博士学位論文

量子もつれを用いた高次元量子鍵配送のための
スケーラブルなタイムビン量子状態制御

生田　拓也

2023 年 1 月

大阪大学大学院工学研究科

内容梗概

本論文は，筆者が大阪大学 大学院工学研究科 電気電子情報通信工学専攻に在学中および NTT 物性科学基礎研究所においておこなった，量子もつれを用いた高次元量子鍵配送のためのスケーラブルなタイムビン量子状態制御に関する研究をまとめたものであり，以下の 6 章で構成される．

第 1 章は序論であり，本研究の背景として，量子コンピュータ技術の発展などに伴う現代暗号通信の抱えるリスクと，その対策としての量子鍵配送 (QKD) 技術，また近年の高次元量子状態を用いた QKD の研究について述べる．QKD は，どのような計算機を用いても解読不可能な，ワンタイムパッド暗号のための共通鍵を配布する手法である．量子もつれ状態と呼ばれる特異な相関特性を持つ光子対を用いると，QKD システムが実装可能なだけでなく，その安全性を相関特性に基づいて証明することが可能である．QKD としては 2 次元量子状態 (2 値の物理量を取る量子状態) を用いたシステムが長年研究されているが，近年，秘密鍵生成率の向上を目的として，高次元量子状態 (多値の物理量を取る量子状態) を用いた QKD システムの研究が活発化している．様々な光のモードを利用した高次元量子状態が検討されている中で，タイムビン量子状態は光ファイバ伝送中の擾乱に強く，通信に適した量子状態として知られる．序論では，2 次元 QKD システムや様々な光のモードを用いた研究などを概観し，通信の基本三要素である信号の生成/伝送/測定の観点から，高次元タイムビン量子もつれ状態を用いる本研究の位置づけを明確化する．

第 2 章では，まずタイムビン量子状態や量子もつれ状態の定義，後の章の基盤となる状態密度演算子や測定演算子の意味，量子もつれ状態が持つ特異な相関特性などの，量子情報理論の基礎的事項について述べる．また，2 次元量子もつれ QKD の代表的なプロトコルの一つである BBM92 およびその安全性証明の概略について紹介し，高次元 QKD への拡張やその安全性を議論するための基礎とする．

第 3 章では，高次元量子もつれ状態を実験的に検証するために用いられる CGLMP 不等式について議論する．まず，量子もつれ状態が持つ特異な相関特性を検証するためのベル不等式を紹介し，古典的な相関を記述する隠れた変数理論では説明不可能な測定値の相関が得られることを，2 次元量子もつれ状態の場合について紹介する．この不等式を高

次元量子もつれ状態に拡張した CGLMP 不等式の場合，量子情報理論でしばしば用いられる最大量子もつれ状態ではなく，CGLMP 不等式のために最適化した量子もつれ状態により不等式の大きな破れが得られる．このような最適化した量子もつれ状態を，高次元タイムビン量子状態の場合に簡便かつ安定に生成/測定する手法について述べたのち，CGLMP 不等式の破れおよび最適化による破れの増大を実験的に検証する．これにより，高次元タイムビン量子もつれ状態が特異な相関特性を示すこと，最適化による差が明確に確認できるほどに安定した状態制御が可能であることを実証する．

第 4 章では，量子状態トモグラフィー (QST) と呼ばれる，高次元タイムビン量子状態を記述する状態密度演算子の推定法を提案し，この手法により高次元タイムビン量子もつれ状態の 100km 伝送後の特性を評価する．量子もつれ状態を通信プロトコルに応用するには，光ファイバを介した量子状態の長距離伝送が不可欠であるが，この場合，伝搬損失により光子が失われるために，伝搬後の量子状態測定は長時間化する．提案手法を用いることで，少ない装置数および設定パラメータ数で測定が可能となることを示す．また，QST により得られた状態密度演算子から様々な物理量/情報量を見積もることで，伝送後における高次元タイムビン量子状態の 2 次元量子状態に対する優位性を示す．

第 5 章では，高次元量子状態を用いた QKD プロトコルの一つである，$(d+1)$ 測定基底 QKD プロトコルとその実装法について議論する．d 次元量子状態の場合には，$(d+1)$ 種類の測定系を用いることにより，2 つの測定系しか用いない QKD プロトコルよりも高い秘密鍵生成率を達成することができる．これまで，このようなプロトコルの安全性証明は次元数 d が素数の場合に限られていた．そこでまず，有限体を利用した一般化 Weyl 演算子，一般化ベル基底および対応する測定基底である相互不偏基底 (MUB) を用いることにより，安全性証明の適用可能範囲を素数の累乗次元に拡張する．また，この証明に利用される MUB を高次元タイムビン量子状態に対して効率的に実装する手法を提案する．4 次元タイムビン量子状態に対して提案手法を実装し，$(d+1)$ 測定基底 QKD プロトコルに適用可能な低いシンボルエラーレートを達成できることを示す．

第 6 章は，本論文の結論であり，本研究で得られた結果を総括する．

謝辞

本論文は，大阪大学 大学院工学研究科 電気電子情報通信工学専攻教授 井上恭博士の御指導の下，筆者が大阪大学 大学院工学研究科 電気電子情報通信工学専攻在学中および日本電信電話株式会社 NTT 物性科学基礎研究所において行った研究をまとめたものである．本研究を進めるにあたり井上教授から賜った多くの御教示，御鞭撻に対し，深く感謝の意を表する．

ならびに，本研究を遂行し研究成果をまとめるにあたり，多くの御教示，御助言を頂いた大阪大学 大学院工学研究科 電気電子情報通信工学専攻教授 丸田章博博士，同准教授 五十嵐浩司博士に深く感謝の意を表する．

また，講義等を通じ情報通信工学の各分野に関して多大な御指導を頂いた大阪大学 大学院工学研究科 電気電子情報通信工学専攻教授 滝根哲哉博士，同教授 三瓶政一博士，同教授 宮地充子博士，同教授 鷲尾隆博士，同教授 駒谷和範博士をはじめとする先生方に厚く感謝を申し上げる．

本研究遂行にあたり，量子光学・量子通信実験について多くの御指導，御協力を頂いた日本電信電話株式会社 NTT 物性科学基礎研究所 上席特別研究員 武居弘樹博士，同主幹研究員 本庄利守博士，同主任研究員 Hsin Pin Lo 博士，同研究員 米津佑哉博士，また研究業務支援として多くの御協力を頂いた同主任研究員 田村浩之博士をはじめとする諸兄に厚く感謝を申し上げる．

また，常日頃から量子情報理論について議論を交わすとともに，量子鍵配送の安全性証明について多くの議論を頂いた日本電信電話株式会社 NTT コミュニケーション科学基礎研究所 研究主任 秋笛清石博士に深く感謝の意を表する．

最後に，COVID-19 流行下での学業・研究遂行において大きな精神的支えとなってくれた友人達，そして常日頃より惜しみない援助と進学への理解を頂いた私の家族に心より御礼申し上げる．

目次

図目次

表目次

第 1 章

序論

現代の情報社会の安全性を保証するうえで，通信の暗号化は必要不可欠である．現代暗号で広く使われている公開鍵暗号の安全性は，一方向性関数と呼ばれる計算量が非対称である関数の性質を拠り所としている．例えば，代表的な公開鍵暗号である RSA 暗号は，素数の積の計算は容易である一方，その逆過程である素因数分解は現代コンピュータでは困難であることを利用して安全性を保証している．これに対し，近年開発が活発化している量子コンピュータ [1, 2] を用いて，Shor のアルゴリズム [3] と呼ばれる量子力学の性質を利用したアルゴリズムを実行すると，素因数分解が多項式時間で解けることが知られている．ただし，一部エラーが生じても正しく計算される誤り耐性量子コンピュータの実現には技術的な課題がまだ多く，ただちに公開鍵暗号が解読されるというわけではない．さらには，量子コンピュータに対しても安全性を保証するポスト量子暗号と呼ばれる暗号技術の研究も盛んにおこなわれているが，基本的には計算量的安全性に基づいており，新規のアルゴリズムにより暗号が解読されるリスクからは逃れられない．上記の公開鍵暗号方式に対し，共通鍵暗号の一つであるワンタイムパッド暗号は，情報理論的に安全であり，どのような計算機やアルゴリズムを用いても絶対に解読が不可能なことが数学的に証明されている [4]．ただし，非常に強固な安全性を持たせるために，送信情報と同じビット数の乱数列を共通鍵として 1 回だけ使用するものとしている．そのため，乱数列をどのように安全かつ効率的に送受信者間で共有するかがワンタイムパッド暗号通信の重要な課題となる．

量子鍵配送 (QKD：Quantum Key Distribution) は量子状態のもつ性質を利用して，ワンタイムパッド暗号のための乱数列を離れた 2 者間で共有する技術である．例えば，最初に提案された QKD プロトコルである BB84[5] では，量子力学的な光の状態である光子の 2 次元基底状態，およびその重ね合わせ状態に 0 と 1 のビット情報をエンコードした量子ビットを用いて，乱数列を共有する．特定の基底状態のみを使って共有する乱数列は容易に盗聴可能であるが，重ね合わせ状態を含めた一般的な量子状態をコピーすると，

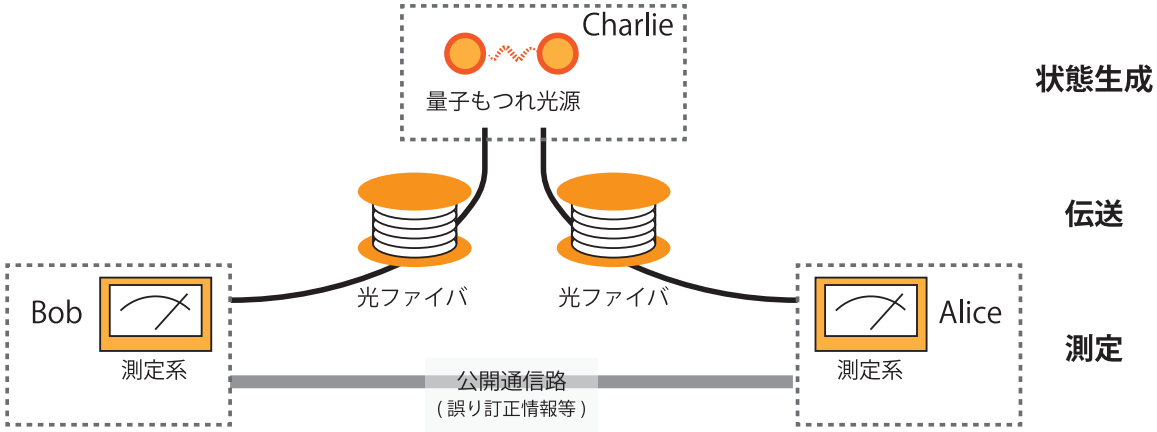

図 1.1　量子もつれ状態を用いた QKD の模式図

ノークローニング定理 [6] により量子状態が変化してビットエラーが生じる．そのため，通信エラーから盗聴量の上限を見積もることができ，データ処理によりその分を除外することにより安全な鍵を共有することが可能である．

BB84 は，送信者 Alice が 1 光子の量子状態を準備して受信者 Bob が量子状態を測定する，Prepare and Measure (P&M) 型の非対称な QKD プロトコルである．一方，図 1.1 に示すように，量子もつれ状態 [7] という量子力学的な相関をもった 2 光子状態を第三者 Charlie が用意し，Alice と Bob がともに量子もつれ状態に対する測定を行うことで乱数列を共有する，BBM92 と呼ばれる対称形のプロトコルが知られている [8]．このようなプロトコルは，P&M 型に対して Entanglement-based (EB) 型のプロトコルと呼ばれる．BBM92 で用いられる 2 光子量子もつれ状態は最大もつれ状態と呼ばれる状態 (ベル基底状態とも呼ばれる) であり，第 2 章で詳しく議論するように，次のような性質をもつ．

- 各光子を Alice，Bob が各々測定した結果は完全にランダムである．
- 一方の測定結果を得ると，他方の量子状態が一意かつ瞬時に定まるという相関性がある．
- もつれを構成する 2 光子以外とは一切の相関を持たない．

1 番目と 2 番目の性質より，Alice が測定を行った後の Bob が持つ光子の状態は，ランダムに量子状態を準備することで得られる量子状態と等価とみることができる．Charlie ではなく Alice 自身が量子もつれ状態を準備すると，これは BB84 における Alice の状態準備と同じである．そのため，安全性を理論的に考察する上では，BB84 と BBM92 は等価なプロトコルといえる．一方，実装上は，システム構成や用いる光源に差異がある．P&M 型は，通常の光通信で用いられる装置により送信系を実装できるが，状態生成のた

めに数百 MHz から GHz クロックで動作する真の乱数源を必要とする．また一般に微弱コヒーレント光を疑似的な単一光子として用いるために，光子数分岐攻撃と呼ばれる盗聴に対して脆弱であり，それに対処するためデコイ法 [9–11] と呼ばれる対策が必要となる．これにはランダムな強度変調および位相変調が必要であり，送信系が複雑化する．これに対し EB 型は，量子もつれ状態生成のために特殊な非線形光学結晶を必要とする一方，状態生成に関する乱数生成やランダムな強度変調/位相変調などは不要である．また，BB84 の安全性を BBM92 との等価性に基づいて論じる際には，Alice が生成する状態について，平均的な生成状態が基底によらないなどの仮定を置くことになる一方，BBM92 の安全性証明にはそのような制約がない．さらに，BBM92 は Alice と Bob の位置づけが対称的であるため，Charlie をセンターノードとするスター型ネットワークを構成すれば，要求に応じて通信相手を切り替えることができる．

BBM92 では，前記ベル基底状態の 2 番目の性質を利用して共通鍵を生成する．すなわち，Alice と Bob は特定の対となる測定手法を用いて各光子を測定することにより共通の乱数を得る．さらに，モノガミー性として知られる 3 番目の性質により，得られた共通乱数の情報は外部に一切漏洩していない，すなわち秘密鍵であることが証明される．ただし，これらの性質は理想的なベル基底状態の場合である．不完全な量子もつれ状態についての安全性証明にはさらなる工夫が必要であるが，量子もつれ蒸留という処理を用いた証明方法 [12–14] では，不完全な量子もつれ状態から純粋量子もつれ状態を抽出する手順を追加し，純粋量子もつれ状態の特性をもとに QKD の安全性を証明している．

量子もつれ蒸留を用いた安全性証明の概略は次の通りである．この証明において，鍵共有過程は通信路を介して量子もつれ状態を共有することと等価とみなす．通信路は盗聴行為や外部環境からのノイズなどの影響を受けるため，Alice，Bob 間で共有される量子もつれ状態は不完全なものとなる．第 2 章で詳しく述べるが，不完全な量子もつれ状態は，時間位置エラーと位相エラーの 2 種類のエラーを複合的に伴う 4 種の量子もつれ状態により記述できる．ここで，CSS 符号 [1] と呼ばれる量子誤り訂正符号を用いると，この 2 種類のエラーに対するシンドローム測定によって，各エラーがどの光子に対して生じたかを検出することができる．測定により一部の量子ビットは失われるものの，検出したエラーパターンに応じて誤りを訂正することで，シンドローム測定時に失われず残った量子もつれ状態を不完全さが補償された純粋な量子もつれ状態とすることができる．先に述べたように，Alice と Bob はエラー訂正後の純粋な量子もつれ状態を特定のペアとなる手法で測定することにより，ランダムかつ同一の乱数列を安全に共有する事ができる．従って，エラー訂正さえ可能であるならば，盗聴者の攻撃を限定することなく，Alice，Bob 間で秘密鍵を共有することができる．なお，CSS 符号の実装には，不完全な量子状態に対する誤り訂正が必要であり，これには量子コンピュータを用いる．ただし，Shor-Preskill の証明 [13] では，この量子誤り訂正を用いる QKD は，ビット誤り訂正と秘匿性増強と呼

ばれる測定後のデータ処理によって等価的に実装できることが示されている．すなわち，量子誤り訂正後に測定を行う手順と，測定後に現代コンピュータによるデータ処理を行う手順がブラックボックス的に等価であり，実際に量子コンピュータを用いる必要はない．これは，意図した量子状態を保持して誤り訂正を行わなくてはならない量子コンピュータと，通常は情報として意味のない乱数の共有を目的とした QKD の違いに起因しており，QKD が実用化に近い技術であることの大きな理由と言える．

以上述べたように，量子もつれ状態は QKD プロトコルに利用できるのみならず，QKD の安全性証明にも密接に関連している．したがって，量子もつれ状態の性質を理解することは，単に量子状態の検証のみならず，QKD の安全性証明の観点からも重要である．

上述のように，QKD では高度な量子技術 (例えば量子コンピューティング) を用いることなく安全性が証明されたシステムが実装可能である．そのため，量子情報技術のなかでももっとも実用化に近い技術の一つと考えられており，多くのプロトコルの提案や原理実証実験が行われ [15–26]，世界各国で QKD ネットワークのテストベッド実験も報告されている [27–30]．ただし，実用化に向けて活発に研究が進められている QKD であるが，これまでは，上述の 0 と 1 の二値の情報である量子ビット，すなわち二次元量子状態を用いたプロトコルが主に研究開発されてきた．これに対し近年，より多くのビット情報を単一光子にエンコードできる高次元量子状態を用いた QKD の研究が活発化している [31–40]．高次元量子状態は，多値の情報を扱うことができる量子状態である．高次元の量子状態を用いると，一つの光子で多ビット情報を送ることが可能であり，これは現代光通信で直交振幅変調 (QAM：Quadrature Amplitude Modulation) の多値度を増加させる際の利点に相当する．さらには，QKD において高次元量子状態を利用すると，秘密鍵生成に必要なエラーレート閾値を改善できることが理論的に知られており [41–44]，QKD の性能改善に繋がることが期待されている．

高次元量子状態としては，時間モードを利用したタイムビン量子状態または時間エネルギー不確定性に基づく量子もつれ状態 [31–33, 45–49]，周波数モードを利用した周波数ビン量子状態 [50–54]，ビーム断面の振幅分布モード (マルチモード多重に相当) を利用した光軌道角運動量 (OAM：Orbital Angular Momentum) 量子状態 [34–36, 55–59]，ビームの空間位置モード (マルチコア多重に相当) を利用した量子状態 [37–40, 60]，さらには偏波などを含めた複数の異なるモードを組み合わせた量子状態 [61–63] など，様々な形態が研究されている．中でも OAM を用いた高次元量子状態は，液晶空間位相変調器 (SLM：Spatial Light Modulator) を用いることにより自由度の高い変調が可能であり，100 次元の量子もつれ状態が実現されている [59]．しかしながら，空間モードは状態を保持したまま伝送することが難しく [64]，QKD へ応用するには多くの技術的課題がある．

これに対しタイムビン量子状態は，光子の時間位置および隣接パルス間の位相差を物理量とする量子状態であるために，ファイバ伝送中の擾乱に対して安定である．また，第 3

章で述べるように，コヒーレンスの高いレーザ光源と非線形光学結晶により，容易に高品質な高次元量子もつれ状態を生成できる．高次元化にあたっては，占有する時間幅が拡がるため，単位時間当たりの状態数は制約されることになる．ただし，実際の伝送装置では，単一光子検出器や検出信号を記録するタイムインターバルアナライザ (TIA：Time Interval Analyzer) によって単位時間当たりの状態測定回数が律速されるため，QKD 性能の大きな劣化要因とはならない．実際に，4 次元のタイムビン量子状態を用いて，26.2 Mbps という QKD としては高速な秘密鍵生成実験が報告されている [32]．しかしながら，QKD の高性能化が期待できる高次元タイムビン量子状態ではあるが，いくつかの原理実証実験が報告されているのみで，高次元量子状態を用いた QKD の高性能特性を最大限引き出す研究はなされていない．

例えば，量子もつれ状態の検証として，隠れた変数理論が長年 2 次元量子もつれ状態について検証されている．秘密鍵として Alice と Bob の間で相関のある乱数列を共有するだけであれば，量子もつれでなくてもコイントスなどの確率事象も利用可能である．この場合の測定結果は元となるコインという変数に紐づいた相関を持ち，これから共通の乱数列が得られる．しかしながら，仮にこのコインの状態を盗聴者 Eve が知ってしまうと，すべての乱数は盗み取られていることになる．一方，第 2 章および第 3 章で詳しく述べるように，純粋な量子もつれ状態が示す相関特性は，このような何らかの変数 (隠れた変数) を媒介する相関特性とは全く異なる．逆に言えば，相関特性が隠れた変数を媒介とするものか否かが，量子もつれ状態であるか否かの指標となる．この課題について，隠れた変数があるとすれば測定結果が満たすべき不等式が知られており，提案者にちなんでベル不等式と呼ばれている [65]．ベル不等式が破られれば量子もつれ状態であるといえる．そのため，ベル不等式の検証は量子もつれ状態生成の検証手法として広く用いられている．ベル不等式の高次元バージョンである CGLMP 不等式 [66] の検証は，これまでいくつかの高次元量子状態について報告されているが [47, 48, 50, 51, 55, 57]，高次元タイムビン量子状態に対する検証はなされていない．また，CGLMP 不等式では，最大もつれ状態よりも，ある種の最適化を施した量子もつれ状態の方がより大きな破れを示すことが理論的に示されているが [50, 57]，最適化による不等式の破れの明瞭な増加は観測されていなかった．

また，QKD システムの実用化には長距離伝送が不可欠である．2 次元量子もつれ状態については，300 km 光ファイバ伝送実験 [67] や人工衛星による 1200 km 伝送実験 [68] など，多数の伝送実験が行われており [69–72]，さらに量子もつれ状態を利用した 100 km 超の量子通信プロトコル実装実験も報告されている [73–76]．100 km というのは，主要エリア間を接続するメトロアクセスネットワークでの利用や，離島間での量子通信が可能となる距離である．一方，これまでの高次元量子もつれ状態の伝送距離は自由空間で 1.2 km，光ファイバで 15 km にとどまっており [52, 63]，長距離伝送の報告例はない．高次

元タイムビン量子状態は，2 次元タイムビン量子状態と同様に，安定な長距離伝送の可能性を有しているが，実際の実験的検証は報告がなかった．

さらに，実際に QKD システムを構築するにあたっては，用いる QKD プロトコルに応じた測定系を実装する必要がある．これまで，BB84/BBM92 の高次元量子状態を用いた QKD への拡張として，2 種類の測定を用いた 2 測定基底 QKD プロトコルが主に実装されている [31–40]．ここで，測定基底の数は異なる種類の測定数に対応し，状態の次元数は一つの測定が取りうる値の数に対応する．相互不偏基底 (MUB：Mutually Unbiased Bases) と呼ばれる 2 種類の特別な基底で測定することで，それぞれ高次元系に拡張したシステムの時間位置エラーと位相エラーを推定し，それに応じたデータ処理を施すことにより安全な秘密鍵共有が可能となる．一方，第 2 章で BBM92 と Six-state プロトコルの差異として詳述するが，測定基底の数が多いと時間位置エラーと位相エラーの結合確率分布の推定が可能となり，誤り訂正を効率化して高い秘密鍵生成率を得ることができる．d 次元量子状態の場合，$(d+1)$ 種類の MUB を用いることで，このような高次元量子状態の優位性を活かした鍵生成率向上が可能である [41–44, 77]．しかしながら，2 測定基底 QKD プロトコルに対しては任意の次元の量子状態について安全性証明がなされていた一方，$(d+1)$ 測定基底 QKD プロトコルに対して安全性が証明されているのは素数次元の量子状態についてのみであった．また，OAM 量子状態を用いた実装報告がある一方 [77]，タイムビン量子状態の場合に $(d+1)$MUB を効率よく実装する手法は知られていない．

上記のような背景のもと，本論文では，高速でロバストな高次元量子もつれ QKD 実現に向けた，スケーラブルなタイムビン量子状態の状態制御を研究目的とする．具体的には，以下の 3 つの項目を主な内容とする．

- 高次元タイムビン量子もつれ状態変調手法の実装と CGLMP 不等式の破れ測定による検証 (第 3 章)
- プロトコル無依存量子もつれ状態評価手法によるタイムビン量子もつれ状態の長距離伝送特性の検証 (第 4 章)
- 高次元量子状態の高性能性を最大限引き出す QKD プロトコルのためのスケーラブルな測定系実装 (第 5 章)

これらの研究項目は，高次元量子もつれ QKD に関して，通信の 3 つの基本動作である信号の生成 (送信)/伝送/測定 (受信) をカバーしたものと言える．

本論文の構成は以下の通りである．

第 1 章「序論」に続いて，第 2 章では，タイムビン量子状態の基礎的事項について述べる．具体的には，1 光子のタイムビン量子状態，量子もつれ状態を代表例とする複数光子のタイムビン量子状態の定義および測定方法，純粋量子もつれ状態の測定によって得られる相関のある乱数列の秘匿性，などについて述べる．さらに，QKD に関して，量子もつ

れ QKD の基本形である BBM92，量子もつれ蒸留に基づくノイズがある QKD の安全性証明の概略，測定法の多様化により鍵生成率が向上する Six-state プロトコル，などを紹介する．

第 3 章では，非線形光学結晶を用いた高次元タイムビン量子もつれ状態の生成，および状態最適化を利用した，ベル不等式の一種である CGLMP 不等式 [66] の破れの増加に関して議論する．先述の通り，高次元タイムビン量子もつれ状態に対して CGLMP 不等式の破れが観測されていないだけでなく，CGLMP 不等式の破れを最大化する特殊な量子もつれ状態による不等式の破れの明瞭な増加はこれまで観測されていない．本章では，このような特殊なタイムビン量子もつれ状態を振幅変調を用いて生成する手法を実装し，実際に生成した状態について CGLMP 不等式の破れの増加を観測している．これにより高次元タイムビン量子もつれ状態の隠れた変数理論を検証するとともに，その状態生成手法の有効性を示す．

第 4 章では，前章の手法により生成した高次元タイムビン量子状態を，長距離ファイバ伝送し，その伝送特性を量子状態トモグラフィー (QST：Quantum State Tomography) により検証する．QST とは，量子状態そのものを表す状態密度演算子を推定する技術である．状態密度演算子は量子状態の確率に関する全情報を有しており，状態が備えている任意の物理量や情報量などは状態密度演算子から導かれる．そのため，特定の測定物理量によらず，量子もつれ状態の品質を定量的に評価できる．ただし，d 次元量子もつれ状態の QST には，d^4 種類の異なる測定結果が必要となる．長距離ファイバ伝送では伝送損失のため測定される光子対数はごくわずかであり，高次元量子もつれ状態の QST には長い測定時間を要する．そのため，多種の測定結果を効率的に得ることが求められる．そこで本章では，多段接続した Mach-Zehnder 干渉計 (MZI：Mach-Zehnder Interferometer) を用いた，タイムビン量子状態に対する効率的な QST を提案/実装し，100 km 光ファイバ伝送後の高次元タイムビン量子もつれ状態に対して現実的な測定時間内での QST を行う．そして，その結果をもとに，伝送可能な秘密鍵生成率の指標となるコヒーレント情報量を評価し，この高次元タイムビン量子もつれ状態を利用した場合の QKD のシステム性能を議論する．

第 5 章では，d 次元量子状態を用いた QKD の具体的なプロトコルの一つである，$(d+1)$ 測定基底 QKD プロトコルで用いられる MUB の実装法を提案し，QKD への適用性を検証する．第 4 章では，量子もつれ状態自体の評価を目的として，特定の物理量によらない測定法 (QST) を採用したが，QKD 実装においてはプロトコルに応じた測定が必要である．先述の通り，$(d+1)$ 個の MUB を用いることで，高次元量子状態の優位性を活かした鍵生成率向上が可能であるが，その安全性証明，またタイムビン量子状態への実装について課題があった．そこで本章では，既存の安全性証明をもとに，有限体を用いた演算子や高次元量子もつれ状態の表現を用いて，素数の累乗次元状態へ安全性証明を拡張する．

さらに，拡張した安全性証明で想定した測定基底と等価な表現に基づき，次元数 $d = p^N$ のタイムビン量子状態について多段接続された $\log_p d$ 個の多腕干渉計と位相変調器による構成で，$(d+1)$ 種の MUB を実装する手法について議論する．

最後に第 6 章では，本研究で得られた成果を総括する．

以上述べた各章の関係を図 1.2 に示す．

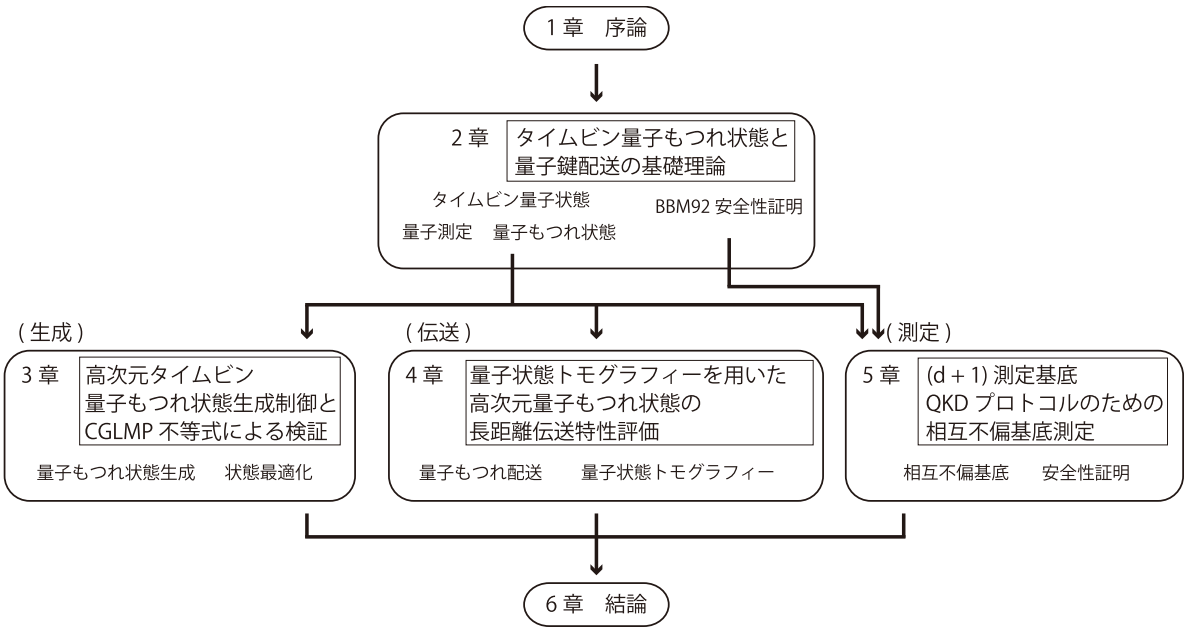

図 1.2　本論文の各章の関係．3, 4, 5 章が図 1.1 における状態生成，伝送，測定に対応する．

第 2 章

タイムビン量子もつれ状態と量子鍵配送の基礎理論

2.1 緒言

本章では，本論文の研究対象であるタイムビン量子状態に関して，第 3 章，4 章，5 章の内容に共通する量子情報理論の基礎事項について述べる [1, 78]．まず 2.2 節で，1 光子のタイムビン量子状態についての定義，および測定方法について述べる．さらに 2.3 節で，多光子の場合のタイムビン量子状態やその測定手法，量子もつれ状態の測定結果が持つ相関や秘匿性について述べる．また 2.4 節で，量子もつれを用いる QKD プロトコルである BBM92 の具体的な鍵生成手順について述べ，量子もつれ状態が QKD システムの実装，および安全性証明にどのように用いられるかを紹介する．さらに，Six-state プロトコルと呼ばれる 3 種の相互不偏基底 (MUB: Mutually Unbiased Basis) を用いたプロトコルに拡張すると，より高い鍵生成率が得られることを述べる．

2.2 1 光子のタイムビン量子状態

2.2.1 純粋量子状態と状態ベクトル

タイムビン量子状態は光子の時間位置を物理量とする量子状態である．光のエネルギーを極限まで減衰すると，離散的なエネルギー値となる．この光エネルギーの最小単位を光子と呼ぶ．ここで，この単一光子を用いる変復調方式として，2 値パルス位置変調 (PPM：Pulse Position Modulation) を考える．すなわち，2 つの時間スロット $\{t_0, t_1\}$ を用意し，光子が時間位置 t_0 にあればビット 0，時間位置 t_1 にあればビット 1 とする．量子力学では，それぞれをヒルベルト空間上のケットベクトルとして，$|0\rangle, |1\rangle$ と表す [図 2.1(a),

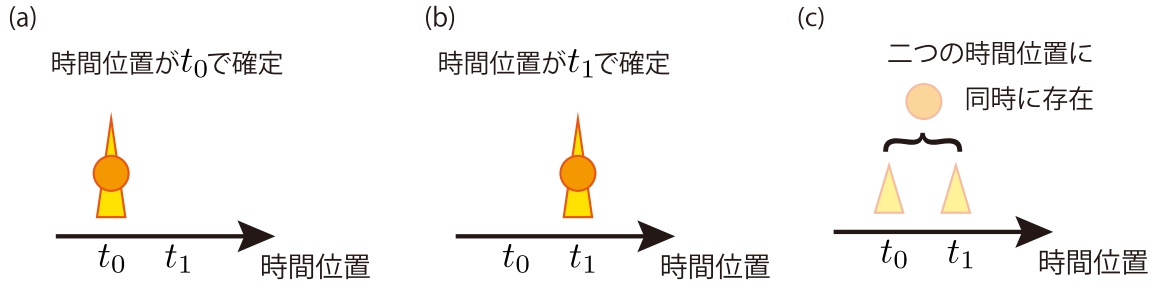

図 2.1　2 次元タイムビン量子状態の模式図．(a) 単一光子が必ず時間位置 t_0 で検出される状態．(b) 単一光子が必ず時間位置 t_1 で検出される状態．(c) 単一光子がどちらの時間位置にも同時に存在する重ね合わせ状態．

(b)]．このような二値の量子状態は時間スロット (タイムビン) によってビットを表現できることから，タイムビン量子ビットと呼ばれる．二つの状態は量子状態であるため，両者の確率的な重ね合わせ状態も一つの量子状態 $|\psi\rangle$ とみなすことができる [図 2.1(c)]．この状態は次のように表される．

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle \tag{2.1}$$

ただし，c_0, c_1 は $|c_0|^2 + |c_1|^2 = 1$ を満たす複素数であり，確率振幅という．単一光子のみを考えているため厳密には異なるが，レーザ光を減衰して疑似的な単一光子として用いる微弱コヒーレント光では，各パルスの持つ複素電界振幅の相対的な関係が確率振幅に対応すると考えてよい．

一般に，量子状態 $|\psi\rangle$ にある光子を測定したときに状態 $|\phi\rangle$ として測定される確率は，$|\langle\psi|\phi\rangle|^2$ で与えられる (Born の規則)．ただし，$\langle\psi|$ は $|\psi\rangle$ のエルミート共役であり，$\langle\psi|\phi\rangle$ は $|\psi\rangle$ と $|\phi\rangle$ のヒルベルト空間上の内積を表す．例えば，$|\psi\rangle = |0\rangle, |\phi\rangle = |1\rangle$ とすれば，時間スロット t_0 に用意した光子を測定し，時間スロット t_1 で光子が検出される確率が $|\langle 0|1\rangle|^2$ で与えられる．上記の二つの時間位置のパルスがそれぞれ明確に区別可能であれば，$|0\rangle$ が $|1\rangle$，または $|1\rangle$ が $|0\rangle$ として測定されることはなく，$|0\rangle$ は $|0\rangle$，$|1\rangle$ は $|1\rangle$ と必ず測定される．この条件は次式により表現される．

$$|\langle i|j\rangle|^2 = \delta_{i,j} \tag{2.2}$$

ただし，$i, j \in \{0, 1\}$，$\delta_{i,j}$ はクロネッカーのデルタである．このような状態を基底状態といい (ユークリッド空間上の単位ベクトルに相当)，基底状態の集合を正規直交基底という．この基底は時間位置を観測物理量とする量子状態の集合 $\{|0\rangle, |1\rangle\}$ であるため，時間位置基底と呼ばれる．一方，式 (2.1) で表される重ね合わせ状態を状態 $|i\rangle$ として測定す

る確率は,

$$\begin{aligned} |\langle\psi|i\rangle|^2 &= |(c_0^* \langle 0| + c_1^* \langle 1|)|i\rangle|^2 \\ &= |c_i^* \langle i|i\rangle|^2 \\ &= |c_i|^2 \end{aligned} \tag{2.3}$$

となる．ただし，上付きの $*$ は複素共役を表す．上式は，確率振幅の絶対値の二乗が対応する時間位置における光子検出確率を表すことを示している．これは，古典電磁気学において，複素電界振幅の絶対値の二乗が光強度を表すことに対応する．

これらの規則から，式 (2.1) の量子状態 $|\psi\rangle$，およびそのエルミート共役である $\langle\psi|$ を次のような縦ベクトル，および横ベクトルを用いて表現することができる．

$$|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \tag{2.4}$$

$$\langle\psi| = \begin{pmatrix} c_0^* & c_1^* \end{pmatrix} \tag{2.5}$$

このようなベクトルによる表記を用いることで，Born の規則 $|\langle\psi|\phi\rangle|^2$ がベクトルの内積を用いて計算できる．なお，規格化条件 $|c_0|^2 + |c_1|^2 = 1$ を満たさない量子状態は，規格化することでここまで述べた状態と物理的には同一視できる．一方，非規格化状態を含めたベクトル空間を考察対象とすると，数学的な取り扱いにおいて都合がよい．非規格化状態を含めた任意の $|\psi\rangle$ が属するベクトル空間 V は，$\forall|\psi\rangle, \forall|\phi\rangle \in V$ について，$\langle\psi|\psi\rangle \geq 0$ を満たす内積 $\langle\psi|\phi\rangle$ を備えた 2 次元ヒルベルト空間である．

BB84/BBM92 や，後述する Six-state プロトコルでは，状態 $|0\rangle, |1\rangle$ に加えて次のような重ね合わせ状態を利用する．

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{2.6}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2.7}$$

$$|L\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \tag{2.8}$$

$$|R\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \tag{2.9}$$

これらのタイムビン量子状態は偏波量子状態に対応付けることができ，式 (2.6)–(2.9) は順に，右斜め 45 度直線偏波，左斜め 45 度直線偏波，左回り円偏波，右回り円偏波と等価である．各状態を表す記号は，$|+\rangle, |-\rangle$ は右辺に現れる記号からそのように表され，$|L\rangle, |R\rangle$ は対応する円偏波状態のジョーンズベクトルとの類似性から，このように表される．これらの状態では，$|0\rangle$ と $|1\rangle$ の確率振幅の絶対値が等しく，相対位相が異なっている．Born の規則により，$\{|+\rangle, |-\rangle\}$，および $\{|R\rangle, |L\rangle\}$ の各集合が正規直交基底を成す

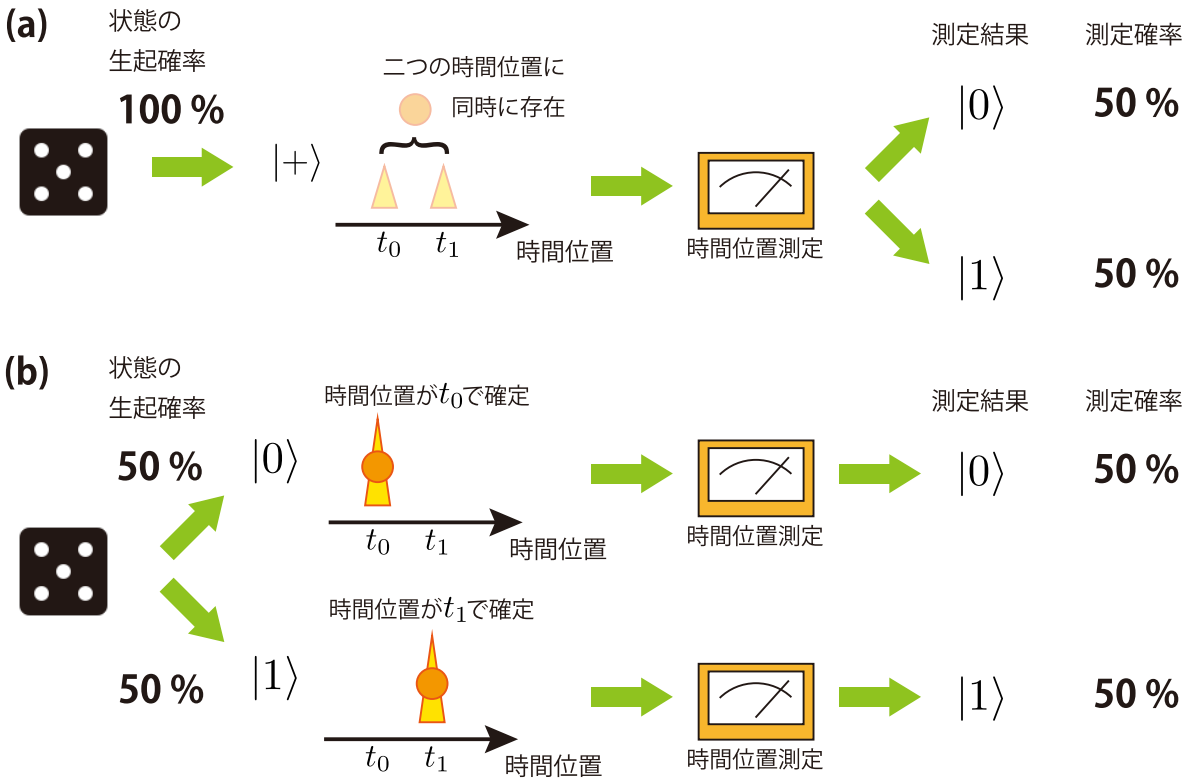

図 2.2　同じ測定確率分布を与える二つの異なる状態の測定過程．(a) 量子状態 $|+\rangle$ に対する時間位置測定．(b) 一様ランダムに選ばれた量子状態 $|0\rangle, |1\rangle$ に対する時間位置測定．

ことが確認できる．したがって，タイムビン量子状態を，式 (2.1) のような $|0\rangle, |1\rangle$ の展開形に代わり，$|+\rangle, |-\rangle$ の線形結合，あるいは $|R\rangle, |L\rangle$ の線形結合で表すことができる．これらの基底は相対位相が状態を区別する物理量であるため，位相基底と呼ばれる．なお，ここでは二つの位相基底を区別する際には，位相基底 $\{|+\rangle, |-\rangle\}$，位相基底 $\{|R\rangle, |L\rangle\}$ と具体的に集合を明示して区別する．第 5 章で高次元量子状態の位相基底について述べる際には，各位相基底を表す集合にインデックスを割り当てて区別する．

式 (2.6)–(2.9) で表される 4 つの重ね合わせ状態は，各確率振幅の絶対値の二乗が等しく 1/2 であるため，時間位置に関する測定，すなわち状態 $|0\rangle$ か $|1\rangle$ かを判定する測定を行うと，測定結果は一様ランダムとなる [図 2.2(a)]．このランダム性は量子状態に原理的に備わっているものであり，例えば 0, 1 の乱数に基づいて $|0\rangle$ または $|1\rangle$ が選ばれた状態のランダム性 [図 2.2(b)] とは質的に異なる．後者の場合，乱数を発生させた時点で原理的に $|0\rangle$ か $|1\rangle$ は定まっている一方，前者は測定するまでどちらか分からない，重ね合わせ状態である．前者のような純粋量子状態は，後者のような非量子状態または古典状態とは一線を画す．古典状態はここまで述べた純粋量子状態として記述できないため，2.2.2 節

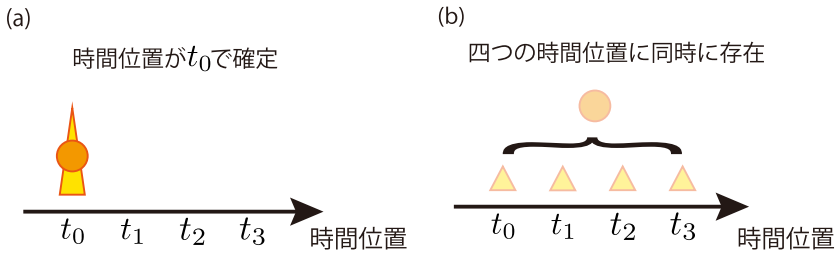

図 2.3　$d = 4$ の時の高次元タイムビン量子状態の模式図．(a) 単一光子が必ず時間位置 t_0 で検出される状態．(b) 単一光子が全ての時間位置に同時に存在する重ね合わせ状態．

で古典状態を記述できる状態密度演算子を導入した後，再びこの違いについて議論する．

$\{|+\rangle, |-\rangle\}$ および $\{|R\rangle, |L\rangle\}$ の各状態について，時間位置の測定を行うと $|0\rangle$ か $|1\rangle$ かは一様ランダムになるのと同様に，$\{|+\rangle, |-\rangle\}$ の各状態に対して，$|R\rangle$ であるか $|L\rangle$ であるか，またはその逆の測定を行った場合も，測定結果は一様ランダムとなる．このように二つの正規直交基底について，一方の基底状態を他方の基底状態として測定した時に，結果が一様ランダムであるとき，二つの基底は相互不偏であるという．

一般に，閉じた系での量子状態の変化は，確率の保存則のためにユニタリー演算子 $\hat{U}$ によって記述される．外部との相互作用がある場合の確率保存則を満たす状態変化では，完全正値トレース保存 (CPTP：Completely Positive Trace Preserving) 写像に拡張されるが，ここでは深入りしない．元の量子状態 $|\psi\rangle$ が $\hat{U}$ によって変換されるとき，変換後の状態は $\hat{U}|\psi\rangle$ となる．例えば，時間位置基底状態 $|0\rangle, |1\rangle$ をそれぞれ位相基底状態 $|+\rangle, |-\rangle$ へ変化させるアダマール変換は，次のユニタリー演算子 $\hat{H}$ で与えられる．

$$\hat{H} = |+\rangle\langle 0| + |-\rangle\langle 1| \tag{2.10}$$

なお，アダマール変換は，量子コンピュータで量子状態を重ね合わせ状態として初期化する際などにしばしば用いられるほか，第 5 章で述べる 2^N 次元における相互不偏基底と密接な関わりがある．

より高次元のタイムビン量子状態は，用意する時間スロットの数を増加させることで定義できる (図 2.3)．明確に区別可能な d 個の時間スロットについて，時間位置 $t_i (i \in [0, \cdots, d-1])$ に単一光子が確定的に存在する状態を $|i\rangle$ と表記すると，任意の純粋量子状態 $|\psi\rangle$ は $|\psi\rangle = \sum_i c_i |i\rangle$ と表される．ただし，c_i は $\sum_i |c_i|^2 = 1$ を満たす確率振幅であり，$|\psi\rangle$ は d 次元ヒルベルト空間の元 (ケットベクトル) である．また，高次元量子状態の場合も，$\{|0\rangle, \cdots, |d-1\rangle\}$ は時間位置基底と呼ばれる．また，$|+\rangle, |-\rangle$ の高次

元量子状態への拡張として，例えば 4 次元量子状態の場合に，

$$\left|\psi^{++}\right\rangle = \frac{1}{2}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right) \tag{2.11}$$

$$\left|\psi^{+-}\right\rangle = \frac{1}{2}\left(|0\rangle - |1\rangle + |2\rangle - |3\rangle\right) \tag{2.12}$$

$$\left|\psi^{-+}\right\rangle = \frac{1}{2}\left(|0\rangle + |1\rangle - |2\rangle - |3\rangle\right) \tag{2.13}$$

$$\left|\psi^{--}\right\rangle = \frac{1}{2}\left(|0\rangle - |1\rangle - |2\rangle + |3\rangle\right) \tag{2.14}$$

といった量子状態を考えることができる．これらの状態は，単一光子が 4 つの時間位置に同時に存在する重ね合わせ状態 [図 2.3(b)] であり，各パルス間の相対位相だけが異なっている．上記 4 つの量子状態は，4 次元ヒルベルト空間の正規直交基底を構成する．また，各確率振幅の二乗が $|c_i|^2 = 1/4$，すなわち 4 値の測定値の場合の一様ランダムな分布となるため，時間位置基底に対して相互不偏である．高次元量子状態の相互不偏基底については第 5 章で詳細に議論する．

2.2.2　混合量子状態と状態密度演算子

前節において，図 2.2 に示す二つのモデルを例題として議論したように，重ね合わせ状態により表現される確率事象と，サイコロなどによる古典的な確率事象は質的に異なっている．前者は状態そのものだけでなく，測定系との組み合わせで初めて確率的になる事象であり，状態生成時あるいは状態自体のランダムさによる確率事象ではない．そのため，状態ベクトルによる純粋量子状態の表現ではこのような古典状態を表すことができず，より一般的な表現手法が必要となる．そのような古典状態を含んだ一般的な混合量子状態は，状態密度演算子によって記述される．本節ではこのことについて述べる．

まず，純粋量子状態 $|\psi\rangle = \sum_i c_i |i\rangle$ に対して測定を行い，その結果，$|\phi\rangle = \sum_i d_i |i\rangle$ として観測される確率 $|\langle\psi|\phi\rangle|^2$ について考察する．これは前節の，$|+\rangle$ 状態に対して時間位置を測定し，時間スロット t_0 で光子が観測されたため状態 $|0\rangle$ と判定される例などの一般化である ($|\psi\rangle = |+\rangle, |\phi\rangle = |0\rangle$)．この確率の表記を次のように変形する．

$$\begin{aligned} |\langle\psi|\phi\rangle|^2 &= \left|\sum_i c_i^* d_i\right|^2 = \left(\sum_i d_i^* c_i\right)\cdot\left(\sum_i c_i^* d_i\right) \\ &= \langle\phi|\psi\rangle\langle\psi|\phi\rangle \\ &= \langle\phi|\,\hat{\rho}_\psi\,|\phi\rangle \end{aligned} \tag{2.15}$$

ただし，$\hat{\rho}_\psi := |\psi\rangle\langle\psi|$ を導入した．この $\hat{\rho}_\psi$ を純粋状態 $|\psi\rangle$ に対する状態密度演算子とい

う．あるいは，上記測定確率は次のようにも表される．

$$\begin{aligned}
|\langle\psi|\phi\rangle|^2 &= \left|\sum_i c_i^* d_i\right|^2 = \sum_i c_i \left(\sum_j c_j^* d_j\right) d_i^* \\
&= \sum_i \langle i|\psi\rangle \cdot \langle\psi|\phi\rangle \cdot \langle\phi|i\rangle \\
&= \mathrm{Tr}(|\psi\rangle\langle\psi|\phi\rangle\langle\phi|) \\
&= \mathrm{Tr}\left(\hat{\rho}_\psi \hat{P}_\phi\right) = \mathrm{Tr}\left(\hat{P}_\phi \hat{\rho}_\psi\right)
\end{aligned} \tag{2.16}$$

ここで，Tr はトレース，すなわち演算子 $\hat{A}$ に対して $\mathrm{Tr}\left(\hat{A}\right) = \sum_i \langle i|\,\hat{A}\,|i\rangle$ を計算する操作を表す．また，$\hat{P}_\phi = |\phi\rangle\langle\phi|$ は状態 $|\phi\rangle$ への測定を表す射影測定演算子である．式 (2.15), (2.16) 自体は Born の規則の変形であり，物理的に新しいものを導入したわけではない．しかし，元の Born の規則が状態ベクトルの内積の絶対値の二乗という形式であるのに対し，式 (2.15), (2.16) では状態密度演算子 $\hat{\rho}_\psi$ についての 1 次式で測定確率を求めている．このため，複数の純粋量子状態が確率的に生成される状況において，平均測定確率を生起確率による重みづけ線形和として求めるのに適した記述となっている．

そこで図 2.4(a) のように，量子状態 $|\psi_i\rangle$ の生起確率が p_i で与えられる混合量子状態の，状態 $|\phi\rangle$ への射影測定について考える．この時，測定結果が状態 $|\phi\rangle$ となる確率は，上記の式展開を適用することにより，次のように表される．

$$\begin{aligned}
\sum_i p_i |\langle\psi_i|\phi\rangle|^2 &= \sum_i p_i \langle\phi|\psi_i\rangle\langle\psi_i|\phi\rangle \\
&= \langle\phi| \left(\sum_i p_i |\psi_i\rangle\langle\psi_i|\right) |\phi\rangle \\
&= \mathrm{Tr}\left(\hat{P}_\phi \sum_i p_i \hat{\rho}_{\psi_i}\right)
\end{aligned} \tag{2.17}$$

ここで，混合量子状態に対応する状態密度演算子 $\hat{\rho}$ を，構成する各量子状態 $|\psi_i\rangle$ の状態密度演算子 $\hat{\rho}_{\psi_i}$ の生成確率 p_i による重みづけ総和，

$$\hat{\rho} = \sum_i p_i \hat{\rho}_{\psi_i} \tag{2.18}$$

とする．このように，混合量子状態の状態密度演算子を考えると，純粋量子状態 (あるひとつの i で $p_i = 1$) であるか，混合量子状態 (複数の i で $p_i > 0$) であるかに関わらず，式 (2.17) より，量子状態 $\hat{\rho}$ に対する測定結果が $|\phi\rangle$ となる確率が $\langle\phi|\,\hat{\rho}\,|\phi\rangle$ あるいは $\mathrm{Tr}(P_\phi\hat{\rho})$ で与えられる．これは図 2.4(a) の量子状態を，図 2.4(b) のように平均的な量子状態として取り扱うことに相当する．一般に，測定確率は 0 以上，また確率の総和は 1 であること

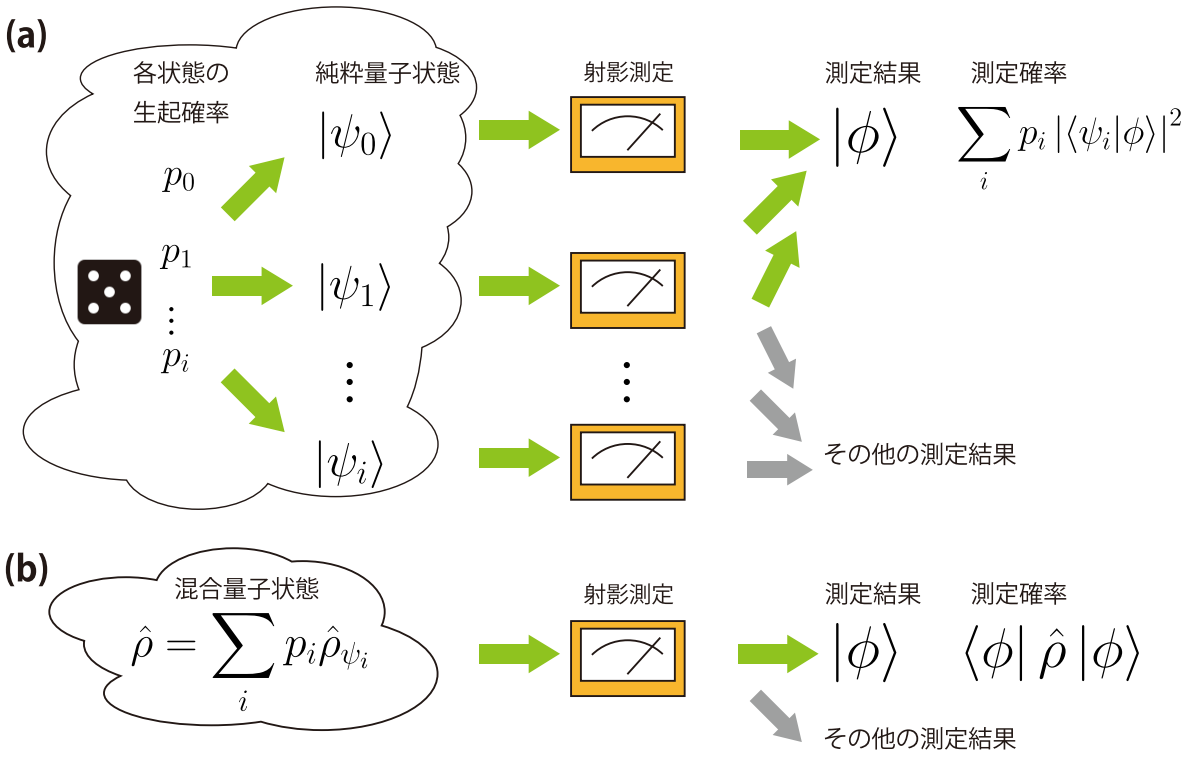

図 2.4　複数の純粋量子状態の平均としての混合量子状態．(a) ランダムに生成された純粋量子状態に対する測定と，(b) 純粋量子状態の平均としての混合量子状態に対する測定は，完全に同一の測定確率分布を与える．なお，(a) において並列に描かれている測定装置は，それぞれの確率的な事象にあわせて便宜上描いているだけであり，観測者が用いる測定装置は単一かつ同一のものである．

から，$\langle\phi|\hat{\rho}|\phi\rangle \geq 0$ かつ $\sum_i \langle i|\hat{\rho}|i\rangle = \mathrm{Tr}(\hat{\rho}) = 1$ が満たされており，$\hat{\rho}$ はトレース 1 の半正定値エルミート演算子となっている．半正定値性 ($\langle\phi|\hat{\rho}|\phi\rangle \geq 0$) から，状態密度演算子は全て非負の実数固有値を持つ．また，トレースは固有値の総和に等しく，その総和が 1 であるから，形式的には固有値を何らかの確率と解釈できる．実際，式 (2.18) を構成する量子状態 $|\psi_i\rangle$ が全て直交していれば，固有値は各状態の生起確率に等しく，その固有状態は $|\psi_i\rangle$ である．

式 (2.18) を状態密度演算子の定義とするには，各純粋量子状態やその生成モデルが既知である必要があるが，この情報が常に得られる保証はない．さらには，後で議論する量子もつれ状態にある二光子のうち，一方の光子のみに着目した時の状態密度演算子に対して，上記のような古典的な乱数によるモデルは厳密には不適切である．そのため，より一般化して，単にトレース 1 の半正定値エルミート演算子を状態密度演算子の定義とする．

上記の混合量子状態に対する状態密度演算子の導入において，図 2.4(a) の状況であれば，式 (2.18) によって図 2.4(b) の状態密度演算子を考える事ができた．一方，逆の命題

である「図 2.4(b) の量子状態は図 2.4(a) のモデルによって実現された」，すなわち「ある状態 $\hat{\rho}$ が $\hat{\rho} = \sum_i p_i \hat{\rho}_{\psi_i}$ と分解できる時，その状態は量子状態 $\hat{\rho}_{\psi_i}$ を確率 p_i で生成することにより得られた」は一般に正しくない．例えば，確率 1/2 で $|0\rangle$ または $|1\rangle$ である量子状態の状態密度演算子 $\hat{\rho}_{0/1}$ と，確率 1/2 で $|+\rangle$ または $|-\rangle$ である量子状態の状態密度演算子 $\hat{\rho}_{\pm}$ は，実際にそれぞれ生成された過程は違っているにも関わらず同じ演算子 $\hat{\rho}_{0/1} = \hat{\rho}_{\pm}$ となる．さらに，上記の $\hat{\rho}$ の導入から分かるように，$\hat{\rho}$ は射影される状態 $|\phi\rangle$ に依存しない．したがって，任意の $|\phi\rangle$ に対して $\langle\phi|\,\hat{\rho}_{0/1}\,|\phi\rangle = \langle\phi|\,\hat{\rho}_{\pm}\,|\phi\rangle$ であり，測定確率は量子状態を生成する過程に依存せず，状態密度演算子のみで定まる．そのため，量子状態を生成するモデルが不明な場合，観測値から量子状態について知りうる最大の情報は状態密度演算子である．このように，観測者にとって $\hat{\rho}_{0/1}, \hat{\rho}_{\pm}$ の量子状態に違いはなく，状態密度演算子は量子状態についての全ての情報を含む．

純粋量子状態がベクトルで記述できたように，状態密度演算子は行列で表すことができる．例えば，状態密度演算子は，時間位置基底状態 $|i\rangle$ およびそのエルミート共役 $\langle j|$ の展開形として，一般に次式のように表される．

$$\hat{\rho} = \sum_{ij} r_{ij}\,|i\rangle\langle j| \tag{2.19}$$

上式は，i 行 j 列の要素を r_{ij} とした行列表現により状態密度演算子が記述できることを示している．逆に言うと，r_{ij} を要素とする行列を求めることで状態密度演算子が推定される．先に述べたように，観測者にとって状態密度演算子は量子状態に関する全ての情報を含む．したがって，状態密度演算子の推定は量子状態そのものの測定であると言ってよい．このようにして量子状態を調べる手法を量子状態トモグラフィーという．第 4 章では，この手法により高次元タイムビン量子状態を評価する．

上記のように，状態密度演算子は与えられた量子状態についての測定確率に関するすべての情報を含むため，状態密度演算子から任意の物理量や状態に関する情報を得ることができる．例えば，量子状態のエントロピーを表す von Neuman エントロピー $S(\hat{\rho})$ は次式で定義される．

$$S(\hat{\rho}) = -\,\mathrm{Tr}(\hat{\rho}\log_2\hat{\rho}) \tag{2.20}$$

上式に状態密度演算子の対角化表示 $\hat{\rho} = \sum_i p_i\,|\psi_i\rangle\langle\psi_i|$ を代入すると，$S(\hat{\rho}) = -\sum_i p_i \log_2 p_i$ となる．すなわち，確率 p_i で直交量子状態 $|\psi_i\rangle$ をとる量子状態の状態密度演算子 $\hat{\rho}$ の von Neuman エントロピーは，その状態の生起確率 p_i の Shannon エントロピー $\mathrm{H}(p_i)$ となる．

前節にて，図 2.2 に示す 2 つのモデルを題材として議論した通り，式 (2.6) で表される純粋状態 $|+\rangle$ の時間位置についての測定と，一様ランダムに $|0\rangle, |1\rangle$ を生成した混合状態の時間位置についての測定は，どちらも一様ランダムな測定結果を与える．したがって，

その測定結果の確率分布が持つエントロピーはどちらも 1 ビットである．一方，状態密度演算子は前者が $\hat{\rho} = |+\rangle\langle+|$，後者が $\hat{\rho} = 1/2\,|0\rangle\langle 0| + 1/2\,|1\rangle\langle 1|$ と表される．これより，前者の von Neuman エントロピーは 0 ビットとなり，これは不確定さがない状態であることを意味する．これに対し，後者の von Neuman エントロピーは 1 ビットであり，1 量子ビットとしては最大不確定状態となる．この違いは，測定結果の確率分布は量子状態と測定の組み合わせによって定まるのに対し，von Neuman エントロピーは量子状態自体の持つエントロピーであることに起因する．すなわち，状態 $|+\rangle$ について時間位置測定ではなく，$|+\rangle$ もしくは $|-\rangle$ のどちらであるかを判定する射影測定を行えば，必ず $|+\rangle$ となり不確定さがない測定結果が得られる．一方，後者の量子状態について，$|+\rangle, |-\rangle$ への射影測定を行ってもやはり一様ランダムな結果となる．

2.2.3　量子測定演算子と遅延 Mach-Zehnder 干渉計による測定

2.2.2 節にて，状態密度演算子 $\hat{\rho}_\psi$ を導入するとともに，測定操作を記述する演算子として射影測定演算子 $\hat{P}_\phi$ について述べた．本節では，この射影測定演算子のより一般的な測定演算子への拡張，および関連する演算子である正定値作用素測度について述べたのち，本論文で主な測定手段となる遅延 Mach-Zehnder 干渉計の場合の具体例について議論する．

まず，一般化の前に，先の射影測定演算子が持つ性質を整理する．二次元ヒルベルト空間を考え，時間位置基底状態 $|0\rangle, |1\rangle$ への射影測定演算子を $\hat{P}_0, \hat{P}_1$ と表す (それぞれ時間位置 t_0, t_1 での光子の検出に対応)．量子状態 $\hat{\rho}$ に対してこの射影測定を行った時の測定確率は，先述の通りそれぞれ $\mathrm{Tr}\left(\hat{P}_0\hat{\rho}\right), \mathrm{Tr}\left(\hat{P}_1\hat{\rho}\right)$ で与えられる．2 次元タイムビン量子状態では，光子は必ず時間位置 t_0, t_1 のどちらかで検出できる．したがって，任意の状態密度演算子 $\hat{\rho}$ に対する測定確率の保存則として，

$$\mathrm{Tr}\left(\hat{P}_0\hat{\rho}\right) + \mathrm{Tr}\left(\hat{P}_1\hat{\rho}\right) = 1 \tag{2.21}$$

が成り立つ．トレースの線形性から，$\mathrm{Tr}\left(\hat{P}_0\hat{\rho}\right) + \mathrm{Tr}\left(\hat{P}_1\hat{\rho}\right) = \mathrm{Tr}\left\{(\hat{P}_0 + \hat{P}_1)\hat{\rho}\right\}$ である．この関係が任意の $\hat{\rho}$ に対して成り立つこと，また $\hat{\rho}$ のトレースが 1 であることから，

$$\hat{P}_0 + \hat{P}_1 = \hat{\mathbb{1}} \tag{2.22}$$

が成り立つ．ただし，$\hat{\mathbb{1}}$ は恒等演算子である (変化を生じない演算子であり，実数の乗算での 1 に相当)．

一方，測定後の量子状態について考える．2.2.1 節で述べたように，純粋量子状態 $|\psi\rangle$ にユニタリー変換 $\hat{U}$ を施した後の状態は $\hat{U}\,|\psi\rangle$ となる．また，そのエルミート共役から，ユニタリー変換により $\langle\psi| \to \langle\psi|\,\hat{U}^\dagger$ となる．ただし，上付きの $\dagger$ は元の演算子のエルミート

共役, $\rightarrow$ は時間発展による状態の変化を表す．よって，状態密度演算子 $\hat{\rho} = \sum_i p_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right|$ を考えれば，そのユニタリー変換後の量子状態は，$\hat{U}\hat{\rho}\hat{U}^\dagger = \sum_i p_i \hat{U} \left|\psi_i\right\rangle\!\left\langle\psi_i\right| \hat{U}^\dagger$ と表せる．射影測定演算子による状態変化も同様の記述が可能であるが，ユニタリー変換と異なり単一の演算子での確率保存は成り立たないため，測定後の状態は規格化が必要である．例えば，時間位置 t_0 で光子が検出されたという条件下での測定後の量子状態について考える．測定前の状態が純粋量子状態 $\left|\psi\right\rangle = c_0 \left|0\right\rangle + c_1 \left|1\right\rangle$ の場合，射影測定後の量子状態は次式で与えられる．

$$\begin{aligned} \left|\psi\right\rangle \rightarrow \hat{P}_0 \left|\psi\right\rangle &= \left|0\right\rangle \left\langle 0|\psi\right\rangle \\ &= \left(\left\langle 0|\psi\right\rangle\right) \left|0\right\rangle \\ &= c_0 \left|0\right\rangle \end{aligned} \tag{2.23}$$

これは，測定前に重ね合わせ状態状態 $\left|\psi\right\rangle$ であったタイムビン量子状態が，時間位置 t_0 での光子検出により，時間位置基底状態 $\left|0\right\rangle$ に変化したことを表している (波動関数の収縮)．ただし，これは非規格化量子状態であるから，c_0 で割って規格化する必要がある．同様に，測定によって $\left\langle\psi\right| \rightarrow \left\langle\psi\right| \hat{P}_0^\dagger = c_0^* \left\langle 0\right|$ の状態変化が生じる．よって，純粋量子状態の密度演算子 $\hat{\rho}_\psi = \left|\psi\right\rangle\!\left\langle\psi\right|$ の時間発展は次式のように表せる．

$$\begin{aligned} \hat{\rho}_\psi \rightarrow \hat{P}_0 \hat{\rho}_\psi \hat{P}_0^\dagger &= \left|c_0\right|^2 \left|0\right\rangle\!\left\langle 0\right| \\ &= \mathrm{Tr}\Big(\hat{P}_0 \hat{\rho}_\psi\Big) \left|0\right\rangle\!\left\langle 0\right| \end{aligned} \tag{2.24}$$

これらの関係から，混合量子状態の密度演算子 $\hat{\rho}$ の場合の，規格化を含めた時間発展が次式のように表せる．

$$\hat{\rho} \rightarrow \frac{\hat{P}_0 \hat{\rho} \hat{P}_0^\dagger}{\mathrm{Tr}\Big(\hat{P}_0 \hat{\rho}\Big)} \tag{2.25}$$

上式は，条件付き確率分布の状態密度演算子版と考えればよい．なお，$\hat{P}_0 = \left|0\right\rangle\!\left\langle 0\right|$ を用いて式 (2.25) を展開すれば，混合量子状態に対する測定後の状態密度演算子も $\left|0\right\rangle\!\left\langle 0\right|$，すなわち時間位置 t_0 に光子が存在する状態であるという自明な結果が得られる．射影測定演算子 P_1 についても同様である．

また，射影測定演算子は $\hat{P}_i \hat{P}_i = \hat{P}_i$ を満たす．これは，例えば時間位置 t_0 で光子を観測したのちに，続けて時間位置 t_0 への射影測定を行っても，一度だけ射影測定するのと結果的に変わらないことを意味する．これは後の一般の測定には要求されない，射影測定特有の性質である．射影測定演算子はエルミート演算子であるため，$\hat{P}_i^\dagger \hat{P}_i = \hat{P}_i \hat{P}_i = \hat{P}_i$ も成り立つ．そのため，トレースの巡回性 $\mathrm{Tr}\Big(\hat{A}\hat{B}\hat{C}\Big) = \mathrm{Tr}\Big(\hat{B}\hat{C}\hat{A}\Big) = \mathrm{Tr}\Big(\hat{C}\hat{A}\hat{B}\Big)$ を用いて，$\mathrm{Tr}\Big(\hat{P}_0\hat{\rho}\Big) = \mathrm{Tr}\Big(\hat{P}_0^\dagger \hat{P}_0 \hat{\rho}\Big) = \mathrm{Tr}\Big(\hat{P}_0 \hat{\rho} \hat{P}_0^\dagger\Big)$ などの書き換えが可能である．

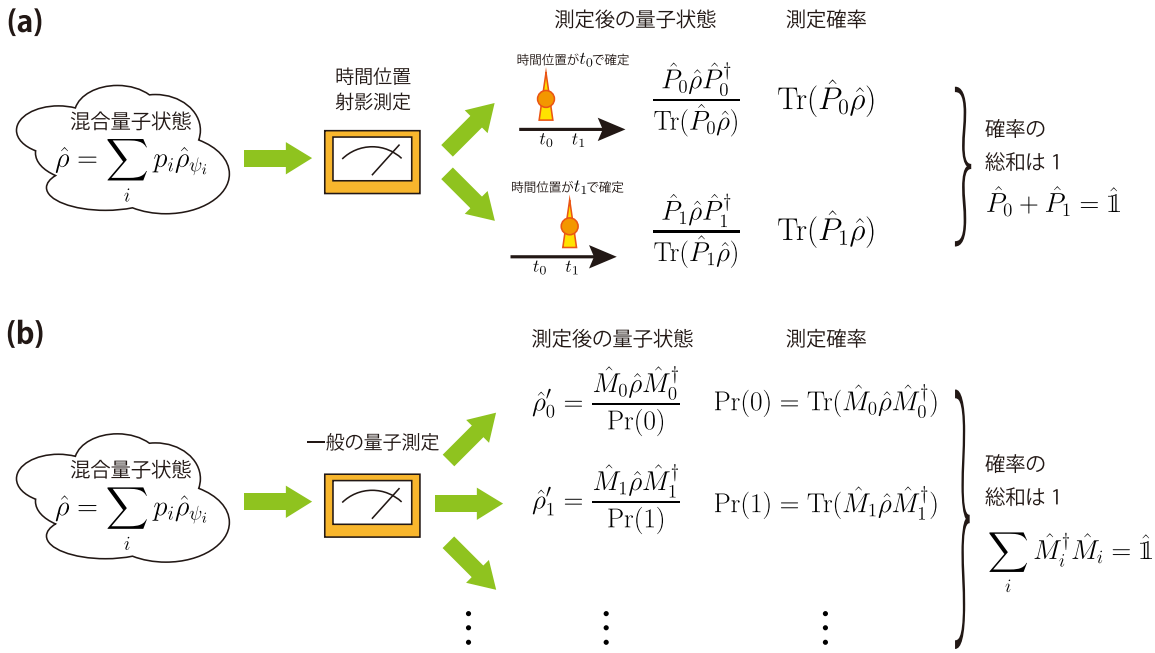

図 2.5　測定演算子と測定後の状態および測定確率の関係．(a) 2 次元タイムビン量子状態と時間位置基底状態への射影測定の場合．(b) 一般の量子状態と量子測定演算子の場合．

ここまで射影測定演算子の性質をいくつか確認したが，測定演算子として重要な点は，1) 状態密度演算子と組み合わせて測定確率が計算できる，2) 測定後の状態密度演算子が記述できる，3) 測定確率の総和が 1 となる，の 3 点である [図 2.5(a)]．

上記の射影測定演算子は，単一の純粋量子状態への射影測定演算子であり，行列で表現した際のランクが 1 であるため，ランク 1 の射影測定演算子と呼ばれる．この他にも，例えば d 次元タイムビン量子状態の場合に，$k < d-1$ として，時間位置が $k-1$ 以下であるか，k 以上であるかを一括で判定する射影測定演算子 $\hat{P}_{<k} = \sum_{i<k} |i\rangle\langle i|$ と $\hat{P}_{\geq k} = \sum_{i\geq k} |i\rangle\langle i|$ を考えることができる．これらの射影測定演算子はそれぞれランク $k, d-k$ の射影測定演算子である．また，この後詳述する遅延 Mach-Zehnder 干渉計のように，測定前のヒルベルト空間の次元と，測定後のヒルベルト空間の次元が一致しないような測定を考えることもできる．これらの一般の量子測定は次の条件を満たす測定演算子

$\hat{M}_i$ によって記述される．

$$\Pr(i) = \mathrm{Tr}\Big(\hat{M}_i \hat{\rho} \hat{M}_i^\dagger\Big) \tag{2.26}$$

$$\hat{\rho}'_i = \frac{\hat{M}_i \hat{\rho} \hat{M}_i^\dagger}{\Pr(i)} \tag{2.27}$$

$$\sum_i \hat{M}_i^\dagger \hat{M}_i = \hat{\mathbb{1}} \tag{2.28}$$

ただし，$\Pr(i)$ はラベル i の測定結果を得る確率，$\hat{\rho}'_i$ はラベル i の測定結果を得た後の条件付き量子状態を表す状態密度演算子である．式 (2.28) は確率の保存則，すなわち $\sum_i \Pr(i) = \sum_i \mathrm{Tr}\Big(\hat{M}_i \hat{\rho} \hat{M}_i^\dagger\Big) = \mathrm{Tr}\Big(\sum_i \hat{M}_i^\dagger \hat{M}_i \hat{\rho}\Big) = 1$ から要請される．ただし，トレースの巡回性，およびトレースの線形性による Tr と総和の入れ替えを用いた．射影測定演算子とは異なり，$\hat{M}_i \hat{M}_i = \hat{M}_i$ は満たされなくてもよい．例えば，タイムビン量子状態を一度偏波量子状態に変換して測定を行う演算子などを考える事が出来るが，いったん時間自由度から偏波自由度に変換をした後，続けて同じ変換を施すことは出来ないため，$\hat{M}_i \hat{M}_i = \hat{M}_i$ は成り立たない．

以上の関係は図 2.5(b) のようにまとめられる．図 2.5(a) の射影測定演算子の場合と，測定確率などの形式が異なって見えるが，先に述べた射影測定演算子特有の性質を用いれば，同等の関係であることが分かる．

量子測定演算子や射影測定演算子を用いると，測定結果の確率だけでなく測定後の量子状態も記述できる．例えば，偏波を状態変数とする量子状態に対して偏光子に通すという測定を行うと，偏光子通過後の状態は，直線偏光光子状態となる．タイムビン量子状態の場合も，例えば光カー効果による相互位相変調を利用した光子数測定 [79] などにより，測定後に光子が残るような測定を原理的には考えることが出来る (量子非破壊測定 [79–81])．一方，時間位置の測定を光子検出器を用いて行う場合には，測定後の光子状態は存在せず，測定確率のみが関心事となる．ここで $\hat{E}_i = \hat{M}_i^\dagger \hat{M}_i$ と表記すると，測定確率が

$$\begin{aligned}\Pr(i) &= \mathrm{Tr}\Big(\hat{M}_i \hat{\rho} \hat{M}_i^\dagger\Big) \\ &= \mathrm{Tr}\Big(\hat{M}_i^\dagger \hat{M}_i \hat{\rho}\Big) \\ &= \mathrm{Tr}\Big(\hat{E}_i \hat{\rho}\Big)\end{aligned} \tag{2.29}$$

と表され，これは演算子 $\hat{E}_i$ によって測定確率が与えられることを示している．ここで，式 (2.28) より，$\sum_i \hat{E}_i = \hat{\mathbb{1}}$ である．また，任意の純粋量子状態 $\hat{\rho} = |\psi\rangle\langle\psi|$ に対して $\Pr(i) = \mathrm{Tr}\Big(\hat{E}_i \hat{\rho}\Big) = \langle\psi| \hat{E}_i |\psi\rangle \geq 0$ であり，密度演算子同様に $\hat{E}_i$ も半正定値演算子となっている．このように，測定確率のみを推定する演算子の集合 $\{\hat{E}_i\}$ を正定値作用素測度 (POVM：Positive Operator-Valued Measure) という．例えば，単一光子検出器

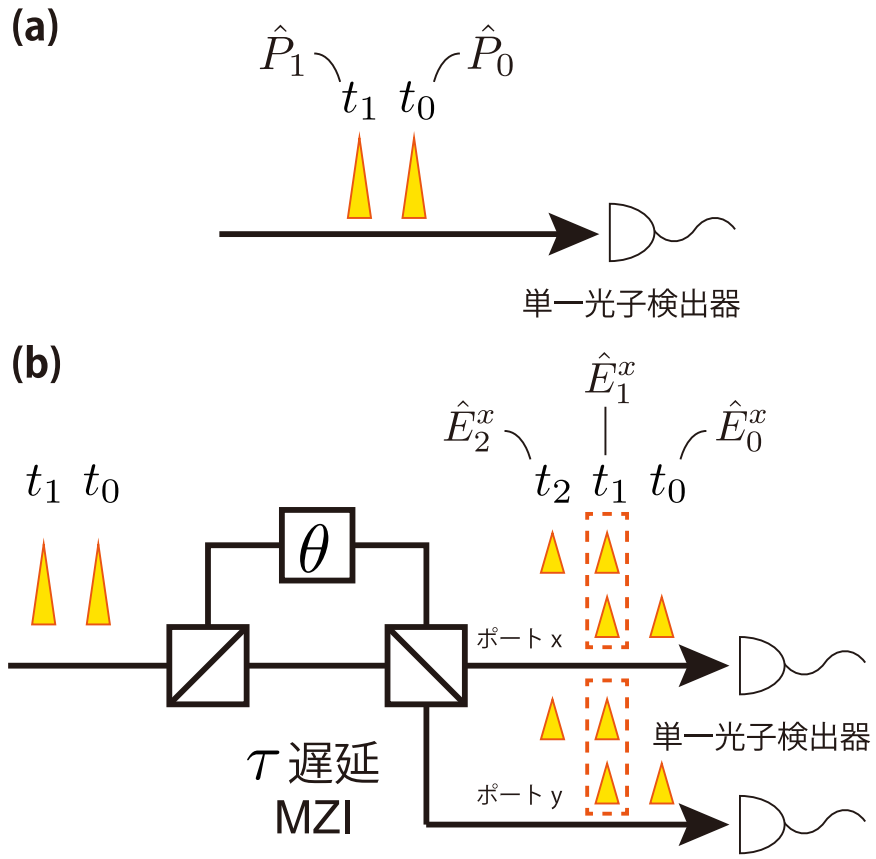

図 2.6　タイムビン量子状態に対する具体的な測定実装法．(a) 単一光子検出器による時間位置測定．(b) 遅延 Mach-Zehnder 干渉計を使った重ね合わせ状態の測定．

を用いて時間位置を測定する場合，時間位置 t_i で光子が検出される事象は，射影測定 $\hat{M}_i = \hat{P}_i = |i\rangle\langle i|$ に対応すると考えられ，その POVM 要素 $\hat{E}_i$ は $\hat{E}_i = \hat{P}_i^\dagger \hat{P}_i = \hat{P}_i$ となる．

ここまで，量子測定演算子および POVM に関する一般論を述べた．以降は，タイムビン量子状態の場合の，これらの具体的な演算子の表式と実装法について議論する．時間位置に関する測定は，図 2.6(a) のようにタイムビン量子状態を光子検出器に入力して検出時刻を測定する，というシンプルな構成で行われる．上述のように，この場合の量子測定演算子や POVM 要素には，時間位置基底状態への射影測定演算子が対応する．

一方，$|+\rangle$ や $|R\rangle$ などの重ね合わせ状態に対する測定には，遅延 Mach-Zehnder 干渉計 (MZI：Mach-Zehnder Interferometer) がよく用いられる．例えば，二次元タイムビン量子状態に対する $|+\rangle, |-\rangle$ への射影測定系は，図 2.6(b) に示す構成により実装される．被測定状態を時間スロットの間隔 τ に等しい遅延時間を持つ MZI に入力する．MZI では，入力側ビームスプリッタによって光子が二経路へ分岐され，長経路では τ だけ時間遅延されるとともに伝搬遅延位相 θ が付与される．これにより，被測定状態中の $|0\rangle, |1\rangle$ は次式

のように時間発展する．

$$|0\rangle \to \frac{1}{\sqrt{2}} |0\rangle_s + e^{i\theta} \frac{i}{\sqrt{2}} |1\rangle_l \tag{2.30}$$

$$|1\rangle \to \frac{1}{\sqrt{2}} |1\rangle_s + e^{i\theta} \frac{i}{\sqrt{2}} |2\rangle_l \tag{2.31}$$

ただし，添え字の s, l はそれぞれ干渉計の短経路と長経路を通る光子，$|2\rangle$ は時間位置 $t_2 = t_1 + \tau$ に光子が存在する状態を表す．これが，MZI 出力側ビームスプリッタ直前の状態となる．二経路を経た光子状態は出力側ビームスプリッタで合波される．ここで，$|k\rangle_s, |k\rangle_l$ はそれぞれ次式のように時間発展する．

$$|k\rangle_s \to \frac{1}{\sqrt{2}} |k\rangle_x + \frac{i}{\sqrt{2}} |k\rangle_y \tag{2.32}$$

$$|k\rangle_l \to \frac{i}{\sqrt{2}} |k\rangle_x + \frac{1}{\sqrt{2}} |k\rangle_y \tag{2.33}$$

ただし，添え字の x, y はそれぞれ図 2.6(b) 中の出力ポート x, y に出力される光子状態を表す．式 (2.32), (2.33) を式 (2.30), (2.31) に代入すると，MZI 入力前の状態 $|0\rangle, |1\rangle$ の，MZI 通過に伴う一連の時間発展が次のように表される．

$$|0\rangle \to \frac{1}{2} \left(|0\rangle_x + i |0\rangle_y - e^{i\theta} |1\rangle_x + ie^{i\theta} |1\rangle_y \right) \tag{2.34}$$

$$|1\rangle \to \frac{1}{2} \left(|1\rangle_x + i |1\rangle_y - e^{i\theta} |2\rangle_x + ie^{i\theta} |2\rangle_y \right) \tag{2.35}$$

ここで，改めて $\theta \to \theta + \pi$ とし，ポート x への出力状態に着目すると，MZI 通過を表す演算子 $\hat{M}_x$ が次式で与えられることが分かる．

$$\hat{M}_x = \frac{1}{2} \sum_{k=0}^{1} \left(|k\rangle_x + e^{i\theta} |k+1\rangle_x \right) \langle k| \tag{2.36}$$

同様に，出力ポート y への透過を表す演算子 $\hat{M}_y$ が次式で与えられる．

$$\hat{M}_y = \frac{1}{2} \sum_{k=0}^{1} \left(- |k\rangle_y + e^{i\theta} |k+1\rangle_y \right) \langle k| \tag{2.37}$$

ただし，MZI 出力後の光子に対する伝搬位相分の任意性があるため，全体にかかる位相項は無視した．MZI からの出力状態を単一光子検出器で測定すると，図 2.6(b) の単一光子検出器直前に描かれた時間位置 t_0, t_1, t_2 のどこか一つで光子が検出される．先述の通り，光子検出器による測定は時間位置への射影測定に対応する．よって，ポート x における時間位置 j での光子検出に対応する測定演算子 $\hat{M}_j^x$ および POVM 要素 $\hat{E}_j^x$ は，次式で与え

られる．

$$\hat{M}_j^x = |j\rangle\langle j|_x \hat{M}_x \tag{2.38}$$

$$\hat{E}_j^x = \hat{M}_j^{x\dagger}\hat{M}_j^x = \hat{M}_x^\dagger |j\rangle\langle j|_x \hat{M}_x \tag{2.39}$$

式 (2.36) を式 (2.39) に代入すると，POVM 要素が具体的に次式のように表される．

$$\hat{E}_0^x = \frac{1}{4}|0\rangle\langle 0| \tag{2.40}$$

$$\hat{E}_1^x = \frac{1}{2}\left(\frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| + e^{-i\theta}\langle 1|}{\sqrt{2}}\right) \tag{2.41}$$

$$\hat{E}_2^x = \frac{1}{4}|1\rangle\langle 1| \tag{2.42}$$

出力ポート y についても同様である．上式は，時間位置 t_0, t_2 における光子検出確率が，状態 $|0\rangle, |1\rangle$ への射影測定の測定確率に比例し，時間位置 t_1 における光子検出確率が状態 $\left(|0\rangle + e^{i\theta}|1\rangle\right)/\sqrt{2}$ への射影測定の測定確率に比例することを示している．これは時間位置 t_1 では，入力した 2 パルスが遅延によって重なり合って干渉し，干渉の結果が重ね合わせ状態への射影測定に対応するためである．一方，出力ポート y においてはビームスプリッタでの位相シフトにより干渉パターンが反転しており，POVM 要素は次式となっている．

$$\hat{E}_1^y = \frac{1}{2}\left(\frac{|0\rangle - e^{i\theta}|1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| - e^{-i\theta}\langle 1|}{\sqrt{2}}\right) \tag{2.43}$$

すなわち，時間位置 t_1 での光子検出確率は状態 $\left(|0\rangle - e^{i\theta}|1\rangle\right)/\sqrt{2}$ への射影測定の測定確率に比例する．なお，上式においては，$\sum_j \left(\hat{E}_j^x + \hat{E}_j^y\right) = \hat{\mathbb{1}}$ となっている．これは，エネルギー保存則を表しており，MZI での測定では入力された光子 (最小単位の光エネルギー) がどちらかのポートおよびいずれかの時間位置において必ず検出されることを示している．式 (2.41), (2.43) において $\theta = 0$ とすると，$\hat{E}_1^x = (1/2)|+\rangle\langle +|, \hat{E}_1^y = (1/2)|-\rangle\langle -|$ となる．これは，ポート x では状態 $|+\rangle$ が，ポート y では $|-\rangle$ が測定されることを意味している．

これまで述べたのは 2 次元タイムビン量子状態についてであったが，より高次元の場合には，用意した数の時間スロットを収容するように式 (2.36), (2.37) の総和の範囲を拡張すればよい．また，異なる遅延時間の MZI の場合には，式中の $|k+1\rangle_x$ などの時間シフト $+1$ を対応する遅延時間に変更することで，測定演算子を得ることができる．後の第 3 章，および第 4 章では，複数の MZI 通過を表す演算子を，通過する回数分乗ずることによって，多段接続した MZI の測定演算子を導出する．

2.3　多光子のタイムビン量子状態

2.3.1　多光子の量子状態と量子もつれ状態

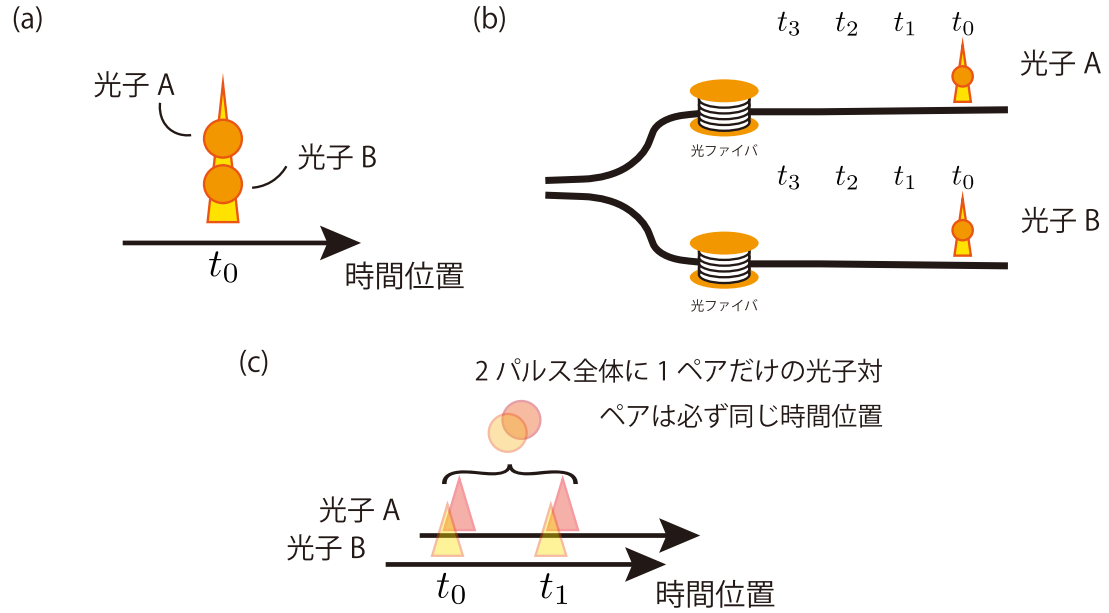

図 2.7　(a) 二光子が同一の時間スロット中に存在する状態の模式図．便宜上光子 A, B としているが区別はできない．(b) 二つの異なる伝送路を伝搬するタイムビン量子状態 $|00\rangle_{AB}$ の模式図．二光子は伝送路により識別できる．(c) 光子対の重ね合わせ状態 (量子もつれ状態) の模式図．

2.2 節では，1 光子の純粋量子状態と混合量子状態およびその測定について述べた．本節では，量子もつれ状態を含む複数光子の量子状態について述べる．なお，2 光子状態としては，同一の時間スロットに複数個の光子が存在する状態 [図 2.7(a)] ではなく，異なる伝送路に光子が存在する状態 [図 2.7(b)] について考える．2 光子をまとめてひとつの量子状態とみなした状態は，各 1 光子量子状態ベクトルの組合せを記述可能な，テンソル積を用いて表される．たとえば，二つの光子 A, B がともに時間位置 t_0 に確定的に存在する状態は，$|0\rangle_A \otimes |0\rangle_B$ と表される．ただし $\otimes$ はテンソル積であり，文脈上明らかな時には $\otimes$ を省略し，$|0\rangle_A |0\rangle_B$ や $|00\rangle_{AB}$ ，あるいは単に $|00\rangle$ と表記する．この表記を一般化すると，時間位置 t_i, t_j に 2 光子がそれぞれ確定的に存在する状態は $|i\rangle_A |j\rangle_B$ と表される．さらにこれを重ね合わせ状態まで拡張した一般の 2 光子の純粋タイムビン量子状態 $|\psi\rangle_{AB}$ は，次式で表される．

$$|\psi\rangle_{AB} = \sum_{ij} c_{ij} |i\rangle_A |j\rangle_B \tag{2.44}$$

ただし，c_{ij} は $\sum_{ij}|c_{ij}|^2 = 1$ を満たす確率振幅である．例えば，次式のような状態を考える．

$$\left|\Psi^{00}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{AB} \tag{2.45}$$

この状態は，図 2.7(c) に示すように，光子 A, B がともに時間位置 t_0 に存在する状態 $|00\rangle$ と，光子 A, B がともに時間位置 t_1 に存在する状態 $|11\rangle$ の重ね合わせ状態である．また，すぐ後に確認するように，この状態は量子もつれ状態である．さらに光子の数および経路数が多い場合には，$|i\rangle_A|j\rangle_B|k\rangle_C\cdots$ というように，光子数分だけテンソル積の数を増やせばよい．

$|i\rangle_A \otimes |j\rangle_B$ などの状態は，光子 A, B それぞれの状態の単純な掛け合わせによって表されている．このように，全体の量子状態 $|\psi\rangle_{AB}$ が個々の量子状態 $|\phi\rangle_A, |\chi\rangle_B$ の積 $|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\chi\rangle_B$ と表される状態を，プロダクト (掛け合わせ) 状態という．古典的な確率分布でいえば，独立な確率変数 A, B の結合確率分布が，それぞれの確率変数の周辺確率分布の積で表されることに相当する，独立な 2 光子状態である．状態ベクトルと同様に，プロダクト状態の状態密度演算子も各光子の状態密度演算子のテンソル積として表すことができる．すなわち，光子 A, B を表す状態密度演算子を $\hat{\rho}_A, \hat{\rho}_B$ とすると，2 光子全体の状態密度演算子は $\hat{\rho}_{AB} = \hat{\rho}_A \otimes \hat{\rho}_B$ と表される．

さらに，これを一般化して，確率分布 p_i に従ってプロダクト状態 $\hat{\rho}^i_{AB} = \hat{\rho}^i_A \otimes \hat{\rho}^i_B$ が存在する状態の密度演算子は，平均として

$$\hat{\rho}_{AB} = \sum_i p_i \hat{\rho}^i_A \otimes \hat{\rho}^i_B \tag{2.46}$$

と表される．式 (2.46) のように書くことができる状態をセパラブル (Separable) 状態という．このような状態は，生起確率が p_i で与えられるある変数 i を介した古典的な相関をもった状態と言える．

一方，式 (2.45) の量子状態 $\left|\Psi^{00}\right\rangle$ は，その状態密度演算子 $\hat{\rho}_{AB} = \left|\Psi^{00}\right\rangle\!\left\langle\Psi^{00}\right|$ をどのように分解しても，式 (2.46) のように各プロダクト状態の線形結合で書くことができない．このようなセパラブルではない 2 光子量子状態を量子もつれ状態という．量子もつれ状態をセパラブル “ではない” 状態という間接的な定義をする理由は，第 3 章で詳しく議論する隠れた変数理論と関わりがある．先に述べたように，セパラブル状態はある変数 i を介した古典的な相関をもった状態と言える．2.2.2 節で述べたように，状態密度演算子が式 (2.46) のように分解できることは，そのような変数 i を介して量子状態が実際に生成されたことを意味しない．しかしながら，そのようなモデルによって測定値の分布を再現することは可能である．一方，量子もつれ状態を式 (2.46) のように表されない状態と定義するということは，量子もつれ状態が有する測定値の分布/相関特性は，なんらかの変数 i が介在するとしたモデルでは説明できないことを示唆する．すなわち，ここまでその

他の状態に対して補足したような古典的なアナロジーやイメージで説明できない，量子力学的な記述によって初めて記述できる状態が量子もつれ状態である．逆に言うと，そのようなモデルでは説明できない測定結果が得られれば，被測定状態は量子もつれ状態であると結論できる．第 3 章では，そのような相関特性評価により量子もつれ状態を実験的に検証している．

上記では, 2 光子量子状態を記述するヒルベルト空間の基底状態として, $|ij\rangle_{AB}$ を採用した．一方, 1 光子状態が $\{|0\rangle, |1\rangle\}, \{|+\rangle, |-\rangle\}$, または $\{|R\rangle, |L\rangle\}$ の線形結合で表されたのと同様に, 同じ 2 光子量子状態を別の基底状態で記述することもできる．例えば, 式 (2.45) で表される重ね合わせ状態 $\left|\Psi^{00}\right\rangle$ に，次式で定義される量子状態 $\left|\Psi^{01}\right\rangle, \left|\Psi^{10}\right\rangle, \left|\Psi^{11}\right\rangle$ を加えた 4 つの状態は互いに直交しており，これらを基底状態として 2 次元 2 光子のヒルベルト空間の基底が定義される．

$$\left|\Psi^{01}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)_{AB} \tag{2.47}$$

$$\left|\Psi^{10}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)_{AB} \tag{2.48}$$

$$\left|\Psi^{11}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)_{AB} \tag{2.49}$$

上記の 4 状態が正規直交基底をなすこと，すなわち

$$\left|\left\langle \Psi^{ij} \middle| \Psi^{i'j'} \right\rangle\right|^2 = \delta_{ii'}\delta_{jj'} \tag{2.50}$$

が成り立つことは，式 (2.45)–(2.49) より容易に確認できる．したがって，任意の 2 次元 2 光子純粋状態を $|\psi\rangle_{AB} = \sum_{ij} c_{ij} \left|\Psi^{ij}\right\rangle$ と記述することができる．なお，上記 4 状態はすべて量子もつれ状態となっている．この基底 $\{\left|\Psi^{ij}\right\rangle\}$ はベル基底とも呼ばれ，BBM92 の安全性証明など量子情報分野の様々な場面で登場する．また，第 5 章では，有限体を利用して高次元量子状態に拡張した一般化ベル基底を用いることで，高次元 QKD プロトコルの安全性証明を行う．

2.3.2 量子状態の全系と部分系および最大もつれ状態

図 2.8 のように，全量子系が与えられている時の，その部分系について考える．2 光子の状態密度演算子 $\hat{\rho}_{AB}$ が与えられたとき，その部分系であるどちらか一方の光子の状態密度演算子は，他方の光子についての部分トレースを取ることで得られる．光子 B に対する部分トレースは $\mathrm{Tr}_B(\hat{\rho}_{AB}) = \sum_i \langle i|_B \hat{\rho}_{AB} |i\rangle_B$ で与えられるが，これは物理的には手元に光子 A のみがあり，光子 B について何も情報が得られないことを意味する．この時，光子 B は何も処理がされていなくてもよいし，測定やユニタリー変換など何らかの操作が施されていてもよいが，光子 A の状態を考えるにあたり，光子 B についてのこれ

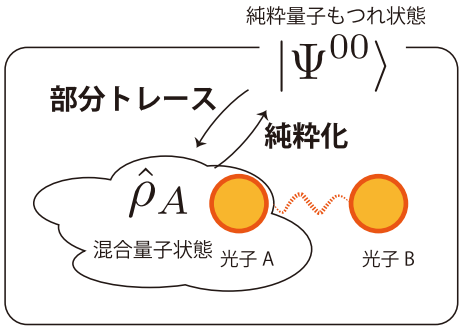

図 2.8　量子状態の全系と部分系の関係図．部分トレースは，全系から部分系を抽出する操作である．一方，純粋化は部分系のみが与えられた時に，取りうる全系を数学的に再構成することに相当する．図では全系=2 光子，部分系=光子 A であるが，多光子や光子 B なども同様である．

らの情報は考慮されない．古典的な確率分布で言えば，確率変数 A, B の結合確率分布から，確率変数 A のみの周辺確率分布を求める操作に相当する．光子 B の情報を用いないのは，条件付き確率分布ではなく周辺確率分布に相当する状態を考える，ということである．例えば，ベル基底状態 $|\Psi^{00}\rangle$ にある 2 光子のうち光子 A の状態密度演算子 $\hat{\rho}_A$ は，次のように得ることができる．

$$\begin{aligned}\hat{\rho}_A &= \mathrm{Tr}_B(|\Psi^{00}\rangle\langle\Psi^{00}|) \\ &= \sum_{i=0}^{1} \langle i|_B \left(|\Psi^{00}\rangle\langle\Psi^{00}|\right) |i\rangle_B \\ &= \frac{1}{2}\left(|0\rangle\langle 0|_A + |1\rangle\langle 1|_A\right) \\ &= \frac{1}{2}\hat{\mathbb{1}}_A \end{aligned} \tag{2.51}$$

この状態密度演算子は，2.2 節で議論した，状態 $|0\rangle, |1\rangle$ が一様ランダムな乱数によって選びだされた古典状態の状態密度演算子と同じである．前述の通り，この量子状態 $\hat{\rho}_A$ の von Neuman エントロピー $S(\hat{\rho}_A)$ は，2 次元量子状態としては最大の 1 ビットである．このような von Neuman エントロピーが最大である状態を最大混合状態という．$\hat{\rho}_A$ は恒等演算子に比例しており，任意の 2 次元正規直交基底 $\{|\phi_0\rangle, |\phi_1\rangle\}$ において，どちらかの状態への射影測定の測定確率が $\langle\phi_i|\hat{\rho}_A|\phi_i\rangle = 1/2 \cdot \langle\phi_i|\hat{\mathbb{1}}|\phi_i\rangle = 1/2$，すなわち一様ランダムとなる．次節でみるように，このランダムな測定結果は光子 B に対する測定結果と相関があるが，部分トレースではその情報が得られない．この場合，上記の考察において，光子 A を状態 $|\phi_0\rangle, |\phi_1\rangle$ とするための乱数の役割を，光子 B が担っていると考えることができる．ただし，光子 B の測定が光子 A より先に行われる必要はなく，あくまで乱数の役割を担うモデルが構築可能なだけである．同様にして，光子 B についても最大混合状態であることが確認できる．

一方，もとのベル基底状態 $\left|\Psi^{00}\right\rangle$ 自体は純粋量子状態であり，その von Neuman エントロピーは $S\left(\left|\Psi^{00}\right\rangle\!\left\langle\Psi^{00}\right|\right)=0$ ビットである．このことは，状態 $\left|\Psi^{00}\right\rangle$ に対してベル基底 $\left\{\left|\Psi^{ij}\right\rangle\right\}$ のどの状態であるかを判定する射影測定 (これをベル測定という) を行えば，確率 1 で $\left|\Psi^{00}\right\rangle$ という測定結果が得られることからも示唆される．このようにベル基底状態は，個々の光子に関して測定を行うと，どのような測定を用いても完全にランダムな結果となる一方，全状態の測定には不確定さがない．

ベル基底状態のように，一方の光子の量子状態が最大混合状態となるような純粋量子もつれ状態は，最大もつれ状態と呼ばれる．次式で与えられる量子状態 $|\Psi_{\mathrm{MES}}\rangle_{AB}$ は，d 次元最大もつれ状態の例である．

$$|\Psi_{\mathrm{MES}}\rangle_{AB}=\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle_{AB} \tag{2.52}$$

この状態における光子 A の状態密度演算子は $\hat{\rho}_A=\hat{\mathbb{1}}/d$ であり，$S(\hat{\rho}_A)=\log_2 d$ の最大混合状態となっている．

ここまで，ある 2 光子の純粋状態 $|\psi\rangle_{AB}$ が与えられたときに，その部分系の量子状態 $\hat{\rho}_A$ を求める手法について述べた．一方，ある混合状態 $\hat{\rho}_A$ が与えられたときに，補助系 R を加えることにより，全系として純粋状態とすることができる．この手法を純粋化 (Purification) という．純粋化によって，例えば図 2.8 のように，最大混合状態から最大もつれ状態を構成することができる．ただし，純粋化はあくまで数式的な操作であって，光子 A が与えられたときに，対応する純粋量子状態を物理的に得る手法ではない．最大混合状態から最大もつれ状態を構成する例のように，補助系 R に対応する物理系が実際に存在する可能性はあるが，そのような系が実在する保証はない．なお，後述する量子もつれ蒸留は，不完全な量子もつれ状態から純粋量子もつれ状態を取り出す物理的な手法であるが，純粋化とは別の概念である．

光子 A の状態密度演算子が $\hat{\rho}_A=\sum_i \lambda_i\,|\psi_i\rangle\langle\psi_i|$ と対角化できる場合，補助系 R を用いた $\hat{\rho}_A$ の純粋化状態は次式で表される．

$$|\psi\rangle_{AR}=\sum_i \sqrt{\lambda_i}\,|\psi_i\rangle_A\,|i\rangle_R \tag{2.53}$$

ここで，$|i\rangle_R$ は系 R での d 次元正規直交基底の元である．正規化された直交状態であれば，この状態は任意に形成することができる．したがって，次式の状態もまた $\hat{\rho}_A$ の純粋化状態となる．

$$|\psi\rangle_{AR}=\sum_i \sqrt{\lambda_i}\,|\psi_i\rangle_A\otimes\hat{U}_R\,|i\rangle_R \tag{2.54}$$

ここで，$\hat{U}_R$ は $d'\times d$ アイソメトリー演算子である (ただし $d'\geq d$)．アイソメトリー演算子はユニタリー演算子の拡張であり，d 次元ヒルベルト空間から，d' 次元ヒルベルト空間

中の d 次元部分空間へのユニタリー変換である．この場合，見かけ上次元が増加するが，実質的には $d \times d$ ユニタリー変換となっている．例えば，古典的なアイソメトリー演算子の例として，3 入力 3 出力ビームスプリッタ透過による，光電場の経路状態の変化について考えてみる．ビームスプリッタの入力ポートの一つは光ターミネータで終端されているとする．3 入力 3 出力ビームスプリッタによる光電場の変換は，原理的には 3 次元ユニタリー演算子で記述できるが，終端のために，実効的には 2 入力 3 出力のビームスプリッタとなっており，光電場の状態変化は入力が 2 次元，出力が 3 次元の演算子で記述される．この場合，出力として観測される電場の状態は，見かけ上 3 次元ベクトルで表される．しかし，仮にこのビームスプリッタによる時間発展を巻き戻した時に，終端した入力ポートから光が入力されているような出力側の光電場は現れない．したがって，見かけ上 3 次元であるが，実効的には入力と同じ次元，すなわち 2 次元部分空間上の光電場しか出力側には現れない．このように，見かけ上の入出力の次元が異なるが実効的な次元が等しく，エネルギー保存 (量子力学では確率の保存) が成り立つ演算子がアイソメトリー演算子である．光子 A については次元が既知であるが，一般の補助系については次元に制限がないために，このような拡張が必要となる．任意の純粋化状態は式 (2.54) のように記述できる．

このように純粋化において，系 R にアイソメトリー変換の自由度があることは，4 つのベル基底状態 $\left|\Psi^{ij}\right\rangle$ すべてにおいて，光子 A の状態が最大混合状態となっていることからも示唆される．自由度があるということは，補助系 R が実際にどのような状態であるかは，系 R 自身を測定しない限りわからないということである．ただし，情報に関連する量は，アイソメトリー変換を施してもしばしば不変である．例えば，式 (2.54) の状態から，補助系 R の密度演算子が次式で与えられる．

$$\hat{\rho}_R = \sum_i \lambda_i \hat{U}_R \left|i\right\rangle\!\left\langle i\right|_R \hat{U}_R^\dagger \tag{2.55}$$

上式において，$\left|i'\right\rangle_R = \hat{U}_R \left|i\right\rangle_R$ とすれば，$\left|i'\right\rangle$ の直交性より，$\hat{\rho}_R$ は固有値 λ_i をもつ状態 $\left|i'\right\rangle$ で対角化される．よって，任意の純粋化において，補助系 R の von Neuman エントロピー $S(\hat{\rho}_R)$ は，固有値 λ_i を確率分布とみなした Shannon エントロピー $\mathrm{H}(\lambda_i)$ に一致する．ほとんどの場合，このように状態を再定義することでアイソメトリー変換の自由度を考慮する必要がなくなり，基本的には純粋化状態として式 (2.53) のみを考えればよいことになる．さらに，補助系 R の von Neuman エントロピーは，もとの光子 A の von Neuman エントロピー $S(\hat{\rho}_A)$ に等しい．特に，光子 A が純粋状態であり，その von Neuman エントロピーが 0 であるならば，純粋化における補助系 R の von Neuman エントロピーは，いかなる場合でも 0 である．第 5 章では，高次元 QKD において，この補助系 R がすべて盗聴者 Eve に所有されているという最悪の状況を想定することで，盗聴者 Eve の持ちうる情報量の上限を求め，この情報量を除去した安全な秘密鍵の生成効率を見積もっている．

2.3.3　2 光子の量子測定とベル基底状態の相関

量子もつれ状態の相関特性の具体例として，2 光子状態の測定について考える．演算子 $\hat{M}_A, \hat{M}_B$ で表される測定を光子 A, B それぞれに対して行う場合の，全体の測定演算子 $\hat{M}_{AB}$ は $\hat{M}_A \otimes \hat{M}_B$ で表される．例えば，図 2.9(a) のように，光子 A は射影測定により $|0\rangle_A$ に射影され，光子 B については何もしないという測定を記述する演算子は，$\hat{M}_{AB} = |0\rangle\langle 0|_A \otimes \hat{\mathbb{1}}_B$ である．この測定を式 (2.45) で表される量子もつれ状態 $|\Psi^{00}\rangle$ に対して行った時の状態変化は，次のように記述される．

$$\begin{aligned}\left(|0\rangle\langle 0|_A \otimes \hat{\mathbb{1}}_B\right)|\Psi^{00}\rangle &= \left(|0\rangle\langle 0|_A \otimes \hat{\mathbb{1}}_B\right)\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{AB} \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0|_A |00\rangle_{AB} + |0\rangle\langle 0|_A |11\rangle_{AB}\right) \\ &= \frac{1}{\sqrt{2}}|00\rangle_{AB} \end{aligned} \tag{2.56}$$

上式は，1/2 の確率で，測定後の状態が $|00\rangle_{AB}$ となることを示している．同様に，光子 A に対して状態 $|1\rangle$ へ射影測定を行うと，1/2 の確率で状態 $|11\rangle_{AB}$ となる．この考察は，

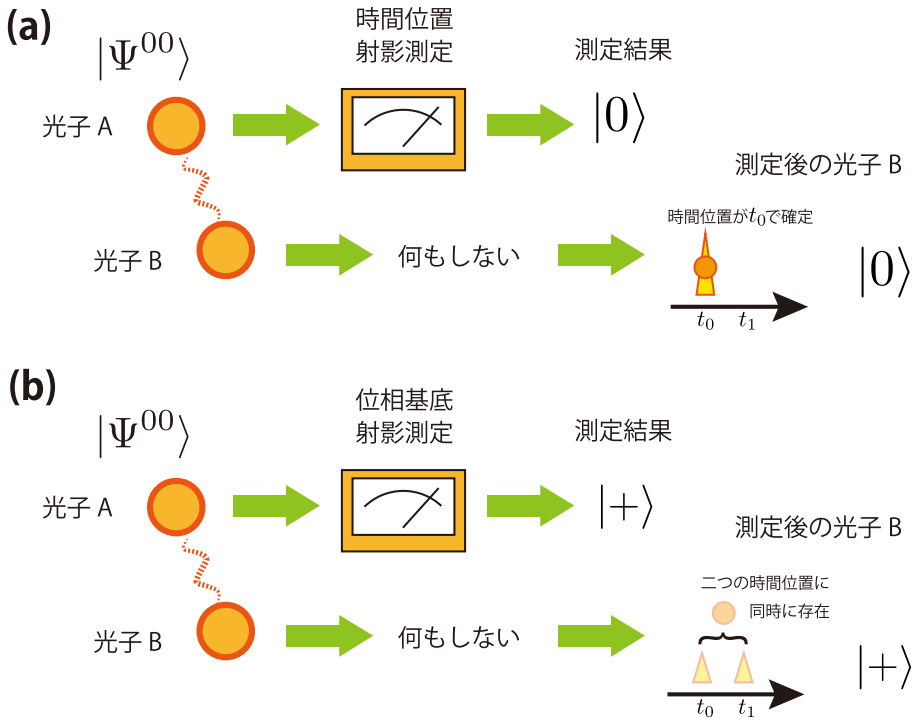

図 2.9　量子もつれ状態に対する測定値の相関関係．(a) 光子 A に時間位置基底状態への射影測定を行い，$|0\rangle$ が観測されたときの光子 B の状態．(b) 光子 A に位相基底状態への射影測定を行い，$|+\rangle$ が観測されたときの光子 B の状態．

光子 A に対して時間位置基底状態への射影測定を行うと，その測定結果は一様ランダムであり，かつ光子 B に対して何も行わなかったにも関わらず，2 光子ともに同じ時間位置基底状態に射影されることを示している．そのほかのベル基底状態についても同様の測定を行うと，2 光子 A, B は $\left|\Psi^{01}\right\rangle$ では同じ時間位置基底状態に，$\left|\Psi^{10}\right\rangle, \left|\Psi^{11}\right\rangle$ では光子 B の時間位置を反転した時間位置基底状態 ($|01\rangle$ もしくは $|10\rangle$) にそれぞれ射影される．このように，量子もつれ状態にある 2 光子間には，ベル基底状態のインデックスに従った相関特性が存在する．この相関特性を利用すると，離れた 2 者がそれぞれの光子 AB を時間位置基底状態に射影測定することにより，同一の 2 値乱数を共有することができる．

一方，図 2.9(b) のように，$\left|\Psi^{00}\right\rangle$ の光子 A を位相基底状態 $|+\rangle, |-\rangle$ へ射影測定した時の状態変化は，次のように記述される．

$$\begin{aligned}
\left(|+\rangle\langle+|_A \otimes \hat{\mathbb{1}}_B\right)\left|\Psi^{00}\right\rangle &= \left(|+\rangle\left(\frac{\langle 0|+\langle 1|}{\sqrt{2}}\right)_A \otimes \hat{\mathbb{1}}_B\right)\left|\Psi^{00}\right\rangle \\
&= \frac{1}{\sqrt{2}}\left(|+\rangle\langle 0|_A\left|\Psi^{00}\right\rangle + |+\rangle\langle 1|_A\left|\Psi^{00}\right\rangle\right) \\
&= \frac{1}{2}\left(|+\rangle_A|0\rangle_B + |+\rangle_A|1\rangle_B\right) \\
&= \frac{1}{\sqrt{2}}|+\rangle_A \otimes \left(\frac{|0\rangle_B + |1\rangle_B}{\sqrt{2}}\right) \\
&= \frac{1}{\sqrt{2}}|{+}{+}\rangle_{AB}
\end{aligned} \tag{2.57}$$

上式は，確率 1/2 で 2 光子ともに $|+\rangle$ である測定結果が得られることを示している．$|-\rangle$ についても同様である．これらの結果は，ベル基底状態を位相基底状態 $|+\rangle, |-\rangle$ を用いて次式のように書き直すことでも理解できる．

$$\left|\Psi^{00}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle + |{-}{-}\rangle\right)_{AB} \tag{2.58}$$

$$\left|\Psi^{01}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|{+}{-}\rangle + |{-}{+}\rangle\right)_{AB} \tag{2.59}$$

$$\left|\Psi^{10}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle - |{-}{-}\rangle\right)_{AB} \tag{2.60}$$

$$\left|\Psi^{11}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|{-}{+}\rangle - |{+}{-}\rangle\right)_{AB} \tag{2.61}$$

このように，$\left|\Psi^{00}\right\rangle, \left|\Psi^{10}\right\rangle$ では光子 A, B ともに同じ測定結果，$\left|\Psi^{01}\right\rangle, \left|\Psi^{11}\right\rangle$ では反転した測定結果が得られる．時間位置基底測定時の相関特性と合わせて整理すると，$\left|\Psi^{ij}\right\rangle$ は，$i = 1$ だと時間位置基底での測定結果が光子 A, B で反転し，$j = 1$ だと位相基底での測定結果が反転する．ベル基底状態においては，光子 A, B のどちらか一方の量子ビットに対して，時間位置基底状態 $|0\rangle$ と $|1\rangle$ を入れ替える時間位置反転，あるいは $|+\rangle$ と $|-\rangle$ を入れ替える位相反転により，4 つの状態を相互に変換することができる．光子 A, B に

ついて同じ測定結果が得られるように設計されたシステムにおいては，$\left|\Psi^{00}\right\rangle$ のみがどちらの基底についても正しい結果を与え，その他の状態は時間位置エラーまたは位相エラーを誘起する．

ここで，ベル基底状態に備わっている量子相関特性と古典的相関特性の違いについて述べる．まず，次の密度演算子 $\hat{\rho}_{AB}$ で表される混合量子状態を考える．

$$\hat{\rho}_{AB} = \frac{1}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)_{AB} \tag{2.62}$$

このような状態は，一様ランダムな 0, 1 の乱数に従って状態 $|00\rangle, |11\rangle$ を生成することにより得られる．この状態は，時間位置基底状態への射影測定では，2 光子 A, B 間で完全な相関性を有する．しかしながら，同じ状態に対して光子 A を位相基底状態 $|+\rangle$ に射影測定すると，光子 B は完全混合状態となる．この場合，光子 B に対していかなる測定を行ったとしても，その測定結果は光子 A の測定結果とは全く無相関となる．前述のように，量子もつれ状態に対しては，射影する基底を変えた測定を行っても，2 光子の測定結果は完全な相関を持つ．これに対し，式 (2.62) で表されるような混合状態，すなわち古典的相関のある 2 光子状態では，そのような相関がない．

また，純粋化においても量子もつれ状態と式 (2.62) の古典状態には違いがある．まず，式 (2.62) で表される古典状態の純粋化を考える．これに補助系 R を加えて純粋化した状態 $|\psi\rangle_{ABR}$ は次式で与えられる．

$$|\psi\rangle_{ABR} = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{ABR} \tag{2.63}$$

上式は，光子 A, B に加えて，補助系 R の状態も時間位置基底に関して完全な相関性を示している．したがって，この光子 A, B を用いる QKD システムにおいて，補助系 R が盗聴者 Eve に入手されると，光子 A, B の時間位置基底に関する情報は完全に盗聴されていることになる．これに対し，ベル基底状態はそのままで純粋状態である．あえて補助系 R を加えた純粋化状態として表すと，補助系 R の状態を任意の量子状態 $|\phi\rangle_R$ として，

$$|\psi\rangle_{ABR} = \left|\Psi^{00}\right\rangle_{AB} \otimes |\phi\rangle_R \tag{2.64}$$

となる．この場合，光子 A, B の状態や測定結果に関わらず，補助系 R は任意の状態 $|\phi\rangle_R$ となっており，光子 A, B とは全く相関が無い．

以上述べたように，純粋量子もつれ状態には

- 各光子 A, B を各々測定した結果は完全にランダムである．
- 一方の測定結果を得ることで，他方の量子状態が一意に定まる．
- もつれを構成する 2 光子以外とは一切の相関を持たない．

という，古典状態とは異なる特異な性質が備わっている．この性質を利用することで，究極的に安全な QKD システムを構築することができる．

2.4　BBM92 の安全性証明と Six-state プロトコル

前節にて，純粋な量子もつれ状態は外部と相関を持たないことを述べた．本節では，ノイズのある QKD システムにおいて，外部と相関のない安全な鍵を共有する手法の概略を紹介する．ただしここでは，第 1 章で述べた Shor-Preskill の証明 [13] ではなく，原理的に等価でより直感的な，小芦による Shor-Preskill の証明の解説に基づいて説明する [14].

BBM92 では次頁に示すプロトコル 1 の手順に従って，秘密鍵を生成する．なおここでは，BB84 の安全性証明に展開可能なように，オリジナルの BBM92(図 1.1) ではなく，それを Prepare and Measure 型と等価とみなせるように変形したプロトコルを示してある．以下，プロトコル 1 について，いくつか補足する．Alice/Bob の測定結果の不一致，すなわち共有した乱数列のエラーはすべて伝送路の影響によるものと考え，実際の測定装置の不完全性に起因するエラーはここでは考えない．別の言い方をすると，検出器のノイズなどの装置の不完全性によるエラーも伝送路によるものとみなすということである．これは最悪設定として，共有した乱数のエラーは全て盗聴行為によるものとみなす考え方に基づく．ただし，厳密には全ての装置の不完全性に対して，このような取り扱いが可能なわけではない．例えば，Alice と Bob 双方の位相基底の実装が大きくずれており，実際には位相基底の代わりに時間位置基底が実装されるような不完全性が生じた場合，後で述べる位相エラーが評価できなくなり，安全性を担保できない．このような実装と理論のずれの定量化や，装置の具体的な動作に依存しないプロトコルの研究は，理想的な安全性証明と実用的な安全性の乖離を補完する研究として進められているが [21, 82–84]，ここではそこまで深入りしない．なお，ここでは原理説明のため，伝送損失による光子の損失はないものとしているが，Bob に光子が届いた事象のみを対象とすれば，鍵生成手順としての不具合はない．さらに，手順 6 において，パリティ検査行列を用いた誤り訂正を想定しているが，これは後述のプロトコル 2 との等価性を考慮したためであり，実際には他の誤り訂正法を用いてもよい．

プロトコル 1 では，光子送受信後に「認証付き一般通信路」を用いて，各種情報交換を行っている．このことについて説明する．Alice と Bob は光子を送るための伝送路だけでなく，基底情報交換/誤り訂正などのために一般通信路も併用している．この一般通信路としては，通常のインターネット通信などを用いる．ただし，Alice，Bob は互いの送信情報について必ず認証を行うものとする．これは，一般通信情報を改竄されると鍵の安全性が保証できなくなるからである．この認証は，一般通信情報について，ランダムに選んだハッシュ関数によりハッシュ値を計算し，さらにハッシュ値をワンタイムパッド方式

プロトコル **1** BBM92

1: Alice は 2 つの光子 A, B をベル基底状態 $\left|\Psi^{00}\right\rangle$ として準備する．そして，一方の光子を伝送路を介して Bob に送る．この伝送路に対しては，あらゆる盗聴が可能であるとする．

2: Alice と Bob は各々が保有している光子に対して，ランダムに時間位置基底状態 $\{|0\rangle, |1\rangle\}$ もしくは位相基底状態 $\{|+\rangle, |-\rangle\}$ への射影測定を行う．

3: Alice と Bob は上記の送受信を繰り返した後，各測定に際して時間位置/位相基底のどちらへの射影測定を行ったかを認証付き一般通信路 (盗み聞きはできるが改竄はできない通信路) を用いて通知しあう．そして，元々ペアであった 2 光子について，基底が異なる測定結果は破棄し，同じであった測定結果を残す．

4: Alice と Bob はベル基底状態にあった 2 光子から得られた測定結果のペアの一部をランダムに選んで通知しあい，時間位置/位相基底それぞれの測定結果の誤り率 (不一致率) を推定する．誤り率推定に用いた測定結果は廃棄する．

5: 残った測定結果ついて，状態 $|0\rangle$ または $|+\rangle$ の測定結果を得た場合にビット 0 を，状態 $|1\rangle$ または $|-\rangle$ を得た場合にビット 1 を割り当て，ランダムなビット列を生成する．これをシフト (sift) 鍵と呼ぶ．

6: 手順 4 で推定した誤り率を基に，Alice は線形誤り訂正符号に従ってパリティ検査行列 $\mathbf{H}_z$ を生成し，それを自身のシフト鍵 κ_A に乗じた $\mathbf{z}_A = \kappa_A \mathbf{H}_z^T$ を計算する．Alice は用いた符号情報と $\mathbf{z}_A$ を，認証付き一般通信路を用いて Bob に通知する．Bob は自身のシフト鍵 κ_B に対して $\mathbf{z}_B = \kappa_B \mathbf{H}_z^T$ を計算し，シンドローム $\mathbf{s}_z = \kappa_A \oplus \kappa_B$ を得る．さらに，Bob は得られたシンドロームを用いてシフト鍵に対する誤り訂正を行い，Alice と同一のビット列を得る．これを訂正鍵という．

7: 先の誤り率から，盗聴者 Eve に漏洩し得る情報量の上限を推定し，訂正鍵に対して秘匿性増強と呼ばれる鍵の圧縮処理を施して，外部漏洩のない秘密鍵を得る．

で暗号化して送ることで，安全に実装することができる [85]．ハッシュ値の長さは一般通信情報ビット数や QKD によって新たに共有される秘密鍵ビット数と比べて十分短くてよく，認証に用いる秘密鍵量は十分に小さい．このように QKD では，認証のための短い秘密鍵を事前に共有しておく必要がある．したがって，厳密には，QKD は小さい秘密鍵量を増幅するシステムであり，ゼロから秘密鍵を生成するものではない．

BBM92 で生成される秘密鍵の安全性は，次頁の量子もつれ蒸留を用いたプロトコル 2 によって得られる秘密鍵と等価であることが知られている [13, 14]．なお，プロトコル 2 には安全性証明に関わるビット数などの量も記してある．

このプロトコル 2 の安全性は以下のように考察される．プロトコル 2 では，Alice は 2

プロトコル **2** 量子もつれ蒸留による等価プロトコル

1: Alice は 2 つの光子 A, B をベル基底状態 $\left|\Psi^{00}\right\rangle$ として準備し，光子 B を伝送路を介して Bob に送る．この過程を $N(1+2\xi)$ 回繰り返す．
2: Alice はランダムに $N\xi$ 個の光子対を選び，認証付き一般通信路を介して，どの光子対を選んだかを Bob に通知する．その後，Alice と Bob は当該光子対を時間位置基底状態に射影測定する．同様に，残りの光子対からランダムに選んだ $N\xi$ 個の光子対を位相基底状態に射影測定する．そして，認証付き一般通信路を介して，全ての測定結果を通知しあう．
3: 手順 2 で得られた測定結果から，残りの N 光子対について，時間位置基底への射影測定を行うとした場合の誤り (時間位置エラー) の個数の上限 N_z を推定する．同様に，位相基底への射影測定を行うとした場合の誤り (位相エラー) の個数の上限 N_x も推定する．
4: Alice と Bob は，最大 N_z 個の誤りを訂正する線形誤り訂正符号に基づいて，各々の N 個の光子に対してユニタリー変換を施す．そして，Alice と Bob はシンドロームに対応する光子を時間位置基底へ射影測定する．Alice は，Bob にシンドロームの測定結果を通知する．Bob は，Alice の測定結果と自身の測定結果を基に時間位置誤りパターンを特定し，光子 B に対して時間位置基底における誤り訂正を行う (時間位置エラー訂正)．
5: Alice と Bob は，上限 N_x 個の誤りがある時の誤りパターンの総数と同じパターン数の誤りを訂正可能な線形誤り訂正符号に基づいて，手順 4 で時間位置誤り訂正された光子にユニタリー変換を施す．Alice と Bob はシンドロームに対応する光子に対して位相基底への射影測定を行う．Alice は，Bob にシンドロームの測定結果を通知する．Bob は，Alice の測定結果と自身の測定結果を基に位相誤りパターンを特定し，光子 B に対して位相基底における誤り訂正を行う (位相エラー訂正)．
6: Alice と Bob は残りの光子対を時間位置基底状態へ射影測定し，その測定結果を秘密鍵とする．

つの光子 A, B をベル基底状態 $\left|\Psi^{00}\right\rangle$ として生成し，光子 B を Bob に送信するが，伝送路ではノイズの発生や盗聴行為による状態変化などが起こるため，伝送後に元のベル基底状態 $\left|\Psi^{00}\right\rangle$ が保たれている保証はない．前述の通り，ベル基底状態は 2 次元 2 光子の量子状態を記述するヒルベルト空間の基底をなすため，任意の 2 光子状態の密度演算子 $\hat{\rho}_{AB}$ はベル基底状態の線形結合として，$\hat{\rho}_{AB} = \sum_{iji'j'} r_{iji'j'} \left|\Psi^{ij}\right\rangle\!\left\langle\Psi^{i'j'}\right|$ と表される．さらに，プロトコル 2 では複数の光子対をまとめて取り扱っているため，プロトコル 2 の手順 4 開始時点における全体の量子状態は，光子対 $A_0B_0, A_1B_1, \cdots, A_{N-1}B_{N-1}$ それぞれに

ついてのベル基底状態のテンソル積の線形結合で表され，2^{2N} 次元ヒルベルト空間中の量子状態として記述される．ここで，考察対象としている N 光子対状態は，この 2^{2N} 次元ヒルベルト空間上の任意のケット状態からなる密度演算子ではなく，ベル基底状態によって対角化される特殊な状態であると仮定する．すると，N 光子対量子状態の密度演算子 $\hat{\rho}_{AB}$ は次式で与えられる．

$$\begin{aligned}\hat{\rho}_{AB} &= \sum_{\mathbf{i},\mathbf{j}} p(\mathbf{i},\mathbf{j}) \left|\Psi^{i_0 j_0}\right\rangle\!\left\langle\Psi^{i_0 j_0}\right|_{A_0 B_0} \otimes \cdots \otimes \left|\Psi^{i_{N-1} j_{N-1}}\right\rangle\!\left\langle\Psi^{i_{N-1} j_{N-1}}\right|_{A_{N-1} B_{N-1}} \\ &= \sum_{\mathbf{i},\mathbf{j}} p(\mathbf{i},\mathbf{j}) \left|\Psi_N^{\mathbf{i},\mathbf{j}}\right\rangle\!\left\langle\Psi_N^{\mathbf{i},\mathbf{j}}\right| \end{aligned} \tag{2.65}$$

ここで，i_n，j_n は n 番目光子対のベル基底における状態を示すインデックス，$\mathbf{i} = (i_0, \cdots, i_{N-1})$，$\mathbf{j} = (j_0, \cdots, j_{N-1})$ は各光子対状態を表すインデックスを要素とするベクトル，$p(\mathbf{i},\mathbf{j})$ は N 光子対が状態 $(\mathbf{i},\mathbf{j})$ である確率であり，$\left|\Psi_N^{\mathbf{i},\mathbf{j}}\right\rangle := \left|\Psi^{i_0 j_0}\right\rangle_{A_0 B_0} \otimes \cdots \otimes \left|\Psi^{i_{N-1} j_{N-1}}\right\rangle_{A_{N-1} B_{N-1}}$ である．式 (2.65) の状態は，確率 $p(\mathbf{i},\mathbf{j})$ に従って各光子対をベル基底状態からランダムに選んだ状態と言える．

図 2.10 に，プロトコル 2 の手順 4 以降の処理を図示する．プロトコル 2 では，手順 2, 3 によって，ランダムに選んだ $2N\xi$ 個の光子対に対する測定結果から，未測定の N 光子対における時間位置/位相エラーの個数の上限 N_z, N_x が見積もられている．そのため，確率 $p(\mathbf{i},\mathbf{j})$ は，これらの上限よりも少ないエラーを持つ N 光子対状態 $(\mathbf{i},\mathbf{j})$ のみが無視できない確率を持つ．2.3.3 節で述べたように，ベル基底状態 $\left|\Psi^{ij}\right\rangle$ のインデックス i が 1 の場合は時間位置基底における測定結果が反転する．よって，ベクトル $\mathbf{i}$ において，値が 1 である要素数は高々 N_z 個であり，それ以上である確率は十分小さい．もし $\mathbf{i}$ の中身が推定できれば，要素が 1 である光子対の光子 B に対し，時間位置基底状態 $|0\rangle, |1\rangle$ を反転する操作を施すことによって，$\mathbf{i} \to \mathbf{0}$，すなわち $\left|\Psi_N^{\mathbf{i},\mathbf{j}}\right\rangle \to \left|\Psi_N^{\mathbf{0},\mathbf{j}}\right\rangle$ と状態を変化させ，時間位置誤りを訂正することができる．ベクトル $\mathbf{i}$ は 0, 1 のビット列であり，1 の箇所が時間位置誤りを示す誤りパターンとみなすことができる．このように，$\mathbf{i}$ を古典的な誤りパターンとみなせば，時間位置基底測定の誤り率を $e_z = N_z/N$ として，長さ $\approx N\mathrm{H}(e_z)$ のシンドロームを持つ線形誤り訂正符号によって $\mathbf{i}$ を推定し，誤りを訂正することができる．このような古典的な誤り訂正手法が，以下の手順により量子ビットに対しても適用可能である．

まず，N_z 個のビット誤りを訂正可能な線形誤り訂正符号が存在し，そのシンドローム $\mathbf{s}_z$ がパリティ検査行列 H_z により $\mathbf{s}_z = \mathbf{i}\mathrm{H}_z^T$ と与えられるものとする．Alice は自身の持つ N 光子全体にユニタリー演算子 $\hat{U}_z$ を作用させ，ユニタリー変換後の光子の最後の $\approx N\mathrm{H}(e_z)$ 個の光子を，時間位置基底状態に射影測定する．同様に，Bob も同じユニタリー演算子 $\hat{U}_z$ による変換および時間位置基底状態への射影測定を行う．次に，Alice は一般通信路を介して，Bob に測定結果を送り，Bob は受け取った測定結果と自身の測定結

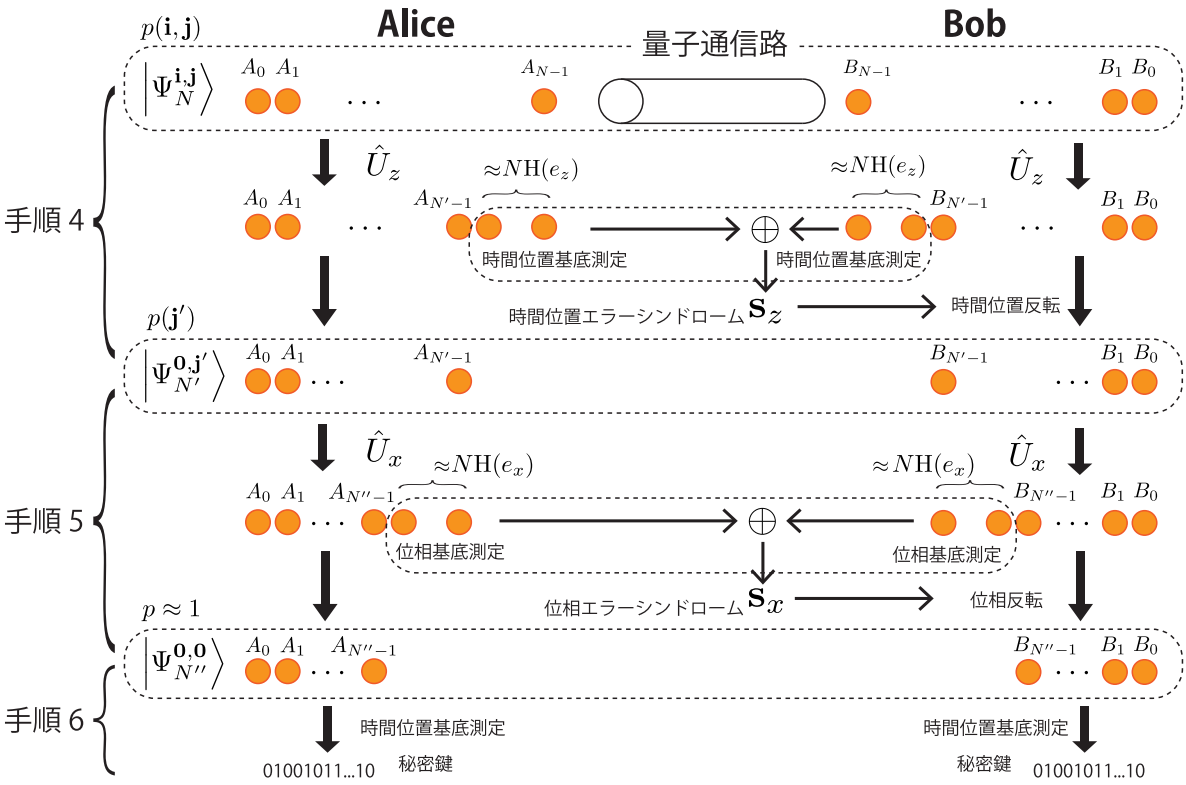

図 2.10　プロトコル 2 の手順 4 以降の処理を表す模式図．量子通信路を用いて N 光子対が共有されたところから誤り訂正を行い，純粋量子もつれ状態 $\left|\Psi_{N''}^{\mathbf{0},\mathbf{0}}\right\rangle$ を蒸留したのち，秘密鍵を得る．

果との排他的論理和を取る．この時，排他的論理和によって得られた結果がシンドローム $\mathbf{s}_z$ となるようなユニタリー演算子 $\hat{U}_z$ を構成することが可能である [14]．この過程では，Alice の測定結果を得ることによってランダムな符号選択が行われ，Bob はシンドロームと符号情報の和から符号の情報を取り除くことで，シンドロームを得る．そして，Bob はこのシンドローム $\mathbf{s}_z$ を用いてユニタリー変換前のエラーパターン $\mathbf{i}$ を推定し，これとユニタリー演算子 $\hat{U}_z$ から変換後のエラーパターンを得る．こうして得られた変換後のエラーパターンを基に，状態 $|0\rangle, |1\rangle$ を反転する操作を施すことにより，ビットエラーが訂正された量子もつれ状態 $\left|\Psi_{N'}^{\mathbf{0},\mathbf{j}'}\right\rangle$ が得られる．ただし，シンドローム作成に用いた光子対は測定によって失われるため，量子もつれ光子対の数は $N' \approx N\left(1 - \mathrm{H}(e_z)\right)$ に減少している．また，位相エラーパターンも $\hat{U}_z$ および光子対数減少の影響で $\mathbf{j} \to \mathbf{j}'$ と変化している．

次に，上記により得られた時間位置誤りが訂正された状態に対して，上記と同様の操作を位相基底についても施す．これにより，$\left|\Psi_{N'}^{\mathbf{0},\mathbf{j}'}\right\rangle \to \left|\Psi_{N''}^{\mathbf{0},\mathbf{0}}\right\rangle$ と誤り訂正された状態を得る．ただし，得られた光子対の数は位相誤り訂正のシンドローム作成のための測定数だ

け減少しており，位相基底測定の誤り率を $e_x = N_x/N$ とすると，残った光子対の数は $N'' \approx N\,(1 - \mathrm{H}(e_z) - \mathrm{H}(e_x))$ 個となっている．なお，時間位置誤りの訂正時に，$\mathbf{j} \to \mathbf{j}'$ と位相エラーパターンが変化しているために，ベクトル $\mathbf{j}'$ の値が 1 となる要素数は N_x 個が上限とはならない．ただし，$\mathbf{j}'$ のパターン数は，元のベクトル $\mathbf{j}$ の値が 1 となる要素数が N_z 個以下であるパターン数を超えないため，$\mathbf{j}'$ を訂正可能な符号を見つけることは可能である．誤り訂正後の量子もつれ状態は十分 1 に近い確率で純粋な量子もつれ状態であることから，手順 6 において，すべての光子対について時間位置基底で測定を行うと，Alice と Bob は，同一かつ外部に漏洩していない秘密鍵を得ることができる．すなわち，プロトコル 2 で共有された鍵は，非常に小さな確率で誤り訂正が失敗することはあるものの，十分に安全であると言える．

上記プロトコル 2 についての安全性の議論は，プロトコル 1 にも適用することができる．上記誤り訂正過程では N 光子全体に対するユニタリー変換 $\hat{U}_z$ を用いている．この実装には量子コンピュータが必要であり，一見プロトコル 1 とは別物に思えるが，プロトコル 2 における時間位置エラー訂正/位相エラー訂正過程は，プロトコル 1 におけるシフト鍵に対する誤り訂正/ 訂正済み鍵に対する秘匿性増強とそれぞれ等価であることが知られている [13, 14]．そのため，そのままプロトコル 1 に対応付けることができる．

上記プロトコルで共有される，1 光子対当たりの秘密鍵生成率は，光子対の数 N が無限大の極限では，次式で与えられる．

$$r_\infty = 1 - \mathrm{H}(e_z) - \mathrm{H}(e_x) \tag{2.66}$$

ただし，$\mathrm{H}(e) = -e\log_2 e - (1-e)\log_2(1-e)$ は Shannon エントロピーであり，e_z, e_x はそれぞれ伝送路の時間位置エラーレートおよび位相エラーレートである．式 (2.66) は，時間位置エラー訂正と位相エラー訂正をそれぞれ独立に施した場合の表式となっている．これは，時間位置基底 $\{|0\rangle, |1\rangle\}$，位相基底 $\{|+\rangle, |-\rangle\}$ のみを用いた測定では，手順 2, 3 においてそれぞれのエラーの独立な確率分布しか推定できないことによる．一方，式 (2.8) (2.9) で表される別の位相基底 $\{|L\rangle, |R\rangle\}$ への射影測定を用いると，時間位置エラーと位相エラーの結合確率分布を得ることができる．これを利用すると，位相エラー訂正において，時間位置エラーが生じた光子対と，生じなかった光子対とに分けて位相エラー訂正を行うことにより，より高い秘密鍵生成率が得られることが知られている [86]．このようなプロトコルは，6 つの量子状態への射影測定を用いるため，Six-state プロトコルと呼ばれる [16].

第 5 章では，d 次元量子状態の場合の Six-state プロトコルに対応する，$(d+1)$ 測定基底 QKD プロトコルの安全性証明を提示し，さらにプロトコルに必要な測定の効率的な実装方法を提案/実証している．

2.5　結言

本章では，本論文の基盤として，1 光子および 2 光子のタイムビン量子状態とその測定の基礎について述べた．2 光子状態の特殊な形態である量子もつれ状態に備わっている相関特性について，古典的な相関との違いおよび秘匿性に言及しながら述べ，純粋量子もつれ状態を用いることで秘密鍵が共有可能であることを示した．さらに，BBM92 およびそれと等価な量子もつれ蒸留を用いた QKD プロトコルを紹介し，後者に基づいた QKD の安全性証明の概略について述べた．

第 3 章

高次元タイムビン量子もつれ状態生成制御と CGLMP 不等式による検証

3.1　緒言

本章では，高次元タイムビン量子もつれ状態の生成および検証について述べる．量子もつれ状態の検証には，2 光子間の相関特性が隠れた変数により記述可能か否かを検証するベル不等式の，高次元量子状態への拡張である CGLMP 不等式を用いている．そこで，まず 3.2 節で隠れた変数理論およびその検証に用いる不等式を紹介する．その後，CGLMP 不等式の破れを最大化する最適量子もつれ状態について述べ，3.3 節でタイムビン量子もつれ状態について最適量子もつれ状態の効率的な生成方法について述べる．続いて 3.4 節で，CGLMP 不等式の検証に必要なフーリエ変換基底状態への射影測定の実装方法として，マッハツェンダー干渉計 (MZI) を 2 段カスケード接続する構成による測定について述べたのち，3.5 節および 3.6 節で，これらの手法の実効性を実験により検証する．

3.2　局所的な隠れた変数理論

3.2.1　CHSH 不等式

第 2 章で，量子もつれ状態 [式 (2.45), (2.47)–(2.49)] のもつ相関特性と，乱数に基づいて状態 $|00\rangle, |11\rangle$ を生成して得られた状態 [式 (2.62)] の持つ相関特性の違いについて述べた．どちらの場合でも，各光子の測定結果はランダムとなるが，後者の場合にランダムとなるのは，元となる乱数を知らないためであり，測定結果自体は測定前に既に決まっている．一方，量子もつれ状態の場合にランダムな結果が得られるのは，本質的に確率的な重ね合わせに由来しており，測定前には測定値は原理的に確定していない．

また，純粋量子もつれ状態は，片方の光子について測定を行うと，他方の光子の量子状態が瞬時に混合量子状態から純粋量子状態に変化する．今，光子 A, B の観測者をそれぞれ Alice, Bob とする．例えば，図 2.9 のように光子 A を時間位置基底 (または位相基底) で測定すると，光子 B も時間位置基底状態 (位相基底状態) に射影される．このような量子状態の変化は，二つの光子がどれほど離れていても瞬時に起こるため，一見すると，光子 A の測定結果が，光速を超えた速度で光子 B に伝わったかのように見える．しかしながら，この状態の変化は光子 A の測定結果を実際に知るまで分からない．そのため，光子 A を測定した Alice から見たときには光子 B の状態が変化するが，Bob から見た光子 B の状態は，別途 Alice から測定結果を知らされるまで完全混合状態のままである．したがって，状態の変化を情報伝達に利用するには追加の通信が必要であり，光速を超えるといった相対性理論に反した情報伝達を可能にする現象ではない．

上記の現象は，一つの波動関数が物理的に離れた 2 地点にわたって存在することに起因する．これを波動関数の非局在性という．Einstein, Podolsky, Rosen は上記の測定結果の非実在性，また波動関数の非局在性に疑問を呈し [7]，その反証として隠れた変数理論が提示された．これは，観測不可能な何らかの物理量 (隠れた変数) が存在し，これを介在して二光子がつながっており，これを知らないために観測結果はランダムに見える (古典相関状態において乱数を知らないことに類似)，とする考え方である．この理論によれば，隠れた変数を含めれば，物理現象は決定論的に記述されることになる．いわば，量子力学が与える予測結果と同じものを，古典的に説明可能な論理構成により与える理論と言える．このように，光速を超えた情報伝達が起こらないような隠れた変数によって，測定結果の相関を説明する理論を，局所的な隠れた変数理論という．量子力学によらずにそのような古典的理論でも，もつれ現象が説明可能であるならば，隠れた変数を知ることで測定結果を確定的に予測できることになり，前章で述べた QKD の安全性証明が成り立たなくなる．Einstein らの問題提起に答えるべく，局所的な隠れた変数理論が正しいとすれば，測定結果において成り立つべき不等式としてベル不等式が提案された [65]．この不等式が成り立たなければ (これをベル不等式の破れという)，隠れた変数というものでは相関性が説明できず，量子力学が正しいということになる．そのため，ベル不等式は量子もつれ状態を実験的に検証する手法として広く用いられている．なお，量子もつれ対のことを上記問題提唱者の名前をとって，EPR ペアと呼ぶことがある．

ベル不等式にはいくつかのバリエーションがあり，ここでは，その一つである CHSH 不等式 [87] を紹介する．CHSH 不等式とは，次頁のプロトコル 3 で得られた測定値 (図 3.1) が満たすべき不等式である．これが破られるか否かで，隠れた変数理論が検証される．

なおプロトコル 3 では，実験と対応付けしやすいよう，Charlie は光子 A, B を送るとしているが，送信するものは，量子力学的な粒子 (量子) に限定されない．相関パラメータ S を得る要件は，Alice と Bob それぞれの測定系の選択肢が二つであること，および測定

プロトコル **3** CHSH 不等式

1: Charlie は，十分離れた地点にいる Alice と Bob に，二つの光子 A, B をそれぞれ送信する (図 3.1).

2: Alice と Bob はそれぞれ，2 種類の測定系をランダムに選んで，光子 A, B を測定する．ここで，選択する測定系を $a, b \in \{0, 1\}$ で表し，Alice と Bob の測定結果をそれぞれ $A_a, B_b = \pm 1$ と表すこととする．

3: Alice と Bob は選択した測定系，および測定結果を通知しあい，その積 $A_a B_b$ を計算する．

4: 上記の手順 1〜3 を繰り返し，相関の強さを表す相関パラメータ

$$S = A_0 B_0 + A_0 B_1 - A_1 B_0 + A_1 B_1 \tag{3.1}$$

の平均値 $\langle S \rangle$ を計算する．この $\langle S \rangle$ が満たす不等式，$-2 \leq \langle S \rangle \leq 2$ を CHSH 不等式という．

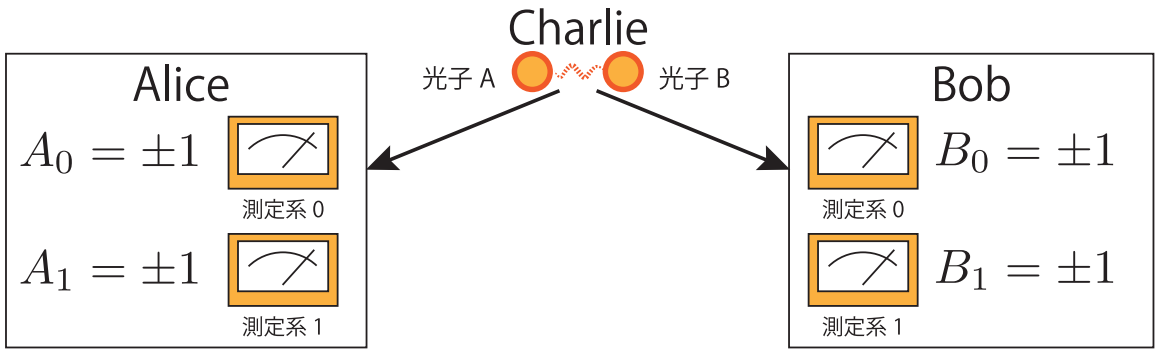

図 3.1　プロトコル 3 の模式図

により得られる結果は二値であることである．例えば，カードの表裏それぞれに ± 1 のどちらかを記入し，シールで見えないようにしたものを Alice と Bob に配布した後，Alice と Bob が表裏の一方だけシールをめくって ± 1 を観測することを考えると，表裏の選択は測定系の選択，シールをめくって観測した値は観測結果，とみなすことができ，この系は CHSH 不等式の検証に用いることができる．以下，隠れた変数のモデルとして，このカードの例を引用しながら，隠れた変数があるとすれば上記 CHSH 不等式が満たされることを説明する．

まず，局所実在性という概念を導入する．実在性とは，測定を行う前に測定結果そのものはすでに定まっている，という性質のことを指す．上記のカードの例で言えば，Alice/Bob がシールをめくって ± 1 を観測する前に，Charlie がカードを配布した時点で

観測結果は定まっている，つまり実在している．一方，局所性は，片方の測定は，他方の測定に影響を与えないという性質である．例えば，Alice がカードの表のシールをめくって $+1$ を得る場合，Bob の測定をいかに工夫しても Alice の観測結果は変わらない．すなわち，$A_0 = +1$ という値が実在する時，Bob の測定の選択がどうであろうと $A_0 = +1$ である．言い換えると，配られたカードに対して A_0B_0 を測定する場合と，A_0B_1 を測定する場合とで，A_0 の値が変わることはない．ただし，Charlie が Alice/Bob が選択する測定系を事前に知っている場合，Charlie は測定系に応じたカードを配ることで，両者の測定結果に局所性が成り立たないような相関を持たせることができる．そのため，隠れた変数に対して局所性が成り立つためには，Alice/Bob が Charlie に分からないように測定系を選択することが前提条件となる．なお，局所性の検証を厳密に行うには，一方の測定情報が他方の測定時点で伝達不可能なように十分離れた Alice と Bob がほぼ同時に測定をする必要がある．このような厳密な実験は極めて大がかりとなるため，通常はそのような大規模な実験は行わず，Alice と Bob の装置を独立に用意することで，局所性を検証する．

ここで，Alice と Bob は片方の測定系の測定結果だけではなく，二つの測定系の測定結果双方を得ることができたとする．この時，局所実在性のため，一回の試行の測定結果 A_a, B_b は ± 1 のいずれかに確定している．ここで，Alice と Bob の測定結果の相関度を表すパラメータとして，

$$S \coloneqq A_0B_0 + A_0B_1 - A_1B_0 + A_1B_1 \tag{3.2}$$

を導入する．$A_{0/1}, B_{0/1}$ の値は ± 1 であるので，S の絶対値は，次式となる．

$$\begin{aligned} |S| &= |A_0B_0 + A_0B_1 - A_1B_0 + A_1B_1| \\ &= |A_0(B_0 + B_1) - A_1(B_0 - B_1)| \\ &= 2 \end{aligned} \tag{3.3}$$

ただし，$(B_0 + B_1), (B_0 - B_1)$ の二つの値は，必ず 0 と 2 の組となることを用いた．上式は S が ± 2 のどちらかの値しか取りえないことを示している．

次に，上記測定を多数回行うことを考える．その際，Alice と Bob の測定結果には，何らかの変数 (隠れた変数)λ を仲立ちとした相関があるとする．すなわち，測定結果 A_a, B_b は λ の関数 $A_a(\lambda), B_b(\lambda)$ とする．さらに，この λ はカード配布が各回ごとに独立に行われることから，各回ごとに異なる値をとるものとし，その確率密度分布を $p(\lambda)$ とする．

すると，S の平均値 $\langle S\rangle$ は次式のように表される．

$$\begin{aligned}|\langle S\rangle| &= |\langle A_0B_0\rangle + \langle A_0B_1\rangle - \langle A_1B_0\rangle + \langle A_1B_1\rangle| \\ &= \left|\int_{-\infty}^{\infty} \mathrm{d}\lambda\, p(\lambda)\left\{A_0(\lambda)B_0(\lambda) + A_0(\lambda)B_1(\lambda) - A_1(\lambda)B_0(\lambda) + A_1(\lambda)B_1(\lambda)\right\}\right| \\ &\leq \int_{-\infty}^{\infty} \mathrm{d}\lambda\, p(\lambda)\left|A_0(\lambda)B_0(\lambda) + A_0(\lambda)B_1(\lambda) - A_1(\lambda)B_0(\lambda) + A_1(\lambda)B_1(\lambda)\right| \\ &= 2 \end{aligned} \tag{3.4}$$

したがって，次式が成り立つ．

$$-2 \leq \langle S\rangle \leq 2 \tag{3.5}$$

上式は，隠れた変数 λ を仮定したときに満たされるべき不等式であり，提案者である Clauser, Horn, Shimony, Holt の頭文字からCHSH 不等式と呼ばれる [87].

次に，上記測定において，Charlie がカードではなくベル基底状態 $\left|\Psi^{00}\right\rangle$ を配るものとする．そして，測定として次の量子状態

$$|+1;\theta\rangle = \frac{|0\rangle + e^{i\theta}\,|1\rangle}{\sqrt{2}} \tag{3.6}$$

$$|-1;\theta\rangle = \frac{|0\rangle - e^{i\theta}\,|1\rangle}{\sqrt{2}} \tag{3.7}$$

への射影測定を想定し，状態 $|+1;\theta\rangle$ が観測された時の測定結果を $+1$，状態 $|-1;\theta\rangle$ が観測された時の測定結果を -1 とする．この場合，測定系の選択 (カードの例では表をめくるか裏をめくるか) は，θ の設定で行われる．すなわち，Alice については $\theta = 0$ とすれば測定系 $0(a=0)$，$\theta = \pi/2$ とすれば測定系 $1(a=1)$，Bob については $\theta = \pi/4$ とすれば測定系 $0(b=0)$，$\theta = -\pi/4$ とすれば測定系 $1(b=1)$，がそれぞれ選択される．このように測定系を定義すると，測定を多数回行った時の Alice と Bob の測定結果 A_a と B_b の積の平均値が，次式で与えられる．

$$\begin{aligned}\langle A_aB_b\rangle &= \sum_{A_a,B_b\in\{\pm1\}} A_aB_b\left|\langle A_a;\theta_a|\left\langle B_b;\theta_b\middle|\Psi^{00}\right\rangle_{AB}\right|^2 \\ &= \sum_{A_a,B_b\in\{\pm1\}} A_aB_b\left|\frac{1}{2\sqrt{2}}\left(1 + A_aB_be^{-i(\theta_a+\theta_b)}\right)\right|^2 \\ &= \cos\left(\theta_a+\theta_b\right) \end{aligned} \tag{3.8}$$

これを $\langle S\rangle = \langle A_0B_0\rangle + \langle A_0B_1\rangle - \langle A_1B_0\rangle + \langle A_1B_1\rangle$ に代入し，さらに $\theta_a \in \{0, \pi/2\}, \theta_b \in \{\pi/4, -\pi/4\}$ を用いると，次式が得られる．

$$\langle S\rangle = 2\sqrt{2} \tag{3.9}$$

上式は，量子もつれ状態を配布/測定すると，$\langle S\rangle$ は CHSH 不等式の上限値の $\sqrt{2}$ 倍となることを示している．すなわち，CHSH 不等式が破られる．なお，この $\sqrt{2}$ 倍というのは量子力学が与える最大値であり，Tsirelson 限界として知られている [88]．以上述べたように，量子もつれ状態を測定すると，隠れた変数理論では説明できない結果が得られる．なお，量子状態であっても，セパラブル状態 (非量子もつれ状態) の場合には，測定結果の相関を説明可能な隠れた変数によるモデルを作ることができるため，CHSH 不等式が満たされる．言い方を変えると，CHSH 不等式の破れは量子もつれ状態特有の現象と言える．そのため，量子もつれ状態の実験的検証手段として広く用いられている．

3.2.2　CGLMP 不等式と最適量子もつれ状態

前節では，測定値が ±1 の 2 値である測定系についてのベル不等式である，CHSH 不等式を紹介した．一方，d 次元量子状態の場合には，d 個の測定値が得られる．このような多値の測定系についてのベル不等式として，Collins, Gisin, Linden, Massar, Popescu 提案によるCGLMP 不等式が知られている [66]．CGLMP 不等式においても，Alice と Bob はそれぞれ 2 種類の測定系 $a, b \in \{0, 1\}$ を用いて測定する．ただし，得られる測定値は $A_a, B_b \in \{0, \cdots, d-1\}$ の d 値となる．この場合の相関パラメータ S_d は，次式で定義される．

$$\begin{aligned} S_d = \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) \{ &+ [\Pr(A_0 = B_0 + k) + \Pr(B_0 = A_1 + k + 1) \\ &\quad + \Pr(A_1 = B_1 + k) + \Pr(B_1 = A_0 + k)] \\ &- [\Pr(A_0 = B_0 - k - 1) + \Pr(B_0 = A_1 - k) \\ &\quad + \Pr(A_1 = B_1 - k - 1) + \Pr(B_1 = A_0 - k - 1)]\} \end{aligned} \tag{3.10}$$

ただし，$\Pr(*)$ は括弧内の引数を $\bmod d$ で評価した時の確率である．なお，CHSH 不等式の場合とは異なり，相関パラメータを確率を用いた期待値として定義している．この相関パラメータ S_d は，$d = 2$ とすると，CHSH 不等式の相関パラメータの期待値 $\langle S\rangle$ に一致する．式 (3.10) で与えられる S_d に対して，前節と同様にして局所的な隠れた変数理論を適用すると，$S_d \leq 2$ であることが導かれる．これが CGLMP 不等式である．

ここで，式 (2.52) で表される d 次元最大量子もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$ を測定対象とした場合の S_d について考える．まず，量子もつれ状態への射影測定として，次式で与えられるフーリエ基底状態への測定を考える．

$$|\theta_l\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp(i\theta_l k)\, |k\rangle \tag{3.11}$$

ただし，$l \in \{0, \cdots, d-1\}$ は測定値 A_a, B_b を示すインデックスであり，θ_l は Alice と Bob の測定系 a, b によって定まるパラメータである．具体的には，測定系 $a, b \in \{0, 1\}$ について θ_l は次式のように設定される．

$$\theta_l = \frac{2\pi}{d} \times \begin{cases} (l + \alpha_a) & \text{for Alice} \\ (-l + \beta_b) & \text{for Bob} \end{cases} \tag{3.12}$$

$$\alpha_a = \begin{cases} 0 & \text{for} \quad a = 0 \\ 1/2 & \text{for} \quad a = 1 \end{cases} \tag{3.13}$$

$$\beta_b = \begin{cases} 1/4 & \text{for} \quad b = 0 \\ -1/4 & \text{for} \quad b = 1 \end{cases} \tag{3.14}$$

上記のように表した射影測定系および d 次元最大量子もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$ を用いて式 (3.10) を計算すると，相関パラメータ S_d が次式のように表される．

$$S_d = \frac{2}{d^2} \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) \left(\frac{1}{\sin^2[\pi(k+1/4)/d]} - \frac{1}{\sin^2[\pi(k+3/4)/d]}\right) \tag{3.15}$$

上式は，$d = 2$ では CHSH 不等式と同じく $S_2 = 2\sqrt{2} \approx 2.8284$，$d = 4$ では $S_4 \approx 2.8962$ となる．これらの値は，CGLMP 不等式 $S_d \leq 2$ を満たしていない．したがって，d 次元最大量子もつれ状態を測定すると，CGLMP 不等式の破れが観測されることになる．

2 次元系，すなわち $d = 2$ の場合，最大量子もつれ状態の測定によって得られる S_2 値は $S_2 = 2\sqrt{2}$ であり，これが量子力学が与える最大値となっている．したがって，原理的にこれより大きな不等式の破れを観測することはできない．一方，$d \geq 3$ の場合，上記の量子もつれ状態測定で得られる S_d 値が量子理論限界とは限らない．CGLMP 不等式の提案においては，数値計算による測定の最適化により，上記のフーリエ基底を用いた測定が不等式の破れを最大化することが示唆されており [66]，さらに，フーリエ基底に測定を固定して状態を最適化した場合に，最大量子もつれ状態よりも大きな破れを示す，最適化された量子もつれ状態が存在することが指摘されている [50, 57].

CGLMP 不等式の破れを最大化する量子もつれ状態 (以後，最適量子もつれ状態と呼ぶ) は，相関パラメータ S_d を演算子化することによって導くことができる．式 (3.10) の定義式が示すように，S_d は，Alice と Bob の測定結果が一定の条件を満たす確率の線形結合となっている．一方，Alice/Bob の測定系は，式 (3.11) で表されるフーリエ基底状態への射影測定となっている．したがって，任意の二光子状態 $\hat{\rho}_{AB}$ に対して，Alice が測定結果 $A_a = l_a$，Bob が測定結果 $B_b = l_b$ を得る確率は，次式で定義される射影測定演算子 $\hat{P}_{QM}(A_a = l_a, B_b = l_b)$ を用いて，$\mathrm{Tr}\{\hat{P}_{QM}(A_a = l_a, B_b = l_b)\hat{\rho}_{AB}\}$ と表すことができる．

$$\hat{P}_{QM}(A_a = l_a, B_b = l_b) = |\theta_{l_a}\rangle_A |\theta_{l_b}\rangle_B \langle\theta_{l_a}|_A \langle\theta_{l_b}|_B \tag{3.16}$$

式 (3.10) 中の確率 $\Pr(*)$ は上記射影測定結果に関する確率の線形和で表される．よっ

て，各 $\Pr(*)$ に対応した測定演算子を，上記のランク 1 の射影測定演算子の線形和として表すことができる．例えば，$\Pr(A_0 = B_0 + k)$ に対応する，ランク d の射影測定演算子 $\hat{P}(A_0 = B_0 + k)$ は次式のように表される．

$$\hat{P}(A_0 = B_0 + k) = \sum_{c=0}^{d-1} \hat{P}_{QM}(A_a = c + k, B_b = c) \tag{3.17}$$

その他の確率についても同様である．式 (3.10) 中の確率 $\Pr(*)$ をこれらの射影測定演算子で置き換えると，演算子化した相関パラメータ $\hat{S}_d$ を得ることができる．この $\hat{S}_d$ を用いれば，任意の量子状態 $\hat{\rho}_{AB}$ に対する相関パラメータの値が，$S_d = \mathrm{Tr}\left(\hat{S}_d \hat{\rho}_{AB}\right)$ として求まる．これは，射影測定演算子 $\hat{P}$ や POVM 要素 $\hat{E}$ について，対応する測定確率が $\mathrm{Tr}\left(\hat{P}\hat{\rho}_{AB}\right), \mathrm{Tr}\left(\hat{E}\hat{\rho}_{AB}\right)$ で求まるように導出したのと同様に，相関パラメータを演算子化したものである．

ここで，二光子の状態密度演算子を $\hat{\rho}_{AB} = \sum_i \lambda_i \left|\psi^i\right\rangle\!\left\langle\psi^i\right|_{AB}$ と対角化すれば，次式が成り立つ．

$$\begin{aligned} S_d &= \mathrm{Tr}\left(\hat{S}_d \hat{\rho}_{AB}\right) \\ &= \sum_i \lambda_i \,\mathrm{Tr}\left(\hat{S}_d \left|\psi^i\right\rangle\!\left\langle\psi^i\right|_{AB}\right) \\ &= \sum_i \lambda_i \left\langle\psi^i\right|_{AB} \hat{S}_d \left|\psi^i\right\rangle_{AB} \\ &\leq \left\langle\psi^{\max}\right|_{AB} \hat{S}_d \left|\psi^{\max}\right\rangle_{AB} \end{aligned} \tag{3.18}$$

ただし，状態 $\left|\psi^i\right\rangle_{AB}$ の中で $\left\langle\psi^i\right|_{AB} \hat{S}_d \left|\psi^i\right\rangle_{AB}$ が最大となる状態を $\left|\psi^{\max}\right\rangle_{AB}$ とした．よって，S_d を最大化する量子状態としては，混合量子状態ではなく純粋量子状態のみを考えればよい．そこで，$\left\langle\psi\right|_{AB} \hat{S}_d \left|\psi\right\rangle_{AB}$ を最大化する純粋量子状態 $\left|\psi\right\rangle_{AB}$ を考える．これは，相関パラメータ演算子 $\hat{S}_d$ の固有状態のうち，固有値が最大の量子状態である．そこで，相関パラメータ演算子 $\hat{S}_d$ を対角化することにより，最適量子もつれ状態を得ることができる．この手順を $d = 4$ のシステムについて行うと，次式で表される最適量子もつれ状態 $|\Psi_{\mathrm{OES}}\rangle$ が得られる．

$$|\Psi_{\mathrm{OES}}\rangle = \frac{1}{\sqrt{2(1+\gamma^2)}} \left(|00\rangle + \gamma\,|11\rangle + \gamma\,|22\rangle + |33\rangle\right) \tag{3.19}$$

ただし，$\gamma \approx 0.739$ である．この最適量子もつれ状態を測定すると $S_4 \approx 2.9727$ となり，最大量子もつれ状態を測定した場合の $S_4 \approx 2.8962$ よりも不等式の破れが大きくなる．その他の次元についても，表 3.1 に示すように，状態の最適化によって CGLMP 不等式の破れを増加させることができる [57, 66].

表 3.1 最大量子もつれ状態および最適量子もつれ状態に対する相関パラメータ S_d

d	$\|\Psi_{\mathrm{MES}}\rangle$ の場合	$\|\Psi_{\mathrm{OES}}\rangle$ の場合
2	2.8284	2.8284
3	2.8729	2.9149
4	2.8962	2.9727
5	2.9105	3.0157
⋮	⋮	⋮

第 1 章でも述べた通り，これまで CGLMP 不等式の破れは，周波数の位置や光軌道角運動量 (OAM)，時間エネルギー不確定性を利用した高次元量子状態を用いて観測されているが [47, 48, 50, 51, 55, 57]，高次元タイムビン量子状態については未報告であった．あるいは異なる角周波数光を基底状態とする，周波数ビン量子もつれ状態を利用した $|\Psi_{\mathrm{OES}}\rangle$ の生成実験が報告されているが [50]，最大量子もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$ と最適量子もつれ状態 $|\Psi_{\mathrm{OES}}\rangle$ との明確な差は観測されていない．そこで本研究では，自発的パラメトリック下方変換による制御性の高い高次元タイムビン量子もつれ状態生成法，およびカスケード接続した MZI による安定な測定法を実装し，高次元タイムビン量子状態に対する上記の CGLMP 不等式の破れの増加特性を実証することで，これらの状態生成法/測定法の有用性を示す．

3.3 自発的パラメトリック下方変換による高次元タイムビン量子もつれ状態生成

実験的にタイムビン量子もつれ状態を生成するには，光非線形現象のひとつである，自発的パラメトリック下方変換 (SPDC：Spontaneous Parametric Down Conversion) が主に用いられる．本節ではこれについて述べる．なお，SPDC としては，2 次の非線形光学効果を用いるタイプと，3 次の非線形光学効果を用いるタイプがある．ここでは前者について述べるが，量子もつれ状態生成という観点からは両者は本質的に同じである．

2 次非線形光学効果による SPDC は，角周波数 ω_3 の光から，$\omega_3 = \omega_1 + \omega_2$ を満たす 2 つの角周波数の光が発生する過程である．ここで，角周波数 ω_3 の光をポンプ光，角周波数 ω_1, ω_2 の光をそれぞれシグナル光，アイドラー光と呼ぶ．角周波数 ω の単一光子のエネルギーは，プランク定数 h を 2π で割った値である，換算プランク定数 $\hbar = h/2\pi$ を用いて $\hbar\omega$ で与えられる．したがって，光子描像では，SPDC は高いエネルギー $\hbar\omega_3$ の光子一つが，エネルギー保存則を満たすように，$\hbar\omega_1, \hbar\omega_2$ のエネルギーをもつ二つの光子に変換される過程とみなすことができる (図 3.2)．なお，この周波数関係から必ず

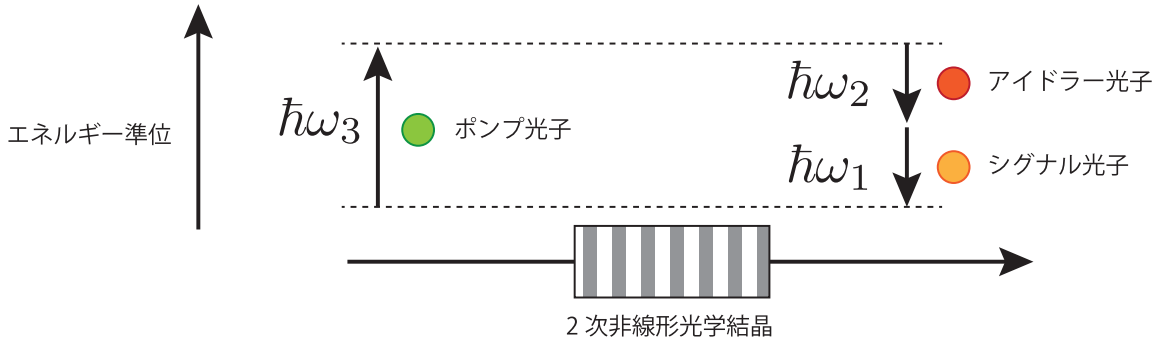

図 3.2　2 次非線形光学結晶を用いた SPDC 過程の模式図

$\omega_3 > \omega_1, \omega_2$ であり，高い周波数の光から低い周波数の光が発生することから，下方変換と呼ばれている．

SPDC は，非線形光学結晶に対して高強度のポンプ光を入射することで発生する．ここで，ポンプ光は十分高強度であるため古典力学的な電磁場として取り扱い，シグナル光とアイドラー光は，光子数 0 の真空場から数光子程度の状態であるため，量子力学的な電磁場として扱う．量子力学では，電磁場は生成消滅演算子によって記述される．角周波数 ω_l の光子の電界振幅に対応する演算子 (消滅演算子) を $\hat{a}_l$，そのエルミート共役 (生成演算子，電界振幅の複素共役に相当) を $\hat{a}_l^\dagger$ とする．$\hat{a}_l, \hat{a}_l^\dagger$ は光子数確定状態に対して作用させることで，それぞれ角周波数 ω_l の光子ひとつを減らす/増やす性質がある．非線形光学現象の効率を決める位相整合条件が満たされている状況下で，非線形光学結晶中にポンプ光を入射すると，結晶内の伝搬に伴ってこれらの演算子は次の微分方程式に従って時間発展する [89].

$$\frac{d\hat{a}_1^\dagger}{dt} = i\omega_1 \hat{a}_1^\dagger + is\hat{a}_2 e^{i\omega_3 t} \tag{3.20}$$

$$\frac{d\hat{a}_2}{dt} = -i\omega_2 \hat{a}_2 - is\hat{a}_1^\dagger e^{-i\omega_3 t} \tag{3.21}$$

ただし，s は非線形相互作用の強さを表すパラメータであり，ポンプ光の電場の大きさに比例する．厳密には，ポンプ光は結晶内を伝搬するにつれて，シグナル/アイドラー光子生成のため減少するので (ポンプデプレッション)，s は時間の関数である．ただし，ここではポンプ光は十分強く，また発生するシグナル/アイドラー光子は少数であるため，s は定数とみなしてよい．この場合，式 (3.20), (3.21) は解析的に解くことができ，その解は

次のように表される．

$$\hat{a}_1^\dagger(t) = [\hat{a}_1^\dagger(0)\cosh(st) + i\hat{a}_2(0)\sinh(st)]e^{i\omega_1 t} \tag{3.22}$$

$$\hat{a}_2(t) = [\hat{a}_2(0)\cosh(st) - i\hat{a}_1^\dagger(0)\sinh(st)]e^{i\omega_2 t} \tag{3.23}$$

ただし，$\hat{a}_1^\dagger(0), \hat{a}_2(0)$ は結晶入射時の生成消滅演算子である．先に述べたように，SPDC はエネルギー保存則 $\hbar\omega_3 = \hbar\omega_1 + \hbar\omega_2$ を満たすように，ポンプ光子からシグナル/アイドラー光子が生成される過程であるので，2 つの光子は必ずペアで発生する．ここで，t を光パルスが結晶を通過する時間とすると，結晶出力時のシグナル光の光子数演算子 $\hat{n}_1^{\mathrm{out}}$ は，次式で表される．

$$\begin{aligned}
\hat{n}_1^{\mathrm{out}} =& \hat{a}_1^\dagger(t)\hat{a}_1(t) \\
=& [\hat{a}_1^\dagger(0)\cosh(st) + i\hat{a}_2(0)\sinh(st)][\hat{a}_1(0)\cosh(st) - i\hat{a}_2^\dagger(0)\sinh(st)] \\
=& \hat{a}_1^\dagger(0)\hat{a}_1(0)\cosh^2(st) + \left[\hat{a}_2^\dagger(0)\hat{a}_2(0) + 1\right]\sinh^2(st) \\
&+ i\sinh(st)\cosh(st)\left(\hat{a}_1(0)\hat{a}_2(0) - \hat{a}_1^\dagger(0)\hat{a}_2^\dagger(0)\right)
\end{aligned} \tag{3.24}$$

上式を導くにあたり，生成消滅演算子の交換関係 $[\hat{a}_i, \hat{a}_j^\dagger] = \hat{a}_i\hat{a}_j^\dagger - \hat{a}_j^\dagger\hat{a}_i = \delta_{ij}$ を用いた．

量子力学では，観測物理量の平均値は，時間発展した物理量演算子を初期状態のブラとケットではさみ込んだ内積で与えられる (ハイゼンベルグ描像)．そこで，入力状態はシグナル光，アイドラー光がともに真空場 $|vac\rangle$ であるとすると，出力シグナル光の平均光子数 μ_1 が，

$$\mu_1 = \langle vac|\,\hat{n}_1^{\mathrm{out}}\,|vac\rangle \tag{3.25}$$

で与えられる．真空状態から光子数を減らすことはできないため，$\hat{a}_l(0)\,|vac\rangle = 0$ が成り立つ $(l = 1, 2)$．また，この式のエルミート共役から，$\langle vac|\,\hat{a}_l^\dagger(0) = 0$ も成り立つ．これらより，式 (3.24) を式 (3.25) に代入すると，$\mu_1 = \sinh^2(st)$ となる．この表式は，$|st| \ll 1$ であり，生成される光子数が十分少ない場合には，$\mu_1 \approx s^2t^2$ と近似される．ここで，媒質伝搬時間 t は定数であり，s はポンプ光の振幅に比例しているので，出力平均光子数は s^2 に比例，すなわちポンプ光強度に比例する．そこで，ポンプ光強度を適切に設定して $s^2t^2 \ll 1$ とすると，発生する光子対は概ね 1 ペアのみとなる．この時，平均光子数と 1 光子対の生成確率は近似的に比例関係にあるため，1 光子対の確率振幅の大きさ (すなわち，生成確率の平方根) は，ポンプ光強度の平方根に比例する．

ここまで，ひとつのパルス内での SPDC について述べた．すなわち，このパルスの時間位置を t_0 とすると，同じ時間位置 t_0 にシグナル光子，アイドラー光子が存在する状態 $|00\rangle$ が生成される．ここで，図 3.3 のように時間位置 t_1 のパルスを追加して 2 連ポンプパルスとし，二つの時間位置をあわせて光子対が 1 ペアだけ生成されるようにポンプ光強度を設定する．すると，光子対が発生した場合，それがどちらの時間位置にあるかは観測

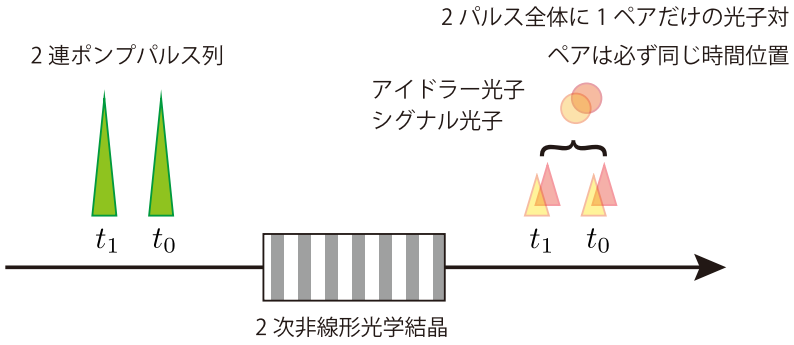

図 3.3　SPDC による 2 次元タイムビン量子もつれ状態生成

しないとわからない．これはすなわち，時間位置 t_0, t_1 それぞれに 1 光子対が存在する状態 $|00\rangle, |11\rangle$ の重ね合わせ状態である [90]．この状態 $|\psi\rangle$ は次式のように表される．

$$|\psi\rangle \propto s_0 |00\rangle + s_1 e^{i\phi} |11\rangle \tag{3.26}$$

ただし，s_0, s_1 は，それぞれ時間位置 t_0, t_1 におけるポンプ光強度で決まる定数であり，ϕ は二つのポンプ光パルスの相対位相である．ここで，$s_0 = s_1$, $\phi = 0$ とすれば，発生状態は，光子対が発生したという条件下で，ベル基底状態 $\left|\Psi^{00}\right\rangle$ となる．

同様にして，上記を d 連続ポンプパルス列に拡張すると，次式で表される d 次元のタイムビン量子もつれ状態が得られる [45, 91]．

$$|\psi\rangle \propto \sum_{k=0}^{d-1} s_k e^{i\phi_k} |kk\rangle \tag{3.27}$$

ただし，s_k, ϕ_k は，それぞれパルス時間位置 t_k のポンプ光強度および位相で決まる定数である．ここで，ポンプパルスの強度は同一，かつ同位相とすると，上式は式 (2.52) と等価となり，d 次元最大量子もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$ が得られることになる．また，前節で述べた，CGLMP 不等式の破れを最大化する量子もつれ状態 $|\Psi_{\mathrm{OES}}\rangle$[式 (3.19)] は，$d = 4$ の場合，ポンプパルス光強度の比を $1 : \gamma^2 : \gamma^2 : 1$ とすると生成される (図 3.4)．このように，SPDC においてポンプパルス列を適切に設定することにより，制御された高次元タイムビン量子もつれ状態を生成することができる．

前節で述べた通り，これまでに異なる角周波数光を基底状態とする，周波数ビン量子もつれ状態を利用した $|\Psi_{\mathrm{OES}}\rangle$ の生成実験が報告されているが [50]，ベル不等式の破れに関して，最大量子もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$ と最適量子もつれ状態 $|\Psi_{\mathrm{OES}}\rangle$ との明確な差は確認されていなかった．周波数ビン量子もつれ状態の生成にも，SPDC が用いられるが，非線形光学結晶の分散などのために，非線形デバイス構造の調整により発生光子対の確率振幅を制御することは難しい．そこで報告例 [50] では，SPDC で生成した量子もつれ状態に対し，プログラマブル周波数フィルタを用いた周波数等化による振幅調整を施し，$|\Psi_{\mathrm{MES}}\rangle$

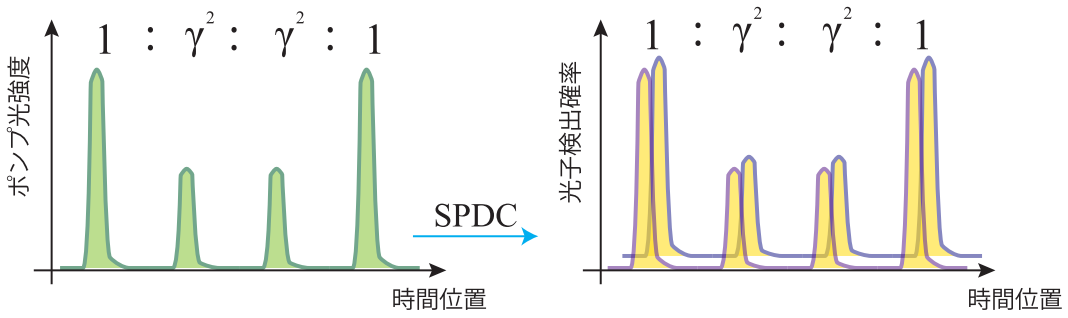

図 3.4　最適もつれ状態 $|\Psi_{\mathrm{OES}}\rangle$ を生成するためのポンプ光の強度変調

あるいは $|\Psi_{\mathrm{OES}}\rangle$ を生成している．この場合，原理的に光子損失があるため，生成効率が低い．これに対し，上記で述べたタイムビン量子もつれ状態生成は，ポンプ光により光子対の確率振幅を制御することができ，このような等化操作が不要である．さらに第二次高調波生成 (SHG：The Second Harmonic Generation) を用いてポンプ光を生成することで，ポンプ光パルスの制御は，光通信で広く使われている光変調器を用いて精度よく実装することができる．そこで本論文では，この量子もつれ状態生成手法を用いて CGLMP 不等式の破れの増加観測実験を行った．

3.4　多段接続 Mach-Zehnder 干渉計によるもつれ状態測定

3.4.1　フーリエ基底状態への射影測定

本節では，CGLMP 不等式の評価に必要なフーリエ基底状態への射影測定を，多段接続した MZI を用いて実装する手法について述べる [31, 32, 92]．前節で述べた通り，フーリエ基底状態は，式 (3.11) で表される時間位置基底状態の重ね合わせ状態である．2.2.3 節にて，2 次元タイムビン量子状態については，遅延 MZI を用いてこのような重ね合わせ状態への射影測定が実装可能であることを述べた．より高次元のタイムビン量子状態の場合は，図 3.5 に示すように，遅延時間の異なる MZI を多段に接続することで，すべての時間位置基底状態の重ね合わせ状態への射影測定が可能となる．

ここで，4 次元タイムビン量子状態に対する，多段接続 MZI の測定演算子について述べる．まず，遅延時間 τ の MZI に 4 次元タイムビン量子状態を入力したときの，一方の出力ポートへの光子の透過を表す測定演算子は，式 (2.36) の総和の範囲を拡張することにより，次式のように与えられる．

$$\hat{M}_{1x} = \frac{1}{2}\sum_{k=0}^{3}\left(|k\rangle + e^{i\theta}\,|k+1\rangle\right)\langle k| \tag{3.28}$$

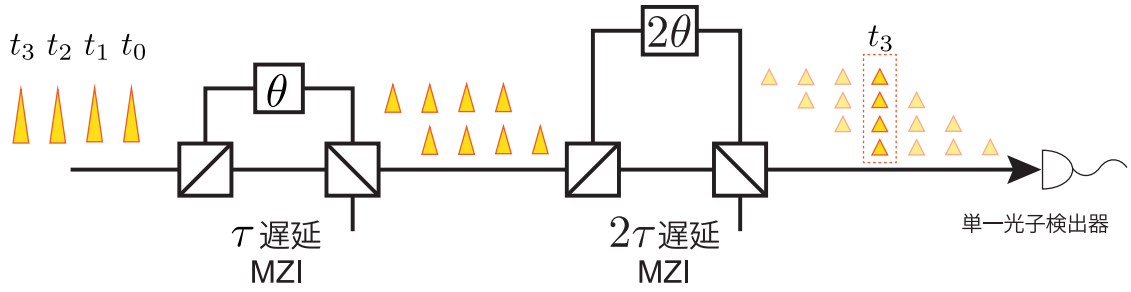

図 3.5　多段接続した MZI によるフーリエ基底測定

ただし，表記の煩雑さを避けるため，出力ポートを示すインデックスは省略した．

遅延時間が τ かつ 2 経路の伝搬遅延位相差が θ の 1 段目 MZI からの出力は，遅延時間が 2τ かつ 2 経路の伝搬遅延位相差が 2θ の 2 段目 MZI に入力される．この 2 段目 MZI への入力状態は，1 段目 MZI の出力なので，5 次元状態となっている (図 3.5)．よって，この入力状態に対する 2 段目 MZI 透過を表す測定演算子は，次式で与えられる．

$$\hat{M}_{2x} = \frac{1}{2}\sum_{k=0}^{4}\left(|k\rangle + e^{i2\theta}\,|k+2\rangle\right)\langle k| \tag{3.29}$$

図 3.5 に示すように，2 段目 MZI の出力端に置かれた光子検出器では，7 つの時間スロットで光子を検出しうる．このうち中央の時間位置 t_3 での光子検出事象は，入力された 4 つの時間位置状態すべての干渉の結果として生じる．この測定系は，1 段目の τ 遅延干渉計透過，2 段目の 2τ 遅延干渉計透過，時間位置 t_3 での光子検出，の多段構成となっているので，測定全体を記述する演算子 $\hat{M}_{\mathrm{total}}$ および対応する POVM 要素 $\hat{E}_{\mathrm{total}}$ は，それぞれ次式のように表される．

$$\begin{aligned}
\hat{M}_{\mathrm{total}} &= |3\rangle\langle 3|\,\hat{M}_{2x}\hat{M}_{1x} \\
&= |3\rangle\langle 3|\left\{\frac{1}{2}\sum_{k=0}^{4}\left(|k\rangle + e^{i2\theta}\,|k+2\rangle\right)\langle k|\right\}\left\{\frac{1}{2}\sum_{k=0}^{3}\left(|k\rangle + e^{i\theta}\,|k+1\rangle\right)\langle k|\right\} \\
&= \frac{e^{i3\theta}}{2}\,|3\rangle\left\{\frac{1}{2}\left(e^{-i3\theta}\,\langle 3| + e^{-i2\theta}\,\langle 2| + e^{-i\theta}\,\langle 1| + \langle 0|\right)\right\} \\
&= \frac{e^{i3\theta}}{2}\,|3\rangle\langle\theta| \qquad (3.30) \\
\hat{E}_{\mathrm{total}} &= \hat{M}_{\mathrm{total}}^{\dagger}\hat{M}_{\mathrm{total}} \\
&= \frac{1}{4}\,|\theta\rangle\langle\theta| \qquad (3.31)
\end{aligned}$$

上式は，多段接続された二つの MZI の伝搬遅延位相を，各 MZI の遅延時間に比例した値に設定すると，フーリエ基底状態 $|\theta\rangle$ への射影測定が実装できることを示している．そこで，θ を式 (3.12)–(3.14) を満たす値とすることで，CGLMP 不等式の評価に必要な測定系が実装できる．

以上では，4 次元量子状態に対する測定系の実装方法について述べた．この手法は，さらに 4τ 遅延 MZI，8τ 遅延 MZI，$\cdots$，$2^{N-1}\tau$ 遅延 MZI と，干渉計を多段に接続することにより，2^N 次元系に拡張できる．また，本論文では単一の検出器を用い，θ を変化させる手法を用いているが，ツリー構造で多段に MZI を接続することで，2^N-1 個の MZI と 2^N 個の検出器を用いた 2^N 個のフーリエ基底状態への射影測定の一括実装が可能であり，近年の 2 測定基底 QKD プロトコルの実装で用いられている [31, 32, 92]．なお，干渉計を用いたフーリエ基底状態への射影測定の実装方法としては，マルチポートビームスプリッタからなる，多腕干渉計を用いる手法も知られている [47]．この測定系は，被測定量子状態の次元数と同じ数の分岐遅延経路で構成されており，測定にあたってはそれらの制御/安定化が必要となる．これに対して，本論文で用いる多段 MZI 系は，d 次元状態に対して $\log_2 d$ 個の伝搬遅延位相のみ制御/安定化が必要であり，実験で制御すべきパラメータ数が少ないという利点を持つ．

3.4.2　対称なノイズモデルと干渉縞の明瞭度

前節で，CGLMP 不等式の評価に必要なフーリエ基底状態への射影測定を，多段接続 MZI により実装する手法について述べた．CGLMP 不等式の破れの検証では，特定の位相の組み合わせにおける光子検出割合を測定する．一方，CGLMP 不等式の簡易な評価法として，上記のフーリエ基底状態の位相 θ を 0 から 2π まで連続的に変えた時の光子検出数に現れる干渉縞の明瞭度を調べる手法がしばしば用いられる．

CGLMP 不等式の S_d と明瞭度を対応させるには，特定のノイズモデルを仮定する必要があり，これには通常，対称なノイズを表す分極解消チャネルが採用される．密度演算子が $\hat{\rho}_{AB}$ で表される d 次元 2 光子量子状態を，分極解消チャネルに入力したときの出力状態を表す状態密度演算子は，次式で与えられる．

$$\hat{\rho}_{\mathrm{mix}} = \lambda_{\mathrm{mix}}\hat{\rho}_{AB} + \frac{1-\lambda_{\mathrm{mix}}}{d^2}\hat{\mathbb{1}} \tag{3.32}$$

ただし，λ_{mix} はノイズによる理想状態からの劣化度合を示すパラメータである．d 次元 2 光子完全混合状態 $\hat{\mathbb{1}}/d^2$ は，ノイズにより完全ランダムになった状態に対応する．すなわち，このノイズモデルは，確率 λ_{mix} で元の量子状態 $\hat{\rho}_{AB}$ を，確率 $1-\lambda_{\mathrm{mix}}$ でランダムなノイズ状態 $\hat{\mathbb{1}}/d^2$ を出力するモデルとなっている．ここで，演算子化した相関パラメータ $\hat{S}_d$ を用いると，ノイズにより劣化した CGLMP 不等式の相関パラメータ $\tilde{S}_d$ は，元の

量子状態に対する S_d を用いて，次式のように与えられる．

$$\begin{aligned}\tilde{S}_d &= \mathrm{Tr}\left(\hat{S}_d\hat{\rho}_{\mathrm{mix}}\right)\\ &= \lambda_{\mathrm{mix}}\,\mathrm{Tr}\left(\hat{S}_d\hat{\rho}_{AB}\right) + \frac{1-\lambda_{\mathrm{mix}}}{d^2}\,\mathrm{Tr}\left(\hat{S}_d\hat{\mathbb{1}}\right)\\ &= \lambda_{\mathrm{mix}}\,\mathrm{Tr}\left(\hat{S}_d\hat{\rho}_{AB}\right)\\ &= \lambda_{\mathrm{mix}}S_d\end{aligned} \tag{3.33}$$

ただし，上記計算過程では $\mathrm{Tr}\left(\hat{S}_d\right)=0$ であることを用いた．上式は，CGLMP 不等式を破る，すなわち $\tilde{S}_d \geq 2$ となるために必要なノイズパラメータの閾値 λ_c が，$\lambda_c = 2/S_d$ で与えられることを示している．これより，高い S_d 値を与える量子状態を測定すると，小さい λ_c 値で CGLMP 不等式を破ることが可能となり，測定系のノイズ耐性が高いことが分かる．

CGLMP 不等式の破れを実証するのに必要な λ_c は，以下のようにして干渉縞の明瞭度と対応付けられる．まず，式 (3.32) の状態密度演算子で表される量子状態が，フーリエ基底状態へ射影測定される確率を求める．フーリエ基底状態の位相として，Alice の位相が θ_A，Bob の位相が θ_B である時の，Alice と Bob の同時検出確率 $\Pr(\theta_A,\theta_B)$ は次式で与えられる．

$$\begin{aligned}\Pr(\theta_A,\theta_B) &= \langle\theta_A|\langle\theta_B|\hat{\rho}_{\mathrm{mix}}|\theta_A\rangle|\theta_B\rangle\\ &= \lambda_{\mathrm{mix}}\langle\theta_A|\langle\theta_B|\hat{\rho}_{AB}|\theta_A\rangle|\theta_B\rangle + \frac{1-\lambda_{\mathrm{mix}}}{d^2}\langle\theta_A|\langle\theta_B|\hat{\mathbb{1}}|\theta_A\rangle|\theta_B\rangle\\ &= \lambda_{\mathrm{mix}}\langle\theta_A|\langle\theta_B|\hat{\rho}_{AB}|\theta_A\rangle|\theta_B\rangle + \frac{1-\lambda_{\mathrm{mix}}}{d^2}\\ &= \lambda_{\mathrm{mix}}\Pr(\theta_A,\theta_B;\hat{\rho}_{AB}) + \frac{1-\lambda_{\mathrm{mix}}}{d^2}\end{aligned} \tag{3.34}$$

ただし，$\Pr(\theta_A,\theta_B;\hat{\rho}_{AB}) = \langle\theta_A|\langle\theta_B|\hat{\rho}_{AB}|\theta_A\rangle|\theta_B\rangle$ とした．具体的には，被測定状態が 4 次元最大量子もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$ または 4 次元最適量子もつれ状態 $|\Psi_{\mathrm{OES}}\rangle$ である時，$\Pr(\theta_A,\theta_B;\hat{\rho}_{AB})$ はそれぞれ次式で与えられる．

$$\begin{aligned}\Pr(\theta_A,\theta_B;|\Psi_{\mathrm{MES}}\rangle\langle\Psi_{\mathrm{MES}}|) &= \left|\langle\theta_A|\langle\theta_B|\Psi_{\mathrm{MES}}\rangle\right|^2\\ &= \frac{1}{4}\cos^2\left(\frac{\theta_A+\theta_B}{2}\right)\cos^2(\theta_A+\theta_B)\end{aligned} \tag{3.35}$$

$$\begin{aligned}\Pr(\theta_A,\theta_B;|\Psi_{\mathrm{OES}}\rangle\langle\Psi_{\mathrm{OES}}|) &= \left|\langle\theta_A|\langle\theta_B|\Psi_{\mathrm{OES}}\rangle\right|^2\\ &= \frac{1}{8(1+\gamma^2)}\left[\cos\left\{\frac{3}{2}(\theta_A+\theta_B)\right\} + \gamma\cos\left(\frac{\theta_A+\theta_B}{2}\right)\right]^2\end{aligned} \tag{3.36}$$

これらの確率の最大値はそれぞれ 1/4 または $\frac{(1+\gamma)^2}{8(1+\gamma^2)}$ であり，最小値はともに 0 である．

干渉縞の明瞭度 V は，θ_A, θ_B をそれぞれ $[0, 2\pi]$ の範囲で変化させた時の，光子検出確率 $\Pr(\theta_A, \theta_B)$ の最大値 $\max \Pr(\theta_A, \theta_B)$ および最小値 $\min \Pr(\theta_A, \theta_B)$ を用いて，次のように定義される．

$$V \coloneqq \frac{\max \Pr(\theta_A, \theta_B) - \min \Pr(\theta_A, \theta_B)}{\max \Pr(\theta_A, \theta_B) + \min \Pr(\theta_A, \theta_B)} \tag{3.37}$$

式 (3.34)–(3.37) および式 (3.33) から求まる，CGLMP 不等式の破れの観測に必要なノイズパラメータの閾値 λ_c を用いると，CGLMP 不等式の破れの観測に必要な明瞭度の下限 V_c が求まる．具体的には，4 次元最大量子もつれ状態の場合は $V_c = 81.7\%$，4 次元最適量子もつれ状態の場合は $V_c = 80.1\%$ となる．よって，最適もつれ状態を用いると，よりノイズが大きく明瞭度が低い場合でも，量子もつれ状態を検証しやすくなる．

ただし，明瞭度による検証法はあくまで簡易な手法であり，高い明瞭度を観測したからといって，直ちに CGLMP 不等式の破れが実証できたとは結論付けられない．例えば，干渉縞の形状が歪んでいる場合には，CGLMP 不等式の破れが観測できたとは言えない．また，通常，明瞭度を測る際には，θ_B を固定し，θ_A を $[0, 2\pi]$ の間で変化させて明瞭度を測定するが，θ_B の設定値が一つだけだと，セパラブル状態 (非もつれ状態) であっても同様の干渉縞を示すことがあり得る．したがって，真に量子もつれ状態を検証するには，CGLMP 不等式を直接評価することが必要となる．

3.5 実験系

前節までで述べた，4 次元タイムビン量子もつれ状態生成法および CGLMP 不等式評価法を，実験により検証した．本節ではその実験系について述べる．

図 3.6 に実験系構成を示す．波長 1551.1 nm のCW レーザ光を 2 段接続 $LiNbO_3$ 光強度変調器 (IM) により変調し，パルス幅 100 ps/パルス間隔 1 ns の 4 連続パルス列を繰り返し周波数 125 MHz で生成する．IM1 はポンプ光強度比が最適もつれ状態を生成する比率となるように強度変調するため，IM2 はNRZ 光をパルス化するために用いる．4 連パルスは，エルビウム添加光ファイバ増幅器 (EDFA) で増幅後，ファイバブラッググレーティングフィルタ (FBG) により雑音光が除去されたのち，可変光減衰器 (VATT) により，後段の SPDC で発生する光子対の数が 4 連パルス当たり平均で 0.01 となるように光パワーが設定される．その後，4 連パルス列は周期的分極反転ニオブ酸リチウム (PPLN) 導波路に入力され，導波路内で生じる第二次高調波生成 (SHG) によって，波長 780 nm の光パルス列に変換される．そして，光バンドパスフィルタ (BPF) により，波長 1551.1 nm の光を除去したパルス列を，SPDC による量子もつれ状態生成のためのポンプ光とする．このポンプパルス列は次段の PPLN 導波路に入力され，ここで発生する SPDC により 4 次元タイムビン量子もつれ状態が生成される．ここで発生するシグナル/アイドラー

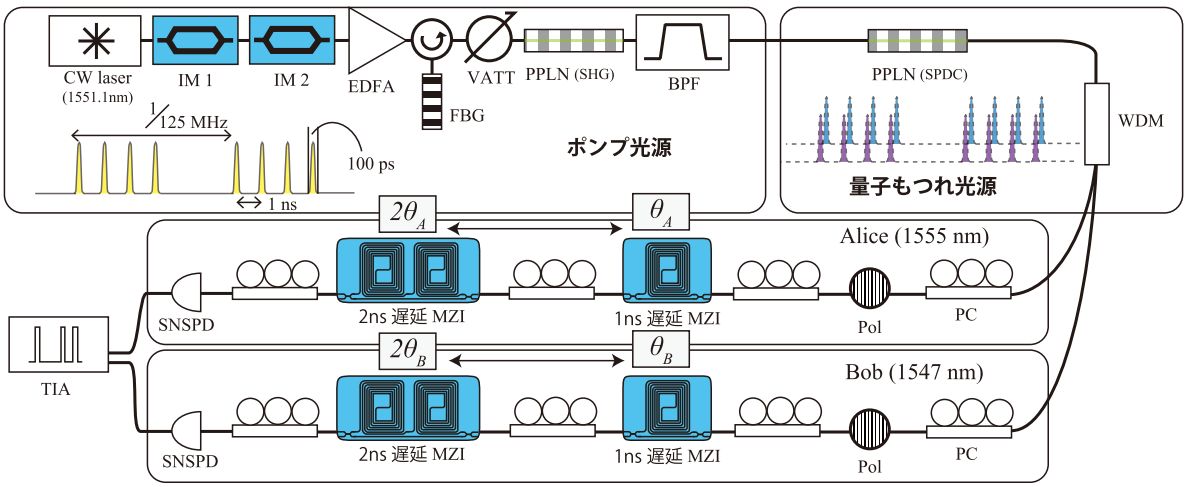

図 3.6　実験系．CW laser: CW レーザ光源，IM: 光強度変調器，EDFA: エルビウム添加光ファイバ増幅器，FBG: ファイバブラッググレーティングフィルタ，VATT: 可変光減衰器，PPLN: 周期的分極反転ニオブ酸リチウム，BPF: 光バンドパスフィルタ，WDM: 波長分離フィルタ，PC: 偏波コントローラ，Pol: 偏光子，遅延 MZI: 遅延 Mach-Zehnder 干渉計，SNSPD: 超伝導ナノワイヤ単一光子検出器，TIA: タイムインターバルアナライザ

光は，位相整合条件を満たす広い波長域にわたり生成される．この中から 3.3 節で述べた $\omega_1 + \omega_2 = \omega_3$ を満たす，1555 nm と 1547 nm の光を透過帯域幅 100 GHz の波長分離フィルタ (WDM) によって抜き出し，前者を Alice に，後者を Bob にそれぞれ送信する．実験に用いた干渉計には偏波依存性があるため，送信された光パルス列は，偏波コントローラ (PC) および偏光子 (Pol) によって偏波状態が調整された後，多段遅延 MZI に入力される．この MZI は平面光波回路 (PLC) 技術により作製されており，基板の温度制御，および光路上に取り付けられた薄膜ヒータによる熱光学効果を介した屈折率制御によって，安定した干渉動作が得られる [93, 94]．この薄膜ヒータへの印加電流により MZI の 2 経路の伝搬位相差を設定して，3.4.1 節で述べたフーリエ基底状態への射影測定を実装する．2 段 MZI から出力されたパルス列は，光子検出効率が最大となるように偏波が調整された後，超伝導ナノワイヤ単一光子検出器 (SNSPD) に入力される．SNSPD の光子検出効率は，Alice と Bob でそれぞれ 19, 17% であった．SNSPD では，光子を入力していないときにも，誤って検出信号を出力するダークカウントという現象が生じるが，どちらの検出器においてもダークカウント率は 10 cps (counts/sec) 以下であった．SNSPD からの検出信号はタイムインターバルアナライザ (TIA) に入力され，測定対象となる時間位置における，2 つの SNSPD での同時検出数 (同時計数) がカウントされる．以上により，CGLMP 不等式の評価に必要な測定値を得る．

3.6　実験結果

3.6.1　最大量子もつれ状態の場合

前節で述べた実験系により，最大量子もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$ を生成/測定した．本節では，その実験結果を述べる．

3.4.2 節で述べたように，CGLMP 不等式の簡易な評価法として，Bob 側の位相 θ_B を固定し，Alice 側の位相 θ_A を $[0, 2\pi]$ で変化させたときの，干渉パターンの明瞭度を測定する方法がしばしば用いられる．そこでまず，この干渉縞測定を行った．図 3.7 に，Bob の射影位相を $\theta_B = 0$ または $\pi/4$ とした時の，90 秒間同時計数の測定結果を示す．横軸は Alice の射影測定フーリエ基底状態 $|\theta_A\rangle$ の位相，縦軸は同時計数である．赤丸は Bob 側の位相が $\theta_B = 0$ の時，青三角は $\theta_B = \pi/4$ の時の結果である．また，同時計数がポアソン分布に従うという仮定の下での標準偏差をエラーバーにより示している．

最大量子もつれ状態を測定した場合の干渉縞の θ_A, θ_B 依存性は，式 (3.35) の $\Pr(\theta_A, \theta_B; |\Psi_{\mathrm{MES}}\rangle\langle\Psi_{\mathrm{MES}}|)$ で与えられる．そこで，測定によって得られた同時計数に対し，次式によるフィッティングを行った．

$$C^{\mathrm{fit}}_{\mathrm{MES}}(\theta_A, \theta_B) = m_1 \frac{\Pr(\theta_A, \theta_B; |\Psi_{\mathrm{MES}}\rangle\langle\Psi_{\mathrm{MES}}|)}{\max \Pr(\theta_A, \theta_B; |\Psi_{\mathrm{MES}}\rangle\langle\Psi_{\mathrm{MES}}|)} + m_2 \tag{3.38}$$

ただし，$\max \Pr(\theta_A, \theta_B; |\Psi_{\mathrm{MES}}\rangle\langle\Psi_{\mathrm{MES}}|) = 1/4$ であり，m_1, m_2 は曲線のフィッティングパラメータである．同じ図 3.7 に，$\theta_B = 0, \pi/4$ の同時計数それぞれについて，上式に

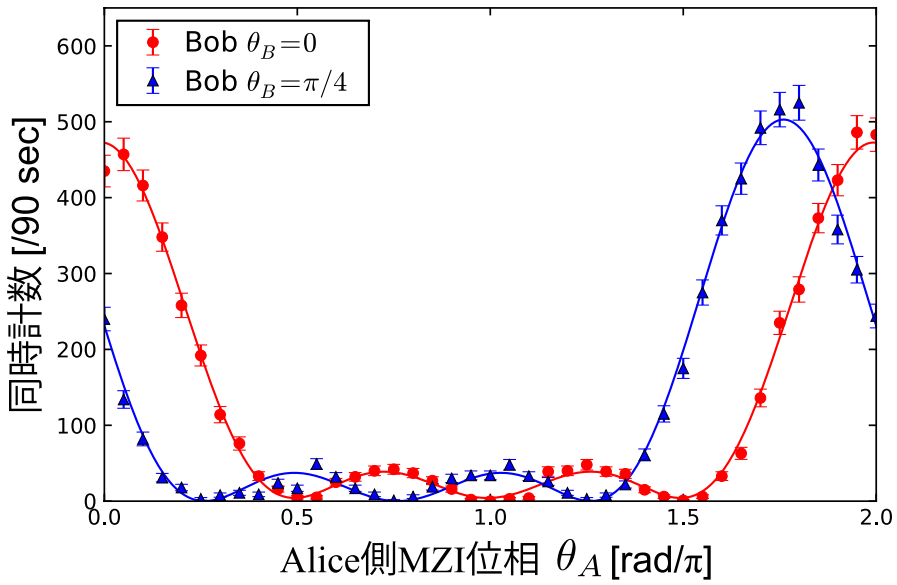

図 3.7　最大もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$ を測定した場合の，Alice の干渉計位相 θ_A に対する同時計数

表 3.2　最大量子もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$ に対する，CGLMP 不等式検証のための同時計数 [/2 min]

			Bob							
			基底 $b=0$				基底 $b=1$			
		[rad]	$\frac{\pi}{8}$	$-\frac{3}{8}\pi$	$-\frac{7}{8}\pi$	$-\frac{11}{8}\pi$	$-\frac{\pi}{8}$	$-\frac{5}{8}\pi$	$-\frac{9}{8}\pi$	$-\frac{13}{8}\pi$
Alice	基底 $a=0$	0	605	72	34	49	493	36	37	67
		$\frac{\pi}{2}$	46	453	74	17	62	545	31	38
		π	29	40	508	85	30	45	555	27
		$\frac{3}{2}\pi$	102	32	33	535	26	26	48	671
	基底 $a=1$	$\frac{\pi}{4}$	102	529	40	47	515	94	23	53
		$\frac{3}{4}\pi$	30	28	473	28	22	445	92	24
		$\frac{5}{4}\pi$	47	15	97	581	25	28	581	98
		$\frac{7}{4}\pi$	611	22	18	48	67	27	34	600

よるフィッティング曲線を赤と青の実線で示す．このフィッティングパラメータから，式 (3.37) の明瞭度 V が次式によって求められる．

$$V = \frac{m_1}{m_1 + 2m_2} \tag{3.39}$$

フィッティングの結果, $\theta_B = 0, \pi/4$ それぞれに対して, $V = 98.25\pm0.86, 99.96\pm0.94\%$ であった．3.4.2 節で述べた通り，最大量子もつれ状態の場合に，CGLMP 不等式の破れを観測するために必要な明瞭度は $V \geq 81.7\%$ である．したがって，$\theta_B = 0, \pi/4$ のどちらの場合においても，CGLMP 不等式の破れを示唆する干渉パターンが観測できたと言える．

ただし，3.4.2 節で述べた通り，明瞭度による評価は特定のノイズモデルを仮定した簡易な手法であり，CGLMP 不等式の破れを直接示すものではない．そこで，式 (3.12)–(3.14) で与えられる位相の組合せにおける同時計数測定を行い，CGLMP 不等式の相関パラメータ S_4 を直接評価した．表 3.2 に，各 θ_A, θ_B の組合せについて，2 分間測定を行った時の同時計数を示す．この測定結果から，式 (3.10) 中の確率を求め，相関パラメータを計算したところ，$S_4 = 2.774 \pm 0.025$ を得た．ただし，誤差範囲は同時計数がポアソン分布に従うと仮定して計算したものである．この値は，CGLMP 不等式 $S_4 \leq 2$ と比べ，標準偏差の 31 倍大きな値となっている．よって，4 次元タイムビン量子もつれ状態を用いて，CGLMP 不等式の破れを明確に観測することができたといえる．

3.6.2　最適量子もつれ状態の場合

次に，CGLMP 不等式の破れを最大化する，最適量子もつれ状態 $|\Psi_{\mathrm{OES}}\rangle$ の生成/測定実験を行った．本節ではその実験結果について述べる．

3.3 節で述べたように，SPDC のポンプ光パルス列を強度変調する事によって，最適量子もつれ状態を生成することができる．図 3.6 に示す実験系の IM1 により，4 連ポンプパルスの強度比を $1:\gamma^2:\gamma^2:1$(ただし，$\gamma<1$) に変調して，最適もつれ状態を生成した．波長分離フィルタにより取り出したシグナル光を，直接 SNSPD で測定した時の，光子検出数のヒストグラムを図 3.8 に示す．横軸は TIA 上の光子検出時刻，縦軸は各時刻における光子検出数の相対値である．図には 3 周期分の 4 連パルスの測定結果が示されており，各ピークの高さが，それぞれの時間位置での光子検出確率に対応する．この光子検出数の比から，$|\Psi_{\mathrm{OES}}\rangle$ の振幅の変調パラメータ γ は $\gamma=0.738$ と推定された．この値は，最適値 $\gamma=0.739$ に近い値であり，強度変調器によるポンプ光変調というシンプルな手法により，最適量子もつれ状態が生成されたことが示唆される．

上記のように生成した最適量子もつれ状態に対して，干渉縞測定実験を行った．図 3.9 に，Bob 側の位相を $\theta_B=0$ で固定して Alice 側の位相を変化させたときの，60 秒間の同時計数を示す．4 連パルス当たりの平均光子数は 0.02 とした．横軸は Alice の射影測定フーリエ基底状態 $|\theta_A\rangle$ の位相，縦軸は最大値で規格化した同時計数である．比較のため，図には最大量子もつれ状態測定時の規格化同時計数 [図 (3.7)] もプロットしてある．赤丸

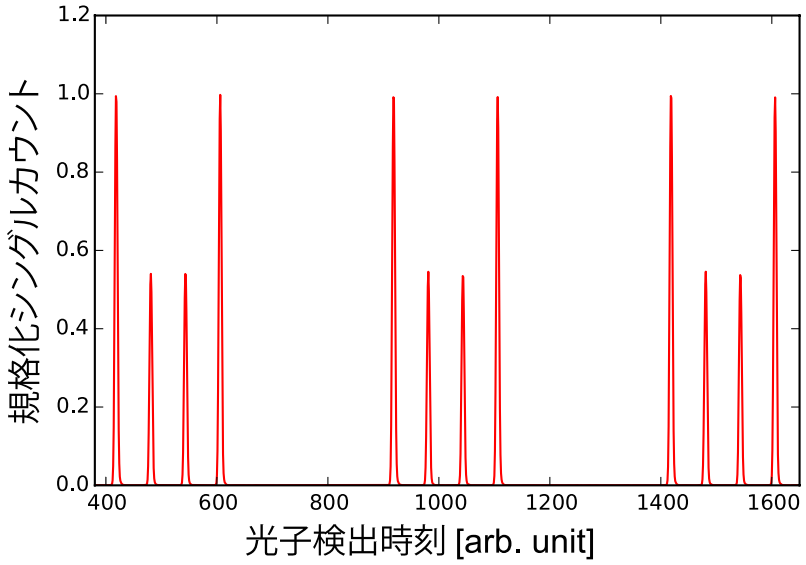

図 3.8　波長分離フィルタ直後で測定した，最適量子もつれ状態 $|\Psi_{\mathrm{OES}}\rangle$ に対する規格化シングルカウント

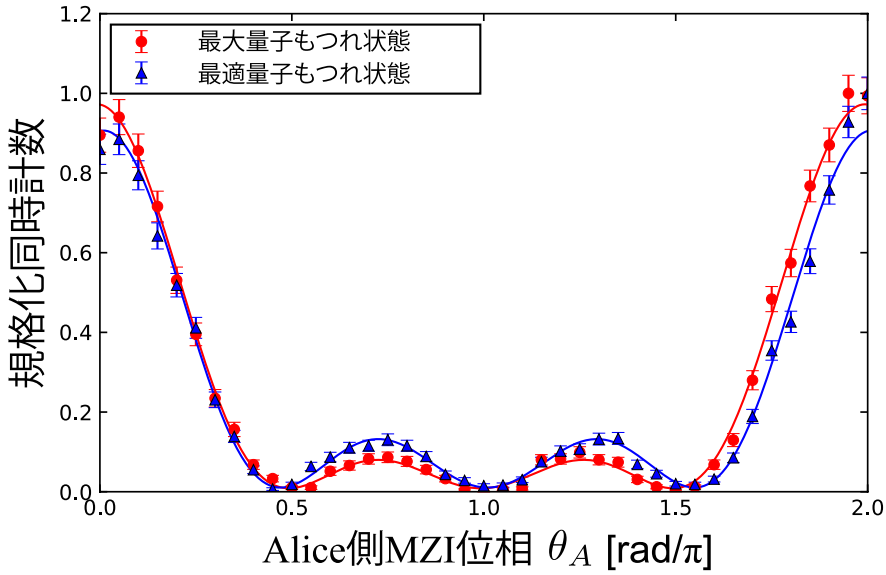

図 3.9　最適もつれ状態 $|\Psi_{\rm OES}\rangle$ を測定した場合の，Alice の干渉計位相 θ_A に対する同時計数 [/60 sec](Bob の位相は $\theta_B = 0$)

が最大量子もつれ状態に対する測定結果，青三角が最適量子もつれ状態に対する測定結果である．エラーバーは，同時計数がポアソン分布に従うとした時の標準偏差である．最適量子もつれ状態の測定結果は，最大量子もつれ状態の測定結果に比べて，$\theta_A = 3\pi/4$ および $5\pi/4$ 付近の小さなピークの値が高く，また，$\theta_A = \pi/2, 3\pi/2$ 近傍の極小値の位置がそれぞれやや左または右側にシフトしている．この測定結果に対して，前節と同様に，次式によるフィッティングを行った．

$$C^{\rm fit}_{\rm OES}(\theta_A, \theta_B) = m_1 \frac{\Pr(\theta_A, \theta_B; |\Psi_{\rm OES}\rangle\langle\Psi_{\rm OES}|)}{\max \Pr(\theta_A, \theta_B; |\Psi_{\rm OES}\rangle\langle\Psi_{\rm OES}|)} + m_2 \tag{3.40}$$

ただし，$\max \Pr(\theta_A, \theta_B; |\Psi_{\rm OES}\rangle\langle\Psi_{\rm OES}|) = \dfrac{(1+\gamma)^2}{8(1+\gamma^2)}$ であり，m_1, m_2 は曲線のフィッティングパラメータである．図 3.9 に青色の実線で示されているのが，フィッティングによって得られた曲線である．これより得られる干渉縞の明瞭度は $V = 97.72 \pm 1.30\%$ であった．さらに，同様の測定/フィッティングを Bob 側の位相を $\theta_B = \pi/4$ として行ったところ，$V = 97.44 \pm 0.96\%$ であった．最適量子もつれ状態を測定した場合の，CGLMP 不等式の破れ観測に必要な明瞭度は $V \geq 80.1\%$ である．したがって，本実験により，CGLMP 不等式の破れを示唆する干渉パターンが観測がされたと言える．

次に，CGLMP 不等式そのものを評価する相関パラメータの位相の組み合わせについて，同時計数を測定した．表 3.3 に，各 θ_A, θ_B の組合せについて，2 分間測定した結果を示す．この測定結果から相関パラメータを計算したところ，$S_4 = 2.913 \pm 0.023$ であった．この値は，CGLMP 不等式の閾値 2 を標準偏差の 39 倍上回っており，最大量子もつ

表 3.3 最適量子もつれ状態 $|\Psi_{\mathrm{OES}}\rangle$ に対する，CGLMP 不等式の検証のための同時計数 [/2 min]

			Bob							
			基底 $b=0$				基底 $b=1$			
		[rad]	$\frac{\pi}{8}$	$-\frac{3}{8}\pi$	$-\frac{7}{8}\pi$	$-\frac{11}{8}\pi$	$-\frac{\pi}{8}$	$-\frac{5}{8}\pi$	$-\frac{9}{8}\pi$	$-\frac{13}{8}\pi$
Alice	基底 $a=0$	0	544	38	21	60	517	54	33	30
		$\frac{\pi}{2}$	57	426	46	24	24	458	47	53
		π	29	63	470	25	20	26	453	53
		$\frac{3}{2}\pi$	30	49	63	408	57	43	21	445
	基底 $a=1$	$\frac{\pi}{4}$	57	462	64	42	517	40	18	84
		$\frac{3}{4}\pi$	52	29	422	35	57	398	44	20
		$\frac{5}{4}\pi$	70	28	51	439	56	80	430	31
		$\frac{7}{4}\pi$	459	55	48	30	44	40	71	408

れ状態測定時の値より大きい．すなわち，本実験により最適化された高次元タイムビン量子もつれ状態により，CGLMP 不等式の破れが増大することが初めて観測された．最適量子もつれ状態自体は QKD 性能を向上させるものではないが，これまで検証されていなかった不等式の明確な破れの増加が実証できるほどに，高い安定性と制御性をもつ高次元タイムビン量子もつれ状態が生成/測定できることが示されたと言える．

3.7 結言

本章では，高次元量子もつれ状態の生成方法およびその実験的検証について述べた．一般に，量子もつれ状態の判定には，古典的な隠れた変数理論から導き出されるベル不等式が破られるか否かが基準となる．そこでまず，ベル不等式の高次元量子状態への拡張である CGLMP 不等式について述べ，量子もつれ状態を最適化することで，より大きな不等式の破れが観測可能であることを示した．そして，SPDC を用いたタイムビン量子もつれ状態の生成法において，ポンプ光の強度制御という簡便な方法により，不等式の破れを最大化する最適量子もつれ状態が生成できることを示した．また，CGLMP 不等式の破れ観測に必要なフーリエ基底状態への射影測定を，多段接続 MZI を用いて実装する手法について述べた．そして，これら SPDC による状態生成法と MZI による測定法を用いた検証実験を行い，4 次元タイムビン量子もつれ状態についての CGLMP 不等式の破れを初めて観測した．また，ポンプ光強度変調を用いた最適量子もつれ状態生成法により，CGLMP 不等式の破れが増大することを初めて実験的に観測し，上記量子もつれ状態生成/測定法の高い安定性と制御性を示した．

第 4 章

量子状態トモグラフィーを用いた高次元量子もつれ状態の長距離伝送特性評価

4.1 緒言

本論文では，QKD への応用を想定し，長距離ファイバ伝送が可能な高次元量子もつれ状態として，タイムビン状態を採り上げている．そこで本章では，前章の手法で生成した高次元タイムビン量子状態の長距離伝送特性を検証する．ただし，特性評価にあたっては，QKD プロトコルで用いられている測定法ではなく，量子状態トモグラフィー (QST: Quantum State Tomography) と呼ばれる手法を用いる．これは，QKD に限らず，他の量子通信システムへの応用も視野に入れているためである．QST を用いれば，特定の測定法によらず，もつれ状態そのものの特性あるいは品質を一般的に評価することができる．まず 4.2 節にて，QST による状態密度演算子の推定について述べる．長距離伝送された量子状態を測定する場合，伝搬損失のためにごく少数の光子しか受信できず，統計的な測定に長時間を要する．そのため，簡便なセットアップによる効率的な測定系の実装が必要となる．そこで本論文では，既存の 2 次元タイムビン量子状態に対する QST[90] を拡張し，2 値の遅延位相をもつ MZI をカスケード接続した構成による，高次元タイムビン量子状態に対する効率的な QST の実装法を提案する．

量子状態の定量的な評価にあたっては，QST によって推定された状態密度演算子から様々な指標を見積もることになる．そこで 4.3 節では，高次元量子もつれ状態に関わるいくつかの指標を紹介する．そして 4.4 節にて，提案した QST の原理実証実験，および 100 km ファイバ伝送後の量子状態に対する QST により，長距離伝送後の 4 次元タイムビン量子もつれ状態の品質を検証する．

4.2　量子状態トモグラフィー

2.2.2 節で述べたように，古典状態を含む一般的な混合量子状態は，状態密度演算子によって記述される．状態密度演算子は与えられた量子状態についての測定確率に関するすべての情報を含んでおり，状態密度演算子から任意の物理量や状態に関する情報を得ることができる．したがって，状態密度演算子を推定することで，特定の量子通信プロトコルによらない，量子状態そのものの評価が可能となる．

量子状態トモグラフィー (QST: Quantum State Tomography)[95, 96] は，複数の測定結果の確率分布から，状態密度演算子を推定する手法である．これまで，高次元量子状態に対する QST としては，光軌道角運動量 (OAM)/周波数位置/時間エネルギー不確定性に基づく量子状態に対する実装法が知られている他 [50, 56, 97]，高次元タイムビン量子状態に対する QST も近年報告されている [49]．この手法では，d 次元時間位置基底状態のうち，特定の二つの時間位置基底状態 $|i\rangle, |j\rangle$ を縦/横偏波状態 $|H\rangle, |V\rangle$ に変換し，偏波量子状態に対する QST を適用することで高次元量子状態に対する QST を行っている．しかしながら，実験系が複雑であることに加え，二次元部分空間への射影を用いるために，多数のパラメータの組み合わせについて測定する必要がある．本章では，QST により長距離伝送後の量子もつれ状態を検証するが，ファイバ損失によって多数の光子が失われるため，測定に長時間を要する．したがって，測定に用いる設定パラメータ数が少ない QST が望まれる．そこで本節では，既存の 2 次元タイムビン量子状態に対する QST[90] を拡張して，高次元タイムビン量子状態に対するコンパクトな QST を提案する．

4.2.1　2 次元タイムビン量子状態に対する QST

本節では，本論文で提案する手法の基礎となる，既存の 2 次元タイムビン量子状態に対する QST[90] について説明する．なお，複数光子全体を表す状態密度演算子の QST には，各光子に対する QST 実装に必要な測定を組み合わせればよいことが知られているため [95]，ここでは量子もつれ状態のような 2 光子に対する QST ではなく，1 光子の 2 次元タイムビン量子状態に対する QST についてのみ述べることとする．

状態密度演算子 $\hat{\rho}$ は，時間位置基底による展開形として，一般に式 (2.19) のように表すことができる．2 次元の場合，式 (2.19) は次式となる．

$$\hat{\rho} = \sum_{i,j\in\{0,1\}} r_{ij} \, |i\rangle\langle j| \tag{4.1}$$

QST とは，上記の r_{ij} を要素とするエルミート行列を推定することである．2 次元の場合は 2×2 の行列であるため，合計 4 つの実数パラメータを推定することになる．ただし，

状態密度演算子は，確率の総和である $\mathrm{Tr}(\hat{\rho}) = 1$，すなわち $r_{00} + r_{11} = 1$ という制約条件があるため，推定すべきパラメータ数は 3 である．

$\hat{\rho}$ がエルミート演算子であることを利用すると，式 (4.1) は Pauli 演算子を用いた展開形でも表現できる．ここで，Pauli 演算子とは，次式で与えられる 3 つのエルミートかつユニタリーな演算子である．

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |+\rangle\langle+| - |-\rangle\langle-| \tag{4.2}$$

$$\hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = |L\rangle\langle L| - |R\rangle\langle R| \tag{4.3}$$

$$\hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{4.4}$$

ただし，行列表現は，演算子を時間位置基底 $|0\rangle, |1\rangle$ およびそのエルミート共役 $\langle 0|, \langle 1|$ により展開した時の表式である．一般に演算子を異なる基底で表現すると行列表現は異なるものとなるが，本章ではつねに時間位置基底による行列表現を用いる．また，式 (4.4) の $\hat{\sigma}_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ という表式は，$\hat{\sigma}_z$ の固有状態は $|0\rangle, |1\rangle$，その固有値がそれぞれ $+1, -1$ であることを示している．$\hat{\sigma}_x, \hat{\sigma}_y$ も同様に，固有状態がそれぞれ $\{|+\rangle, |-\rangle\}, \{|L\rangle, |R\rangle\}$ であり，± 1 の固有値を持つ．

Pauli 演算子は，全てトレースレス，すなわちトレースが 0 の演算子であり，さらに次の関係式を満たしている．

$$\hat{\sigma}_x^2 = \hat{\sigma}_y^2 = \hat{\sigma}_z^2 = \hat{\mathbb{1}} \tag{4.5}$$

$$\begin{cases} \hat{\sigma}_x\hat{\sigma}_y = -\hat{\sigma}_y\hat{\sigma}_x = i\hat{\sigma}_z \\ \hat{\sigma}_y\hat{\sigma}_z = -\hat{\sigma}_z\hat{\sigma}_y = i\hat{\sigma}_x \\ \hat{\sigma}_z\hat{\sigma}_x = -\hat{\sigma}_x\hat{\sigma}_z = i\hat{\sigma}_y \end{cases} \tag{4.6}$$

Pauli 演算子を用いると，式 (4.1) の状態密度演算子 $\hat{\rho}$ は次式のように書き直される．

$$\hat{\rho} = \frac{1}{2}\left(\hat{\mathbb{1}} + s_x\hat{\sigma}_x + s_y\hat{\sigma}_y + s_z\hat{\sigma}_z\right) \tag{4.7}$$

ここで s_x, s_y, s_z は実数パラメータである．上式は，QST としてはこの 3 つの実数 s_x, s_y, s_z を推定すればよいことを示している．ここで，Pauli 演算子がトレースレスであること，および式 (4.5), (4.6) から，次式が成り立っている．

$$s_z = \mathrm{Tr}(\hat{\sigma}_z\hat{\rho}) \tag{4.8}$$

式 (4.4) の固有値展開形を用いると，この表式は次のように書き直される．

$$\begin{aligned} s_z &= \mathrm{Tr}(|0\rangle\langle 0|\,\hat{\rho}) - \mathrm{Tr}(|1\rangle\langle 1|\,\hat{\rho}) \\ &= \langle 0|\,\hat{\rho}\,|0\rangle - \langle 1|\,\hat{\rho}\,|1\rangle \end{aligned} \tag{4.9}$$

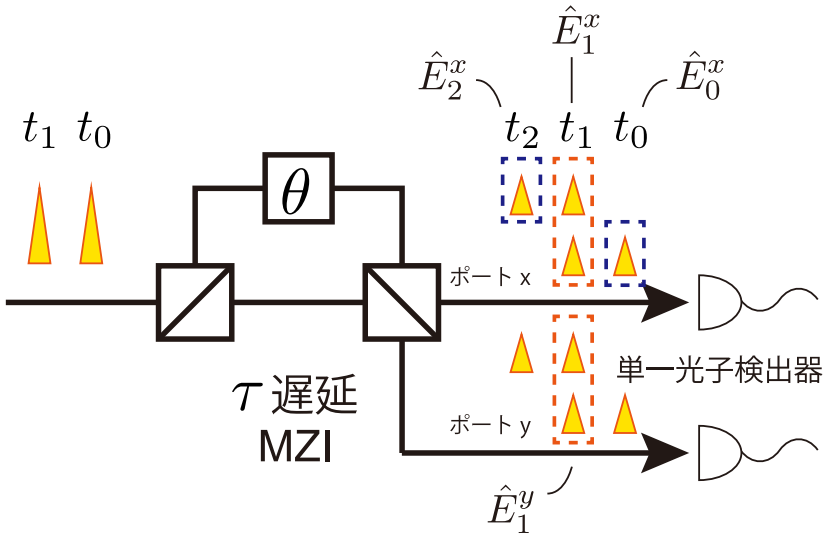

図 4.1　遅延 MZI を用いた 2 次元タイムビン量子状態の QST

$\hat{\sigma}_x, \hat{\sigma}_y$ についても同様である．上式は，Pauli 演算子 $\hat{\sigma}_i (i \in \{x, y, z\})$ の固有状態に対する測定確率の差によって，対応する s_i が決定できることを示している．式 (4.2)–(4.4) に示されているように，3 つの Pauli 演算子の固有状態は，それぞれ時間位置基底 $\{|0\rangle, |1\rangle\}$，位相基底 $\{|+\rangle, |-\rangle\}$，位相基底 $\{|L\rangle, |R\rangle\}$ の各基底状態である．したがって，これらの状態への射影測定を実装すれば，2 次元タイムビン量子状態への QST が実装できたことになる．

なお，2.2.1 節で述べた通り，位相基底 $\{|+\rangle, |-\rangle\}$ および $\{|L\rangle, |R\rangle\}$ は，水平/垂直偏波を基底とするジョーンズベクトルとの類似性からこのように表記される．この類似性から式 (4.9) をながめると，s_x, s_y, s_z は規格化したストークスベクトルの 3 つの成分に対応することが分かる．したがって，2 次元量子状態の QST は，古典電磁気学ではストークスベクトルによる偏波状態の推定に対応すると言える．

上記 3 つのパラメータは，遅延 MZI を用いて測定することができる [90]．2.2.3 節で述べたように，2 次元タイムビン量子状態を遅延 MZI に入力すると，3 つの異なる時間位置で光子が検出され得る (図 4.1)．この時，式 (2.40), (2.42) の POVM 要素 $\hat{E}_0^x, \hat{E}_2^x$ が示すように，MZI 出力における時間位置 t_0, t_2 での光子検出は，被測定状態に対する時間位置基底への射影測定となる．一方，式 (2.41), (2.43) の POVM 要素 $\hat{E}_1^x, \hat{E}_1^y$ が示すように，時間位置 t_1 での光子検出は，出力ポートに応じてそれぞれ状態 $\left(|0\rangle + e^{i\theta}|1\rangle\right)/\sqrt{2}$ および状態 $\left(|0\rangle - e^{i\theta}|1\rangle\right)/\sqrt{2}$ への射影測定となる．ここで，$\theta = 0$ とすれば位相基底 $\{|+\rangle, |-\rangle\}$ への射影測定が，$\theta = \pi/2$ とすれば位相基底 $\{|L\rangle, |R\rangle\}$ への射影測定が実装される．すなわち，設定パラメータが二値の遅延位相である遅延 MZI を用いることにより，2 次元タイムビン量子状態の QST が実装できる．

なお，図 4.1 の構成では，MZI の出力双方に光子検出器を配置しているが，QST 実装においては一方が不要となる．これは，位相基底の 2 つの基底状態，例えば状態 $|+\rangle$ と $|-\rangle$ への射影測定確率の和が 1 であり，一方の測定確率が分かれば他方の測定確率は観測しなくても分かるためである．ただし，時間位置基底の測定は双方用いる必要がある．これは，ある状態への射影測定確率を実験的に推定するためには，その状態への射影測定で検出された光子数を，基底を構成する全ての状態への射影測定で検出された光子数で規格化した，検出割合によって推定するためである．ただし，規格化のための光子数はどれか一つの基底での検出光子の総数が分かればよい．これはどの基底においても確率の合計は 1 であるから，別の基底での検出光子の総数が期待値としては同じであるためである．よって時間位置基底での検出光子数の総数が分かれば，位相基底での検出光子数の総数を実際に測定する必要はない．図 4.1 で言えば，青色の点線で囲われた部分での光子検出の総数が分かれば，橙色の点線で囲われた部分での光子検出の総数は不要である (ただし，分岐比にあたる POVM 要素の係数分の補正は必要)．したがって，単一の MZI，単一の光子検出器，および 2 種の位相パラメータのみで QST をコンパクトに実装できる．

4.2.2 高次元タイムビン量子状態に対する QST

本節では，前節で述べた 2 次元タイムビン量子状態に対する QST を，高次元タイムビン量子状態に拡張する．

まず，高次元量子状態の QST のために，測定系が満たすべき条件を考察する．d 次元量子状態の密度演算子 $\hat{\rho}$ は，式 (2.19) 中の r_{ij} を要素とする $d \times d$ エルミート行列によって表される．2 次元量子状態の密度演算子は式 (4.2)–(4.4) の Pauli 演算子の線形和で表された．同様に，d 次元量子状態の密度演算子は，エルミート性に着目して Pauli 演算子を高次元化した，一般化 Gell–Mann 演算子 $\hat{G}_i$ の線形和として記述できる [96].

まず，一般化 Gell–Mann 演算子は次のようにして定義される．時間位置基底で展開した行列表現において，j 行 k 列の要素のみが 1 であり $(j, k \in [0, \cdots, d-1])$，その他の要素が全て 0 である演算子を $\hat{e}_j^k \coloneqq |j\rangle\langle k|$ とする．この $\hat{e}_j^k$ を用いて，次の 3 つの演算子を定義する．

$$\hat{\Theta}_j^k \coloneqq \hat{e}_j^k + \hat{e}_k^j \tag{4.10}$$

$$\hat{\Xi}_j^k \coloneqq -i(\hat{e}_j^k - \hat{e}_k^j) \tag{4.11}$$

$$\hat{\Upsilon}_r^r \coloneqq \sqrt{\frac{2}{r(r+1)}} \left[\sum_{j=0}^{r-1} \hat{e}_j^j - r\hat{e}_r^r \right] \tag{4.12}$$

ただし，$0 \leq j < k \leq d-1$，および $0 < r \leq d-1$ である．例えば，$d = 3$ の場合，$\hat{\Theta}_j^k$

および $\hat{\Xi}_j^k$ は下記の演算子となる．

$$\hat{\Theta}_0^1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \hat{\Theta}_0^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \qquad \hat{\Theta}_1^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \tag{4.13}$$

$$\hat{\Xi}_0^1 = \begin{pmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \hat{\Xi}_0^2 = \begin{pmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{pmatrix}, \qquad \hat{\Xi}_1^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{pmatrix} \tag{4.14}$$

式 (4.13), (4.14) を，それぞれ $\hat{\sigma}_x, \hat{\sigma}_y$ の行列表現である式 (4.2), (4.3) と比較すれば，そのインデックスの行と列のみを抽出した小行列が同一であり，その他の成分は 0 の行列であることが分かる．すなわち，$\hat{\Theta}_j^k$ および $\hat{\Xi}_j^k$ は，$|j\rangle, |k\rangle$ により形成される 2 次元部分空間において，それぞれ $\hat{\sigma}_x, \hat{\sigma}_y$ に対応する演算子となっている．一方，$d = 3$ の場合の $\hat{\Upsilon}_r^r$ は，次式のように表される．

$$\hat{\Upsilon}_1^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \hat{\Upsilon}_2^2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix} \tag{4.15}$$

式 (4.4) の $\hat{\sigma}_z$ の行列表現と比較すれば，$\hat{\Upsilon}_1^1$ の左上 2×2 の小行列が $\hat{\sigma}_z$ に等しいことが分かる．また，$\hat{\Upsilon}_2^2$ についても，トレースレスな対角行列という $\hat{\sigma}_z$ と同じ特徴を持っている．すなわち，$\hat{\Upsilon}_r^r$ は $\hat{\sigma}_z$ の d 次元系への拡張とみなす事ができる．一般化 Gell–Mann 演算子 $\hat{G}_i$ とは，上記演算子 $\hat{\Theta}_j^k, \hat{\Xi}_j^k, \hat{\Upsilon}_r^r$ に恒等演算子 $\hat{\mathbb{1}}$ を加えたものである．なお，本論文においては $\hat{G}_i$ のインデックス i の順序は重要ではないため，$\hat{G}_0 = \hat{\mathbb{1}}$ となることのみ定めておく．

上記一般化 Gell–Mann 演算子 $\hat{G}_i$ を用いると，d 次元量子状態の密度演算子 $\hat{\rho}$ が次のように表される．

$$\hat{\rho} = \sum_{i=0}^{d^2-1} g_i \hat{G}_i \tag{4.16}$$

ただし，g_i は実数パラメータであり，確率の総和の $\mathrm{Tr}(\hat{\rho}) = 1$ から $g_0 = 1/d$ である．

ここで，状態密度演算子が $\hat{\rho}$ である光子を N 個用意し，射影測定演算子 $\hat{P}_j$ で表される測定を各光子に対して行うことを考える．この時の検出光子数の期待値 n_j^E は次式で与えられる．

$$n_j^E = N \,\mathrm{Tr}\left(\hat{P}_j \hat{\rho}\right) = N \sum_{i=0}^{d^2-1} A_{ij} g_i \tag{4.17}$$

ただし，$A_{ij} \coloneqq \mathrm{Tr}\left(\hat{P}_j \hat{G}_i\right)$ とした．式 (4.17) は，射影測定 $\hat{P}_j$ を行った時の検出光子数 n_j^E と，式 (4.16) の展開係数 g_i を関係付ける線形方程式となっている．したがって，任意の g_i を求めるためには，A_{ij} を i 行 j 列目の要素とする行列のランクが，g_i の自由度，す

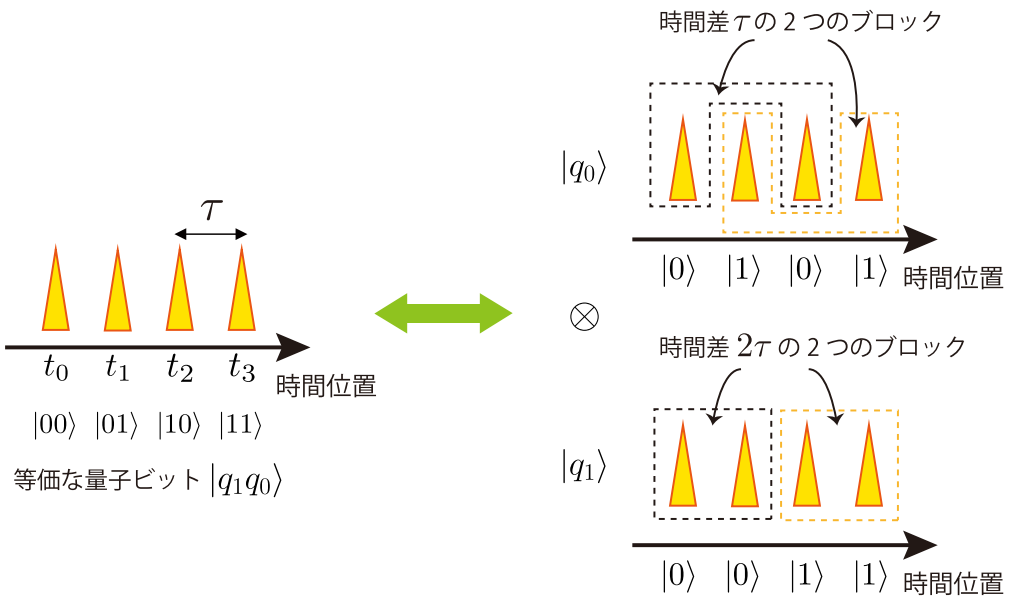

図 4.2　4 次元タイムビン量子状態の等価な量子ビット表現

なわち $d^2 - 1$ である必要がある．さらに，実際の実験の際には，検出光子数の合計 N も測定することになる．そこで，改めて Ng_i を QST で推定すべきパラメータと考えれば，QST が実行可能である条件は，A_{ij} を要素とする行列のランクが d^2 となることである．

上記条件を満たす測定演算子 $\hat{P}_j$ を考えるには，2^K 次元タイムビン量子状態を，K 個の等価な 2 次元量子状態で表現するアプローチが有効である．具体例として，4 次元タイムビン量子状態，すなわち $K = 2$ の場合について考える (図 4.2)．この場合の時間位置基底状態を $|0\rangle, |1\rangle, |2\rangle, |3\rangle$ とする．各状態 $|i\rangle$ のインデックス i を 2 桁のビット $q_1 q_0$ を用いて表すと，各時間位置基底状態は 2 つの量子ビットからなる状態，$|00\rangle, |01\rangle, |10\rangle, |11\rangle$ として表現できる (図 4.2 左側)．このような等価な表現は，量子コンピュータ上で整数値を複数量子ビットによって表現する際など，量子情報分野でしばしば用いられる [1]．ここで，q_0 が表す量子ビットに着目すると，図 4.2 右上に示すように，黒の点線で囲んだ時間位置 $\{t_0, t_2\}$ が $|0\rangle$ を，黄色の点線で囲んだ時間位置 $\{t_1, t_3\}$ が $|1\rangle$ をそれぞれ表している．この 2 つのブロックは点線で囲んだ構造が等しくかつ時間差が τ となっている．したがって，q_0 が表す等価な量子ビットは，物理的にはブロック間の時間差 τ を持つ 2 次元タイムビン量子状態と言える．同様に，図 4.2 右下に示すように，q_1 が表す等価な量子ビットは，物理的にはブロック構造の時間差 2τ を持つ 2 次元タイムビン量子状態である．

前節で述べたように，2 次元タイムビン量子状態への QST は，遅延時間がタイムビン量子状態の時間差に等しい MZI により実装可能である．さらに，二つの量子ビットからなる全系の状態密度演算子に対する QST は，各量子ビットに対する QST 測定の組み合わせで実装できることが知られている [95]．2 次元タイムビン量子状態の QST に必要な

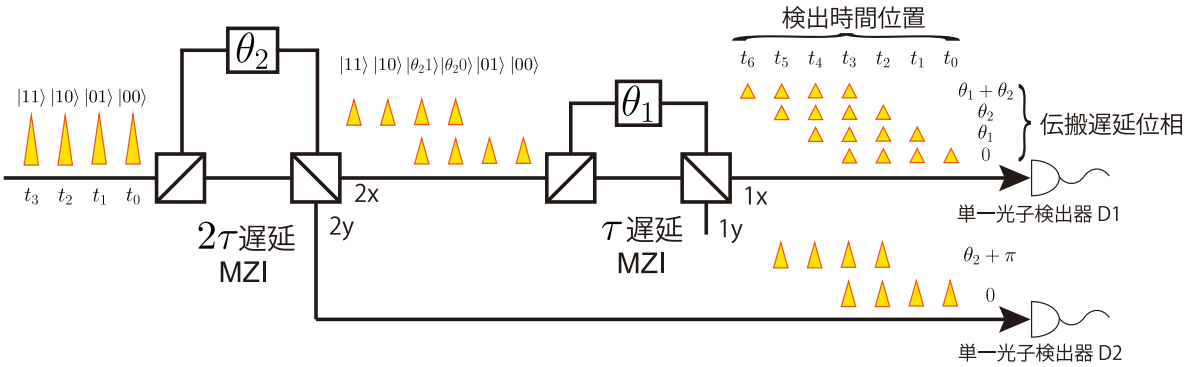

図 4.3　多段接続 MZI を用いた 4 次元タイムビン量子状態の QST

測定は，$\{|0\rangle, |1\rangle, |+\rangle, |L\rangle\}$ の 4 状態への射影測定であった．これらの組み合わせとしては，例えば，$|00\rangle, |01\rangle$ や $|0+\rangle, |0L\rangle, |++\rangle$ などの状態への射影測定が考えられる．

このような測定系実装としては，3.4.1 節でも述べた多段接続 MZI が有効である．図 4.3 に，4 次元タイムビン量子状態に対する QST 測定系の構成を示す．ただし，3.4.1 節で示した構成とは MZI の順序が入れ替わっているが，QST の実行可能性について本質的に差異はない．ここでは，後述する測定の効率化を目的として 2τ 遅延 MZI を前段に配置している．

4 次元タイムビン量子状態を，遅延時間 2τ かつ伝搬位相差が θ_2 の MZI に入力すると，その出力端では入力パルスが 2 タイムスロット分ずれて重なり合うため，6 つのタイムスロットに光子が存在しうる．このうち，中心の 2 つのタイムスロットでは干渉が起こる一方，その他のタイムスロットでは干渉が生じない．q_1 と等価な量子ビット (図 4.2 右下) に着目すると，最初の 2 パルスでの光子検出が $|0\rangle$ への射影測定，最後の 2 パルスでの光子検出が $|1\rangle$ への射影測定，そして中心の 2 パルスでの光子検出が $|\theta_2\rangle$ の射影測定に対応している．これは，前節で述べた 2 次元タイムビン量子状態の QST 測定と同様であり，2τ 遅延 MZI 透過過程は q_1 で表される量子ビットへの QST 測定と等価とみなすことができる．

この 2τ 遅延 MZI 出力を τ 遅延 MZI に入力する．τ 遅延 MZI 透過過程は q_0 で表される量子ビットへの QST 測定に対応すると考えられ，その出力ポートにおける各タイムスロットでの光子検出確率を求めることで，2 つの量子ビット全体，すなわち高次元タイムビン量子状態全体の QST が可能となる．ここで，各 MZI の伝搬遅延位相 θ_2, θ_1 は，それぞれ 0 もしくは $\pi/2$ とすればよい．すなわち，4 つの測定パラメータ設定により QST が実装される．

ただし，上記測定系による QST の説明は，2 次元測定系の原理による直感的なものであり，提案手法は先述の $|00\rangle, |01\rangle$ や $|0+\rangle, |0L\rangle, |++\rangle$ などへの射影測定による QST で

はない．例えば，入力時の時間位置が t_1 にあるパルスからは，後段 MZI 出力タイムスロット $t_1, \cdots, t_4$ のいずれかで光子が検出されるが，これらでは全て他のパルスと干渉している (図 4.3)．そのため，MZI の伝搬遅延位相を変化させるだけでは，$|01\rangle$ への射影測定を行うことはできない．したがって，上記測定系が真に QST を実装可能かどうかを検証する必要がある．

QST の可否を決める条件は，式 (4.17) に現れる A_{ij} を要素とした行列のランクが d^2 か否かであった．そこで，2 段 MZI 構成で実行可能な全ての POVM 要素を求め，A_{ij} のランクを調べることにより，上記提案測定系で QST が可能かどうかを判定する．本測定系による全ての POVM 要素は次のように求められる．第 2 章および第 3 章で述べた通り，図 4.3 の 2τ 遅延 MZI の出力ポート $2x$ への透過を表す測定演算子は次式で与えられる．

$$\hat{M}_{2x} = \frac{1}{2}\sum_{k=0}^{3}\left(|k\rangle + e^{i\theta_2}|k+2\rangle\right)\langle k| \tag{4.18}$$

同様に，τ 遅延 MZI の出力ポート $1x$ への透過を表す測定演算子は次式となる．

$$\hat{M}_{1x} = \frac{1}{2}\sum_{k=0}^{5}\left(|k\rangle + e^{i\theta_1}|k+1\rangle\right)\langle k| \tag{4.19}$$

後段の τ 遅延 MZI 出力ポートでは，7 つの時間位置で光子を検出し得る．時間スロット $t_l (l \in [0,6])$ での光子検出は時間位置基底状態 $|l\rangle$ への射影測定となっており，その測定演算子は $\hat{M}_{D1} = |l\rangle\langle l|$ で与えられる．したがって，2τ 遅延 MZI および τ 遅延 MZI の遅延位相をそれぞれ θ_2, θ_1 とすると，時間位置 t_l で光子を検出する場合の，量子測定演算子 $\hat{M}^{D1}_{l\theta_1\theta_2}$ および対応する POVM 要素 $\hat{E}^{D1}_{l\theta_1\theta_2}$ は，次式で表される．

$$\hat{M}^{D1}_{l\theta_1\theta_2} = \hat{M}_{D1}\hat{M}_{1x}\hat{M}_{2x} \tag{4.20}$$

$$\hat{E}^{D1}_{l\theta_1\theta_2} = (\hat{M}^{D1}_{l\theta_1\theta_2})^{\dagger}\hat{M}^{D1}_{l\theta_1\theta_2} \tag{4.21}$$

ここで，$\hat{M}_{D1}$ はランク 1 の射影測定演算子なので，$\hat{E}^{D1}_{l\theta_1\theta_2}$ も何らかの純粋量子状態への射影を表す，ランク 1 の射影測定演算子を定数倍した演算子となる．表 4.1 上段に，各検出時間位置の $\hat{M}^{D1}_{l\theta_1\theta_2}$ を示す．表には，図 4.3 中の検出時間位置および伝搬遅延位相との対応関係が分かりやすいように，インデントを挿入してある．

状態密度演算子が $\hat{\rho}$ である光子に対して，ここで想定している条件の測定を N 回繰り返す時の検出光子数の期待値 $n^{D1}_{l\theta_1\theta_2}$ は，次式で与えられる．

$$n^{D1}_{l\theta_1\theta_2} = N\,\mathrm{Tr}\left(\hat{E}^{D1}_{l\theta_1\theta_2}\hat{\rho}\right) \tag{4.22}$$

式 (4.22) と式 (4.17) を比較すると，$\hat{E}^{D1}_{l\theta_1\theta_2}$ に適切な順序でインデックスを与えなおし，$\hat{P}_j$ と対応付けることで，行列のランク評価による QST 実行の可否を評価できることが分かる．

表 4.1　光子検出器および光子検出の時間位置毎の量子測定演算子

光子検出器	検出時間位置	量子測定演算子 $\hat{M}^{DX}_{l\theta_1\theta_2}$
D1	t_0	$\frac{1}{4}\left\|0\right\rangle\left\langle 0\right\|$
	t_1	$\frac{1}{4}\left\|1\right\rangle(\left\langle 1\right\|+e^{i\theta_1}\left\langle 0\right\|$)
	t_2	$\frac{1}{4}\left\|2\right\rangle(\left\langle 2\right\|+e^{i\theta_1}\left\langle 1\right\|+e^{i\theta_2}\left\langle 0\right\|$)
	t_3	$\frac{1}{4}\left\|3\right\rangle(\left\langle 3\right\|+e^{i\theta_1}\left\langle 2\right\|+e^{i\theta_2}\left\langle 1\right\|+e^{i(\theta_1+\theta_2)}\left\langle 0\right\|)$
	t_4	$\frac{1}{4}\left\|4\right\rangle($ $e^{i\theta_1}\left\langle 3\right\|+e^{i\theta_2}\left\langle 2\right\|+e^{i(\theta_1+\theta_2)}\left\langle 1\right\|)$
	t_5	$\frac{1}{4}\left\|5\right\rangle($ $e^{i\theta_2}\left\langle 3\right\|+e^{i(\theta_1+\theta_2)}\left\langle 2\right\|)$
	t_6	$\frac{1}{4}\left\|6\right\rangle($ $e^{i(\theta_1+\theta_2)}\left\langle 3\right\|)$
D2	t_0	$-\frac{1}{2}\left\|0\right\rangle\left\langle 0\right\|$
	t_1	$-\frac{1}{2}\left\|1\right\rangle\left\langle 1\right\|$
	t_2	$-\frac{1}{2}\left\|2\right\rangle(\left\langle 2\right\|$ $-e^{i\theta_2}\left\langle 0\right\|$)
	t_3	$-\frac{1}{2}\left\|3\right\rangle(\left\langle 3\right\|$ $-e^{i\theta_2}\left\langle 1\right\|$)
	t_4	$-\frac{1}{2}\left\|4\right\rangle($ $-e^{i\theta_2}\left\langle 2\right\|$)
	t_5	$-\frac{1}{2}\left\|5\right\rangle($ $-e^{i\theta_2}\left\langle 3\right\|$)

上記のランク評価により，各 MZI の位相 θ_1, θ_2 をそれぞれ $0, \pi/2$ とした時の後段 MZI 出力ポートでの全ての光子検出事象を用いることで，QST が可能であることが確認できる．さらに，その他の出力ポートでの光子検出事象を用いると，より多くの情報を得ることができる．上記と同様の手順により，図 4.3 の光子検出器 $D2$ での測定演算子が，表 4.1 下段のように表される．光子検出器 $D2$ での光子検出は，光子検出器 D1 のみの構成で検出されない分の光子損失を回避するとともに，光子検出器 $D1$ とは異なる測定演算子となるため，得られる情報量の増加をもたらす．MZI の順序が異なる場合でも得られる情報量は増加するが，1 段目の MZI の遅延時間を 2τ とする方が多くの種類の測定演算子を実装できるため，測定の効率化が期待できる．さらに，τ 遅延 MZI のもう一つのポート $1y$ での光子検出を利用すると得られる情報量をさらに増やすことができるが，本論文の実験では用意できる光子検出器数と検出効率の制限から，図 4.3 の構成を用いている．

先に述べたように，高次元タイムビン量子状態に対する QST としては，特定の二つの時間位置基底状態 $\left|i\right\rangle, \left|j\right\rangle$ を取り出し，それぞれを直線偏波状態に変換する測定法が報告されている [49]．この手法では，2 次元の偏波状態への射影測定を行うため，一度に実装可能な測定演算子は 2 個であり，全体の QST のためには設定パラメータを多数組み合わせた測定を行う必要がある．また，本提案構成に類似の多段干渉計を用いて，時間エネルギー不確定性に基づく量子もつれ状態に対する QST を行った報告例がある [97]．しかしながら，そこでは，前述の等価量子ビット上の $\{\left|0\right\rangle, \left|1\right\rangle, \left|+\right\rangle, \left|L\right\rangle\}$ の組み合わせに相当す

る測定を正確に実装するために，特定の組み合わせにおいて干渉計の片側のパスをブロックしている．また，時間エネルギー不確定性に基づく量子もつれ状態の場合，検出時刻の相対時間によって状態が定義されるため，その他の検出時刻における光子検出を利用することができず，多数の測定パラメータを必要とする．これに対し，本提案手法は，単一の測定パラメータにおける複数の時間位置での光子検出を用いており，解析は複雑であるものの，$\log_2 d$ 個の MZI と d 個の測定パラメータという簡便なセットアップにより QST が実装できる．このことは，効率の良い測定が要求される長距離伝送された量子状態の QST として，大きな利点となる．

4.2.3 MZI 経路毎の伝搬損失の補正

前節で述べた多段 MZI の測定演算子は，デバイスが理想的である時のものであり，現実の測定系の測定演算子として，さらに理想状態からの差分を取り込むことが可能である．本研究の測定系では PLC 干渉計を用いるが，この場合，干渉計内のビームスプリッタの分岐比誤差や，2 経路の伝搬損失差が装置の不完全性として避けられない．また，光子検出効率が検出器ごとに異なり，これは実効的に光子損失の不均一性となる．これらの光子損失の差は，干渉時の重ね合わせの重み付けで補正することにより測定演算子に取り込むことができる．これらの補正を加えた演算子は次のように表される．

$$\hat{M}_{2x} = \frac{\sum_{k=0}^{3}\left(|k\rangle + \sqrt{\Delta\eta_{2x}}e^{i\theta_2}|k+2\rangle\right)\langle k|}{\sqrt{2\left(1+\Delta\eta_{2x}\right)}} \tag{4.23}$$

$$\hat{M}_{2y} = \frac{\sum_{k=0}^{3}\left(-|k\rangle + \sqrt{\Delta\eta_{2y}}e^{i\theta_2}|k+2\rangle\right)\langle k|}{\sqrt{2\left(1+\Delta\eta_{2y}\right)}} \tag{4.24}$$

$$\hat{M}_{1x} = \frac{\sum_{k=0}^{5}\left(|k\rangle + \sqrt{\Delta\eta_{1x}}e^{i\theta_1}|k+1\rangle\right)\langle k|}{\sqrt{2\left(1+\Delta\eta_{1x}\right)}} \tag{4.25}$$

$$\hat{E}^{D1}_{l\theta_1\theta_2} = \Delta\eta_1\hat{M}^{\dagger}_{2x}\hat{M}^{\dagger}_{1x}\hat{M}^{\dagger}_{D1}\hat{M}_{D1}\hat{M}_{1x}\hat{M}_{2x} \tag{4.26}$$

$$\hat{E}^{D2}_{l\theta_1\theta_2} = \hat{M}^{\dagger}_{2y}\hat{M}^{\dagger}_{D2}\hat{M}_{D2}\hat{M}_{2y} \tag{4.27}$$

ここで，$\Delta\eta_{2x}, \Delta\eta_{2y}, \Delta\eta_{1x}$ は，対応するインデックスの出力ポートから観測したときの，MZI の分岐光路に依存した相対的な透過率，$\Delta\eta_1$ は検出器 $D1, D2$ の検出効率を損失に換算したときの比を表す．なお，この補正を加えた場合，光子損失により光子検出確率の合計が 1 にならないため，厳密にはこれらの演算子の集合を POVM とみなすことはできない．ただし，QST で必要な情報は相対的な検出割合であるため，精度改善のために補正を行った演算子を用いることができる．

4.2.4　最尤推定法による演算子の正定値化

前節までに述べた QST は，式 (4.17) の線形方程式を解くことで，測定結果から密度演算子を求める手法である．原理的にはこれにより密度演算子を求めることが可能であるが，前節で述べた以外の実装上の誤差やノイズ，観測光子数の統計的な誤差などの要因により，得られた密度演算子はしばしば不正確なものとなる．特に重要な課題として，得られた密度演算子が非物理的な演算子となることが知られている．すなわち，密度演算子は本来半正定値であり，全ての固有値が非負であるはずのところを，推定した密度演算子が負の固有値を持ってしまうことがある．QST を用いる理由は，推定した演算子を用いて様々な物理量や情報量を見積もるためであるが，負の固有値をもつ演算子では，これらが正しく評価できない．例えば，第 2 章で述べた von Neumann エントロピーは，固有値を確率とみなした時の Shannon エントロピーとなるため，固有値が負であると確率が負ということになり，エントロピーは計算不可能である．

この問題を解決するために，密度演算子が必ず正定値演算子となるようにパラメータ化した上で，最尤推定法を用いてパラメータを求める手法が通常用いられる [56, 90, 95, 97]．ある行列 R が正定値エルミート行列であることと，三角行列 T およびそのエルミート共役 $T^\dagger$ を用いたコレスキー分解 $R = TT^\dagger$ が存在することは，等価である．なお，コレスキー分解は T を下三角行列とした分解であるが，正定値性の観点では上三角行列としても本質的には変わらない．逆に，このように分解した T の各要素をパラメータとすれば，R は常に正定値エルミート行列となる．そこで，式 (2.19) 中の r_{ij} を要素とする $d \times d$ エルミート行列を，三角行列によってパラメータ化して，密度演算子が必ず正定値演算子となるようにする．具体的には，まず，三角行列 T に対応する演算子 $\hat{T}$ を用いて，密度演算子 $\hat{\rho}$ および，測定系への入射光子数 N を次式のように表す．

$$\hat{\rho} = \frac{\hat{T}\hat{T}^\dagger}{\mathrm{Tr}\left(\hat{T}\hat{T}^\dagger\right)} \tag{4.28}$$

$$N = \mathrm{Tr}\left(\hat{T}\hat{T}^\dagger\right) \tag{4.29}$$

次に，パラメータ推定に最尤推定法を適用するために，演算子 $\hat{T}$ が与えられたときの，測定光子数の確率分布を求める．式 (4.17), (4.22), (4.28) および (4.29) から求まる，j 番目の測定での検出光子数の期待値を n_j^E，対応する測定結果を n_j^M とする．一般に光子検出数はポアソン分布に従うと考えられる．これをガウス分布で近似すると，期待値 $\{n_j^E\}$

が与えられた時，検出光子数 $\{n_j^M\}$ を得る確率が次式で表される．

$$\Pr\left(\{n_j^M\};\{n_j^E\}\right) = \prod_j \frac{1}{\sqrt{2\pi n_j^E}} \exp\left[-\frac{\left(n_j^M - n_j^E\right)^2}{2n_j^E}\right] \tag{4.30}$$

したがって，最尤推定を行うには，次式で与えられる対数尤度関数 L を最小化するような $\hat{T}$ を数値計算によって求めればよい．

$$L\left(\hat{T}\right) = \sum_j \left[\frac{\left(n_j^M - n_j^E\right)^2}{n_j^E} + \ln n_j^E\right] \tag{4.31}$$

ただし，上式を得るには，対数を取った後，符号は反転した上で余分な定数を除去している．

式 (4.31) を最小化する $\hat{T}$ を用いて尤もらしい密度演算子 $\hat{\rho}$ を再構成することができる．ただし，その計算に必要な n_j^E などは，単純に式 (4.17), (4.22) の対応関係のみを用いると，重複した結果を含む．例えば，光子検出器 D1 が時間位置 t_0 で光子検出する事象は，MZI の相対位相の設定に関わらず，常に $|0\rangle$ への射影測定に対応する (図 4.3)．したがって，これらの結果は一つの結果としてまとめたうえで，最尤推定に用いる必要がある．そこで，次の条件を満たすような，検出器のラベル $DX \in \{D1, D2\}$，光子検出の時間位置 l，MZI の相対位相 θ_1, θ_2 の組を要素とする集合 V_j を導入する．

$$\begin{aligned}
&{}^{\forall}(DX, l, \theta_1, \theta_2) \in V_j \ , \ {}^{\forall}(DX', l', \theta_1', \theta_2') \in V_{j'} \\
&\frac{\hat{E}^{DX}_{l\theta_1\theta_2}}{\mathrm{Tr}\left(\hat{E}^{DX}_{l\theta_1\theta_2}\right)} = \frac{\hat{E}^{DX'}_{l'\theta_1'\theta_2'}}{\mathrm{Tr}\left(\hat{E}^{DX'}_{l'\theta_1'\theta_2'}\right)} \qquad \text{for} \qquad j = j' \qquad (4.32) \\
&\frac{\hat{E}^{DX}_{l\theta_1\theta_2}}{\mathrm{Tr}\left(\hat{E}^{DX}_{l\theta_1\theta_2}\right)} \neq \frac{\hat{E}^{DX'}_{l'\theta_1'\theta_2'}}{\mathrm{Tr}\left(\hat{E}^{DX'}_{l'\theta_1'\theta_2'}\right)} \qquad \text{for} \qquad j \neq j' \qquad (4.33)
\end{aligned}$$

上記の条件を満たす集合 V_j を総当たりによる条件評価によって構成することで，冗長性を除去した $n_j^E, \hat{E}_j$ が，次のように得られる．

$$n_j^E = \sum_{(DX,l,\theta_1,\theta_2)\in V_j} n^E_{DXl\theta_1\theta_2} = N\,\mathrm{Tr}\left(\hat{E}_j\hat{\rho}\right) \tag{4.34}$$

$$\hat{E}_j = \sum_{(DX,l,\theta_1,\theta_2)\in V_j} \hat{E}^{DX}_{l\theta_1\theta_2} \tag{4.35}$$

測定結果 n_j^M も同様にして得られる．このように測定結果をまとめたのち，式 (4.31) の最小化による最尤推定によって，正定値性が保証された密度演算子 $\hat{\rho}$ を再構成する．

4.3　量子もつれ状態の評価指標

前節で述べた高次元量子状態に対する QST によって得られるのは密度演算子であり，量子状態の定量的な評価には，得られた密度演算子から目的にあった指標を見積もる必要がある．本節では，いくつかの評価指標とその意味について述べる．

4.3.1　フィデリティ

フィデリティ [1, 78] は，二つの状態密度演算子 $\hat{\rho}$ と $\hat{\sigma}$ の近さを表す指標であり，次式で定義される．

$$F(\hat{\rho},\hat{\sigma}) \coloneqq \left[\mathrm{Tr}\sqrt{\sqrt{\hat{\sigma}}\hat{\rho}\sqrt{\hat{\sigma}}}\right]^2 \tag{4.36}$$

ただし，$\sqrt{\hat{\sigma}}$ は，演算子 $\hat{\sigma}$ の各固有状態について，対応する固有値の平方根を取る操作を表す．フィデリティは $0 \leq F(\hat{\rho},\hat{\sigma}) \leq 1$ を満たし，$\hat{\rho} = \hat{\sigma}$ の時，かつその時に限り $F(\hat{\rho},\hat{\sigma}) = 1$ となる．また，$\hat{\rho},\hat{\sigma}$ それぞれの台 (各演算子の固有状態のうち，非ゼロの固有値を持つ固有状態によって形成される部分空間) が，互いに直交する時，かつその時に限り $F(\hat{\rho},\hat{\sigma}) = 0$ となる．したがって，1 に近いほど二つの状態は類似しており，0 に近いほど二つの状態は異なっていると言える．特に，一方の量子状態が $\hat{\sigma} = |\psi\rangle\langle\psi|$ の純粋量子状態である場合，$F(\hat{\rho},\hat{\sigma}) = \langle\psi|\,\hat{\rho}\,|\psi\rangle$ であり，これは $\hat{\rho}$ を $\hat{\sigma}$ へ射影測定したときの測定確率を意味する．このことは，フィデリティ F が，ある量子状態 $\hat{\rho}$ を別の量子状態 $\hat{\sigma}$ として射影測定した時の測定確率を一般化したものとみなせることを示唆している．なお，2 乗を用いる式 (4.36) に代わり，$F(\hat{\rho},\hat{\sigma}) \coloneqq \mathrm{Tr}\sqrt{\sqrt{\hat{\sigma}}\hat{\rho}\sqrt{\hat{\sigma}}}$ とする流儀も広く用いられているが，本論文では測定確率としてより直感的な解釈に近い式 (4.36) を採用する．$\hat{\rho}$ を QST によって再構成した被観測状態の密度演算子，$\hat{\sigma}$ を理想的な量子もつれ状態 (例えば $|\Psi_{\mathrm{MES}}\rangle$[式 (2.52)]) とすれば，フィデリティが 1 に近いほど，理想的な量子もつれ状態が観測できたと言える．

4.3.2 トレース距離

トレース距離 [1, 78] は，二つの状態密度演算子 $\hat{\rho}$ と $\hat{\sigma}$ の間の距離を表す指標であり，次式で定義される．

$$\begin{aligned} D(\hat{\rho},\hat{\sigma}) &\coloneqq \frac{1}{2}\operatorname{Tr}|\hat{\rho}-\hat{\sigma}| \\ &= \frac{1}{2}\operatorname{Tr}\sqrt{(\hat{\rho}-\hat{\sigma})^{\dagger}(\hat{\rho}-\hat{\sigma})} \\ &= \frac{1}{2}\operatorname{Tr}\sqrt{(\hat{\rho}-\hat{\sigma})^{2}} \end{aligned} \tag{4.37}$$

トレース距離は $0 \leq D(\hat{\rho},\hat{\sigma}) \leq 1$ を満たし，$\hat{\rho}=\hat{\sigma}$ の時，かつその時に限り，$D(\hat{\rho},\hat{\sigma})=0$ となる．また，$\hat{\rho},\hat{\sigma}$ それぞれの台が互いに直交する時，かつその時に限り，$D(\hat{\rho},\hat{\sigma})=1$ となる．したがって，トレース距離が 0 に近いほど二つの状態は類似しており，1 に近いほど二つの状態は異なっていると言える．なお，トレース距離の定義として係数 $1/2$ の規格化を行わない流儀もしばしば用いられるが，本論文ではより直感的な式 (4.37) を採用する．トレース距離は，三角不等式などの距離に関する公理を満たし，理論上扱いやすいため，量子情報分野で広く用いられている．

トレース距離には次のような操作論的な解釈が与えられている．量子状態 $\hat{\rho}$ あるいは $\hat{\sigma}$ がそれぞれ確率 $1/2$ で与えられた時に，どちらの状態であるのかを 2 値の測定結果によって判定することを考える．この時，正しく識別する確率 p_{succ} の最大値は次式となることが知られている (Helstrom 限界)[78].

$$\max\, p_{succ} = \frac{1}{2}\{1 + D(\hat{\rho},\hat{\sigma})\} \tag{4.38}$$

上式より，トレース距離は，二つの量子状態 $\hat{\rho},\hat{\sigma}$ を識別する時の，ランダム推定 (確率 $1/2$) からの増分と考えることができる．$p_{succ}=1/2$ ということは，2 状態が全く区別できないことを意味する．したがって，$\hat{\rho}$ を QST によって再構成した被測定状態の密度演算子，$\hat{\sigma}$ を理想的な量子もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$[式 (2.52)] とすれば，トレース距離が 0 に近いほど，理想的な量子もつれ状態を観測できたと言える．

4.3.3 リニアエントロピー

リニアエントロピー [95] は，量子状態のランダムさを表す指標であり，次式で定義される．

$$S_{lin} \coloneqq 1 - \operatorname{Tr}\left(\hat{\rho}^{2}\right) \tag{4.39}$$

この値は，量子状態が純粋状態であるときに 0 となり，完全混合状態の時に最大値 $(d-1)/d$ となる．したがって，リニアエントロピーが小さいほど純粋状態に近く，ノイ

ズなどの影響が小さい状態であると言える．なお，値域が $[0,1]$ となるように規格化した $\frac{d}{d-1}\left\{1-\mathrm{Tr}\left(\hat{\rho}^2\right)\right\}$ が用いられることもあるが，ここではピュリティ [78] として知られる量である $\mathrm{Tr}\left(\hat{\rho}^2\right)$ との対応が分かりやすい式 (4.39) を採用する．$\hat{\rho}$ を QST によって再構成した被測定状態の密度演算子とすれば，リニアエントロピーが小さいほど，より純粋な量子もつれ状態を観測できたと言える．

4.3.4　von Neumann エントロピー

2 章で述べたように，von Neumann エントロピー [1, 78] は量子状態のランダムさを表す指標であり，式 (2.20) で定義される．

$$S(\hat{\rho}) \coloneqq -\mathrm{Tr}(\hat{\rho}\log_2\hat{\rho}) \tag{2.20}$$

$\hat{\rho}$ の固有値を確率分布とみなすと，式 (2.20) は固有値の Shannon エントロピーに一致する．したがって，d 次元量子状態については，$0 \leq S(\hat{\rho}) \leq \log_2 d$ が成り立っており，$S(\hat{\rho}) = 0$ は純粋量子状態，$S(\hat{\rho}) = \log_2 d$ は最大混合状態であることを意味する．$\hat{\rho}$ を QST によって再構成した被測定状態の密度演算子とすれば，von Neumann エントロピーが小さいほど，より純粋に近い量子もつれ状態を観測できたと言える．

4.3.5　条件付きエントロピーおよびコヒーレント情報量

条件付きエントロピー [1, 78] は，二つの光子 AB に関するエントロピーであり，次式で定義される．

$$S(\hat{\rho}_{AB} \mid \hat{\rho}_X) \coloneqq S(\hat{\rho}_{AB}) - S(\hat{\rho}_X) \tag{4.40}$$

ただし，$X \in \{A, B\}$ である．式 (4.40) は，古典的な確率分布に対する条件付きエントロピーを状態密度演算子に拡張したものであり，古典的な条件付きエントロピーが満たす多くの性質が成り立つ．ただし，大きな違いとして，古典的な条件付きエントロピーは常に非負であるのに対し，量子状態に対する条件付きエントロピーは負の値を取りうる．例えば，純粋 d 次元最大量子もつれ状態 $\hat{\rho}_{AB} = |\Psi_{\mathrm{MES}}\rangle\langle\Psi_{\mathrm{MES}}|$ を光子 B で条件付けしたときの条件付きエントロピーは，

$$\begin{aligned} S(\hat{\rho}_{AB} \mid \hat{\rho}_B) &= S(\hat{\rho}_{AB}) - S(\hat{\rho}_B) \\ &= S(|\Psi_{\mathrm{MES}}\rangle\langle\Psi_{\mathrm{MES}}|) - S\left(\frac{1}{d}\hat{\mathbb{1}}_B\right) \\ &= 0 - \log_2 d \\ &= -\log_2 d \end{aligned} \tag{4.41}$$

となり，最大量子もつれ状態に対しては負の値となる．なお，条件付きエントロピーが負の値を取るのは，二つの光子がもつれている時のみであることが知られている [98, 99].

したがって，条件付きエントロピーにより観測した状態が量子もつれ状態であるか否かが判定できる．さらに，光子 A の次元を d_A とした時，

$$|S(\hat{\rho}_{AB} \mid \hat{\rho}_B)| \leq \log_2 d_A \tag{4.42}$$

が成り立つ [78]．光子 A で条件づける場合も同様である．上式は，2 次元量子状態では -1 bit より小さな条件付きエントロピーは得られないことを示唆している．したがって，-1 bit より小さな条件付きエントロピーは，高次元量子もつれ状態 ($d > 2$) であることを意味する．

このように，負の条件付きエントロピーは量子もつれ状態と密接な関係があるだけでなく，いくつかの量子通信プロトコルにおいて重要な指標となるため，コヒーレント情報量 [1, 78, 100] としても知られている．光子 A から光子 B へのコヒーレント情報量は，次式で定義される．

$$I(A\rangle B) \coloneqq S(\hat{\rho}_B) - S(\hat{\rho}_{AB}) \tag{4.43}$$

なお，同様によく用いられる相互情報量 $I(A;B) \coloneqq S(\hat{\rho}_A) + S(\hat{\rho}_B) - S(\hat{\rho}_{AB})$ と異なり，A, B について一般に非対称な情報量であり，この意味で向きがある．特に，QKD において，Alice と Bob が $\hat{\rho}_{AB}$ で記述される 2 光子対を共有している時，秘密鍵生成率 $r = I(A\rangle B)$ を満たすプロトコルが原理的に存在することが知られている [100]．例えば，最大量子もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$ を分極解消チャネルに通した後の状態を $\hat{\rho}_{AB}$ とすると，第 5 章で述べる $(d+1)$ 測定基底プロトコルは，この鍵生成率を満たす [42]．したがって，$\hat{\rho}_{AB}$ を QST で推定した被測定状態の密度演算子とすれば，コヒーレント情報量が大きいほど，より高い QKD 鍵生成率を達成する量子もつれ状態を共有できたと言える．

4.4 量子状態トモグラフィーの実装実験

前節までに述べた，高次元タイムビン量子状態に対する QST 実装法を実験により検証した．本節では，その実験系および得られた結果について述べる．

4.4.1 実験系

本節では，高次元タイムビン量子もつれ状態に対する QST 実装の実験系について述べる．図 4.4 に実験系を示す．第 3 章の実験と同様に，波長 1551.1 nm の CW レーザ光を強度変調器 (IM) を用いて，パルス幅 100 ps/パルス間隔 1 ns の 4 連パルスを，繰り返し周波数 125 MHz で生成する．本実験では第 3 章とは異なり，各パルスの強度が等しい最大量子もつれ状態のみを生成するため，強度変調器は一段構成としている．この 4 連パルスを EDFA により増幅したのち，2 段接続 PPLN 導波路に入力し，第二次高調波発生

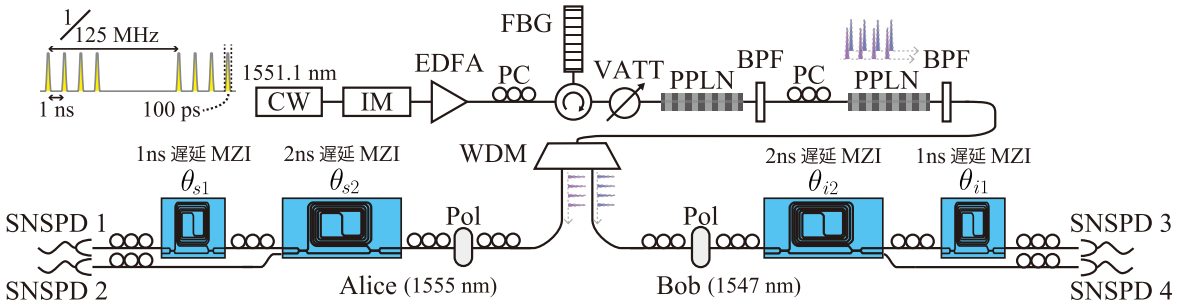

図 4.4　実験系．CW laser: CW レーザ光源，IM: 光強度変調器，EDFA: エルビウム添加光ファイバ増幅器，PC: 偏波コントローラ，FBG: ファイバブラッググレーティングフィルタ，VATT: 可変光減衰器，PPLN: 周期的分極反転ニオブ酸リチウム，BPF: 光バンドパスフィルタ，WDM: 波長分離フィルタ，Pol: 偏光子，遅延 MZI: 遅延 Mach-Zehnder 干渉計，SNSPD: 超伝導ナノワイヤ単一光子検出器

によるポンプ光生成およびそれに続く SPDC により，4 次元タイムビン量子もつれ状態を生成する．PPLN 出力光から中心波長 1555 nm および 1547 nm のシグナル光子およびアイドラー光子を波長分離フィルタ (WDM) によって抜き出し，それぞれを Alice と Bob へ送信する．Alice/Bob は，偏波コントローラ (PC) と偏光子 (Pol) を用いて偏波状態を調整したのち，各光子を多段接続された PLC-MZI に入力する．各 MZI の 2 経路の伝搬位相差をそれぞれ 0 もしくは $\pi/2$ に設定することにより，4.2.2 節で述べた高次元タイムビン量子状態の QST 測定系を実装する．各 MZI の一方の出力ポートからのパルス列が，検出効率を最大化するように偏波状態が調整されたのち，SNSPD へ入力される．SNSPD の検出効率は SNSPD1, 2, 3, 4 について，それぞれ 40%, 56%, 34%, 43%, ダークカウントはいずれも <30 cps であった．

4.4.2　実験結果

本節では，前節の実験系による実験結果について述べる．

4.2.3 節で述べたように，正確な QST のためには MZI の経路毎の伝搬損失およびビームスプリッタ分岐比を補正する必要がある．そこでまず，相対的な透過率を測定した．MZI 内で干渉が起きないように，時間間隔を空けたパルス列を，MZI へ入力したときの出力光を光子検出した．図 4.5 に，各光子検出器の光子検出数を示す．図 4.5(a) および (c) の 4 つのピークが，それぞれ時間位置 t_0〜t_3 での光子検出に対応し，図 4.5(b) および (d) の 2 つのピークが，それぞれ時間位置 t_0 および t_2 での光子検出に対応する．これらの光子検出結果から，MZI 経路の相対的な透過率を求めることができる．例えば，

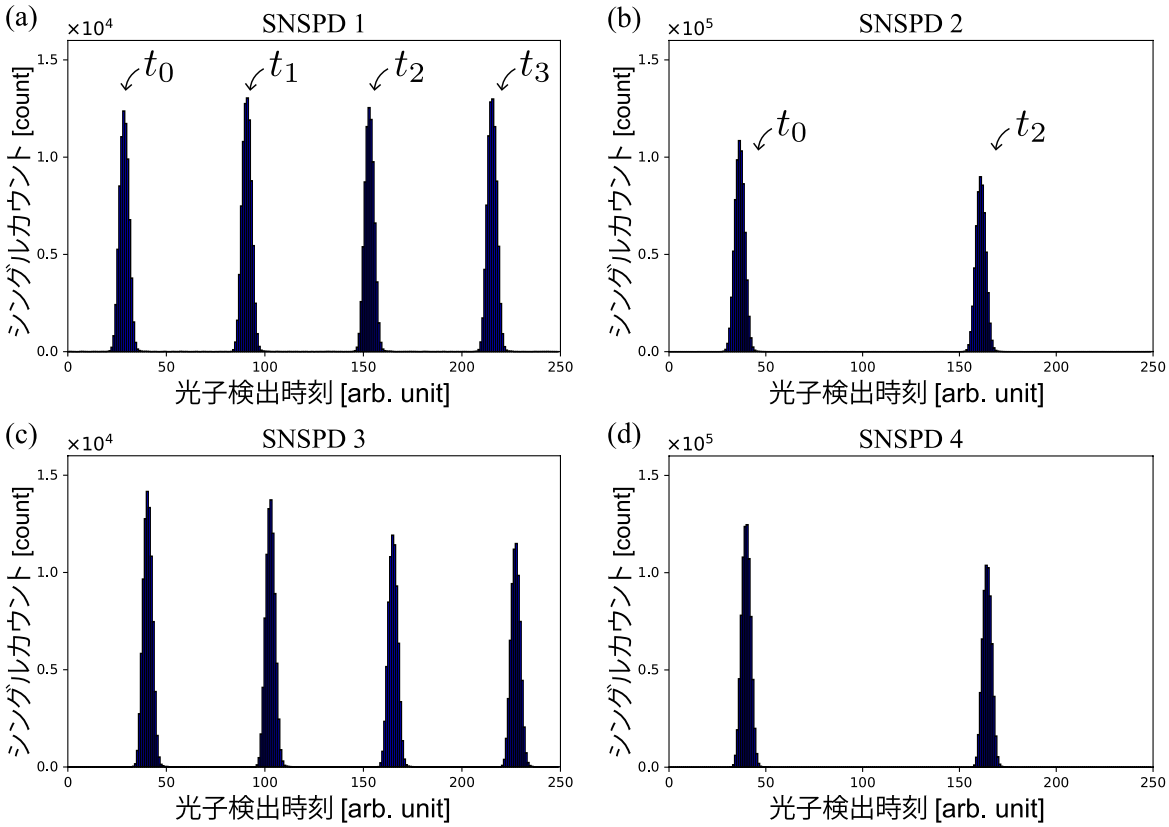

図 4.5　単一パルスのポンプから生成した光子対に対する各光子検出器におけるシングルカウントのヒストグラム．測定時間は 30 秒．(a) SNSPD 1, (b) SNSPD 2, (c) SNSPD 3, (d) SNSPD 4

SNSPD 1 における時間位置 t_l での光子検出数 S_l^1 は，次の関係を満たす．

$$S_0^1 : S_1^1 : S_2^1 : S_3^1 = 1 : \Delta\eta_{1x} : \Delta\eta_{2x} : \Delta\eta_{1x}\Delta\eta_{2x} \tag{4.44}$$

ただし，$\Delta\eta_{2x}$ および $\Delta\eta_{1x}$ は，用いた MZI の各経路の相対的な透過率である (図 4.3 の各 MZI 出力ポートのインデックスおよび式 (4.23)–(4.25) を参照)．上式より，各相対透過率を，$\Delta\eta_{2x} = \left(S_2^1 + S_3^1\right) / \left(S_0^1 + S_1^1\right)$ および $\Delta\eta_{1x} = \left(S_1^1 + S_3^1\right) / \left(S_0^1 + S_2^1\right)$ として求めることができる．他の相対透過率についても同様に求めた結果を表 4.2 に示す．以下の QST では，この相対的な透過率を取り込んでいる．

次に，ポンプ光を 4 連パルス列として 4 次元タイムビン量子もつれ状態を生成した．なお，本実験では，MZI の位相の設定は可変 CW 光源を用いて行った．そのため，可変 CW 光源ともつれ光子の周波数差による位相誤差が観測結果に重畳されるため，測定され

表 4.2　MZI 各経路の相対透過率

	シグナル光	アイドラー光
$\Delta\eta_{2x}$	1.009	0.8495
$\Delta\eta_{2y}$	0.8300	0.8302
$\Delta\eta_{1x}$	1.063	0.9669

る状態は次式で表される最大量子もつれ状態となる．

$$\left|\Psi^4_{\mathrm{MES}}(\phi)\right\rangle = \frac{1}{2}\sum_{k=0}^{3}\exp(i\phi k)\left|kk\right\rangle \tag{4.45}$$

ただし，ϕ は隣接 2 パルスの相対位相である．この量子もつれ状態に対して，前節の実験系による測定を行った．この時，SNSPD1, 2, 3, 4 でのシングルカウントレートは，それぞれ 17.1, 72.4, 20.6, 82.1 kcps であった．このカウントレートから，式 (4.26) 中の各検出器の相対透過率 $\Delta\eta_1$ は，シグナル光，アイドラー光それぞれに対して 0.474 および 0.501 と見積もられた．また，4 連パルス当たりの平均光子ペア数は 0.02 であった．MZI 位相の設定値の各組合せについて 10 秒間の同時計数を測定し，その結果を用いて QST を行った．図 4.6 に，QST によって推定した密度演算子を示す．ただし，式 (4.45) の位相を考慮し，シグナル光子に対する位相回転ユニタリー演算子 $\hat{U} = \sum_k \exp(-i\phi' k)\left|k\right\rangle\!\left\langle k\right|$ を用いて，$\left|\Psi^4_{\mathrm{MES}}(0)\right\rangle$ に近くなるようにした $\hat{U}\hat{\rho}\hat{U}^\dagger$ を図示している．理想的な 4 次元量子もつれ状態の場合，

$$\hat{\rho}_{AB} = \left|\Psi^4_{\mathrm{MES}}(0)\right\rangle\!\left\langle\Psi^4_{\mathrm{MES}}(0)\right| = \sum_{ij}\frac{1}{4}\left|ii\right\rangle\!\left\langle jj\right| \tag{4.46}$$

であり，$|ii\rangle\langle jj|$ 成分のみが 1/4 の大きさを持ち，その他の要素および虚部の値は全て 0 となる．図 4.6 では，このような理想的な最大量子もつれ状態に見られる，等間隔のくし状構造の密度演算子が観測されている．

さらに，より定量的に評価するため，4.3 節で述べた各種指標を，QST により得られた密度演算子から見積もった．表 4.3 に，15 回の QST における各指標の平均値および標準偏差を示す．ただし，$\hat{\sigma}_{AB} = \left|\Psi^4_{\mathrm{MES}}(\phi)\right\rangle\!\left\langle\Psi^4_{\mathrm{MES}}(\phi)\right|$ とし，位相 ϕ はフィデリティとトレース距離をそれぞれ最大化，最小化するように最適化した．表には，3.4.2 節で用いた，CGLMP 不等式の破れを観測するための干渉縞明瞭度の閾値と同様の手順により計算した，分極解消チャネルの仮定のもとで CGLMP 不等式を破る各指標の閾値を併記している．高いフィデリティ，および小さなトレース距離から，理想的な最大量子もつれ状態に近い状態が観測できていることが分かる．また，低いリニアエントロピーおよび von Neumann エントロピーから，ノイズが小さく純粋状態に近い量子状態が観測できたこと

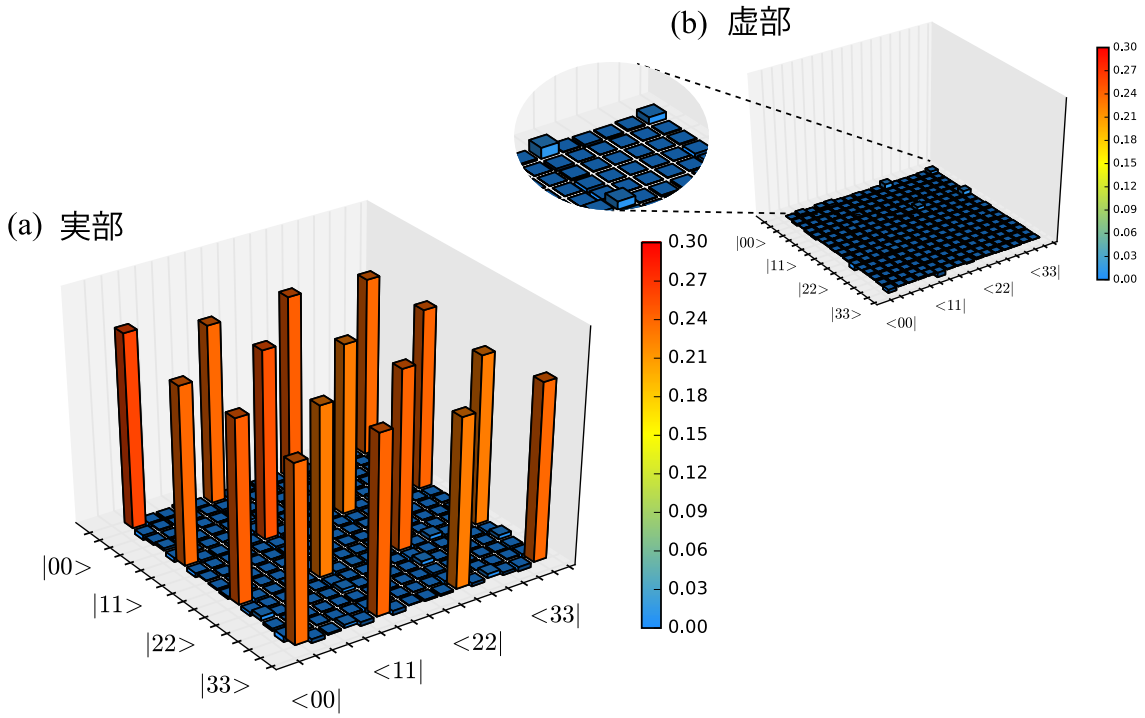

図 4.6　再構成した密度演算子 $\hat{\rho}_{AB}$ の (a) 実部および (b) 虚部

表 4.3　15 回の QST によって得られた密度演算子 $\hat{\rho}$ から得られた各種指標，および分極解消チャネルの仮定のもとで CGLMP 不等式を破るための閾値.

	測定値	閾値
フィデリティ	$F(\hat{\rho}_{AB}, \hat{\sigma}_{AB}) = 0.950 \pm 0.003$	> 0.710
トレース距離	$D(\hat{\rho}_{AB}, \hat{\sigma}_{AB}) = 0.068 \pm 0.003$	< 0.290
リニアエントロピー	$S_{lin}(\hat{\rho}_{AB}) = 0.093 \pm 0.006$	< 0.490
von Neuman エントロピー	$S(\hat{\rho}_{AB}) = 0.343 \pm 0.016$	< 2.002
条件付きエントロピー	$\begin{cases} S(\hat{\rho}_{AB}\|\hat{\rho}_A) = -1.654 \pm 0.016 \\ S(\hat{\rho}_{AB}\|\hat{\rho}_B) = -1.653 \pm 0.016 \end{cases}$	< 0.002

もうかがえる．さらに，2 つの条件付きエントロピーはどちらも-1 ビット以下の値を示しており，高次元量子もつれ状態が観測されたことも示されている．以上の結果より，提案した測定系による QST の原理実証に成功したと言える．

4.5　高次元量子もつれ状態の伝送実験

前節で原理実証した QST 測定法を用いて，4 次元タイムビン量子もつれ状態の 100 km 伝送特性を検証した．本節では，その実験系および実験結果について述べる．

4.5.1　実験系

図 4.7 に実験系を示す．前節と同様に，波長 1551.1 nm の CW レーザ光を強度変調して，パルス幅 100 ps/パルス間隔 1 ns の 4 連パルスを繰り返し周波数 125 MHz で生成し，2 段接続した PPLN 導波路中の二次高調波生成 (SHG) および SPDC により，4 次元タイムビン量子もつれ状態を生成する．波長分離フィルタ (WDM) によって波長 1555 nm および 1547 nm の光子を抜き出したのち，各光子をそれぞれ長さ 50 km の分散シフトファイバ (DSF) を通して伝送した．本実験では，ファイバ分散により隣接パルスが重なることを避けるため，DSF を用いている．DSF 50 km の伝搬損失は，シグナル光とアイドラー光それぞれについて，11.8 dB および 11.2 dB であった．

DSF 伝送後，各光子は Alice/Bob の受信系に入力される．ここで，受信系で用いた MZI および SNSPD には偏波依存性があるため，入力偏波状態を調節する必要がある．前節の QST 原理実証実験では測定時間が十分短いため，この調節は手動の偏波コントロー

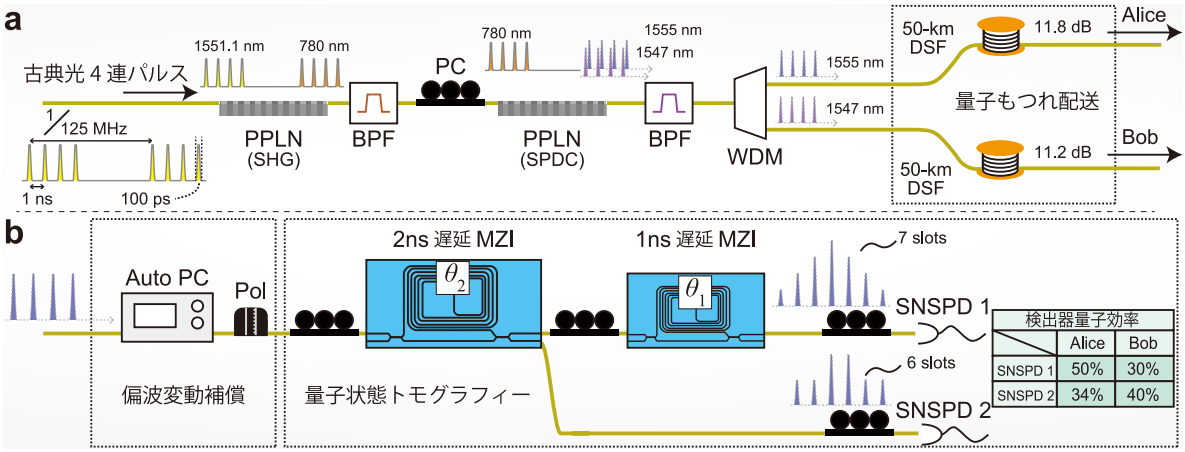

図 4.7　実験系．(a) 4 次元タイムビン量子もつれ状態の生成および伝送系．(b)Alice と Bob それぞれの測定系．挿入図に本実験での SNSPD の量子効率を示す．PPLN: 周期的分極反転ニオブ酸リチウム，BPF: 光バンドパスフィルタ，PC: 偏波コントローラ，WDM: 波長分離フィルタ，DSF: 分散シフトファイバ，Auto PC: リモート制御型偏波コントローラ，Pol: 偏光子，遅延 MZI: 遅延 Mach-Zehnder 干渉計，SNSPD: 超伝導ナノワイヤ単一光子検出器

ラで十分であったが，本実験では伝搬による光子損失を補うため測定時間が長く，DSF 伝搬による偏波回転が時間的に変動するため，これに追従して偏波状態を調節する必要がある．そこで，ここでは自動制御型偏波コントローラを用いた．この偏波コントローラは 4 段構成のファイバベースの偏波回転部からなり，奇数段目がポアンカレ球上で斜め直線偏波軸周りの回転，偶数段目が水平/垂直偏波軸周りの回転を与える．この各段の回転角の値を $\pm 0.1\pi$ rad の範囲で 0.01π rad ずつ変化させ，SNSPD の検出光子数が最大となるように制御する．偏波制御後の光子を，2 段に接続した MZI および SNSPD を用いて測定し，前節と同様にして QST を行った．

4.5.2　実験結果

本節では，4 次元タイムビン量子もつれ状態の 100 km 伝送実験の結果について述べる．

前節で述べたように，本実験では測定の長時間化に伴う偏波変動を逐次補償しているが，その他の変動として，温度変動に伴うファイバ長・屈折率の変化等のために，光子の到着時刻に揺らぎがある．この変動に追従するため，データ解析の際に，光子検出数のヒストグラムと相互相関関数を用いて，タイムスロットを決定した．SNSPD で検出されるのは MZI 通過後の光子であるため，一般には干渉パターンが観測される．しかしながら，シグナル光子/アイドラー光子それぞれの状態は最大混合状態であるため，量子もつれ状態は同時計数においてのみ干渉特性を示し，単独の光子検出については干渉特性は示さない．したがって，単独光子検出数のヒストグラムは MZI の位相の設定によらず，各タイムスロットの検出数比は MZI の各径路のパワー分岐比のみによって決まる．そこで，次式の相互相関関数 $g(\tau)$ が最大となる τ を求めることで，タイムスロットの位置を検出することができる．

$$g(\tau) = \int_0^{8T} h_i(t - \tau \bmod 8T) h_m(t) dt \tag{4.47}$$

ただし，$h_i(t)$ および $h_m(t)$ はそれぞれ，理想的な光子検出数の基準ヒストグラムと実際に測定されたヒストグラム，T はパルス間隔である．また，基準ヒストグラムは，SNSPD 1 に対しては $h_i(t) = \sum_{l=0}^{3} \sum_{k=0}^{3} \delta(t - kT - lT)$，SNSPD 2 に対しては $h_i(t) = \sum_{l=0}^{1} \sum_{k=0}^{3} \delta(t - kT - 2lT)$，とした．ただし，$\delta(t)$ は Dirac のデルタ関数である．

図 4.8 に，Alice の SNSPD 2 におけるタイムスロットのトラッキング結果を示す．横軸は TIA での光子検出時刻，縦軸は光子検出数であり，長時間測定の間のデータを一定の時刻ごとに縦にずらしてプロットしている．また，式 (4.47) の相互相関関数によって推定したタイムスロットの中心を元に，幅 0.33 ns のタイムウィンドウを橙色の破線で示す．図に示されているように，QST 1 回分にあたる 4 時間の測定の間に，タイムスロッ

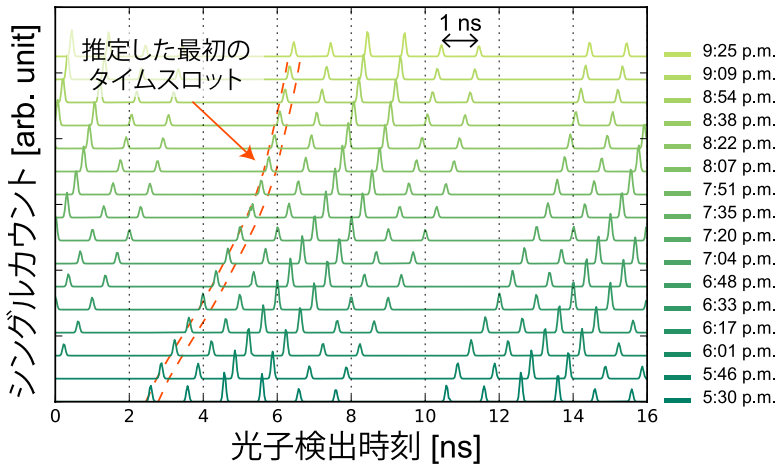

図 4.8　Alice の SNSPD 2 におけるタイムスロットのトラッキング結果．長時間測定中の各時刻における，1 分間のシングルカウントのヒストグラムを一定の間隔でずらしてプロットしている．

トが 4 ns と大きくシフトしているが，上記の手法で正確に追従できている．このタイムスロットを自動的に追従させて解析した同時計数をもとに，QST を行った．なお，TIA で記録される時刻は，TIA の同期用チャネルへの電気信号を基準とした相対的な時刻である．本実験では，同期用チャネルへの電気信号は，同じ実験室内の送信系用パルスジェネレータからの信号に同期させているが，この同期信号を別途光信号に変換し送信することで，実際の長距離通信においてもこの手法は有効である [29]．あるいは，波長分割多重技術を利用して，同一のファイバでもつれ光子対と同期信号を伝送することにより，上記タイムスロット推定を簡略化あるいは高精度化することも可能である．

100 km 伝送後の 4 次元タイムビン量子もつれ状態に対する QST を連続して 4 回行った．各 MZI の設定値毎の測定時間は 15 分であり，QST 1 回分の測定時間は 4 時間であった．この時の，4 連パルス当たりの送信平均光子ペア数は 0.03，Alice(Bob) の SNSPD 1 および 2 での光子検出レートはそれぞれ 3.3 および 7.7 (2.9 および 12) kcps であった．この光子検出レートの比から，各検出器間の相対的な透過率 $\Delta\eta_1$ は，シグナル光，アイドラー光それぞれに対して，0.8507 および 0.4812 と推定された．一方，$\Delta\eta_{2x}$ など，その他の相対透過率は SNSPD 等に依存せず，MZI の特性によって決まるため，前節の実験結果である表 4.2 の値を用いた．これらの値と同時計数を元に，QST により 2 光子の密度演算子 $\hat{\rho}_{AB}$ を推定した．

図 4.9 に，QST によって推定した密度演算子を示す．前節の実験と同様に，4 次元量子もつれ状態特有のくし状の密度演算子が得られている．また，この QST によって得られた密度演算子 $\hat{\rho}_{AB}$ から，量子もつれ状態の品質を示す各種指標を見積もった．表 4.4 に，

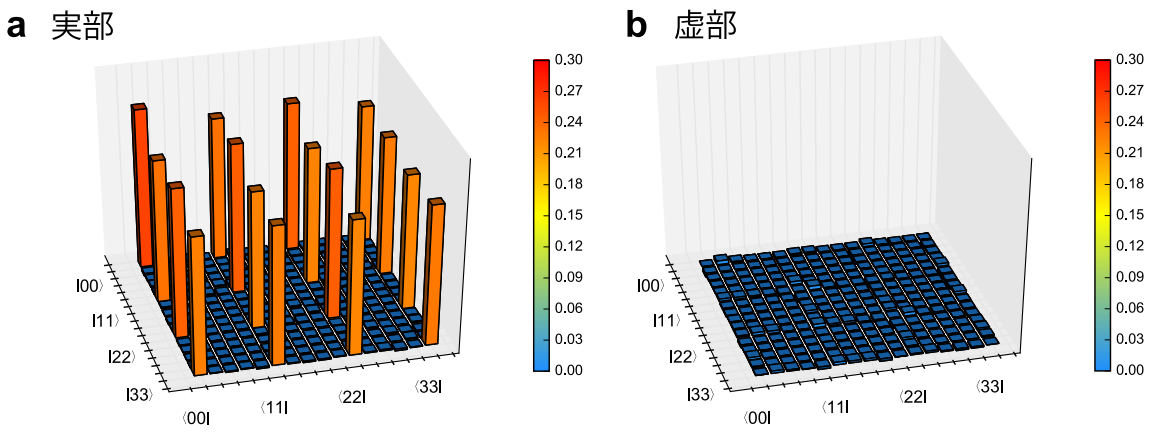

図 4.9　再構成した密度演算子 $\hat{\rho}_{AB}$ の (a) 実部および (b) 虚部．ただし，4 回の QST の結果を平均したものを示している．

表 4.4　100 km 伝送後の QST によって得られた密度演算子 $\hat{\rho}_{AB}$ から得られた各種指標．

フィデリティ	$F(\hat{\rho}_{AB}, \hat{\sigma}_{AB}) =$	0.935 ± 0.015
トレース距離	$D(\hat{\rho}_{AB}, \hat{\sigma}_{AB}) =$	0.081 ± 0.019
リニアエントロピー	$S_{lin}(\hat{\rho}_{AB}) =$	0.121 ± 0.026
von Neumann エントロピー	$S(\hat{\rho}_{AB}) =$	0.437 ± 0.063
条件付きエントロピー	$S(\hat{\rho}_{AB}\|\hat{\rho}_A) =$	-1.557 ± 0.067
	$S(\hat{\rho}_{AB}\|\hat{\rho}_B) =$	-1.557 ± 0.066

4 回の QST から得られた各指標の平均値，および標準偏差を示す．前節と同様に，100 km 伝送後においても高品質な 4 次元タイムビン量子もつれ状態が観測されていることが分かる．特に，-1.557 ビットという条件付きエントロピーの値は，伝送後でも確かに高次元のもつれ状態が保たれていることを示している．また，4.3.5 節で述べた通り，負の条件付きエントロピーであるコヒーレント情報量は，その情報量に等しい秘密鍵生成率を達成する QKD プロトコルの存在を示唆する．したがって，何らかの適切なプロトコルを用いると，この伝送後の量子もつれ状態から，光子対検出イベント当たり 1.557 ビットの秘密鍵を生成することができる．

以上の結果から，高次元 QKD に利用可能な高品質な高次元量子もつれ状態の 100 km 伝送に初めて成功したと言える．

4.6　結言

本章では，高次元タイムビン量子もつれ状態に対する QST を用いたもつれ状態の長距離伝送について述べた．長距離伝送においては，光ファイバ伝送中の伝搬損失によって光子が失われるため，統計的物理量を得る測定に長時間を要する．そこで，既存の 2 次元タイムビン量子状態に対するコンパクトな QST を基礎として，少数の干渉計と測定パラメータによる現実的な時間で測定可能な高次元タイムビン量子状態に対する QST を提案した．また，QST によって得られる状態密度演算子から定量的な品質評価を行うための，各種評価指標について述べた．その後，第 3 章の手法により生成した 4 次元タイムビン量子もつれ状態に対して，提案した QST の原理実証実験を行った．QST により推定した密度演算子から条件付きエントロピーなど，各種評価指標を見積もり，高品質な 4 次元タイムビン量子もつれ状態生成を確認するとともに，提案した QST の有効性を示した．さらに，100 km 光ファイバ伝送後の 4 次元タイムビン量子もつれ状態に対して同様の QST を行い，伝送後の量子もつれ状態の品質を評価した．推定した密度演算子から見積もられたコヒーレント情報量は 1.557 ビットであり，2 次元量子もつれ状態では不可能である光子対当たり 1 ビット以上の秘密鍵生成を可能とする高品質な 4 次元量子もつれ状態が，100 km 伝送後でも保たれることを実証した．

第 5 章

$(d+1)$ 測定基底 QKD プロトコルのための相互不偏基底測定

5.1 緒言

本論文ではここまで，高次元 QKD への応用を目的とした，高次元タイムビン量子もつれ状態の生成と伝送について述べてきた．本章では，高次元 QKD プロトコルの安全性証明の詳細と，QKD 実装に必要となる相互不偏基底 (MUB: Mutually unbiased bases) の，タイムビン量子状態に対する実装法について述べる．まず 5.2 節にて，d 次元量子状態を用いた，$(d+1)$ 測定基底 QKD プロトコルについて述べる．次に 5.3 節にて，上記プロトコルの安全性証明に必要となる，有限体を用いた一般化 Weyl 演算子および一般化ベル基底 [101] を導入し，これらを用いて既存の安全性証明 [42] の適用可能範囲を，素数次元から素数の累乗次元へと拡張する．また，2 測定基底 QKD プロトコルの安全性証明についても触れ，2 種類のプロトコルの違いである，エラーの相関特性の見積もりに関して議論する．

上記プロトコルの実装にあたっては，各基底状態への射影測定系を少ない装置数で効率的に構成することが望まれる．そこで 5.4 節では，安全性証明に利用した MUB[101] と等価な別の MUB の表現 [102] が持つ構造を利用し，p^N 次元タイムビン量子状態に対して，1 個の位相変調器，$\log_p d$ 個の干渉計，$(p+1)$ 個の単一光子検出器を構成要素とする，$(d+1)$ 個の MUB の基底状態への射影測定法を提案する．そして 5.5 節および 5.6 節にて，上記提案手法を 4 次元タイムビン量子状態に対して実装し，その有用性を実験的に検証する．

5.2 $(d+1)$ 測定基底 QKD プロトコル

本節では，$(d+1)$ 測定基底 QKD プロトコルについて述べる．

2.4 節で述べたように，BB84/BBM92 では二つの正規直交基底を測定基底として用いるが，これらの基底は相互不偏基底 (MUB)[101, 102] と呼ばれる基底となっている．今，$\mathcal{B}_0, \mathcal{B}_1$ を d 次元ヒルベルト空間の二つの正規直交基底とする．各基底から選んだ 2 状態 $^\forall |\psi_0\rangle \in \mathcal{B}_0, ^\forall |\psi_1\rangle \in \mathcal{B}_1$ に対して，

$$|\langle\psi_0|\psi_1\rangle|^2 = 1/d \tag{5.1}$$

が成り立つとき，二つの基底 $\mathcal{B}_0, \mathcal{B}_1$ は相互不偏であるという．言い換えれば，ある基底の基底状態を別の基底の基底状態で射影測定した時，測定結果が一様ランダムであるような基底が MUB である．d 次元ヒルベルト空間においては，全て互いに相互不偏である基底が最大で $(d+1)$ 個存在する．2.2.1 節で述べたように，2 次元ヒルベルト空間では，時間位置基底および 2 つの位相基底は全て互いに相互不偏の条件を満たしており，上記の $(d+1)$ 個の MUB の例となっている (図 5.1)．この 3 つの MUB のうちの 2 つを利用することで BB84 や BBM92 のように安全な QKD プロトコルを実装できる．さらに，2.4 節で触れたように，この 3 つの基底に含まれる計 6 つの量子状態を用いた Six-state プロトコルは，BB84/BBM92 よりも高い鍵生成率を達成することができる．すなわち，より多くの基底を実装することで，鍵生成率を向上することが可能となる．

第 1 章で述べたように，高次元の量子状態を利用することで，光子あたりのエンコード可能な情報量を増加させ，QKD の鍵生成率を向上させることが可能である．d 次元 QKD

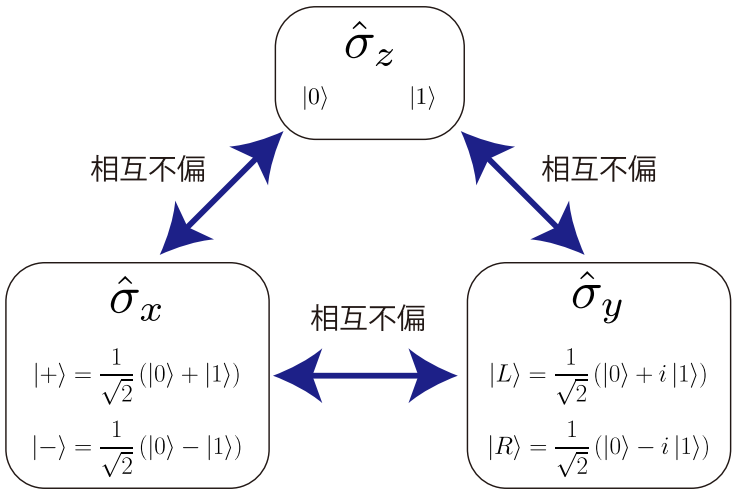

図 5.1 2 次元ヒルベルト空間での (2+1) 個の MUB の関係．各基底は Pauli 演算子 $\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z$ の固有状態である．

プロトコル **4** $(d+1)$ 測定基底 QKD プロトコル

1: Alice は 2 つの光子 AB を d 次元最大もつれ状態 $|\Psi_{\mathrm{MES}}\rangle$ として準備する．そして，一方の光子を伝送路を介して Bob に送る．この伝送路に対しては，あらゆる盗聴が可能であるとする．

2: Alice(Bob) は自身が保有している光子に対して，ランダムに $(d+1)$ 個の MUB の基底状態 (複素共役を取った基底状態) への射影測定を行う．

3: Alice と Bob は上記の送受信を繰り返した後，各測定に際してどの基底を用いて射影測定を行ったかを認証付き一般通信路を用いて通知しあう．そして，元々ペアであった 2 光子について，基底が異なる測定結果は破棄し，同じであった測定結果を残す．

4: Alice と Bob はベル基底状態にあった 2 光子から得られた測定結果のペアの一部をランダムに選んで通知しあい，各基底の測定結果の誤り分布ベクトル $\underline{q}_Z$ および $\underline{q}_r$(測定結果の差の確率分布) を推定する．誤り分布ベクトル推定に用いた測定結果は廃棄する．

5: 残った測定結果ついて，各基底内の状態のインデックスに応じた値を割り当て，多値の乱数列を生成する．これをシフト (sift) 鍵と呼ぶ．

6: 手順 4 で推定した誤り分布ベクトルをもとに，認証付き一般通信路を用いて Alice と Bob は情報を交換し，シフト鍵に対する誤り訂正を行う．これを訂正鍵という．

7: 先の誤り分布ベクトルから，盗聴者 Eve に漏洩し得る情報量の上限を推定し，訂正鍵に対して秘匿性増強と呼ばれる鍵の圧縮処理を施して，外部漏洩のない秘密鍵を得る．

においても，BB84/BBM92 の高次元拡張に当たる 2 測定基底 QKD と，Six-state プロトコルの高次元拡張に当たる $(d+1)$ 測定基底 QKD が存在し，このプロトコルではより多くの基底を用いるため，同じシンボルエラーレートで高い鍵生成率を達成可能である [41–44].

$(d+1)$ 測定基底 QKD プロトコルを，上記のプロトコル 4 に示す．以下，プロトコル 4 についていくつか補足する．

まず，次元 d は素数の累乗次元 $(d = p^N)$ であるとする．$(d+1)$ 個の MUB のうち，一つの基底を時間位置基底 $\mathcal{B}_Z = \left\{ \left| e_i^{(Z)} \right\rangle = |i\rangle \;\middle|\; i \in \{0, \cdots, d-1\} \right\}$ とし，その他 d 種類の基底を全て位相基底とする．また，$r \in \{0, \cdots, d-1\}$ 番目の位相基底を $\mathcal{B}_r = \left\{ \left| e_j^{(r)} \right\rangle = \sum_i H_{ij}^{(r)} |i\rangle \;\middle|\; j \in \{0, \cdots, d-1\} \right\}$ とする．具体的な確率振幅 $H_{ij}^{(r)}$ は次節で与える．また，$\left| e_j^{(r)*} \right\rangle = \sum_i H_{ij}^{(r)*} |i\rangle$ のように，時間位置基底で展開したうえで，その確率振幅の複素共役を取った状態を，複素共役を取った基底状態とする (これはエルミート共役とは異なる)．時間位置基底の確率振幅は常に 1 であるため，時間位置基底状態の複素共役を取った状態は，時間位置基底状態に等しい．

r 番目の位相基底における Alice の測定値は，$\left|e_a^{(r)}\right\rangle$ を測定した場合 a となる．Bob の測定値については，$\left|e_b^{(r)*}\right\rangle$ を測定した場合 b となる．時間位置基底についても同様である．これらの測定結果をもとに，r 番目の位相基底における誤り分布ベクトルが，次式で定義される．

$$\underline{q}_r = \{q_r^0, q_r^1, \cdots, q_r^{(d-1)}\} \tag{5.2}$$

$$q_r^t = \Pr\left(a \ominus b = t \mid r\right) \tag{5.3}$$

ただし，$\ominus$ は，a, b を有限体 $GF[p^N]$ 上の元とみなした時の，有限体上の減算を表す演算子であり，t はエラーを表す．時間位置基底についても同様に $\underline{q}_Z, q_Z^t$ を定義する．

このように，$(d+1)$ 個の MUB の基底状態への射影測定を実装し，そのエラーの分布から安全な鍵の長さを推定するプロトコルが $(d+1)$ 測定基底 QKD プロトコルである．なお，プロトコル 4 では，第 1 章および第 2 章で述べた，量子もつれ状態を準備する Entangledment-based(EB) 型のプロトコルとしているが，BBM92 と BB84 が対応するように，このプロトコルにおいても Prepare and Measure(P&M) 型のプロトコルを考えることができる．例えば，Alice が $|\Psi_{\mathrm{MES}}\rangle$ を測定した結果，自身の持つ光子が $\left|e_j^{(r)}\right\rangle$ であったとする．この条件の元で Bob へ送る量子状態 $|\psi_j\rangle_{B'}$ は，次式で与えられる．

$$\begin{aligned}
|\psi_j\rangle_{B'} &= \left\langle e_j^{(r)}\right|_A |\Psi_{\mathrm{MES}}\rangle_{AB'} \\
&= \left(\sum_i \langle i|_A H_{ij}^{(r)*}\right)\left(\frac{1}{\sqrt{d}}\sum_i |ii\rangle_{AB'}\right) \\
&= \frac{1}{\sqrt{d}}\sum_i H_{ij}^{(r)*}\,|i\rangle_{B'}
\end{aligned} \tag{5.4}$$

上記の状態 $|\psi_j\rangle_{B'}$ を規格化すると，$\left|e_j^{(r)*}\right\rangle_{B'}$ に等しいことが分かる．時間位置基底についても同様である．したがって，プロトコル 4 は，量子もつれ状態を準備する代わりに，状態 $\left|e_j^{(r)*}\right\rangle_{B'}$ をランダムに生成して Bob に送信し，Bob が複素共役を取った $(d+1)$ 個の MUB を用いて測定するプロトコルと等価である．また，Alice と Bob の用いる基底を入れ替えれば，複素共役を取らずに元の MUB を用いた P&M 型のプロトコルも，同じ安全性を持つことが分かる．

この $(d+1)$ 測定基底 QKD プロトコルの安全性証明は，これまで次元 d が素数の場合に限り示されている [42–44]．また，液晶空間位相変調器 (SLM：Spatial Light Modulator) により生成した光軌道角運動量 (OAM：Orbital Angular Momentum) 量子状態を用いたプロトコルの実装は報告されているものの [77]，タイムビン量子状態については SLM のようなフレキシブルな変調装置がなく，タイムビン量子状態に対する上記プロトコルのスケーラブルな実装法は知られていない．以降の節では，この安全性証明の素数の累乗次元への拡張およびタイムビン量子状態の場合のスケーラブルな実装手法について述べる．

5.3 $d = p^N$ についての安全性証明

5.3.1 有限体を用いた一般化 Weyl 演算子およびベル基底と MUB

本節では，$(d+1)$ 測定基底 QKD プロトコルの安全性証明の基となる，有限体を用いた Weyl 演算子および一般化ベル基底と，$(d+1)$ 個の MUB について述べる．

2.3.1 節で述べた通り，ベル基底は下記の 4 つの量子もつれ状態からなる，2 次元 2 光子状態が属するヒルベルト空間の基底である．

$$\left|\Psi^{00}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{AB} \tag{2.45}$$

$$\left|\Psi^{01}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)_{AB} \tag{2.47}$$

$$\left|\Psi^{10}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)_{AB} \tag{2.48}$$

$$\left|\Psi^{11}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)_{AB} \tag{2.49}$$

これらの状態は，光子 A もしくは B どちらかに対して，時間位置反転 ($|0\rangle$ と $|1\rangle$ の入れ替え)，位相反転 ($|+\rangle$ と $|-\rangle$ の入れ替え)，あるいはその両方を施すことで，他のベル基底状態に変換することができる．この状態変化は何らかのユニタリー変換を施すことによって実現される．4.2.1 節で述べた Pauli 演算子がこれらのユニタリー変換となっており，式 (4.2) および式 (4.4) から，$\hat{\sigma}_x$ が時間位置反転，$\hat{\sigma}_z$ が位相反転のユニタリー変換であることが分かる．これらを用いると，ベル基底状態を次のように表すことができる．

$$\left|\Psi^{ij}\right\rangle_{AB} = \left(\hat{\mathbb{1}} \otimes \hat{\sigma}_z^j \hat{\sigma}_x^i\right)\left|\Psi^{00}\right\rangle_{AB} \tag{5.5}$$

また，$\hat{\sigma}_z\hat{\sigma}_x = i\hat{\sigma}_y$ なので，グローバルな位相を無視すれば，4 つのベル基底状態は基準となる $\left|\Psi^{00}\right\rangle_{AB}$ およびそれに 3 つの Pauli 演算子のいずれかを乗じて得られた状態からなることが分かる (図 5.2)．一方，各 Pauli 演算子の固有状態からなる基底が，2 次元ヒルベルト空間の 3 つの MUB であった (図 5.1)．これらの関係から，3 つの MUB と QKD のエラーの間は，Pauli 演算子を介して関連していることが示唆される．Six-state プロトコルでは，この関係を利用して 3 つの MUB での測定結果から，時間位置反転エラーと位相反転エラーの結合確率分布を推定している．そこで，高次元 QKD への拡張にあたっては，Pauli 演算子の高次元化方法が手掛かりとなる．

4.2.2 節では，Pauli 演算子のエルミート性に着目した高次元化として，一般化 Gell–Mann 演算子を導入した．一方，Pauli 演算子のユニタリー性に着目した高次元化として，

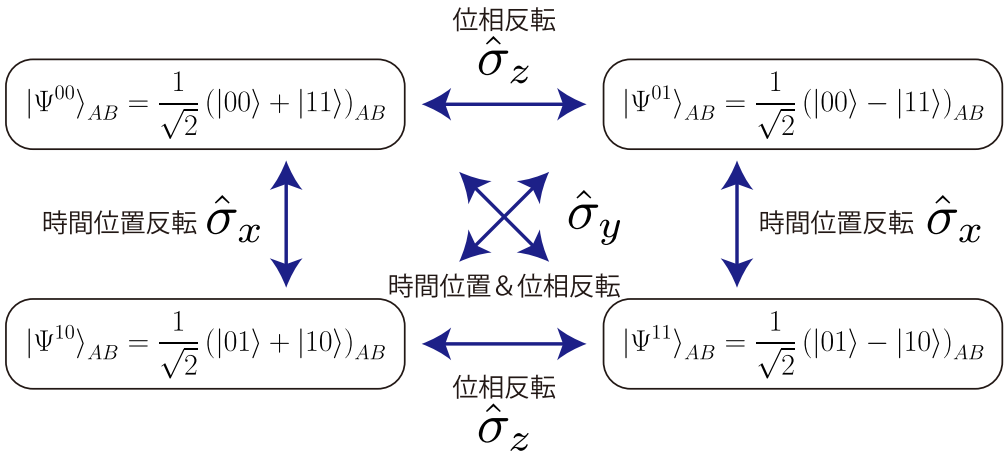

図 5.2 式 (5.5) で表される，ベル基底状態と Pauli 演算子による状態変化の関係

次の Weyl 演算子が知られている [42].

$$\hat{U}_{ij} = \sum_{k=0}^{d-1} \omega^{kj} \left|k + i \mod d\right\rangle \langle k| \tag{5.6}$$

ただし，$i, j \in \{0, \cdots, d-1\}$，$\omega$ は 1 の d 乗根，mod d は d で割った余りの算出を表す．$\hat{U}_{i0} = \sum_{k=0}^{d-1} |k + i \bmod d\rangle \langle k|$ は，時間位置基底状態に作用したときに状態を i シフトする演算子であるから，時間位置反転演算子 $\hat{\sigma}_x$ のユニタリーな高次元拡張である．また，$\hat{U}_{0j} = \sum_{k=0}^{d-1} \omega^{kj} |k\rangle \langle k|$ は，時間位置基底状態に作用したときに，状態のインデックスに比例して位相を $2\pi j/d$ シフトする演算子であるから，位相反転演算子 $\hat{\sigma}_z$ のユニタリーな高次元拡張である．$\hat{\sigma}_y$ が $\hat{\sigma}_x$ と $\hat{\sigma}_z$ の積で表せたように，その他の $\hat{U}_{ij}$ をこの二つの演算子の積によって表すことができる．

Pauli 演算子の固有状態が 3 つの MUB を成したのと同様に，次元 d が素数である時，Weyl 演算子の固有状態は $(d+1)$ 個の MUB を成す．ただし，$U_{00} = \hat{\mathbb{1}}$ を除き $\hat{U}_{ij}$ は (d^2-1) 種類存在するため，Pauli 演算子の場合とは異なり固有状態が重複し，(d^2-1) 種類の演算子のうち $(d-1)$ 種類が同一の固有状態を持つ．

この Weyl 演算子を用いると，d 次元に一般化したベル基底状態 $\left|\Psi^{ij}\right\rangle_{AB} = (\hat{U}_{ij} \otimes \hat{\mathbb{1}}) |\Psi_{\mathrm{MES}}\rangle_{AB}$ が定義できる．この状態は全て d 次元最大量子もつれ状態であり，d 次元 2 光子状態が属するヒルベルト空間の基底を成す．先行研究 [42] では，この Weyl 演算子によって一般化したベル基底状態を用いて，QKD プロトコルの安全性解析を行っている．上記で述べた通り，Weyl 演算子を用いた $(d+1)$ 個の MUB の構成方法は，素数次元についてのみ成り立つ．そのため，BB84 や BBM92 の拡張である 2 測定基底 QKD プロトコルの安全性解析は任意の d に対して成り立つ一方，$(d+1)$ 測定基底 QKD プロトコルの安全性解析は，MUB が構成できないため，素数次元以外では成り立たない．

しかしながら，有限体を利用して Weyl 演算子を拡張することにより，素数の累乗次元においても $(d+1)$ 個の MUB を構成することができる [101, 103]．例えば，d が素数 p と正整数 N により，$d = p^N$ と表されるものとする．このとき，有限体を用いた一般化 Weyl 演算子が次式で与えられる．

$$\hat{V}_{ij} = \sum_{k=0}^{d-1} \gamma^{(k\oplus i)\odot j} \left|k \oplus i\right\rangle \left\langle k\right| \tag{5.7}$$

ただし，γ は 1 の p 乗根，$\oplus, \odot$ はそれぞれ有限体上の加算および乗算を表す 2 項演算子である．また，i, j, k は，有限体上の 2 項演算子に対しては有限体 $GF(p^N)$ の元として扱い，その他の通常の演算子や関数においては，整数として扱うものとする．例えば，$\gamma^{(k\oplus i)\odot j}$ を計算するにあたっては，まず $(k \oplus i) \odot j$ を有限体として計算した後，その結果を整数として γ のべき乗を求める．ここで，有限体の定め方は無数に存在するが，$r \in GF(p^N)$ について，そのベクトル表現 $\vec{r} = (r_0, r_1, \cdots, r_{N-1})^T$ (ただし，$r = \sum_{n=0}^{N-1} r_n p^n$ かつ $r_i \in \{0, \cdots, p-1\}$) を考えたときに，有限体上の加算 $\oplus$ が，各ベクトル成分毎の通常の代数和と $\bmod p$ 演算によって得られるように定める．

一般化 Weyl 演算子の固有状態を考えることにより，$(d+1)$ 個の MUB を構成することができる [101]．ただし，素数次元の Weyl 演算子 $\hat{U}_{ij}$ と異なり，1 の d 乗根 ω ではなく 1 の p 乗根 γ を用いるため，一般化 Weyl 演算子の固有値は縮退しており，単一の演算子だけでは固有状態は一意に定まらない．しかし，いくつかの一般化 Weyl 演算子の同時固有状態を考えることで，固有状態を一意に定めることができる．時間位置基底状態 $\left|e_k^{(Z)}\right\rangle$ は，$^\forall l$ に対する $\hat{V}_{0,l}$ の同時固有状態である．また，前節の位相基底状態 $\left|e_k^{(r)}\right\rangle$ は，$^\forall l$ に対する $\hat{V}_{l,r\odot l}$ の同時固有状態である．さらに，位相基底状態 $\left|e_j^{(r)}\right\rangle = \sum_i H_{ij}^{(r)} \left|i\right\rangle$ の確率振幅 $H_{ij}^{(r)}$ は，有限体を用いて次式のように表される．

$$H_{ij}^{(r)} := \frac{1}{\sqrt{p^N}} \left\{\alpha_{\ominus i}^r\right\}^* \gamma^{\ominus i\odot j} \tag{5.8}$$

ただし，

$$\alpha_i^r = \begin{cases} \prod_{m,n=0}^{N-1} i^{r\odot(i_m 2^m)\odot(i_n 2^n)} & (p=2) \\ \gamma^{\ominus(r\odot i\odot i)\oslash 2} & (p \text{ は奇素数}) \end{cases} \tag{5.9}$$

であり，$\ominus, \oslash$ は有限体上の減算および除算を表す 2 項演算子である．また，これらの状態と一般化 Weyl 演算子の間に，次の関係が成り立つ．

$$\hat{V}_{ij} \left|e_k^{(r)}\right\rangle = \gamma^{i\odot k} \left\{\alpha_i^r\right\}^* \left|e_{r\odot i\ominus j\oplus k}^{(r)}\right\rangle \tag{5.10}$$

$$\hat{V}_{ij} \left|e_k^{(Z)}\right\rangle = \gamma^{(k\oplus i)\odot j} \left|e_{i\oplus k}^{(Z)}\right\rangle \tag{5.11}$$

一般化 Weyl 演算子を用いた場合，一般化ベル基底状態を次式のように定義できる．

$$\left|\Psi^{ij}\right\rangle_{AB} = (\hat{V}_{ij} \otimes \hat{\mathbb{1}}) \left|\Psi_{\mathrm{MES}}\right\rangle_{AB} \tag{5.12}$$

この一般化ベル基底状態は，一般化 Weyl 演算子およびその複素共役のテンソル積からなる演算子の固有状態であり，次式が成り立つ．

$$\hat{V}_{ij} \otimes \hat{V}_{ij}^{*} \left|\Psi^{i'j'}\right\rangle_{AB} = \gamma^{i' \odot j \ominus i \odot j'} \left|\Psi^{i'j'}\right\rangle_{AB} \tag{5.13}$$

これらの一般化 Weyl 演算子と一般化ベル基底状態および MUB の性質を用いることで，$(d+1)$ 測定基底 QKD プロトコルの安全性を示すことができる．

5.3.2 安全性証明

本節では，$(d+1)$ 測定基底 QKD プロトコルの安全性証明について述べる．

2.4 節で概略を述べた BBM92 の安全性証明では，複数の光子ペアに対して量子誤り訂正を行い，誤りのない量子もつれ状態を抽出した後に測定を行うことで，盗聴の恐れのない乱数列の共有が可能であることを示した．そこでは，伝送路で盗聴者 Eve が行う盗聴方法については一切の仮定を置いておらず，物理的に可能なあらゆる盗聴に対して安全であることが示された．より詳しくは，Eve の盗聴法としては，コヒーレント攻撃 (Coherent attack) と呼ばれる複数の光子ペアにまたがった，もっとも一般的なユニタリー操作を想定していた．この他，安全性証明においてしばしば仮定される盗聴法として，一般化個別攻撃 (General individual attack) やコレクティブ攻撃 (Collective attack) が知られており，一般化個別攻撃 < コレクティブ攻撃 < コヒーレント攻撃，の順に強力な盗聴法となっている [104].

一般化個別攻撃では，Alice が送信した伝送路中の各光子に対して，Eve が用意した補助系との間に相関を持たせるユニタリー変換を施した後に，Alice/Bob の公開通信情報に関わらず，各補助系に対して同一の測定を行うことで鍵情報を得る [図 5.3(a)]．この際，各光子と補助系に作用させるユニタリー変換は同一のものとし，Alice と Bob の間で共有される光子ペア列は，独立同一分布 (IID：Independent and identically distributed) な状態密度演算子となる．

コレクティブ攻撃は，Eve が伝送路中の各光子と補助系との間に同一のユニタリー変換を施す点は，一般化個別攻撃と同様である．ただし，ユニタリー変換後の各補助系を個別に測定するのではなく，補助系全体にまたがった量子力学的な一括測定を行う [図 5.3(b)]．この際，ユニタリー変換後の補助系は量子メモリに保存しておき，量子状態伝送後に Alice/Bob が公開する情報に基づいて最適化した測定を補助系に施す．補助系の測定タイミングや方法は，Alice/Bob 間で共有される状態に影響を与えないため，共有され

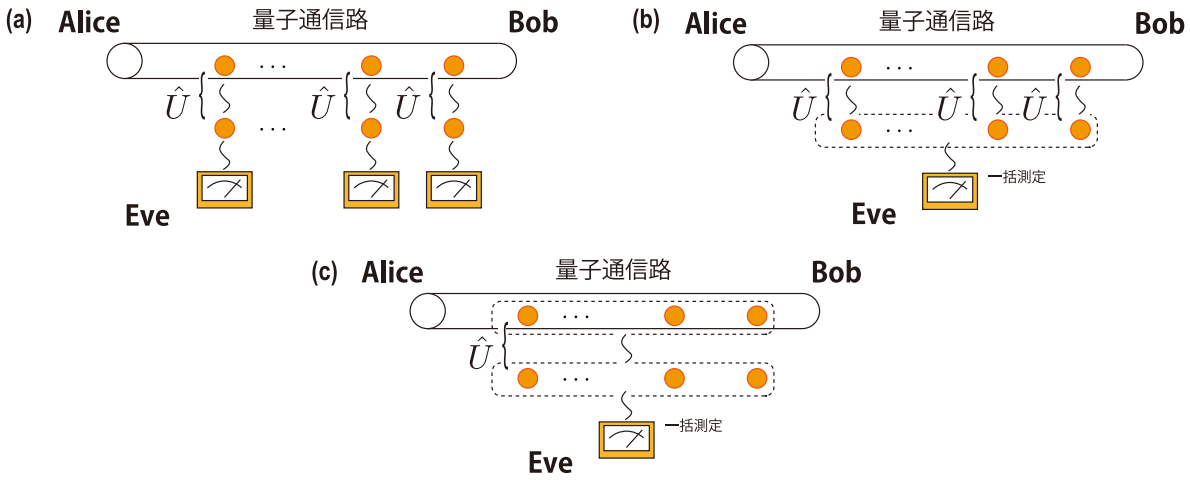

図 5.3　3 種類の盗聴方法．(a) 一般化個別攻撃 (b) コレクティブ攻撃 (c) コヒーレント攻撃

る光子ペアの分布が IID である点などは一般化個別攻撃と同様であるが，最適化された一括測定を行うため，より多くの情報が得られ，IID という条件下ではもっとも強力な盗聴法となる．

一方，コヒーレント攻撃は，各光子と補助系個別にユニタリー変換を施すのではなく，それら全てにまたがった大きなユニタリー変換を施す，もっとも一般的かつ強力な盗聴方法である [図 5.3(c)]．この場合，Alice/Bob 間の光子ペアの分布は一般に IID とはならない．コヒーレント攻撃に対して安全性が証明されれば，最も強力な安全性が保証されたことになるが，非常に多くのパラメータが関わるために，コレクティブ攻撃より安全性の証明が難しい．

なお，上記の他に，伝送路で光子を一度測定し，測定値に応じて新しく光子を用意し再送する，なりすまし攻撃 (Intercept resend attack) がよく知られているが，これは一般化個別攻撃におけるユニタリー変換を，想定しやすい形態に具体化した盗聴法と言える．

以下，コレクティブ攻撃に対する安全性証明について議論する．上記の通り，これはコヒーレント攻撃よりも弱い盗聴方法であり，一見するともっとも一般的なものではない．しかしながら，用いる光子ペア数が無限大の極限において，安全性証明から見積もられる秘密鍵生成率は，多くのプロトコルにおいてコヒーレント攻撃とコレクティブ攻撃で一致する．本論文で扱う QKD プロトコルについても，量子 de Finneti 定理 [105, 106] を適用することにより，両者で秘密鍵生成率が一致することが示される．量子 de Finneti 定理とは，i 番目の光子と j 番目の光子を入れ替えても，量子状態に変化がない対称な量子状態について成り立つ定理である．本論文のプロトコルでは，Alice/Bob は各光子ペアをそれぞれ測定した結果からシフト鍵ビットを生成するが，一般通信路を利用して適当な置

換情報を共有し，鍵とする乱数列の順番をランダムに置換しても，鍵の安全性は変わらない．この置換は，原理的には光子ペアの測定前に行ってもよく，したがって光子ペア列は対称な量子状態とみなせるため，量子 de Finneti 定理が適用可能である．

量子 de Finneti 定理によれば，対称な量子状態から一部の光子ペアを捨てたとき，残された光子ペアの状態は，トレース距離の観点からはほとんど IID な量子状態の確率混合と十分近い状態となる．光子ペア数が無限大の極限においては，捨てる光子ペアの割合，IID でないペアの割合およびトレース距離は 0 に漸近する．したがって，光子ペア数が無限大の極限では，無視できる数の光子ペアを捨てることで，IID を仮定した安全性の議論が有効となり，コレクティブ攻撃に対する安全性証明によって，一般に安全な秘密鍵生成率を導出することができる．なお，同じく IID の条件下でも，通常一般化個別攻撃による盗聴量はコレクティブ攻撃によるものよりも少ない．すなわち，IID の条件下では，コレクティブ攻撃がもっとも強力な盗聴法となる．

では，コレクティブ攻撃に対する安全性を論じる．まず，Alice と Bob が共有する光子ペア列は IID であり，各光子ペアの状態密度演算子が $\hat{\rho}'_{AB}$ で与えられるとする．Alice と Bob は，各々の MUB での測定結果から式 (5.2), (5.3) のエラー確率を推定する．r 番目の位相基底での Alice と Bob の測定結果が t だけシフトする確率は，集合 $\left\{ \left| e_a^{(r)} e_b^{(r)*} \right\rangle \;\middle|\; t = a \ominus b \right\}$ の各状態への射影測定確率の和として表せる．ここで，式 (5.10) より，$\left\{ \hat{V}_{ij} \otimes \hat{V}_{ij}^* \left| e_a^{(r)} e_b^{(r)*} \right\rangle \;\middle|\; t = a \ominus b \right\}$ も同じエラー t を表す状態の集合である．したがって，r 番目の位相基底で t だけシフトするエラーを観測する確率は次式のように表される．

$$\begin{aligned} q_r^t &= \sum_{a \ominus b = t} \left\langle e_a^{(r)} e_b^{(r)*} \right| \hat{\rho}'_{AB} \left| e_a^{(r)} e_b^{(r)*} \right\rangle \\ &= \sum_{a \ominus b = t} \left\langle e_a^{(r)} e_b^{(r)*} \right| \frac{1}{d^2} \sum_{ij} \hat{V}_{ij}^\dagger \otimes \hat{V}_{ij}^T \hat{\rho}'_{AB} \hat{V}_{ij} \otimes \hat{V}_{ij}^* \left| e_a^{(r)} e_b^{(r)*} \right\rangle \end{aligned} \tag{5.14}$$

上式は，$\hat{\rho}'_{AB}$ の代わりに，演算子 $\hat{V}_{ij}^\dagger \otimes \hat{V}_{ij}^T$ でランダム化した状態である

$$\hat{\rho}_{AB} = \frac{1}{d^2} \sum_{ij} \hat{V}_{ij}^\dagger \otimes \hat{V}_{ij}^T \hat{\rho}'_{AB} \hat{V}_{ij} \otimes \hat{V}_{ij}^* \tag{5.15}$$

を測定したとしても，そのエラー確率は変わらないことを表している．時間位置基底のエラー確率についても同様である．ランダム化しても Alice/Bob が得る鍵の分布は変わらないため，実際にこのランダム化を行っても行わなくても，鍵の安全性に変化はない．このランダム化を仮に行うとすると，Alice と Bob で一般化 Weyl 演算子のインデックス ij を共有した上でランダム化する必要がある．この情報は一般通信路から Eve に漏洩するが，インデックス ij を知っている Eve から見た状態 $\hat{V}_{ij}^\dagger \otimes \hat{V}_{ij}^T \hat{\rho}'_{AB} \hat{V}_{ij} \otimes \hat{V}_{ij}^*$ と状態 $\hat{\rho}'_{AB}$

は，ユニタリーな変化分しか差がないため，情報量として違いがない [107]．したがって，$\hat{\rho}_{AB}$ に対する秘密鍵生成率は，元の $\hat{\rho}'_{AB}$ に対する秘密鍵生成率の下限を与える．

ここで，$\hat{\rho}_{AB}$ の一般化ベル基底による展開形を考える．一般化 Weyl 演算子と一般化ベル基底状態の固有方程式 [式 (5.13)] より，次式が成り立つ．

$$\begin{aligned}
\left\langle \Psi^{i'j'} \middle| \hat{\rho}_{AB} \middle| \Psi^{i''j''} \right\rangle &= \frac{1}{d^2} \left\langle \Psi^{i'j'} \middle| \sum_{ij} \hat{V}_{ij}^{\dagger} \otimes \hat{V}_{ij}^{T} \hat{\rho}'_{AB} \hat{V}_{ij} \otimes \hat{V}_{ij}^{*} \middle| \Psi^{i''j''} \right\rangle \\
&= \frac{1}{d^2} \sum_{ij} \left\langle \Psi^{i'j'} \middle| \gamma^{\ominus i' \odot j \oplus i \odot j'} \hat{\rho}'_{AB} \gamma^{i'' \odot j \ominus i \odot j''} \middle| \Psi^{i''j''} \right\rangle \\
&= \frac{1}{d^2} \sum_{ij} \gamma^{i \odot (j' \ominus j'') \ominus (i' \ominus i'') \odot j} \left\langle \Psi^{i'j'} \middle| \hat{\rho}'_{AB} \middle| \Psi^{i''j''} \right\rangle \\
&= \delta_{i',i''} \delta_{j',j''} \left\langle \Psi^{i'j'} \middle| \hat{\rho}'_{AB} \middle| \Psi^{i''j''} \right\rangle
\end{aligned} \tag{5.16}$$

ただし，上式を導くにあたり $\sum_i \gamma^{i \odot (j' \ominus j'')} = d\delta_{j',j''}$ を用いた．上式は，$\hat{\rho}_{AB}$ は，$\hat{\rho}'_{AB}$ を一般化ベル基底で展開し，対角成分のみを残した状態であることを示している．これらの考察から，安全性解析としての一般性を失うことなく，Alice/Bob 間で共有される量子状態を，次式の一般化ベル基底対角化状態として取り扱うことができる．

$$\hat{\rho}_{AB} = \sum_{j,k=0}^{d-1} \lambda_{jk} \left| \Psi^{jk} \right\rangle\!\!\left\langle \Psi^{jk} \right|_{AB} \tag{5.17}$$

ただし，$\lambda_{jk} \geq 0$ かつ $\sum_{jk} \lambda_{jk} = 1$ である．上式の一般化ベル基底対角化状態に対するエラー測定確率を求めると，λ_{jk} と誤り分布ベクトルの関係式として，次式を得る．

$$q_Z^t = \sum_{k=0}^{d-1} \lambda_{tk} \tag{5.18}$$

$$q_k^t = \sum_{j=0}^{d-1} \lambda_{j,k \odot j \ominus t} \quad \text{for} \quad k \in \{0, \cdots, d-1\} \tag{5.19}$$

また，これらの逆関係として，次式を得る．

$$\lambda_{jk} = \frac{1}{d} \left(\sum_{s=0}^{d-1} q_s^{s \odot j \ominus k} + q_Z^j - 1 \right) \tag{5.20}$$

式 (5.20) は，$(d+1)$ 個の MUB 測定によって得られた誤り分布ベクトルから，式 (5.17) の Alice/Bob 間で共有したとみなせる状態 $\hat{\rho}_{AB}$ が推定できることを示している．これは，対角化という限定的な状況下での量子状態トモグラフィーと言える．このようにして推定された $\hat{\rho}_{AB}$ を用いて，Eve の盗聴量の最大値を見積もり，それから最終秘密鍵生成率を得る．

2.3.2 節および 2.3.3 節で述べたように，混合状態に対して補助系を付け加えると，全体として純粋状態を構成することができる．補助系 E による $\hat{\rho}_{AB}$ の純粋化は，次式で与えられる．

$$|\psi\rangle_{ABE} = \sum_{j,k=0}^{d-1} \sqrt{\lambda_{jk}} \left|\Psi^{jk}\right\rangle_{AB} \left|\phi^{jk}\right\rangle_{E} \tag{5.21}$$

ここで，$\left|\phi^{jk}\right\rangle_{E}$ は，少なくとも d^2 次元より大きなヒルベルト空間中の正規直交状態である．上式の状態に更に追加で補助系を増やしても，$|\psi\rangle_{ABE}$ は純粋状態であるため追加補助系とは無相関であり，そこから盗聴されることはない．また，補助系 E をさらに補助系 $E_1, E_2, \cdots$ と細かく分割し，その一部のみを Eve が所持することも可能であるが，分割した部分系から得られる情報量は，全系 E から得られる情報量よりも小さい．あるいは，Eve が補助系 E を持っていれば，後から自身でそのような分割操作が可能であり，部分系のみを持っているという条件は Eve が補助系 E を持っている時の測定最適化に含まれる，と考えてもよい．したがって，盗聴者 Eve が補助系 E を所有していると想定して，盗聴量の上限を見積もることができる．

そこで以降では，Eve が補助系 E を所有しているものとして議論を展開する．Eve の盗聴量としては，Alice のシフト鍵について Eve が知っている情報量を考える．またここでは，Alice と Bob は，高い割合で時間位置基底測定を行い，その測定結果からシフト鍵を生成することとし，位相基底での測定結果は，誤り分布ベクトルの推定による盗聴量の上限見積もりにのみ利用するものとする．このような非対称な基底選択は，安全性解析を簡単化するだけでなく，Alice/Bob が一様ランダムに基底選択した場合の基底不一致によるビット廃棄の割合を低減できる．

古典的には Eve の盗聴量は，Alice/Eve それぞれの測定値を表す確率変数間の相互情報量 $I(A;E)$ から見積もられる．しかし今の場合，Alice の測定は具体的に定義されている一方，Eve は物理法則に反しない限りあらゆる測定が可能としており，測定値を定式化できない．このような量子測定で得られる相互情報量の上限は Holevo 限界として知られており [1, 78]，その上限値である Holevo 情報量は次式で与えられる．

$$\chi(A;E) = S(\hat{\rho}_E) - \sum_a p(a) S(\hat{\rho}_{E|a}) \tag{5.22}$$

ただし，$\hat{\rho}_E$ は Eve の持つ補助系の状態密度演算子，$\hat{\rho}_{E|a}$ は Alice の測定結果 a で条件付けた Eve の持つ補助系の状態密度演算子，$p(a)$ は Alice の測定結果 a が観測される確率である．

任意の一般化ベル基底状態の部分系の量子状態は最大混合状態となるため，式 (5.21) の状態をもとに考えると，式 (5.22) において $p(a) = 1/d$ である．また，2.3.2 節で述べたように，純粋化前の密度演算子 $\hat{\rho}_{AB}$ の von Neumann エントロピーと，純粋化で付与

された補助系 E の密度演算子 $\hat{\rho}_E$ の von Neumann エントロピーは等しいため，λ_{jk} を要素としたベクトル $\underline{\lambda}$ を用いて，$S(\hat{\rho}_E) = \mathrm{H}(\underline{\lambda})$ となる．そこで以下，式 (5.22) の残る項 $S(\hat{\rho}_{E|a})$ を計算するために，$\hat{\rho}_{E|a}$ を求める．前述のように，シフト鍵は時間位置基底での測定結果から生成される．Alice/Bob がそれぞれ測定値 a, b を得たという条件下での，Eve の補助系 E の非規格化量子状態は，次式で与えられる．

$$\langle ab|_{AB} |\psi\rangle_{ABE} = \sum_{j,k=0}^{d-1} \sqrt{\lambda_{jk}} \left\langle ab \middle| \Psi^{jk} \right\rangle_{AB} \left|\phi^{jk}\right\rangle_E \tag{5.23}$$

ここで，式 (5.7), (5.12) より，

$$\begin{aligned}
\left\langle ab \middle| \Psi^{jk} \right\rangle &= \langle ab| \sum_i \frac{1}{\sqrt{d}} \gamma^{(i\oplus j)\odot k} |i \oplus j, i\rangle \\
&= \frac{1}{\sqrt{d}} \langle ab|b \oplus j, b\rangle \gamma^{(b\oplus j)\odot k} \\
&= \frac{1}{\sqrt{d}} \delta_{a,b\oplus j} \gamma^{a\odot k}
\end{aligned} \tag{5.24}$$

であるから，式 (5.23) は次のように書き換えられる．

$$\begin{aligned}
\langle ab|_{AB} |\psi\rangle_{ABE} &= \frac{1}{\sqrt{d}} \sum_k \sqrt{\lambda_{a\ominus b,k}} \gamma^{a\odot k} \left|\phi^{a\ominus b,k}\right\rangle_E \\
&= \sqrt{\frac{\sum_{k'} \lambda_{a\ominus b,k'}}{d}} \sum_k \frac{\sqrt{\lambda_{a\ominus b,k}} \gamma^{a\odot k}}{\sqrt{\sum_{k'} \lambda_{a\ominus b,k'}}} \left|\phi^{a\ominus b,k}\right\rangle_E \\
&= \sqrt{\frac{q_Z^{a\ominus b}}{d}} \sum_k \frac{\sqrt{\lambda_{a\ominus b,k}} \gamma^{a\odot k}}{\sqrt{q_Z^{a\ominus b}}} \left|\phi^{a\ominus b,k}\right\rangle_E
\end{aligned} \tag{5.25}$$

ただし，上式の 2 行目から 3 行目への式変形において式 (5.18) を用いた．ここで，

$$\left|\widetilde{\phi}^{a\ominus b}\right\rangle_E = \sum_k \frac{\sqrt{\lambda_{a\ominus b,k}} \gamma^{a\odot k}}{\sqrt{q_Z^{a\ominus b}}} \left|\phi^{a\ominus b,k}\right\rangle_E \tag{5.26}$$

とする．この $\left|\widetilde{\phi}^{a\ominus b}\right\rangle_E$ は規格化された純粋状態となっている．また，a を固定したとき，$\left|\phi^{a\ominus b,k}\right\rangle_E$ が異なる b, k について直交しているため，$\left|\widetilde{\phi}^{a\ominus b}\right\rangle_E$ は異なる b について直交している．式 (5.25), (5.26) より，

$$\begin{aligned}
p(a)\hat{\rho}_{E|a} &= \sum_b \langle ab|_{AB} |\psi\rangle_{ABE} \langle\psi|_{ABE} |ab\rangle_{AB} \\
&= \frac{1}{d} \sum_b q_Z^{a\ominus b} \left|\widetilde{\phi}^{a\ominus b}\right\rangle\left\langle\widetilde{\phi}^{a\ominus b}\right|_E
\end{aligned} \tag{5.27}$$

となり，$p(a) = 1/d$ であるから，次式が成り立つ．

$$\hat{\rho}_{E|a} = \sum_b q_Z^{a\ominus b} \left|\widetilde{\phi}^{a\ominus b}\right\rangle\!\left\langle\widetilde{\phi}^{a\ominus b}\right|_E \tag{5.28}$$

$\left|\widetilde{\phi}^{a\ominus b}\right\rangle_E$ は異なる b について直交しているので，上式は対角化されており，固有値が時間位置基底での誤り分布ベクトル $\underline{q}_Z$ の要素で与えられている．したがって，a の値にかかわらず，$S(\hat{\rho}_{E|a}) = \mathrm{H}(\underline{q}_Z)$ となる．

以上をまとめると，Alice のシフト鍵に対する Eve の盗聴量の上限値である Holevo 情報量が，次式で与えられる．

$$\chi(A;E) = \mathrm{H}(\underline{\lambda}) - \mathrm{H}(\underline{q}_Z) \tag{5.29}$$

Alice と Bob は，シフト鍵に誤り訂正を施した後，秘匿性増強により盗聴量分を鍵圧縮して最終的な秘密鍵を共有する．誤り訂正鍵の長さは，Alice/Bob の測定値を表す確率変数間の相互情報量 $I(A;B)$ から求まる．今，Alice が測定値 a を得る確率は全て等しく $p(a) = 1/d$ であり，さらに a で条件付けた Bob の測定値 b の確率分布が誤り分布ベクトル $\underline{q}_Z$ で与えられるため，

$$I(A;B) = \log_2 d - \mathrm{H}(\underline{q}_Z) \tag{5.30}$$

である．したがって，鍵生成に用いる光子ペア数が無限大の極限で，Alice/Bob がシャノン限界を達成する誤り訂正手法を用いるとき，$(d+1)$ 測定基底 QKD プロトコルの秘密鍵生成率は次式で与えられる．

$$\begin{aligned} r_\infty &= I(A:B) - \chi(A:E) \\ &= \log_2 d - \mathrm{H}(\underline{\lambda}) \end{aligned} \tag{5.31}$$

上記鍵生成率となるように，秘匿性増強による鍵圧縮を施すことで，盗聴の恐れのない一様乱数を Alice, Bob 間で共有することが出来る．すなわち，素数の累乗次元での $(d+1)$ 測定基底 QKD プロトコルの安全性が証明されたと言える．

なお，上記の秘密鍵生成率の導出過程は，先行研究 [42] の議論を有限体によって一般化したものとなっている．先行研究においては，誤り分布ベクトルと λ_{jk} の関係式 (5.19), (5.20) などの有限体での計算式が，通常の四則演算および mod d 演算となっている．次元 d が素数である時，有限体の計算は四則演算および mod d で実現できるから，上記の証明で得られた結果は素数次元において先行研究の内容を含んでおり，素数次元から素数の累乗次元への一般化となっている．

以上論じたのは素数の累乗次元への拡張であり，その他の次元への一般化が課題として残るが，この実現は難しいことが予想される．素数の累乗次元における $(d+1)$ 個の MUB の構成方法は，1989 年に Wootters らによって初めて与えられた [102]．以降，その他の

次元における $(d+1)$ 個の MUB の構成は様々に試みられているが，最も小さな次元である $d = 6$ においても 3 つしか見つかっておらず，そもそも構成可能であるか否かが不明である [101, 108]．このように一般の次元での $(d+1)$ 個の MUB の存在は未だ未解決な問題であり，MUB が $(d+1)$ 個存在しなければ QKD プロトコルとして実装できない．

上記の安全性証明を利用して，2 測定基底 QKD プロトコルの鍵生成率も導出できる．2 測定基底 QKD プロトコルでは，$(d+1)$ 個の MUB のうち 2 つの基底だけを利用する．ここで，時間位置基底と $r = 0$ の位相基底の二つを用いるものとする．この場合，誤り分布ベクトルのうち，$\underline{q}_Z$ および $\underline{q}_0$ しか得ることができないため，λ_{jk} を一意に定めることができない．そのため，最悪条件として，Eve の盗聴量上限値である Holevo 情報量 $\chi(A;E)$ を推定する際，$\underline{q}_Z$ および $\underline{q}_0$ による拘束条件の下で，$\chi(A;E)$ を最大化するように λ_{jk} を最適化することになる．

λ_{jk} は，Alice/Bob 間で共有される状態が $\left|\Psi^{jk}\right\rangle_{AB}$ となる確率である．拘束条件は，式 (5.18), (5.19) より，

$$q_Z^t = \sum_{k=0}^{d-1} \lambda_{tk} \tag{5.18}$$

$$q_0^t = \sum_{j=0}^{d-1} \lambda_{j,\ominus t} \tag{5.32}$$

である．上式は，時間位置基底および $r = 0$ の位相基底における誤り確率は，λ_{jk} の周辺確率分布になっており，λ_{jk} が時間位置シフトエラーおよび位相シフトエラーの結合確率分布であることを示している．このことは，次のように考えることでも理解できる．

量子もつれ状態 $\left|\Psi^{jk}\right\rangle_{AB}$ は，一般化 Weyl 演算子を最大量子もつれ状態 $|\Psi_{\mathrm{MES}}\rangle_{AB}$ の光子 A に作用させることで得られる．一般化 Weyl 演算子は次のように二つの Weyl 演算子の積に分解できる．

$$\hat{V}_{ij} = \hat{V}_{0j}\hat{V}_{i0} \tag{5.33}$$

ここで，分解した二つの一般化 Weyl 演算子は，次式のように表すことができる．

$$\hat{V}_{i0} = \sum_{k=0}^{d-1} |k \oplus i\rangle \langle k| = \sum_{k=0}^{d-1} \left|e_{k\oplus i}^{(Z)}\right\rangle \left\langle e_k^{(Z)}\right| \tag{5.34}$$

$$\hat{V}_{0j} = \sum_{k=0}^{d-1} \gamma^{k\odot j} |k\rangle \langle k| = \sum_{k=0}^{d-1} \left|e_{k\ominus j}^{(0)}\right\rangle \left\langle e_k^{(0)}\right| \tag{5.35}$$

式 (5.34) より，$\hat{V}_{i0}$ は時間位置基底の値を i シフトする演算子，また式 (5.35) より，$\hat{V}_{0j}$ は $r = 0$ の位相基底の値を $\ominus j$ シフトする演算子，である．式 (5.33) のように $\hat{V}_{ij}$ が二つの演算子の積で表せるため，$\left|\Psi^{jk}\right\rangle_{AB}$ は，二つの基底の状態のインデックスを Alice 側

だけシフトした，すなわちエラーが生じた状態とみなせる．したがって，λ_{jk} は二つのエラーの結合確率分布となっている．

式 (5.29) より，Holevo 情報量は $\chi(A;E) = \mathrm{H}(\underline{\lambda}) - \mathrm{H}(\underline{q}_Z)$ で与えられる．λ_{jk} が 2 種類のエラーの結合確率分布であることから，$\chi(A;E)$ は時間位置基底でのエラーで条件付けた，$r = 0$ の位相基底でのエラーの条件付きエントロピーとなっている．条件付きエントロピーは二つのエラーが無相関である時に最大化される．したがって，2 測定基底 QKD プロトコルにおける Eve の盗聴量の上限は，

$$\begin{aligned}\chi(A;E) &= \mathrm{H}(\underline{q}_0) - \Big\{\mathrm{H}(\underline{q}_0) + \mathrm{H}(\underline{q}_Z) - \mathrm{H}(\underline{\lambda})\Big\} \\ &= \mathrm{H}(\underline{q}_0) - I(\underline{q}_0;\underline{q}_Z) \\ &= \mathrm{H}(\underline{q}_0)\end{aligned} \tag{5.36}$$

で与えられ，秘密鍵生成率は

$$\begin{aligned}r_\infty &= I(A:B) - \chi(A:E) \\ &= \log_2 d - \mathrm{H}(\underline{q}_Z) - \mathrm{H}(\underline{q}_0)\end{aligned} \tag{5.37}$$

となる．

上記 2 測定基底 QKD プロトコルの秘密鍵生成率は，$d = 2$ の時，式 (2.66) で与えられる BB84/BBM92 の秘密鍵生成率と一致する．2.4 節で，BB84/BBM92 と Six-state プロトコルの違いは，2 種類のエラーの間の相関が見積もれるか否かであることを述べた．上記 2 種類の高次元 QKD プロトコルの安全性証明は，相関が見積もれるか否かがプロトコルの違いとして現れることを示している．このように，$(d+1)$ 測定基底 QKD プロトコルは，2 種類のエラーの相関を見積もることにより高い秘密鍵生成率を実現するプロトコルと言える．

5.3.3 平均シンボルエラーレート閾値の導出

前節では，各基底の誤り分布ベクトルから λ_{jk} を求めることにより，$(d+1)$ 測定基底 QKD プロトコルの秘密鍵生成率 [式 (5.31)] を導出した．しかしながら，誤り分布ベクトルは多数のパラメータを含むため，QKD システム性能の直感的な指標には不向きである．そこで本節では，式 (5.31) をもとに，秘密鍵を生成するために満たすべき，平均シンボルエラーレートの上限 (閾値) を導出する．

まず，$\underline{\lambda}$ のエントロピーについて，次式が成り立つ．

$$\begin{aligned}
\mathrm{H}(\underline{\lambda}) &= \sum_{j,k} -\lambda_{jk} \log_2 \lambda_{jk} \\
&= -\lambda_{00} \log_2 \lambda_{00} - \sum_{(j,k)\neq(0,0)} \lambda_{jk} \log_2 \lambda_{jk} \\
&= -\lambda_{00} \log_2 \lambda_{00} - (1-\lambda_{00}) \log_2 (1-\lambda_{00}) \\
&\quad + (1-\lambda_{00}) \sum_{(j,k)\neq(0,0)} \left[-\frac{\lambda_{jk}}{1-\lambda_{00}} \log_2 \frac{\lambda_{jk}}{1-\lambda_{00}} \right] \\
&\leq -\lambda_{00} \log_2 \lambda_{00} - (1-\lambda_{00}) \log_2 (1-\lambda_{00}) + (1-\lambda_{00}) \log_2 (d^2-1) \\
&= -\lambda_{00} \log_2 \lambda_{00} - (1-\lambda_{00}) \log_2 \frac{1-\lambda_{00}}{d^2-1}
\end{aligned} \tag{5.38}$$

ただし，不等式への移行には，(d^2-1) 次元のエントロピーの最大値が $\log_2(d^2-1)$ であることを用いた．ここで，式 (5.20) から，λ_{00} が次式で与えられる．

$$\begin{aligned}
\lambda_{00} &= \frac{1}{d} \left(\sum_{r=0}^{d-1} q_r^0 + q_Z^0 - 1 \right) \\
&= \frac{1}{d} \left(d - \sum_{r=0}^{d-1} e_r - e_Z \right) \\
&= 1 - \frac{d+1}{d} \bar{e}
\end{aligned} \tag{5.39}$$

ただし，e_Z, e_r はそれぞれ時間位置基底および r 番目の位相基底のシンボルエラーレート，$\bar{e}$ はこれらの相加平均である．したがって，平均シンボルエラーレート $\bar{e}$ を用いて，秘密鍵生成率の下限が次式で与えられる．

$$\begin{aligned}
r_\infty &= \log_2 d - \mathrm{H}(\underline{\lambda}) \\
&\geq \log_2 d + \lambda_{00} \log_2 \lambda_{00} + (1-\lambda_{00}) \log_2 \frac{1-\lambda_{00}}{d^2-1} \\
&= \log_2 d + \left(1 - \frac{d+1}{d} \bar{e} \right) \log_2 \left(1 - \frac{d+1}{d} \bar{e} \right) + \frac{d+1}{d} \bar{e} \log_2 \left\{ \frac{1}{d(d-1)} \bar{e} \right\}
\end{aligned} \tag{5.40}$$

なお，上式は対称なノイズモデルである，分極解消チャネルの場合の秘密鍵生成率 [42] に一致する．式 (5.40) において，r_∞ の下限が 0 となる時の $\bar{e}$ が平均シンボルエラーレート閾値となる．例えば，$d = 4$ ではこの閾値は 23.17 % となり，平均シンボルエラーレートがこれより小さければ，常に秘密鍵生成が可能である．平均シンボルエラーレート閾値を用いる性能評価法は，詳細なエラー分布によらないため，扱いが容易という利点を有する．ただし，これは秘密鍵生成率の下限から算出した閾値であり，仮にこの閾値より大きな平均シンボルエラーレートであっても，式 (5.31) と元の誤り分布ベクトルをもとに算

出すると，秘密鍵が生成可能となる場合がある．したがって，$(d+1)$ 測定基底 QKD プロトコルの性能を正しく評価するには，式 (5.31) に基づいて行うことが必要である．

5.4 高次元タイムビン量子状態に対する $(d+1)$ 相互不偏基底測定手法

本節では，前節で述べた $(d+1)$ 個の MUB の，タイムビン量子状態に対する実装法について述べる．

これまで高次元 QKD としては，2 測定基底 QKD プロトコルが主に実装されており [31–40]，高次元タイムビン量子状態については，3.4.1 節で述べたツリー上に多段接続した MZI 構成が報告されている [31, 32]．ただし，ツリー構造のため MZI を $(d-1)$ 個，光子検出器を d 個用いており，d が大きいとデバイス数が増大する．さらに，式 (3.11) に示すフーリエ基底を利用しているため，状態生成や測定系の位相精度が $1/d$ に比例し，装置の高い制御性が要求される．特定の次元でこれらの問題が緩和された基底を用いた実装 [33] や，一つの基底に含まれる一部の状態だけを利用する手法 [109, 110] が報告されているが，スケーラブルな一般的実装法は確立されていない．また，$(d+1)$ 基底 QKD プロトコルとしては SLM で生成した OAM 量子状態を用いた実装報告があるが [77]，タイムビン量子状態については，SLM のようなフレキシブルな変調器がないため，用いる MUB の特性を適切に利用した実装の工夫が必要である．

前節で述べた式 (5.8) の位相基底以外に，次式で表される位相基底を用いても，$d = p^N$ である $(d+1)$ 個の MUB を構成することができる [102]．

$$\left|\psi_n^{(r)}\right\rangle = \sum_m B_{mn}^{(r)} |m\rangle \tag{5.41}$$

$$B_{mn}^{(r)} = \begin{cases} \frac{1}{\sqrt{2^N}} \exp\left[\frac{\pi}{2} i \left(\sum_{j=0}^{N-1} r_j \vec{m}^{\mathrm{T}} \mathbf{A}^{(j)} \vec{m} + 2\vec{m}\cdot\vec{n}\right)\right] & (p=2) \\ \frac{1}{\sqrt{p^N}} \exp\left[\frac{2\pi}{p} i \left(\sum_{j=0}^{N-1} r_j \vec{m}^{\mathrm{T}} \mathbf{A}^{(j)} \vec{m} + \vec{m}\cdot\vec{n}\right)\right] & (p \text{ は奇素数}) \end{cases} \tag{5.42}$$

ただし，$\vec{m}, \vec{n}, \vec{r}$ はそれぞれ整数 m, n, r の p 進数ベクトル，r_j は $\vec{r}$ の j 番目の要素，である．また，$\mathbf{A}^{(j)}$ は $N \times N$ 対称行列であり，その m 行 n 列要素 A_{mn} は次式を満たす．

$$p^m \odot p^n = \oplus_{k=0}^{N-1} A_{mn}^{(k)} p^k \tag{5.43}$$

上式より，$\mathbf{A}^{(j)}$ は有限体の乗算によって一意に定められる．また，式 (5.42) は整数を要素とするベクトルと行列のみで計算可能であるが，$\mathbf{A}^{(j)}$ により有限体の代数的構造を反映した計算式となっている．前節で述べた位相基底状態 [式 (5.8)] と，上記の位相基底状態 [式 (5.42)] は表式が大きく異なっているが，状態や基底のインデックス r, n を並べ替

えると，同一の MUB であることが示される (付録 A)．したがって，式 (5.41), (5.42) の MUB によっても，前節と同様にして，$(d+1)$ 測定基底 QKD プロトコルを実装できる．

式 (5.42) は $p=2$ と $p=$ 奇素数 とで場合分けされているため，まずは $p=2$ の場合の実装法について論じる．式 (5.42) より，位相基底状態は，時間基底で展開したときの確率振幅の大きさが等しく，位相だけが変調された重ね合わせ状態となっている．また，位相項の $\sum_{j=0}^{N-1} r_j \vec{m}^{\mathrm{T}} \mathbf{A}^{(j)} \vec{m} + 2\vec{m}\cdot\vec{n}$ は，0 または 1 を要素とするベクトルと行列からなるため，必ず整数値となり，任意の N において，必要な位相は $\{0, \pi/2, \pi, 3\pi/2\}$ の高々 4 値である．したがって，位相基底状態は，d 連続パルスに対し，4 値位相変調 (QPSK：Quadrature Phase Shift Keying) を施した状態と言える．一方，時間位置基底状態は，d 連続のタイムスロットのうち，一つのタイムスロットにのみ 1 光子が存在する状態である．$(d+1)$ 測定基底 QKD プロトコルの実装法には，量子もつれ状態を用いる EB 型と，単一光子の状態を Alice が準備して Bob に送る P&M 型があるが，後者では上記の状態を準備すればよいことになる．理想的には単一光子を用いるプロトコルであるが，実用上は平均光子数 1 以下の微弱コヒーレント光を疑似単一光子として代用できる．したがって，光IQ 変調器 (In-phase and Quadrature-phase modulator) によりレーザからのコヒーレント光を変調し，光減衰器で単一光子レベルまで減衰すれば，$(d+1)$ 個の MUB の基底状態を容易に生成できる．

一方の測定系構築については，上記の $B_{mn}^{(r)}$ を要素とする行列 $\mathbf{B}^{(r)}$ の構造を利用する．この行列は，二つの行列の積 $\mathbf{B}^{(r)} = \mathbf{D}^{(r)}\mathbf{B}^{(0)}$ と分解することができる．ここで，$\mathbf{D}^{(r)}$ は対角ユニタリー行列であり，m 番目の対角要素が次式で与えられる．

$$D_{mm}^{(r)} = \exp\left\{ i\frac{\pi}{2}\left(\sum_{j=0}^{N-1} r_j \vec{m}^{\mathrm{T}} \mathbf{A}^{(j)} \vec{m} \right) \right\} \tag{5.44}$$

ここで，行列 $\mathbf{B}^{(r)}, \mathbf{D}^{(r)}$ に対応する演算子 $\hat{B}^{(r)}, \hat{D}^{(r)}$ を用いると，r 番目の位相基底における n 番目の基底状態 $\left|\psi_n^{(r)}\right\rangle$ を，次式のように表すことができる．

$$\begin{aligned} \left|\psi_n^{(r)}\right\rangle &= \sum_m B_{mn}^{(r)} |m\rangle = \hat{B}^{(r)} |n\rangle \\ &= \hat{D}^{(r)} \hat{B}^{(0)} |n\rangle \\ &= \hat{D}^{(r)} \left|\psi_n^{(0)}\right\rangle \end{aligned} \tag{5.45}$$

したがって，任意の d 次元量子状態の状態密度演算子 $\hat{\rho}$ が与えられた時，量子状態 $\left|\psi_n^{(r)}\right\rangle$ への射影測定確率が，次式で与えられる．

$$\left\langle \psi_n^{(r)} \middle| \hat{\rho} \middle| \psi_n^{(r)} \right\rangle = \left\langle \psi_n^{(0)} \middle| \hat{D}^{(r)\dagger} \hat{\rho} \hat{D}^{(r)} \middle| \psi_n^{(0)} \right\rangle \tag{5.46}$$

上式は，状態 $\left|\psi_n^{(r)}\right\rangle$ への射影測定は，$\hat{D}^{(r)\dagger}$ によるユニタリー変換を施したのちに状態 $\left|\psi_n^{(0)}\right\rangle$ への射影測定を行うことと等価であることを示している．ここで，時間位置基底状態 $|m\rangle$ に対して $\hat{D}^{(r)\dagger}|m\rangle = D_{mm}^{(r)*}|m\rangle$ であり，これは $\hat{D}^{(r)\dagger}$ が表すユニタリー変換は，位相基底のインデックス r に応じたパターンで，時間位置基底状態に位相変調を施す操作に対応することを示している．したがって，高次元タイムビン量子状態に対するこのユニタリー変換は，位相変調器によって実装できる．よって，r 番目の基底選択のための位相変調を施した後，$\left\{\left|\psi_n^{(0)}\right\rangle\right\}$ への射影測定を行う構成により，任意の r 番目の位相基底測定が実装できる．

$\left|\psi_n^{(0)}\right\rangle = \hat{B}^{(0)}|n\rangle$ であるから，この状態は時間位置基底状態に対して $\hat{B}^{(0)}$ のユニタリー変換を施した状態である．ここで，式 (5.43) より，

$$B_{mn}^{(0)} = \frac{1}{\sqrt{2^N}} \exp(i\pi \vec{m} \cdot \vec{n}) \tag{5.47}$$

と表されるが，これは 2^N 次元アダマール変換となっている．4.2.2 節では，2^N 次元の高次元タイムビン量子状態を，N 個の 2 次元タイムビン量子状態 (図 4.2) にモデル化して，効率的な QST を提案した．2^N 次元アダマール変換は，この等価な N 個の 2 次元タイムビン量子状態全てに対して，2 次元アダマール変換を施す操作に等しい．2 次元アダマール変換のユニタリー演算子は，式 (2.10) で与えられる．

$$\hat{H} = |+\rangle\langle 0| + |-\rangle\langle 1| \tag{2.10}$$

したがって，量子状態 $\left|\psi_n^{(0)}\right\rangle = \hat{B}^{(0)}|n\rangle$ は，等価な N 個の 2 次元量子状態を用いて記述すると，量子状態 $|+\rangle, |-\rangle$ の N プロダクト状態 (アダマール基底状態) となる．4.2.2 節で述べたように，このような状態への射影測定は，多段接続した遅延 MZI を用いて実装可能である．

図 5.4(a) に，ツリー構造の多段接続 MZI による 4 次元アダマール基底への射影測定実装法を示す．パルス間隔 τ の 4 次元タイムビン量子状態を 2τ 遅延 MZI に入力すると，出力の 6 つのタイムスロットのうち，点線で囲われた中心の 2 つのタイムスロットにおいて，入力パルス列内の 2 つのパルスが干渉する．この干渉は，MZI の伝搬遅延位相を 0 とすると，時間間隔 2τ の等価な量子ビット q_1 に対する，$|+\rangle, |-\rangle$ 状態への射影測定に対応する．この出力パルス列をさらに τ 遅延 MZI に入力すると，初段 MZI で干渉したパルス列が中心の出力タイムスロットで干渉する．τ 遅延 MZI の伝搬遅延位相も 0 とすることで，この干渉を時間間隔 τ の等価な量子ビット q_0 に対する，$|+\rangle, |-\rangle$ 状態への射影測定に対応づけることができる．したがって，多段接続した MZI の全ての出力ポートにおいて，中心のタイムスロットにおける光子検出事象を記録すれば，各等価な量子ビットに対する $|+\rangle, |-\rangle$ 状態のテンソル積の，全組み合わせの射影測定が実装できる．この手法

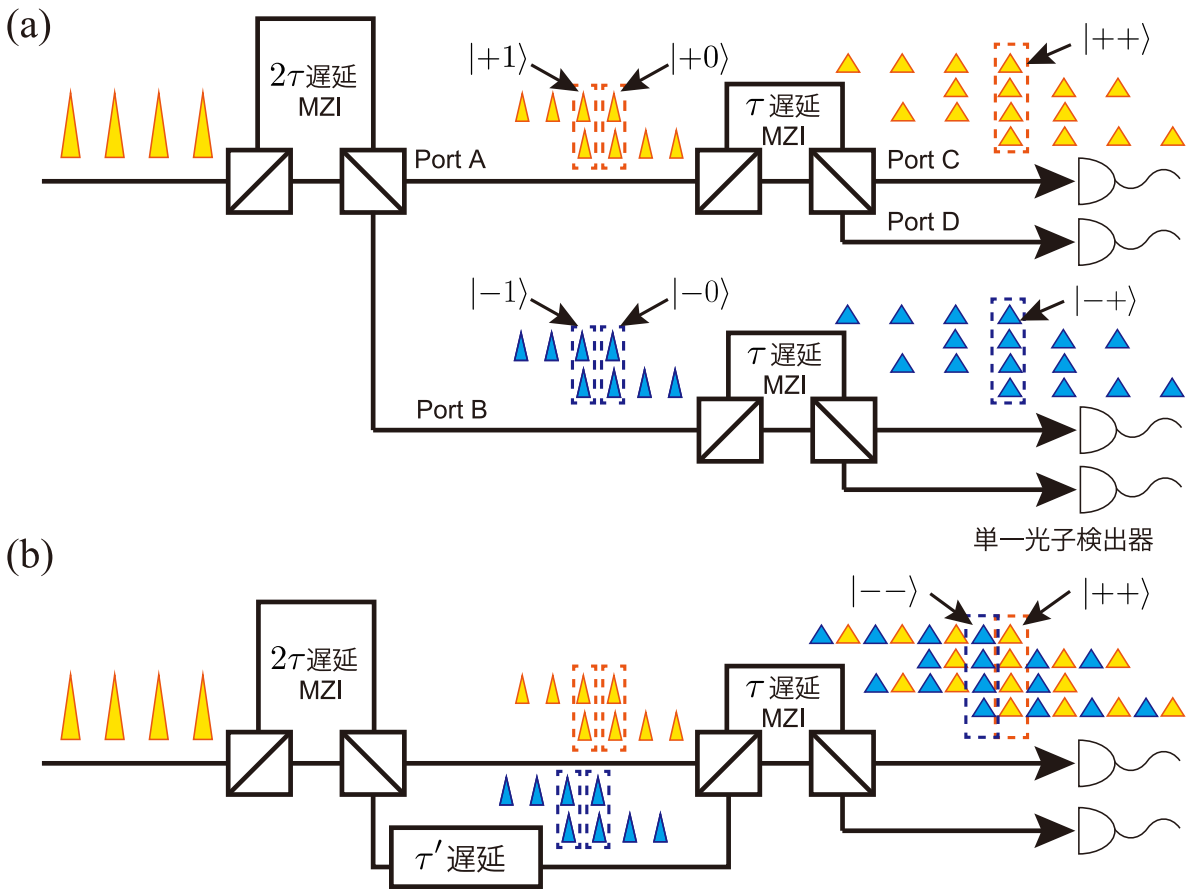

図 5.4　多段接続 MZI によるアダマール基底への射影測定実装法．(a) ツリー構造，(b) 遅延線による時分割多重構成

はさらに 4τ 遅延 MZI，8τ 遅延 MZI とツリー構造を拡張することで，任意の 2^N 次元タイムビン量子状態の測定系に拡張できる．しかしながら，上記ツリー構造を用いた測定系は，$d-1$ 個の MZI および d 個の単一光子検出器を必要とする．これはフーリエ基底を用いた実装 [31, 32] と同じであり，スケーラブルな装置構成とはならない．ただし，フーリエ基底への測定系とアダマール基底への測定系では，MZI の伝搬遅延位相が異なっている．前者では，後段の 2 つの τ 遅延 MZI は異なる伝搬遅延位相を持つ．一方，アダマール基底測定系では全ての MZI の伝搬遅延位相が 0 であり，後段の 2 つの τ 遅延 MZI は遅延時間/伝搬遅延位相ともに同一である．本論文ではこのことに着目して，測定に必要な MZI の個数を削減する．

図 5.4(b) に，本論文で提案する 4 次元アダマール基底への射影測定系構成を示す．ここでは，2τ 遅延 MZI の 2 つの出力が τ 遅延 MZI の 2 つの入力にそれぞれ接続されている．ただし，接続経路の一方に遅延時間 τ' の遅延線が挿入されており，τ 遅延干渉計の

入力部のビームスプリッタにおいて，二つの入力が干渉しないように設定されている．なお，図 5.4(b) では，$\tau' = \tau/2$ とした場合の時間位置関係が図示されているが，入力部のビームスプリッタで干渉が生じない限り，τ' は任意の値とすることができる．例えば，状態生成の繰り返しレートを低下させ，$\tau' \geq 8\tau$ 等にすれば，光子検出器の時間分解能に対する要求条件を緩和できる．2 入力の τ 遅延 MZI では，$|+\rangle$ と $|-\rangle$ の出力ポートが上側ポート入力と下側ポート入力で反転するが，$|+\rangle, |-\rangle$ への射影測定としては変わりはない．したがって，遅延線による時分割多重効果により，図 5.4(b) の構成も 4 次元アダマール基底測定系となっている．より高次元の 2^N 次元アダマール基底についても，同様に遅延線による時分割多重を用いることにより，$N = \log_2 d$ 個の MZI および 2 台の単一光子検出器により射影測定系が構成できる．さらに，先に述べた位相基底切り替え手法と組み合わせると，1 台の位相変調器，$\log_2 d$ 個の遅延 MZI および 2 個の光子検出器からなる構成で，全ての位相基底についての射影測定が実現できる．

一方，時間位置基底での射影測定は，パルス列を干渉させずに単一光子検出器で測定することにより実装される．これには，多段 MZI 測定系前段でビームスプリッタによりパルス列を分岐し，分岐したパルス列を単一光子検出器で測定すればよい．このような受信系では，MZI 出力にて光子検出されるか (位相基底測定)，ビームスプリッタ分岐光から光子検出されるか (時間位置基底測定) によって，受動的かつ確率的に測定基底が選択されることになる．5.3.2 節で述べた非対称な基底選択の選択確率は，ビームスプリッタの分岐比で設定される．時間位置基底測定系を加えることによる単一光子検出器数の増加分は高々 1 台，すなわち任意の 2^N 次元の $(d+1)$ 測定基底を 3 個の光子検出器で実装可能であり，スケーラブルであることに変わりはない．

なお，上記構成では，最終段の MZI 出力のうち，全ての入力パルスの干渉が生じるタイムスロットのみを利用するため，その他のタイムスロットでの光子検出は実効的に光子損失となる．実効的な光子損失の大きさは $N \times 3$ dB であるため，光子損失を含めるとスケーラブルな構成とは言い難い．ただし，遅延 MZI の入力部のビームスプリッタを高速な光スイッチで置換することで，原理的には実効的な光子損失のないアダマール基底測定が実現できる [111, 112]．これは次のように理解できる．図 5.4(b) において，2τ 遅延 MZI の入力部ビームスプリッタを高速光スイッチで置換すると，等価な量子ビット q_1 の $|0\rangle$ に対応するパルスを長経路，$|1\rangle$ に対応するパルスを短経路に振り分けることができる．このスイッチによる経路振り分けを行うと，図中の点線で囲われたタイムスロットのみに光子が存在し，それ以外のタイムスロットで光子は検出されない．この操作を τ 遅延 MZI で等価な量子ビット q_0 にも施すことで，アダマール基底測定で用いるタイムスロットでのみ，光子が検出されるようにできる．高速光スイッチは追加の挿入損失を通常伴うが，受動的な構成の実効光子損失との比較から，光スイッチ当たり 3 dB 以下の挿入損失であれば，スイッチを利用した能動的な構成により損失を改善できる．

ここまで，$d(=2^N)$ 次元タイムビン量子状態に対する $(d+1)$ 個の MUB 実装法について述べた．上記の議論は，他の素数の累乗次元にも容易に拡張できる．p が奇素数の場合，式 (5.42) の位相項は $\sum_{j=0}^{N-1} r_j \vec{m}^{\mathrm{T}} \mathbf{A}^{(j)} \vec{m} + \vec{m}\cdot\vec{n}$ で与えられ，この項は 0 から $p-1$ までの値を要素とするベクトルおよび行列から成るため，$p=2$ の場合と同様に整数値となる．この整数値に，$i\frac{2\pi}{p}$ を乗じたものが位相値となるため，$d=p^N$ の場合に取りうる位相値は $\left\{ \frac{2\pi}{p}k \;\middle|\; k\in[0,p-1] \right\}$ の p 値である．したがって，p を固定して N を大きくしても必要な位相精度は変わらない．p が装置実装可能な位相値数より十分小さければ，大きな p^N 次元状態についても，光 IQ 変調器により容易に生成可能である．

上記は $(d+1)$MUB の量子状態生成に関する議論であるが，状態測定についても，$p=2$ の場合と同様に，行列の分解 $\mathbf{B}^{(r)} = \mathbf{D}^{(r)}\mathbf{B}^{(0)}$ が利用できる．$\mathbf{D}^{(r)}$ は対角ユニタリー行列であり，この変換に対応する基底切り替え操作は位相変調器によって実現できる．一方，式 (5.42) より，$\mathbf{B}^{(0)}$ の要素は次式で与えられる．

$$B^{(0)}_{mn} = \frac{1}{\sqrt{p^N}} \exp\left(i\frac{2\pi}{p}\vec{m}\cdot\vec{n} \right) \tag{5.48}$$

上式は，N 個の p 次元フーリエ変換のテンソル積となっている．したがって，2^N 次元アダマール基底状態が $|+\rangle, |-\rangle$ の N プロダクト状態となったのと同様に，p^N 次元タイムビン量子状態と等価な N 個の p 次元量子状態を考えることができ，各 p 次元量子状態のフーリエ基底状態

$$|f_k\rangle = \frac{1}{\sqrt{p}} \sum_m \exp\left(i\frac{2\pi mk}{p} \right) |m\rangle \quad \text{for} \quad k\in[0,p-1] \tag{5.49}$$

の N プロダクト状態が $\left|\psi_n^{(0)}\right\rangle$ となっている．したがって，式 (5.49) で表される p 次元フーリエ基底への射影測定に対応する干渉計を N 個多段に接続することにより，所要の測定系が構築される．3.4.1 節で述べたように，時間エネルギー不確定性を利用した 3 次元量子もつれ状態に対するフーリエ基底測定の実装法として，3 本腕遅延干渉計を用いる手法が報告されている [47]．この手法はタイムビン量子状態にも適用でき，さらに p 本腕遅延干渉計とすることで，p 次元タイムビン量子状態にも拡張できる．この p 本腕遅延干渉計において，$p=2$ であれば，これまで述べてきた遅延 MZI となる．したがって，p が奇素数である高次元状態については，1 台の位相変調器，$\log_p d$ 個の p 本腕遅延干渉計および p 個の光子検出器からなる構成で，全ての位相基底についての射影測定が実現できる．時間位置基底への射影測定が，ビームスプリッタによる分岐で並列実装できることも同様である．このように，提案手法を用いることで，任意の素数の累乗次元について，装置数が次元に対して対数的に増加する構成により，$(d+1)$ 個の MUB 測定が実装できる．

5.5　実験系

前節で提案した 4 次元タイムビン量子状態に対する $(d+1)$MUB 状態生成法および測定法を実験により検証した．本節ではその実験系について述べる．なお，本実験では，量子もつれ状態を利用した QKD プロトコルの実証ではなく，提案した状態生成/測定手法の原理実証を目的とするため，量子もつれ光源に代わり，P&M 型の送信系を用いる．本節の測定系を二つ用意して量子もつれ状態の各光子にそれぞれ適用すれば，EB 型のプロトコルが実装できる．

図 5.5 に実験構成を示す．波長 1559.0 nm の CW レーザ光を $LiNbO_3$ 光 IQ 変調器により変調し，時間位置基底状態に対応する単一パルス，もしくは位相基底状態に対応する 4 連続パルス列を，パルス幅 33 ps/パルス間隔 500 ps および繰り返し周波数 250 MHz で生成する．上述のように，QKD プロトコルの実装ではなく提案する生成/測定系の原理実証が目的であるため，ここではランダムな変調パターンではなく，時間位置基底状態および位相基底状態を順に生成する変調パターンを用いた．生成したパルス列は 2 台の光可変減衰器 (VATT) により，平均光子数が 1 M photons/s の微弱コヒーレント光となるように減衰される．

生成した微弱コヒーレント光は，二つの測定系によって検出される．一つは，位相基底への射影測定系である．まず微弱コヒーレント光の偏波を偏波コントローラ (PC) によって調整した後，$LiNbO_3$ 位相変調器 (PM) に入力する．ここでの位相変調パターンによって，対角ユニタリー行列 $\mathbf{D}^{(r)}$ に対応した位相基底切り替えを行う．位相変調された微弱コヒーレント光は，遅延時間 1 ns，伝搬遅延位相 0 の PLC-MZI に入力される．この PLC-MZI からの出力を光ディレイライン (DL) に入力し，約 250 ps の相対遅延を与えたのち，遅延時間 500 ps，伝搬遅延位相 0 の PLC-MZI に入力する．この出力を超伝導ナノワイヤ単一光子検出器 (SNSPD) で検出し，光子検出時刻をタイムインターバルア

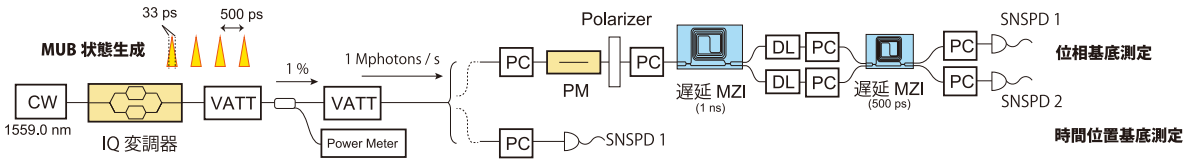

図 5.5　4 次元タイムビン量子状態に対する MUB 状態生成/測定の実験系．点線部はファイバパッチケーブルの接続によって選択される．CW: CW レーザ光源，IQ 変調器: $LiNbO_3$ in-phase and quadrature-phase 変調器，VATT: 可変光減衰器，PC: 偏波コントローラ，PM: $LiNbO_3$ 位相変調器，MZI: 遅延 Mach-Zehnder 干渉計，DL: 光ディレイライン，SNSPD: 超伝導ナノワイヤ単一光子検出器

ナライザ (TIA) で 60 秒間記録して，前節で述べた位相基底状態への射影測定を行う．2 つの SNSPD の検出効率はともに 56 %，ダークカウント率は 100 cps 以下であった．また，SNSPD1，2 での，シングルカウントレートはそれぞれ 52，47 kcps であった．一方，時間位置基底への射影測定では，PM および MZI を取り除き，パルス列を直接 SNSPD に入力して光子検出時刻を TIA にて記録した．この時のシングルカウントレートは 546 kcps であった．なお，SNSPD や TIA 等の電気回路で生じるタイミングジッタのため，TIA で記録された光子検出時刻のヒストグラムの半値全幅は，入力光パルス幅 33 ps よりも広い 78 ps であった．

5.6 実験結果

本節では，前節で述べた実験系の測定結果について述べる．

図 5.6(a) に，光子が r_a 番目基底の n_a 番目状態として準備され，かつ測定基底が r_b 番目基底とした時に，光子が n_b 番目状態として検出された条件付確率 $\Pr(n_b|r_a, n_a, r_b)$ を示す．ここで，$r_a(r_b) = 0$ が時間位置基底であり，式 (5.41) で表される r 番目位相基底は $r_a(r_b) = r + 1$ により対応付けられる．生成量子状態 $\left|\psi_{n_a}^{(r_a)}\right\rangle$ と測定量子状態 $\left|\psi_{n_b}^{(r_b)}\right\rangle$ が同じ基底，すなわち $r_a = r_b$ の場合，これらは正規直交基底であることから，$\left|\left\langle\psi_{n_a}^{(r_a)}\middle|\psi_{n_b}^{(r_b)}\right\rangle\right|^2 = \delta_{n_a,n_b}$ となる．図 5.6(a) のブロック対角項では，このような特性を示す確率分布が観測されており，それぞれの基底が正規直交基底となっていることが分かる．一方，生成量子状態 $\left|\psi_{n_a}^{(r_a)}\right\rangle$ と測定量子状態 $\left|\psi_{n_b}^{(r_b)}\right\rangle$ が異なる基底，すなわち $r_a \neq r_b$ の場合，MUB の条件式 (5.1) より，$\left|\left\langle\psi_{n_a}^{(r_a)}\middle|\psi_{n_b}^{(r_b)}\right\rangle\right|^2 = 1/d$ となる．図 5.6(a) の非ブロック対角項では，このような一様分布に近い確率分布が観測されている．したがって，本実験により 5 つの 4 次元 MUB から予想される確率分布を，簡便な生成/測定系を用いて観測できたと言える．

QKD に応用する際の重要な性能指標はシンボルエラーレートであり，これは図 5.6(a) のブロック対角項から見積もることができる．図 5.6(b) に，見積もられた各基底ごとの平均シンボルエラーレートを示す．SNSPD の低ダークカウント，低ジッタ特性のために，時間位置基底 ($r_b = 0$) にて 0.6 % という，QKD としては低いシンボルエラーレートが得られている．一方，$r_b = 1$ の位相基底，すなわちアダマール基底では，2.3 % とやや高く，その他の位相基底 ($r_b = 2, 3, 4$) ではさらに高いエラーレート (4.5, 4.0, 4.3 %) となっている．アダマール基底でのやや高いシンボルエラーレートの原因としては，IQ 変調器で生成したパルス振幅の不均一性や，4.2.3 節で述べた遅延 MZI における経路に依存する伝搬損失による消光比劣化などが考えられる．これらは，IQ 変調器への印加信号の最適化や，遅延 MZI 内の光経路での対称 MZI 型可変減衰器の利用 [113, 114] などによ

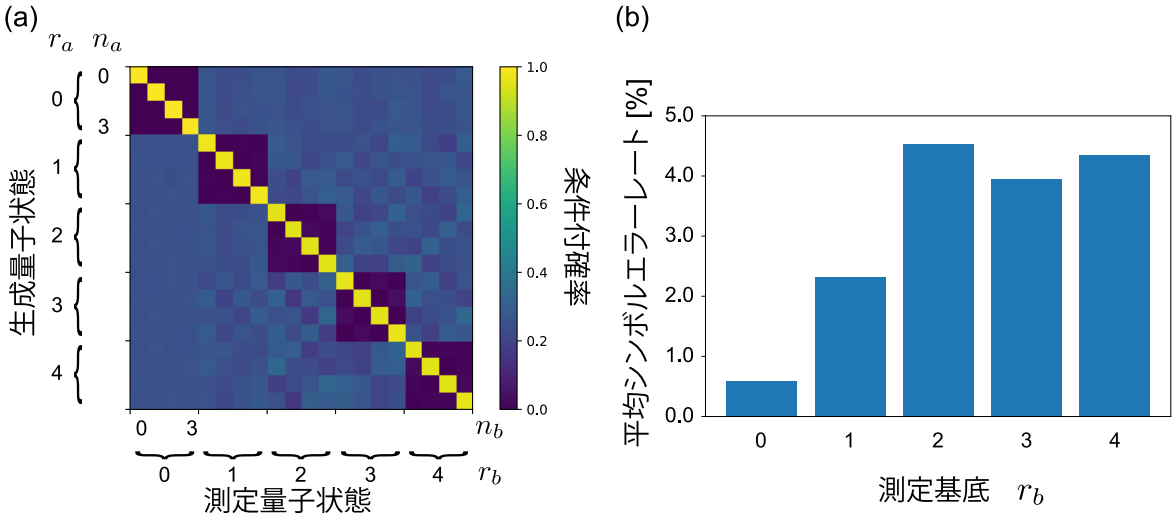

図 5.6　実験結果．(a) 光子検出の条件付確率分布 $\Pr(n_b|r_a, n_a, r_b)$ (b) 基底一致時 $(r_a = r_b)$ の平均シンボルエラーレート $1 - \frac{1}{4}\sum_{n_a=n_b} \Pr(n_b|r_a, n_a, r_b)$

り，改善できる余地がある．アダマール基底以外の位相基底測定での高いエラーレートは，送信側 IQ 変調器および受信側位相変調器の不整合が原因と考えられる．5.4 節で述べた通り，4 次元アダマール基底状態は，等価な 2 量子ビット上の $|+\rangle, |-\rangle$ のプロダクト状態であり，各パルスの確率振幅は全て実数である．そのため，送信側 IQ 変調器は実質的には強度変調器として動作し，受信側位相変調器は無変調でよい．一方，その他の位相基底状態の確率振幅は複素数であり，送受信において，適切に位相変調する必要がある．この位相変調ずれにより，測定エラーが増加したものと考えられる．このエラーレートは変調器の動作条件の最適化によって改善される余地がある．

以上述べたように，基底によってばらつきはあるものの，どの基底においても，5.3.3 節で求めた QKD 動作閾値である 23.17 % より十分小さなシンボルエラーレートが得られた．したがって，提案手法により，$(d+1)$ 測定基底 QKD プロトコルに適用可能な MUB 状態生成/測定系が実証されたと言える．

5.3.2 節で述べた通り，図 5.6(a) のブロック対角項の実験結果に対して，式 (5.20) を用いて λ_{jk} を導出することで，2 種類のエラーの相関の詳細を取り込んだ鍵生成率 [式 (5.31)] の評価ができる．表 5.1 に結果を示す．表から，λ_{00} が支配的な項であり，等価な EB 型プロトコルで言えば，エラーのない一般化ベル基底状態 $\left|\Psi^{00}\right\rangle$ に近い状態が測定されているため，高い鍵生成率が期待される．しかしながら，得られた値のうちいくつかは負の値となっており，これは非物理的な結果である．4.2.4 節で述べた QST における問題と類似の問題と言え，原因として，理想的な状態生成/測定からのずれや，統計的な揺らぎによるずれなどが考えられる．この負の値のために，この結果から式 (5.31) により

表 5.1 実験結果から見積もられた一般化ベル基底の係数 λ_{jk}

	k			
j	0	1	2	3
0	0.9606	0.0084	0.0159	0.0091
1	0.0052	-0.0039	0.0049	-0.0040
2	0.0047	0.0046	-0.0053	-0.0022
3	0.0063	-0.0029	-0.0047	0.0033

秘密鍵生成率を求めることはできない．QST の場合には，三角行列により正定値化した上で，最尤推定により物理的な制約の中で尤もらしいパラメータを求めた．一方，秘密鍵生成率を求めるにあたって重要な点は安全性であり，例え尤もらしい値であっても，真に生成可能な秘密鍵生成率よりも大きな生成率を見積もってしまった場合，その差の分だけ最終的な秘密鍵は盗聴されていることとなる．そのため，上記ずれの問題を考慮した秘密鍵生成率評価手法の開発が，より実用的な QKD 実装のための今後の課題と言える．

5.7 結言

本章では，d 次元タイムビン量子状態を用いる $(d+1)$ 測定基底 QKD プロトコルおよびその実装法について述べた．QKD において最も重要な事柄は安全性である．そこで，まずプロトコルの具体的な手順について述べた後，さらに有限体を利用して一般化した Weyl 演算子および一般化ベル基底を用いて，素数の累乗次元における $(d+1)$ 測定基底 QKD プロトコルの安全性証明を展開した．また，上記安全性証明を応用して 2 測定基底 QKD プロトコルの秘密鍵生成率を導出し，二つのプロトコルの相違点として，推定されるエラーの相関特性の差について議論した．

続いて，安全性証明で用いた MUB と等価な別の MUB の表現が持つ構造を利用して，p^N 次元タイムビン量子状態に対して，装置数が次元数に対して対数的に増加する，$(d+1)$MUB の基底状態への射影測定装置を提案した．提案手法を 4 次元タイムビン量子状態に対して実装し，光子検出の条件付確率分布およびシンボルエラーレートを評価した．5 つの基底全てにおいて，秘密鍵を生成するための平均シンボルエラーレート閾値 23.17 % より小さなシンボルエラーレートを観測し，提案手法を用いて $(d+1)$ 測定基底 QKD プロトコルのための，高次元タイムビン量子状態生成/測定が可能であることを実証した．

第 6 章

結論

本論文は，筆者が大阪大学 大学院工学研究科 電気電子情報通信工学専攻在学中および NTT 物性科学基礎研究所在籍中に行った，量子もつれを用いた高次元量子鍵配送のためのスケーラブルなタイムビン量子状態制御に関する研究成果をまとめたものである．以下，本研究で得られた成果を総括する．

第 2 章では，本論文の研究対象であるタイムビン量子状態に関する量子情報理論の基礎事項について述べた．特に，これまで深く研究が進んでいる，2 次元タイムビン量子状態および 2 次元量子もつれ状態を題材にして，量子もつれ状態の持つ特異な性質である，部分系のランダム性，もつれた光子間の強い相関性，およびその他の系と相関を持たないモノガミー性の議論を展開した．さらに，2 次元量子もつれ状態を利用した QKD プロトコルの代表例である，BBM92 の具体的な鍵生成手順について述べたのち，量子もつれ状態により QKD システムが実装できるのみならず，量子もつれ状態を用いない QKD プロトコルの安全性を証明できる点を明示した．

第 3 章では，高次元量子もつれ QKD の信号生成に対応する，高次元タイムビン量子もつれ状態の生成制御および CGLMP 不等式による検証について述べた．まず，局所的な隠れた変数理論と，2 次元量子もつれ状態の検証に用いられる CHSH 不等式について詳述した後，高次元量子もつれ状態の検証に用いられる CGLMP 不等式およびその破れを最大化する最適量子もつれ状態について議論した．また，自発的パラメトリック下方変換および多段接続した遅延 MZI を用いた測定による CGLMP 不等式の破れの検証実験を行い，最大量子もつれ状態と最適量子もつれ状態の破れの差が明確に観測されるような，安定かつ高品質な高次元タイムビン量子もつれ状態の生成/制御が可能であることを明らかにした．

第 4 章では，高次元量子もつれ QKD の信号伝送に関わる事項として，量子状態トモグラフィー (QST) を用いた高次元量子もつれ状態の長距離伝送特性評価について述べた．まず，既存の 2 次元タイムビン量子状態に対する遅延 MZI を用いた QST について述べ

たのち，多段遅延 MZI を用いて効率的に高次元タイムビン量子状態に拡張する手法を提案した．次に，伝送特性評価に用いる各種指標について議論し，提案手法の原理実証実験および 100 km ファイバ伝送後の特性評価実験を行った．提案 QST によって得られた伝送後の状態密度演算子をもとに評価したコヒーレント情報量から，伝送後も，2 次元量子状態では得られない 1 ビット以上の QKD 秘密鍵生成に利用可能な，高品質な高次元タイムビン量子状態が保持されていることを明らかにした．

第 5 章では，高次元量子もつれ QKD の信号測定に関連して，$(d+1)$ 測定基底 QKD プロトコルのための相互不偏基底 (MUB) 測定について述べた．まず，$(d+1)$ 測定基底 QKD プロトコルの具体的な鍵生成手順について述べたのち，有限体を用いた一般化 Weyl 演算子および一般化ベル基底について述べ，これらを利用して上記プロトコルの安全性証明適用可能範囲を素数次元から素数の累乗次元へと拡張した．また，上記安全性証明で利用される MUB の，高次元タイムビン量子状態に対する効率的な実装法を提案した．4 次元タイムビン量子状態の場合に提案手法を実装し，QKD 秘密鍵生成に必要な値よりも十分低いシンボルエラーレートが達成できることを明らかにした．

以上の研究成果により，高次元量子もつれ QKD に向けた通信の 3 つの基本動作である状態生成 (送信)/伝送/測定 (受信) に関して，高次元タイムビン量子状態を用いたシステムが高品質で安定かつスケーラブルに構築できる可能性が示された．今後は，これらの各要素を実際に組合せ，高速で安全な QKD システムとして評価していくことが課題となる．QKD は，一時は “無条件安全な” 暗号通信と呼ばれることもあったが，近年ではこのような呼称は避ける傾向にある．これは，第 2 章や第 5 章で触れたように，本論文での安全性の議論は，状態生成/測定装置が理想的に動作した時の，“通信路に対するあらゆる盗聴法に対して” 安全性を評価したものであり，これらの装置に関する暗黙の仮定が破れたとき，システムの安全性は必ずしも保証されないためである．そのため，本論文の要素を単に組み合わせることで，直ちに実用的な QKD 装置として動作するというものではなく，システム全体としての安全性の評価が不可欠である．第 2 章でも触れたように，このようなより高い安全性を確保するために，装置の不完全性も議論に取り込んだ安全性解析や，装置についての仮定を極力なくした装置無依存型 QKD などが，2 次元 QKD や 2 測定基底プロトコルについて進展を見せており，本論文で議論した $(d+1)$ 測定基底プロトコルにおいても同様の進展が期待される．このプロトコルに限らず，QKD の最終目標である高速で安全な暗号通信には，実装の技術的課題に加え標準化やアプリケーションへの応用研究など広い領域で課題が存在するが，本論文の研究成果が将来の安全な情報通信を支える研究の一助となれば幸いである．

付録 A

2 種類の相互不偏基底の等価性証明

付録 A では，式 (5.42) で表される確率振幅を持つ位相基底と，式 (5.8) で表される確率振幅を持つ位相基底が，インデックスの並び替え以外は等価であることを示す．これらの位相基底は，次元数 $d = p^N$ の場合，p が 2 か奇素数かによって表式が異なる．そこでまず，A.1 節にて $p = 2$ の場合について述べる．p が奇素数の場合の等価性は既に文献 [103] で知られているが，簡潔な証明を A.2 節で紹介する．

各論の前に，どちらの場合についても共通する事項について述べておく．$d = p^N$ 次元ヒルベルト空間 MUB の考察にあたっては，位数 p^N の有限体 $GF(p^N)$ を考える．位相基底や状態のインデックスは $GF(2^N)$ の元，例えば $r \in [0, d-1]$ とする．r は有限体 $GF(p^N)$ の元であり，また整数 $\mathbb{Z}$ の元でもあるとする．原則として，有限体の元として扱う場合には四則演算子 $\oplus, \ominus, \odot, \oslash$ を用いることとし，整数 $\mathbb{Z}$ の元として扱う場合には四則演算子 $+, -, \times, /$ や総和演算子 $\sum$ 等を用いる．$\pi/2$ などの実数値との積は実数値として扱うものとする．また，整数や有限体の元としてだけでなく，$r = \sum_{n=0}^{N-1} r_n p^n$ に対して，そのベクトル表現 $\vec{r} = (r_0, r_1, \cdots, r_{N-1})^T$ も用いる．有限体上の加算 $\oplus$ は，このベクトル表現において要素ごとの和を取ったのち，各要素の剰余 $\bmod p$ により与えられる．また，有限体上の乗法の構造を反映した，$N \times N$ 対称行列の集合 $\{\mathbf{A}^{(k)}\}_{k=0}^{N-1}$ を次式によって定める．

$$p^m \odot p^n = \oplus_{k=0}^{N-1} A_{mn}^{(k)} p^k \tag{5.43}$$

ただし，$A_{mn}^{(k)}$ は行列 $\mathbf{A}^{(k)}$ の m 行 n 列目の要素である．$\mathbf{A}^{(k)}$ は可逆である．すなわち，写像 $f_k : GF[p^N] \to GF[p^N]$ を

$$f_k(r) = \mathbf{A}^{(k)} \vec{r} \bmod p = \oplus_{m,n=0}^{N-1} A_{mn}^{(k)} r_n p^m \tag{A.1}$$

によって定めた時，この写像は全単射である．

また，1 の p 乗根を $\gamma = \exp\left(i\frac{2\pi}{p}\right)$ と表す．繰り返し用いる性質として，γ はべき乗の周期が p であるから，$r \in GF(p^N)$ に対し r の最小桁 r_0 を用いて，$\gamma^r = \gamma^{r_0}$ が成り立つ．

A.1　2 の累乗次元の場合

$r, i, j \in \{0, \ldots, 2^N - 1\}$，$r$ 番目位相基底における j 番目基底状態を $\left|\psi_j^{(r)}\right\rangle = \sum_i B_{ij}^{(r)} |i\rangle$ とし，$B_{ij}^{(r)}$ を次式とすると，これらの位相基底は MUB を成す [102].

$$B_{ij}^{(r)} := \frac{1}{\sqrt{2^N}} \exp\left\{ i\frac{\pi}{2} \left(\sum_{k=0}^{N-1} r_k \vec{i}^T \mathbf{A}^{(k)} \vec{i} + 2\vec{i} \cdot \vec{j} \right) \right\} \tag{A.2}$$

一方，r 番目位相基底における j 番目基底状態を $\left|e_j^{(r)}\right\rangle = \sum_i H_{ij}^{(r)} |i\rangle$ とし，$H_{ij}^{(r)}$ を次式とすると，これらの位相基底は MUB を成す [101].

$$H_{ij}^{(r)} := \frac{1}{\sqrt{2^N}} \left\{ \alpha_{\ominus i}^r \right\}^* \gamma^{\ominus i \odot j} \tag{A.3}$$

ただし，

$$\alpha_i^r := \prod_{m,n=0}^{N-1} i^{r \odot (i_m 2^m) \odot (i_n 2^n)} \tag{A.4}$$

である．

以下では，これらの位相基底が等価である，すなわち $B_{ij'}^{(r')}, H_{ij}^{(r)}$ について，ある r, r' 間および j, j' 間の置換に対応する写像が存在することを示す．まず，$GF(2^N)$ では加算 $\oplus$ と減算 $\ominus$ が等しいことより，次式が成り立つ．

$$\begin{aligned} \gamma^{\ominus i \odot j} &= \gamma^{i \odot j} \\ &= \exp\left(i\pi \left(\vec{i}^T \mathbf{A}^{(0)} \vec{j} \right) \right) \\ &= \exp\left(i\pi \left(\vec{i} \cdot \overrightarrow{f_0(j)} \right) \right) \end{aligned} \tag{A.5}$$

また，

$$\begin{aligned} \left\{ \alpha_{\ominus i}^r \right\}^* &= \left\{ \alpha_i^r \right\}^* \\ &= \prod_{m,n=0}^{N-1} (-i)^{r \odot (i_m 2^m) \odot (i_n 2^n)} \\ &= \prod_{m,n=0}^{N-1} (-1)^{\sum_{k,l=0}^{N-1} r_k A_{kl}^{(1)} i_m A_{mn}^{(l)} i_n} \\ &\quad \times \prod_{m,n=0}^{N-1} (-i)^{\sum_{k=0}^{N-1} r'_k i_m A_{mn}^{(k)} i_n \mod 2} \end{aligned} \tag{A.6}$$

が成り立つ．ただし，$r' = f_0(r)$ とした．$\mathbf{A}^{(k)}$ が対称行列であることを用いると，式 (A.6) の第 1 項は次式のように表される．

$$\begin{aligned}\prod_{m,n=0}^{N-1}(-1)^{\sum_{k,l=0}^{N-1} r_k A_{kl}^{(1)} i_m A_{mn}^{(l)} i_n} &= \prod_{n=0}^{N-1}(-1)^{\sum_{k,l=0}^{N-1} r_k A_{kl}^{(1)} A_{nn}^{(l)} i_n^2} \\ &= \exp\left(i\pi\left(\vec{i}\cdot\vec{a}\right)\right) \end{aligned} \tag{A.7}$$

ただし，$a_n = \sum_{k,l=0}^{N-1} r_k A_{kl}^{(1)} A_{nn}^{(l)} \bmod 2$ とした．また，$\mathbf{A}^{(k)}$ が対称行列であることから，次式が成り立つ．

$$\begin{aligned}\prod_{n\neq m}(-i)^{\sum_{k=0}^{N-1} r'_k i_m A_{mn}^{(k)} i_n \bmod 2} &= \prod_{n\leq m}(-1)^{\sum_{k=0}^{N-1} r'_k i_m A_{mn}^{(k)} i_n \bmod 2} \\ &= \prod_{n\leq m}(-1)^{\sum_{k=0}^{N-1} r'_k i_m A_{mn}^{(k)} i_n} \\ &= \prod_{n\neq m} i^{\sum_{k=0}^{N-1} r'_k i_m A_{mn}^{(k)} i_n} \end{aligned} \tag{A.8}$$

したがって，式 (A.6) の第 2 項を，次式のように表すことができる．

$$\begin{aligned}\prod_{m,n=0}^{N-1}(-i)^{\sum_{k=0}^{N-1} r'_k i_m A_{mn}^{(k)} i_n \bmod 2} &= \prod_{n=0}^{N-1}(-i)^{\sum_{k=0}^{N-1} r'_k A_{nn}^{(k)} i_n \bmod 2} \prod_{m\neq n} i^{\sum_{k=0}^{N-1} r'_k i_m A_{mn}^{(k)} i_n} \\ &= \exp\left\{i\frac{\pi}{2}\left(\sum_{k=0}^{N-1} r'_k \vec{i}^{\,T} A^{(k)} \vec{i}\right)\right\} \\ &\times \prod_{n=0}^{N-1}(-i)^{(\sum_{k=0}^{N-1} r'_k A_{nn}^{(k)} i_n \bmod 2)+\sum_{k=0}^{N-1} r'_k A_{nn}^{(k)} i_n} \\ &= \exp\left\{i\frac{\pi}{2}\left(\sum_{k=0}^{N-1} r'_k \vec{i}^{\,T} A^{(k)} \vec{i}\right)\right\} \exp\left(\pi i\left(\vec{i}\cdot\vec{b}\right)\right) \end{aligned} \tag{A.9}$$

ただし，

$$b_n = \begin{cases} 0 & \text{if} \quad \sum_{k=0}^{N-1} r'_k A_{nn}^{(k)} \in \{0,3\} \mod 4 \\ 1 & \text{if} \quad \sum_{k=0}^{N-1} r'_k A_{nn}^{(k)} \in \{1,2\} \mod 4 \end{cases} \tag{A.10}$$

とした．

式 (A.2) で表される確率振幅と，式 (A.3) の確率振幅を変形して得られる式 (A.5)–(A.7) および式 (A.9) を比較すると，次式の写像によるインデックスの割り当てにより，$H_{ij}^{(r)} = B_{ij'}^{(r')}$ が成り立つことが分かる．

$$r' = f_0(r) \tag{A.11}$$

$$j' = f_0(j) \oplus a \oplus b \tag{A.12}$$

f_0 が全単射であることから，上記 2 式の写像はともに全単射である．したがって，$\left\{\left\{\left|e_j^{(r)}\right\rangle \,\middle|\, j\right\} \,\middle|\, r\right\}$ と $\left\{\left\{\left|\psi_{j'}^{(r')}\right\rangle \,\middle|\, j'\right\} \,\middle|\, r'\right\}$ は，基底および状態のインデックスの置換のもとで，同一の MUB である．

A.2　奇素数の累乗次元の場合

$r, i, j \in \{0, \ldots, 2^N - 1\}$，$r$ 番目位相基底における j 番目基底状態を $\left|\psi_j^{(r)}\right\rangle = \sum_i B_{ij}^{(r)} |i\rangle$ とし，$B_{ij}^{(r)}$ を次式とすると，これらの位相基底は MUB を成す [102].

$$B_{ij}^{(r)} := \frac{1}{\sqrt{p^N}} \exp\left\{ i\frac{2\pi}{p} \left(\sum_{k=0}^{N-1} r_k \vec{i}^T A^{(k)} \vec{i} + \vec{i} \cdot \vec{j} \right) \right\} \tag{A.13}$$

一方，r 番目位相基底における j 番目基底状態を $\left|e_j^{(r)}\right\rangle = \sum_i H_{ij}^{(r)} |i\rangle$ とし，$H_{ij}^{(r)}$ を次式とすると，これらの位相基底は MUB を成す [101, 103].

$$H_{ij}^{(r)} := \frac{1}{\sqrt{p^N}} \left\{\alpha_{\ominus i}^r\right\}^* \gamma^{\ominus i \odot j} \tag{A.14}$$

ただし，

$$\alpha_i^r := \gamma^{\ominus(r \odot i \odot i) \oslash 2} \tag{A.15}$$

である．この場合，γ のべき乗の周期性と式 (A.1) から，次式が成り立つ．

$$\begin{aligned} \left\{\alpha_{\ominus i}^r\right\}^* &= \gamma^{(r \oslash 2) \odot i \odot i} \\ &= \exp\left(i\frac{2\pi}{p} \sum_{k=0}^{N-1} f_0(r \oslash 2)_k \vec{i}^T A^{(k)} \vec{i} \right) \qquad \text{(A.16)} \\ \gamma^{\ominus i \odot j} &= \exp\left\{ i\frac{2\pi}{p} \left(\vec{i} \cdot \overrightarrow{f_0(\ominus j)} \right) \right\} \qquad \text{(A.17)} \end{aligned}$$

したがって，次式の写像によるインデックスの割り当てにより，$H_{ij}^{(r)} = B_{ij'}^{(r')}$ が成り立つことが分かる．

$$r' = f_0(r \oslash 2) \tag{A.18}$$
$$j' = f_0(\ominus j) \tag{A.19}$$

f_0 が全単射であることから，上記 2 式の写像はともに全単射である．したがって，$\left\{\left\{\left|e_j^{(r)}\right\rangle \,\middle|\, j\right\} \,\middle|\, r\right\}$ と $\left\{\left\{\left|\psi_{j'}^{(r')}\right\rangle \,\middle|\, j'\right\} \,\middle|\, r'\right\}$ は，基底および状態のインデックスの置換のもとで，同一の MUB である．

参考文献

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. (Cambridge University Press, Cambridge, 2010).

[2] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Quantum supremacy using a programmable superconducting processor, Nature **574**, 505 (2019).

[3] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994) pp. 124–134.

[4] C. E. Shannon, Communication theory of secrecy systems, The Bell System Technical Journal **28**, 656 (1949).

[5] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers Systems and Signal Processing* (Bangalore India, 1984) pp. 175–179.

[6] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature **299**, 802 (1982).

[7] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, Physical Review **47**, 777 (1935).

[8] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without Bell's theorem, Physical Review Letters **68**, 557 (1992).

[9] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Physical Review Letters **91**, 057901 (2003).

[10] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Physical Review Letters **94**, 230504 (2005).

[11] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Physical Review A **72**, 012326 (2005).

[12] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

[13] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Physical Review Letters **85**, 441 (2000).

[14] 小芦雅斗, 小柴健史, **量子暗号理論の展開** (サイエンス社, 2008).

[15] A. K. Ekert, Quantum cryptography based on Bell's theorem, Physical Review Letters **67**, 661 (1991).

[16] D. Bruß, Optimal eavesdropping in quantum cryptography with six states, Physical Review Letters **81**, 3018 (1998).

[17] D. G. Enzer, P. G. Hadley, R. J. Hughes, C. G. Peterson, and P. G. Kwiat, Entangled-photon six-state quantum cryptography, New Journal of Physics **4**, 45 (2002).

[18] K. Inoue, E. Waks, and Y. Yamamoto, Differential phase shift quantum key distribution, Physical Review Letters **89**, 037902 (2002).

[19] 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**, 343 (2007).

[20] T. Schmitt-Manderbach, H. Weier, M. Fürst, 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, Physical Review Letters **98**, 010504 (2007).

[21] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Physical Review Letters **108**, 130503 (2012).

[22] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, Nature **509**, 475 (2014).

[23] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Experimental quantum key distribution without monitoring signal disturbance, Nature Photonics **9**, 827 (2015).

[24] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-device-independent quantum key distribution over a 404 km optical fiber, Physical Review Letters **117**, 190501 (2016).

[25] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Satellite-to-ground quantum key distribution, Nature **549**, 43 (2017).

[26] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure quantum key distribution over 421 km of optical fiber, Physical Review Letters **121**, 190502 (2018).

[27] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and Y. Henry, Current status of the DARPA quantum network, in *Proc. SPIE 5815, Quantum Information and Computation III*, Vol. 5815 (2005).

[28] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, Long-term performance of the SwissQuantum quantum key distribution network in a field environment, New Journal of Physics **13**, 123001 (2011).

[29] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, Field test of quantum key distribution in the Tokyo

QKD Network, Optics Express **19**, 10387 (2011).

[30] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature **589**, 214 (2021).

[31] N. T. Islam, C. Cahall, A. Aragoneses, A. Lezama, J. Kim, and D. J. Gauthier, Robust and stable delay interferometers with application to d-dimensional time-frequency quantum key distribution, Physical Review Applied **7**, 044010 (2017).

[32] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, Science Advances **3**, e1701491 (2017).

[33] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, Efficient time-bin encoding for practical high-dimensional quantum key distribution, Physical Review Applied **14**, 014051 (2020).

[34] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, High-dimensional quantum cryptography with twisted light, New Journal of Physics **17**, 033033 (2015).

[35] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, High-dimensional intracity quantum cryptography with structured photons, Optica **4**, 1006 (2017).

[36] Q.-K. Wang, F.-X. Wang, J. Liu, W. Chen, Z.-F. Han, A. Forbes, and J. Wang, High-dimensional quantum cryptography with hybrid orbital-angular-momentum states through 25 km of ring-core fiber: A proof-of-concept demonstration, Physical Review Applied **15**, 064034 (2021).

[37] S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, Quantum key distribution session with 16-dimensional photonic states, Scientific Reports **3**, 2316 (2013).

[38] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits, npj Quantum Information **3**, 25 (2017).

[39] G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. F. da Silva, G. B. Xavier, and G. Lima, High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers, Physical Review A **96**, 022317 (2017).

[40] X.-M. Hu, C. Zhang, Y. Guo, F.-X. Wang, W.-B. Xing, C.-X. Huang, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, X. Gao, M. Pivoluska, and M. Huber, Pathways for entanglement-based quantum communication in the face of high noise, Physical Review Letters **127**, 110505 (2021).

[41] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of quantum key distribution using d-level systems, Physical Review Letters **88**, 127902 (2002).

[42] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, Physical Review A **82**, 030301(R) (2010).

[43] A. Ferenczi and N. Lütkenhaus, Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning, Physical Review A **85**, 052310 (2012).

[44] R. Wang, Z.-Q. Yin, H. Liu, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Tight finite-key analysis for generalized high-dimensional quantum key distribution, Physical Review Research **3**, 023019 (2021).

[45] H. de Riedmatten, I. Marcikic, V. Scarani, W. Tittel, H. Zbinden, and N. Gisin, Tailoring photonic entanglement in high-dimensional Hilbert spaces, Physical Review A **69**, 050304(R) (2004).

[46] R. T. Thew, A. Acín, H. Zbinden, N. Gisin, E. Polzik, R. T. Thew, A. Acin, H. Zbinden, and N. Gisin, Experimental realization of entangled qutrits for quantum communication, Quantum Information and Computation **4**, 93 (2004).

[47] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin, Bell-type test of energy-time entangled qutrits, Physical Review Letters **93**, 010503 (2004).

[48] D. Richart, Y. Fischer, and H. Weinfurter, Experimental implementation of higher dimensional time-energy entanglement, Applied Physics B **106**, 543 (2012).

[49] S. J. Nowierski, N. N. Oza, P. Kumar, and G. S. Kanter, Tomographic reconstruction of time-bin-entangled qudits, Physical Review A **94**, 042328 (2016).

[50] C. Bernhard, B. Bessire, T. Feurer, and A. Stefanov, Shaping frequency-entangled qudits, Physical Review A **88**, 032322 (2013).

[51] B. Bessire, C. Bernhard, T. Feurer, and A. Stefanov, Versatile shaper-assisted

discretization of energy-time entangled photons, New Journal of Physics **16**, 033017 (2014).

[52] R.-B. Jin, R. Shimizu, M. Fujiwara, M. Takeoka, R. Wakabayashi, T. Yamashita, S. Miki, H. Terai, T. Gerrits, and M. Sasaki, Simple method of generating and distributing frequency-entangled qudits, Quantum Science and Technology **1**, 015004 (2016).

[53] M. Kues, C. Reimer, P. Roztocki, L. R. Cortés, S. Sciara, B. Wetzel, Y. Zhang, A. Cino, S. T. Chu, B. E. Little, D. J. Moss, L. Caspani, J. Azaña, and R. Morandotti, On-chip generation of high-dimensional entangled quantum states and their coherent control, Nature **546**, 622 (2017).

[54] P. Imany, J. A. Jaramillo-Villegas, O. D. Odele, K. Han, D. E. Leaird, J. M. Lukens, P. Lougovski, M. Qi, and A. M. Weiner, 50-GHz-spaced comb of high-dimensional frequency-bin entangled photons from an on-chip silicon nitride microresonator, Optics Express **26**, 1825 (2018).

[55] A. Vaziri, G. Weihs, and A. Zeilinger, Experimental two-photon, three-dimensional entanglement for quantum communication, Physical Review Letters **89**, 240401 (2002).

[56] M. Agnew, J. Leach, M. McLaren, F. S. Roux, and R. W. Boyd, Tomography of the quantum state of photons entangled in high dimensions, Physical Review A **84**, 062101 (2011).

[57] A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, and E. Andersson, Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities, Nature Physics **7**, 677 (2011).

[58] R. Fickler, R. Lapkiewicz, W. N. Plick, M. Krenn, C. Schaeff, S. Ramelow, and A. Zeilinger, Quantum entanglement of high angular momenta, Science **338**, 640 (2012).

[59] M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, and A. Zeilinger, Generation and confirmation of a (100×100)-dimensional entangled quantum system, Proceedings of the National Academy of Sciences **111**, 6243 (2014).

[60] X.-M. Hu, W.-B. Xing, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, P. Erker, and M. Huber, Efficient generation of high-dimensional entanglement through multipath down-conversion, Physical Review Letters **125**, 090503 (2020).

[61] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Generation of hyperentangled photon pairs, Physical Review Letters **95**, 260501 (2005).

[62] S. Dong, L. Yu, W. Zhang, J. Wu, W. Zhang, L. You, and Y. Huang,

Generation of hyper-entanglement in polarization/energy-time and discrete-frequency/energy-time in optical fibers, Scientific Reports **5**, 9195 (2015).

[63] F. Steinlechner, S. Ecker, M. Fink, B. Liu, J. Bavaresco, M. Huber, T. Scheidl, and R. Ursin, Distribution of high-dimensional entanglement via an intra-city free-space link, Nature Communications **8**, 15971 (2017).

[64] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, R. Ursin, M. Malik, and A. Zeilinger, Twisted light transmission over 143 km, Proceedings of the National Academy of Sciences **113**, 13648 (2016).

[65] J. S. Bell, On the Einstein Podolsky Rosen paradox, Physics Physique Fizika **1**, 195 (1964).

[66] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Bell inequalities for arbitrarily high-dimensional systems, Physical Review Letters **88**, 040404 (2002).

[67] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, Entanglement distribution over 300 km of fiber, Optics Express **21**, 23241 (2013).

[68] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Satellite-based entanglement distribution over 1200 kilometers, Science **356**, 1140 (2017).

[69] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, Distribution of time-bin entangled qubits over 50 km of optical fiber, Physical Review Letters **93**, 180502 (2004).

[70] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, High-fidelity transmission of entanglement over a high-loss free-space channel, Nature Physics **5**, 389 (2009).

[71] J. F. Dynes, H. Takesue, Z. L. Yuan, A. W. Sharpe, K. Harada, T. Honjo, H. Kamada, O. Tadanaga, Y. Nishida, M. Asobe, and A. J. Shields, Efficient entanglement distribution over 200 kilometers, Optics Express **17**, 11440 (2009).

[72] A. Cuevas, G. Carvacho, G. Saavedra, J. Cariñe, W. Nogueira, M. Figueroa, A. Cabello, P. Mataloni, G. Lima, and G. Xavier, Long-distance distribution of genuine energy-time entanglement, Nature Communications **4**, 2871 (2013).

[73] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek,

B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Entanglement-based quantum communication over 144 km, Nature Physics **3**, 481 (2007).

[74] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, Quantum teleportation over 143 kilometres using active feed-forward, Nature **489**, 269 (2012).

[75] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, X.-D. Cai, P. Xu, G.-S. Pan, J.-J. Jia, Y.-M. Huang, H. Yin, J.-Y. Wang, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, Quantum teleportation and entanglement distribution over 100-kilometre free-space channels, Nature **488**, 185 (2012).

[76] H. Takesue, S. D. Dyer, M. J. Stevens, V. Verma, R. P. Mirin, and S. W. Nam, Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors, Optica **2**, 832 (2015).

[77] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases, Physical Review A **88**, 032305 (2013).

[78] M. M. Wilde, From classical to quantum shannon theory, the latest version of the book "Quantum information theory" published by Cambridge University Press, arXiv:1106.1445v8 [quant-ph] .

[79] N. Imoto, H. A. Haus, and Y. Yamamoto, Quantum nondemolition measurement of the photon number via the optical Kerr effect, Physical Review A **32**, 2287 (1985).

[80] V. B. Braginskiĭ and Y. I. Vorontsov, Quantum-mechanical limitations in macroscopic experiments and modern experimental technique, Soviet Physics Uspekhi **17**, 644 (1975).

[81] V. B. Braginsky, Y. I. Vorontsov, and K. S. Thorne, Quantum Nondemolition Measurements, Science **209**, 547 (1980).

[82] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, Physical Review Letters **98**, 230501 (2007).

[83] U. Vazirani and T. Vidick, Fully device-independent quantum key distribution, Physical Review Letters **113**, 140501 (2014).

[84] Álvaro Navarrete, M. Pereira, M. Curty, and K. Tamaki, Practical quantum key distribution that is secure against side channels, Physical Review Applied **15**, 034072 (2021).

[85] C.-H. F. Fung, X. Ma, and H. F. Chau, Practical issues in quantum-key-distribution postprocessing, Physical Review A **81**, 012318 (2010).

[86] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New Journal of Physics **11**, 045018 (2009).

[87] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed experiment to test local hidden-variable theories, Physical Review Letters **23**, 880 (1969).

[88] B. S. Cirel'son, Quantum generalizations of Bell's inequality, Letters in Mathematical Physics **4**, 93 (1980).

[89] A. Yariv, *Quantum Electronics, Third Edition* (John Wiley & Sons, 1989).

[90] H. Takesue and Y. Noguchi, Implementation of quantum state tomography for time-bin entangled photon pairs, Optics Express **17**, 10976 (2009).

[91] H. Takesue and K. Inoue, Quantum secret sharing based on modulated high-dimensional time-bin entanglement, Physical Review A **74**, 012315 (2006).

[92] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, Security of high-dimensional quantum key distribution protocols using franson interferometers, Journal of Physics B: Atomic, Molecular and Optical Physics **46**, 104010 (2013).

[93] T. Honjo, K. Inoue, and H. Takahashi, Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer, Optics Letters **29**, 2797 (2004).

[94] H. Takesue and K. Inoue, Generation of 1.5-μm band time-bin entanglement using spontaneous fiber four-wave mixing and planar light-wave circuit interferometers, Physical Review A **72**, 041804(R) (2005).

[95] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Measurement of qubits, Physical Review A **64**, 052312 (2001).

[96] R. T. Thew, K. Nemoto, A. G. White, and W. J. Munro, Qudit quantum-state tomography, Physical Review A **66**, 012303 (2002).

[97] L. Richart, *Higher Dimensional Time-Energy Entanglement*, Ph.D. thesis, Ludwig-Maximilians-Universität München (2014).

[98] R. Horodecki, P. Horodecki, and M. Horodecki, Quantum α-entropy inequalities: independent condition for local realism?, Physics Letters A **210**, 377 (1996).

[99] R. Horodecki and M. Horodecki, Information-theoretic aspects of inseparability

of mixed states, Physical Review A **54**, 1838 (1996).

[100] I. Devetak and A. Winter, Relating quantum privacy and quantum coherence: An operational approach, Physical Review Letters **93**, 080501 (2004).

[101] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, On mutually unbiased bases, International Journal of Quantum Information **8**, 535 (2010).

[102] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, Annals of Physics **191**, 363 (1989).

[103] T. Durt, About mutually unbiased bases in even and odd prime power dimensions, Journal of Physics A: Mathematical and General **38**, 5267 (2005).

[104] R. Renner, N. Gisin, and B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Physical Review A **72**, 012332 (2005).

[105] R. Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, ETH Zürich, Switzerland (2005).

[106] R. Renner, Symmetry of large physical systems implies independence of subsystems, Nature Physics **3**, 645 (2007).

[107] 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, Physical Review Letters **95**, 080501 (2005).

[108] P. Horodecki, L. Rudnicki, and K. Życzkowski, Five open problems in quantum information theory, PRX Quantum **3**, 010101 (2022).

[109] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Securing quantum key distribution systems using fewer states, Physical Review A **97**, 042347 (2018).

[110] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim, and D. J. Gauthier, Scalable high-rate, high-dimensional time-bin encoding quantum key distribution, Quantum Science and Technology **4**, 035008 (2019).

[111] F. Bussieres, Y. Soudagar, G. Berlin, S. Lacroix, and N. Godbout, Deterministic unitary operations on time-bin qudits for quantum communication (2006), arXiv:quant-ph/0608183 [quant-ph] .

[112] T. M. Rambo, *Low-Loss, All-Optical, Quantum Switching for Interferometric Processing of Weak Signals*, Ph.D. thesis, Northwestern University (2016).

[113] H.-P. Lo, T. Ikuta, N. Matsuda, T. Honjo, and H. Takesue, Entanglement generation using a controlled-phase gate for time-bin qubits, Applied Physics Express **11**, 092801 (2018).

[114] H.-P. Lo, T. Ikuta, N. Matsuda, T. Honjo, W. J. Munro, and H. Takesue,

Quantum process tomography of a controlled-phase gate for time-bin qubits, Physical Review Applied **13**, 034013 (2020).

本論文に関する原著論文

I 学術論文

1. Takuya Ikuta and Hiroki Takesue, Enhanced violation of the Collins-Gisin-Linden-Massar-Popescu inequality with optimized time-bin-entangled ququarts, Physical Review A **93**, 022307 (2016). [第 3 章]

2. Takuya Ikuta and Hiroki Takesue, Implementation of quantum state tomography for time-bin qudits, New Journal of Physics **19**, 013039 (2017). [第 4 章]

3. Takuya Ikuta and Hiroki Takesue, Four-dimensional entanglement distribution over 100 km, Scientific Reports **8**, 817 (2018). [第 4 章]

4. Takuya Ikuta[†], Seiseki Akibue[†], Yuya Yonezu, Toshimori Honjo, Hiroki Takesue, and Kyo Inoue, Scalable implementation of $(d+1)$ mutually unbiased bases for d-dimensional quantum key distribution, Physical Review Research **4**, L042007 (2022). ([†]These authors equally contributed.) [第 5 章]

II 国際会議

1. Takuya Ikuta and Hiroki Takesue, Violation of the CGLMP inequality with entangled time-bin ququarts, The 5th International Conference on Quantum Cryptography (QCrypt) 2015, poster 109, Sep. 29th 2015, Tokyo. [第 3 章]

2. Takuya Ikuta and Hiroki Takesue, Distribution of four-dimensional time-bin entangled state over 100 km of fiber, Conference on Lasers and Electro-Optics (CLEO) 2017, FTh4E.7, May 18th 2017, San Jose. [第 4 章]

3. Takuya Ikuta, Seiseki Akibue, Yuya Yonezu, Toshimori Honjo, Hiroki Take-

sue, and Kyo Inoue, Scalable preparation and measurement of 2^N-dimensional time-bin states in $(2^N + 1)$ mutually unbiased bases, Conference on Lasers and Electro-Optics (CLEO) 2022, FTu5A.7, May 17th 2022, San Jose (online hybrid). [第 5 章]

III 国内会議/研究会

1. 生田拓也, 武居弘樹, 4 次元 Time-bin 量子もつれによる CGLMP 不等式の破れの観測, 応用物理学会秋季学術講演会, 15a-4D-8, 名古屋, 2015 年 9 月. [第 3 章]
2. 生田拓也, 武居弘樹, 4 次元 Time-bin 量子もつれによるベル不等式の破れの観測, ImPACT 未来開拓研究会 2015, ポスター発表, 北海道, 2015 年 10 月. [第 3 章]
3. 生田拓也, 武居弘樹, 高次元 Time-bin 量子もつれに対する量子状態トモグラフィの実装, 応用物理学会秋季学術講演会, 13p-B2-9, 新潟, 2016 年 9 月. [第 4 章]
4. 生田拓也, 武居弘樹, 4 次元 Time-bin 量子もつれに対する量子状態トモグラフィの実装, ImPACT 未来開拓研究会 2016, ポスター発表, 京都, 2016 年 11 月. [第 4 章]
5. 生田拓也, 武居弘樹, 高次元 Time-bin 量子もつれ状態の長距離配送実験, 応用物理学会春季学術講演会, 17p-414-1, 神奈川, 2017 年 3 月 (講演奨励賞受賞記念講演). [第 4 章]
6. 生田拓也, 武居弘樹, 4 次元量子もつれ状態の長距離ファイバー伝送実験, ImPACT 未来開拓研究会 2018, ポスター発表, 富山, 2018 年 5 月. [第 4 章]
7. 生田拓也, 秋笛清石, 米津佑哉, 本庄利守, 武居弘樹, 井上恭, 2^N 次元量子状態に対する $(2^N + 1)$ 相互不偏基底測定のスケーラブルな実装, 第 45 回量子情報技術研究会 (QIT45), 13, オンライン開催, 2021 年 11 月. [第 5 章]

略語一覧

BPF　Band-pass filter, バンドパスフィルタ 57

CGLMP 不等式　Collins–Gisin–Linden–Massar–Popescu 不等式 46

CHSH 不等式　Clauser–Horn–Shimony–Holt 不等式 45

cps　counts per sec 58

CPTP　Completely positive trace preserving, 完全正値トレース保存 13

CW　Continuous wave, 連続波 57

DL　Delay line, 光ディレイライン 114

DSF　Dispersion shifted fiber, 分散シフトファイバ 86

EB　Entanglement-based 型 2

EDFA　Erbium-doped fiber amplifier, エルビウム添加光ファイバ増幅器 57

EPR ペア　Einstein–Podolsky–Rosen ペア 42

FBG　Fiber bragg gratings, ファイバブラッググレーティング 57

IID　Independent and identically distributed, 独立同一分布 98

IM Intensity modulator, 光強度変調器 57

IQ 変調器 In-phase and Quadrature-phase modulator 109

MUB Mutually unbiased bases, 相互不偏基底 6

MZI Mach-Zehnder interferometer, Mach-Zehnder 干渉計 7

NRZ Non return to zero, 非ゼロ復帰 57

OAM Orbital angular momentum, 光軌道角運動量 4

P&M Prepare and Measure 型 2

PC Polarization controller, 偏波コントローラ 58

PLC Planar lightwave circuit, 平面光波回路 58

PM Phase modulator, 位相変調器 114

Pol Polarizer, 偏光子 58

POVM Positive operator-valued measure, 正定値作用素測度 21

PPLN Periodically poled lithium niobate, 周期的分極反転ニオブ酸リチウム 57

PPM Pulse position modulation, パルス位置変調 9

QAM Quadrature amplitude modulation, 直交振幅変調 4

QKD Quantum key distribution, 量子鍵配送 1

QPSK Quadrature phase shift keying, 4 値位相変調 109

QST Quantum state tomography, 量子状態トモグラフィー 7

SHG The second harmonic generation, 第二次高調波生成 53

SLM Spatial light modulator, 液晶空間位相変調器 4

SNSPD Superconducting nanowire single-photon detector, 超伝導ナノワイヤ単一光子検出器 58

SPDC Spontaneous parametric down conversion, 自発的パラメトリック下方変換 . 49

TIA Time interval analyzer, タイムインターバルアナライザ 5

VATT Variable attenuator, 可変光減衰器 57

WDM Wavelength demultiplexing filter, 波長分離フィルタ 58