(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4638478号
(P4638478)
(45)発行日　平成23年2月23日(2011.2.23)　(24)登録日　平成22年12月3日(2010.12.3)

(51)Int.Cl.　F I
H04L 9/12 (2006.01)　H04L 9/00 631

請求項の数 11 (全 15 頁)

(21)出願番号	特願2007-501849 (P2007-501849)
(86)(22)出願日	平成17年2月24日 (2005.2.24)
(65)公表番号	特表2007-526722 (P2007-526722A)
(43)公表日	平成19年9月13日 (2007.9.13)
(86)国際出願番号	PCT/US2005/006015
(87)国際公開番号	WO2005/086410
(87)国際公開日	平成17年9月15日 (2005.9.15)
審査請求日	平成18年10月24日 (2006.10.24)
(31)優先権主張番号	60/549,356
(32)優先日	平成16年3月2日 (2004.3.2)
(33)優先権主張国	米国(US)

(73)特許権者　505188939
マジック　テクノロジーズ，インコーポレーテッド
ＭＡＧＩＱ　ＴＥＣＨＮＯＬＯＧＩＥＳ，ＩＮＣ．
アメリカ合衆国，マサチューセッツ州　０２１４３－４２１４，サマービル，１１ワード　ストリート，スイート　３００
(74)代理人　100094145
弁理士　小野　由己男
(74)代理人　100129012
弁理士　元山　雅史

最終頁に続く

(54)【発明の名称】量子キー分配に対する変調器タイミング

(57)【特許請求の範囲】
【請求項１】
量子キー分配（ＱＫＤ）システムにおいて第１ＱＫＤステーション（ボブ）の第１変調器及び第２ＱＫＤステーション（アリス）の第２変調器のタイミングを確立する方法であって、
前記第２変調器の変調を固定又は第２の変調器をオフにし、
前記第１変調器に対する作動信号をタイミング値の範囲にわたってインクリメンタルに走査して、前記第１変調器に対する作動信号タイミングを交換された非量子信号に含まれる光子の検出器カウントにおける変化のタイミングに設定することにより前記第１変調器に対する作動信号タイミングを決定し、
前記第１変調器の変調を固定し、
前記第２変調器に対する作動信号をタイミング値の範囲にわたってインクリメンタルに走査して、前記第２変調器に対する作動信号を交換された非量子信号に含まれる光子の検出器カウントにおける変化のタイミングに設定することにより前記第２変調器に対する作動信号タイミングを決定する、方法。
【請求項２】
前記ＱＫＤシステムは双方向型システムであり、前記第１および前記第２変調器は位相変調器である、請求項１に記載の方法。
【請求項３】
前記第１変調器は、前記非量子信号を生成する第１ＱＫＤステーション（ボブ）にあり

、前記第２変調器は、前記非量子信号を反射して前記第１ＱＫＤステーションに戻す第２ＱＫＤステーション（アリス）にあり、前記方法は、さらに、
光子が前記第２ＱＫＤステーションに向かう間に第１変調器によって変調されるときに生じる第１時間間隔と、前記第２ＱＫＤステーションから戻る光子が第１変調器を通過するときに生じる第２時間間隔とを判別し、前記第２ＱＫＤステーションから前記第１ＱＫＤステーションに戻る非量子あるいは量子信号のみが前記第１変調器によって変調されることを確実に行う、
請求項２に記載の方法。
【請求項４】
前記第１および前記第２変調器に対する前記作動信号は、それぞれ、量子キーの確立のため前記ＱＫＤシステムによって行われる基準変調ではない変調をそれぞれ提供する、請求項１に記載の方法。
【請求項５】
強め合うよう干渉された非量子信号が前記第１検出器において検出され、弱め合うよう干渉された非量子信号が前記第２検出器に検出されるように配置された第１および第２検出器において、光子のカウントを行う、請求項１に記載の方法。
【請求項６】
前記第１及び第２の変調器それぞれに対して、
粗いタイミング間隔を確立し、
前記粗いタイミング間隔を、ある数の細分間隔に分割し、
より正確な変調器タイミングを確立するために、インクリメンタルに前記細分間隔を走査する、請求項１に記載の方法。
【請求項７】
前記第１及び第２変調器それぞれに対する前記変調器作動信号の幅を低減する、請求項６に記載の方法。
【請求項８】
非量子パルスの交換によりＱＫＤシステムにおける２つの変調器間のタイミングを確立する方法であって、前記２つの変調器それぞれに対して、
ａ）前記２つの変調器のうちの１つの変調器の変調を固定し、又は前記１つの変調器をオフにし、
ｂ）前記２つの変調器それぞれを通る非量子信号を交換し、
ｃ）第１の幅を有する第１変調器作動信号を、可能な変調器タイミングの範囲にわたってインクリメンタルに走査して粗いタイミング調整を行うことにより、前記非量子信号の変調の変化に起因して検出される光子カウントの変化に対応する粗いタイミングを確立し、
ｄ）前記第１の幅よりも狭い第２の幅を有する第２変調器作動信号を、ｂ）において決定された前記粗いタイミングに合わせられたタイミング間隔にわたって、インクリメンタルに走査して細かいタイミング調整を行うことにより、前記非量子信号の変調の変化に起因して検出される光子カウントの変化に対応する細かいタイミングを確立する、
方法。
【請求項９】
ｄ）における前記タイミング間隔は、ｃ）における前記第１変調器作動信号の第１の幅と同じである、請求項８に記載の方法。
【請求項１０】
第１および第２の光学的にリンクされたＱＫＤステーションを有する量子キー分配（ＱＫＤ）システムにおいて、前記第１のＱＫＤステーションであるボブにおける第１変調器ＭＢおよび前記第２のＱＫＤステーションであるアリスにおける第２変調器ＭＡに対する、第１および第２変調器作動信号Ｖ１，Ｖ２のタイミングをそれぞれ確立する方法であって、
ａ）第２変調器ＭＡを固定し、又は第２変調器ＭＡをオフにし、

ｂ）前記第１作動信号Ｖ１を初期幅Ｗ１Ｃにセットし、
ｃ）前記第１作動信号タイミングを、初期タイミングＴ１０に関する粗いインクリメントΔＴ１で変化させて、前記第１作動信号の粗いタイミングＴ１Ｃを、交換された非量子パルスに含まれる光子の検出器カウントにおける変化を検出し前記粗いタイミングＴ１Ｃをその変化のタイミングに設定することによって確立し、
ｄ）前記第１作動信号を低減された幅Ｗ１Ｒ＜Ｗ１Ｃにセットし、
ｅ）前記第１作動信号タイミングを、前記粗いタイミングＴＣ１に関する低減されたタイミング間隔ΔＴＲ＜ΔＴ１で変化させて、前記第１作動信号の細かいタイミングＴ１Ｆを、交換された非量子パルスに含まれる光子の検出器カウントにおける変化を検出し前記細かいタイミングＴ１Ｆをその変化のタイミングに設定することによって確立し、
ｆ）前記第１変調器ＭＢの変調を固定し、
ｇ）前記第２作動信号Ｖ２を比較的大きな初期幅Ｗ２Ｃにセットし、
ｈ）前記第２作動信号タイミングを初期タイミングＴ２０に関する粗いタイミング間隔ΔＴ２で変化させて、前記第２作動信号の粗いタイミングＴ２Ｃを、交換された非量子パルスに含まれる光子の検出器カウントにおける変化を検出し前記粗いタイミングＴ２Ｃをその変化のタイミングに設定することによって確立し、
ｉ）前記第２作動信号を低減された幅Ｗ２Ｒ＜Ｗ２Ｃにセットし、
ｊ）前記第１作動信号タイミングを、前記粗いタイミングＴＣ２に関する低減されたタイミングインクリメントΔＴ２Ｒ＜ΔＴ２で変化させて、前記第２作動信号の細かいタイミングＴ２Ｆを、交換された非量子パルスに含まれる光子の検出器カウントにおける変化を検出し前記細かいタイミングＴ２Ｆをその変化のタイミングに設定することによって確立する、方法。
【請求項１１】
前記ＱＫＤシステムが、「ボブ」としての前記第１のＱＫＤステーションを有する双方向型システムであって、前記方法は、さらに、
光子が前記第２のＱＫＤステーションに向かう間に第１変調器によって変調されるときに生じる第１時間間隔と、前記第２のＱＫＤステーションから戻る光子が第１変調器を通過するときに生じる第２時間間隔とを判別し、量子鍵を確立するために前記量子パルスを交換する前記ＱＫＤシステムの動作の間に、前記第２のＱＫＤステーションから前記第１のＱＫＤステーションに戻る量子パルスのみが、変調されることを確実に行う、
請求項１０に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は量子暗号に関し、特に、量子キー分配（ＱＫＤ）システムにおける変調器の動作のタイミングを確立するための方法に関する。
【背景技術】
【０００２】
量子キー分配は、「量子チャネル」越しに送信された弱い光信号（例えば、平均で０．１光子）を用いて、送信者（「アリス」）と受信者（「ボブ」）との間で、キーを設定することに関係する。キー分配の安全性は、不確定状態にある量子系はどれでも測定するとその状態を変えるという、量子力学の原則に基づいている。結果として、量子信号を妨害あるいは測定しようとする盗聴者（「イブ」）は、送信信号にエラーを引き起こしてしまうため、その存在が明らかになる。
【０００３】
量子暗号の一般的な原則は、ベネットとブラッザールの論文（非特許文献１参照）の中で、初めて発表された。具体的なＱＫＤシステムは、Ｃ．Ｈ．Ｂｅｎｎｅｔｔらの論文（非特許文献２参照）、Ｃ．Ｈ．Ｂｅｎｎｅｔｔの論文（非特許文献３参照）、およびベネットの特許文献１（以下‘４１０特許と称す）に記載されている。ＱＫＤを実行する一般的なプロセスは、ボーミスターらの著作（非特許文献４参照）に記載されている。

【０００４】
上述のベネットによる文献および特許公報では、それぞれ、いわゆる「一方向」型ＱＫＤシステムについて述べられている。一方向型ＱＫＤシステムとは、アリスが単一光子の偏光又は位相をランダムに暗号化して、ボブがそれら光子の偏光又は位相をランダムに測定するものである。１９９２年のベネットの論文に述べられている一方向型システムは、二光束マッハ・ツェンダー干渉計に基づいている。アリスおよびボブは、干渉計の位相を制御できるように、干渉計の各部にアクセスすることが可能である。干渉計は、熱的ドリフトを補償するために、伝送中は量子信号波長の一部分内で動的に安定する必要がある。
【０００５】
ギシンの特許文献２（以下、‘２３４特許と称す）では、干渉計を通って往復するようにパルスを送信することによって、偏光や熱ゆらぎを自己補正する、いわゆる「双方向」型ＱＫＤシステムについて開示されている。このように、‘２３４特許の双方向型ＱＫＤシステムの光学レイヤは、一方向型システムに比べて環境の影響を受けにくい。
【特許文献１】米国特許第５，３０７，４１０号公報
【特許文献２】米国特許第６，４３８，２３４号公報
【非特許文献１】Ｑｕａｎｔｕｍ Ｃｒｙｐｔｏｇｒａｐｈｙ：Ｐｕｂｌｉｃ ｋｅｙ ｄｉｓｔｒｉｂｕｔｉｏｎ ａｎｄ ｃｏｉｎ ｔｏｓｓｉｎｇ，Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ｔｈｅ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｃｏｎｆｅｒｅｎｃｅ ｏｎ Ｃｏｍｐｕｔｅｒｓ、Ｓｙｓｔｅｍｓ ａｎｄ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｉｎｇ，Ｂａｎｇａｌｏｒｅ，Ｉｎｄｉａ，１９８４，ｐｐ．１７５－１７９（ＩＥＥＥ、Ｎｅｗ Ｙｏｒｋ、１９８４）
【非特許文献２】“Ｅｘｐｅｒｉｍｅｎｔａｌ Ｑｕａｎｔｕｍ Ｃｒｙｐｔｏｇｒａｐｈｙ，” Ｊ．Ｃｒｙｐｔｏｌｏｇｙ ５：３－２８（１９９２）
【非特許文献３】“Ｑｕａｎｔｕｍ Ｃｒｙｐｔｏｇｒａｐｈｙ Ｕｓｉｎｇ Ａｎｙ Ｔｗｏ Ｎｏｎ－Ｏｒｔｈｏｇｏｎａｌ Ｓｔａｔｅｓ，” Ｐｈｙｓ．Ｒｅｖ．Ｌｅｔｔ．６８ ２１２１ （１９９２）
【非特許文献４】Ｔｈｅ Ｐｈｙｓｉｃｓ ｏｆ Ｑｕａｎｔｕｍ Ｉｎｆｏｒｍａｔｉｏｎ，Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ ２００１，ｉｎ Ｓｅｃｔｉｏｎ２．３，ｐａｇｅｓ２７－３３
【発明の開示】
【発明が解決しようとする課題】
【０００６】
‘４１０特許および‘２３４特許で述べられたような一方向型および双方向型ＱＫＤシステムは、典型的には、理想的な状態にどのようにして到達するかについて全く記載なしに、システムの理想的な作動状態で作動すると記載されている。さらに、自己補正や動的安定性は、システムの光学レイヤについて言及されており、システムのセットアップについては適用されていない。あるいは、電子システムやタイミングシステムのように、しばしば議論がされないようなＱＫＤシステムの他の全ての側面と組み合わせて、システムを理想的もしくはほぼ理想的な状態で作動させることについて述べられていない。
【課題を解決するための手段】
【０００７】
以下に詳細に説明する通り、本発明の第１の面は、ＱＫＤシステムの変調器のタイミングをセットアップする方法である。例示のために、双方向型ＱＫＤシステムとして考える。双方向型ＱＫＤシステムにおいては、この方法では、初期タイミングと、初期変調電圧と、比較的大きな初期変調器電圧信号幅とを、変調器の一方、例えば、ボブの変調器に対して選択する。また、ボブからアリスに遅延非量子パルスを送信し、そのパルスをアリスの変調器ＭＡでの変調なしにボブに戻して受信する。さらに、この方法は、ボブによってボブの検出器で変調されるパルスをカウントすることを備えている。ボブの変調器による変調が生じないとき場合は、変調器作動信号タイミングを粗い時間間隔によって反復的にインクリメントし、検出器が変調が生じたことを示すかどうかを観測する。変調が生じる

と、検出器間のカウントにおけるシフトによって示され、この場合、電圧タイミングが、検出器カウントにおける変化を生じる時間にリセットされる。粗い時間間隔は、次いで、細かい時間間隔に細分化される。変調器作動信号幅は減少され、そして、高精度な作動信号タイミングをさらに狭めるために、タイミングは細かい時間間隔のインクリメントによって調整される。タイミングを反復的にリセットすること、以前の時間間隔を細分化すること、次いで、タイミングを新しい細分間隔によってインクリメントすることの、このプロセスは、最終変調器電圧タイミングＴ１Ｆが所望の程度の精度と推定されるまで、繰り返される。作動信号タイミングを最終的に、変調器作動信号を変調されるパルスの到達に合わせつつ、調整することができる。

【０００８】

ボブのタイミングが確立されると、次いで、ボブの変調器電圧は固定され、また、アリスの変調器作動信号は選択変調を提供するようセットされる。また、アリスの変調器信号幅は、比較的大きくセットされ、（新しい）初期作動信号タイミングが選択される。上述したボブの反復プロセスは、最終タイミングを確立するために、アリスの変調器ＭＡのタイミングの粗い・細かい調整および変調器作動信号幅の調整に関して、基本的にアリスと同じように繰り返される。

【０００９】

ＱＫＤシステムが双方向型システムである態様の一例において、パルスの１つは、アリスに入るとき、およびアリスから出ていくときの両方で変調される。これにより、アリスの変調器は、直交偏光に対してパルスを変調することができる。位相変調器は偏光感度がよい傾向にあるので、このアプローチは、パルスにおける偏光変化に起因する変調エラーを低減することに貢献する。

【発明を実施するための最良の形態】

【００１０】

本発明は、量子暗号法に関する産業実用性に関連するとともに、それを有するものであり、ＱＫＤシステムにおける量子信号の変調を行うシステムおよび方法に対してなされたものである。本発明を、以下に、双方向型ＱＫＤシステムに関して説明するが、本発明は一方向型および双方向型システムのどちらにも適用可能である。以下の説明において、「量子信号」あるいは「量子パルス」は光子の平均数μ≦１を有し、「非量子信号」あるいは「非量子パルス」は光子の平均数μ＞１を有する。

＜双方向型ＱＫＤシステムの理想的な動作＞

例示を目的として、本発明を、双方向型ＱＫＤシステムに関して説明する。図１は、２つのＱＫＤステーション、アリスとボブとを備える双方向型ＱＫＤシステム１００の概略図である。ボブは、光パルスＰ０を出射するレーザ１２を備える。レーザ１２は、時分割多重化／逆多重化（Ｍ／Ｄ）光学系１０４に連結される。Ｍ／Ｄ光学系１０４は、レーザ１２から入力パルスＰ０を受け取り、個々のパルスを２つの時分割多重化パルス（「量子信号」）Ｐ１，Ｐ２に分割する。同様に、Ｍ／Ｄ光学系１０４は、（後述する）アリスから、時分割多重化パルスの組を受け取り、それらを結合し（干渉させ）、単一パルスとする。Ｍ／Ｄ光学系１０４は、Ｍ／Ｄ光学系１０４に連結された位相変調器ＭＢを備えている。光ファイバリンクＦＬは、Ｍ／Ｄ光学系１０４に連結されており、ボブをアリスに接続する。ボブは、また、変調器ＭＢに連結された電圧制御器４４と、電圧制御器に連結された乱数発生器（ＲＮＧ）ユニット４６と、を備える。

【００１１】

ボブは、また、Ｍ／Ｄ光学系１０４に連結された２つの検出器３２ａ，３２ｂ、を備える。ボブは、さらに、レーザ１２に、検出器３２ａ，３２ｂ、電圧制御器４４、そしてＲＮＧユニット４６に、機能的に（例えば電気的に）連結された制御器５０を備える。

アリスは、一端で光ファイバリンクＦＬに、そして反対側の他端でファラデーミラーＦＭに連結される位相変調器ＭＡ、を備える。アリスは、また、変調器ＭＡに連結された電圧制御器１４と、電圧制御器に連結された乱数発生器（ＲＮＧ）ユニット１６と、を備える。アリスは、さらに、ＲＮＧユニット１６、そして電圧制御器１４に連結された制御器

２０を備える。

【００１２】

ボブの制御器５０は、アリスおよびボブの動作を同期させるために、アリスの制御器２０に同期リンク（チャネル）ＳＬを介して（光学的あるいは電子的に）連結される。詳細には、位相変調器ＭＡ，ＭＢの動作は、同期信号ＳＳを同期リンクＳＬ上で交換する制御器２０，５０によって、連携される。実施例の一例において、本発明の変調器タイミングセットアップを備えるＱＫＤシステム全体の動作は、制御器２０あるいは制御器５０のいずれかから制御される。

＜双方向型ＱＫＤシステムの理想化された動作＞

ＱＫＤシステム１００の動作の実施例の一例において、ボブの制御器５０は、信号Ｓ０をレーザ１２へ送信し、それに応じて、比較的強く短いレーザパルスＰ０を発生する。実施例の一例において、次いで、パルスＰ０は、オプションの可変光学的減衰器ＶＯＡ１３Ｂによって減衰される。パルスＰ０は、Ｍ／Ｄ光学系１０４に到達し、Ｍ／Ｄ光学系１０４は、そのパルスを、直交偏光を有する２つの弱いパルスＰ１，Ｐ２に分割する。パルスＰ１は、直接、アリスへ向かうが、Ｐ２は遅延する。パルスＰ１，Ｐ２の一方－例として、Ｐ２－が遅延して、ＭＢ（この時点では非作動状態のままである）を通り、一方のパルスが他方の後で、例えば、図示する通り、パルスＰ２がパルスＰ１の後で、これらパルスが光ファイバリンクＦＬをアリスへと進む。

【００１３】

なお、ここで、システム１００の他の実施例において、パルスＰ０，Ｐ１を、アリスに配置されたＶＯＡ１３Ａを用いてアリスによって減衰される比較的強いパルスとすることもでき、これらパルスは、ボブに戻る前に、弱い（量子）パルスになるよう減衰されることを述べておく。

パルスは、アリスの変調器ＭＡを通り、パルスの偏光を９０°変化させるファラデーミラーＦＭで反射して離れる。これらパルスが変調器ＭＡを通って戻ってくるとき、アリスは第１パルスＰ１を未変調で通過させるが、第２パルスＰ２の位相を変調する（つまり、位相シフトΦ_Aを与える）。

【００１４】

この時点では、システムは、まさに一方向型システムのように機能し、アリスが量子パルスを変調して、それをボブに送信し、ボブも、また、信号を変調し、それを検出器３２ａ，３２ｂの一方で検出する。

以下により詳しく説明する通り、アリスの変調器ＭＡの変調のタイミングは、制御器２０，５０の間で共有される同期信号ＳＳによって提供される。アリスの変調は、制御器２０によって実行される。制御器２０は、よくタイミングが合わされた信号Ｓ１をＲＮＧユニット１６へ出力する。ＲＮＧユニット１６は、乱数を表す信号Ｓ２を電圧制御器１４へ出力する。これに応じて、電圧制御器１４は、１セットの基準信号（電圧）、例えば、Ｖ［＋３π／４］、Ｖ［－３π／４］、Ｖ［＋π／４］、Ｖ［－π／４］、からランダムに選択された作動信号（電圧）$V2 = V_A$を送信する。これにより、変調器ＭＡの位相が、対応する基準位相、例えば、＋３π／４、－３π／４、π／４、－π／４の１つにセットされる。

【００１５】

次に、２つのパルスＰ１，Ｐ２がボブに戻り、そしてそこで、例えば、パルスＰ２は変わらないままＭ／Ｄ光学系１０４を通過するが、パルスＰ１は遅延されて変調器ＭＢを通る。しかし、そこでは、変調器ＭＢはパルスＰ１に位相シフトΦ_Bを与えるのである。以下により詳しく説明する通り、ボブでのパルスＰ１（あるいは他の選択されたパルス）の変調のタイミングは、制御器２０，５０の間で共有される同期信号ＳＳによって提供される。変調は、制御器５０によって実行される。制御器５０は、よくタイミングが合わされた信号Ｓ３をＲＮＧユニット４６へ出力する。ＲＮＧユニット４６は、乱数表す信号Ｓ４を電圧制御器４４へ出力する。これに応じて、電圧制御器４４は、１セットの基準信号（電圧）、例えば、Ｖ［＋π／４］、Ｖ［－π／４］、からランダムに選択された作動信号

（電圧）Ｖ１＝V_Bを送信する。これにより、変調器ＭＢの位相が、対応する基準位相値、例えば＋π／４、－π／４、の１つにセットされる。

【００１６】

さらに、パルスＰ１，Ｐ２がＭ／Ｄ光学系１０４に入るとき、パルスＰ１は、パルスＰ２に対して、パルスがボブから出ていくとき、そこで、当初に与えられるものと等しい同じ量だけ遅延される。次いで、Ｍ／Ｄ光学系は、干渉パルス（図示せず）を生成するために、パルスＰ１，Ｐ２を干渉させる。

検出器３２ａ，３２ｂは、強めあう干渉（$\Phi_A-\Phi_B=0$）が検出器３２ａによって検出され、弱め合う干渉（$\Phi_A-\Phi_B=\pi$）が検出器３２ｂによって検出されるように配置される。ボブがアリスと同じ基準位相を与えるとき、検出器３２ａにおけるカウントは二値で０を示し、検出器３２ｂにおけるカウントは二値で１を示す。しかしながら、ボブの基準位相がアリスとは異なるとき、相関性はなく、カウントは、検出器３２ａ，３２ｂのいずれでも同じ確率となる（つまり、干渉パルスは、５０：５０のチャンスでいずれの検出器にも検出される）。

＜変調器タイミングセットアップ＞

上述の説明は、理想化されたＱＫＤシステム動作に対してなされた。しかしながら、実際には、ＱＫＤシステムは、自動的に理想的な状態で動作し続けることはない。さらに、商業的に実現可能なシステムは、まず、動作するよう、素早くセットアップしなければならず、次に、継続的な、理想的あるいはほぼ理想的な動作を確実に行うよう、その動作の状態の変化に対して補償可能でなければならない。

【００１７】

したがって、上述した、理想化された方法におけるＱＫＤシステムを実行する前に、システムを、適正に動作するよう、セットアップし較正しなければならない。これには、適切な変調が達成されるよう、変調器（位相あるいは偏光）を較正することが含まれる。

しかしながら、ＱＫＤシステムにおける変調器を較正するためには、変調器の作動の適切なタイミングを、まず確立しなければならない。詳細には、それぞれの変調器は、変調される必要のある量子パルスが特定の変調器を通る正確な瞬間に、作動されなければならない。変調器が起動される時間量を最小限にすることは、交換されたキーに関する情報を得ようとして変調器状態を割り出そうとしている盗聴者の機会を減らす。

【００１８】

したがって、本発明の実施例の一例は、変調器タイミングをセットアップすることを備えている。それぞれの変調器については、方法は、２つの主要な行程を備えている。すなわち、比較的幅の広い変調作動信号での粗いタイミング調整と、それに続く、幅の狭い変調作動信号幅での細かいタイミング調整である。

これらの基礎的なステップを、次に、図１のＱＫＤシステム１００および図２のフローチャート２００を参照して、よりに詳しく以下に説明する。なお、ここで、実施例の一例において、制御器２０，５０は、ＲＮＧユニット１６，４６を通じてではなく、変調器タイミングセットアップにおいて、それぞれの較正信号ＳＣ１，ＳＣ２を通じてそれぞれの電圧制御器１４，４４と直接通信することを述べておく。

＜ボブの変調器のタイミング＞

初めにアリスのタイミングを確立することもできるが、本実施例の一例においては、ボブの変調器ＭＢのためのタイミングを確立する。

【００１９】

図２のフローチャート２００を参照すると、２０２において、ボブの制御器５０は、信号ＳＳを同期チャネルＳＬ上に制御器２０へ送信し、制御器２０にアリスの位相変調器を、それがまだオフでない場合は、オフにするよう指示する。あるいは、アリスの変調器を固定変調にセットすることもできるが、単にオフのままにしておく方がより簡単である。この意味において、アリスの変調器は、変調器が非作動であるときの変調がない場合も含めて「固定変調」にある、と言う。

【００２０】

２０４において、制御器５０は、次いで、電圧制御器４４に、変調器ＭＢの作動信号（電圧）Ｖ１＝V_Bを、π位相シフトを生成するV_B［π］など比較的大きな変調値に、セットさせる。電圧セッティングをV_B［π］とすることは好ましい。なぜなら、これにより、多くの（つまり、何千の）パルス当たりの光子を要する他の変調セッティングと比較して、使用されるパルス当たりの光子を、より少数（例えば、何百）に低減することができるからである。これは、走査時間をより速くすると言え、したがって、タイミングセットアップ手順をより速くすると言える。このように、キー交換動作において用いられる特定のベースがπの基準位相セッティングを含んでいない場合であっても、実施例の一例においては、可能な限り素早い変調器タイミングをセットアップする目的で、このような位相セッティング－つまり、非基準位相セッティング－が用いられる。

【００２１】

２０６において、制御器５０はまた、電圧制御器４４に、一般に２ｎｓから１０ｎｓの範囲にある最終作動信号幅Ｗ１と比較して、変調器作動信号Ｖ１の幅を相対的に大きく（例えば、５０ｎｓに）させる。この比較的粗い幅を、Ｗ１Ｃとする。２０８において、制御器５０は、時間作動信号V_B［π］が変調器ＭＢに印加されるべき初期変調器電圧時間Ｔ０１、を選択する。実施例の一例では、Ｔ０１＝０である。

【００２２】

２１０において、制御器５０は、パルスＰ０を１ＭＨｚなど特定の繰り返しレートで生成するために、次いで、信号Ｓ０をレーザ１２へ送信する。パルスＰ０は、量子パルスである必要がなく、例えば、何百、何千の光子を有することができる。実施例の一例において、パルスＰ０は、非量子パルスである。したがって、検出器３２ａ，３２ｂにおいて検出される光学信号を容易に識別するために十分な光子を有しており、このような場合、μは、典型的には１～１０の間である。

【００２３】

２１２において、変調器ＭＢは、時間Ｔ０１、幅Ｗ１Ｃで、作動信号Ｖ１＝V_B［π］を通じて変調され、検出器３２ａ，３２ｂの光子カウントが測定される。変調器ＭＢのタイミングが正しくなければ、パルスは変調されることなく、そして、検出器３２ａの光子カウントは高くなり、一方、検出器３２ｂの光子カウントは、低くなって、ほとんど暗電流および他のスプリアス効果に起因するものとなろう。

【００２４】

なお、ここで、図１のシステム１００において、２つのパルスＰ１，Ｐ２は、パルスＰ０から生成されることを述べておく。これらのパルスは、アリスから反射され、ボブに戻る。上述のシステム１００において、光ファイバリンクＦＬに沿った往復行程の端部で、Ｐ１とＰ２の相対的な位相差が、検出器３２ａ，３２ｂによって測定される。

システム１００において、変調器ＭＡ，ＭＢからの位相変調を、Ｐ１にアリスとボブの両方によって与えることができ、Ｐ２にアリスとボブの両方によって与えることができ、Ｐ１にボブによって与えることができ、Ｐ２にアリスによって与えることができ、また、その逆も同様である。それは、最終的に測定されるのが、パルス間の全体の相対的な位相差であって、どの特定のパルスの位相でもないからである。しかしながら、変調器電圧振幅および電圧パルスタイミングを正確なレベルでセットするためには、特定の位相変調方法が、事前に、アリスとボブによって一致していなければならない。

【００２５】

以下に説明する実施例の一例においては、例示の目的で、パルスＰ１がアリスとボブ両方によって変調される場合を考える。位相シフトは、それぞれの変調器から与えられた総計であり、未変調のパルスＰ２の位相と比較される。したがって、変調器タイミングセットアップの実施例の一例において、タイミングを合わせる必要があるのはアリスを通るパルスＰ１の変調である。パルスＰ１，Ｐ２の両方が変調される場合、本発明のタイミングセットアップ方法は、直接的に、この場合に適用される。例えば、Ｐ１がボブによって変調され、Ｐ２がアリスによって変調されるとき、この場合、ゼロ位相差を確実にするために、V_B＝V_A＝Ｖ［π］のバイアス位相電圧の態様の変調器作動信号を両方の変調器に出

力する。

【００２６】

セキュリティのために、ボブの出ていくパルスＰ１，Ｐ２が変調されないことは重要である。なぜなら、これにより、ボブの変調器状態の情報が盗聴者に漏れることがあるからである。このことは、特に、高い平均光子レベルμが用いられる場合に当てはまる。なぜなら、盗聴者が検出されることなくファイバリンクＦＬに盗聴器を仕掛けることを可能にするからである。

【００２７】

十分なサンプリング間隔の後に、例えば、外部雑音がある状態において、１０の非量子信号以上の検出が少なくともできるサンプリング間隔の後に、それぞれの検出器の光子カウント（つまり、「クリック」数）が記録され、そして、２１４において、パルスタイミングＴ０１（例えば、電圧信号の前側のエッジで測定される）が、タイミング間隔ΔＴ１でインクリメントされる。ΔＴ１の値は、多少、初期の幅の広い作動信号$V1=V_B$より小さく選択されている。例えば、レーザ１２からの１ＭＨｚの繰り返しレートでは、パルスＰ０は１μｓに分離される。この間隔は、（粗い）時間インクリメントΔＴ１＝４０ｎｓの範囲を定めるために、例えば、２５のセグメントに分割することができる。この（粗い）時間インクリメントΔＴ１＝４０ｎｓは、５０ｎｓの変調器パルス幅によってカバーされ、こうして、オーバーラップを保証することができる。

【００２８】

また、２１４において、光子カウントがチェックされ、再度、変調が生じているかをチェックする。変調が生じていなければ、この場合、Ｔ０はさらなるΔＴ１などによってインクリメントされて、そして、２１２が繰り返されてから、２１４の光子カウントチェックが繰り返される。実施例の一例において、連続する非量子パルス間のタイミング間隔全体（つまりタイミング領域）がカバーされるまで、２１２，２１４が、ｎ回、Ｔ０１＋ｎΔＴ１で繰り返されて（反復されて）、検出器カウントにおける変化をもたらすタイミング間隔が確立される。他の実施例の一例では、検出器カウントにおける変化が検出されたとき、反復がストップする。

【００２９】

なお、ここで、量子キーを確立する際に通常のＱＫＤシステム動作の場合の変調器作動信号$V1$を$V_B[\pi/4]$にセットする場合と比較して、変調器作動信号$V1$を$V_B[\pi]$にセットすることによって、最終的に位相変調が生じるときの検出器３２ａ，３２ｂでの光子カウントにおけるシフトは飛躍的となることを述べておく。

双方向型ＱＫＤシステムでは、このプロセスが、２つの時間間隔をもたらす。この２つの時間間隔において、光子が、検出器３２ａではなく検出器３２ｂで検出される。このような時間間隔の１つは、レーザ１２からの光子がアリスへ向かって進む際に、変調器ＭＢによって変調されたときに生じる。また、１つの間隔とは、アリスから戻る光子が変調器ＭＢを通って進むときである。もし、ファイバリンクＦＬの長さが変更されて、往復移動時間が増加したとき、この場合、出ていくパルスは、同じ時間で変調を示すことになり、また、戻ってくるパルスは、往復移動時間の増加による遅延に対応する時間で変調する結果になる。

【００３０】

同様の効果は、光子パルスＰ０がシステムに送信されるレートの変更によって、物理的ファイバを変更することなく、達成しうる。ファイバリンクＦＬには１つ以上のパルスがあるので、これにより、戻ってくるパルスのロケーションの明らかな変化をもたらすことになる。したがって、２１５において、変調器ＭＢは、ボブに入力されるパルスをただ変調し、ロケーションを変更するパルスに対応する、粗いタイミングＴ１Ｃにセットされる。

【００３１】

一方の検出器から他方の検出器への光子カウントにおけるシフトが生じて、これにより、出て行く（粗い）作動信号タイミングＴ１Ｃが特定されると、次に、プロセスは２１６

に移行する。そこでは作動信号タイミングは、実際にはＴ１Ｃにセットされる。しかしながら、この時点での変調タイミングは、比較的大きな値、例えば５０ｎｓ、に初期設定されているタイミング間隔ΔＴ１の内にあるとわかるのみである。

【００３２】

比較的粗い変調作動信号幅Ｗ１Ｃは、より妥当な値Ｗ１Ｒに低減される必要がある。理想的には、作動信号Ｖ１＝V_Bは、可能な限り小さい最終的な幅Ｗ１Ｆを有しており、これにより、変調器ＭＢが、入ってくるパルスＰ１を変調するために必要な最も短い時間だけ作動される。また、最終作動信号幅Ｗ１＝Ｗ１Ｆは、入ってくるパルスＰ２が、変調されることなく変調器ＭＢを通るように、十分に小さい必要がある。ここで、入ってくるパルスＰ２は、入ってくるパルスＰ１（例えば、数ナノ秒以内）に近い。

【００３３】

したがって、２１７において、作動信号幅は、例えばＷ１Ｒ＝５ｎｓに、低減される。この値は、物理的バンド幅および変調器電圧ドライバ１４の決定時間制限を想定して選択される。このようにして、２１８において、タイミング間隔ΔＴ１は、ある数の低減サイズ間隔ΔＴ１Ｒ、例えば（５０ｎｓ）／（２５）＝２ｎｓ、に分割される。この間隔は、走査の際のオーバーラップを可能にするために、新しい低減作動信号幅Ｗ１Ｒより小さい必要がある。

【００３４】

そして、２２２において、Ｔ１Ｒ（低減されたタイミング）の実際の値がΔＴ１Ｒ（ここでは、ΔＴ１Ｒ＝２ｎｓ）以内に決定されるまで、２１２～２１８が、低減された時間インクリメントを用い、Ｔ１Ｒ＝Ｔ１＋ｎΔＴ１Ｒの関係に基づいてタイミングを変化させて、繰り返される。２２４において、作動タイミング信号Ｖ１が、検出器の光子カウントが変調器ＭＢによる変調を示す変化を表す間隔に合わせられる。

【００３５】

必要に応じて、２２６において、２１７～２２４における、変調作動タイミングＴ１，Ｔ１Ｒを検出し、（オプションで）電圧信号幅Ｗ１を低減された幅Ｗ１Ｒにまで狭め、時間間隔ΔＴ１をいっそう小さいセグメントΔＴ１Ｒに細分するプロセスが、さらにより低減された作動タイミング信号Ｔ１Ｒと、対応するより小さい時間間隔と、オプションとしてより小さい作動信号幅Ｗ１Ｒとを用いて、繰り返される。変調器ＭＢに対する変調器作動信号Ｖ１＝V_Bの最終タイミングＴ１Ｆが、所望の程度の正確さ、例えば約２ｎｓ程度に確立されるまで、および、所望の最終作動信号幅Ｗ１Ｆ、例えば約２ｎｓ程度が達成されるまで、このプロセスは繰り返される。

＜アリスの変調器のタイミング＞

ボブの変調器ＭＢのタイミングが確立されると、次いで、アリスの変調のタイミングを確立する必要がある。

【００３６】

したがって、引き続き図１を参照するとともに図３のフローチャート３００を参照すると、３０２において、ボブの変調器電圧がＶ１＝V_B［π］で一定にセットされる。

３０４において、アリスの制御器２０は、信号ＳＣ２を電圧制御器１４へ送信し、電圧制御器１４に変調器作動（電圧）信号Ｖ２＝V_A＝－V_B＝V_A［－π］を変調器ＭＡへ送信させる。これは、変調器ＭＡの位相を（名目上）－πにセットするよう機能する。ボブの変調器ＭＢは、アリスの変調器タイミングセットアップの際、Ｖ１＝V_B［π］で一定に保持される。ボブの変調器作動信号Ｖ１＝V_Bのように、アリスの変調器作動信号V_Aが、Ｖ２＝V_A［－π］など、比較的大きな変調値にセットされ、これにより、変調が変調器ＭＡで生じる場合、（名目上）０の全体の位相シフトによって、基本的にすべての変調された光子が、検出器３２ａで検出される。変調が変調器ＭＡで生じなければ、その場合、パルスは、ボブの変調器ＭＢによって与えられたπの位相を有することになり、その結果、基本的にすべての変調されたパルスが、検出器３２ｂで検出される。

【００３７】

３０６において、ボブに対する２０６のように、制御器２０は、また、電圧制御器４４

に、変調器作動信号Ｖ２＝V_A［π］の幅Ｗ２＝ＷＡを、（一般に約１０ｎｓである）最終信号幅Ｗ２Ｆと比較して、相対的に大きく（例えば、５０ｎｓに）させる。この相対的に大きい（粗い）幅を、Ｗ２Ｃとする。

３０８において、ボブに対する２０８のように、制御器２０は、時間変調器作動信号Ｖ２＝V_A［－π］が変調器ＭＡに印加されるべき（新しい）初期時間Ｔ０２、を選択する。

【００３８】

なお、ここで、実施例の一例において、アリスで変調されるべき光学パルスが、アリスの入口および出口の両方で、変調されることを述べておく。これには、変調器を通ってファラデーミラーへ進み、変調器を通って戻ってくるときに、パルスを変調するのに十分な幅であり、かつパルスＰ１，Ｐ２の両方とも変調しないよう十分に狭い作動信号幅Ｗ２Ｃ、を必要とする。この変調手法は、変調器の偏光感度をパルス偏光における変動にまで低減するという利点がある。

【００３９】

３１０において、ボブに対する２１０のように、パルスＰ０を１ＭＨｚなど特定の繰り返しレートで生成するために、制御器５０は、次いで信号Ｓ０をレーザ１２へ送信する。

３１２において、ボブに対する２１２のように、検出器３２ａ，３２ｂの光子カウントが測定される。変調器ＭＡのタイミングが正確でないとき、この場合、変調器を通ってボブへと戻る途中のパルスＰ２はアリスで変調されることなく、そして、検出器３２ｂの光子カウントは高くなる。一方、検出器３２ａの光子カウントは低くなり、ほとんど暗電流および他のスプリアス効果に起因するものとなろう。

【００４０】

再び、ここで、図１のシステム１００において、２つのパルスＰ１，Ｐ２は、パルスＰ０から生成されることを述べておく。これらのパルスは、アリスから反射され、ボブに戻る。上述したシステム１００において、パルスＰ１あるいはパルスＰ２のいずれかが、アリスによって変調され、そして、パルスＰ１あるいはパルスＰ２のいずれかが、ボブによって変調される。このように、アリスに対する変調器タイミングセットアップにおいて、タイミングを合わせる必要があるのは、あらかじめ一致しているパルスＰ１あるいはＰ２の変調であり、また、アリスの入口およびアリスの出口の両方で変調される必要がある。

【００４１】

ボブの状況と異なり、光子が変調器ＭＡからファラデーミラーＭＦへ進み、そして変調器ＭＡへと戻ってくる往復時間は、はっきり認められるほどには変化しないことが、よく知られている。この往復移動時間は、Ｐ１とＰ２を分離する時間より小さい。光子検出器カウントにおける２つの変化を観測するために、変調器ＭＡは、十分に狭い変調器作動信号で駆動される。すなわち、１つの変化は、Ｐ１の入力と出力の遷移に対応するものであり、２つ目の変化は、Ｐ２の出力の遷移に対応するものである。変調器作動信号Ｖ２は、Ｐ１あるいはＰ２の行程の両方向を同時にカバーするのに十分な幅を有する。

【００４２】

変調が生じていないことを光子カウントが示しているとき、この場合、３１４において、ボブに対する２１４のように、初期電圧信号タイミングＴ０２は、ΔＴ２でインクリメントされる。１つのパルスだけが一度に変調されることを保証するために、ΔＴ２の値は、例えば、パルスＰ１，Ｐ２間の時間間隔を知ることによって選択される。３１４において、光子カウントがチェックされ、再度、変調が生じているかをチェックする。変調が生じていなければ、この場合、Ｔ０２はさらなるΔＴ２などでインクリメントされて、光子カウントチェックが繰り返される。連続するパルス間の時間間隔全体（領域）がカバーされるまで、このプロセスは、ｎ回、Ｔ２Ｃ＝Ｔ０２＋ｎΔＴ２で、繰り返される。３１６において、検出器カウントにおける変化をもたらすＴ２Ｃの値は、次いで、変調器ＭＡに対する粗いタイミング値にセットされる。

【００４３】

再び、ここで、ボブでは、パルスＰ１あるいはＰ２の行程の一方向のみが、変調器作動

信号Ｖ１＝V_Bによってカバーされることを述べておく。しかしながら、アリスにおいて、パルスの行程の両方向は、変調器作動信号Ｖ２＝V_Aによってカバーされる。こうして、ボブの場合には、例えば、約５０％より少ない光子カウントにおける変化は、変調における変化を全く示さないことになろう。一方、アリスでの、そのような変化は、変調されるべきパルスの２つの変調の少なくとも一方が生じたこと、および、少なくとも、タイミングの概算が確立されたこと、を非常によく示すことができよう。

【００４４】

変調器作動信号Ｖ２＝V_A［－π］に対するタイミングＴ２が、３１６において、確立されると、次いで、ボブに対する２１７のように、３１７において、盗聴者による変調器ＭＡの探索をより難しくするために、粗い作動信号幅Ｗ２Ｃはより小さい（低減された）サイズＷ２Ｒに減少する。実施例の一例において、作動信号幅Ｗ２Ｃは、低減された作動信号幅Ｗ２Ｒを形成するために、インクリメンタルにより小さくなる。そして、３１２～３１６が、より小さくされた信号幅で繰り返される。

【００４５】

次いで、ボブの２１８のように、３１８において、タイミング間隔ΔＴ２がより細かい（低減された）細分間隔ΔＴ２Ｒに分割され、３２２において、３１２～３１７が繰り返される。「変調がない」状態に戻る変化を表す光子カウントにおける変化が生じれば、この場合、３２４において、ボブに対する２２４のように、変調器電圧タイミングＴ２Ｒが調整され、これにより、変調が再確立されるまで狭められた電圧信号をシフトし、そして、好ましくは、そのように狭まった電圧信号がパルスＰ２に合わせられる。そして、３２６において、３１７～３２４（あるいは３１８～３２４）が、最終の所望の作動信号幅Ｗ２Ｆとともに、最終の所望の作動信号タイミングＴ２Ｆが確立されるまで繰り返される。実施例の一例において、アリスの最終の作動信号幅Ｗ２Ｆは、ボブの作動信号Ｗ１Ｆの約５倍であり、例えば、Ｗ１Ｆ＝２ｎｓ、Ｗ２Ｆ＝１０ｎｓである。

【００４６】

実施例の一例において、変調器タイミングセットアップは、上述し、かつフローチャートにおいて例示したタイミング方法を実行する命令を有する制御器２０，５０において、ソフトウェアを有することにより達成される。

けれども、また、ファイバ長が変更された場合（例えば、新しいファイバリンクＦＬへの連結、あるいは新しい光学パスへの光学的な切り換え）、あるいは、ｑｂｉｔ最新レートが変わる場合、変調器タイミングセットアッププロセスが繰り返される必要があるわけではない。これは、商業的に実行可能なＱＫＤシステムに対して、このような変調器タイミングセットアップ手順を有することが重要であるという他の理由でもある。

【００４７】

本発明の利点は、方法の実施例の一例が、非量子信号を使用して、変調器タイミングを較正し、これにより、ＱＫＤシステムの通常動作の間に量子信号の交換を可能にすることができるということにある。

さらに、変調器タイミングを再確立するために、光子カウントがＱＫＤシステムの通常動作の際に低下する場合、あるいは、光子カウントにおける低下が変調器タイミングに起因するものかどうかを判定する診断の場合に、本発明の方法を周期的に実行することができる。変調器の周期再タイミングは、ＱＫＤシステムが理想あるいはほぼ理想的な条件で動作することを確実とするのに役立つ。

【００４８】

以上、本特許出願は、２００４年3月2日に出願された、米国特許出願第６０／５４９，３５６号から、優先権を主張するものである。

前述の実施形態においては、理解を簡単にするために様々な実施例において様々な特徴をまとめた。本発明の特徴及び効果の多くは詳細な明細書から明らかであり、それ故、添付の明細書は、本発明の真の趣旨及び範囲に従う開示された装置のそのような特徴及び効果を全て網羅することを意図している。さらに、当技術分野の技術者ならば多くの修正や変更を容易に思いつくであろうから、本発明は、ここで述べた構成、動作、及び実施例に

厳密に限定されるものではない。従って、他の実施形態は、添付の特許請求の範囲に含まれる。

【図面の簡単な説明】

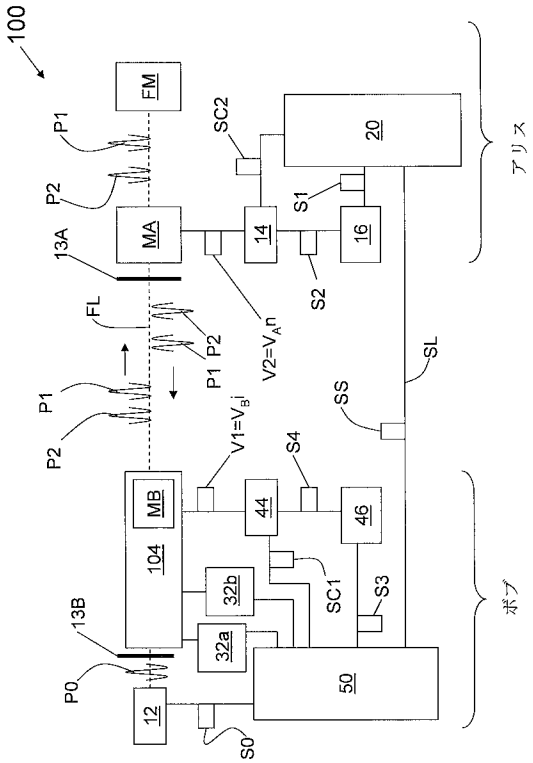
【００４９】

【図１】ＱＫＤシステムの一例としての双方向型ＱＫＤシステムの概略図。

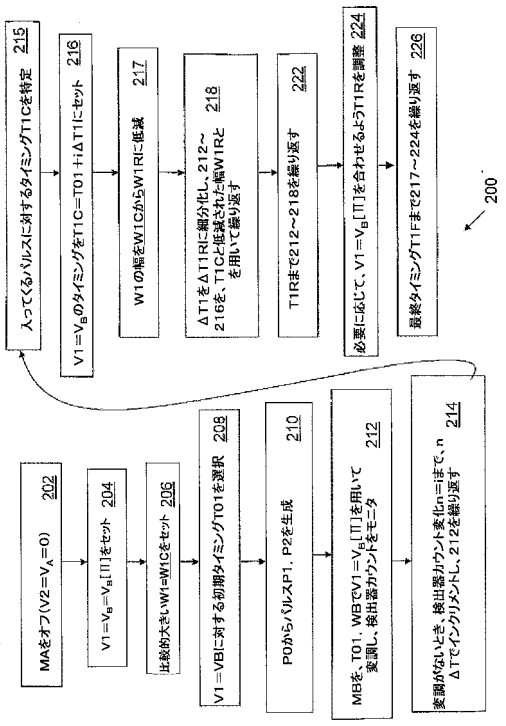
【図２】ボブの変調器に対する、図１のＱＫＤシステムにおける、変調器タイミングを確立する方法の実施例の一例のフローチャート。

【図３】アリスの変調器に対する、図１のＱＫＤシステムにおける、変調器タイミングを確立する方法の実施例の一例のフローチャート。

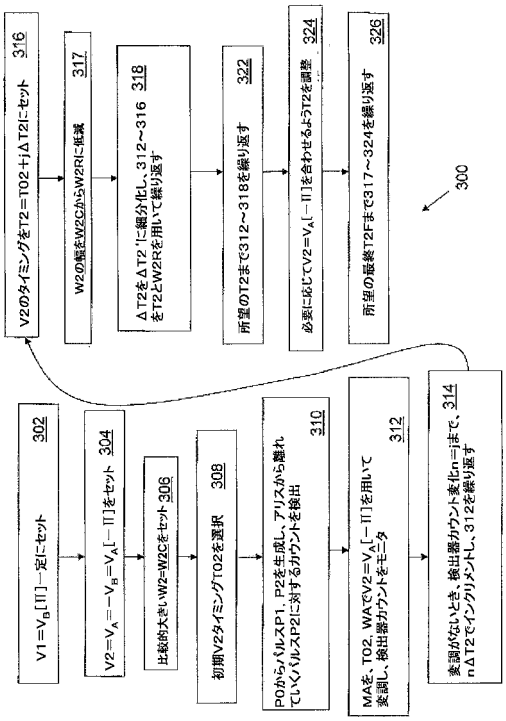
【図１】



【図２】



【図３】


V1=VB[Π]一定にセット 302
V2=VA=−VB=VA[−Π]をセット 304
比較的大きいW2=W2Cをセット 306
初期V2タイミングT02を選択 308
P0からパルスP1、P2を生成し、アリスから離れていくパルスP2に対するカウントを検出 310
MAを、T02、WAでV2=VA[−Π]を用いて変調し、検出器カウントをモニタ 312
変調がないとき、検出器カウント変化n=iまで、nΔT2でインクリメントし、312を繰り返す 314
V2のタイミングをT2=T02+jΔT2にセット 316
W2の振幅をW2CからW2Rに低減 317
ΔT2をΔT2'に細分化し、312〜316をT22とW2Rを用いて繰り返す 318
所望のT2まで312〜318を繰り返す 322
必要に応じてV2=VA[−Π]を合わせるようT2を調整 324
所望の最終T2Fまで317〜324を繰り返す 326
300

フロントページの続き

(72)発明者　ヴィグ，ハリー
アメリカ合衆国，マサチューセッツ州　０１８６２，ノース　ビレリカ，　８　コールローシュ　アベニュー

審査官　松平　英

(56)参考文献　特開平０２－０９６９３０（ＪＰ，Ａ）
特開２００１－３２４６２７（ＪＰ，Ａ）
特開２０００－２９８８６１（ＪＰ，Ａ）
特開２０００－３３００７９（ＪＰ，Ａ）
特表平０９－５０２３２２（ＪＰ，Ａ）
長谷川　俊夫，量子暗号技術，三菱電機技報　第７６巻　第４号，三菱電機エンジニアリング株式会社，２００２年　４月２５日，第７６巻　第４号，p. 27～30
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１５日，第４３巻　第８号，p. 866～872

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/00
G09C　1/00