信理論では，通信路行列 $P(y|x)$ の背後にある一段深い構造まで制御することを考える．つまり，与えられた通信路モデル $\mathcal{L}$ に対して，入力側と出力側で量子力学が許すあらゆる可能性を考慮して最適化を行い，最終的な通信路容量を写像 $\mathcal{L}$ の関数として求める（図 1･1 下）．信号状態 $\hat{\rho}_x$ とその生起確率 $P(x)$，信号検出過程 $\{\hat{\Pi}_y\}$ はもとより，符号化 $\{\mathbf{x} = x_1 \cdots x_n \mapsto \hat{\Psi}_{\mathbf{x}}\}$ と復号化 $\{\hat{\Pi}_{\mathbf{y}} : \mathbf{y} = y_1 \cdots y_n\}$ も最適化の対象である．搬送波には，通常のレーザ光（コヒーレント状態）のほか，光子数状態やスクィーズド状態を使ってもよいし，$a|0\rangle + b|1\rangle$ のようなキュービットを使ってもよい（$|0\rangle, |1\rangle$ は正規直交基底）．更に，$a|0000\rangle + b|1111\rangle$ のように異なるパルス列の重ね合せ状態，いわゆる量子もつれ状態で符号化してもよい．受信側では，最高の検出器に更に量子計算まで組み合わせた量子一括復号を考える．

これを一般的な量子通信路に対して行うのは極めて困難な問題であるが，線形損失通信路という最も現実的で重要なモデルに対して 2004 年に最終的な回答が与えられた．

1-1-4 量子一括復号

そこにいたる長い道のりの第一歩となったのは，ゴードンによって予想されホレボー（A.S. Holevo）によって証明された相互情報量 $I(X:Y)$ に対する上界定理である[7]．それは，ある与えられた量子情報源 $\mathcal{E} = \{\hat{\rho}_x, P(x)\}$ に対して，その出力信号状態 $\{\mathcal{L}(\hat{\rho}_x)\}$ を $\mathcal{D} = \{\hat{\Pi}_y\}$ なる POVM で検出する場合，相互情報量の最大値は

$$\chi(\mathcal{E}) = S\left(\sum_x P(x)\mathcal{L}(\hat{\rho}_x)\right) - \sum_x P(x) S\left(\mathcal{L}(\hat{\rho}_x)\right) \tag{1･3}$$

という量を使って $\max_{\mathcal{D}} I(X:Y) \leq \chi(\mathcal{E})$ で抑えられるというものである．ここで $S(\hat{\rho}) = -\mathrm{Tr}\,\hat{\rho}\log_2\hat{\rho}$ はフォン・ノイマンエントロピーで，量子統計力学で現れる重要な量である．

次に考えられたのは，与えられた情報源 $\mathcal{E}$ のテンソル積による符号化（量子もつれ状態は考

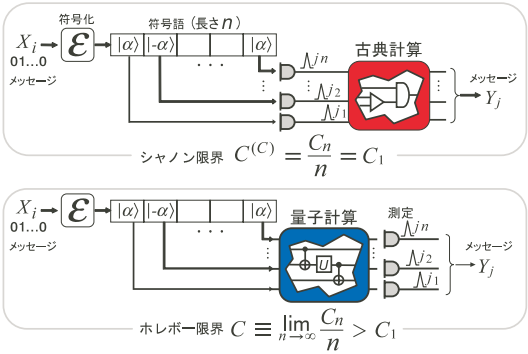

図 1･2　量子一括復号と個別測定に基づく従来の復号戦略の比較

えない）$\hat{\Psi}_{\mathbf{x}} = \hat{\rho}_{x_1} \otimes \hat{\rho}_{x_2} \otimes \cdots \otimes \hat{\rho}_{x_n}$ に対して，復号戦略を最適化した場合の通信路容量である．それは n 次の相互情報量を符号語の選択 $\mathcal{E}^n = \{\mathbf{x}; P(\mathbf{x})\}$ と復号戦略 $\mathcal{D}^n = \{\hat{\Pi}_{\mathbf{y}} : \mathbf{y} = y_1 \cdots y_n\}$ に関して最大化した量で $C_{1,n} = \max_{\mathcal{E}^n, \mathcal{D}^n} I(X^n : Y^n)$, で定義される．ここで添え字 $(1, n)$ のうち “1” は，符号化をテンソル積に制限し文字 x_i 間での量子もつれはないという制限を表す．一方，“n” は復号過程で長さ n の系列状態にわたる量子もつれ制御を含んだ一般的な量子一括復号まで許すことを意味する（図 1･2 下）．

例えば，コヒーレント状態による符号化 $|\Psi_{\mathbf{x}}\rangle \equiv |\alpha_{x_1}\rangle \otimes \cdots \otimes |\alpha_{x_n}\rangle$ を考える．コヒーレント状態は線形損失があっても純粋状態のまま $|\Psi^{\eta}_{\mathbf{x}}\rangle \equiv \mathcal{L}(|\Psi_{\mathbf{x}}\rangle) = |\eta\alpha_{x_1}\rangle \otimes \cdots \otimes |\eta\alpha_{x_n}\rangle$ のように出力される（η は透過係数）．量子一括復号では，出力パルス列 $|\Psi^{\eta}_{\mathbf{x}}\rangle$ をまず適切な量子計算処理 $\hat{U}$ によっていくつかの候補となる符号語パターンの重ね合せ状態 $\hat{U}|\Psi^{\eta}_{\mathbf{x}}\rangle = \sum_{\mathbf{x}'} c_{\mathbf{x}\mathbf{x}'} |\Psi^{\eta}_{\mathbf{x}'}\rangle$ に変換してから，各パルスごとに測定（$|\mathbf{y}\rangle = |y_1\rangle \otimes \cdots \otimes |y_n\rangle$ への射影）を行って信号を復号する．$\mathbf{x}$ が入力され $\mathbf{y}$ と復号される条件付確率は $P(\mathbf{y}|\mathbf{x}) = \left|\langle \mathbf{y}| \hat{U} |\Psi^{\eta}_{\mathbf{x}}\rangle\right|^2 = \left|\sum_{\mathbf{x}'} c_{\mathbf{x}\mathbf{x}'} \langle \mathbf{y}| \Psi^{\eta}_{\mathbf{x}'}\rangle\right|^2$ で与えられる．これは確率振幅の重ね合せの絶対値の 2 乗の形をしており，測定の際に量子力学的な干渉効果が起こりうることを意味する．いわば，適切な符号語が高い確率で復号されるよう量子干渉効果で自動的に誤り訂正を行っていることに相当する．

もし，量子もつれ制御 $\hat{U}$ のない個別測定に基づく従来どおりの復号戦略を用いる場合，$P(\mathbf{y}|\mathbf{x}) = P(y_1|x_1) \cdots P(y_n|x_n)$ となるため $C_{1,n} = nC_{1,1}$ であり，通信路容量は

$$C^{(C)} = \lim_{n\to\infty} \frac{C_{1,n}}{n} = C_{1,1} \tag{1･4}$$

となって，符号化する前の個別測定に対する特性 $C_{1,1}$ で一意に決まることになる[3]．

一方，量子一括復号では通信路行列は一般に $P(\mathbf{y}|\mathbf{x}) \neq P(y_1|x_1) \cdots P(y_n|x_n)$ となり，量子復号回路をうまく設計すると最大伝送情報量は符号長の増加とともに $C_{1,n} > nC_{1,1}$ のように超加法的に増加することが知られている[10, 11]．これは超加法的量子符号化利得と呼ばれ，従来の符号理論にはない新しい量子効果である．符号長無限大の極限値 $C^{(P)} \equiv \lim_{n\to\infty} \frac{C_{1,n}}{n}$ のことを特に積状態容量と呼ぶ．

積状態容量に関しては，ホレボー上界定理と符号語状態がテンソル積であることから，$C^{(P)} \le \bar{C} \equiv \max_{\{P(x)\}} \chi(\mathcal{E})$ という上界が与えられる．1996 年には，純粋状態信号の場合，この上界が実際に達成可能な伝送レートであることがハウスラーデン（P. Hausladen）らによって証明された[12]．この結果は，その後すぐに混合状態の場合へホレボー及びシューマッハー（B. Schumacher）とウエストモーランド（M. Westmoreland）によって拡張され，

$$C^{(P)} = \bar{C} = \max_{\{P(x)\}} \chi(\mathcal{E}) \tag{1･5}$$

となることが証明された[13, 14]．

現在では，与えられた通信路行列 $P(y|x)$ を固定したもとで個別測定に基づく復号操作によって達成される従来の容量限界 $C^{(C)}$ $(= C_{1,1})$ のことをシャノン限界と呼ぶ．一方，量子一括復号によって通信路行列の背後にある確率振幅まで制御することで達成される積状態容量 $C^{(P)}$ を先駆者にちなんでホレボー限界（あるいはホレボー・シューマッハー・ウェストモーランド限界）と呼んでいる．

1-1-5 究極の通信路容量

次に，符号化をテンソル積状態に制限しないで，m 次拡大空間上で任意の状態を許す場合について考える．この拡大空間上で，文字 x を運ぶ量子状態を $\hat{\Phi}_x^{\mathrm{in}}$ とする．これをまた一つの文字状態とみなして，長さ m のテンソル積状態からなる符号化を考えることができる．その場合の積状態容量は $C_{m,\infty} = \max_{p(x),\hat{\Phi}_x^{\mathrm{in}}} \chi(\{p(x), \hat{\mathcal{L}}^{\otimes m}(\hat{\Phi}_x^{\mathrm{in}})\})$ で与えられる．物理的には，非常に長い出力状態系列 $\hat{\mathcal{L}}^{\otimes m}(\hat{\Phi}_{x_1}^{\mathrm{in}}) \otimes \hat{\mathcal{L}}^{\otimes m}(\hat{\Phi}_{x_2}^{\mathrm{in}}) \otimes \cdots \otimes \hat{\mathcal{L}}^{\otimes m}(\hat{\Phi}_{x_n}^{\mathrm{in}})$ に対する量子一括復号を行っていることに相当する．量子通信路 $\mathcal{L}$ に対する最終的な通信路容量は，入力状態のサポート空間のサイズ m を十分大きく取った極限で $C = \lim_{m\to\infty} \frac{C_{m,\infty}}{m}$ と定義される．

現在，この究極の通信路容量が厳密に求められているのは，ボソン系の線形損失通信路である．入力状態の最適化まで考える場合，意味のある議論をするためには，エネルギー拘束条件を課す必要がある（拘束条件がないと通信路容量は発散する）．エネルギー拘束条件は，モード k の消滅演算子を $\hat{a}_k$，角周波数を ω_k として $\sum_k \hbar\omega_k \bar{n}_k = S$, $\bar{n}_k = \langle \hat{a}_k^\dagger \hat{a}_k \rangle$ と書かれる．

Giovannetti らは，この拘束条件のもとで $C_{1,\infty} \le \frac{C_{m,\infty}}{m} \le \max_{\bar{n}_k} \sum_k g(\eta_k \bar{n}_k)$ なる不等式が成立し（η_k は線形損失通信路におけるモード k の透過率），しかも上限と下限が一致することを示した[9]．つまり，究極の通信路容量は

$$C = \max_{\bar{n}_k} \sum_k g\left(\eta_k \bar{n}_k\right) \tag{1･6}$$

で与えられる．特に，下限は入力をコヒーレント状態からなるテンソル積状態とし，その振幅の先験確率を $p_k(\alpha) = \frac{1}{\pi \bar{n}_k} \exp\left(-\frac{|\alpha|^2}{\bar{n}_k}\right)$ というガウス分布としたときの積状態容量である．これは，送信側では特段の量子制御は必要なく，単にレーザ光のパルス列で符号化を行えばよいことを意味する．実際，光子数状態やスクィーズド状態などの非古典状態は，わずかな損失で壊れてしまい干渉性が著しく劣化して混合状態になる．一方，コヒーレント状態は位

相のそろった綺麗な波で，量子雑音も最小不確定状態にあり，これは損失を受けても変化しない．これがコヒーレント状態が最適な解となる理由である．

一方，復号過程では，やはり量子一括復号が必要となる．連続変調したコヒーレント状態信号は，情報を密に詰め込める反面，不確定性原理による SN 比の劣化を直接受けてしまう．最小の誤り率で信号を識別するためには，受信過程で量子干渉効果をうまく活用する必要がある．系列状態を最適に復号するためにも，系列全体にわたる量子干渉効果を引き起こす必要がある．情報を密に詰め込むことによる量子雑音の影響を，量子一括復号で解消できる最適限界が究極の通信路容量を決めていると考えることができる．

狭帯域通信路

通信路が狭い周波数幅に帯域制限されている場合，あるいは各周波数 ω ごとに独立に伝送を行う場合の通信路容量は $C = g\left(\frac{\eta S}{\hbar\omega}\right)$ で与えられる．一方，ダイン型検波による個別測定を用いる場合の通信路容量，式 (1･4) は $C^{(C)} = C_{1,1}^{(H)} \equiv \xi \log_2\left(1 + \frac{\eta S}{\xi^2 \hbar\omega}\right)$ で与えられる．ここで ξ はホモダイン検波の場合 $\xi = 1/2$，ヘテロダイン検波の場合 $\xi = 1$ である．

広帯域通信路

信号パルスの時間幅が T で，特にきつい帯域制限がなく，通信路の透過率が関与するモードにわたって一様 $\eta_k = \eta$ である場合，通信路容量は $C = \frac{\sqrt{\eta}}{\ln 2}\sqrt{\frac{\pi\mathcal{P}}{3\hbar}}T$ という簡単な式に帰着する．ここで $\mathcal{P} = S/T$ は伝送に費やす平均電力である．

許される信号エネルギーが大きい極限では，信号の非可換性の度合いが小さくなり，ヘテロダイン検波に基づく個別測定でも，実は，C に近い容量が達成できる．従って，信号エネルギーにそれほど深刻な制限がない場合や量子レベルの低雑音増幅器が使えるようになれば，コヒーレント多値変調と高性能のヘテロダイン検波技術を組み合わせた通信方式を採用すればよいことになる．光ファイバ基幹回線の将来的な方向もこれと大きくは変わらないだろう．

一方，限られた信号エネルギーで少しでも多くのユーザへ情報を配信する場合や，電力供給に大きな制限がかかる深宇宙での衛星間光通信などでは，量子一括測定による利得の効果を真剣に考えなければならなくなる．ただし，それでも通信路容量の値そのものは，量子論の C と従来のホモダイン検波に基づく個別測定での通信路容量 $C_{1,1}^{(H)}$ との間で数倍程度しか違わない．

量子利得と実効的伝送速度

しかし，この数倍程度の容量の違いは実際の通信性能に大きな違いとなって現れる．それは実際のデバイス処理速度は有限で，しかも微弱信号ほど，非常に長い符号化を行って信号の減衰や混信を防ぎ，信頼性を確保する必要があるからである．大規模な符号化を行うほど通信の精度は向上するが，復号に要する手間や装置コストが増えるため，これとの兼合いで符号が設計される．実際，符号長が長くなれば，それだけ復号に要する計算ステップ数も増えてゆくため，通信に時間がかかることになる．現在使われている連接符号の復号計算量は $O(n^2 \log^2 n)$ の程度であり，このような復号計算量まで考慮して実際の通信性能を評価する必要がある．想定する状況によって答えは千差万別であり，これ自体がまだ研究対象である．

例えば，受信端でパルス当たりの平均光子数が 1 個を下回るような深宇宙通信光通信では，受信感度の高い 2 値コヒーレント位相変調方式の採用が検討され，衛星間での実証試験も始

まっている．そのような場合，大規模な量子一括復号を実現できると，実効的な伝送速度を100 万倍程度改善できるとの予想もなされている[8]．これは量子計算によって復号計算量を大幅に短縮できることの結果であるが，具体的な量子回路の構成，つまり，量子復号アルゴリズムの導出はまだ未解決の問題である．

このような予測が現実のものになるのはいつの時代か定かではないが，たとえ小規模でも量子一括測定が実現できれば，従来の光符号と組み合わせることで復号計算量を大幅に削減でき，実効的な通信性能を着実に改善することができる．このようないわゆる量子-古典ハイブリッド符号化では，量子一括測定の規模が増えるごとに通信性能は一歩一歩着実に向上してゆく[15]．そして，量子一括測定を十分大きな規模で行えるようになったとき，与えられた信号エネルギーと帯域制限のもとで究極の通信路容量を達成することが可能になるのである．現在の光通信から量子通信へと発展する最も自然なルートである．量子一括測定は，光信号のみならず，各種の物質粒子や固体中の励起モードの測定にも当てはまる．従って，様々な計測や分光，計測計量分野でも，重要な技術になるだろう．

■参考文献

1) C.E. Shannon, “A Mathematical Theory of Communication,” Bell System Tech. J. (Part I), vol.27, pp.379-423, 1948; Bell System Tech. J. (Part II), pp.623-656, 1948.
2) R.G. Gallager, “Information Theory and Reliable Communication,” John Wiley and Sons, New York, 1968.
3) T. Cover and J. Thomas, “Elements of Information Theory,” John Wiley and Sons, New York, 1991.
4) C.W. Helstrom, “Detection theory and quantum mechanics,” Inform. Contr., vol.10, pp.254-291, 1967.
5) C.W. Helstrom, Quantum Detection and Estimation Theory, Academic Press, New York, 1976.
6) 広田修, 光通信理論, 森北出版, 1985.
7) A.S. Holevo, “Some estimates for information quantity transmitted by quantum communication channels,” Probl. Peredachi Inform., vol.9, no.3, pp.3-11, 1973; 英訳: Problems of Inform. Transm., vol.9, no.3, pp.177-183, 1973.
8) 佐々木雅英, 松岡正浩監修, 量子情報通信, オプトロニクス社, 2006.
9) V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J.H. Shapiro, and H.P. Yuen, “Classical Capacity of the Lossy Bosonic Channel: The Exact Solution,” Phys. Rev. Lett., vol.92, p.027902, 2004.
10) M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, “A demonstration of superadditivity in the classical capacity of a quantum channel,” Phys. Lett. A, vol.236, pp.1-4, 1997.
11) M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, “Quantum channels showing superadditivity in classical capacity,” Phys. Rev. A, vol.58, pp.146-158, 1998.
12) P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W.K. Wootters, “Classical information capacity of a quantum channel,” Phys. Rev. A, vol.54, pp.1869-1876, 1996.
13) A.S. Holevo, “The capacity of the quantum channel with general signal states,” IEEE Trans. Inf. Theory, vol.IT-44, pp.269-273, 1998.
14) B. Schumacher and M. Westmoreland, “Sending classical information via noisy quantum channels,” Phys. Rev. A, vol.56, pp.131-138, 1997.
15) M. Takeoka, M. Fujiwara, J. Mizuno, and M. Sasaki, Phys. Rev. A, vol.69, p.052329, 2004.

■S2 群 - 5 編 - 1 章

1-2 量子鍵配布理論

（執筆者：玉木　潔）[2008 年 4 月 受領]

量子鍵配布は，送信者（通常アリスと呼ぶ）と受信者（ボブ）の間に，ワンタイムパッド（乱数表を 1 回だけ使う暗号通信）[1]で用いる乱数表（秘密鍵）を盗聴者（イブ）に情報をほとんど漏らすことなく安全に共有する方法であり，実現に向けた実験及び理論的研究の両方が活発に行われている．公開鍵暗号[2]などの計算量に基づく既存の暗号との大きな違いは，盗聴者が無制限の計算能力をもち，かつ量子力学で許される任意の操作を実行可能だとしても，秘密鍵の安全性が保障されることである．重ね合せの原理，純粋状態の性質，不確定性原理などの量子力学の基本的な性質を巧妙に用いているので，量子鍵配布の理論的な研究は量子力学のより深い理解にも役立つものである．

本節では，量子鍵配布の無条件安全性理論を中心にレビューを行う．

1-2-1 量子鍵配布の基礎

まずはじめに，量子鍵配布の基礎的な事項を最も有名なプロトコルである BB84[4]の説明を交えて説明する．

量子鍵配布では，2 種類のチャネルを用意する．一つは量子力学的状態で表される物理系をやり取りするための量子チャネル，もう一つは古典チャネルである．古典チャネルでは，アリスとボブが基底公開，古典エラー訂正[2]，秘匿性増強プロトコル[2]のための通信を行う．これらの古典情報処理を正しく行うためには，認証プロトコル[3]を適用することにより，古典チャネル上の情報の改ざんを防ぐことが必要となる．認証プロトコルのためには，アリスとボブは少量の秘密鍵を前もって共有しなければならないので，量子鍵配布の行うことは，秘密鍵拡張である．

次に具体的なプロトコルの例として BB84 を説明する．まず，アリスはビット値 i をランダムに選び，次に 2 準位系（通常キュービットと呼ぶ．単一光子の偏光状態などがその例である）のある基底（Z 基底）の固有状態 $|i_z\rangle$，またはそれと共役な基底（X 基底）の固有状態 $|i_x\rangle$ にビット値をエンコードし，2 順位系を量子チャネルを用いてボブに送る．ボブは測定軸として Z 基底か X 基底をランダムに選び 2 準位系に対して測定を行う．アリスとボブはこれらの手順を何回か繰り返した後，古典チャネルを用いて選択した基底を公開し，両者が同じ基底を選んだ事象のみを残す，というのがプロトコルである．

このように生成されたビット値（シフト鍵）には通常ビット値の食い違い（ビットエラー）があるが，それを古典チャネルを用いた古典エラー訂正で直し，そしてビット列を縮めることによりビット列の安全性を高め（秘匿性増強プロトコル），秘密鍵を蒸留することになる．以下の小節では，無条件安全性証明の概略とその周辺について紹介する．ここで，量子鍵配送プロトコルの無条件安全性とは，イブが原理的に許される任意の操作が行える，という状況でのプロトコルの安全性を指す．

1-2-2 エンタングルメント蒸留プロトコルに基づく安全なプロトコル

量子鍵配布の無条件安全性を初めて示したのは Mayers であるが[5]，この方法は難解であるために現在までの安全性証明の研究で最も広く用いられている方法はエンタングルメント蒸

留に基づく方法である[6]．この方法では，まず安全性を証明したいプロトコル（プロトコル A と呼ぶことにする）と数学的に等価なエンタングルメント蒸留プロトコル（Entanglement Distillation Protocol: EDP）を構築する．ここで数学的に等価とは，二つのプロトコルが盗聴者から見ると全く区別が付かず，蒸留される秘密鍵が安全性を含めて全く同一，という意味である．従って，この EDP の安全性はそのままプロトコル A の安全性を意味する．EDP の安全性を示すことは，プロトコル A の安全性を直接示すことよりも容易であるために，この証明方法はプロトコル A の安全性を示すための強力な手段となっている．

EDP に基づく証明方法の大きな目標は，アリスとボブが次の状態で表される最大限にエンタングルしたキュービットペア（ベル状態）を複数ペア蒸留することである．

$$\left|\phi^{+}\right\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}\left(|0_z\rangle_{\mathrm{A}}\,|0_z\rangle_{\mathrm{B}} + |1_z\rangle_{\mathrm{A}}\,|1_z\rangle_{\mathrm{B}}\right) \tag{1・7}$$

ポイントは，アリスとボブが 2 人とも Z 基底で測定をした場合，測定結果がランダムでかつ常に一致することである．更に，この状態は純粋状態であるのでイブが所持する系を含めて，いかなる系とも相関がない．従って，N ペアの $|\phi^{+}\rangle_{\mathrm{AB}}$ に対して Z 基底測定から取り出される N ビット列は秘密鍵として用いることができるのである．

EDP では，まずアリスがベル状態を複数ペア用意し，系 B のみをボブに送信する．一般に，盗聴や雑音の影響により，アリスとボブが共有するペアの状態は $|\phi^{+}\rangle_{\mathrm{AB}}$ とはなっていない．しかし，それらペアのビットエラーと位相エラーと呼ばれるエラーの割合を推定し，それらを CSS コード[2]を用いて訂正，及び復号をするといくつかのほぼ完全な $|\phi^{+}\rangle_{\mathrm{AB}}$ が蒸留される．最後にそれらのペアに対する Z 基底測定から秘密鍵を得る，というのが EDP に基づく証明方法の基本的なアイディアである．ここで，2 種類のエラーのみ正しく見積もれば安全性が示せるということが，証明方法の簡潔さの本質となっている．

EDP の具体的な形は安全性を示したいプロトコルによって当然異なるが（例えば，BB84 の場合ハダマール変換[2]をアリスとボブがランダムに行う EDP が対応する），ビットエラーと位相エラーを訂正し，ベル状態を蒸留するという基本は変わらない．文献 6) では，BB84 におけるシフト鍵のビットエラーの割合が 11 %以下なら，安全な鍵が蒸留できることが示されている．

1-2-3 エンタングルメント蒸留プロトコルに基づく安全性証明の発展とそのほかの証明方法

前小節で紹介した証明方法は，簡潔であるので多くの研究に適用されてきた．現実的な装置を用いた通信[7, 8]や，安全な通信のためのビットエラーの閾値を向上させるための研究[9]などが，その例に当たる．また，B92[10, 11]，SARG04[12, 13]などの安全性証明にも，用いられている．この小節では，EDP に基づく証明方法の発展，及びそのほかの証明方法について触れる．

まず，文献 6) の証明ではアリスが送信するパルスはすべて単一光子であることを仮定している．この単一光子源を実現することは容易ではなく，実際の実験では代わりにレーザ光を弱めた光源を擬似単一光子源として用いることが多い．ここで注意しなければならないことは，レーザからの光は単一光子のみならず，2 光子，3 光子などの多光子を含むことである．これらの多光子発生のイベントからは，いわゆる光子数分離攻撃（Photon number splitting attack）[14]により，盗聴者はビットエラーなどを一切生じさせることなくビット値を盗み出せ

ることが知られている．このために，レーザ光を用いた BB84 の鍵生成率 G は量子チャネルの伝達率 η の 2 乗に比例することが知られている [7]（ちなみに，2 光子放出部分からも鍵が取り出すことができる SARG04[13]では $G \propto \eta^{\frac{3}{2}}$ である[15]）．

この光子数分離攻撃をより強く監視するために，おとり状態と呼ばれる光をアリスがランダムにボブに送る方法が提案された[8]．これを用いると，BB84 では $G \propto \eta$ へと向上する[8]．この方法は SARG04 などのように，光子に情報を載せるタイプのプロトコルにも直接適用できる[13]．また，古典エラー訂正の方法についてであるが，エラーシンドロームの情報がアリスからボブ（または逆）の一方向にしか流れない単一方向エラー訂正と，アリスとボブが情報をお互いにやりとりする双方向エラー訂正の 2 種類がある．文献 6) は単一方向エラー訂正を念頭においたものであるが，この証明方法は双方向エラー訂正にも発展させることができる[9]．更にこの双方向エラー訂正はおとり状態の方法と組み合わせることも可能である[16]．

一方ボブの側であるが，EDP に基づくほとんどの安全性証明では，ボブの検出器が受信した光子が単一光子か否かを見分けることができる，と暗に仮定している．というのも，EDP ではボブがキュービットを所持することが必須であり，この状態は多くの場合単一光子の偏光状態として定義できるからである．最近，BB84 または BB84 の双方向量子通信版の BBM92 プロトコル[17]については，EDP に基づく証明方法からこの仮定を取り除くことに成功した[18, 19]．従って，EDP に基づいて得られた BB84 及び，BBM92 プロトコルのすべての安全性の研究は，光子が存在するかしないか，という二つの事象しか見分けられない通常の閾値検出器を用いてもそのまま成立することになる[18]．

EDP に基づく証明以外の方法を見てみると，Mayers による BB84 の初めての安全性証明[5]と，その本質を抽出した不確定性原理（または相補性）に基づく Koashi による証明方法[20]では，検出効率が基底に依存しない限り，閾値検出器を含め任意の検出装置が使用できる．特に，文献 20) の方法は非常に簡潔であり，おとり状態も証明に組み込むこともでき，更に EDP に基づく証明方法よりも，若干長距離でも安全な鍵が生成できることを示すことができる．ただし，ボブ側のキュービットの性質に強く依存しているプロトコル，例えば双方向の古典エラー訂正を用いたプロトコルなどの安全性解析が，任意の検出装置を用いた場合にも有効なのかどうかは，今のところ未解決の問題である．

上に述べた方法以外の証明方法として，Kraus, Renner, Gisin らによって導入された情報理論に基づくアプローチがある[21]．この方法により BB84，偏光を用いた B92 など，光子の偏光状態を用いたプロトコルの安全性が示されている[21]．また，この方法によると，アリスが自分のビット値をある確率で反転させることにより，安全な通信のためのビットエラー閾値を向上できることが発見された（Pre-processing と呼ばれる）．直感的には，この意図的なビットフリップにより，アリスとイブの相関が，アリスとボブの相関より強く壊される場合がある，と理解される．更に，ボブの検出器が単一光子か否かを見分けられるという仮定のもとで双方向の古典エラー訂正，おとり状態の方法も取り得れることができる [22]．なお，Pre-processing による向上については，エンタングルメント蒸留の流儀の方法でも説明がなされている [23]．

やや脇道にそれるが，BB84 のようにパルス一つひとつに情報をエンコードするのではなく，コヒーレント光のパルス列に情報を乗せる DPS プロトコル[24]は比較的簡潔な実験装置での長距離通信が期待されているが，このプロトコルが無条件に安全か否かは現在のところ未解決な問題である．

また，多くの議論では鍵の長さが無限の極限を考えているが，実際の実験から得られるデータ長は当然有限である．有限長の問題は実装の観点から重要であり，いくつかの研究が行われている[25]．

最後にエンタングルメント蒸留は秘密鍵を生成するための十分条件であるが，必要条件ではないことに触れておく．秘密鍵蒸留のための必要十分条件はいわゆる Private state を蒸留することであるが詳細については 文献 23, 24) を参考にされたい．

1-2-4 現実的な装置の危険性とその対策，及び結び

量子鍵配布においては，装置の不完全性を利用する盗聴方法もいくつか考えられている．例えば，アリスがどのような状態を送信しているのか，イブが直接覗き見するという盗聴方法がその例である．実際，強い光をアリス側に送り，その反射光を観測することにより情報を盗み取る攻撃が提案されている[27]．

またボブの検出器であるが，ビット値 0 と 1 を読み出す検出器の検出効率に違いがあるとそれだけで情報が漏れてしまうことになるが，このことに基づいた盗聴方法の提案[28]，及びその対策が研究されている[29]．また，位相変調器の不完全性に基づいた攻撃方法も提案されている[30]．

これらの盗聴方法は Trojan horse attack または Side channel attack と呼ばれているものであり，いままでの安全性証明ではあまり考慮されていなかった類の攻撃方法である．定性的には，イブに漏れる情報量がある程度限られている場合には，秘匿性増強プロトコルを適切に行うことによりこの種の攻撃方法を防ぐことができるであろうが，その定量的な研究は今後ますます重要になってくると思われる．このように，現実的な装置を用いて安全な通信を目指すことは今までも，そして今後も量子鍵配布理論の一つの核となり続けるであろう．

最後に量子鍵配布のより詳細なレビューとして，文献 31) を薦める．

■参考文献

1) G.S. Vernam, “Cipher printing telegraph systems for secret wire and racho telegraphm communications,” J. AIEE, vol.45, p.109, 1926.
2) 例えば, M.A. Nielsen and I. L. Chuang, “Quantum Computation and Quantum Information,” Cambridge University Press, 2000 などを参照のこと.
3) M.N. Wegman and J.L. Carter, “New Hash Functions and their Use in Authentication and Set Equality,” J. Comp. Syst. Sci., vol.22, p.265, 1981.
4) C.H. Bennett and G. Brassard, “Quantum Cryptography, Public Key Distribution and Coin Tossing,” Proc. IEEE Inter. Conf. Comput., Systems and Signal Processing, p.175, 1984.
5) D. Mayers, “Quantum Key Distribution and String Oblivious Transfer in Noisy Channels,” Lecture Notes in Computer Science, vol.1109, p.343, Springer–Verlag, 1996.
6) P.W. Shor and J. Preskill, “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol,” Phys. Rev. Lett., vol.85, p.441, 2000.
7) D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” Quantum Information and Computation, vol.4, no.5, p.325-360, 2004.
8) W.Y. Hwang, “Quantum Key Distribution with High Loss, Toward Global Secure Communication,” Phys. Rev. Lett., vol.91, p.057901, 2003; H.-K. Lo, X. Ma, and K. Chen, “Decoy State Quantum Key Distribution,” Phys. Rev. Lett., vol.94, p.230504, 2005.

9) D. Gottesman and H.-K. Lo, “Proof of security of quantum key distribution with two-way classical communications,” IEEE Trans. Inform. Theory, vol.49, p.457, 2003.
10) C.H. Bennett, “Quantum cryptography using any two nonorthogonal states,” Phys. Rev. Lett., vol.68, p.3121, 1992.
11) K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, “Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse,” arXiv: quant-ph/0607082v1.
12) V. Scarani, A. Acin, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations,” Phys. Rev. Lett., vol.92, p.057901, 2004.
13) C.-H. F. Fung, K. Tamaki, and H.-K. Lo, “On the performance of two protocols: SARG04 and BB84,” Phys. Rev. A, vol.73, p.012337, 2006.
14) N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” Phys. Rev. A, vol.61, p.052304, 2000.
15) M. Koashi, “Security of quantum key distribution with discrete rotational symmetry,” arXiv: quant-ph/0507154.
16) X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, Phys. Rev. A, vol.74, p.032330, 2006.
17) C.H. Bennett, G. Brassard, and N.D. Mermin, “Quantum cryptography without Bell’s theorem,” Phys. Rev. Lett., vol.68, p.557, 1992.
18) T. Tsurumaru and K. Tamaki, “Security proof for QKD systems with threshold detectors,” arXiv: 0803.4226.
19) M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto, “Security of entanglement-based quantum key distribution with practical detectors,” arXiv: 0804.0891.
20) M. Koashi, “Simple security proof of quantum key distribution via uncertainty principle,” arXiv: quant-ph/0505108, 2006.
21) B. Kraus, N. Gisin, and R. Renner, “Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication,” Phys. Rev. Lett., vol.95, p.080501, 2005.
22) B. Kraus, C. Branciard, and R. Renner, “Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses,” Phys. Rev. A, vol.75, p.012316, 2007.
23) J.M. Renes and G. Smith, “Noisy Processing and Distillation of Private Quantum States,” Phys. Rev. Lett., vol.98, p.020502, 2007.
24) K. Inoue, E. Waks, and Y. Yamamoto, “Differential Phase Shift Quantum Key Distribution,” Phys. Rev. Lett., vol.89, p.037902, 2002.
25) M. Hayashi, “Practical Evaluation of Security for Quantum Key Distribution,” Phys. Rev. A, vol.74, p.022307, 2006.
26) K. Horodecki, D. Leung, H.-K. Lo, and J. Oppenheim, “Quantum Key Distribution Based on Arbitrarily Weak Distillable Entangled States,” Phys. Rev. Lett., vol.96, p.070501, 2006.
27) N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, “Trojan-horse attacks on quantum-key-distribution systems,” Phys. Rev. A, vol.73, p.022320, 2006.
28) B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, “Time-shift attack in practical quantum cryptosystems,” Quantum Information and Computation, vol.7, p.73, 2007.
29) C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, “Security proof of quantum key distribution with detection efficiency mismatch,” arXiv: 0802.3788, 2008.
30) C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, “Phase-Remapping Attack in Practical Quantum Key Distribution Systems,” Phys. Rev. A, vol.75, p.032314, 2007.

31) M. Dusek, N. Lütkenhaus, and M. Hendrych, “Quantum Cryptography,” arXiv: quant-ph/0601207; V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, “A Framework for Practical Quantum Cryptography,” arXiv: 0802.4155.

■S2 群 - 5 編 - 1 章

1-3 量子鍵配布実験：離散量 QKD

（執筆者：井上　恭）[2008 年 4 月 受領]

量子鍵配布（QKD）には，単一光子検出器を用いて光子の有無から秘密鍵を生成する離散量 QKD と，ホモダイン検出により光電場の状態を測定して鍵を生成する連続量 QKD とがある．量子鍵配布として最初に提案されたのは前者であり，こちらが量子鍵配布の原型ともいえる．この節では，離散量 QKD について，主に実験の観点から述べる．

離散量 QKD にも，単一光子信号光を送信して光子検出する方式と，送信信号はコヒーレント光でそれを光子検出する方式とがある．量子鍵配布の代表的プロトコルである BB84 は前者に属し，B92 や DPS は後者に属する．ここでは，主流である BB84 について中心的に述べ，その後に DPS に触れることにする．

1-3-1 BB84 量子鍵配布システム

BB84 では，非直交の 4 状態が送受信される．具体的には，縦・横直線偏波状態と右・左円偏波状態（または右・左斜め直線偏波），あるいは，1 光子を時間的に離れた 2 パルスの重ね合せとしたときの 2 パルス間の位相差が $\{0, \pi\}$ $\{\pi/2, 3\pi/2\}$ である状態，などである（図 1･3）．最初の提案では前者が利用されており，当初は偏波を使った実験がなされたが，後述のように光ファイバ伝送には後者が適しているため，最近の実験では位相差状態を用いることが多い．以下，送信系/伝送系/受信系それぞれについて具体的な実験構成を述べていく．

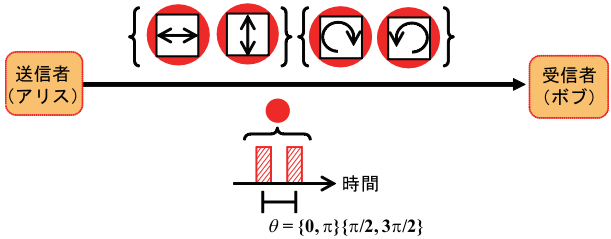

図 1･3　BB84 量子鍵配布

(1) 送信系

オリジナル BB84 の送信系では，1 パルスに 1 光子（またはそれ以下）のみを出力する単一光子光源が基本デバイスとなる．これについては本章 1-5 で述べられているので，詳しくはそちらを参照されたい．しかしながら，今のところ単一光子光源の実装は非常に難しく，ほとんどすべての鍵配布実験は、レーザ光を極度に減衰させた光（例えば平均 0.1 光子/パルス）を擬似的な単一光子信号光として用いている．ただしこの場合，1 パルスに 2 個以上の光子が存在することがあり，そのうちの 1 個から効率よく鍵ビットを盗み取る盗聴法（光子数分岐攻撃）を許すため，鍵生成率や伝送距離などのシステム性能が著しく制限される．これへの対処法として，平均光子数の異なるパルス（デコイパルス）を挿入する方式が提案され，実験も行われている．デコイ方式を実装する場合には，LD 光源を直接電流変調するか，

または外部変調器により強度変調する．

偏波状態を送信する方式では，信号光を LN 変調器により直接偏波変調するか，4 偏波状態を出力する光源を用意してタイミングを合わせて各出力をスイッチする（図 1･4 左）．一方，位相差状態を送信する場合には，光源からの光を 2 分岐し，一方に遅延を与えた後，再び合波する（図 1･4 右）．この際，遅延線上で位相変調を加えるか，あるいは，合波後に一方のパルスのみを位相変調すれば，位相差が付与された 2 パルス重ね合せ状態が出力される．

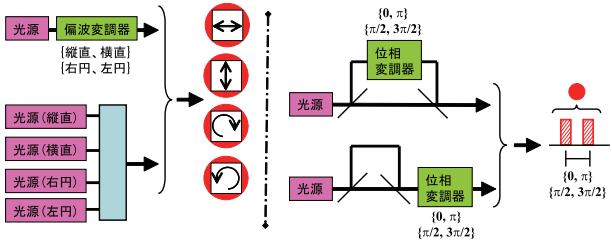

図 1･4　BB84 送信系

(2) 伝送系

伝送系には，伝送損失の観点から光ファイバを用いるのが通例である．ただし，一般にファイバには外圧や作製時の非対称性などにより微小な複屈折性が存在し，かつその方向や大きさは外部環境により時間的に変動する．このため光の偏波状態は伝搬につれて変化するので，偏波を利用する方式はそのままでは実装できず，偏波補償手段が必要となる．この困難さを避けるため，光ファイバによる鍵配布実験では 2 パルス間の位相差を利用することが多い．ファイバの屈折率は外部環境により変動するが，その時間変化より十分短い時間間隔（例えばナノ秒オーダ）の 2 パルスを用いれば，相対位相は一定に保たれる．また，偏波変動の時定数も屈折率変動のそれと同程度であり，2 パルスの偏波状態も常に同一とみなせる．このことは，2 パルスを干渉させて位相差を読み取る際にも都合がよい．なお，通常の光ファイバ通信では光直接増幅伝送が一般的であるが、量子鍵配布の伝送信号は 1 光子レベルであり，光増幅器を通ると自然放出雑音光に埋もれてしまうため，光増幅器を伝送系に挿入することはできない．

光ファイバを用いるシステムの信号光波長は，最低損失波長である 1.5 μm 帯となる．しかしながら，光子検出に広く用いられる APD（avalanche photo diode）は，この波長帯では検出効率や雑音特性があまり良くない．一方，短波長帯（0.5～0.8 μm）では性能のよい APD が利用可能である．そこで，光子検出の有利さから，短波長帯を用いる自由空間伝送系の実験も行われている．

(3) 受信系

受信系では，観測基底系をランダムに選択して信号光を受信する．偏波状態に対してこれを行うには、偏波変調器と偏波ビームスプリッタ（PBS）を用いるのが直接的であるが，偏波変調の煩雑さを避けるため，受信光をビームスプリッタ（BS）に通し，その出力を PBS 観測系と｛λ/4 波長板＋ PBS｝観測系にそれぞれ入力する構成を採ることが多い（図 1･5 左）．

前者は縦・横直線偏波の基底観測系であり，後者は円偏波の基底観測系となる．1 光子はそれ以上には分割されないので，ビームスプリッタに入射された光子は二つのポートのいずれか一方に出力される．どちらに出力されるかは完全にランダムであり，これにより観測系の選択が受動的に行われる．

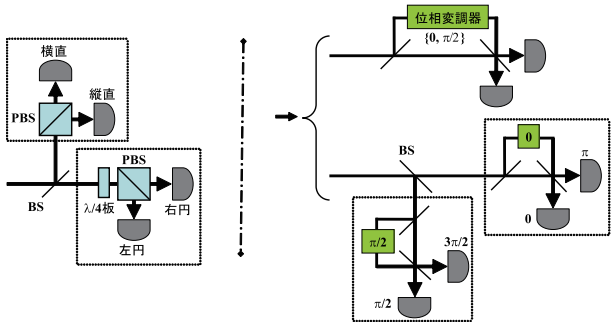

図 1･5　BB84 **受信系**

位相差状態を観測するためには，受信信号を送信系と同一の分岐・遅延・合波系（遅延干渉計）に通し，合波ビームスプリッタの二つの出力ポートで光子検出する（図 1･5 右）．このようにすると，長経路を通った第 1 パルスと短経路を通った第 2 パルスが干渉し合い，2 パルスの位相差に応じてどちらかのポートで光子が検出される．この際，2 経路の伝搬位相差が 0 ならば $\{0, \pi\}$ が確定的に観測され，$\pi/2$ ならば $\{\pi/2, 3\pi/2\}$ が確定的に観測される．すなわち，前者が $\{0, \pi\}$ の基底観測系，後者が $\{\pi/2, 3\pi/2\}$ の基底観測系となる．二つの基底観測系を選択するには，一方の経路上で $\{0, \pi/2\}$ の位相変調を加えればよい．あるいは，位相変調の煩雑さを避けるため，受信信号をビームスプリッタに通し，各出力を位相差 0 の干渉計と位相差 $\pi/2$ の干渉計にそれぞれ入力する．

干渉計の構成に際しては，伝播位相差の安定性が課題となる．位相差状態の 2 パルスの時間間隔は光子検出器の時間分解能で決まり，通常，ナノ秒程度である．光の伝搬長に換算すると，光ファイバの場合，1 ns が 20 cm に相当し，遅延干渉計としては数 10 cm オーダの光路長差のものを用意しなければならない．これだけのサイズの遅延干渉計を安定に動作させるためには，何かしらの工夫が必要である（この事情は送信系でも同様）．最近では，通常の光通信用として開発された PLC（planar lightwave circuit）と呼ばれるガラス導波路技術の活用により，安定な干渉動作が得られるようになってきている．

実際の実験系では，時刻同期をとることも重要である．元々の送信信号が約 0.1 光子／パルスと微弱でありかつ伝送路損失があるため，受信系ではごく稀にしか光子は検出されない．秘密鍵ビットは光子検出された事象から生成されるので，送信者と受信者とで送信パルスと光子検出パルスを対応付ける必要があり，そのためには送受信者間で時刻情報を共有しなければならない．そこで実際の伝送システムでは，別線または波長多重によりクロック信号を別途送受信することが行われる．

なお，量子鍵配布システムの受信系で最も重要なデバイスは光子検出器であるが，これに

ついては本章 1-6 で述べられているので，そちらを参照していただきたい．

(4) プラグ＆プレイ構成

以上が BB84 の基本形であるが，実際の実験では，受信系の項で述べた干渉計の安定性という課題に対処するために，「プラグ＆プレイ」と呼ばれる構成が用いられることも多い[3]．図 1･6 に，プラグ＆プレイ BB84 実験系の基本構成を示す．ボブ側に光源が置かれ，その出力光は分岐・遅延・PBS 合波系を経て，偏波が直交する 2 連続パルスとしてアリスへ送られる．アリスはこれをファラデーミラーにより偏波を直交変換し，擬似単一光子レベルまで減衰させてからボブへ送り返す．するとボブ側では，出力時には短経路を通った第 1 パルスは長経路を，長経路を通った第 2 パルスは短経路をそれぞれ経ることになり，両者は同時刻に合波され干渉する．一方のパルスに，アリス側で $\{0, \pi\}$ $\{\pi/2, 3\pi/2\}$，ボブ側で $\{0, \pi/2\}$，の位相変調を加えれば，BB84 プロトコルが実行される．この構成では，二つのパルスは同じ経路を逆向きに伝搬するので，相対位相が自動的に安定化され，安定な干渉動作を得ることができる．ただし，ボブからアリスへ送られる光のレイリー散乱光が雑音として作用するという難点があり，長距離・高レートの鍵配布には不向きである．

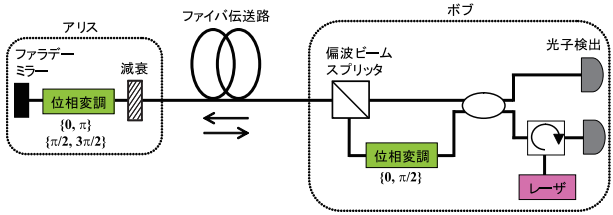

図 1･6　プラグ＆プレイ鍵配布システム

1-3-2 DPS 量子鍵配布システム

BB84 以外では，DPS（差動位相シフト）あるいはその類似版である COW（コヒーレント一方向）の実験が行われている[2]．図 1･7 に，DPS-QKD 実験の基本構成を示す．アリスは，レーザ光からの連続光を強度変調器により連続パルス列とし，各パルスに位相変調を加え，平均 0.1～0.2 光子／パルスまで減衰させてから送信する．ボブは、遅延干渉計により隣り合う 2 パルス間の位相差を測定し，その結果から鍵ビットを生成する．ここで所望の干渉を起こさせるためには，光源のコヒーレンス時間がパルス間隔より十分長いことが必要であり，そのため，パルス列の生成には連続光を外部変調する構成が採られる．また，報告されている DPS-QKD 実験で特徴的なのは，遅延干渉計としてガラス導波路回路を用いていることである．これにより，安定な干渉動作を得ている．

DPS 方式の特徴としては，構成が簡便、基底不一致で廃棄するビットがない，連続パルスを用いるため時間領域が有効利用されクロックレートが高くできる，光子数分岐攻撃に強い，といったことがあげられる．これらの特徴を活かし，個別盗聴に対してという限定付きではあるが，最長・最高速の実験データが得られている．

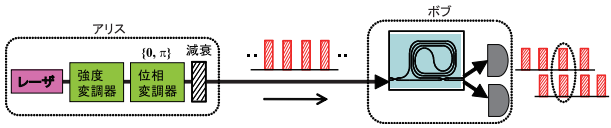

図 1･7　DPS 量子鍵配布システム

1-3-3 システム性能

鍵配布システムの性能指標は伝送距離と鍵生成レートである．伝送距離は，主に光子検出器のダークカウントで制限される．距離が長くなると，伝送路損失のため受信系に到達する光子数が少なくなる．すると，信号カウントに対してダークカウントの比率が相対的に大きくなり，ビット誤りが増加して最終秘密鍵が生成できなくなる．

鍵生成レートは，（送信クロックレート）×（送信光子数／パルス）×（伝送透過率＋受信系損失）×（光子検出器効率）×（光子検出器動作速度），に比例する．このうち，伝送透過率・送信光子数は必然的に与えられるパラメータであり，実験的に鍵生成レートを決めるのは主に光子検出器の検出効率と動作速度となる．更に，検出器の時間分解能が高ければ，検出器が非ゲート動作である場合に，パルス間隔を短くして（すなわち送信クロックレートを高くして），鍵生成レートを上げることができる．これらの性能を向上させ，高い QKD システム性能を得る努力が続けられている．

最後に，これまでの実験報告例をあげておく．ただし，鍵の安全度が統一されておらず，おおよその目安として見ていただきたい．

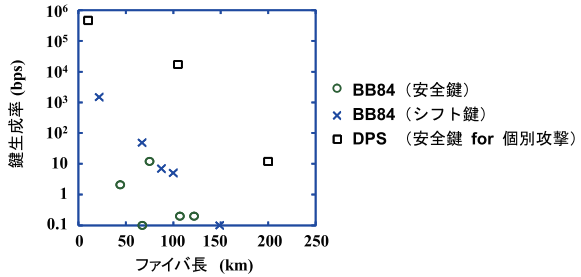

図 1･8　システム実験の報告例

■参考文献

1) N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys., vol.74, no.1, pp.145-195, 2002.
2) K. Inoue, “Quantum key distribution technologies,” IEEE J. Sel. Top. Quantum Electron., vol.12, no.4, pp.888-896, 2006.
3) A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, “Plug and play systems for quantum cryptography,” Appl. Phys. Lett., vol.70, no.7, pp.793-795, 1997.

■S2 群 - 5 編 - 1 章

1-4 量子鍵配布実験：連続量 QKD

（執筆者：平野琢也）[2008 年 6 月 受領]

量子情報処理は，スピンや単一光子の偏光などで実現される量子ビット（qubit）を基本単位として用いることが多いが，連続量を扱う量子情報処理も可能である[1]．このことは，通常の（量子ではない）情報理論や通信においても，離散量だけでなく連続量も扱われることと対比できよう〔1 群 1 編，5 群 1 編参照〕．量子通信では，通常，光が媒体として用いられる．電波と比べて振動数の高い光の場合は，室温においても量子雑音が支配的な雑音となること，光ファイバーを用いて位相情報を遠距離まで伝達できるといった利点を有するからである．光の直交振幅（quadrature-phase amplitude）は，連続的なスペクトルをもつ連続変数であり，光の直交振幅を用いて連続量の量子情報処理を実現することができる．

本節では，連続量を用いた量子鍵配布（Quantum Key Distribution: QKD）について述べる[2]．離散量 QKD と比べると〔1-3 節参照〕，研究の歴史が比較的新しいこともあり未開拓のことがらも多いが，単一光子源や単一光子検出器といった特殊なデバイスが不必要でコヒーレント光通信と親和性のよい方式であること，パルス当たりの鍵生成率の向上が可能であるなどの特徴がある．

1-4-1 連続量 QKD の分類

連続量 QKD には変調方式や安全な鍵をつくる手順にいくつかの方式が提案されている．この項では，それらの概要について説明する．

(1) 連続量 QKD における変調と検出

連続量 QKD では，送信者は光の直交振幅を変調して送信し，受信者は受信した光の直交振幅を測定する．直交振幅は，電場を複素表示したとき，その実部と虚部に相当する物理量である．受信者は，測定の結果，ある実数値を得ることになる．この実数値は，送信者の行う変調と関係があるので，送信者と受信者は情報を共有することが可能である．このとき，盗聴者が得ることができる情報量よりも，正規の送受信者が共有する情報量の方が多いとき，QKD が成立する．連続量 QKD は，電磁波の振幅を扱うので，光の波としての性質を利用するものであるといえる．一方，単一光子を用いる QKD は，基本的にはあるモードに光子がいるかどうかを扱うものであり，光の粒子としての性質を利用しており，光子のオン・オフを変調するものといえる．

連続量 QKD では，直交振幅変調を行うわけであるが，原理的に二つの変調方式がありうる．最もよく研究されている変調方式は，送信する光の直交振幅が複素平面上でガウス分布するように変調を行う方式である[3]．もう一つの可能性は，有限とおりの位相変調を与える方式であり，例えば，4 通りの位相変調を与える QKD を考えることができる[4]．前者のガウス変調方式では，送信者の行う直交振幅変調は実数値で指定されるので，送信者と受信者は相関をもった実数値のペアをもつことになる．後者の場合には，送信者の行う変調は離散量で指定されるので，連続量と離散量の雑種的な方式であるといえる[1]．安全性についての理論的な研究については，実験装置の不完全性を考慮した現実的な状況下で，コレクティブ攻撃に対して安全な鍵の生成レートが求められている[5, 6, 7]．そして，コレクティブ攻撃に対して安全であれば無条件に安全であることが示され[8]，連続量 QKD の無条件安全性も示され

た．さらに，4 通りの位相変調（±45 度，±135 度）を与える連続量 QKD は，長距離でも無条件に安全な秘密鍵を高効率に生成可能であることが示された[9]．

連続量 QKD に対する量子力学的な効果は，量子揺らぎの存在に現れる．量子揺らぎは，ハイゼンベルクの不確定性関係から導き出されるもので，質点の位置と運動量の両方を同時に正確に定めることが原理的にできないのと同じように，位相が 90 度ずれた（複素平面上で直交する）二つの直交振幅を同時に正確に定めることはできない．レーザ光の状態は，量子論では，コヒーレント状態として扱うことができる．コヒーレント状態は，二つの直交振幅の不確定さが等しい最小不確定状態であり，位相に依存しない一定の量子揺らぎをもっている（その揺らぎの大きさは真空状態と等しい）．微弱なレーザ光に，0 度，90 度，180 度，270 度の四つの位相変調のいずれかを与えたとする（図 1･9(a) 参照）．

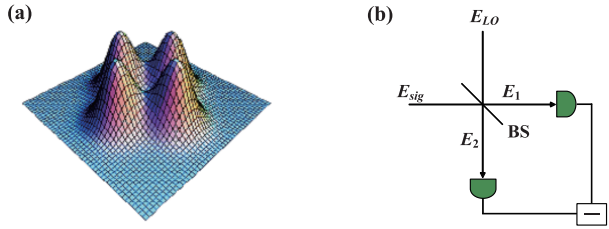

図 1･9　(a) **四つのコヒーレント状態の混合状態の伏見関数表示．**(b) **ホモダイン検出の概念図**

量子揺らぎがなければ，これら四つの状態は複素平面上の四つの点で表される．しかし，量子揺らぎのために，直交振幅の測定値にはばらつきが生じる．コヒーレント状態は互いに非直交な状態であるため，図 1･9(a) に示すように，四つの状態の直交振幅の分布は重なり合い，これらの状態を常に誤りなく区別することは原理的にできない．このとき，レーザ光が微弱になればなるほど振幅が小さくなり，状態を区別することが難しくなる．このように，量子揺らぎがあるために，盗聴者が位相変調量を確実に読み出すことはできない．連続量 QKD では，基本的に，この事情を安全な鍵の配送を実現するために使う．

受信者はホモダイン検出を行うことで直交位相振幅を測定することができる．ホモダイン検出は，図 1･9(b) に示すように，測定したい光の電場 E_{sig} を局部発振光（LO 光）と 50：50 のビームスプリッタで重ね合わせ，その二つの出力光の強度の差を測定するものである．LO 光には比較的強度の強い光を用いるので，室温で動作させるフォトダイオードで光の強度を測定し，量子雑音限界の測定を行うことが可能である．しかし，信号光に対して位相がロックされた LO 光をどのようにして受信者が用意するかという点が実験上の課題となる．

(2) 連続量 QKD の安全性

現実的な状況下で連続量 QKD の安全性を議論するためには，通信路の損失と過剰雑音（excess noise）について考慮する必要がある[4]．

通信路の透過率が 50 %以下の場合，盗聴者が受け取りうる光の強度の方が正規の受信者よりも強くなる．これは，物理法則によってのみ能力を制限される盗聴者は，元の通信路の損失分をビームスプリッタで分岐して自分が測定し，残りを損失のない通信路で正規の受信者に送るという盗聴が可能ためである．このような場合においても安全な鍵を得るための方

法として，事後選択（post selection）と逆調整（reverse reconciliation）という方式が提案されている．

事後選択は，受信者が自分に都合のよい測定値を得たときのみ選択して鍵をつくる手続きである[4]．量子揺らぎにより受信者の得る測定値はランダムに変動するが，一般に，振幅の大きな測定値を得たときは，送信者の行った直交変調を推測する際の誤り率が小さくなる（正規の送受信者の相互情報量が多くなる）．正規の送受信者は，自分たちに都合のよいパルスを選ぶことができるが，盗聴者が都合のよいパルスを選ぶことはできないという量子鍵配布における立場の違いを事後選択は利用している．あとで述べる過剰雑音がない場合は，どんなに損失が大きくても，事後選択により安全な鍵を配布することが可能である．

逆調整では，送受信者がもつ相関をもったデータから，第三者の知らない正しいビット列を送受信者がどのようにして共有するかという手続きに注目する．通常は，送信者のデータに一致するように受信者が自分のデータを修正していくのに対し，逆調整では，受信者のデータに一致するように送信者のデータを修正する．通常の手続きでは，送信者と盗聴者の相互情報量が，送信者と受信者の相互情報量よりも多い場合は，安全な鍵を配送できないが，逆調整では，受信者と盗聴者の相互情報量が，送信者と受信者の相互情報量よりも少ないことを利用して安全な鍵をつくることができる[3]．例えば，送信者の送った光の強度が 1 で，そのうちの 0.7 を盗聴者が受け取り，残りの 0.3 を受信者が受け取った場合を考えると，送信者のデータについては，受信者よりも盗聴者がよく知っていることになるが，受信者のもつデータについては，送信者の方が盗聴者よりもよりよく知っていることを逆調整では利用する．

過剰雑音は，受信者の測定する直交振幅のばらつきが量子雑音限界と比べてどの程度大きいかを表す．定量的には，受信者の直交振幅の分散が量子雑音限界よりも $(1+\delta)$ 倍であるとき，δ を過剰雑音と呼ぶことが多い．離散量 QKD において，第三者による盗聴で誤り率の増大が起こるのと同じように，連続量 QKD では盗聴は過剰雑音の増加をもたらす．逆に，実験装置の不完全性などにより，受信者のデータに過剰雑音が存在しているときは，その過剰雑音が盗聴者によって引き起こされたという可能性を原理的には排除できない．そのため，過剰雑音が存在している場合は，盗聴者に情報が漏れている可能性があることになる．

連続量 QKD の安全性を考えるうえで，同時測定を行う “なりすまし攻撃”（intercept/resend attack）は重要な攻撃である[10]．ここでの同時測定は，複素平面上で 90 度位相のずれた二つの直交振幅を同時に測定することで，具体的には，盗聴者は信号光をビームスプリッタで半分ずつに分割し，片方で直交振幅の実数成分，もう片方は 90 度位相をずらした虚数成分をホモダイン検出する．そして，測定で得た直交振幅を $\sqrt{2}$ 倍して，正規の受信者へ再送する．このなりすまし攻撃が行われた場合，受信者の受け取る状態は盗聴者が送信したものであり，量子揺らぎに基づく正規の送受信者の盗聴者に対する優位性は失われ，安全な鍵を配送することは不可能となる．では，どのような場合に，なりすまし攻撃が成立してしまうのだろうか？ なりすまし攻撃の過程で盗聴者が再送する信号光の分散は，元のコヒーレント状態の 3 倍まで増加するが，透過率 η の通信路を通った後は，$2\eta+1$ 倍まで小さくなる．そのため，連続量 QKD で安全な鍵を配送するためには，$\delta < 2\eta$ である必要がある．これは，コヒーレント状態を送受信し，ホモダイン検出を行う QKD であれば，プロトコルの詳細によらず満たさなければならない条件である[10]．例えば，通信路の透過率が 1 %である場合は（長さ 100 km の低損失光ファイバーに相当），過剰雑音は 2 %以下でなければならない．

1-4-2 連続量 QKD 実験

(1) ガウス変調方式

2003 年に Grosshans らは，ガウス変調方式と逆調整を用いた連続量 QKD の実験を報告し，通信路の透過率が 2 分の 1 以下でも個別攻撃（individual attack）に対して安全な鍵を配送できることを示した[3]．この実験は短距離の自由空間を通信路とするテーブルトップの原理検証実験であり，通信路に光損失がないときの鍵生成率は 1.7 Mbps，3.1 dB の損失があるときは 75 Mbps であった．同グループは 2007 年に通信波長帯のレーザ光源を用い，長さ 25 km の光ファイバを通信路（透過率は 0.302）とする実験を報告した[6]．これは一方向の伝送実験であり，送信者から受信者へ向けて，LO 光も同じファイバで伝送する．時間幅 100 ナノ秒のパルス光を 500 KHz の繰返しで送信し，collective attack に対して安全な鍵を 2 kbps で配送している．光学系は二重マッハ–ツェンダー干渉計を用いたもので，信号光と LO 光は送信者の装置のなかのディレイファイバで時間差をつけて通信路となるファイバを伝わり，受信者のディレイファイバで再度時間差を一致させることで干渉するようになっている．信号光と LO 光間の位相差の同期は，全体のパルスのうち 5 分の 1 をレファレンスに用いて実現している．

Bing Qi らは同じくガウス変調と逆調整を用い，長さ 5 km のシングルモードファイバを通信路とする連続量 QKD 実験を報告している[7]．この実験も二重マッハ–ツェンダー干渉計を用いたものであるが，信号光と LO 光を偏光と周波数によっても分離することで，両者を 70 dB 以上分離できたことを報告している．また，信号光と LO 光の位相差については，事後に送信者のデータを回転させて解釈することを提案している．この実験では，盗聴者は通信路のみにアクセスでき，送受信者の装置にはアクセスできないという現実的なモデル（realistic model）において，1 パルス当たり 0.3 ビットの秘密鍵が配送できるとしており，これは離散量 QKD よりも 2 桁優れた性能である．

Symul らは，ガウス変調と事後選択を用いる QKD 実験について報告している[5]．これは自由空間を通信路とするテーブルトップの実験であるが，通信路の透過率が 0.2 で過剰雑音が 0.1 であっても collective attack に対して安全な鍵を配送できることを示した．この実験では，送信者はサイドバンドの直交振幅に変調を行い，受信者は二つの直交振幅を両方測定する方法を用いている．サイドバンドを用いる方法は，周波数領域に多重化することが原理的に可能であるので，高い鍵配送レートを実現できる可能性がある．

(2) 4 状態プロトコル

送信者がコヒーレント状態に 4 通りの位相変調を与える 4 状態のプロトコルは，実験的な実装が行われている，現時点では，唯一の有限とおりの直交振幅変調 QKD である．送信者は位相変調を行うだけでよいという実装上の容易さがある．2003 年に出版された論文は，通信波長帯のパルスレーザを使用し，長さ 1 km の光ファイバを通信路とするものである[4]．受信者の測定する直交振幅はガウス分布でよく表されるが過剰雑音があること，事後選択を行うことで誤り率の低減が可能であることなどを実験的に示した．光学系は，二重マッハ–ツェンダー干渉計を用いるものであったが，バルクの光学部品を用いていたこともあり，信号光と LO 光の位相を安定に保つのは困難であった．

位相を安定に保つ一つの方法は，通信路を往復させる，いわゆるプラグ・アンド・プレイ方式がある[2]．この方式では，受信者の側に光源があり，光ファイバを往復させることで，ファ

イバ中で生じる偏光の乱れを自動補正できるほか，信号光と LO 光の相対的な位相差も安定に保たれる．離散量 QKD の場合でも，光学系の安定性を容易に実現できるというメリットから，よく用いられてきた方式であるが，受信者から送信者へ送る光の後方散乱光が受信者へ戻ってくるので，通信距離を延長する際には問題となっている．同様に，連続量 QKD の場合も，後方散乱光による過剰雑音の増加が問題となる．単一光子検出と比較すると，ホモダイン検出は迷光に強いという利点があるが，強度の強い LO 光を送らなければならないことは不利な面である．過剰雑音の増加を抑える方法として，音響光学素子を用いて，光の周波数をシフトさせる方法が知られており，10 km の伝送距離で，なりすまし攻撃に対して安全な鍵配送を実現できることが示されている[2)]．もう一つの位相を安定に保つ方法は，媒質中の屈折率の異方性を利用して，同軸の光学系で二重マッハ–ツェンダー干渉計を構成する方法である[2)]．連続量 QKD の自由空間伝送を目指した原理検証実験も行われている[11)]．

1-4-3 まとめ

連続量 QKD の概略と実験の現状について述べた．室温で動作可能で小型化に有利である，迷光に強いなどの実装上のメリットがあるが，長距離化，高速化，多重化，安全性の証明など多くの課題が残されているほか，基礎的な方式についても今後研究を進めていく必要があると思われる．

■参考文献

1) S.L. Braunstein and P. van Loock, “Quantum information with continuous variables,” Rev. Mod. Phys., vol.77, p.513, 2005.
2) 平野琢也, 川元洋平, 並木亮, “コヒーレント光とホモダイン検波による量子鍵配送,” 量子情報通信, pp.179-204, オプトロニクス社, 2006.
3) F. Grosshans, G.V. Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier, “Quantum key distribution using gaussian-modulated coherent states,” Nature, vol.421, p.238, 2003.
4) T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, “Quantum cryptography using pulsed homodyne detection,” Phys. Rev. A, vol.68, p.042331, 2003.
5) T. Symul, D.J. Alton, S.M. Assad, A.M. Lance, C. Weedbrook, T.C. Ralph, and P. Koy Lam, “Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise,” Phys. Rev. A, vol.76, p.030303(R), 2007.
6) J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N.J. Cerf, R. Tualle-Brouri, S.W. McLaughlin, and P. Grangier, “Quantum key distribution over 25 km with an all-fiber continuous-variable system,” Phys. Rev. A, vol.76, p.042305, 2007.
7) B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, “Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers,” Phys. Rev. A, vol.76, p.052323, 2007.
8) R. Renner and J. I. Cirac, “de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography,” Phys. Rev. Lett., vol.102, p.110504, 2009.
9) A. Leverrier and P. Grangier, “Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation,” Phys. Rev. Lett., vol.102, p.180504, 2009.
10) R. Namiki and T. Hirano, “Practical Limitation for Continuous-Variable Quantum Cryptography using Coherent States,” Phys. Rev. Lett., vol.92, p.117901, 2004.
11) D. Elser, T. Bartley, B. Heim, Ch. Wittmann, D. Sych, and G. Leuchs, “Feasibility of free space quantum key distribution with coherent polarization states,” New J. Phys., vol.11, p.045014, 2009.

■S2 群 - 5 編 - 1 章

1-5 光源技術

（執筆者：枝松圭一）[2008 年 5 月 受領]

近年，光子を用いた量子情報通信技術の発展が著しい．光子を用いた量子暗号通信などにおいては，「光子の単一性」，すなわち同時に 2 個以上の光子が存在しないことが秘匿性の保持や誤り率の低下などの点において本質的に重要である．また，量子情報を遠隔地間で授受するための方法として種々の「量子中継」プロトコルが提案されているが，そこでは量子状態間の「量子もつれ」の発生と検出が本質的役割を果たし，良質かつ高効率な量子もつれ光源の開発もまた重要な技術課題である．本節では，単一光子及び相関光子，量子もつれ光子の発生技術に関する基本的事項とそれらの最近の進展について概観する．

1-5-1 単一光子源

(1) 単一光子の発生

「単一光子」とは，一つの時空間モードに対して光子が 1 個励起されている状態を指すが，実用的には，ある時空間において光子を検出した際に 2 個以上の光子が検出される確率が 0 である状態を指す場合が多い．このような，光子の時間的な単一性は，2 次の自己相関関数（強度相関関数）

$$g^{(2)}(\tau) = \frac{\langle \hat{a}^\dagger(t)\hat{a}^\dagger(t+\tau)\hat{a}(t+\tau)\hat{a}(t)\rangle}{\langle \hat{a}^\dagger(t)\hat{a}(t)\rangle^2} \tag{1・8}$$

で定量的に表すことができる[1]．ここで，$\hat{a}^\dagger(t)$ 及び $\hat{a}(t)$ は各々時刻 t における光子の生成，消滅演算子である．単一光子状態では，同時に 2 個以上の光子が観測されることはないから，$g^{(2)}(0) = 0$ である．

単一光子の発生にはいくつかの方法が提案されているが，その一つが，単一の原子，分子，束縛電子など，単一の量子状態からの発光を利用する方法である．すなわち，これらの単一量子状態中の電子のフェルミオン性に基づき，同じ時刻・状態に複数の光子が発生しないよう制御された光源として利用するものである．実際に $g^{(2)}(0) \simeq 0$ となるような単一光子に近い状態は，Na などの単一の原子の共鳴発光において初めて観測された[2]．これは，単一原子においては 2 電子が同時に同じスピン・軌道準位に励起されないという，電子のフェルミオン性を反映した強い光学非線形性によるものである．このような単一光子状態は，単一原子以外にも，単一イオンの共鳴発光[3]，単一分子の発光[4, 5]，固体中の単一不純物準位からの発光[6]，半導体中の単一量子ドットからの発光[7)−10)]，単一有機ナノ結晶からの発光[11)]のように，単一の量子準位からの電子遷移による発光を分離して受光することによって観測されている．このような単一光子発生に関する解説論文として，単一原子を用いた初期の研究に関するもの[12, 13)]や，単一分子や固体を用いた研究に関するもの[14)]が参考になるだろう．

(2) 半導体単一光子源

半導体を用いた単一光子発生が初めて確認されたのは，コロイド溶液法で作製された CdSe 量子ドットを用いた実験[7, 8)]である．また，Ⅲ-Ⅴ 族半導体表面上に自己組織化成長した単一量子ドット試料からの単一光子発生も観測されている[9, 10)]．これらの実験はレーザによる光励起を用いていたが，半導体中に埋め込まれた単一量子ドットを用いれば，発光ダイオード

のように電流注入による単一光子発生も期待される．実際，このような電流注入による単一光子発生もほどなくして実現された[15]．

更に最近では，単一光子源の波長帯や動作温度域の拡大も試みられている．その一つは，通信波長帯への拡大であり，InAs/InP 量子ドットを用いて 1.5 μm 帯における単一光子発生[16, 17]が報告されている．もう一つは，より高温で動作する単一光子源を実現する試みである．前述のコロイド量子ドットは Ⅱ-Ⅵ 族半導体であり，室温でも高収率で発光する．そのため，初期の段階から室温でのアンチバンチングが測定されている[7]が，GaAs などの Ⅲ-Ⅴ 族量子ドットでは励起子の束縛エネルギーが小さく，単一光子源としての高温での動作は困難である．これに対し，励起子が高温まで安定な物質の量子ドットを用いれば，より高温での動作が期待される．これまでに，GaN 量子ドットを用いた単一光子発生において 200 K での動作が報告されている[18]．

1-5-2 相関光子，量子もつれ光子源

(1) 相関光子の発生

図 1･10 に示すように，3 準位系からのカスケード光放出や，2 次の非線形光学効果である自発パラメトリック下方変換を用いると，1 個の光子（ポンプ光子）から時間的に強く相関した 1 対の光子を発生することができる．3 準位系の場合，光子対の時間相関は中間状態の輻射寿命によって決まる．自発パラメトリック下方変換の場合，発生した光子（シグナル及びアイドラ光子）は位相整合条件で決まる比較的広いスペクトル幅をもち，その相関時間はスペクトル幅の畳み込みの逆数程度の幅（典型的な条件においては 100 fs 程度）をもつ．

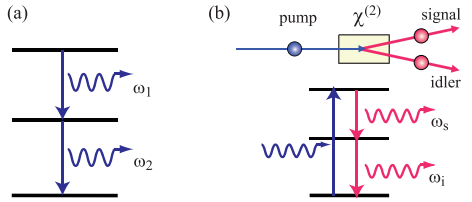

図 1･10　相関光子発生の概念図．(a) 3 **準位系，及び** (b) **パラメトリック下方変換**

(2) 相関光子を用いた単一光子（伝令付き光子）状態の生成

電子系のフェルミオン性を利用して直接単一光子を発生する方法については上述したが，実用上「単一」と見なせる光子状態は，相関光子対から生成することができる．例えば，パラメトリック下方変換によって発生した光子対のうち，アイドラ光子が検出されたことを条件としたときのシグナル光子の状態を考える．このとき，励起光強度を十分に弱くした上，アイドラ光子を検出した際にシグナル光子を観測する時間幅を十分に短くすることにより，シグナル光子の状態に全く光子が含まれない割合及び 2 光子以上が含まれる割合を実用上無視できる程度まで小さくし，近似的な単一光子（伝令付き光子）状態を実現できる[19]．相関光子対を利用した伝令付き光子はパラメトリック下方変換を用いて比較的簡便に発生させることができるため，量子暗号などの量子情報通信プロトコルにおいて，安全性や効率を高めるためにしばしば利用される．

(3) 量子もつれ光子の発生

物理量の間に古典的には説明できないような量子的相関（量子もつれ: エンタングルメント）をもつような光子対を，量子もつれ光子と呼ぶ．量子もつれ光子の発生とその検出方法については，解説論文[20]に詳しいが，ここでは，それらのなかでも最も基本的な，偏光に関する量子もつれ光子対の発生方法について概観する．以下では，2 光子の偏光状態を表す記号として，|HV⟩ などを用いる．ここで，2 個の英字は各々の光子の偏光状態を表し，H, V は各々水平, 垂直方向の直線偏光，L, R は各々左回り及び右回りの円偏光を表すものとする．

量子もつれは，原子からカスケード放出される光子対を用いて初めて確認された．例えば，^{40}Ca 原子の三つの準位間のカスケード遷移では，原子系の角運動量変化（$J = 0 \to 1 \to 0$）を反映して，放出される 2 光子の間に偏光に関する量子もつれが生じる．このとき，互いに逆方向に放出される光子対を検出すると，それらの偏光状態は

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\mathrm{LL}\rangle + |\mathrm{RR}\rangle) = \frac{1}{\sqrt{2}}(|\mathrm{HH}\rangle - |\mathrm{VV}\rangle) \qquad (1\cdot9)$$

のような量子もつれ状態となる．アスペ（Aspect）らはこの光源を用いて 2 光子の偏光相関の測定を行い，ベルの不等式が明らかに破れていることを初めて示した[21]．

量子もつれ光子対の発生方法として今日最も頻繁に用いられる方法は，パラメトリック下方変換と呼ばれる非線形光学過程である．図 1･10(b) に示すように，この過程では，2 次の非線形感受率（$\chi^{(2)}$）を有する非線形光学結晶によって入射光子 1 個が 2 個の光子に変換されるが，その際に生成された光子の物理量の間には強い相関がある．特に，位相整合条件を上手く用いることによって，種々の方法で偏光に関する量子もつれ光子を発生することができる[20]．この方法を用いると良質な量子もつれ光子対を比較的簡便に発生させることができるため，量子情報通信に関連した様々な原理検証実験に広く用いられている．

これらの方法はいずれも，光励起によって量子もつれ光子対を発生させるものであった．これらの方法に対し，将来的には電流励起が可能となる半導体を用いた光源の開発が強く望まれる．半導体中に励起子（exciton）が 2 個生成されると，強い相互作用によって電子・正孔 2 対が結合した励起子分子（biexciton）と呼ばれる状態が生じる．励起子分子から励起子を経由して基底状態へと遷移するカスケード遷移を用いると，原子カスケード放出とほぼ同じ原理を用いて偏光に関する量子もつれ光子対を生成できる[22]．図 1･11 に示すように，この過程では電子状態の角運動量が励起子分子（$J = 0$）から中間状態である励起子（$J = 1$）を経て終状態である基底状態（$J = 0$）へと変化する．従って，その角運動量変化（$J = 0 \to 1 \to 0$）を反映して，同じ方向へ放出される 2 光子の偏光状態は

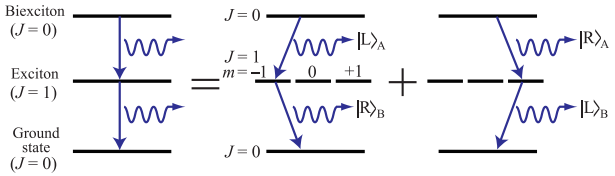

図 1･11　励起子分子からのカスケード遷移による量子もつれ光子対発生の概念図

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\mathrm{LR}\rangle + |\mathrm{RL}\rangle) = \frac{1}{\sqrt{2}}(|\mathrm{HH}\rangle + |\mathrm{VV}\rangle) \qquad (1\cdot10)$$

となる*．この方法を用いて，CuCl バルク結晶中の励起子分子を用いた量子もつれ光子の発生が確認された[23, 24]．一方，量子ドット中の励起子分子を利用することにより，単一光子発生と同様に「単一の」光子対発生が期待される．しかし，通常の方法で作製される量子ドットでは，その形状異方性のために H 偏光と V 偏光とで放出光子のエネルギーがわずかに異なり，|HH⟩ と |VV⟩ との間のコヒーレンスが失われて量子もつれ状態が壊れてしまう問題点が知られていた[25]．最近，形状異方性を小さくした量子ドットに横磁場を印加して H, V 成分のスペクトルを一致させる方法[26]や，分裂したスペクトルの中間の光子エネルギー領域のみを選択して観測する方法[27]などによって，量子もつれを観測した例が報告された．更に，この方法で発生した光子対の単一性も観測されている[28]．

また，二つの単一光子状態の重ね合せを利用することによって量子もつれ光子対を生成することもできる．二つの同期した単一光子源を用意し，一方からは H 偏光，他方からは V 偏光の単一光子を，無偏光ビームスプリッタ（50 %透過 50 %反射）の両側から入射・合成する．このとき，2 光子が二つのポート A 及び B に分かれて出力された状態のみを取り上げれば（post-selection），出力の状態は

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\mathrm{HV}\rangle + |\mathrm{VH}\rangle) \qquad (1\cdot11)$$

すなわち量子もつれ状態となる．この方法による量子もつれ光子の発生は，パラメトリック下方変換によって発生した光子対を用いて行われたのが最初である[29]が，その後，半導体量子ドットから発生した単一光子パルス列に対しても応用された[30]．この過程で重要なことは，二つのパルスを干渉させるために，それらの間に偏光以外の識別がつかないことが要請されることである．そのためには，単一光子状態は位相緩和のないフーリエ限界パルスとして出力されていなければならない．高品質な量子ドットでは，その発光スペクトル幅はほぼ輻射寿命で決定され，上記の要請を満たすことが知られている[30]．Post-selection を用いているため，この方法による量子もつれの発生は決定論的な方法ではないが，相関をもたない二つの単一光子から量子もつれを生成できる点が特長である．

1-5-3 展望

今後の量子情報通信技術の進展にとって，高性能かつ簡便な単一光子源及び相関（量子もつれ）光子源の開発はたいへん重要である．従来，これらの光源は光励起によるものが主流であったが，電流励起した量子ドットからの単一光子発生が報告されるなど，半導体を用いた単一光子，量子もつれ光子の光源技術が急速に進展している．従来の光通信技術を支えてきた光源である LED（light emitting diode）や LD（laser diode）のように，単一光子を発生する SPED（single photon emitting diode）や量子もつれ光子を発生する EPED（entangled photon emitting diode）が実用化され，量子情報通信技術の更なる発展につながることを期待

* 式 (1･9) と円偏光相関の組合せが違うのは，式 (1･9) では逆方向に放出される光子対を，式 (1･10) では同方向に放出される光子対を考えているからである．

したい.

■参考文献

1) R. Loudon, “The quantum theory of light,” 3rd ed., Oxford University Press, Oxford, 2000.
2) H.J. Kimble, M. Dagenais, and L. Mandel, “Photon antibunching in resonance fluorescence,” Phys. Rev. Lett., vol.39, no.11, pp.691-695, 1977.
3) F. Diedrich and H. Walther, “Nonclassical radiation of a single stored ion,” Phys. Rev. Lett., vol.58, no.3, pp.203-206, 1987.
4) T. Basché, W.E. Moerner, M. Orrit, and H. Talon, “Photon antibunching in the fluorescence of a single dye molecule trapped in a solid,” Phys. Rev. Lett., vol.69, no.10, pp.1516-1519, 1992.
5) B. Lounis and W.E. Moerner, “Single photons on demand from a single molecule at room temperature,” Nature, vol.407, no.6803, pp.491-493, 2000.
6) R. Brouri, A. Beveratos, J.-P. Poizat, and P. Grangier, “Photon antibunching in the fluorescence of individual color centers in diamond,” Opt. Lett., vol.25, no.17, pp.1294-1296, 2000.
7) P. Michler, A. Imamoglu, M.D. Mason, P.J. Carson, G.F. Strouse, and S.K. Buratto, “Quantum correlation among photons from a single quantum dot at room temperature,” Nature, vol.406, pp.968-970, 2000.
8) B. Lounis, H.A. Bechtel, D. Gerion, P. Alivisatos, and W.E. Moerner, “Photon antibunching in single cdse/zns quantum dot fluorescence,” Chem. Phys. Lett., vol.329, nos.5-6, pp.399-404, 2000.
9) P. Michler, A. Kiraz, C. Becher, W.V. Schoenfeld, P.M. Petroff, L. Zhang, E. Hu, and A. Imamoglu, “A Quantum Dot Single-Photon Turnstile Device,” Science, vol.290, no.5500, pp.2282-2285, 2000.
10) C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, “Triggered single photons from a quantum dot,” Phys. Rev. Lett., vol.86, no.8, pp.1502-1505, 2001.
11) S. Masuo, A. Masuhara, T. Akashi, M. Muranushi, S. Machida, H. Kasai, H. Nakanishi, H. Oikawa, and A. Itaya, “Photon antibunching in the emission from a single organic dye nanocrystal,” Jpn. J. Appl. Phys., vol.46, no.12, pp. L268-L270, 2007.
12) D.F. Walls, “Evidence for the quantum nature of light,” Nature, vol.280, no.5722, pp.451-454, 1979.
13) R. Loudon, “Non-classical effects in the statistical properties of light,” Rep. Prog. Phys., vol.43, no.7, pp.913-949, 1980.
14) B. Lounis and M. Orrit, “Single-photon sources,” Rep. Prog. Phys., vol.68, no.5, pp.1129-1179, 2005.
15) Z. Yuan, B.E. Kardynal, R.M. Stevenson, A.J. Shields, C.J. Lobo, K. Cooper, N.S. Beattie, D.A. Ritchie, and M. Pepper, “Electrically Driven Single-Photon Source,” Science, vol.295, no.5552, pp.102-105, 2002.
16) T. Miyazawa, K. Takemoto, Y. Sakuma, S. Hirose, T. Usuki, N. Yokoyama, M. Takatsu, and Y. Arakawa, “Single-photon generation in the 1.55-μm optical-fiber band from an InAs/InP quantum dot,” Jpn. J. Appl. Phys., vol.44, no.20, pp.L620-L622, 2005.
17) K. Takemoto, M. Takatsu, S. Hirose, N. Yokoyama, Y. Sakuma, T. Usuki, T. Miyazawa, and Y. Arakawa, “An optical horn structure for single-photon source using quantum dots at telecommunication wavelength,” J. Appl. Phys., vol.101, no.8, p.081720, 2007.
18) S. Kako, C. Santori, K. Hoshino, S. Gotzinger, Y. Yamamoto, and Y. Arakawa, “A gallium nitride single-photon source operating at 200 K,” Nat. Mater., vol.5, no.11, pp.887-892, 2006.
19) P. Grangier, G. Roger, and A. Aspect, “Experimental evidence for a photon anticorrelation effect on a beam splitter, A new light on single-photon interferences,” Europhys. Lett., vol.1, no.4, pp.173-179, 1986.
20) K. Edamatsu, “Entangled photons, generation, observation, and characterization,” Jpn. J. Appl. Phys., vol.46, no.11, pp.7175-7187, 2007.

21) A. Aspect, P. Grangier, and G. Roger, “Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment, A new violation of bell’s inequalities,” Phys. Rev. Lett., vol.49, no.2, pp.91-94, 1982.
22) O. Benson, C. Santori, M. Pelton, and Y. Yamamoto, “Regulated and entangled photons from a single quantum dot,” Phys. Rev. Lett., vol.84, no.11, pp.2513-2516, 2000.
23) K. Edamatsu, G. Oohata, R. Shimizu, and T. Itoh, “Generation of ultraviolet entangled photons in a semiconductor,” Nature, vol.431, no.7005, pp.167-170, 2004.
24) G. Oohata, R. Shimizu, and K. Edamatsu, “Photon polarization entanglement induced by biexciton, Experimental evidence for violation of Bell’s inequality,” Phys. Rev. Lett., vol.98, no.14, p.140503, 2007.
25) C. Santori, D. Fattal, M. Pelton, G.S. Solomon, and Y. Yamamoto, “Polarization-correlated photon pairs from a single quantum dot,” Phys. Rev. B, vol.66, no.4, p.045308, 2002.
26) R.M. Stevenson, R.J. Young, P. Atkinson, K. Cooper, D.A. Ritchie, and A.J. Shields, “A semiconductor source of triggered entangled photon pairs,” Nature, vol.439, no.7073, pp.179-182, 2006.
27) N. Akopian, N.H. Lindner, E. Poem, Y. Berlatzky, J. Avron, D. Gershoni, B.D. Gerardot, and P.M. Petroff, “Entangled photon pairs from semiconductor quantum dots,” Phys. Rev. Lett., vol.96, no.13, p.130501, 2006.
28) R.J. Young, R.M. Stevenson, P. Atkinson, K. Cooper, D.A. Ritchie, and A.J. Shields, “Improved fidelity of triggered entangled photons from single quantum dots,” New J. Phys., vol.8, no.2, p.29, 2006.
29) Z.Y. Ou and L. Mandel, “Violation of Bell’s inequality and classical probability in a two-photon correlation experiment,” Phys. Rev. Lett., vol.61, no.1, pp.50-53, 1988.
30) D. Fattal, K. Inoue, J. Vuckovic, C. Santori, G.S. Solomon, and Y. Yamamoto, “Entanglement formation and violation of Bell’s inequality with a semiconductor single photon source,” Phys. Rev. Lett., vol.92, no.3, p.037903, 2004.

■S2 群 - 5 編 - 1 章

1-6 光子検出器技術

（執筆者：武居弘樹）[2008 年 5 月 受領]

単一光子検出は量子光学や光計測などの分野において重要な要素技術の一つであり，長年にわたって研究，開発されてきた．初期の量子光学実験においては可視近辺の波長の光子が主に使用されてきたが，近年の光ファイバ上での量子鍵配布（quantum key distribution: QKD）システムの進展に伴い，光通信波長帯（1.5 μm 帯）の光子検出が重要な課題となってきた．本節では，光ファイバ上での離散量 QKD システムへの適用を念頭に置いて，代表的な光子検出技術を概観する．

1-6-1 可視域波長帯における光子検出技術:シリコンアバランシェフォトダイオード

p-n または p-i-n フォトダイオードに十分大きい逆バイアスを印加すると，光子の吸収により発生したキャリアが，空乏層内の大きな電界により加速され，impact ionization により電子-正孔対を発生する．この現象がなだれ的に発生することにより，光電子増倍管と同様に光電流が増倍される．これをアバランシェフォトダイオード（avalanche photodiode: APD）と呼ぶ．APD は，光通信などにおいては，降伏電圧よりも小さな逆バイアスを印加し，光電流がほぼ線形に増幅される領域で使用される．しかし，単一光子検出においては通常以下に示すガイガーモード（Geiger mode）と呼ばれる動作条件で用いられる．まず，降伏電圧より大きな逆バイアスを印加する．このとき，APD は熱的に励起されたキャリアもしくは光子の吸収によって生じたキャリアがない場合には，なだれ降伏の起こらない「オフ」状態となっている．ここで光子が入力されると，なだれ降伏が引き起こされる．この動作条件では，1 個の光子の入力によってもなだれ降伏を引き起こすことができるため，単一光子検出器として使用することができる．

シリコン（Si）APD は，可視域から 1 μm の波長帯において，上記のガイガーモード動作に基づく高性能の光子検出器として現在用いられている．波長 700 nm 近辺において量子効率 60 %以上，暗計数率 50 cps 程度の性能の光子検出器が既に市販品として入手可能である．また，なだれ電流を検知すると逆バイアス値を降伏電圧以下になるよう制御するアクティブクエンチ回路[1)]の採用により，10^7 cps を超える計数率での連続的光子計数が可能である．更に，1 μm 程度の薄い空乏層をもつ Si APD を用いて，20 ps 程度の時間分解能をもつ光子検出器も報告されている[1)]．

1-6-2 ゲート動作 InGaAs/InP アバランシェフォトダイオードによる光子検出

前に述べたように，短波長帯においては Si APD が非常によい光子検出器として使用可能であった．残念ながら 1.5 μm 通信波長帯においては Si APD は不感であり，ひ化インジウムガリウム／りん化インジウム（InGaAs/InP）APD が主に用いられている．一般に InGaAs/InP APD は，ガイガーモード動作において熱的に励起されたキャリアによる雑音計数（暗計数）率が大幅に高い．そのため，ガイガーモード動作を光子の検出が予測される時間にのみ間欠的に行うゲートモード動作（gated mode）がこれまで適用されてきた[2, 3)]．

図 1･12(a) に典型的なゲート動作光子検出器の回路図を示す．APD に降伏電圧よりも少し小さな逆バイアスを印加した状態で，矩形の電圧パルスを重畳して降伏電圧よりも大きな

電圧をかける．これにより，電圧パルスが印加されているタイミングで光子が APD に入力されたときにのみなだれ降伏が起こり，光子検出される．本方式を用いると，1 ns 幅のゲートを用いた場合，典型的にはゲート当たりの暗計数率 10^{-5} において 10 %程度の量子効率を得ることができる．このとき，1 秒間当たりに換算した暗計数率は 10^4 cps のオーダとなり，Si APD を用いた光子検出に比べて大幅に大きい．

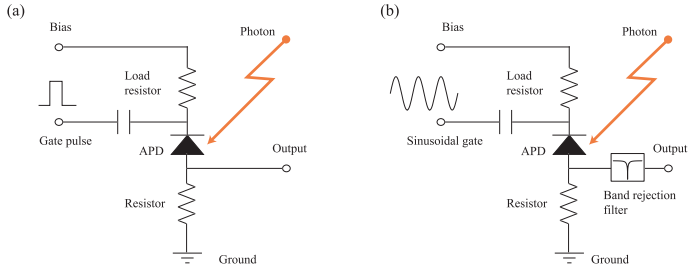

図 1･12　InGaAs/InP APD を用いた光子検出器の回路構成．(a) **ゲート動作光子検出回路．**(b) **正弦波ゲーティング型光子検出回路**

ゲート動作 InGaAs/InP APD を QKD に適用する場合，鍵生成率増大のためにはゲート周波数を増大する必要がある．しかし，アフターパルスと呼ばれる雑音計数が，ゲート高速化により顕著になる．アフターパルスとは，直前のゲートにおいて発生したなだれのキャリアの一部が空乏層中の不純物準位などに捕獲され，次のゲートパルスのタイミングで開放されることにより，光子の入力なしになだれ降伏を引き起こし，誤計数を生じる現象である．これにより，従来のゲート動作におけるゲート周波数は最大 10 MHz 程度に制限されている[3]．

1-6-3 InGaAs/InP アバランシェフォトダイオード光子検出器の高速化の取組み

前述の矩形波のゲートパルスを用いた従来のゲート動作 InGaAs/InP APD の出力においては，ゲートパルスに対する APD の capacitive response 信号となだれによる出力信号が重畳されている．このため，ゲート電圧の絶対値を大きくし，なだれにより発生するキャリア数を増やして，なだれによる信号が capacitive response より大きくなるようにする必要がある．ところが，発生キャリア数が増加すると，APD 中の不純物準位にキャリアが捕獲される確率も増えるため，アフターパルス率が増大する．

一方，図 1･12(b) に示す正弦波ゲーティング法[4]では，矩形波のゲートパルスの替わりに，正弦波信号を DC の逆バイアスに重畳して APD に印加する．このとき，ゲート信号に対する APD の capacitive response もまた正弦波となるから，信号出力において本正弦波信号を抑圧する帯域除去フィルタを挿入することにより，効率よく除去することができる．これによって，より小さなゲート信号により発生したなだれを検出することが可能となる．そのため，ゲート電圧を下げることができ，アフターパルス率が低下する．一定のアフターパルス率のもとでは，ゲート周波数を増大することが可能となる．本方式により，800 MHz のゲート周波数において，量子効率 8.5 %，暗計数率～10^{-5}，アフターパルス率 6 %での光子検出が報告されている[4]．更に，本手法を用いた高速 QKD 実験が行われ，15 km のファイバ伝

送距離において 1.5 Mbit/s のシフト鍵生成を実現している[5].

自己差分回路を用いた手法も報告されている[6]．本手法では，従来どおり矩形波のゲートを用いる．出力信号を 2 分岐し，一方にゲート周期分の遅延を与えた後，2 信号の差を取る．これにより，APD の capacitive response を効率よく除去し，小さなだれを検出することが可能となる．本手法では，1.25 GHz のゲート周波数において，量子効率 10.8 %，暗計数率 2.5×10^{-6}，アフターパルス率 6.2 %が得られている[6].

1-6-4 光周波数変換を用いた光子検出

図 1･13 に示す周波数上方変換型単一光子検出器（up-conversion detector: UCD）は，1.5 μm 光子を短波長帯に光周波数変換し，Si APD で受信することにより，Si APD の高い性能を活かした光子検出を行うものである[7]．受信信号である波長 1550 nm の単一光子と，波長 1319 nm のポンプ光を周期分極反転ニオブ酸リチウム（periodically poled lithium niobate: PPLN）導波路に入力する．PPLN 導波路中の和周波発生過程（sum frequency generation: SFG）により，信号光子とポンプ光子の和に相当する波長 715 nm の光子が発生する．波長 715 nm の光子は，プリズムや光フィルタなどを通過させ，残留ポンプ光やポンプ光の 2 次高調波成分などの雑音を除去した後，Si APD で受信する．これにより，高い量子効率，低い暗計数率，ゲートが不要であり連続計数が可能といった Si APD の特徴を活かした光子計数が 1.5 μm 帯において可能となる．文献 7) の実験では，PPLN 導波路の変換効率，Si APD の量子効率，及び系の光学的損失を含めたネット量子効率が最大で 46 %に達している．

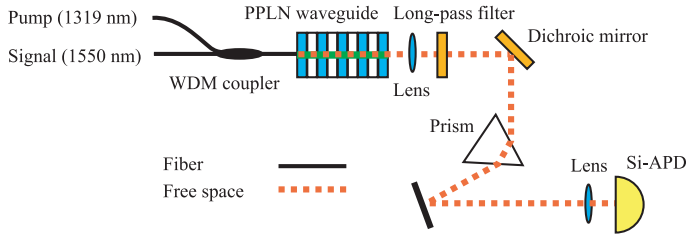

図 1･13　周波数上方変換型単一光子検出器の構成

本方式における問題点として，雑音光子の発生による暗計数の増加が指摘されている．これは，非線形媒質中で自然放出ラマン散乱などにより発生した 1.5 μm 帯に雑音光子に起因する．この雑音光子が SFG により短波長帯に波長変換され，Si APD により検出されることにより暗計数が増大する．雑音光子による暗計数はポンプ光の強度に対してほぼ 2 次関数状に増大するが，ポンプ光強度が比較的低い場合は量子効率はポンプ光強度に対しほぼ線形に増大する．そのため，ポンプ光強度を下げて量子効率を減少させると，信号対雑音比は向上し，長距離 QKD 実験への適用が可能となる．文献 8) では，量子効率 0.4 %，暗計数率 350 cps で UCD を動作させ，100 km の伝送距離での QKD に成功している．

1-6-5 超伝導単一光子検出器

超伝導単一光子検出器（superconducting single photon detector: SSPD）は，低暗計数かつ高時間分解能の光子検出器として近年注目を集めている[9, 10, 11]．ここでは，現在最も研究が進んでいる窒化ニオブ（NbN）細線を用いた SSPD について説明する．厚さ 4 nm，幅 100 nm 程度のメアンダ状の NbN 細線（図 1･14(a)）を約 4 K に冷却し超伝導状態にして，臨界電流より少し低い電流を印加する．このとき，超伝導状態であるため細線の両端間の出力電圧は 0 である．光子が細線に入射すると，細線中のクーパー対が破壊され，部分的に常伝導状態（ホットスポット）ができる（図 1･14(b)）．電流はホットスポットを避けて流れるため，ホットスポット周縁部の電流密度が増大し臨界電流を超える．その結果，新たなホットスポットが発生する．このようにホットスポット部分は増大し，最終的に細線が完全にホットスポットにより遮断され，出力電圧が発生する．出力電圧の発生を閾値検出することにより，光子を検出できる．その後，ホットスポット中の励起電子がエネルギー緩和過程を経て再び超伝導状態となるため，出力電圧も再び 0 に戻る．細線中の励起電子のエネルギー緩和過程は一般に非常に高速であり，NbN の場合 30 ps 程度である[9]．これにより，高速かつ高い時間分解能での光子検出が可能である．文献 12) では，時間分解能 60 ps での光子検出が報告されている．また，暗計数率が非常に小さいことも特徴であり，10 Hz 以下の暗計数率が報告されている．

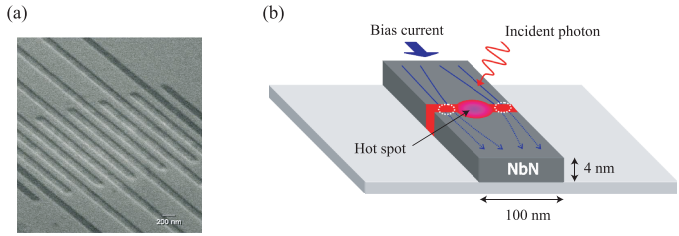

図 1･14　SSPD．(a) **素子の** SEM **写真 (写真提供**: NIST)．(b) **動作原理**

現状の最大の課題は量子効率が比較的低いことである．光ファイバと結合したシステムでは，ネット量子効率は波長 1.5 μm において 1 %程度にとどまっている．これは，ファイバと結合する際の結合損に加え，表面反射による損失が大きく影響していると考えられる．これを解決するために，キャビティ構造を採用することにより光子の吸収効率を増大し，量子効率が改善可能であることを示唆した報告がなされている[13]．

SSPD の高時間分解能と低暗計数特性は，長距離の QKD システムを実現するために大変有効である．現在の QKD の伝送距離の世界記録（200 km）は SSPD を用いて達成された[12]．

1-6-6 まとめ

光子検出器の量子効率を η，ダークカウント率〔Hz〕を d，時間分解能を τ とすると，QKD の鍵生成率は η/τ（ただし，ゲート動作型光子検出器の場合，$1/\tau$ を最大ゲート周波数で置き換える）に，最大鍵配送距離は $\eta/\tau d$ に比例する．これを基にした単純な性能比較では，SSPD が現在 QKD に最も有効な光通信波長帯用光子検出器であるといえる．もちろん，実際のシ

ステム構築に当たっては信頼性，コンパクト性，価格なども考慮に入れる必要がある．

以上，QKD において重要な要素技術である光子検出器について，光通信波長帯用光子検出器を中心に概説した．なお，本稿では項数の都合上，光子数識別可能な光子検出器について触れることができなかった．このような検出器は，量子計算など，より高度な量子情報処理において有用である．ご興味のある方は，文献 14) にあげた解説を参考にしていただきたい．

■参考文献

1) S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, “Avalanche photodiodes and quenching circuits for single-photon detection,” Appl. Opt., vol.35, p.1956, 1996.
2) G. Ribordy, J. D. Gautier, H. Zbinden, and N. Gisin, “Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters,” Appl. Opt., vol.37, p.2272, 1998.
3) 吉澤明男, “光ファイバ通信帯での単一光子検出器,” OPTRONICS, vol.285, p.158, 2005.
4) N. Namekata, S. Sasamori, and S. Inoue, “800 MHz single photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating,” Opt. Express, vol.14, p.10043, 2006.
5) N. Namekata, G. Fujii, S. Inoue, T. Honjo, and H. Takesue, “Differential phase shift quantum key distribution using single-photon detectors based on a sinusoidally gated InGaAs/InP avalanche photodiode,” Appl. Phys. Lett., vol.91, p.011112, 2007.
6) 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., vol.91, p.041114, 2007.
7) C. Langrock, E. Diamanti, R.V. Roussev, Y. Yamamoto, M.M. Fejer, and H. Takesue, “Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled LiNbO3 waveguides,” Opt. Lett., vol.30, p.1725, 2005.
8) E. Diamanti, H. Takesue, C. Langrock, M.M. Fejer, and Y. Yamamoto, “100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors,” Opt. Express, vol.14, p.13073, 2006.
9) G.N. Gol’tsman, O. Kunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, C. Williams, and R. Sobolewski, “Picosecond superconducting single-photon optical detector,” Appl. Phys. Lett., vol.79, p.705, 2001.
10) R.H. Hadfield, M.J. Stevens, S.S. Gruber, A.J. Miller, R.E. Schwall, R.P. Mirin, and S.W. Nam, Opt. Express, vol.13, p.10846, 2005.
11) 王鎮, 三木茂人, 藤原幹生, 佐々木雅英, “量子情報通信用超伝導ナノワイヤー単一光子検出器,” 光学, vol.36, p.375, 2007.
12) H. Takesue, S.W. Nam, Q. Zhang, R.H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, “Quantum key distribution over 40 dB channel loss using superconducting single-photon detectors,” Nat. Photonics, vol.1, p.343, 2007.
13) K.M. Rosfjord, J.K.W. Yang, E.A. Dauler, A.J. Kerman, V. Anant, B.M. Voronov, G.N. Gol’tsman, and K.K. Berggren, “Nanowire single-photon detector with and integrated optical cavity and anti-reflection coating,” Opt. Express, vol.14, p.527, 2006.
14) 佐々木雅英, 松岡正浩監修, 量子情報通信 第 4 部 第 2 章, オプトロニクス社, 2006.