

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2007-535228

(P2007-535228A)

(43) 公表日 平成19年11月29日(2007.11.29)

(51) Int. Cl. F I テーマコード (参考)  
 HO4L 9/12 (2006.01) HO4L 9/00 631 5J104

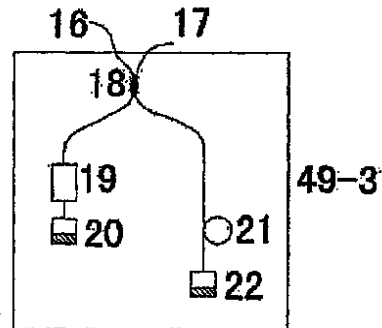
審査請求有 予備審査請求有 (全 22 頁)

(21) 出願番号	特願2006-549831 (P2006-549831)	(71) 出願人	505383316 中国科学技▲術▼大学 中華人民共和国安徽省合肥市金寨路96号
(86) (22) 出願日	平成16年8月19日 (2004.8.19)	(74) 代理人	100064908 弁理士 志賀 正武
(85) 翻訳文提出日	平成18年8月1日 (2006.8.1)	(74) 代理人	100089037 弁理士 渡邊 隆
(86) 国際出願番号	PCT/CN2004/000969	(74) 代理人	100108453 弁理士 村山 靖彦
(87) 国際公開番号	W02005/076517	(74) 代理人	100110364 弁理士 実広 信哉
(87) 国際公開日	平成17年8月18日 (2005.8.18)	(72) 発明者	韓 正甫 中華人民共和国安徽省合肥市金寨路96号
(31) 優先権主張番号	200410013996.6	(72) 発明者	朱 冰 中華人民共和国安徽省合肥市金寨路96号
(32) 優先日	平成16年2月2日 (2004.2.2)		最終頁に続く
(33) 優先権主張国	中国 (CN)		

(54) 【発明の名称】 偏光制御符号化方法、エンコーダ及び量子鍵分配システム

(57) 【要約】

本発明による偏光制御符号化方法、エンコーダ及び量子鍵分配システムは、エンコーダの内部では、偏光保持光路又は90度回転ファラデーミラーでの反射を採用して出力光パルス偏光状態が相同であるようにし、偏光制御エンコーダを核心として量子鍵分配システムを構成して、送信端から出力された光パルスが量子チャンネルを介して受信端に一方向伝送させ、光パルスの干渉重ね結果に応じて、量子鍵分配プロトコルに従って量子鍵分配を実現することを特徴とする。本発明の偏光制御エンコーダによれば、システムは送信装置、受信装置及び量子チャンネルでの干渉に対抗する能力を有する。システムの送信装置の出口及び受信装置の入口に逆方向光子分離検出ユニットを追加することで、木馬光子の侵入と変調情報付けの光子の安全区域からの離脱とを抑制する。本発明の量子鍵分配システムを利用することで、鍵の無条件安全分配を実現できる。



**【特許請求の範囲】****【請求項 1】**

偏光制御符号化方法であって、  
入射された一つの光パルスを二つの光パルスに分波し、二つの異なる光路に沿って伝送させるステップと、

前記二つの光パルスに対して相対遅延を行うステップと、

前記相対遅延された二つのパルスを一つの経路で合波して出力するステップと、を含み

、  
前記方法は、前記分波ステップ又は合波ステップの後に、前記二つの光パルスの少なくとも一つを量子鍵分配プロトコルに従って位相変調するステップと、

前記分波から合波までのプロセスで、前記二つの光パルスの偏光状態を、合波後に出力された二つの光パルスの偏光状態が同じであるように制御するステップと、をさらに含むことを特徴とする偏光制御符号化方法。

10

**【請求項 2】**

前記制御ステップは、前記二つの光パルスの偏光状態を前記分波から合波までのプロセスで一定に保持することを含むことを特徴とする請求項 1 に記載の偏光制御符号化方法。

**【請求項 3】**

前記制御ステップは、前記相対遅延後の二つの光パルスをそれぞれ 90 度回転ファラデーミラーを介して奇数回反射させ、前記分波から合波までのそれぞれの光路を偶数回通過させることを含むことを特徴とする請求項 1 に記載の偏光制御符号化方法。

20

**【請求項 4】**

前記制御ステップは、前記二つの光パルスの一方をそのまま出力させ、他方を 90 度回転ファラデーミラーを介して偶数回反射させ、前記分波から合波までのそれぞれの光路を偶数回通過させることを含むことを特徴とする請求項 1 に記載の偏光制御符号化方法。

**【請求項 5】**

請求項 1 に記載の偏光制御符号化方法に基づいて構成される偏光制御エンコーダであって、

一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させる第 1 の偏光保持ビームスプリッターと、

一方の光パルスを他方の光パルスに対して遅延させる遅延線と、

前記相対遅延された二つの光パルスを一つの光路で合波して出力される第 2 の偏光保持ビームスプリッターと、

前記分波後の二つの光路と合波後の出力光路との三者の少なくとも一つに位置する位相変調器と、を備え、

前記二つの異なる光路は偏光保持光路であることを特徴とする偏光制御エンコーダ。

30

**【請求項 6】**

請求項 1 に記載の偏光制御符号化方法に基づいて構成される偏光制御エンコーダであって、

一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させる偏光保持ビームスプリッターと、

一方の光路に位置し、一方の光パルスを他方の光パルスに対して遅延させる偏光保持遅延線と、

前記相対遅延された二つの光パルスを一つの光路で合波して出力するために、前記相対遅延された二つの光パルスを前記偏光保持ビームスプリッターへ反射させるミラーと、

前記分波後の二つの光路と合波後の出力光路との三者の少なくとも一つに位置する位相変調器と、を備え、

前記二つの異なる光路は偏光保持光路であることを特徴とする偏光制御エンコーダ。

40

**【請求項 7】**

請求項 1 に記載の偏光制御符号化方法に基づいて構成される偏光制御エンコーダであって、

50

一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させるビームスプリッターと、

一方の光路に位置し、一方の光パルスを他方の光パルスに対して遅延させる遅延線と、前記相対遅延された二つの光パルスを一つの光路で合波して出力するために、前記相対遅延された二つの光パルスのそれぞれを前記ビームスプリッターへ反射させさせる二つの90度回転ファラデーミラーと、

前記分波後の二つの光路と合波後の出力光路との三者の少なくとも一つに位置する位相変調器と、を有することを特徴とする偏光制御エンコーダ。

【請求項8】

請求項1に記載の偏光制御符号化方法に基づいて構成される偏光制御エンコーダであって、

一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させ、その一方の光パルスをそのまま出力させる偏光保持可変ビームスプリッターと、

他方の光パルスを反射させ、前記偏光保持可変ビームスプリッターを通過させる第1のミラーと、

前記偏光保持可変ビームスプリッターを通過した他方の光パルスを、そのまま出力された光パルスと一つの光路で合波して出力するために、再び前記偏光保持可変ビームスプリッターへ反射させる第2のミラーと、

前記第1と第2のミラー前の二つの光路中の少なくとも一方に位置する偏光保持遅延線と、

前記ミラー前の二つの光路と合波後の出力光路との三者の少なくとも一つに位置する位相変調器と、を備え、

前記第1と第2のミラー前の光路は偏光保持光路であることを特徴とする偏光制御エンコーダ。

【請求項9】

請求項1に記載の偏光制御符号化方法に基づいて構成される偏光制御エンコーダであって、

一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させ、その一方の光パルスをそのまま出力させる可変ビームスプリッターと、

他方の光パルスを可変ビームスプリッターへ反射させ、可変ビームスプリッターを通過させる第1の90度回転ファラデーミラーと、

前記可変ビームスプリッターを通過した他方の光パルスを、前記そのまま出力された光パルスと一つの光路で合波して出力するために、前記可変ビームスプリッターへ再び反射させる第2の90度回転ファラデーミラーと、

前記第1と第2のミラー前の二つの光路中の少なくとも一方に位置する遅延線と、

前記90度回転ファラデーミラー前の二つの光路と合波後の出力光路との三者の少なくとも一つに位置する位相変調器と、を備えることを特徴とする偏光制御エンコーダ。

【請求項10】

パルス光源から出力された一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させ、前記二つの光パルスの一方を他方に対して相対遅延させ、前記二つのパルスを一つの経路で合波して出力し、前記光パルスの何れかを量子鍵プロトコル規定に従って位相変調する送信端の偏光制御エンコーダと、

前記偏光制御エンコーダから出力された前記二つの光パルスを一方向伝送する量子チャンネルと、

受信された二つの光パルスの各光パルスを、二つの光パルスからなる光パルス群に分波して二つの異なる光路に沿って伝送させ、同じ群となる二つの光パルスに対して量子鍵プロトコル規定に従って相対遅延させ、前記二つの光パルス群を一つの経路で合波して出力し、一つの経路で合波して出力する前に、前記受信した光パルスと分波した光パルスと遅延した光パルスとの少なくとも一つに対して量子鍵プロトコル規定に従って位相変調する受信端の偏光制御エンコーダと、

10

20

30

40

50

前記二つの光パルス群におけるそれぞれの少なくとも一つの光パルスの干渉重ね結果を同期検出し、量子鍵分配プロトコルに従って量子鍵分配を行う単光子検出器と、を備えることを特徴とする量子鍵分配システム。

【請求項 1 1】

送信端偏光制御エンコーダの出口又は受信端偏光制御エンコーダの入口に直列接続した逆方向光子分離検出手段を更に備え、

前記逆方向光子分離検出手段は、光サーキュレータと単光子検出器とからなり、前記光サーキュレータの入力端が偏光制御エンコーダの出力に接続され、前記サーキュレータの同方向出力端が量子チャンネルに接続され、逆方向出力端が単光子検出器に接続されることを特徴とする請求項 1 0 に記載の量子鍵分配システム。

10

【請求項 1 2】

前記逆方向光子分離検出手段は、前記光サーキュレータの入力端に一つの光帯域通過フィルタが直列接続されることを特徴とする請求項 1 1 に記載の量子鍵分配システム。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は、光伝送秘密通信技術分野に属し、特に量子鍵分配における符号化方法及び装置に関する。

【背景技術】

【0 0 0 2】

従来の量子鍵分配は、光子偏光を用いて符号化することになり、このような方式は、自由空間通信に適するが光ファイバー通信体系に適しない。その理由として、普通の光ファイバーは対称性があまり良くなく、伝送経路中の干渉は光の偏光状態に対する影響として現れるので、その中に伝送するときの光の偏光状態を保持できなくなり、偏光符号化も光ファイバーに使用することが好適ではないからである。米国特許第 5 3 0 7 4 1 0 には、一对の非対称アームのマッハツェンダ (M a c h - Z e h n d e r) 干渉計による位相符号化量子鍵分配の技術が開示されており、その受信装置と送信装置内の光パルスは、それぞれマッハツェンダ干渉計の異なるアームを通じており、異なるアームによる干渉が完全に一致することがあり得ないため、互いに完全相殺されることができなくなるので、安定性が悪く、耐干渉の能力が低下する。また、二つの光子パルスはマッハツェンダ干渉計の異なるアームを介して異なる光路を通じ、量子チャンネルに入るときに二つの光子パルスの偏光状態を一定関係に保証できないので、量子チャンネル中の干渉を受けやすく、長程量子鍵分配に際してこのような干渉は特にひどくなり、当該技術の複数の変形例の何れも実質性の改善がなされていない。

20

30

【0 0 0 3】

双不対称アーム M - Z 干渉計に存在した安定性問題に鑑みて、米国「応用物理速報」(A p p l . P h y s . L e t t . 7 7 ( 7 ) , 7 9 3 ( 1 9 9 7 ) ) は、ファラデーミラーによって二つの光パルスを送信点と受信点との間に一回往復させ、各光パルスは全ての光路を一回通して自己補償の効果を奏することができる技術を提案した。この技術は、光子パルスが二回往復で同じ位置を通るときに干渉信号まで変化されなく、光パルスに受ける干渉が一致しており、重なるときに干渉効果が互いに相殺されて耐干渉及び安定化になる目的を達成すると想定される。しかしながら、実際にこのような安定化は、伝送距離がそれほど長くない、かつ干渉周波数があまり高くない場合のみに有効であり、伝送距離が長くなると、光パルスの同一位置を往復に要する時間差が増えるとともに、耐干渉能力も低下する。また、光パルスは量子チャンネルにおいて二回往復することが必要であるので、チャンネルの合計損失は実際量子チャンネルの二倍の長さによる損失と等しくなり、通常、このような欠陥は往路強光と復路単光子の方法を採用して補償するが、このような補償方法は、従来の強減衰レーザ光パルスによって単光子源を模擬する場合のみに適用する。理想量子鍵分配の光源は単光子源であるべきだが、現在、理想的な単光子源がまだ実用化されておらず、理想的な単光子源を使用すると、このような技術案の限界伝送距離は単

40

50

に現在の半分である。さらに、より悪い欠陥は、このような技術案に下記の安全問題が隠れている。即ち、盗聴者は、受信領域に入る前の強信号を比例減衰し、動作波長とごく近接する波長を有する木馬信号（ダミーシグナル）により補充して、受信領域内のトータルモニター信号強度を変化させず、即ち信号強度モニターを無効にさせる。信号が帰還するときに、盗聴者は木馬信号を分離して信号に載せた情報が検出され、更に原始信号光子を「スーパー低損失チャンネル」を介して送信者に回送することができる。盗聴者は信号減衰比例を適当に制御すれば、システムの受信レートに影響を与えず送信者に知られることはない。情報安全技術にとっては、このような盗聴問題が致命的である。

【発明の開示】

【発明が解決しようとする課題】

10

【0004】

本発明は、二つのユーザとの間で盗聴されない量子鍵を形成し、鍵の無条件安全分配を実現できる偏光制御符号化方法、当該方法による偏光制御エンコーダ及びこのようなエンコーダからなる量子鍵分配システムを提供する。

【課題を解決するための手段】

【0005】

本発明による偏光制御符号化方法は、入射された一つの光パルスをもつ二つの光パルスに分波し、両者に対して相対遅延を行い、さらにこの二つのパルスを一つの経路で合波して出力し、分波又は合波した後でこの二つの光パルスの少なくとも一つを量子鍵分配プロトコルに従って位相変調する、即ち符号化、分波から合波までのプロセスでは、出力された二つの光パルスの偏光状態を制御して、合波後に出力されたこの二つの光パルスの偏光状態が同じであるようにすることを特徴とする。

20

【0006】

合波後に出力されたこの二つの光パルスの偏光状態が同じであるようにする前記制御方法は、二つの光パルスを分波から合波までのプロセスで一定の偏光状態に保持し、または、二つの光パルスのそれぞれを90度回転ファラデーミラーを介して奇数回反射させ、分波から合波までのそれぞれの光路を偶数回通過させ、さらにまた、二つの光パルスの一方をそのまま出力させ、他方を90度回転ファラデーミラーを介して偶数回反射させ、分波から合波までのそれぞれの光路を偶数回通過させてもよい。

【0007】

30

本発明の偏光制御符号化方法に基づく第1の偏光制御エンコーダは、一つの光パルスを一つの偏光保持ビームスプリッターによって二つの光パルスに分波して二つの光路に沿って伝送させ、一方の光路は遅延線によって他方の光路に対して遅延された後、さらに偏光保持ビームスプリッターによって一つの光路で合波して出力させ、前記分波後の二つの光路と合波後の出力光路との三者の少なくとも一つには位相変調器を有し、前記偏光保持エンコーダの内部光路の分波から合波までの部分は偏光保持光路であることを特徴とする。

【0008】

本発明の偏光制御符号化方法に基づく第2の偏光制御エンコーダは、一つの光パルスを一つの偏光保持ビームスプリッターによって二つの光パルスに分波して二つの光路に沿って伝送させ、さらにミラーによって反射させ、何れかの光路のミラーの前に偏光保持遅延線を挿入して二つの光路同士が相対遅延されるようにし、元の偏光保持ビームスプリッターによって一つの光路で合波して出力させ、前記分波後の二つの光路と合波後の出力光路との三者の少なくとも一つには位相変調器を有し、前記偏光保持エンコーダの内部光路の分波から合波までの部分は偏光保持光路であることを特徴とする。

40

【0009】

本発明の偏光制御符号化方法に基づく第3の偏光制御エンコーダは、一つの光パルスを一つのビームスプリッターによって二つの光パルスに分波して二つの光路に沿って伝送させ、さらに90度回転ファラデーミラーによって反射させ、何れかの光路の90度回転ファラデーミラーの前に遅延線を挿入してこの二つの光路が相対遅延されるようにし、さらに元のビームスプリッターによって一つの光路で合波して出力させ、前記分波後の二つの

50

光路と合波後の出力光路との三者の少なく一つには位相変調器を有することを特徴とする。

【0010】

本発明の偏光制御符号化方法に基づく第4の偏光制御エンコーダは、一つの光パルスを一つの偏光保持可変ビームスプリッターによって二つの光パルスに分波して二つの光路に沿って伝送させ、その一方の光パルスはそのまま出力させ、他方の光パルスはミラーによって反射させ、元の偏光保持可変ビームスプリッターを通過してからさらにミラーによって反射させ、さらに元の偏光保持可変ビームスプリッターによって前記そのまま出力された光パルスと共に一つの光路で合波して出力させ、前記ミラー前の二つの光路の少なくとも一方には遅延線を有し、前記ミラー前の二つの光路と合波後の出力光路との三者の少なく一つには位相変調器を有し、前記遅延線と位相変調器は、同じ光路に位置するときには前後位置が互換可能であり、前記偏光保持エンコーダの内部光路の分波から合波までの部分は偏光保持光路であることを特徴とする。

10

【0011】

本発明の偏光制御符号化方法に基づく第5偏光制御エンコーダは、一つの光パルスを一つの可変ビームスプリッターによって二つの光パルスに分波して二つの光路に沿って伝送させ、その一方の光パルスはそのまま出力させ、他方の光パルスは90度回転ファラデーミラーによって反射され、元の可変ビームスプリッターを通過してからさらに90度回転ファラデーミラーによって反射させ、また元の可変ビームスプリッターに介して前記そのまま出力された光パルスと共に一つの光路で合波して出力させ、前記ミラー前の二つの光路の少なくとも一方には遅延線を有し、前記90度回転ファラデーミラー前の二つの光路と合波後の出力光路との三者の少なく一つには位相変調器を有し、前記遅延線と位相変調器は、同じ光路に位置するときには前後位置が互換可能であることを特徴とする。

20

【0012】

本発明による量子鍵分配システムは、パルス光源から出力された一つの光パルスを、送信端の偏光制御エンコーダによって二つの光パルスに分波して二つの光路に沿って伝送させ、両方に対して相対遅延させ、さらにこの二つのパルスを一つの経路で合波して出力し、分波又は合波後に少なくとも一つの光パルスを量子鍵プロトコル規定に従って位相変調し、偏光制御エンコーダから出力されたこの二つの光パルスを量子チャンネルに介して受信端に一方向伝送し、受信端の偏光制御エンコーダは、受信されたこの二つの光パルスの各光パルスを、二つの光パルスからなる光パルス群に分波して二つの光路に沿って伝送させ、同じ群となるこの二つの光パルスに対して量子鍵プロトコル規定に従って相対遅延させ、さらにこの二つの光パルス群を一つの経路に合波して出力し、光パルスに対して量子鍵プロトコル規定に従って位相変調し、この二つの光パルス群におけるそれぞれの少なくとも一つの光パルスの干渉重ね結果を単光子検出器によって同期検出し、量子鍵分配プロトコルに従って量子鍵分配を行い、前記五種の偏光制御エンコーダのいずれかが受信端に用いられ且つその位相変調器が出力光路に位置する場合には、当該位相変調器をパルス分波前の入力光路に移動する必要があることを特徴とする。

30

【0013】

当該量子鍵分配システムの送信装置の出口又は受信装置の入口に逆方向光子分離検出手段を直列接続してもよい。逆方向光子分離検出手段は光サーキュレータと単光子検出器とからなり、その光サーキュレータの入力端が偏光制御エンコーダの出力端に接続され、サーキュレータの同方向出力端が量子チャンネルに接続され、逆方向出力端が単光子検出器の入力端に接続される。逆方向光子分離検出手段を追加することで、木馬(ダミー)光子の侵入を抑止するとともに、変調情報付き光子の受信装置の安全区域からの離脱を抑止することもできる。さらに、前記逆方向光子分離検出手段における光サーキュレータの入力端に一つの光帯域通過フィルタが直列接続されてもよい。これによって、光サーキュレータと単光子検出器のレスポンスバンド帯域幅の不足が補充される。

40

【0014】

前記量子チャンネルは、光導波路、光ファイバー、自由空間、独立光学素子、又はそれ

50

らの何れか二つ以上からなる光伝送経路であってもよい。

【発明の効果】

【0015】

従来の両非対称アームのマッハツェンダ干渉計からなるエンコーダと比べると、本発明による偏光制御エンコーダは、その内部で光パルスの偏光状態を制御するので、まず、自身に受ける干渉に対して不敏感となり、量子鍵分配システムの環境に対する要求が大きく低減されるとともに、量子チャンネルに進入された二つの光パルス同士の偏光状態が同じであるため、光パルスの共通経路で受けられた干渉が受信端の干渉重ねに際して互いに相殺され、チャンネル干渉と関係ない信号伝送を実現し、システムの実際安定性が大幅に向上される。本発明による90度回転ファラデーミラー式の偏光制御エンコーダでは、光パルスが位相変調器を二回通過し、且つ通過時の偏光方向が互いに垂直となり、位相変調信号の持続時間が光パルスの二回往復の時間より長くなれば、位相変調の大きさと光パルスの偏光状態とは関係ないので、偏光相関の位相変調器を用いて偏光と関係ない位相変調という目的を達成することができ、位相変調器の速度に対する要求も低減される。本発明による偏光保持ビームスプリッターからなる偏光制御エンコーダは、光パルスが共に特定の偏光状態に保持されるので、当然、偏光相関の位相変調器に適用することもできる。

10

【0016】

本発明の量子鍵分配システムは、送信端と受信端に対して逆方向光子分離検出手段を追加してもよい。逆方向光子分離検出手段を追加することで、信号光パルスが送信装置から量子チャンネルに介して受信装置に一方向伝送されるので、逆方向で伝送された光子を分離し、単光子検出器に導入して検出することができる。これによれば、木馬光子がエンコーダに進入して符号化情報を取り出すことを防止するだけでなく、盗聴者が存在しているか否かを判断でき、木馬で攻撃される可能性が取り除かれる。単光子検出器とサーキュレータとの動作波長が一定範囲にあることを考慮すると、本発明の量子鍵分配システムには、光帯域通過フィルタを追加してもよい。これによれば、システムの動作範囲内の光パルスが通過できるが、動作範囲以外の波長を有する光が通過できないため、単光子検出器とサーキュレータの動作波長範囲幅の不充分の欠陥を改善することができる。

20

【発明を実施するための最良の形態】

【0017】

(実施例1)

本発明の量子鍵分配システムにおける偏光制御エンコーダの第1の構成は、図1に示すように、二つの2×2の3dB偏光保持ビームスプリッター3、6と、一つの偏光保持位相変調器5と、一つの偏光保持遅延線4とを備え、全体として偏光保持マッハツェンダ干渉計を構成する。ここで、3dB偏光保持ビームスプリッター3の一方側の二つのポート1、2の何れかは、偏光制御エンコーダの入力端として機能し、3dB偏光保持ビームスプリッター3の他方側の二つのポート7、8の何れかは出力端として機能する。偏光保持位相変調器5と偏光保持遅延線4(順次は任意)は、共に前記マッハツェンダ干渉計のアームの何れかに挿入されるか、両者が前記マッハツェンダ干渉計の二つのアームにそれぞれ挿入される。動作する時、光パルスは偏光保持ビームスプリッター3のポート1又は2を介して偏光保持ビームスプリッター3に進入して二つの経路に分かれ、その一方は偏光保持位相変調器5を介して位相変調され、他方は偏光保持遅延線4を介して遅延される。相対遅延後の二つの経路の光パルスは、偏光保持ビームスプリッター6を介して一つの経路で合波されてポート7又は8から出力される。全ての光路はともに偏光保持光路であるので、ここから出力される二つのパルスの偏光状態は同じである。偏光保持位相変調器5と偏光保持遅延線4が偏光保持マッハツェンダ干渉計の同一アームに位置する場合には、前記結果にも影響を与えない。

30

40

【0018】

(実施例2)

本発明の量子鍵分配システムにおける偏光制御エンコーダの第2構成は、図2に示すように、一つの2×2の3dB偏光保持ビームスプリッター11と、二つのミラー13、1

50

5 と、一つの偏光保持位相変調器 12 と、一つの偏光保持遅延線 4 とを備える。ここで、3 dB 偏光保持ビームスプリッター 11 の一方側の二つのポート 9, 10 の何れかは、偏光制御エンコーダの入力端と出力端として機能することが可能であり、3 dB 偏光保持ビームスプリッター 11 の他方側の二つのポートの何れかは、偏光保持位相変調器 12 とミラー 13 とに順次に接続され、他のポートは偏光保持遅延線 14 とミラー 15 とに順次に接続される。少し変化があるが同じ機能を有する構成は、偏光保持遅延線 14 と偏光保持位相変調器 12 と（順次は無論）を共に同一のポートに直列接続して、他のポートにただ一つのミラーを接続する。動作する時、光パルスは偏光保持ビームスプリッター 11 のポート 9 に介して偏光保持ビームスプリッター 11 に進入して二つの経路に分け、その一方は偏光保持遅延線 14 に介して遅延されてミラー 15 によって反射され、他方は偏光保持位相変調器 12 に介して位相変調してミラー 13 によって反射される。反射されてくる二つの経路の光パルスは、偏光保持ビームスプリッター 11 を介して一つの経路に合波されてポート 10 から出力される。全ての光路はともに偏光保持光路であるので、ポート 10 から出力される二つのパルスの偏光状態は同じである。偏光保持遅延線 14 と偏光保持位相変調器 12（順次は無論）とが同一のポートに直列接続し、他のポートにただ一つのミラーが接続される場合には、前記結果に影響を与えない。光パルスがポート 10 に入力されポート 9 から出力される場合も、ポート 9 又は 10 を共に入力と出力にする場合と比べて、同じ結果が得られる。

【0019】

（実施例 3）

本発明の量子鍵分配システムにおける偏光制御エンコーダの第 3 構成は、図 3 に示すように、一つの  $2 \times 2$  の 3 dB ビームスプリッター 18 と、二つの 90 度回転ファラデーミラー 20, 22 と、一つの位相変調器 19 と、一つの遅延線 21 とを備える。ここで、3 dB ビームスプリッター 18 の一方側の二つのポート 16, 17 は、それぞれ偏光制御エンコーダの入力端と出力端として機能し、3 dB ビームスプリッター 18 の他方側の二つのポートの何れかは、位相変調器 19 と 90 度回転ファラデーミラー 20 とに順次に接続され、他のポートは遅延線 21 と 90 度回転ファラデーミラー 22 とに順次に接続される。動作する時、光パルスはビームスプリッター 18 のポート 16 に介してビームスプリッター 18 に進入して二つの経路に分かれ、その一方は遅延線 21 を介して遅延されて 90 度回転ファラデーミラー 22 によって反射され、他方は位相変調器 19 を介して位相変調して 90 度回転ファラデーミラー 20 によって反射される。反射されてくる二つの経路の光パルスは、ビームスプリッター 18 を介して一つの経路で合波されてポート 17 から出力される。二つの光路はともに 90 度回転ファラデーミラーによって反射され、それぞれの光路を偶数回通るので、ここから出力される二つのパルスの偏光状態は同じである。光パルスがポート 17 に入力されポート 16 から出力される場合も、ポート 16 又は 17 を共に入力と出力にする場合と比べて、同じ結果が得られる。

【0020】

（実施例 4）

構成が少し変化されるが同じ機能を有する他の偏光制御エンコーダは、図 4 に示すようになり、その区別は下記のようになる、即ち、位相変調器 19 と遅延線 21 と 90 度回転ファラデーミラー 22 とは、カプラーの一つのポート（但し、19 と 21 の順位が置換可能）に順次に接続され、他のポートに一つの 90 度回転ファラデーミラー 20 だけが接続される。動作する時、光パルスはビームスプリッター 18 のポート 16 を介してビームスプリッター 18 に進入して二つの経路に分かれ、その一方は位相変調器 19 を介して位相変調して遅延線 21 を介して遅延されて（順次は無論）から、90 度回転ファラデーミラー 22 によって反射され、他方は 90 度回転ファラデーミラー 20 によって反射される。反射されてくる二つの経路の光パルスは、ビームスプリッター 18 を介して一つの経路で合波されてポート 17 から出力される。二つの光路はともに 90 度回転ファラデーミラーによって反射され、それぞれの光路を偶数回通るので、ここから出力される二つのパルスの偏光状態は同じである。光パルスがポート 17 に入力されポート 16 から出力される場



合も、ポート 16 又は 17 を共に入力と出力にする場合と比べて、同じ結果が得られる。

【0021】

(実施例 5)

本発明の量子鍵分配システムにおける偏光制御エンコーダの第 4 構成は、図 6 に示すよう、一つの  $2 \times 2$  の偏光保持可変ビームスプリッター 25 と、二つのミラー 23, 27 と、一つの偏光保持位相変調器 24 と、一つの偏光保持遅延線 26 とを備える。ここで、偏光保持可変ビームスプリッター 25 の一方側の二つのポートの何れかは、偏光制御エンコーダの出力端 28 として機能し、他のポートは偏光保持遅延線 26 を介してミラー 27 に接続される。偏光保持可変ビームスプリッター 25 の他方側の二つのポートの何れかは、偏光制御エンコーダの入力端 29 として機能し、他のポートは偏光保持位相変調器 24 を介してミラー 23 に接続される。少し変化があるが同じ機能を有する構成は、偏光保持遅延線 26 と偏光保持位相変調器 24 と (順次は無論) を同一のポートに直列接続して、他のポートにただ一つのミラーを接続する。動作する時、光パルスは偏光保持可変ビームスプリッター 25 のポート 29 に介して偏光保持可変ビームスプリッター 25 に進入して二つの経路に分かれており、その一方は偏光保持可変ビームスプリッター 25 のポート 28 からそのまま出力され、他方は偏光保持遅延線 26 を介して遅延されてミラー 27 によって反射されてから、偏光保持可変ビームスプリッター 25 を通じて、偏光保持位相変調器 24 を介して位相変調してミラー 23 によって反射される。反射されてくる光パルスは、偏光保持可変ビームスプリッター 25 を介して、前記そのまま出力された光パルスと共に一つの経路で合波されてポート 28 から出力される。光パルスを分波するとき、ポート 28 から出力された二つの光パルスの幅が同じであるように偏光保持可変ビームスプリッターの分波比率を制御して、全ての光路はともに偏光保持光路であるので、ここから出力される二つの光パルスの偏光状態は同じである。偏光保持遅延線 26 と偏光保持位相変調器 24 と (順次は無論) が同一のポートに直列接続し、他のポートにただ一つのミラーが接続される場合には、前記結果に影響を与えない。パルスがポート 28 に入力されポート 29 から出力される場合も、同じ結果が得られる。

10

20

【0022】

(実施例 6)

本発明の量子鍵分配システムにおける偏光制御エンコーダの第 5 構成は、図 7 に示すように、一つの  $2 \times 2$  の偏光保持可変ビームスプリッター 32 と、二つの 90 度回転ファラデーミラー 30, 34 と、一つの位相変調器 31 と、一つの遅延線 33 とを備える。ここで、可変ビームスプリッター 32 の一方の二つのポートの何れかは、偏光制御エンコーダの出力端 35 として機能し、他のポートは遅延線 33 を介して 90 度回転ファラデーミラー 34 に接続される。可変ビームスプリッター 32 の他方の二つのポートの何れかは、偏光制御エンコーダの入力端 36 として機能し、他のポートは位相変調器 31 を介して 90 度回転ファラデーミラー 30 に接続される。少し変化があるが同じ機能を有する構成は、遅延線 33 と位相変調器 31 と (順次は無論) を同一のポートに直列接続して、他のポートにただ一つの 90 度回転ファラデーミラーを接続する。動作する時、光パルスは可変ビームスプリッター 32 のポート 36 に介して可変ビームスプリッター 32 に進入して二つの経路に分かれ、その一方は可変ビームスプリッター 32 のポート 35 からそのまま出力され、他方は遅延線 33 を介して遅延されて 90 度回転ファラデーミラー 27 によって反射されてから、可変ビームスプリッター 32 を通じて、位相変調器 31 を介して位相変調して 90 度回転ファラデーミラー 30 によって反射される。反射されてくる光パルスは、可変ビームスプリッター 32 を介して、前記そのまま出力された光パルスと共に一つの経路で合波されてポート 35 から出力される。光パルスを分波するとき、ポート 35 から出力された二つのパルスの幅が同じであるように可変ビームスプリッターの分波比率を制御して、二つの光路はともに 90 度回転ファラデーミラーによって反射され、それぞれの光路を偶数回通るので、ここから出力される二つのパルスの偏光状態は同じである。遅延線 33 と位相変調器 31 と (順次は無論) が同一のポートに直列接続し、他のポートにただ一つの 90 度回転ファラデーミラーが接続される場合には、前記結果に影響を与えない

30

40

50

。パルスがポート 35 に入力されポート 36 から出力される場合も、同じ結果が得られる。

【0023】

(実施例 7)

前記実施例に挙げられる五種の偏光制御エンコーダの構成では、位相変調器が出力光路に移動されて同じ位相変調機能を奏することが可能である。例えば、位相変調器が出力光路に位置する偏光制御エンコーダは、図 5 に示すように、一つの 2 × 2 の 3 dB ビームスプリッター 18 と、二つの 90 度回転ファラデーミラー 20, 22 と、一つの位相変調器 19 と、一つの遅延線 21 とを備える。ここで、3 dB ビームスプリッター 18 の一側の二つのポートのうち一つのポート 16 は、偏光制御エンコーダの入力端として機能し、他のポートは位相変調器 19 に接続されてから偏光制御エンコーダの出力端 17 として機能する。3 dB ビームスプリッター 18 の他側の二つのポートの何れかは、90 度回転ファラデーミラー 20 に接続され、他のポートは遅延線 21 と 90 度回転ファラデーミラー 22 とに順次に接続される。前記の偏光制御エンコーダが受信端に使用される場合には、前記の出力光路にある位相変調器がパルス分波前の入力光路に移動される必要がある。例えば、偏光制御エンコーダ 49 - 5 における位相変調器 19 は、ポート 17 に対する直列接続からポート 16 に対する直列接続に変更する必要がある。動作する時、光パルスはビームスプリッター 18 のポート 16 に介してビームスプリッター 18 に進入して二つの経路に分かれており、その一方は遅延線 21 に介して遅延されて 90 度回転ファラデーミラー 22 によって反射され、他方は 90 度回転ファラデーミラー 20 によって反射される。反射されてくる二つの経路の光パルスは、ビームスプリッター 18 を介して一つの経路で合波され、位相変調器 19 によってそれぞれ位相変調してから、ポート 17 から出力される。二つの光路はともに 90 度回転ファラデーミラーによって反射されそれぞれの光路を偶数回通るので、ここから出力される二つのパルスの偏光状態は同じである。このような偏光制御エンコーダが受信端に使用される場合には、前記の出力光路にある位相変調器 19 がパルス分波前の入力光路に移動され、入力された二つの光パルスを位相変調器 19 によってそれぞれ位相変調する必要がある。前記位相変調器が送信端の出力光路に位置する又は受信端の入力光路に位置する場合には、偏光保持特性に対する要求がない。

【0024】

(実施例 8)

本発明の量子鍵分配装置における逆方向光子分離検出ユニットは、光学サーキュレータ 38 と単光子検出器 37 からなる。ここで、サーキュレータの入射ポート 39 は、逆方向光子分離検出ユニットの入力ポートとして機能し、サーキュレータの出射ポート 40 は、逆方向光子分離検出ユニットの同方向出力ポートとして機能する。同方向出力ポート 40 に入射された逆方向光子は、サーキュレータ 38 によって分離されて単光子検出器 37 に導入されて検出され、図 8 に示すようになる。動作する時、サーキュレータの入射ポート 39 に入射された正方向光子は直接に通過して、サーキュレータの出射ポート 40 から出力される。ポート 40 に介して逆方向光子分離検出ユニットに逆方向に進入される光子があれば、サーキュレータ 38 は当該光子のポート 39 からの出力を抑止して、当該光子を単光子検出器 37 に導入し検出して、盗聴木馬光子が存在しているか否かを判断する。それを受信端に使用する場合には、干渉後の信号光子の経路を検出器 37 によって検出し、検出結果を量子鍵情報として使用する。

【0025】

(実施例 9)

サーキュレータと単光子検出器との動作波長範囲に限界があることを考えると、サーキュレータと単光子検出器から離れる波長を有する光子は、偏光制御エンコーダに逆方向に進入する場合もある。少し異なる逆方向光子分離検出ユニットは、図 9 に示すようになる。その異なる点としては、一つの光帯域通過フィルタ 41 を入力ポート 39 の後に増加することにある。動作する時、光帯域通過フィルタ 41 は、システム動作波長範囲内の光を通過させるが、逆方向光子分離検出ユニットの動作波長範囲以外の光子が通過できないよ

10

20

30

40

50

うにすることで、システムの盗聴対抗の能力を向上する。

【0026】

(実施例10)

本発明の偏光制御エンコーダと、逆方向光子分離検出ユニットと、単光子検出器と、パルス光源とを利用して、典型的な量子鍵分配システムを構成することができる。図10に示すように、送信装置は、単光子源42(レーザと強減衰器からなる模擬単光子源に置換可能)と、本発明の偏光制御エンコーダ43と、逆方向光子分離検出ユニット44とからなる。具体的な接続関係は以下ようになる。即ち、偏光制御エンコーダ43(49-1, 49-2, 49-3, 49-6, 49-7又はそれらの変形例の何れかであってもよい)の入力端は単光子光源42の出力ポートに接続し、偏光制御エンコーダ43の出力端は逆方向光子分離検出ユニット44(50-1, 50-2の何れかであってもよい)の入力端に接続し、逆方向光子分離検出ユニット44の同方向出力ポートは、送信装置の信号出力ポートとして安全領域以外にある量子チャンネル45に接続する。

10

【0027】

量子鍵分配システムの受信装置は、本発明の偏光制御エンコーダ47(49-1, 49-2, 49-3, 49-6, 49-7又はそれらの変形例の何れかであってもよいが、特に49-3又は49-7が好ましい)と、逆方向光子分離検出ユニット46(50-1, 50-2の何れかであってもよい)と、単光子検出器48とからなる。具体的な接続関係は以下ようになる。即ち、量子チャンネル45は受信安全領域内に進入して逆方向光子分離検出ユニット46の入力端に接続し、逆方向光子分離検出ユニット46の同方向出力端は偏光制御エンコーダ47の入力端に接続し、偏光制御エンコーダ47の出力端は単光子検出器48に接続する。

20

【0028】

量子鍵分配方法では、送信者が、まず単光子源42によって一つの単光子パルス(実際には、その代わりに強減衰のパルスレーザ光を採用してもよく、各パルスに含まれた光子数が1以下であることを要求する)を送信して偏光制御エンコーダ43に進入し、偏光制御エンコーダは、単光子パルスを分波して相対遅延し、その中の一つに対して量子鍵分配プロトコルに従って位相変調して、同じ偏光状態の二つの光パルスを出力し、逆方向光子分離検出ユニット44を介して、量子チャンネル45に進入し、受信装置に一方向で伝送する。当該二つの光パルスは、量子チャンネル45に介して受信装置に達した後、まず逆方向光子分離検出ユニット46を介して偏光制御エンコーダ47に進入される。偏光制御エンコーダ47は、二つのパルスを再び分波して、量子鍵分配プロトコルに従って相対遅延を行い、量子鍵分配プロトコルに従って位相変調する。偏光制御エンコーダ47の出力された第1の干渉信号は、そのまま単光子検出器48に送信され検出されて(暗計数と未相関部分の干渉を減少するために、ここでの検出は、時間ゲートモードを採用する需要があり、ゲート制御信号が送信端によってチャンネルに介して提供されてもよい)、偏光制御エンコーダ47の出力された第2の干渉信号は、逆方向光子分離検出ユニットによって分離されて検出され、前記の二つの干渉信号の検出結果、送信と受信側の位相変調記録および両者公開照合情報に基づいて、量子鍵分配プロトコルに従って一ビットの量子鍵が得られる。前記プロセスを繰り返すと、任意長さの無条件安全の量子鍵が構築できる。偏光制御エンコーダ内部に偏光保持光路又は90度回転ファラデーミラーを採用することによって、出力された二つの光パルスの偏光状態が同じに保持されるので、システムは優れた耐干渉能力を有する。偏光制御エンコーダが同一のポートを使用して同時に入力と出力ポートとして機能する方式を、送信装置と受信装置を採用する場合は、サーキュレータ及びY型ビームスプリッターなどの分波素子を光路に追加して入力と出力の信号を分離する必要がある。送信装置と受信装置が偏光制御エンコーダ49-6と49-7を採用する場合は、光パルスを分波するとき出力された二つの光パルスの幅が同じであるように分波比率を制御する需要があり、これによって最終に生成された量子鍵のエラーレートを低減することができる。

30

40

【図面の簡単な説明】

50

## 【 0 0 2 9 】

【図 1】 偏光保持光路マッハツェンダ干渉計式の偏光制御エンコーダの基本構成の模式図である。

【図 2】 偏光保持光路ミラー式の偏光制御エンコーダの基本構成の模式図である。

【図 3】 90度回転ファラデーミラー式の偏光制御エンコーダの基本構成の模式図である。

【図 4】 90度回転ファラデーミラー式の偏光制御エンコーダの変形例の基本構成の模式図である。

【図 5】 位相変調器が出力光路に位置する90度回転ファラデーミラー式の偏光制御エンコーダの基本構成の模式図である。

【図 6】 可変ビームスプリッターを使用する偏光保持光路ミラー式の偏光制御エンコーダの基本構成の模式図である。

【図 7】 可変ビームスプリッターを使用する90度回転ファラデーミラー式の偏光制御エンコーダの基本構成の模式図である。

【図 8】 逆方向光子分離検出ユニットを示す。

【図 9】 帯域通過フィルタが追加された他の逆方向光子分離検出ユニットを示す。

【図 10】 偏光制御エンコーダを中心とする位相変調光ファイバー量子鍵分配システムの構成の模式図である。

## 【符号の説明】

## 【 0 0 3 0 】

1、2、7、8、9、10、16、17、28、29、35、36、39、40 ポート

3、6、11、17、18 3dB偏光保持ビームスプリッター

4、14、26 偏光保持遅延線

5、12、24 偏光保持位相変調器

13、15、23、27 ミラー

19、31 位相変調器

20、22、30、34 90度回転ファラデーミラー

21、33 遅延線

25、32 偏光保持可変ビームスプリッター

37、48 単光子検出器

38 光学サーキュレータ

41 光帯域通過フィルタ

42 単光子光源

43、47 偏光制御エンコーダ

44、46 逆方向光子分離検出ユニット

45 量子チャンネル

10

20

30

【 图 1 】

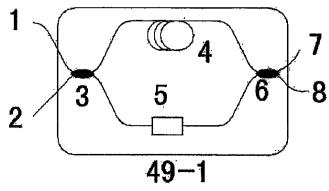


图 1

【 图 2 】

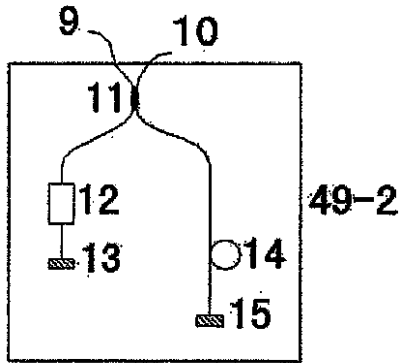


图 2

【 图 3 】

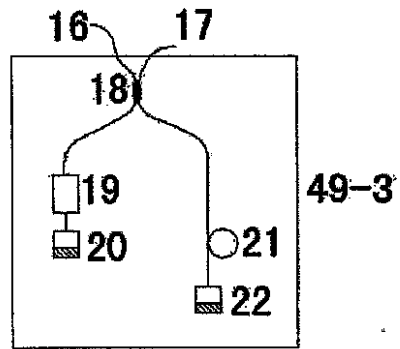


图 3

【 图 4 】

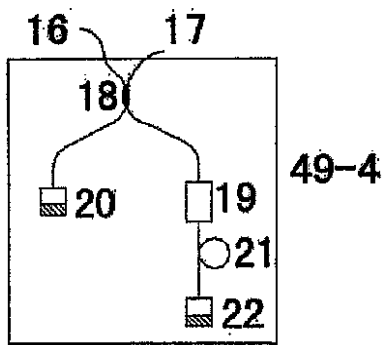


图 4

【 图 5 】

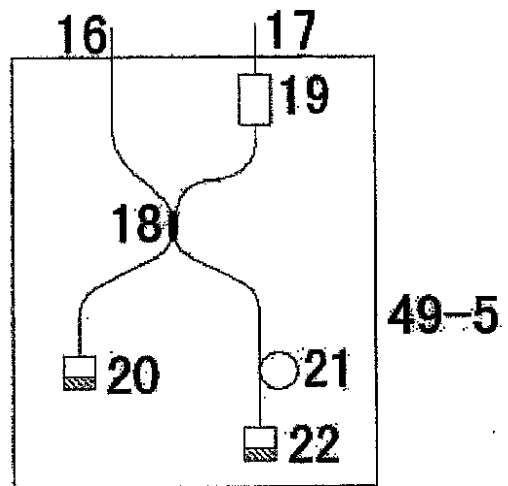


图 5

【图 6】

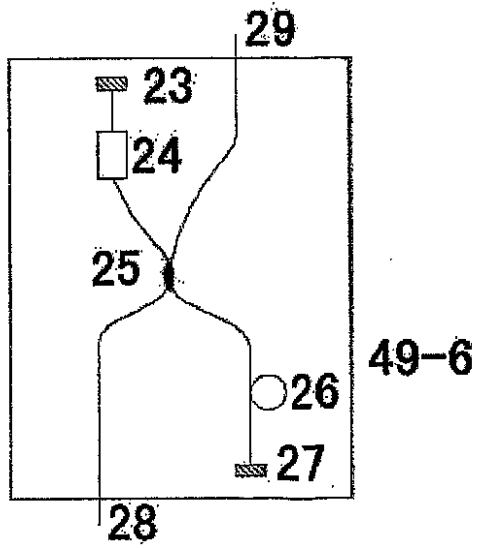


图 6

【图 7】

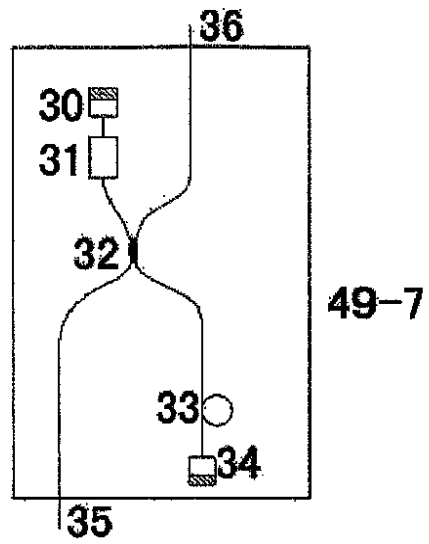


图 7

【图 8】

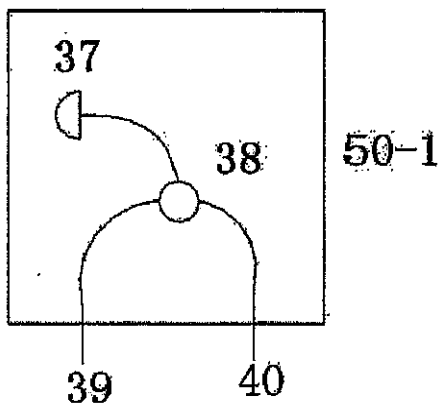


图 8

【图 9】

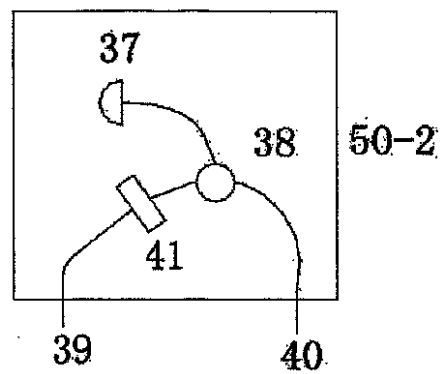


图 9

【图 10】

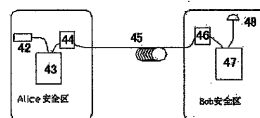


图 10

## 【手続補正書】

【提出日】平成17年10月31日(2005.10.31)

## 【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

偏光制御符号化方法であって、

入射された一つの光パルスを二つの光パルスに分波し、二つの異なる光路に沿って伝送させるステップと、

前記二つの光パルスに対して相対遅延を行うステップと、

前記相対遅延された二つのパルスを一つの経路で合波して出力するステップと、

前記分波ステップ又は合波ステップの後に、前記二つの光パルスの少なくとも一つを量子鍵分配プロトコルに従って位相変調するステップと、を含み、

前記方法は、前記分波から合波までのプロセスで、前記二つの光パルスの偏光状態を、合波後に出力された二つの光パルスの偏光状態が同じであるように制御するステップをさらに含むことを特徴とする偏光制御符号化方法。

【請求項2】

前記制御ステップは、前記二つの光パルスの偏光状態を前記分波から合波までのプロセスで一定に保持することを含むことを特徴とする請求項1に記載の偏光制御符号化方法。

【請求項3】

前記制御ステップは、前記相対遅延後の二つの光パルスをそれぞれ90度回転ファラデーミラーを介して奇数回反射させ、前記分波から合波までのそれぞれの光路を偶数回通過させることを含むことを特徴とする請求項1に記載の偏光制御符号化方法。

【請求項4】

前記制御ステップは、前記二つの光パルスの一方をそのまま出力させ、他方を90度回転ファラデーミラーを介して偶数回反射させ、前記分波から合波までのそれぞれの光路を偶数回通過させることを含むことを特徴とする請求項1に記載の偏光制御符号化方法。

【請求項5】

請求項1に記載の偏光制御符号化方法に基づいて構成される偏光制御エンコーダであって、

一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させる第1の偏光保持ビームスプリッターと、

一方の光パルスを他方の光パルスに対して遅延させる遅延線と、

前記相対遅延された二つの光パルスを一つの光路で合波して出力される第2の偏光保持ビームスプリッターと、

前記分波後の二つの光路と合波後の出力光路との三者の少なくとも一つに位置する位相変調器と、を備え、

前記二つの異なる光路は偏光保持光路であることを特徴とする偏光制御エンコーダ。

【請求項6】

請求項1に記載の偏光制御符号化方法に基づいて構成される偏光制御エンコーダであって、

一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させる偏光保持ビームスプリッターと、

一方の光路に位置し、一方の光パルスを他方の光パルスに対して遅延させる偏光保持遅延線と、

前記相対遅延された二つの光パルスを一つの光路で合波して出力するために、前記相対遅延された二つの光パルスを前記偏光保持ビームスプリッターへ反射させるミラーと、

前記分波後の二つの光路と合波後の出力光路との三者の少なくとも一つに位置する位相変調器と、を備え、

前記二つの異なる光路は偏光保持光路であることを特徴とする偏光制御エンコーダ。

【請求項 7】

請求項 1 に記載の偏光制御符号化方法に基づいて構成される偏光制御エンコーダであって、

一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させるビームスプリッターと、

一方の光路に位置し、一方の光パルスを他方の光パルスに対して遅延させる遅延線と、

前記相対遅延された二つの光パルスを一つの光路で合波して出力するために、前記相対遅延された二つの光パルスのそれぞれを前記ビームスプリッターへ反射させさせる二つの 90 度回転ファラデーミラーと、

前記分波後の二つの光路と合波後の出力光路との三者の少なくとも一つに位置する位相変調器と、を有することを特徴とする偏光制御エンコーダ。

【請求項 8】

請求項 1 に記載の偏光制御符号化方法に基づいて構成される偏光制御エンコーダであって、

一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させ、その一方の光パルスをそのまま出力させる偏光保持可変ビームスプリッターと、

他方の光パルスを反射させ、前記偏光保持可変ビームスプリッターを通過させる第 1 のミラーと、

前記偏光保持可変ビームスプリッターを通過した他方の光パルスを、そのまま出力された光パルスと一つの光路で合波して出力するために、再び前記偏光保持可変ビームスプリッターへ反射させる第 2 のミラーと、

前記第 1 と第 2 のミラー前の二つの光路中の少なくとも一方に位置する偏光保持遅延線と、

前記ミラー前の二つの光路と合波後の出力光路との三者の少なくとも一つに位置する位相変調器と、を備え、

前記第 1 と第 2 のミラー前の光路は偏光保持光路であることを特徴とする偏光制御エンコーダ。

【請求項 9】

請求項 1 に記載の偏光制御符号化方法に基づいて構成される偏光制御エンコーダであって、

一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させ、その一方の光パルスをそのまま出力させる可変ビームスプリッターと、

他方の光パルスを可変ビームスプリッターへ反射させ、可変ビームスプリッターを通過させる第 1 の 90 度回転ファラデーミラーと、

前記可変ビームスプリッターを通過した他方の光パルスを、前記そのまま出力された光パルスと一つの光路で合波して出力するために、前記可変ビームスプリッターへ再び反射させる第 2 の 90 度回転ファラデーミラーと、

前記第 1 と第 2 のミラー前の二つの光路中の少なくとも一方に位置する遅延線と、

前記 90 度回転ファラデーミラー前の二つの光路と合波後の出力光路との三者の少なくとも一つに位置する位相変調器と、を備えることを特徴とする偏光制御エンコーダ。

【請求項 10】

パルス光源から出力された一つの光パルスを二つの光パルスに分波して二つの異なる光路に沿って伝送させ、前記二つの光パルスの一方を他方に対して相対遅延させ、前記二つのパルスを一つの経路で合波して出力し、前記光パルスの何れかを量子鍵プロトコル規定に従って位相変調する送信端の偏光制御エンコーダと、

前記偏光制御エンコーダから出力された前記二つの光パルスを一方向伝送する量子チャンネルと、



受信された二つの光パルスの各光パルスを、二つの光パルスからなる光パルス群に分波して二つの異なる光路に沿って伝送させ、同じ群となる二つの光パルスに対して量子鍵プロトコル規定に従って相対遅延させ、前記二つの光パルス群を一つの経路で合波して出力し、一つの経路で合波して出力する前に、前記受信した光パルスと分波した光パルスと遅延した光パルスとの少なくとも一つに対して量子鍵プロトコル規定に従って位相変調する受信端の偏光制御エンコーダと、

前記二つの光パルス群におけるそれぞれの少なくとも一つの光パルスの干渉重ね結果を同期検出し、量子鍵分配プロトコルに従って量子鍵分配を行う単光子検出器と、を備えることを特徴とする量子鍵分配システム。

【請求項 1 1】


送信端偏光制御エンコーダの出口又は受信端偏光制御エンコーダの入口に直列接続した逆方向光子分離検出手段を更に備え、

前記逆方向光子分離検出手段は、光サーキュレータと単光子検出器とからなり、前記光サーキュレータの入力端が偏光制御エンコーダの出力に接続され、前記サーキュレータの同方向出力端が量子チャンネルに接続され、逆方向出力端が単光子検出器に接続されることを特徴とする請求項 1 0 に記載の量子鍵分配システム。

【請求項 1 2】

前記逆方向光子分離検出手段は、前記光サーキュレータの入力端に一つの光帯域通過フィルタが直列接続されることを特徴とする請求項 1 1 に記載の量子鍵分配システム。

## 【 国际调查报告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/CN2004/000969
A. CLASSIFICATION OF SUBJECT MATTER		
H04L9/08		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
G02B,H04L		
Minimum documentation searched (classification system followed by classification symbols)		
G02B26/08,H04L9/08,9/00		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
CHINA JOURNAL		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
quantum w cryptogra+, quantum w key w distribut+, polariz+, polaris+		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US6529601B1 (Paul D. Townsend, Ipswich (GB);04.Mar.2003,column4,line30 to column7,line50,Fig.1 to 4)	1、 2、 5-10
Y		4
X	US6438234B1(Nicolas Gisin, Geneva(CH) et al;20.Aug.2002,column2,line32 to column6,line 61,Fig.1 to 3)	1、 3
X	US6188768B1(Donald Stimson Bethume, San Jose et al;13.Feb.2001,column3, line42 to column4,line35,Fig.1)	1
Y		4
X	CN1135820A((MINA) UK SEC FOR DEFENCE; (MINA) UK SEC STATE OR DEFENCE; 12.Nov. 1996, page11, the last line to page13, the last	1
A	US5307410A(Charles H. Bennett, Croton-On-Hudson, N.Y.;26.Apr.1994,see the whole document)	1-12
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&"document member of the same patent family		
Date of the actual completion of the international search 21.Apr.2005 (21.04.2005)		Date of mailing of the international search report 11 · MAY 2005 (11 · 05 · 2005)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451		Authorized officer MA, Yan Telephone No. (86-10)62085825 



国际检索报告		国际申请号 PCT/CN2004/000969
<b>A. 主题的分类</b>		
H04L9/08		
按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类		
<b>B. 检索领域 G02B,H04L</b>		
检索的最低限度文献(标明分类系统和分类号)		
G02B26/08,H04L9/08,9/00		
包含在检索领域中的除最低限度文献以外的检索文献		
中国期刊		
在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))		
EPODOC PAJ WPI CNPAT quantum w cryptogr+, quantum w key w distribut+, polarizt, polarist+		
<b>C. 相关文件</b>		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	US6529601B1 (Paul D. Townsend, Ipswich (GB));04.03 月 2003,第 4 栏第 30 行至第 7 栏第 50 行,图 1 至 4)	1、2、5-10
Y	同上	4
X	US6438234B1(Nicolas Gisin, Geneva(CH) et al;20.08 月 2002,第 2 栏第 32 行至第 6 栏第 61 行,图 1 至 3)	1、3
X	US6188768B1(Donald Stimson Bethune, San Jose et al;13.02 月 2001,第 3 栏第 42 行至第 4 栏第 35 行,图 1)	1
Y	同上	4
X	CN1135820A(大不列颠及北爱尔兰联合王国国防大臣;12.11 月 1996, 第 11 页最后 1 行至第 13 页最后 1 行, 图 7)	1
A	US5307410A(Charles H. Bennett, Croton-On-Hudson, N.Y.;26.4 月 1994,全文)	1-12
<input type="checkbox"/> 其余文件在 C 栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。		
* 引用文件的具体类型: "A" 认为不特别相关的表示了现有技术一般状态的文件 "E" 在国际申请日的当天或之后公布的在先申请或专利 "L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 "O" 涉及口头公开、使用、展览或以其他方式公开的文件 "P" 公布日先于国际申请日但迟于所要求的优先权日的文件 "T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 "X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 "Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 "&" 同族专利的文件		
国际检索实际完成的日期 21.04 月 2005 (21.04.2005)		国际检索报告邮寄日期 11.5 月 2005 (11.05.2005)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区衙门桥西土城路 6 号 100088 传真号: (86-10)62019451		授权官员 马燕 电话号码: (86-10)62085825

国际检索报告  
关于同族专利的信息

国际申请号  
PCT/CN 2004/000969

检索报告中引用的 专利文件	公布日期	同族专利	公布日期		
US6529601B1	2003.03.04	WO9744936A1	1997.11.27		
		AU2906897A	1997.12.09		
		EP0972373A1	2000.01.19		
		JP2000511016T	2000.08.22		
		CA2254767C	2002.04.16		
US6438234B1	2002.08.20	CA2265553A	1998.03.12		
		WO9810560A1	1998.03.12		
		AU4206897A	1998.03.26		
		EP0923828A	1999.06.23		
		CZ9900477A3	1999.08.11		
		JP2000517499TT	2000.12.26		
		EP0923828B1	2004.01.28		
		AT258733T	2004.02.15		
		DE69727388EE	2004.03.04		
		DK923828TT	2004.05.24		
		ES2215238TT3	2004.10.01		
		US6188768B1	2001.02.13	None	
		CN1135820A	1996.11.13	WO9510907A1	1995.04.20
CA2173481A	1995.04.20				
EP0722640A1	1996.07.24				
GB2297448A	1996.07.31				
JP9505184TT	1997.05.20				
GB2297448B	1998.06.24				
EP0722640B1	1998.11.25				
DE69414874EE	1999.01.07				
ES2123825TT3	1999.01.16				
DE69414874TT	1999.05.12				
US6028935A	2000.02.22				
US5307410A	1994.04.26	None			

---

フロントページの続き

(81) 指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(72) 発明者 莫 小范

中華人民共和国安徽省合肥市金寨路96号

(72) 発明者 郭 光 カン

中華人民共和国安徽省合肥市金寨路96号

Fターム(参考) 5J104 AA05 EA15 EA21