(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4304298号
(P4304298)

(45)発行日　平成21年7月29日(2009.7.29)　(24)登録日　平成21年5月15日(2009.5.15)

(51)Int.Cl.			F I		
H04L	9/12	(2006.01)	H04L	9/00	631
H04B	10/00	(2006.01)	H04B	9/00	Z
H04L	7/04	(2006.01)	H04L	7/04	B

請求項の数 19　(全 28 頁)

(21)出願番号　特願2004-336955 (P2004-336955)
(22)出願日　平成16年11月22日 (2004.11.22)
(65)公開番号　特開2005-260911 (P2005-260911A)
(43)公開日　平成17年9月22日 (2005.9.22)
審査請求日　平成16年11月22日 (2004.11.22)
(31)優先権主張番号　特願2004-36142 (P2004-36142)
(32)優先日　平成16年2月13日 (2004.2.13)
(33)優先権主張国　日本国 (JP)

（出願人による申告）平成１６年度、独立行政法人情報通信研究機構、「量子暗号技術の研究開発」委託研究、産業再生法第３０条の適用を受ける特許出願

前置審査

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100097157
弁理士　桂木　雄二
(72)発明者　田島　章雄
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　前田　和佳子
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　高橋　成五
東京都港区芝五丁目７番１号　日本電気株式会社内

最終頁に続く

(54)【発明の名称】通信システム及びその同期方法

(57)【特許請求の範囲】
【請求項１】
相対的に光パワーが小さい微弱光状態および大きい通常光状態のいずれかで第１光信号を伝送する第１チャネルと前記通常光状態で第２光信号を伝送する第２チャネルとを含む少なくとも１つの伝送路を介して接続された第１通信装置および第２通信装置を有し、前記第２通信装置が前記第１チャネルを通して前記第１通信装置へ第１光信号を出力し、前記第１通信装置が前記第１光信号を折り返し、その折り返された第１光信号に送信情報を乗せ前記微弱光状態で前記第２通信装置へ送信する通信システムにおいて、
前記第１通信装置および前記第２通信装置の各々に設けられ、前記第２チャネルを通して前記第２光信号により基準信号を送受信する第１通信手段と、
前記第２通信装置に設けられ、前記基準信号に従った前記第１光信号を前記通常光状態で前記第１チャネルを通して前記第１通信装置へ出力し、前記第１通信装置で折り返えされた前記通常光状態の前記第１光信号を受信する第２通信手段と、
前記第１通信装置および前記第２通信装置の各々に設けられ、前記第１チャネルから検出された基準信号と前記第２チャネルから検出された基準信号との間の位相を比較する位相比較手段と、
前記第１通信装置および前記第２通信装置の各々に設けられ、前記位相比較手段の比較結果に基づいて前記第１通信装置および前記第２通信装置の間の同期を確立する同期確立手段と、
前記第１通信装置に設けられ、前記折り返された第１光信号を前記微弱光状態および通

常光状態のいずれかに設定する第３通信手段と、
同期確立動作時には前記第３通信手段を前記通常光状態のトレーニングモードに設定し、同期確立後は前記微弱光状態の通信モードに切り替える通信制御手段と、
を有することを特徴とする通信システム。

【請求項２】
前記基準信号はクロック信号であり、前記同期確立手段は前記第１チャネルで検出されたクロック信号と前記第２チャネルで検出されたクロック信号との位相を合わせるようにタイミングを調整することを特徴とする請求項１に記載の通信システム。

【請求項３】
前記基準信号は、前記第１通信装置および前記第２通信装置の間で共有される情報を生成するための共有情報生成基準信号であり、前記同期確立手段は前記第１チャネルで検出された共有情報生成基準信号と前記第２チャネルで検出された共有情報生成基準信号との位相を合わせるようにタイミングを調整することを特徴とする請求項１に記載の通信システム。

【請求項４】
送信側の量子ユニットと受信側の量子ユニットとが、前記送信側の量子ユニットから前記受信側の量子ユニットへ送信する光パワーが１光子／ビット以下の微弱光状態および前記微弱光状態より大きい通常光状態のいずれかの状態で第１光信号を伝送する量子チャネルと前記通常光状態で第２光信号を伝送する古典チャネルとからなる伝送路で接続され、前記受信側の量子ユニットが前記量子チャネルを通して前記送信側の量子ユニットへ第１光信号を出力し、前記送信側の量子ユニットが前記第１光信号を折り返し、その折り返された第１光信号に送信情報を乗せ前記微弱光状態で前記受信側の量子ユニットへ送信する通信システムであって、
前記量子チャネルにおける前記第１光信号の光パワーを前記通常光状態にするトレーニングモードを前記送信側の量子ユニットおよび前記受信側の量子ユニットに指示する手段と、
前記送信側の量子ユニットおよび前記受信側の量子ユニットの間でクロック信号を前記量子チャネルおよび前記古典チャネルを通してそれぞれ前記通常光状態の第１光信号および第２光信号で伝送する手段と、
前記送信側および前記受信側の量子ユニットに設けられ、かつ、前記トレーニングモードにおいて抽出した前記量子チャネルのクロック信号と前記古典チャネルのクロック信号との位相比較を行って前記送信側の量子ユニットと前記受信側の量子ユニットとの同期を確立する手段と
を有することを特徴とする通信システム。

【請求項５】
前記同期を確立する手段は、前記位相比較の結果を基に前記量子チャネルと前記古典チャネルとの波長分散による伝搬遅延差を較正することを特徴とする請求項４記載の通信システム。

【請求項６】
前記送信側の量子ユニットと前記受信側の量子ユニットとの間における前記送信情報を用いた鍵生成時に、前記同期を確立する手段は、前記古典チャネルによる別波長の同期信号を用いてクロック同期を行うことを特徴とする請求項４に記載の通信システム。

【請求項７】
前記折り返された第１光信号に送信情報を乗せて前記微弱光状態で前記受信側の量子ユニットへ送信する通信モード時に比べて、前記トレーニングモード時には前記第１光信号の光パルス幅を広げることを特徴とする請求項４に記載の通信システム。

【請求項８】
前記クロック同期を行った後に、前記送信側の量子ユニットと前記受信側の量子ユニット間での鍵生成同期を確立する鍵生成同期手段を前記送信側および前記受信側にそれぞれ設けたことを特徴とする請求項４に記載の通信システム。

【請求項９】
前記鍵生成同期手段は、
鍵生成基準信号を前記送信側の量子ユニットから前記受信側の量子ユニットへ前記量子チャネルおよび前記古典チャネルの両方を介して送信する送信手段と、
前記受信側の量子ユニットで前記量子チャネルを介して受信した鍵生成基準信号と前記古典チャネルを介して受信した鍵生成基準信号との位相差を検出する位相差検出手段と、
前記検出した位相差を補正することによって鍵生成同期を実現する鍵生成制御手段と、
を有することを特徴とする請求項８に記載の通信システム。
【請求項１０】
前記量子チャネルと前記古典チャネルとをそれぞれ異なる光ファイバに設定したことを特徴とする請求項４に記載の通信システム。
【請求項１１】
送信側の量子ユニットと受信側の量子ユニットとが、前記送信側の量子ユニットから前記受信側の量子ユニットへ送信する光パワーが１光子／ビット以下の微弱光状態および前記微弱光状態より大きい通常光状態のいずれかの状態で第１光信号を伝送する量子チャネルと前記通常光状態で第２光信号を伝送する古典チャネルとからなる伝送路で接続され、前記受信側の量子ユニットが前記量子チャネルを通して前記送信側の量子ユニットへ第１光信号を出力し、前記送信側の量子ユニットが前記第１光信号を折り返し、その折り返された第１光信号に送信情報を乗せ前記微弱光状態で前記受信側の量子ユニットへ送信する量子暗号鍵配布システムにおける前記送信側の量子ユニットと前記受信側の量子ユニットとの同期をとる同期方法であって、
前記送信側および前記受信側にそれぞれ設けられた制御手段が、前記量子チャネルにおける前記第１光信号の光パワーを前記通常光状態にするトレーニングモードを前記送信側の量子ユニットおよび前記受信側の量子ユニットに指示し、
前記送信側および前記受信側にそれぞれ設けられた通信手段が、前記送信側の量子ユニットおよび前記受信側の量子ユニットの間でクロック信号を前記量子チャネルおよび前記古典チャネルを通してそれぞれ前記通常光状態の第１光信号および第２光信号で伝送し、
前記送信側および前記受信側の量子ユニットに設けられた同期確立手段が、前記トレーニングモードにおいて抽出した前記量子チャネルのクロック信号と前記古典チャネルのクロック信号との位相比較を行って前記送信側の量子ユニットと前記受信側の量子ユニットとの同期を確立する、
ことを特徴とする同期方法。
【請求項１２】
前記同期を確立する際に、前記位相比較の結果を基に前記量子チャネルと前記古典チャネルとの波長分散による伝搬遅延差を較正することを特徴とする請求項１１に記載の同期方法。
【請求項１３】
前記送信側の量子ユニットと前記受信側の量子ユニットとの間における前記送信情報を用いた鍵生成時に、前記同期確立手段が前記古典チャネルによる別波長の同期信号を用いてクロック同期を行うことを特徴とする請求項１１に記載の同期方法。
【請求項１４】
前記折り返された第１光信号に送信情報を乗せて前記微弱光状態で前記受信側の量子ユニットへ送信する通信モード時に比べて、前記トレーニングモード時には前記第１光信号の光パルス幅を広げることを特徴とする請求項１１に記載の同期方法。
【請求項１５】
鍵生成同期手段が、前記クロック同期を行った後に、前記送信側の量子ユニットと前記受信側の量子ユニットとの間で鍵生成同期を確立することを特徴とする請求項１１に記載の同期方法。
【請求項１６】
前記鍵生成同期手段は、

鍵生成基準信号を前記送信側の量子ユニットから前記受信側の量子ユニットへ前記量子チャネルと前記古典チャネルを介して送り、
前記受信側の量子ユニットで前記量子チャネルを介して受信した鍵生成基準信号と前記古典チャネルを介して受信した鍵生成基準信号の位相差を検出し、
前記検出した位相差を補正することによって実現することを特徴とする請求項１５に記載の同期方法。
【請求項１７】
前記送信側および前記受信側における電源投入時に、前記同期確立手段が前記トレーニングモードとして前記送信側の量子ユニットと前記受信側の量子ユニットとの同期を確立することを特徴とする請求項１５に記載の同期方法。
【請求項１８】
前記送信側および前記受信側において障害検出時に、前記同期確立手段が前記トレーニングモードとして前記送信側の量子ユニットと前記受信側の量子ユニットとの同期を確立することを特徴とする請求項１５に記載の同期方法。
【請求項１９】
前記送信側および前記受信側において、前記同期確立手段が、予め設定された所定時間毎に、前記トレーニングモードとして前記送信側の量子ユニットと前記受信側の量子ユニットとの同期を確立することを特徴とする請求項１５に記載の同期方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は相対的に光パワーが小さい状態で信号を伝送する通信チャネルと相対的に大きい通常状態で信号を伝送する通信チャネルとを用いた通信システムに係り、特に通信装置間の同期確立方法に関する。
【背景技術】
【０００２】
量子暗号の分野では、ハイゼンベルクの不確定性原理に基づき、送信器と受信器との間での盗聴を高い確率で検出できることが知られている。このことは、逆に言えば、送信器および受信器の間で盗聴されることなく秘密のビット列（暗号鍵）を共有することが可能であることを示している。秘密情報を共有する手順としては、たとえば４つの量子状態を用いたＢＢ８４（Bennett Brassard 84）プロトコル等が知られている。これを絶対安全性が証明されているバーナム（Ｖｅｒｎａｍ）暗号の鍵として用いることで高度な安全性を達成できる。ＢＢ８４プロトコルによる鍵共有手順について簡単に説明する。
【０００３】
図１０はＢＢ８４に従った鍵共有手順ステップ１～８を説明するための模式図である。
【０００４】
ステップ１：　送信器で暗号鍵の元データとなるランダムデータビットと、変調時の基底情報Ａ（＋基底または×基底）となるランダムデータと、によって位相変調データを生成して記憶する。
【０００５】
ステップ２：　送信器で光パルスを位相変調データによって位相変調し、量子チャネルを介して受信器に送信する。
【０００６】
ステップ３：　受信器でもランダムな基底データ（＋基底または×基底）に基づいて送信器からの光パルスを位相変調して干渉計を経て受信する。
【０００７】
ステップ４：　受信器で受信することができた光データビット（検出出力）と、その時の基底情報Ｂとを記憶し、規定情報Ｂを送信器へ古典チャネルを介して送信する。
【０００８】
ステップ５：　送信器では受信器から送られた基底情報Ｂと記憶していた基底情報Ａとを

比較し、もとデータであるランダムデータビットのうちの基底の合致しないビットを破棄する。

【０００９】

ステップ６：　送信器から受信器へ、破棄されずに残ったビットのビット番号を古典チャネルを介して送信する。

【００１０】

ステップ７：　受信器では送信器から送られたビット番号以外の検出データビットを破棄する。

【００１１】

ステップ８：　最終的に残ったデータビットを送信器と受信器とで共有される暗号化鍵データとする。

【００１２】

このような鍵共有方式を採用した量子暗号鍵配布システムがいくつか提案されている。特にスイスのジュネーブ大学で提案されたＰｌｕｇ＆Ｐｌａｙ方式（非特許文献１～３参照）は、光ファイバ伝送路における偏光の揺らぎを補償することができるため、偏光に敏感な量子暗号鍵配布システムを実用化するための方式として期待されている。Ｐｌｕｇ＆Ｐｌａｙ方式の概略的構成を図１１に示す。

【００１３】

図１１に示すように、Ｐｌｕｇ＆Ｐｌａｙ方式では、まず、量子暗号鍵の受信器のレーザＬＤで光パルスＰを発生させ、それを２分割し、一方の光パルスＰ１は短いパスを通して、他方の光パルスＰ２は長いパスを通して、それぞれ相前後して送信器へ送信される。アリスは光パルスＰ１およびＰ２を順次受信すると、光パルスＰ１をファラデーミラーで反射させ偏光状態を９０度回転させて受信器へ返送し、光パルスＰ２をファラデーミラーで同様に反射させると共に位相変調して位相変調された光パルスＰ２^{*A}を受信器へ返送する。

【００１４】

受信器では、送信器から受信した光パルスＰ１を送信時とは異なる長いパスを通すと共に位相変調し、位相変調された光パルスＰ１^{*B}を得る。他方、送信器で位相変調された光パルスＰ２^{*A}は送信時とは異なる短いパスを通した後、受信器で位相変調された光パルスＰ１^{*B}と干渉させ、その結果を光子検出器ＡＰＤ１またはＡＰＤ２で検出する。全体として、受信器内で２分割された光パルスＰ１およびＰ２は同じ光パスを通過して干渉するので、光子検出器で観測される干渉結果は光ファイバ伝送路の遅延変動が相殺され、送信器の位相変調と受信器の位相変調との差に依存する。

【００１５】

このような構成を有するＰｌｕｇ＆Ｐｌａｙ方式では次のような同期をとる必要がある：

１）送信器において、受信器から送られた光パルスＰ２をパルスに合わせて変調するために光ファイバ伝送路の遅延変動に追従させる；

２）受信器において、送信器から反射されてきた光パルスＰ１を変調するために光ファイバ伝送路の遅延変動に追従させる；および

３）受信器で光パルスを受信する時、光検出器に印加するバイアスを受信光パルスに合わせる（ガイガーモードでの超高感度受信）。

【００１６】

さらに、量子暗号鍵配布システムでは、基本情報のやりとり、鍵生成シーケンスにおいてもビット位置の同期を確立する必要がある。

【００１７】

しかしながら、量子暗号鍵配布システムでは、従来の光通信と大きく異なり、光パワーレベルが高々単一光子レベルと微少であるため、量子チャネルを利用して従来の古典チャネルのようなクロック抽出を行うことが不可能である。量子チャネルとは、送信器から受信器へ送信する光パワーが１ｐｈｏｔｏｎ／ｂｉｔ以下の微弱な状態の通信チャネルをい

い、古典チャネルとは通常の光パワー領域での通信チャネルをいう。

【００１８】

つまり、量子チャネルを利用して光パワーレベルが微少な光で通信している時には、光検出器ＡＰＤにほとんど光が到達しないので、例えば送信側がマーク率１／２のデータを送っても、受信側のマーク率が１／２よりもはるかに小さくなり、データの欠損が生じ、正しい周期のクロックを抽出することができない。このような量子チャネルにおける同期をとるためには、通常、古典チャネルが利用されている。

【００１９】

例えば、特表平０８－５０５０１９号公報（特許文献１）には、古典チャネルを利用してビット同期その他システムの較正を行う方法が提案されている。特許文献１に記載された方法では、同一の伝送路に量子チャネルと古典チャネルとを設け、古典チャネルを利用して光パワーの微弱な量子チャネルのクロック同期を行っている（６ページ４行～２７行、Fig. 4参照）。

【００２０】

また、特開昭６３－１０７３２３号公報（特許文献２）には、光ファイバの伝送特性の変動を受信側で検出し、特性変動の補償を可能にする光伝送方式が開示されている。具体的には、データ信号とは別波長の参照信号を受信器から送信器へ送出し、送信器で折り返されて戻ってきた参照信号から光ファイバの伝送特性の変動を検出する（３ページ左上欄１３行から左下欄１３行、第１図、第２図）。

【００２１】

【特許文献１】特表平０８－５０５０１９号公報（６ページ４行～２７行、Fig. 4参照）

【特許文献２】特開昭６３－１０７３２３号公報（３ページ左上欄１３行から左下欄１３行、第１図、第２図参照）

【非特許文献１】“Ａｕｔｏｍａｔｅｄ ‘ｐｌｕｇ ＆ ｐｌａｙ’ ｑｕａｎｔｕｍ ｋｅｙ ｄｉｓｔｒｉｂｕｔｉｏｎ”（Ｇ. Ｒｉｂｏｒｄｙ, Ｊ. Ｄ. Ｇａｕｔｉｅｒ, Ｏ. Ｇｕｉｎｎａｒｄ ａｎｄ Ｈ. Ｚｂｉｎｄｅｎ, ＥＬＥＣＴＲＯＮＩＣＳ ＬＥＴＴＥＲＳ ２９ｔｈ, Ｏｃｔｏｂｅｒ １９９８, Ｖｏｌ. ３４ Ｎｏ. ２２, ｐｐ. ２１１６－２１１７）

【非特許文献２】「“Ｐｌｕｇ ＆ Ｐｌａｙ” ｓｙｓｔｅｍｓ ｆｏｒ ｑｕａｎｔｕｍ ｃｒｙｐｔｏｇｒａｐｈｙ」（Ａ. Ｍｕｌｌｅｒ, Ｔ. Ｈｅｒｚｏｇ, Ｂ. Ｈｕｔｔｎｅｒ, Ｗ. Ｔｉｔｔｅｌ, Ｈ. Ｚｂｉｎｄｅｎ ａｎｄ Ｎ. Ｇｉｓｉｎ, Ａｐｐｌ. Ｐｈｙｓ. Ｌｅｔｔ. ７０（７）, １７ Ｆｅｂｒｕａｒｙ １９９７, ｐｐ. ７９３－７９５）

【非特許文献３】“ｉｎｔｅｒｆｅｒｏｍｅｔｒｙ ｗｉｔｈ Ｆａｒａｄａｙ ｍｉｒｒｏｒｓ ｆｏｒ ｑｕａｎｔｕｍ ｃｒｙｐｔｏｇｒａｐｈｙ”（Ｈ. Ｚｂｉｎｄｅｎ, Ｊ. Ｄ. Ｇａｕｔｉｅｒ, Ｎ. Ｇｉｓｉｎ, Ｂ. Ｈｕｔｔｎｅｒ, Ａ. Ｍｕｌｌｅｒ ａｎｄ Ｗ. Ｔｉｔｔｅｌ, ＥＬＥＣＴＲＯＮＩＣＳ ＬＥＴＴＥＲＳ ２７ｔｈ, Ｍａｒｃｈ １９９７, Ｖｏｌ. ３３ Ｎｏ. ７, ｐｐ. ５８６－５８８）

【発明の開示】

【発明が解決しようとする課題】

【００２２】

しかしながら、光伝送路には実際には波長分散が存在する。特許文献１に記載されているように同一伝送路であっても、量子チャネルと古典チャネルとでは波長が異なるので両チャネルの伝搬時間が異なる。このため、量子チャネルと古典チャネルとの位相関係は一致しなくなり、量子チャネルのクロック同期および鍵生成のためのビット同期を確立することができない。また、量子チャネルと古典チャネルをと別々の伝送路で構成する場合には、伝搬時間は伝送路の特性（伝搬距離や分散等）に依存するので、伝送路毎の設定が必要となる。いずれにしても、量子チャネルと古典チャネルとの位相関係は一致しなくなり、量子チャネルのクロック同期および鍵生成のためのビット同期を確立することができない。

【００２３】
また、特許文献２に開示された光伝送方式においても、光信号の変動を補正するために別波長の参照信号を送出するのであるから、同様の理由から、量子チャネルのクロック抽出を行うことや鍵生成同期すなわちビット位置の同期を行うための基準信号を受信器へ正確に送ることが不可能である。
【００２４】
そこで本発明の目的は、正確なクロック抽出が可能なチャネルと不可能なチャネルとによって接続された送信器および受信器の間で両チャネルの同期を確立する方法およびシステムを提供することにある。
【課題を解決するための手段】
【００２５】
本発明による通信システムは、相対的に光パワーが小さい微弱光状態および大きい通常光状態のいずれかで第１光信号を伝送する第１チャネルと前記通常光状態で第２光信号を伝送する第２チャネルとを含む少なくとも１つの伝送路を介して接続された第１通信装置および第２通信装置を有し、前記第２通信装置が前記第１チャネルを通して前記第１通信装置へ第１光信号を出力し、前記第１通信装置が前記第１光信号を折り返し、その折り返された第１光信号に送信情報を乗せ前記微弱光状態で前記第２通信装置へ送信する通信システムにおいて、前記第１通信装置および前記第２通信装置の各々に設けられ、前記第２チャネルを通して前記第２光信号により基準信号を送受信する第１通信手段と、前記第２通信装置に設けられ、前記基準信号に従った前記第１光信号を前記通常光状態で前記第１チャネルと通して前記第１通信装置へ出力し、前記第１通信装置で折り返えされた前記通常光状態の前記第１光信号を受信する第２通信手段と、前記第１通信装置および前記第２通信装置の各々に設けられ、前記第１チャネルの前記第１光信号から検出された基準信号と前記第２チャネルの前記第２光信号から検出された基準信号との間の位相を比較する位相比較手段と、前記第１通信装置および前記第２通信装置の各々に設けられ、前記位相比較手段の比較結果に基づいて前記第１通信装置および前記第２通信装置の間の同期を確立する同期確立手段と、を有する。
【００２６】
本発明の第１実施形態によれば、前記基準信号はクロック信号であり、前記同期確立手段は前記第１チャネルで検出されたクロック信号と前記第２チャネルで検出されたクロック信号との位相を合わせるようにタイミングを調整する。
【００２７】
本発明の第２実施形態によれば、前記基準信号は、前記第１通信装置および前記第２通信装置の間で共有される情報を生成するための共有情報生成基準信号（鍵生成基準信号）であり、前記同期確立手段は前記第１チャネルで検出された共有情報生成基準信号と前記第２チャネルで検出された共有情報生成基準信号との位相を合わせるようにタイミングを調整する。
【００２８】
本発明の一実施例によれば、同期確立動作時には前記通信手段を前記光パワーが大きい通常状態の通信モードに設定し、同期確立後は前記光パワーが小さい状態の通信モードに切り替える通信制御手段をさらに有する。
【００２９】
本発明による第１通信装置と第２通信装置との間の同期確立方法は、相対的に光パワーが小さい微弱光状態および大きい通常光状態のいずれかで第１光信号を伝送する第１チャネルと前記通常光状態で第２光信号を伝送する第２チャネルとを含む少なくとも１つの伝送路を介して接続された第１通信装置および、第２通信装置を有し、前記第２通信装置が前記第１チャネルを通して前記第１通信装置へ第１光信号を出力し、前記第１通信装置が前記第１光信号を折り返し、その折り返された第１光信号に送信情報を乗せ前記微弱光状態で前記第２通信装置へ送信する通信システムにおける前記第１通信装置と前記第２通信装置との間で同期を確立する方法において、前記第１通信装置および前記第２通信装置の

間でクロック信号を前記第１チャネルおよび前記第２チャネルを通してそれぞれ前記通常光状態の第１光信号および第２光信号で伝送し、前記第１通信装置および前記第２通信装置の各々に設けられた位相比較手段が前記第１チャネルから検出されたクロック信号と前記第２チャネルから検出されたクロック信号との間の位相を比較し、前記第１通信装置および前記第２通信装置の各々に設けられた同期確立手段が前記検出されたクロック信号の位相を合わせることで前記第１通信装置および前記第２通信装置の間の同期した較正クロック信号を生成する、ことを特徴とする。

【００３０】

さらに、望ましくは、前記較正クロック信号に従って、前記第１通信装置から前記第２通信装置へ、それらの間で共有される情報を生成するための共有情報生成基準信号を前記第１チャネルおよび前記第２チャネルを通してそれぞれ前記光パワーが大きい通常状態で伝送し、前記較正クロック信号に従って、前記第１チャネルから検出された共有情報生成基準信号と前記第２チャネルから検出された共有情報生成基準信号との間の位相を比較し、前記検出された共有情報生成基準信号の間の位相差に基づいて、前記第１通信装置および前記第２通信装置の間で共有される情報を生成するための同期を確立する、ことを特徴とする。

【００３１】

好ましくは、本発明は量子暗号鍵配布システムに適用可能である。すなわち、送信側の量子ユニットと受信側の量子ユニットとが、前記送信側の量子ユニットから前記受信側の量子ユニットへ送信する光パワーが１光子／ビット以下の微弱光状態および前記微弱光状態より大きい通常光状態のいずれかの状態で第１光信号を伝送する量子チャネルと前記通常光状態で第２光信号を伝送する古典チャネルとからなる伝送路で接続され、前記受信側の量子ユニットが前記量子チャネルを通して前記送信側の量子ユニットへ第１光信号を出力し、前記送信側の量子ユニットが前記第１光信号を折り返し、その折り返された第１光信号に送信情報を乗せ前記微弱光状態で前記受信側の量子ユニットへ送信する通信システムであって、前記量子チャネルにおける前記第１光信号の光パワーを前記通常光状態にするトレーニングモードを前記送信側の量子ユニットおよび前記受信側の量子ユニットに指示する手段と、前記送信側の量子ユニットおよび前記受信側の量子ユニットの間でクロック信号を前記量子チャネルおよび前記古典チャネルを通してそれぞれ前記通常光状態の第１光信号および第２光信号で伝送する手段と、前記送信側および前記受信側の量子ユニットに設けられ、かつ、前記トレーニングモードにおいて抽出した前記量子チャネルのクロック信号と前記古典チャネルのクロック信号との位相比較を行って前記送信側の量子ユニットと前記受信側の量子ユニットとの同期を確立する手段とを有することを特徴とする。

【００３２】

さらに、鍵生成基準信号を前記送信側の量子ユニットから前記受信側の量子ユニットへ前記量子チャネルと前記古典チャネルを介して送り、前記受信側の量子ユニットで前記量子チャネルを介して受信した鍵生成基準信号と前記古典チャネルを介して受信した鍵生成基準信号の位相差を検出し、前記検出した位相差を補正することによって鍵生成同期を実現することができる。

【００３３】

本発明による量子暗号鍵配布システムの同期方法は、前記量子チャネルの光パワーを前記通常状態として通信するトレーニングモードを前記送信側の量子ユニット及び前記受信側の量子ユニットに指示し、前記送信側の量子ユニット側で前記トレーニングモードにおいて前記光パワーを前記通常状態として通信し、前記受信側の量子ユニット側で前記トレーニングモードにおいて抽出した前記量子チャネルのクロックと前記古典チャネルのクロックとの位相比較を行って前記送信側の量子ユニットと前記受信側の量子ユニットとのクロック同期を確立する。

【００３４】

さらに鍵生成基準信号を前記送信側の量子ユニットから前記受信側の量子ユニットへ前

記量子チャネルと前記古典チャネルを介して送り、前記受信側の量子ユニットで前記量子チャネルを介して受信した鍵生成基準信号と前記古典チャネルを介して受信した鍵生成基準信号の位相差を検出し、前記検出した位相差を補正することによって鍵生成同期を実現する。

【発明の効果】

【００３５】

本発明によれば、微弱な通信状態の第１チャネルと通常通信状態の第２チャネルとの間の波長分散等に起因する伝搬遅延差を伝送路によらず自動で較正することができる。これにより、クロック抽出や基準信号伝送を正確に行うことができない第１チャネルに代わって、第２チャネルで送信器と受信器との同期を確立することができるという効果が得られる。

【００３６】

本発明を量子暗号鍵配布システムに適用した場合、鍵生成を開始する前に、量子チャネルの光パワーを通常レベルの強い光で通信するモード（以下、トレーニングモードとする）を設け、このトレーニングモードにおいて抽出した量子チャネルのクロックと古典チャネルのクロックとの位相比較を行い、量子チャネルと古典チャネルとの波長分散による伝搬遅延差を自動で較正してクロック同期を確立することができる。

【００３７】

さらに、鍵生成基準信号を前記送信側の量子ユニットから前記受信側の量子ユニットへ前記量子チャネルと前記古典チャネルを介して送り、これらのチャネルで受信した鍵生成基準信号の位相差を検出し、この位相差を補正することによって鍵生成同期を実現することができる。

【００３８】

このように、本発明によれば、鍵生成を開始する前に通常レベルの強い光で通信するトレーニングモードを設け、別波長の同期信号との波長分散による伝搬遅延差を較正し、鍵生成時には別波長の同期信号を用いてクロック同期及び鍵生成同期を行う。これによって、量子チャネルと古典チャネルでの波長分散による伝搬遅延差を伝送路によらず自動で較正することが可能となり、微弱光のためにクロック抽出や基準信号の伝送を正確に行うことができない量子チャネルに代わって、波長の異なる古典チャネルで送信器と受信器との同期を確立することが可能となる。

【発明を実施するための最良の形態】

【００３９】

以下、説明を簡単にするために、２つの通信装置が光ファイバで接続されている通信システムを一例として取り上げ、本発明の実施形態を詳細に説明する。

【００４０】

１．第１実施形態

図１は本発明の第１実施形態による通信システムの概略的構成を示すブロック図である。ここでは、送信器１０と受信器２０とが量子チャネル５１および古典チャネル５２を含む光ファイバ伝送路５により接続されている。量子チャネル５１と古典チャネル５２とは同一伝送路（光ファイバ伝送路５）上の別波長のチャネルである。

【００４１】

送信器１０は量子ユニット１および同期部４を含み、受信器２０は量子ユニット２および同期部３を含む。量子ユニット１と量子ユニット２とは量子チャネル５１を介して生鍵とよばれる暗号鍵を生成し、送信器１０と受信器２０とは、後述するように量子チャネル５１および古典チャネル５２の別波長チャネルを用いて、量子ユニット１および２の間で同期を確立する。

【００４２】

受信器２０の同期部３は、クロック抽出器３１、遅延素子３２および位相比較器３３を有する。後述するように遅延素子３２は、位相比較器３３の比較結果に依存して遅延量が制御される。送信器１０の同期部４は、クロック抽出器４１、遅延素子４２、位相比較器

４３、および、マスタクロック４４を有する。後述するように遅延素子４２は、位相比較器４３の比較結果に依存して遅延量が制御される。また、送信器１０および受信器２０には、図示されていない通信制御部が設けられている。

【００４３】

送信側および受信側の量子ユニット１および量子ユニット２は、それぞれの通信制御部からトレーニングモード切替信号を受取ることでトレーニングモードに移行する。トレーニングモードでは、量子チャネル５１に古典チャネルレベルの強さの光信号を伝送することで、各量子ユニットにおいてクロック抽出が可能となる。

【００４４】

まず、マスタクロック４４はクロック信号を古典チャネル５２を通して受信器２０へ送出している。受信器２０の同期部３におけるクロック抽出部３１は、古典チャネル５２を通して受信した信号からクロック信号を抽出し、それを古典チャネル５２へそのまま折り返し返送する。

【００４５】

送信器１０の同期部４におけるクロック抽出部４１は、古典チャネル５２を通して受信器２０で折り返されてきたクロック信号を抽出する。抽出されたクロック信号は遅延素子４２で遅延され、位相比較器４３および量子ユニット１へ出力される。トレーニングモード切替信号を入力すると、送信側の量子ユニット１は、遅延素子４２から入力したクロック信号に従って、通常の通信に用いられる程度の強い光を量子チャネル５１に送出する。位相比較器４３は、量子ユニット１でモニタされた量子チャネル５１のクロック信号と遅延素子４２から入力した古典チャネル５２のクロック信号との位相比較を行い、その位相のずれを補償するように遅延素子４２の遅延量を制御する。すなわち、位相比較器４３および遅延素子４２は遅延ロックループＤＬＬを構成する。

【００４６】

受信側の量子ユニット２は、量子チャネル５１から受信した信号からクロックを抽出し位相比較器３３へ出力する。受信器２０の同期部３におけるクロック抽出部３１により抽出されたクロック信号は遅延素子３２で遅延され、位相比較器３３および量子ユニット２へ出力される。位相比較器３３は、量子ユニット２でモニタされた量子チャネル５１のクロック信号と遅延素子３２から入力した古典チャネル５２のクロック信号との位相比較を行い、その位相のずれを補償するように遅延素子３２の遅延量を制御する。すなわち、位相比較器３３および遅延素子３２は遅延ロックループＤＬＬを構成する。

【００４７】

このようにして送信器１０および受信器２０において遅延量の調整が行われ、マスタクロック４４を基準とした同期が確立される。同期が確立されると、送信器１０および受信器２０の量子ユニット１および２は、それぞれ同期したクロック信号に従って、所定の動作を行うことができる。

【００４８】

なお、送信器１０と受信器２０とにおいては、トレーニングモードへの切替え時または量子モードへの切替え時に、古典チャネル５２を介して相互にその切替え要求およびそれに対する応答がやりとりされ、それらの切替えが通知される。送信器１０および受信器２０の各通信制御部は、この切替えの通知に従ってトレーニングモード切替信号または量子モード切替信号を出力する。

【００４９】

１．１）第１実施例

（構成）

次に、上記第１実施形態による通信システムをＰｌｕｇ＆Ｐｌａｙ方式の量子暗号鍵配布システムに適用した一例を詳細に説明する。ただし、Ｐｌｕｇ＆Ｐｌａｙシステムの基本的な構成および動作は、図１１を用いて既に説明しているので詳細は省略する。

【００５０】

図２は本発明の第１実施例によるＰｌｕｇ＆Ｐｌａｙ方式の量子暗号鍵配布システムを

示すブロック図である。本実施例では、波長λ１の量子チャネル４０１（図１の量子チャネル５１）と、波長λ２およびλ３の同期信号用の古典チャネル４０２（図１の古典チャネル５２）とが用いられる。波長多重分離器６０１および６０２は光ファイバ伝送路４００（図１の光ファイバ５）を通して接続されている。波長λ１の量子チャネル４０１は量子ユニット１００および２００にそれぞれ接続され、波長λ２およびλ３の同期信号用の古典チャネル４０２は同期部３００および５００にそれぞれ接続されている。

【００５１】

送信側の量子ユニット１００（図１の受信側の量子ユニット１に対応）は、位相変調器（Phase Mod. A）１１１、変調器駆動回路（Ｄｒｖ．）１１２、遅延調整回路（D）１１３、ファラデーミラー１２０、光減衰器（Ａｔｔ．）１３０、および、量子チャネルモニタ用の光電変換器（Ｏ／Ｅ）１４０を有する。量子モード時には、位相変調器１１１は二種類の乱数Ｒ１およびＲ２の組み合わせに従って、ファラデーミラー１２０から反射した光パルスを０、π／２、π、３／２πの４つの位相のいずれかに変調し、光減衰器１３０は減衰量を大きくする。トレーニングモード時には、位相変調器１１１は位相変調を行わず、光減衰器１３０は減衰量を小さくする。量子モードおよびトレーニングモードの切り替えは、図示していない通信制御部により制御される。

【００５２】

受信側の量子ユニット２００（図１の受信側の量子ユニット２に対応）は、波長λ１のパルス光源であるレーザＬＤ２１１と、そのドライバであるレーザ駆動回路（Ｄｒｖ．）２１２とを有し、波長λ１の光パルスが光減衰器（Ａｔｔ．）２１３を通して光サーキュレータ２５０に入射する。光サーキュレータ２５０から出射した光パルスは、光カプラ４０６によって短経路（Ｓｈｏｒｔ　Ｐａｔｈ）４０４と長経路（Ｌｏｎｇ　Ｐａｔｈ）４０５にそれぞれ分岐し、Ｌｏｎｇ　Ｐａｔｈ４０５に分岐した光パルスは位相変調器（Ｐｈａｓｅ　Ｍｏｄ．Ｂ）２２１によって位相変調され、偏光ビームスプリッタＰＢＳ２３０に入射する。位相変調器２２１は乱数Ｒ３に従って変調器駆動回路（Ｄｒｖ．）２２２により駆動され、駆動タイミングは遅延調整回路（D）２２３により調整される。

【００５３】

位相変調器２２１は、既に述べたように送信器側で折り返された信号がＬｏｎｇ　ｐａｔｈ４０５を通るときに、乱数Ｒ３に従った０、π／２の２つの位相で当該光信号を変調する。そして、送信器側の位相変調器１１１で変調された光信号と受信器側の位相変調器２２１で変調された光信号とが光カプラ４０６で干渉し、その結果がアバランシェ光ダイオード（Avalanche Photo Diode）ＡＰＤ２４１またはＡＤＰ２４２で検出される。なお、Ｓｈｏｒｔ　Ｐａｔｈ４０４およびＬｏｎｇ　Ｐａｔｈ４０５は偏波保存ファイバ、光サーキュレータ２５０、光カプラ４０６は偏波保存型である。

【００５４】

また、量子モード時にはレーザＬＤ２１１から出力される光パルスのパルス幅を小さくしてＳｈｏｒｔ　Ｐａｔｈ４０４およびＬｏｎｇ　Ｐａｔｈ４０５の別経路を通った光パルスが十分区別できる間隔に維持する必要がある。しかしながら、トレーニングモード時には量子モード時のような光パルスの間隔を維持する必要はない。したがって、レーザ駆動回路２１２は、量子モードおよびトレーニングモードのいずれであるかによって上記光パルス幅を変化させる。

【００５５】

送信側同期部５００（図１の送信側同期部４に対応）にはマスタクロック５０４と電光変換器（Ｅ／Ｏ）５０５とが設けられ、マスタクロック５０４からのクロック信号がＥ／Ｏ５０５によって波長λ３の光クロック信号に変換され、波長λ３の古典チャネル４０２を通して受信器側へ送出される。さらに、同期部５００は、波長λ２の古典チャネル４０２を通して受信器側から受信した光信号を電気信号に変換する光電変換器（Ｏ／Ｅ）５０１、遅延素子５０２、および、位相比較器５０３を有する。

【００５６】

位相比較器５０３は、Ｏ／Ｅ１４０により検出された波長λ１の量子チャネル４０１の

クロック信号と遅延素子５０２から入力する古典チャネル４０２のクロック信号との位相比較を行い、上述したような遅延調整により較正クロック信号ＣＬＫを生成して量子ユニット１００へ供給する。

【００５７】

受信側同期部３００（図１の受信側同期部３に対応）は、光電変換器（Ｏ／Ｅ）３０１、遅延素子３０２と、位相比較器３０３、および、電光変換器（Ｅ／Ｏ）３０４を有する。Ｏ／Ｅ３０１は、送信器から波長λ３の古典チャネル４０２を通して受信した光クロック信号を電気信号に変換し、そのクロック信号を折り返し信号としてＥ／Ｏ３０４へ出力し、さらに遅延素子３０２および量子ユニット２００のレーザ駆動回路２１２へ出力する。

【００５８】

Ｅ／Ｏ３０４はＯ／Ｅ３０１から受け取った折り返し用のクロック信号を波長λ２の光クロック信号に変換し、波長λ２の古典チャネル４０２を通して送信器へ送出する。これと同時に、Ｏ／Ｅ３０１から受け取った同じクロック信号に従ってレーザ駆動回路２１２はレーザＬＤ２１１を駆動し波長λ１の光パルスを発生させる。その時の光パルスの幅は、上述したように、量子モードおよびトレーニングモードのいずれであるかによって制御される。

【００５９】

トレーニングモード時であれば、受信器から量子チャネル４０１を通して送信器へ到達した波長λ１の光パルスは、送信器側で光減衰も位相変調もされないで折り返され、同じく量子チャネル４０１を通して受信器に到達し、ＡＰＤ２４２によって検出される。ＡＰＤ２４２により検出されたクロック信号は位相比較器３０３によって古典チャネル４０２を通したクロック信号と位相比較され、上述したような遅延調整が行われる。これにより較正クロック信号ＣＬＫが生成され、量子ユニット２００へ供給される。

【００６０】

上述したように、同期部５００および３００における遅延調整によって、マスタクロック５０４を基準とした量子ユニット１００および２００の同期を確立することができる。

【００６１】

（動作）

図３は本発明の第１実施例による量子暗号鍵配布システムにおける送信側および受信側のモード切替え動作を示すフローチャートである。まず、送信器１０および受信器２０の通信制御部（図示せず）はそれぞれ電源オンになると、トレーニングモード切替信号を発生し（ステップＳ１）、それによって送信側の量子ユニット１００および受信側の量子ユニット２００はそれぞれトレーニングモードに遷移する（トレーニングモード：ステップＳ２）。

【００６２】

トレーニングモードは、量子チャネル４０１の光パワーが通常の通信に用いられる程度の強い光で通信するモードである。このトレーニングモード時の強い光は、受信側のレーザ光パルスを減衰させる光源衰器２１３と送信器側の量子チャネル４０１の光減衰器１３０との減衰量を小さくすることで光パワーを大きくし、かつ、レーザ駆動回路２１２がレーザＬＤ２１１を駆動する駆動電流のパルス幅を広くしてマーク率を量子モードより上げることによって実現する。上述したように、トレーニングモードでは、受信器側におけるＳｈｏｒｔ　Ｐａｔｈ４０４およびＬｏｎｇ　Ｐａｔｈ４０５の別経路を通った光パルスを区別する必要がないからである。

【００６３】

量子チャネル４０１の光パワーが通常の通信に用いられる程度の強い場合には、量子チャネル４０１からのクロック抽出が可能となる。送信側の量子ユニット１００では、Ｏ／Ｅ１４０で受信した光信号からクロック信号を抽出し位相比較器５０３へ出力する。受信側の量子ユニット２００では、ＡＰＤ２４２が光クロック信号を検出して抽出したクロック信号を位相比較器３０３へ出力する。

【００６４】
送信側の量子ユニット１００では、量子チャネル４０１からＯ／Ｅ１４０で抽出したクロックと、古典チャネル４０２からＯ／Ｅ５０１で抽出したクロックとを位相比較器５０３で比較し、ここでの位相差が零となるように遅延素子５０２にフィードバックを行う（Ｄｅｌａｙ調整：ステップＳ３）。
【００６５】
量子チャネル４０１の信号はファラデーミラー１２０で折り返され、位相変調器１１１で変調を加えず、光減衰器１３０で光パワーを絞ることもなく、量子チャネル４０１にそのまま折り返される。
【００６６】
一方、受信側の量子ユニット２００では、ＡＰＤ２４２で量子チャネル４０１の光パルスを受信する。これは、送信側の量子ユニット１００の位相変調器１１１で変調を加えなかったので、送信側の量子ユニット１００での変調位相と受信側の量子ユニット２００での変調位相とが一致し、光パルスのＡＰＤ２４２への出力が一意に定まるためである。
【００６７】
ＡＰＤ２４２で受信されたクロック信号（同期信号）と古典チャネル４０２からＯ／Ｅ３０１で抽出されたクロック信号とは位相比較器３０３で比較され、位相差が零となるように遅延素子３０２にフィードバックされる（Ｄｅｌａｙ調整：ステップＳ３）。
【００６８】
送信側の同期部５００および受信側の同期部３００のそれぞれにおいて位相差がゼロになり遅延素子５０２および３０２の遅延量が決定すると、それぞれの通信制御部は量子モード切替信号を発行する（ステップＳ４）。送信側の量子ユニット１００および受信側の量子ユニット２００は量子モード切替信号を受取ると、量子モードに遷移する（ステップＳ５）。
【００６９】
量子モードは量子チャネル４０１での光パワーが１ｐｈｏｔｏｎ／ｂｉｔと非常に微弱なモードである。この量子モード時の微弱な光は、送信器側の量子チャネル４０１の光減衰器１３０の減衰量を大きくすることで光パワーを微弱にし、かつ、受信器側のレーザ駆動回路２１２がレーザＬＤ２１１を駆動する駆動電流のパルス幅を狭くしてマーク率を下げることによって実現する。受信器側におけるＳｈｏｒｔ　Ｐａｔｈ４０４およびＬｏｎｇ　Ｐａｔｈ４０５の別経路を通った光パルスを区別する必要があるからである。量子暗号鍵生成はこの量子モードで行われる。
【００７０】
この量子モード動作時には、上述した遅延調整による遅延量の確定により、量子ユニット１００および２００はいずれもマスタクロック５０４を基準とした同期状態にある。すなわち、送信側の量子ユニット１００の位相変調器１１１は送信側同期部５００で較正したクロックに同期した信号で駆動し、受信側の量子ユニット２００の位相変調器２２１およびＡＰＤ２４１、２４２は受信側同期部３００で較正したクロックに同期した信号で駆動する。
【００７１】
送信器１０及び受信器２０のそれぞれの通信制御部は、上記量子モードにおいて、異常（例えば、ＤＬＬのｌｏｃｋ異常）の有無を判定する（ステップＳ６）。異常発生が検出されると（ステップＳ６のＹＥＳ）、ステップＳ１に戻って再度トレーニング切替信号を発生させる。異常を検出せず（ステップＳ７のＮＯ）、処理終了も検出しなければ（ステップＳ７のＮＯ）、異常検出処理ステップＳ６を繰り返す。一方、処理が終了すると（ステップＳ７のＹＥＳ）、電源オフとなる。
【００７２】
このように、本実施例では、量子チャネル４０１と古典チャネル４０２との間の波長分散による伝搬遅延差を伝送路によらず自動で較正することができる。その結果、本実施例では、微弱光のためにクロックを抽出することができない量子チャネル４０１に代わって

、波長の異なる古典チャネル４０２で送信側の量子ユニット１００と受信側の量子ユニット２００との同期を確立することができる。

【００７３】

従来、量子チャネルを利用して光パワーレベルが微少な光で通信している時には、受信器にほとんど光は届かないため、例えば送信側がマーク率１／２のデータを送っても、受信側のマーク率が１／２よりもはるかに小さくなり、データの欠損が生じ、正しい周期のクロックを抽出することができなかった。これに対し、本実施例では、トレーニングモードとして、量子チャネル４０１での光パワーを通常の通信に用いられる程度の強い光として通信を行うので、例えば送信側がマーク率１／２のデータを送ると、受信側のマーク率も１／２となり、データの欠損が生じることはなく、正しい周期のクロックを抽出することができる。これを利用することで、量子チャネルおよび古典チャネルの伝搬遅延差が存在しても、送信側および受信側の量子ユニット間の同期を容易に確立することができる。

【００７４】

１．２）第２実施例

図４は本発明の第２実施例による送信側および受信側のモード切替動作を示すフローチャートである。第２実施例では、装置構成自体は図２に示す第１実施例と同様であるから、以下、第２実施例における送信側および受信側のモード切替動作についてのみ説明する。

【００７５】

図４において、ステップＳ１１～Ｓ１３は、第１実施例で説明した図３のステップＳ１～Ｓ３にそれぞれ対応し、トレーニングモードにおける遅延調整が実行され、量子ユニット１００および２００の間の同期が確立される。続くステップＳ１４およびＳ１５により量子モードに移行すると、通信制御部は所定時間のタイマをスタートさせると共に、ＤＬＬのｌｏｃｋ異常等の異常が発生したか否かを判定し（ステップＳ１６）、異常発生が検出されると（ステップＳ１６のＹＥＳ）、ステップＳ１１に戻って再度トレーニング切替信号を発生させる。

【００７６】

異常を検出しない場合は（ステップＳ１６のＮＯ）、通信制御部は所定時間が経過したか否かを判断する（ステップＳ１７）。所定時間の経過を検出せず（ステップＳ１７のＮＯ）、処理終了も検出しなければ（ステップＳ１８のＮＯ）、異常検出処理ステップＳ１６を繰り返す。異常が検出されるか（ステップＳ１６のＹＥＳ）、あるいは所定時間が経過すると（ステップＳ１７のＹＥＳ）、ステップＳ１１に戻ってトレーニングモードに遷移する。また、処理終了を検出すると（ステップＳ１８のＹＥＳ）、電源オフとなる。

【００７７】

このように、本実施例では、上述した第１実施例と同様に、量子チャネル４０１と古典チャネル４０２との間の波長分散による伝搬遅延差を伝送路によらず自動で較正することができる。その結果、微弱光のためにクロックを抽出することができない量子チャネル４０１に代わって、波長の異なる古典チャネル４０２で送信側の量子ユニット１００と受信側の量子ユニット２００との同期を確立することができる。さらに、本実施例では、ステップＳ１７で所定時間の経過をモニタし、所定時間が経過した場合には、再度トレーニングモードに切り替わり、量子ユニット間の同期調整が行われる。したがって、所定時間を適切に設定することで所定時間毎の定期校正が可能となり、さらに信頼性の高い量子暗号鍵配布システムを得ることができる。

【００７８】

１．３）第３実施例

図５は本発明の第３実施例による通信システムの構成を示す概略的ブロック図である。なお、図１に示す構成と同一のブロックおよび同一機能部には同一参照番号を付して詳細な説明は省略する。

【００７９】

図１に示す通信システムでは、光ファイバ５を用いた波長分割多重ＷＤＭ（Wavelength

Division Multiplexing）システムであったが、図５に示す通信システムでは、クロック同期を同じケーブル中の別の光ファイバ５ｂを用いて行う構成となっている。

【００８０】

ＷＤＭでは、光信号の分割・多重を行う際に、分割・多重用の光部品による損失が生ずるが、この損失を避けるために、本実施例ではクロック同期を同じケーブル中の別の光ファイバ５ｂを用いて行う。この場合、光ファイバは同じケーブル内に収容されるため、物理的な長さはほぼ同じとなる。しかしながら、同じケーブル内の複数の光ファイバ各々は、製造上のばらつきによって光の伝送路長が必ずしも同じになるとは限らない。

【００８１】

つまり、本実施例では、量子信号と同期信号とが同じ伝送路上を伝搬するわけではないので、伝送路長が厳密には一致せず、量子信号と同期信号との間には伝搬遅延差が生じる。また、本実施例では、別の光ファイバ５ｂを用いているので、同一波長を使用することもできるが、別波長を使用した場合には量子信号と同期信号との間には波長分散による伝搬遅延差も生じる。これらの伝搬遅延差の較正も、既に説明した同期部３および４の遅延調整により可能となる。具体的なトレーニングモード動作や遅延調整は図１で説明したものと同一であるから省略する。

【００８２】

なお、本発明は、上述した第１～第３実施例で用いたＰｌｕｇ＆Ｐｌａｙ方式のような双方向方式だけでなく、一方向の量子通信の場合でも適用可能であり、量子通信の形態によらず、本発明の技術は有効である。また、マスタクロック４４は、送信側同期部４ではなく、受信側同期部３に設けられても良い。さらに、送信器と受信器との１：１接続だけでなく、１：Ｎ（Ｎは２以上の整数）接続でも構わない。

【００８３】

２．第２実施形態

図６は本発明の第２実施形態による通信システムの概略的構成を示すブロック図である。ここでは、送信器１０と受信器２０とが量子チャネル５１および古典チャネル５２を含む光ファイバ伝送路５により接続されている。量子チャネル５１と古典チャネル５２とは同一伝送路（光ファイバ伝送路５）上の別波長のチャネルである。ただし、本実施形態の古典チャネル５２は複数のチャネルからなる。

【００８４】

送信器１０は量子ユニット１、同期部４、鍵生成制御部６１および通信制御部７１を含み、受信器２０は量子ユニット２、同期部３、鍵生成制御部６２および通信制御部７２を含む。後述するように、量子ユニット１と量子ユニット２とは量子チャネル５１を介して生鍵とよばれる暗号鍵を生成し、送信器１０と受信器２０とは量子チャネル５１および古典チャネル５２の別波長チャネルを用いて、量子ユニット１および２の間で同期を確立する。同期確立後、鍵生成制御部６１および６２は、生成した生鍵を元に古典チャネル５２を介して最終鍵を生成・共有する。

【００８５】

受信器２０の同期部３は、クロック抽出器３１、遅延素子３２、位相比較器３３、マスタクロック３４および鍵生成基準検出部３５を有する。後述するように遅延素子３２は、位相比較器３３の比較結果に依存して遅延量が制御される。送信器１０の同期部４は、クロック抽出器４１、遅延素子４２、位相比較器４３、および、鍵生成基準発生部４４を有する。後述するように遅延素子４２は、位相比較器４３の比較結果に依存して遅延量が制御される。

【００８６】

送信側および受信側の量子ユニット１および量子ユニット２は、それぞれの通信制御部７１および７２からトレーニングモード切替信号を受取ることでトレーニングモードに移行する。トレーニングモードでは、量子チャネル５１に古典チャネルレベルの強さの光信号を伝送することで、各量子ユニットにおいてクロック抽出が可能となる。

【００８７】

たとえば、トレーニングモード切替信号を入力すると、受信側の量子ユニット２はマスタクロック３４のクロック信号に従って通常の通信に用いられる程度の強い光を量子チャネル５１に送出する。送信側の量子ユニット１は、量子チャネル５１から受信した光クロック信号からクロックを抽出し位相比較器４３へ出力するとともに、その光クロック信号を受信器側へ折り返す。

【００８８】

マスタクロック３４は、量子ユニット２へ供給した同じクロック信号を古典チャネル５２を通して送信器１０へ送出する。送信器１０の同期部４におけるクロック抽出部４１は、古典チャネル５２を通して受信した信号からクロック信号を抽出し、それを古典チャネル５２へそのまま折り返し返送する。また、抽出されたクロック信号は、遅延素子４２で遅延され、位相比較器４３、鍵生成基準発生部４４および量子ユニット１へ出力される。

【００８９】

位相比較器４３は、量子ユニット１でモニタされた量子チャネル５１のクロック信号と遅延素子４２から入力した古典チャネル５２のクロック信号との位相比較を行い、その位相のずれを補償するように遅延素子４２の遅延量を制御する。すなわち、位相比較器４３および遅延素子４２は遅延ロックループＤＬＬを構成する。

【００９０】

受信器２０の同期部３におけるクロック抽出部３１は、古典チャネル５２を通して送信器１０から折り返されてきたクロック信号を抽出する。抽出されたクロック信号は遅延素子３２で遅延され、位相比較器３３および量子ユニット２へ出力される。位相比較器３３は、量子ユニット２でモニタされた量子チャネル５１のクロック信号と遅延素子３２から入力した古典チャネル５２のクロック信号との位相比較を行い、その位相のずれを補償するように遅延素子３２の遅延量を制御する。すなわち、位相比較器３３および遅延素子３２は遅延ロックループＤＬＬを構成する。

【００９１】

このようにして送信器１０および受信器２０において遅延量の調整が行われ、マスタクロック３４を基準とした同期が確立される。同期が確立されると、送信器１０および受信器２０の量子ユニット１および２は、それぞれ同期したクロック信号に従って、次に述べる鍵生成同期処理を行うことができる。

【００９２】

上述したように、トレーニングモードでは量子チャネル５１に古典チャネルレベルの強さの光信号を伝送することで、各量子ユニットにおいてクロック抽出が可能となる。したがって、鍵生成基準発生部４４で生成された鍵生成基準信号を量子チャネル５１および古典チャネル５２の両方を介して受信器２０へ送信することで、受信器２０の鍵生成基準検出部３５が量子チャネル５１、古典チャネル５２それぞれを介して受信した鍵生成基準信号の位相差を検出することが可能となる。こうして量子チャネル５１と古典チャネル５２とを用いて鍵生成同期を確立することができる。

【００９３】

なお、送信器１０および受信器２０の間では、トレーニングモード、鍵生成同期処理モードあるいは量子モードへの切替え時に、古典チャネル５２を介して相互にその切替え要求およびそれに対する応答がやりとりされ、それらの切替えが通知される。送信器１０および受信器２０の通信制御部７１および７２は、この切替えの通知に従ってトレーニングモード切替信号、鍵生成同期処理切替信号または量子モード切替信号を出力する。

【００９４】

なお、送信器１０の鍵生成制御部６１および通信制御部７１と、受信器２０の鍵生成制御部６２および通信制御部７２とは、それぞれプログラム制御プロセッサ上で後述する通信制御および鍵生成同期制御のプログラムを実行することにより実現することもできる。

【００９５】

２．１）第４実施例

次に、上記第２実施形態による通信システムをＰｌｕｇ＆Ｐｌａｙ方式の量子暗号鍵配

布システムに適用した一例を詳細に説明する。ただし、Ｐｌｕｇ＆Ｐｌａｙシステムの基本的な構成および動作は、図１１を用いて既に説明しているので詳細は省略する。

【００９６】

（構成）

図７は本発明の第４実施例によるＰｌｕｇ＆Ｐｌａｙ方式の量子暗号鍵配布システムを示すブロック図である。本実施例では、波長λ１の量子チャネル４０１（図６の量子チャネル５１）と、波長λ２およびλ３の同期信号用の古典チャネル４０２と、波長λ４およびλ５の鍵生成用の古典チャネル４０３（図６の古典チャネル５２）とが用いられる。波長多重分離器６０１および６０２は光ファイバ伝送路４００（図６の光ファイバ５）を通して接続されている。

【００９７】

波長λ１の量子チャネル４０１は量子ユニット１００および２００にそれぞれ接続され、波長λ２およびλ３の同期信号用の古典チャネル４０２は同期部３００および５００にそれぞれ接続されている。さらに、波長λ４およびλ５の鍵生成用の古典チャネル４０３はＥ／Ｏ６１１およびＯ／Ｅ６１２を介して鍵生成制御部６１０に、Ｏ／Ｅ６２１およびＥ／Ｏ６２２を介して鍵生成制御部６２０に、それぞれ接続されている。

【００９８】

送信側の量子ユニット１００は、位相変調器１１１、変調器駆動回路１１２、遅延調整回路１１３、ファラデーミラー１２０、および、光減衰器１３０を有し、さらに乱数Ｒ１およびＲ２と鍵生成基準信号とのいずれかを選択するセレクタ１１４、および、量子チャネルモニタ用の光電変換器（Ｏ／Ｅ）１４０を有する。

【００９９】

トレーニングモード時には、位相変調器１１１は位相変調を行わず、光減衰器１３０は強い光を送出するために減衰量を小さく設定する。

【０１００】

鍵生成同期処理時にはセレクタ１１４は鍵生成基準信号を選択する。位相変調器１１１は、鍵生成基準信号の０／１に従って、ファラデーミラー１２０から反射した光パルスを０／πの位相で変調する。また、強い光を送出するために光減衰器１３０の減衰量は小さく設定される。

【０１０１】

量子モード時にはセレクタ１１４は乱数Ｒ１およびＲ２を選択する。位相変調器１１１は、同期部５００からの較正クロック信号に従って、乱数Ｒ１およびＲ２の組み合わせに対応する０、π／２、π、３／２πの４つの位相でファラデーミラー１２０から反射した光パルスを変調する。また、光減衰器１３０は微弱な光を送出するために減衰量を大きくする。これらの動作モードの切り替えは通信制御部７１（図６参照）により制御される。

【０１０２】

受信側の量子ユニット２００は、波長λ１のパルス光源であるレーザＬＤ２１１と、そのドライバであるレーザ駆動回路２１２とを有し、波長λ１の光パルスが光減衰器２１３を通して光サーキュレータ２５０に入射する。光サーキュレータ２５０から出射した光パルスは、光カプラ４０６によって短経路（Ｓｈｏｒｔ　Ｐａｔｈ）４０４と長経路（Ｌｏｎｇ　Ｐａｔｈ）４０５にそれぞれ分岐し、Ｌｏｎｇ　Ｐａｔｈ４０５に分岐した光パルスは位相変調器２２１を介して偏光ビームスプリッタＰＢＳ２３０に入射する。位相変調器２２１は、乱数Ｒ３に従って変調器駆動回路２２２により駆動され、駆動タイミングは遅延調整回路２２３により調整される。

【０１０３】

乱数Ｒ３は鍵生成制御部６２０により供給されるが、１つの値だけを供給して位相変調器２２１の位相を１つに固定することもできる。後述するように、鍵生成同期処理時には、位相変調器２２１の位相を０に固定して、送信器から受信した鍵生成基準信号の値１をＡＰＤ２４２で検出するように設定することができる。

【０１０４】

位相変調器２２１は、量子モード時には、既に述べたように送信器側で折り返された信号がＬｏｎｇ　ｐａｔｈ４０５を通るときに、乱数Ｒ３に従った０、π／２の２つの位相で当該光信号を変調する。そして、送信器側の位相変調器１１１で変調された光信号と受信器側の位相変調器２２１で変調された光信号とが光カプラ４０６で干渉し、その結果がアバランシェ光ダイオード（Avalanche Photo Diode）ＡＰＤ２４１またはＡＤＰ２４２で検出される。なお、Ｓｈｏｒｔ　Ｐａｔｈ４０４およびＬｏｎｇ　Ｐａｔｈ４０５は偏波保存ファイバ、光サーキュレータ２５０、光カプラ４０６は偏波保存型である。

【０１０５】

なお、量子モード時には、Ｓｈｏｒｔ　Ｐａｔｈ４０４およびＬｏｎｇ　Ｐａｔｈ４０５の別経路を通った光パルスが十分区別できるように、レーザＬＤ２１１から出力される光パルスのパルス幅を小さくして必要な間隔を維持する必要がある。しかしながら、トレーニングモード時には量子モード時のような光パルスの間隔を維持する必要はない。したがって、レーザ駆動回路２１２は、量子モードおよびトレーニングモードのいずれであるかによって上記光パルス幅を変化させる。

【０１０６】

送信側同期部５００には、波長λ２の古典チャネル４０２を通して受信器側から受信した光クロック信号を電気信号に変換する光電変換器（Ｏ／Ｅ）５０１、遅延素子５０２、および、位相比較器５０３が設けられている。Ｏ／Ｅ５０１で受信されたクロック信号は遅延素子５０２およびセレクタ５０４へ出力される。

【０１０７】

セレクタ５０４は、通常、Ｏ／Ｅ５０１で受信されたクロック信号を電光変換器（Ｅ／Ｏ）５０５へ転送し、Ｅ／Ｏ５０５はこのクロック信号を波長λ３の光クロック信号に変換し波長λ３の古典チャネル４０２を通して受信器側へ折り返す。

【０１０８】

さらに、同期部５００には鍵生成基準発生部５０６が設けられ、鍵生成同期処理時には鍵生成基準信号を量子ユニット１００のセレクタ１１４と同期部５００のセレクタ５０４へ同時に出力する。セレクタ５０４は、鍵生成同期処理時には鍵生成基準信号を選択してＥ／Ｏ５０５へ転送し、Ｅ／Ｏ５０５はこの鍵生成基準信号を波長λ３の光信号に変換し、波長λ３の古典チャネル４０２を通して受信器側へ送出する。

【０１０９】

位相比較器５０３は、トレーニングモード時において、Ｏ／Ｅ１４０により検出された波長λ１の量子チャネル４０１のクロック信号と遅延素子５０２から入力する古典チャネル４０２のクロック信号との位相比較を行い、上述したような遅延調整により較正クロック信号ＣＬＫを生成する。この較正クロック信号ＣＬＫは、量子ユニット１００の遅延調整回路１１３、鍵生成基準発生部５０６および鍵生成制御部６１０へそれぞれ分配される。

【０１１０】

受信側同期部３００は、光電変換器（Ｏ／Ｅ）３０１、遅延素子３０２、位相比較器３０３、電光変換器（Ｅ／Ｏ）３０４、マスタクロック３０５、鍵生成基準検出部３０６および、セレクタ３０７を有する。マスタクロック３０５のクロック信号は、Ｅ／Ｏ３０４によって波長λ２の光クロック信号に変換されて古典チャネル４０２を通して送信器へ送出され、同時に量子ユニット２００のレーザ駆動回路２１２および鍵生成制御部６２０へそれぞれ出力される。レーザ駆動回路２１２はレーザＬＤ２１１を駆動し波長λ１の光パルスを発生させる。その時の光パルスの幅は、上述したように、量子モードおよびトレーニングモードのいずれであるかによって制御される。

【０１１１】

Ｏ／Ｅ３０１は、送信器から波長λ３の古典チャネル４０２を通して受信した光信号を電気信号に変換し、その受信信号はセレクタ３０７によって遅延素子３０２および鍵生成基準検出部３０５のいずれかへ転送される。セレクタ３０７は、通常、受信信号をクロック信号として遅延素子３０２へ転送するが、鍵生成同期処理時には鍵生成基準信号として

鍵生成基準検出部３０５へ転送する。

【０１１２】

トレーニングモード時には、レーザＬＤ２１１から波長λ１の光パルスが長いパルス幅で出力し、量子チャネル４０１を通して送信器へ到達する。そして、送信器側で光減衰も位相変調もされないでそのまま折り返され、同じく量子チャネル４０１を通して受信器に到達し、ＡＰＤ２４２によってクロック信号として検出される。ＡＰＤ２４２により検出されたクロック信号は位相比較器３０３によって古典チャネル４０２を通したクロック信号と位相比較され、上述したような遅延調整が行われる。これにより較正クロック信号ＣＬＫが生成され、この較正クロック信号によって鍵生成同期処理時および量子モード時の量子ユニット２００の位相変調タイミングが正しく設定される。

【０１１３】

鍵生成同期処理時には、受信器のレーザＬＤ２１１からの波長λ１の光パルスは量子チャネル４０１を通して送信器へ到達し、送信器側で鍵生成基準信号に従って位相変調され、同じく量子チャネル４０１を通して受信器に到達する。位相変調器２２１を所定の位相に固定しておくことで、鍵生成基準信号が１の時のみＡＰＤ２４２によって検出されるように設定でき、ＡＰＤ２４２により検出された鍵生成基準信号が鍵生成基準検出部３０５に入力する。また、古典チャネル４０２を通して受信した鍵生成基準信号がセレクタ３０７を通して鍵生成基準検出部３０５に入力する。鍵生成基準検出部３０５は、これらの鍵生成基準信号のタイミングのずれを検出し、その誤差信号を鍵生成制御部６２０へ出力する。

【０１１４】

なお、送信器および受信器の間では、トレーニングモード、鍵生成同期処理モードあるいは量子モードへの切替え時に、古典チャネル４０２を介して相互にその切替え要求およびそれに対する応答がやりとりされ、それらの切替えが通知される。送信器および受信器の通信制御部７１および７２は、この切替えの通知に従ってトレーニングモード切替信号、鍵生成同期処理切替信号または量子モード切替信号を出力する。

【０１１５】

（トレーニングモード）

図８は本発明の第４実施例によるＰｌｕｇ＆Ｐｌａｙ方式の量子暗号鍵配布システムにおける送信側および受信側のモード切替え動作を示すフローチャートである。まず、送信器１０および受信器２０の通信制御部７１および７２はそれぞれ電源オンになると、トレーニングモード切替信号を発生し（ステップＳ２１）、それによって送信側の量子ユニット１００および受信側の量子ユニット２００はそれぞれトレーニングモードに遷移する（ステップＳ２２）。

【０１１６】

トレーニングモードでは、量子チャネル４０１の光パワーが通常の通信に用いられる程度の強い光で通信することができる。このトレーニングモード時の強い光は、受信側のレーザ光パルスを減衰させる光源衰器２１３と送信器側の量子チャネル４０１の光減衰器１３０との減衰量を小さくすることで光パワーを大きくし、かつ、レーザ駆動回路２１２がレーザＬＤ２１１を駆動する駆動電流のパルス幅を広くしてマーク率を量子モードより上げることによって実現する。上述したように、トレーニングモードでは、受信器側におけるＳｈｏｒｔ　Ｐａｔｈ４０４およびＬｏｎｇ　Ｐａｔｈ４０５の別経路を通った光パルスを区別する必要がないからである。

【０１１７】

また、量子チャネル４０１の光パワーが通常の通信に用いられる程度の強い場合には、量子チャネル４０１からのクロック抽出が可能となる。送信側の量子ユニット１００ではＯ／Ｅ１４０が光クロック信号を電気的クロック信号に変換し位相比較器５０３へ出力する。受信側の量子ユニット２００ではＡＰＤ２４２が光クロック信号を検出して電気的クロック信号を位相比較器３０３へ出力する。

【０１１８】

さらに、トレーニングモードでは、送信器側の同期部５００ではセレクタ５０４がＯ／Ｅ５０１の出力を選択し、受信器側の同期部３００ではセレクタ３０７が遅延素子３０２を選択する。マスタクロック３０５で生成されるクロック信号はＥ／Ｏ３０４によって波長λ２の古典チャネルを通して送信器側へ送出され、同時にレーザ駆動回路２１２を駆動してレーザＬＤ２１１から波長λ１の光パルスを放出する。

【０１１９】

送信側の量子ユニット１００では、量子チャネル４０１からＯ／Ｅ１４０で抽出したクロックと、古典チャネル４０２からＯ／Ｅ５０１で抽出したクロックとを位相比較器５０３で比較し、ここでの位相差が零となるように遅延素子５０２にフィードバックを行う（Ｄｅｌａｙ調整：ステップＳ２３）。

【０１２０】

Ｏ／Ｅ５０１で抽出した古典チャネル４０２のクロック信号は、セレクタ５０４を通してＥ／Ｏ５０５へ出力され、波長λ３の古典チャネル４０２を通して受信器側へ折り返される。また、量子チャネル４０１の光信号はファラデーミラー１２０で折り返され、位相変調器１１１で変調されることなく、光減衰器１３０で光パワーを絞ることもなく、量子チャネル４０１を通して受信器側へそのまま折り返される。

【０１２１】

一方、受信側の量子ユニット２００では、ＡＰＤ２４２で量子チャネル４０１の光パルスを受信する。これは、送信側の量子ユニット１００の位相変調器１１１で変調を加えなかったので、送信側の量子ユニット１００での変調位相と受信側の量子ユニット２００での変調位相とが一致し、光パルスのＡＰＤ２４２への出力が一意に定まるためである。

【０１２２】

また、波長λ３の古典チャネル４０２を通してＯ／Ｅ３０１で受信したクロック信号はセレクタ３０７を通して遅延素子３０２へ出力され、遅延されたクロック信号が位相比較器３０３に入力する。

【０１２３】

ＡＰＤ２４２で受信されたクロック信号（同期信号）と古典チャネル４０２からＯ／Ｅ３０１で抽出されたクロック信号とは位相比較器３０３で比較され、位相差が零となるように遅延素子３０２にフィードバックされる（Ｄｅｌａｙ調整：ステップＳ２３）。

【０１２４】

（鍵生成同期）

送信側の同期部５００および受信側の同期部３００のそれぞれにおいて位相差がゼロになり遅延素子５０２および３０２の遅延量が決定すると、それぞれの通信制御部７１および７２は鍵生成同期処理へ移行する（ステップＳ２４）。

【０１２５】

鍵生成同期処理に移行すると、送信器の通信制御部７１は、セレクタ１１４およびセレクタ５０４をそれぞれ鍵生成基準信号を選択するように切り替え、鍵生成基準発生部５０６は較正クロック信号ＣＬＫのタイミングに従って鍵生成基準信号を出力する。これによって、鍵生成基準信号が変調器駆動回路１１２へ入力する。位相変調器１１１は較正クロックＣＬＫのタイミングで動作し、鍵生成基準信号の０／１に従ってファラデーミラー１２０からの反射光を０／πでそれぞれ位相変調して受信器へ送信する。同時に、鍵生成基準信号はセレクタ５０４を介してＥ／Ｏ５０５へ転送され、波長λ３の古典チャネルを通して受信器へ送信される。

【０１２６】

鍵生成同期処理に移行すると、受信器の通信制御部７２は、セレクタ３０７を鍵生成基準検出部３０６側へ切り替え、波長λ３の古典チャネルを通して受信した鍵生成基準信号を鍵生成基準検出部３０６へ転送する。また、通信制御部７２は鍵生成制御部６２０に指示して位相変調器２２１の位相を０に固定する。これによって、位相変調器２２１は較正クロックＣＬＫのタイミングで、送信器の位相変調器１１１で位相変調された光信号を位相変調し、受信した光信号を鍵生成基準信号が０の時はＡＰＤ２４１で、１の時はＡＰＤ

２４２でそれぞれ検出する。

【０１２７】

鍵生成基準検出部３０６は、古典チャネル４０２から受信した鍵生成基準信号と量子チャネル４０１からＡＰＤ２４２で受信した鍵生成基準信号との検出タイミングを比較し、その結果を鍵生成制御部６２０へ通知する。この検出タイミングの誤差を補償することで、図１０で説明したような鍵生成のためのビット同期を確立することができる。検出タイミングの通知が完了すると、通信制御部７２は量子モード切替信号を発生し、鍵生成制御部６２０を量子モードへ移行させるとともに、古典チャネル４０３を通して量子モード切替要求を送信器へ送信し、送信器の鍵生成制御部６１０も量子モードに移行させる（ステップＳ２５）。

【０１２８】

こうして遅延調整（ステップＳ２３）および鍵生成同期（ステップＳ２４）によって、量子チャネルのクロック同期および鍵生成ビット同期の確立が可能となる。

【０１２９】

（量子モード）

量子モードは量子チャネル４０１での光パワーが１ｐｈｏｔｏｎ／ｂｉｔと非常に微弱なモードである。この量子モード時の微弱な光は、送信器側の量子チャネル４０１の光減衰器１３０の減衰量を大きくすることで光パワーを微弱にし、かつ、受信器側のレーザ駆動回路２１２がレーザＬＤ２１１を駆動する駆動電流のパルス幅を狭くしてマーク率を下げることによって実現する。受信器側におけるＳｈｏｒｔ　Ｐａｔｈ４０４およびＬｏｎｇ　Ｐａｔｈ４０５の別経路を通った光パルスを区別する必要があるからである。量子暗号鍵生成はこの量子モードで行われる。

【０１３０】

この量子モード動作時には、上述した遅延調整による遅延量の確定により、量子ユニット１００および２００はいずれもマスタクロック３０５を基準とした同期状態にある。すなわち、送信側の量子ユニット１００の位相変調器１１１は、送信側同期部５００で較正したクロックに同期して動作し、受信側の量子ユニット２００の位相変調器２２１およびＡＰＤ２４１、２４２は受信側同期部３００で較正したクロックに同期して動作する。

【０１３１】

送信器１０及び受信器２０のそれぞれの通信制御部７１および７２は、上記量子モードにおいて、異常（例えば、ＤＬＬのｌｏｃｋ異常）の有無を判定する（ステップＳ２７）。異常発生が検出されると（ステップＳ２７のＹＥＳ）、ステップＳ２１に戻って再度トレーニング切替信号を発生させる。異常を検出せず（ステップＳ２７のＮＯ）、処理終了も検出しなければ（ステップＳ２８のＮＯ）、異常検出処理ステップＳ２７を繰り返す。一方、処理が終了すると（ステップＳ２８のＹＥＳ）、電源オフとなる。

【０１３２】

このように、本実施例では、量子チャネル４０１と古典チャネル４０２との間の波長分散による伝搬遅延差を伝送路によらず自動で較正することができる。その結果、本実施例では、微弱光のためにクロックを抽出することができない量子チャネル４０１に代わって、波長の異なる古典チャネル４０２で送信側の量子ユニット１００と受信側の量子ユニット２００との同期を確立することができる。

【０１３３】

従来、量子チャネルを利用して光パワーレベルが微少な光で通信している時には、受信器にほとんど光は届かないため、例えば送信側がマーク率１／２のデータを送っても、受信側のマーク率が１／２よりもはるかに小さくなり、データの欠損が生じ、正しい周期のクロックを抽出することができなかった。これに対し、本実施例では、トレーニングモードとして、量子チャネル４０１での光パワーを通常の通信に用いられる程度の強い光として通信を行うので、例えば送信側がマーク率１／２のデータを送ると、受信側のマーク率も１／２となり、データの欠損が生じることはなく、正しい周期のクロックを抽出することができる。これを利用することで、量子チャネルおよび古典チャネルの伝搬遅延差が存

在しても、送信側および受信側の量子ユニット間の同期を容易に確立することができる。
【０１３４】
さらに、本実施例によれば、量子ユニット間で同期が確立すると、それに基づいて鍵生成基準信号を送信器から受信器へ量子チャネルおよび古典チャネルの両方を通して同時に送信し、受信器側で両チャネルの検出タイミングを比較することで鍵生成同期を容易に且つ高精度に確立することができる。
【０１３５】
２．２）第５実施例
図９は本発明の第５実施例による送信側および受信側のモード切替動作を示すフローチャートである。第５実施例では、装置構成自体は図７に示す第４実施例と同様であるから、以下、第５実施例における送信側および受信側のモード切替動作についてのみ説明する。
【０１３６】
図４において、ステップＳ３１～Ｓ３４は、第４実施例で説明した図８のステップＳ２１～Ｓ２４にそれぞれ対応し、トレーニングモードにおける遅延調整および鍵生成同期処理が実行され、量子ユニット１００および２００の間のクロック同期および鍵生成同期が確立される。続くステップＳ３５およびＳ３６により量子モードに移行すると、通信制御部は所定時間のタイマをスタートさせると共に、ＤＬＬのｌｏｃｋ異常等の異常が発生したか否かを判定し（ステップＳ３７）、異常発生が検出されると（ステップＳ３７のＹＥＳ）、ステップＳ３１に戻って再度トレーニング切替信号を発生させる。
【０１３７】
異常を検出しない場合は（ステップＳ３７のＮＯ）、通信制御部は所定時間が経過したか否かを判断する（ステップＳ３８）。所定時間の経過を検出せず（ステップＳ３８のＮＯ）、処理終了も検出しなければ（ステップＳ３９のＮＯ）、異常検出処理ステップＳ３７を繰り返す。異常が検出されるか（ステップＳ３７のＹＥＳ）、あるいは所定時間が経過すると（ステップＳ３８のＹＥＳ）、ステップＳ３１に戻ってトレーニングモードに遷移する。また、処理終了を検出すると（ステップＳ３９のＹＥＳ）、電源オフとなる。
【０１３８】
このように、本実施例では、上述した第４実施例と同様に、量子チャネル４０１と古典チャネル４０２との間の波長分散による伝搬遅延差を伝送路によらず自動で較正することができる。その結果、微弱光のためにクロックを抽出することができない量子チャネル４０１に代わって、波長の異なる古典チャネル４０２で送信側の量子ユニット１００と受信側の量子ユニット２００との同期を確立することができる。
【０１３９】
また、本実施例によれば、量子ユニット間で同期が確立すると、それに基づいて鍵生成基準信号を送信器から受信器へ量子チャネルおよび古典チャネルの両方を通して同時に送信し、受信器側で両チャネルの検出タイミングを比較することで鍵生成同期を容易に且つ高精度に確立することができる。
【０１４０】
さらに、本実施例では、ステップＳ３８で所定時間の経過をモニタし、所定時間が経過した場合には、再度トレーニングモードに切り替わり、量子ユニット間の同期調整および鍵生成同期調整が行われる。したがって、所定時間を適切に設定することで所定時間毎の定期校正が可能となり、さらに信頼性の高い量子暗号鍵配布システムを得ることができる。
【０１４１】
２．３）第６実施例
本発明の第６実施例による通信システムでは、たとえば図５に示す通信システムのように、クロック同期を同じケーブル中の別の光ファイバ５ｂを用いて行い、それ以外の送信器１０および受信器２０の内部構成は図６に示すブロック図と同様である。
【０１４２】

図６に示す通信システムでは、光ファイバ５を用いた波長分割多重ＷＤＭ（Wavelength Division Multiplexing）システムであったが、ＷＤＭでは、光信号の分割・多重を行う際に、分割・多重用の光部品による損失が生ずる。この損失を避けるために、本実施例ではクロック同期を同じケーブル中の別の光ファイバ５ｂを用いて行う。この場合、光ファイバは同じケーブル内に収容されるため、物理的な長さはほぼ同じとなる。しかしながら、同じケーブル内の複数の光ファイバ各々は、製造上のばらつきによって光の伝送路長が必ずしも同じになるとは限らない。

【０１４３】

つまり、本実施例では、量子信号と同期信号とが同じ伝送路上を伝搬するわけではないので、伝送路長が厳密には一致せず、量子信号と同期信号との間には伝搬遅延差が生じる。また、本実施例では、別の光ファイバ５ｂを用いているので、同一波長を使用することもできるが、別波長を使用した場合には量子信号と同期信号との間には波長分散による伝搬遅延差も生じる。これらの伝搬遅延差の較正も、既に説明した同期部３および４の遅延調整により可能となる。具体的なトレーニングモード動作や遅延調整および鍵生成同期調整は第４実施例で説明したものと同一であるから省略する。

【０１４４】

なお、本発明は、上述した第４～第６実施例で用いたＰｌｕｇ＆Ｐｌａｙ方式のような双方向方式だけでなく、一方向の量子通信の場合でも適用可能であり、量子通信の形態によらず、本発明の技術は有効である。また、マスタクロック３４は、受信側同期部３ではなく、送信側同期部４に設けられても良い。さらに、送信器と受信器との１：１接続だけでなく、１：Ｎ（Ｎは２以上の整数）接続でも構わない。

【図面の簡単な説明】

【０１４５】

【図１】本発明の第１実施形態による通信システムの概略的構成を示すブロック図である。

【図２】本発明の第１実施例によるＰｌｕｇ＆Ｐｌａｙ方式の量子暗号鍵配布システムを示すブロック図である。

【図３】本発明の第１実施例による量子暗号鍵配布システムにおける送信側および受信側のモード切替え動作を示すフローチャートである。

【図４】本発明の第２実施例による送信側および受信側のモード切替動作を示すフローチャートである。

【図５】本発明の第３実施例による通信システムの構成を示す概略的ブロック図である。

【図６】本発明の第２実施形態による通信システムの概略的構成を示すブロック図である

【図７】本発明の第４実施例によるＰｌｕｇ＆Ｐｌａｙ方式の量子暗号鍵配布システムを示すブロック図である。

【図８】本発明の第４実施例によるＰｌｕｇ＆Ｐｌａｙ方式の量子暗号鍵配布システムにおける送信側および受信側のモード切替え動作を示すフローチャートである。

【図９】本発明の第５実施例による送信側および受信側のモード切替動作を示すフローチャートである。

【図１０】ＢＢ８４に従った鍵共有手順ステップ１～８を説明するための模式図である。

【図１１】Ｐｌｕｇ＆Ｐｌａｙ方式の量子暗号鍵配布システムの従来例を示す概略的ブロック図である。

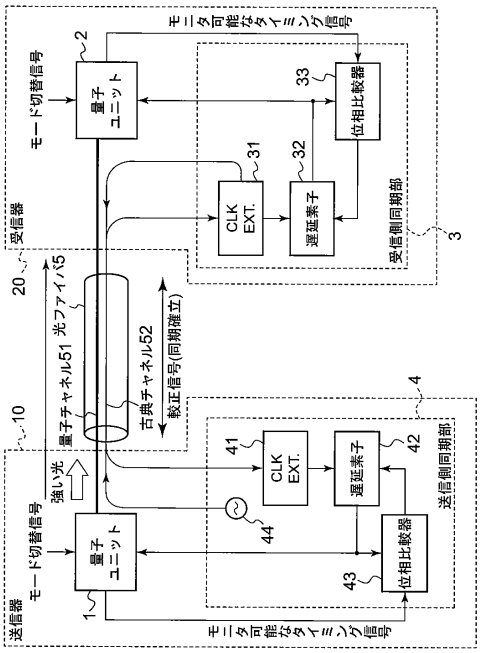
【符号の説明】

【０１４６】

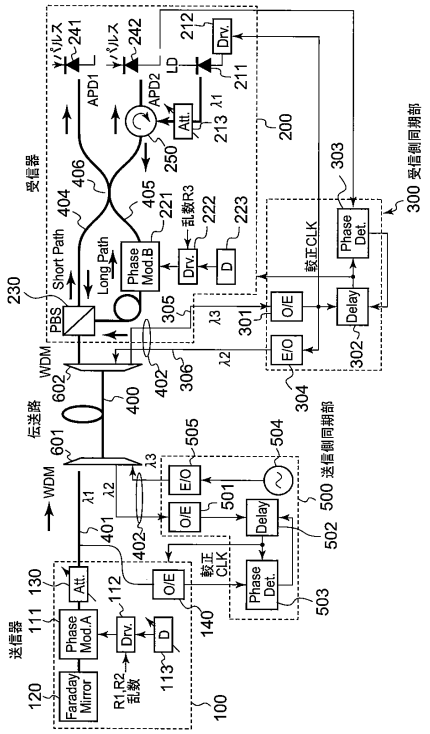
１，１００　送信側の量子ユニット
２，２００　受信側の量子ユニット
３，３００　受信側同期部
４，５００　送信側同期部
５，５ａ，５ｂ，４００　光ファイバ伝送路
１０　送信器

２０　受信器
３１，４１　クロック抽出器
３２，４２　遅延素子
３３，４３，３０３，５０３　位相比較器
３４，３０５　クロック源
５１，４０１　量子チャネル
５２，４０２、４０３　古典チャネル
１１１，２２１　位相変調器
１１２，２２２　変調器駆動回路
１１３，２２３　遅延調整回路
１２０　ファラデーミラー
１３０　光減衰器
１４０，３０１，５０１、６１２、６２１　光電変換器（Ｏ／Ｅ）
２１１　レーザ
２１２　レーザ駆動回路
２１３　光減衰器
２３０　ＰＢＳ
２４１，２４２　ＡＰＤ
２５０　光サーキュレータ
４０４　Ｓｈｏｒｔ　Ｐａｔｈ
４０５　Ｌｏｎｇ　Ｐａｔｈ
４０６　光カップラ
３０２，５０２　遅延素子
３０７、５０４　セレクタ
３０４，５０５、６１１、６２１　電光変換器（Ｅ／Ｏ）
６０１，６０２　波長多重分離器
４４、５０６　鍵生成基準発生部
３５、３０６　鍵生成基準検出部
６１、６２、６１０、６２０　鍵生成制御部
７１、７２　通信制御部

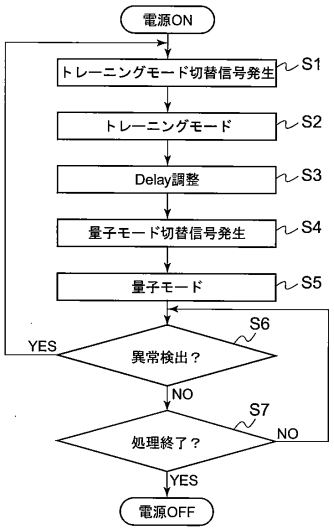
【図１】


モニタ可能なタイミング信号
モード切替信号
量子ユニット
位相比較器
受信器
CLK EXT.
遅延素子
受信側同期部
光ファイバ5
量子チャネル51
古典チャネル52
較正信号(同期確立)
強い光
送信側同期部
送信器

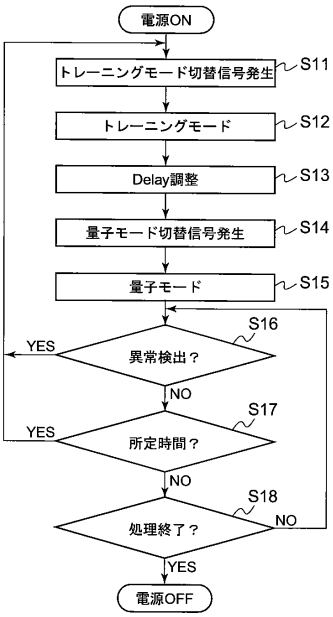
【図２】


受信器
送信器
伝送路
WDM
PBS
Short Path
Long Path
Phase Mod.B
Phase Mod.A
Faraday Mirror
APD1
APD2
Att.
Drv.
D
E/O
O/E
Delay
Phase Det.
較正CLK
受信側同期部
送信側同期部

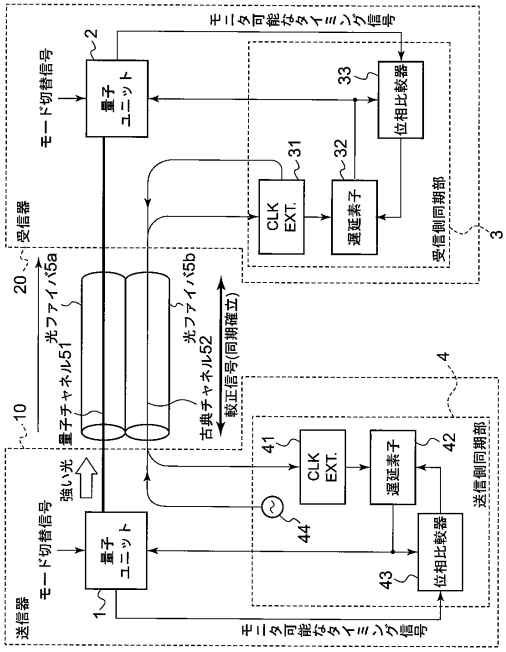
【図３】


電源ON
トレーニングモード切替信号発生
S1
トレーニングモード
S2
Delay調整
S3
量子モード切替信号発生
S4
量子モード
S5
異常検出？
S6
YES
NO
処理終了？
S7
NO
YES
電源OFF

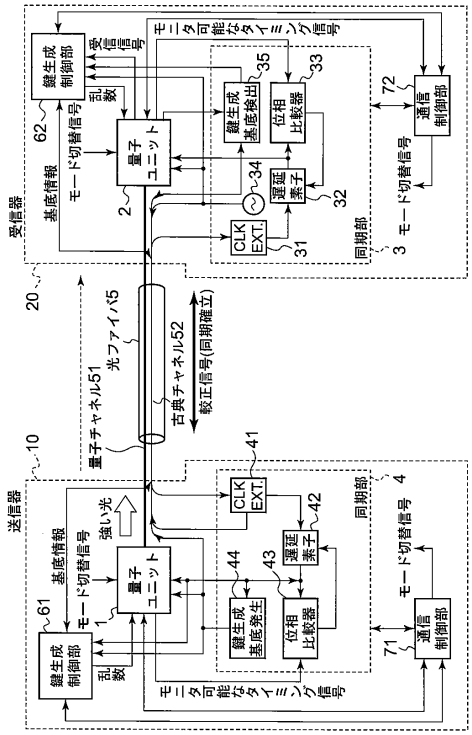
【図４】


電源ON
トレーニングモード切替信号発生
S11
トレーニングモード
S12
Delay調整
S13
量子モード切替信号発生
S14
量子モード
S15
異常検出？
S16
YES
NO
所定時間？
S17
YES
NO
処理終了？
S18
NO
YES
電源OFF

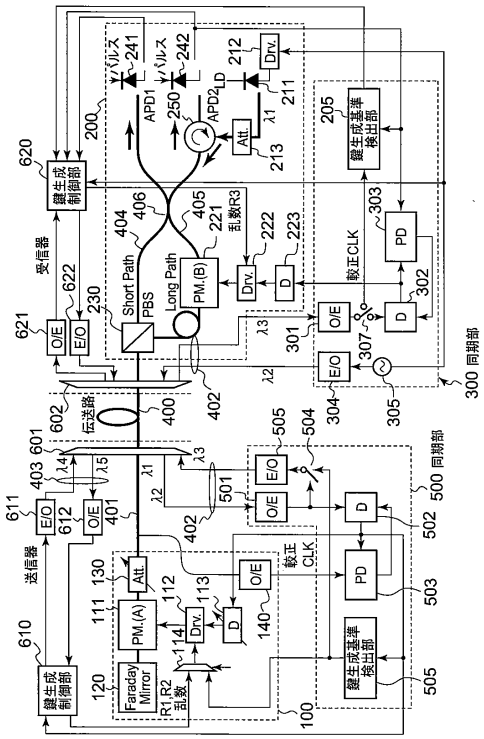
【図５】


送信器
受信器
量子ユニット
モード切替信号
強い光
量子チャネル51
古典チャネル52
光ファイバ5a
光ファイバ5b
較正信号(同期確立)
モニタ可能なタイミング信号
CLK EXT.
遅延素子
位相比較器
受信側同期部
送信側同期部

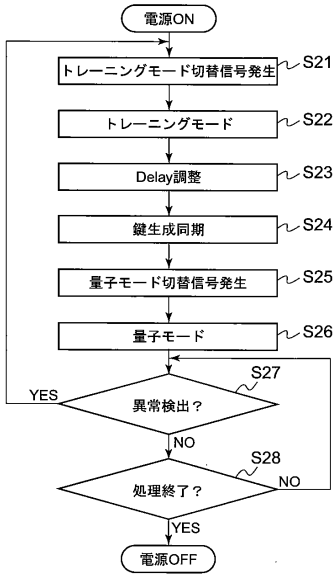
【図６】


送信器
受信器
鍵生成制御部
量子ユニット
基底情報
モード切替信号
乱数
強い光
量子チャネル51
古典チャネル52
較正信号(同期確立)
モニタ可能なタイミング信号
鍵生成基底発生
鍵生成基底検出
位相比較器
遅延素子
CLK EXT.
同期部
通信制御部

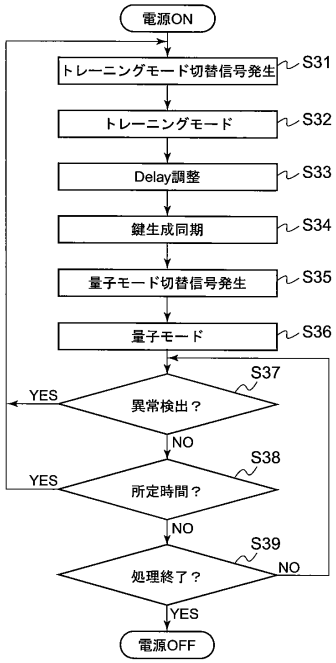
【図７】


送信器
受信器
鍵生成制御部
量子ユニット
Short Path
Long Path
PBS
APD1
APD2
LD
PM.(A)
PM.(B)
Faraday Mirror
Att.
Drv.
E/O
O/E
D
PD
伝送路
較正CLK
鍵生成基準検出部
同期部

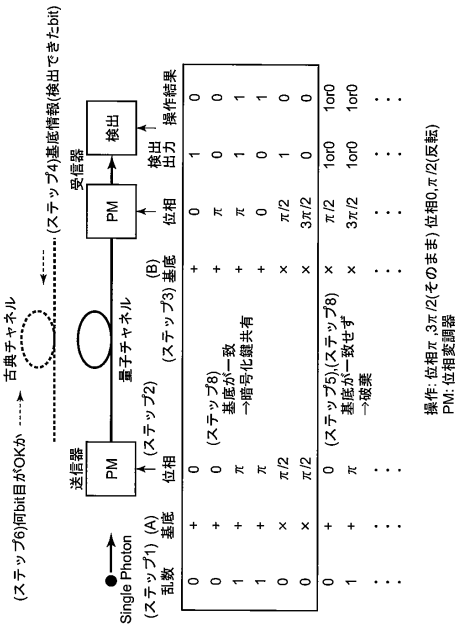
【図８】


電源ON
トレーニングモード切替信号発生
S21
トレーニングモード
S22
Delay調整
S23
鍵生成同期
S24
量子モード切替信号発生
S25
量子モード
S26
異常検出？
S27
YES
NO
処理終了？
S28
NO
YES
電源OFF

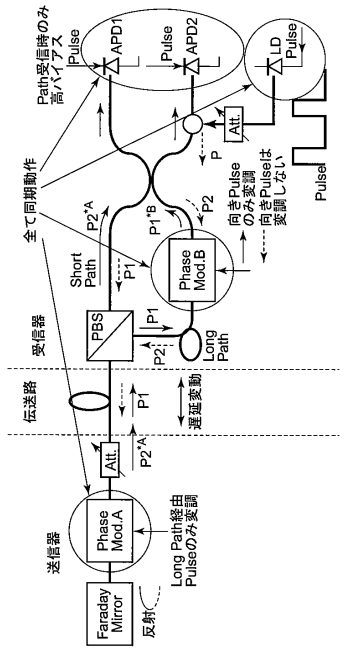
【図９】


電源ON
トレーニングモード切替信号発生
S31
トレーニングモード
S32
Delay調整
S33
鍵生成同期
S34
量子モード切替信号発生
S35
量子モード
S36
異常検出？
S37
YES
NO
所定時間？
S38
YES
NO
処理終了？
S39
NO
YES
電源OFF

【図１０】


(ステップ6)何bit目がOKか
古典チャネル
(ステップ4)基底情報(検出できたbit)
送信器
PM
量子チャネル
受信器
PM
検出
Single Photon
(ステップ1) (A)
乱数 基底
(ステップ2)
位相
(ステップ3) 基底
(B)
位相
検出
出力
操作結果
0 + 0 + 0 0 1 0
0 + 0 (ステップ8) 基底が一致 + π 0 0
1 + π →暗号化鍵共有 + π 1 1
1 + π + 0 0 1
0 × π/2 × π/2 1 0
0 × π/2 × 3π/2 0 0
0 + 0 (ステップ5),(ステップ8) × π/2 1or0 1or0
1 + π 基底が一致せず × 3π/2 1or0 1or0
→破棄
操作: 位相π,3π/2,(ステップ4)(そのまま) 位相0,π/2(反転)
PM: 位相変調器

【図１１】


Path受信時のみ高バイアスPulse
APD1
Pulse
APD2
LD
Pulse
Att.
P
全て同期動作
向きPulseのみ変調
向きPulseは変調しない
Pulse
P2'A
P1'B
P2
Short Path
P1
Phase Mod.B
PBS
P1
P2
Long Path
受信器
伝送路
P1
遅延変動
Att.
P2'A
送信器
Phase Mod.A
Long Path経由Pulseのみ変調
Faraday Mirror
反射

フロントページの続き

(72)発明者　田中　聡寛
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　鈴木　修司
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　青木　重徳

(56)参考文献　国際公開第９４／０１５４２２（WO，Ａ１）
特開平０８－３４０３２０（ＪＰ，Ａ）
特開平０２－１４２２３１（ＪＰ，Ａ）
特開２００３－３７５９４（ＪＰ，Ａ）
長谷川　俊夫　Toshio　HASEGAWA，量子暗号技術とその将来展望　Quantum Cryptography and Its Future View，情報処理　第４３巻　第８号　IPSJ MAGAZINE，日本，社団法人情報処理学会　Information Processing Society of Japan，２００２年　８月，第43巻，p.866-972

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１２
Ｈ０４Ｂ　１０／００
Ｈ０４Ｌ　　７／０４