

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2007-324922
(P2007-324922A)

(43) 公開日 平成19年12月13日(2007.12.13)

(51) Int. Cl.		F I		テーマコード (参考)
HO4L	9/12	(2006.01)	HO4L 9/00 631	5J104
HO4B	10/00	(2006.01)	HO4B 9/00 Z	5K102

審査請求 未請求 請求項の数 4 O L (全 13 頁)

(21) 出願番号	特願2006-152720 (P2006-152720)	(71) 出願人	000004226 日本電信電話株式会社 東京都千代田区大手町二丁目3番1号
(22) 出願日	平成18年5月31日 (2006.5.31)	(74) 代理人	100077481 弁理士 谷 義一
		(74) 代理人	100088915 弁理士 阿部 和夫
		(72) 発明者	本庄 利守 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
		(72) 発明者	井上 恭 東京都文京区西片2-12-6
		Fターム(参考)	5J104 AA05 NA02 5K102 AB11 AH23 AH27 PH42 PH49 PH50 RB01 RD28

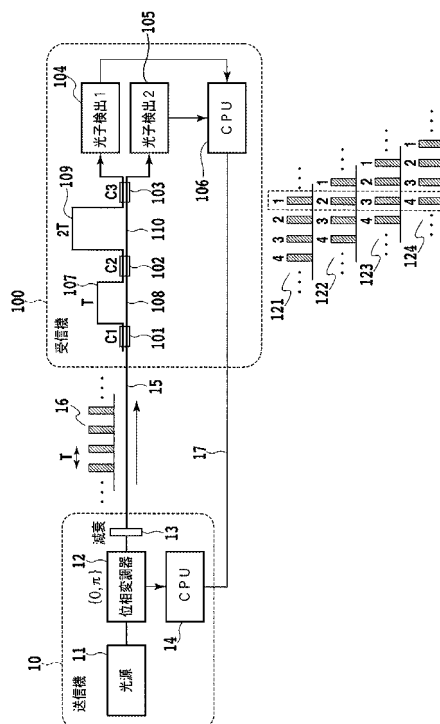
(54) 【発明の名称】 量子暗号通信装置及び量子暗号通信方法

(57) 【要約】

【課題】 なりすまし盗聴の発見確率を向上させるため、なりすまし盗聴によるビット不一致率を向上した量子暗号通信装置及び方法を提供する。

【解決手段】 受信機(100)内の分波器と遅延経路と合波器とからなる遅延合分波部(101~103, 107~110)を多段化することで、検出器(104, 105)の直前の合波器(103)で2パルスよりも多くのパルス(120~124)を合波する。これにより、なりすまし盗聴で生成された正しい位相を有するパルス合波の検出確率が低下し、同時にビット不一致率が増加する。その結果、テストビットにおける不一致検出確率が増加し、盗聴を検出する確率が高くなる。さらに、多段構成により低下する秘密鍵ビット生成率を向上させるため、送信パルスをグループ化して位相変調を実行する。これにより秘密鍵ビット生成率を向上できる。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

0 または のランダムに位相変調された一定時間間隔 T の光パルス列をパルス当り平均 1 光子未満のパワーレベルで送信する送信機と、該送信機から送信された前記光パルス列を受信する受信機とを備えた量子暗号通信装置において、

前記受信機は、

前記送信機から送信された前記光パルス列を 2 分岐する分波器と、

前記分波器で分岐された 2 つの光パルス列の一方に、他方の光パルス列に対して前記送信機からの光パルス列のパルス間隔 T に等しいか、またはその整数倍の時間差を与える遅延経路と、

前記分波器で分岐された前記他方の光パルス列と前記遅延経路で遅延された光パルス列を合波し、合波した光パルス列を 2 分岐する合分波器とを有し、

前記遅延経路と前記合分波器からなる遅延合分波部を複数個、縦続接続し、各遅延合分波部の前記遅延経路の前記時間差がそれぞれ異なることを特徴とする量子暗号通信装置。

10

【請求項 2】

0 または のランダムに位相変調された一定時間間隔 T の光パルス列をパルス当り平均 1 光子未満のパワーレベルで送信する送信機と、該送信機から送信された前記光パルス列を受信する受信機とを備えた量子暗号通信装置において、

前記受信機が、

前記送信機から送信された前記光パルス列を第 1 の長経路と第 1 の短経路に 2 分岐する光分岐手段と、

前記第 1 の長経路と前記第 1 の短経路から出力された 2 つの光パルス列を合波し、合波した光パルス列を第 2 の長経路と第 2 の短経路に 2 分岐する 2×2 の入出力端子を有する第 1 の光カップラーと、

前記第 2 の長経路と前記第 2 の短経路から出力された 2 つの光パルス列を合波し、合波した光パルス列を 2 分岐する 2×2 の入出力端子を有する第 2 の光カップラーと、

前記第 2 の光カップラーの出力端子にそれぞれ接続する 2 つの光子検出器とを含み、

前記第 1 の長経路が該長経路と前記第 1 の短経路との間に前記送信機からの光パルス列のパルス間隔 T に等しい時間差を与え、前記第 2 の長経路が該長経路と前記第 2 の短経路との間に前記パルス間隔 T の 2 倍のパルス間隔 $2T$ に等しい時間差を与えるように設定されていることを特徴とする量子暗号通信装置。

20

30

【請求項 3】

請求項 1 または 2 に記載の量子暗号通信装置を用いて量子暗号通信を行なう方法であって、

前記送信機において 0 または のランダムに位相変調された一定時間間隔 T の光パルス列をパルス当り平均 1 光子未満のパワーレベルで送信する際に、

連続パルス列を所定の複数個のパルスずつにブロック化し、

各ブロック毎に割り当てられる予め用意した複数組の所定の位相パターンのいずれか一つを無作為に選択して各ブロックに割り当て、

前記割り当てに従って各パルスを位相変調することを特徴とする量子暗号通信方法。

40

【請求項 4】

請求項 3 に記載の量子暗号通信方法において、

単位ブロックとなる前記所定の複数個のパルスが 4 個のパルスであり、前記所定の位相パターンが $\{0 - 0 - \dots - 0\}$ および $\{\dots - \dots - 0\}$ であることを特徴とする量子暗号通信方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、鍵配送技術に関し、特に、コヒーレント光パルス列の相対的位相差を利用し

50

、耐盗聴機能を備えた量子暗号通信装置及び量子暗号通信方法に関する。

【背景技術】

【0002】

近年、光子1個レベルの光を用いることにより、計算量を安全性のよりどころにした暗号方式とは異なる方式であり、かつ物理的に安全性が保証された量子暗号通信の研究が進められている。量子暗号は、離れた地点に存在する2者(2つの通信装置)間で暗号通信を行うための秘密鍵を供給するシステムであって、一般に量子鍵配送とも呼ばれている。量子鍵配送にも各種方式があるが、ここでは、従来技術として、差動位相シフト量子鍵配送方式(非特許文献1を参照)について説明する。

【0003】

図3は、従来の差動位相シフト量子鍵配送システムの基本構成を示す。送信機30は、平均1光子未満(例えば、0.1光子/パルス)を含むパルスに0またはの位相変調をランダムに行い、パルス送信のスロット時刻と位相変調とを記録し、その位相変調した一定間隔のコヒーレント光パルス列31を送出する。平均光子数1個未満という状態は、通常のレーザ光を大きく減衰させることにより実現される。このようなパルス列を光子検出すると、あるパルスでは光子が検出されるが、あるパルスでは何も検出されない、という検出結果となる。どのパルスで光子が検出されるかはまったくの確率的で、測定するまで不確定である。

【0004】

送信機30から送出的れたパルス列31は、伝送路32を経て受信機33で受信される。受信機33は、光分岐手段(分波器)34により受信パルス列を2つに分岐し、一方のパルス列に遅延手段(長経路)35により遅延を加えたのち、それら2つのパルス列を2×2の合波カップラー36により再び合波する。合波カップラー36の2つの出力端子には、それぞれ光子検出器37、38が備えられている。この分岐・合波回路34~36の長経路により一方のパルス列に与える遅延時間は、受信機33に入力されるパルス列の時間間隔に等しく設定されている。すなわち、長経路はパルス間隔に相当する遅延時間を有する。その結果、合波カップラー36では、隣り合う前後のパルスが重なり合って合波される。入力パルス列は0またはで位相変調されている。従って、分岐・合波経路の伝播位相が適切であれば、その重なり合うパルスの位相差は0またはとなる。合波の結果、両者(重なり合うパルスの両パルス)は干渉し、位相差が0ならば第1の検出器37が、位相差がならば第2の検出器38が、光子を検出することになる。このように、パルスの位相差0ととに応じて異なる検出器で光子を検出することになる。

【0005】

以上の構成を用いて、送信機30と受信機33は以下の手順により秘密鍵を得る。まず受信機33は、送信機30から送出的れて伝送路32を経た光子を上記の受信メカニズムにより検出する。この時、検出された各光子毎に検出した時刻(スロット時刻)と検出器とを記録する。所定の必要な数だけ光子が送受信された後、受信機33は送信機30に光子が検出された時刻である光子検出時刻を知らせる。送信機30は、その知らされた光子検出時刻(スロット時刻)と送信機自身の位相変調データ(スロット時刻と位相差)とから、受信機33がどちらの検出器(37,38)で光子を検出したかを知ることができる。ここで、第1の検出器37で光子を検出した事象をビット「0」、第2の検出器38で光子を検出した事象をビット「1」と、送信機30と受信機33間で予め取り決めておけば、送信者(送信機30)と受信者(受信機33)は同じビット列(鍵ビット)を得ることができる。

【0006】

上記手順において、受信機33から送信機30へ、すなわち受信者から送信者へ通知される情報は光子検出時刻のみであって、ビット情報はそれら通信機の外部には出されない。したがって、受信者から送信者へ通知される情報からビット情報が盗聴されることはない。また、伝送路32を通じて送られている信号は1パルスあたり平均1光子未満の光なので、盗聴者が伝送路32上の信号の一部を分岐してビット情報を得ることはできない。

10

20

30

40

50

なぜなら、1つの光子が2分割されることは物理的にあり得ないので、盗聴者が分岐により光子を検出すると、その光子は受信機33には届かず、送信者と受信者のビット列にはならないからである。

【0007】

さらに高度な盗聴法としては、なりすまし法と呼ばれる方法がある。図4は従来技術の差動位相シフト量子鍵配送システムに対するなりすまし盗聴の説明図である。盗聴者(盗聴機)43は、伝送路32の途中で、送信機30によって送出された伝送信号を受信機33と同様の構成44~48で受信し、光子検出器47,48での受信結果に基づいてダミー信号を本来の受信機33に自身の光送信器49を用いて送信する。盗聴者43が伝送信号を正しく受信できれば、そのダミー信号は元の送信信号と同一であり、受信機33に盗聴行為が気付かれないようにして情報(秘密鍵)を得ることができる。

10

【0008】

しかしながら、上述したように差動位相シフト量子鍵配送システムにおいては、送信信号は1パルス当たり平均1光子未満、例えば0.1光子/パルス、のパルス列である。このような信号を受信すると、10パルスに1回しか光子は検出されない。したがって盗聴者43は、光子を検出した時刻に対応する2パルスの位相差はわかるが、それ以外の位相差は検出できない。このような検出結果に基づいてダミー信号を送ろうとすると、位相差が検出できなかったパルスについては、当て推量で選んだ位相を割り振って再送する(以下、なりすまし盗聴1と称する)か、何も信号を出さない(以下、なりすまし盗聴2と称する)か、のいずれかの方法を探るしかない。

20

【0009】

前者(なりすまし盗聴1)を採用すると、当て推量で選んだ位相差を受信機33が検出した場合、送信機30が送ったものと異なるものとなる。後者(なりすまし盗聴2)を採用したとしても、やはり送受信信号の不一致が生じる。その理由は、この後者の場合に盗聴者43が送るのは孤立した連続2パルスだからである。孤立した2パルス(図4の50を参照)を受信機33が受信すると、分岐・合波回路34~36の出力段37,38では3つの時刻で光子が検出され得る(図4の53と52を参照)。

【0010】

図4には、光分岐手段34において分岐されたパルス列のうち、遅延されないパルス列53と遅延されたパルス列52を時系列的に図示してある。この図において、両パルス列が重なる時刻のうちの中の時刻(第2の時刻と呼ぶ)で光子が検出された場合には、その検出結果は2パルスの位相差に従っており、送信機30が意図した通りの検出器で光子が検出される。

30

【0011】

ところが一方、2つのパルス列が重なる時刻のうち第2の時刻の前後である第1または第3の時刻で光子が検出される場合には、干渉する相手がおらず、そのため光子はランダムに第1または第2の検出器で検出される。したがって、受信機33が第1または第3の時刻での光子検出結果から秘密鍵ビットを得ると、そのビットは送信機30が意図したものと異なるものになる。

【0012】

このように、なりすまし盗聴が行われると、送受信機間でビットの不一致が生じる。そこで、送受信機30,33は通常の手順に従って秘密鍵を得た後、いくつかのテストビットについて答え合わせをする。システムが正常に動作していれば両者のビット情報は一致するが、なりすまし盗聴があれば一致しないビットが出てくる。不一致ビットがある場合には、システムは正常でないと判断し、その秘密鍵を廃棄する。言い方を変えると、テストビットが一致していれば盗聴行為はなかったと判断することができ、その秘密鍵は安全であることが保証される。

40

【0013】

【非特許文献1】K. Inoue, E. Waks, Y. Yamamoto, 「Differential-phase-shift quantum key distribution using coherent light」、2003年、Physical Review A, vol.68, Pap

50

er number 022317

【発明の開示】

【発明が解決しようとする課題】

【0014】

以上から明らかなように、量子鍵配送システムに求められる重要な性能の1つとして、なりすまし盗聴の発見のしやすさが挙げられる。差動位相シフト量子鍵配送システムにおいて、なりすまし盗聴が行われると、上述の原理により送受信機関にビット不一致が生じ、これより盗聴行為が発覚するが、全てのビットが不一致となるわけではない。

【0015】

例えば、当て推量でダミーパルス列を送る場合（なりすまし盗聴1）、受信機33が光子検出したパルスが、たまたま盗聴者43が実際に光子検出したものであれば、ビット不一致は生じない。また孤立2パルスを送る場合（なりすまし盗聴2）、受信機33が第2の時刻で光子を検出すればビット不一致とはならない。

【0016】

ここで、ビット不一致率が高い方が、盗聴検知能力がより高くなり、より安全度の高い量子暗号システムとすることができる。なりすまし盗聴1に対するビット不一致率は、平均光子数を少なくすることで高くすることができる。平均光子数が少ないと、盗聴機43と受信機33がたまたま同じパルスを光子検出する確率が小さくなる、すなわち正解率が小さくなり、ビット不一致率は高くなる。一方、なりすまし盗聴2に対するビット不一致率は、平均光子数によらず一定で、受信機33が第1または第3の時刻で光子検出する確率は1/2であり、そしてこの光子検出から得られるビットが一致しない確率はさらにその1/2であることから、全体としてのビット不一致率は1/4となる。

【0017】

より安全度の高い量子暗号システムとしては、なりすまし盗聴によって生じるビット不一致の確率がより高いこと、それによりなりすまし盗聴の発見確率がより高くなることが望まれる。

【0018】

本発明は、上述したような課題に鑑みてなされたもので、その目的とするところは、なりすまし盗聴の発見確率を向上させることで通信の安全性の向上を図ることにあり、より具体的には、なりすまし盗聴によるビット不一致率を向上した量子暗号通信装置及び量子暗号通信方法を提供することにある。

【課題を解決するための手段】

【0019】

上記目的を達成するため、請求項1に記載の発明は、0または のランダムに位相変調された一定時間間隔Tの光パルス列をパルス当り平均1光子未満のパワーレベルで送信する送信機と、該送信機から送信された前記光パルス列を受信する受信機とを備えた量子暗号通信装置において、前記受信機は、前記送信機から送信された前記光パルス列を2分岐する分波器と、前記分波器で分岐された2つの光パルス列の一方に、他方の光パルス列に対して前記送信機からの光パルス列のパルス間隔Tに等しいか、またはその整数倍の時間差を与える遅延経路と、前記分波器で分岐された前記他方の光パルス列と前記遅延経路で遅延された光パルス列を合波し、合波した光パルス列を2分岐する合分波器とを有し、前記遅延経路と前記合分波器からなる遅延合分波部を複数個、縦続接続し、各遅延合分波部の前記遅延経路の前記時間差がそれぞれ異なることを特徴とする。

【0020】

請求項2に記載の発明は、請求項1の具体例であり、0または のランダムに位相変調された一定時間間隔Tの光パルス列をパルス当り平均1光子未満のパワーレベルで送信する送信機と、該送信機から送信された前記光パルス列を受信する受信機とを備えた量子暗号通信装置において、前記受信機が、前記送信機から送信された前記光パルス列を第1の長経路と第1の短経路に2分岐する光分岐手段と、前記第1の長経路と前記第1の短経路から出力された2つの光パルス列を合波し、合波した光パルス列を第2の長経路と第2の

10

20

30

40

50

短経路に2分岐する2×2の入出力端子を有する第1の光カップラーと、前記第2の長経路と前記第2の短経路から出力された2つの光パルス列を合波し、合波した光パルス列を2分岐する2×2の入出力端子を有する第2の光カップラーと、前記第2の光カップラーの出力端子にそれぞれ接続する2つの光子検出器とを含み、前記第1の長経路が該長経路と前記第1の短経路との間に前記送信機からの光パルス列のパルス間隔Tに等しい時間差を与え、前記第2の長経路が該長経路と前記第2の短経路との間に前記パルス間隔Tの2倍のパルス間隔2Tに等しい時間差を与えるように設定されていることを特徴とする。

【0021】

請求項3に記載の発明は、請求項1または2に記載の量子暗号通信装置を用いて量子暗号通信を行なう方法であって、前記送信機において0または1のランダムに位相変調された一定時間間隔Tの光パルス列をパルス当たり平均1光子未満のパワーレベルで送信する際に、連続パルス列を所定の複数個のパルスずつにブロック化し、各ブロック毎に割り当てられる予め用意した複数組の所定の位相パターンのいずれか一つを無作為に選択して各ブロックに割り当て、前記割り当てに従って各パルスを位相変調することを特徴とする。請求項4に記載の発明は、請求項3の具体例であり、単位ブロックとなる前記所定の複数個のパルスが4個のパルスであり、前記所定の位相パターンが{0-0-1-0}および{0-1-0-0}であることを特徴とすることができる。

10

【発明の効果】

【0022】

本発明は、上記のように、受信機内の分波器と遅延経路と合波器とからなる遅延合分波部を多段化することで、検出器の直前の合波器で2パルスよりも多くのパルス(2パルス合波は従来技術)を合波する構成にしたので、なりすまし盗聴で生成された正しい位相を有するパルス合波の検出確率が低下し、同時にビット不一致率が増加するため、テストビットにおける不一致検出確率が増加し、盗聴を検出する確率が高くなるという効果を奏する。

20

【0023】

また、本発明は、上記多段構成により低下する秘密鍵ビット生成率を向上させる位相変調方法により、秘密鍵ビット生成率を向上することができるという効果を奏する。

【0024】

以上のように、本発明によれば、なりすまし盗聴によるビット不一致率を高くすることで通信の安全性を向上した量子暗号通信装置及び量子暗号通信方法を提供することができる。

30

【発明を実施するための最良の形態】

【0025】

以下、図面を参照して本発明の好ましい実施形態を詳細に説明する。

【0026】

図1は、本発明の一実施形態における量子暗号通信システムの構成を示す。図1において、送信機10は光源11、位相変調器12、減衰手段13、および制御部(CPU)14を備えている。減衰手段(光減衰器)13は、例えば、NDフィルタ等、レーザ光などの光源11から入射される光を大きく減衰させることができる手段であれば、いずれ公知手段を用いてもよい。この送信機10の構成と動作は、従来技術と同様である。

40

【0027】

光検出装置としての受信機100は、光分岐手段(C1)101と、2つの2×2光カップラー(C2、C3)102、103と、2つの光子検出器104、105と、制御部(CPU)106と、を含んでいる。

【0028】

制御部14、106は、情報処理機能を有しており、専用装置だけでなく、市販のコンピュータも利用可能である。制御部14、106は、例えば、必要な計算や判断、制御等を実行するプロセッサ、光子検出時刻や検出器(または位相)等を記録するためのメモリ、通信路17を介して他の装置(受信機または送信機)と情報の交換をするための回線制

50

御部（モデム）、およびバス等を含む。通信路 17 としては有線、無線の何れも利用でき、光通信路に限らない。

【0029】

受信機 100 へ入力された光は、光分岐手段（分波器）101 により 2 分岐され、長経路の第 1 の遅延経路 107 により一方の光に遅延時間 T を与えられた後、短経路 108 を通った他方の光と第 1 の光カップラー（合波器）102 により再び合波される。ここで、遅延時間 T は入力されたパルス列のパルス間隔に等しく設定される。この光カップラー 102 は、2 つの出力端子を有している。この 2 出力端子から出力された光は、長経路の第 2 の遅延経路 109 によりそのうちの一方の光に $2T$ (T の 2 倍) の遅延時間を与えられた後、短経路 110 を通った他方の光と第 2 の光カップラー 103 により再び合波される。光カップラー 103 の 2 つの出力端子にはそれぞれ、光子検出器 104, 105 が接続されている。

10

【0030】

図 1 の本実施形態の構成と図 3 の従来例の構成とを見比べると、本実施形態では、受信機内の分波器と遅延経路と合波器とからなる遅延合分波部を多段化（縦続接続、カスケード）していることが分かる。

【0031】

以上の構成において、送信機 10 は、光源 11 から発生させたコヒーレントな光パルスを位相変調器 12 を通すことにより、0 または π でランダムに位相変調した一定間隔（パルス間隔） T の光パルス列を、減衰手段 13 を通すことで、1 パルス当り平均 1 個光子未満（例えば、0.1 光子/パルス）として光伝送路 15 に送出する。同時に、制御部 14 により、パルス送信のスロット時刻と位相変調とを記録する。光パルスのコヒーレンス時間はパルス間隔の 3 倍 ($3T$) よりも長いものと設定する。

20

【0032】

受信機 100 は、光伝送路 15 を経て送信機 10 から伝送されてきた光パルス列を、第 1 の光分岐手段（C1）101 に入力する。光分岐手段 101 で分岐された光パルス列は、カスケード状に構成された 2 段の遅延経路 107, 109 を経て、最終段の光カップラー（C3）103 で合波され、光子検出器 104, 105 によりそれぞれ検出される。

【0033】

このように受信機 100 の受信回路を構成すると、最終段の光カップラー 103 では、
 (i) 1 段目長経路 107 - 2 段目長経路 109 を通った第 1 パルス 121、
 (ii) 1 段目短経路 108 - 2 段目長経過 109 を通った第 2 パルス 122、
 (iii) 1 段目長経路 107 - 2 段目短経路 110 を通った第 3 パルス 123、
 (iv) 1 段目短経路 108 - 2 段目短経路 103 を通った第 4 パルス 124、
 の 4 つが同時刻に合波されることになる。なおここで、長経路とは、分岐された経路のうち、遅延が施される遅延経路のことであり、短経路とは、遅延が施されない経路のことである。

30

【0034】

上記のように、最終段の光カップラー 103 で 4 パルスが同時刻に合波されると、その 4 パルスは干渉を起こし、どちらの出力端子の光子検出器 104, 105 で光子が検出されるかは、各パルスの位相関係に依存することになる。

40

【0035】

4 パルス合波の場合の光子検出事象を式で記述すると、第 1 の光子検出器 104 へ出力される光子の確率振幅は、下記の (1) 式で表される。

【0036】

$$\exp(i\phi_1) + \exp(i\phi_2) - \exp(i\phi_3) + \exp(i\phi_4) \quad \dots (1)$$

第 2 の光子検出器 105 へ出力される光子の確率振幅は、下記の (2) 式で表される。

【0037】

$$\exp(i\phi_1) + \exp(i\phi_2) + \exp(i\phi_3) - \exp(i\phi_4) \quad \dots (2)$$

ここで、第 1 項は第 1 パルス 121、第 2 項は第 2 パルス 122、第 3 項は第 3 パルス 1

50

23、第4項は第4パルス124、をそれぞれ表し、 θ_i ($i = 1 \sim 4$) は各パルスの位相である。ただし、簡単のため、全体に共通する項は省略した。各パルスの位相は0または π で変調されている。それぞれの位相状態についての上記の確率振幅は下記の表1のようになる。

【0038】

【表1】

表1：パルス位相と出力振幅の関係

θ_1	θ_2	θ_3	θ_4	検出器1	検出器2
0	0	0	0	2	2
0	0	0	π	0	4
0	0	π	0	4	0
0	π	0	0	0	0
π	0	0	0	0	0
0	0	π	π	2	2
0	π	0	π	-2	2
π	0	0	π	-2	2
0	π	π	0	2	-2
π	0	π	0	2	-2
π	π	0	0	-2	-2
0	π	π	π	0	0
π	0	π	π	0	0
π	π	0	π	-4	0
π	π	π	0	0	-4
π	π	π	π	-2	-2

10

20

30

【0039】

光子の検出確率は確率振幅の絶対値の2乗で与えられる。表1中、一方の確率振幅が ± 4 で他方が0というのは、光子が検出される場合には、必ず振幅が ± 4 である方の検出器で検出されることを示している。以後、これを確定的光子検出と呼ぶ。確率振幅が ± 2 である場合は、どちらの検出で光子検出されるかは確率的である。

【0040】

表1で示された特性を利用すると、以下の手順により、送信機10と受信機100は共通のビットを得ることができる。

(1) 送信機10と受信機100は、上記の構成により、必要な長さのパルス列を送受信する。同時に、送信機100は、制御部14によりパルス送信のスロット時刻と位相変調とを記録する。

40

(2) 受信機100は制御部106と通信路17を介して光子を検出した時間スロットを送信機10に通知する。同時に、受信機100は検出のスロット時刻と検出器を制御部106に記録する。

(3) 送信機10は受信した時間スロットのデータと記録されている自身の位相変調データ(パルス送信のスロット時刻と位相)とを制御部14において参照することで、受信機100の検出事象が確定的光子検出であるか否かを判定し、判定結果を通信路17を介して受信機100へ通知する。

(4) 送信機10と受信機100は、確定的光子検出である事象について、第1の検出器

50

104によるものであればビット「0」を、第2の検出器105によるものであればビット「1」を、付与する。確定的光子検出については、どちらの検出器で光子検出されたかは送信機10にも分かるので、送受信機10, 100は同じビット値を得ることになる。このビットを秘密鍵ビットとする。

【0041】

以上の構成・手順によるシステムにおいては、なりすまし盗聴によるビット不一致率が従来よりも高くなる。その理由を、図2を用いて説明する。

【0042】

図2において、送信機10と受信機100の内部構成は図1と同様である。符号200は光伝送路15の途中に挿入する盗聴者(盗聴機)であって、受信機100と実質的に同一の構成201~205, 207~210を含み、更に両光子検出器204, 205の出力端子に接続する光送信器220を備えている。盗聴機200の構成要素201~205, 207~210は、図1に示した受信機の構成要素101~105, 107~110に対応するので、その構成の詳細な説明は省略する。

10

【0043】

なりすまし盗聴では、盗聴者200は、光伝送路15の途中で受信機100と同様の受信回路により光子を検出する。そして、盗聴者200は、光子検出結果に基づき、正規の受信機100が同じ検出結果となるようにダミー信号を光伝送路15を介して送出する。このとき、送信機10が送出しているパルス列16は、前述のように、送信レベルが1パルス当たり平均1個光子未満、例えば0.1個光子/パルスであるパルス列である。したがって、盗聴者200は平均1スロットに1回しか光子を検出し、盗聴者200は、光子を検出したスロットについては、正規の受信機100が所定の検出器で光子検出すると同様に、位相が設定された4連続パルスを送出する一方、光子検出しないスロットについては何も送らない。これにより、孤立した4連続パルス120が受信機100に送られることになる。

20

【0044】

受信機100が孤立4連続パルス120を受信すると、光子検出器104, 105においては、図2に示すように、1パルスずつシフトした4連続パルス列131~135が重なり合うことになる。この場合、7つの時間スロットで光子が検出し得る。どの検出器104, 105で光子が検出されるかは、上記の表1で説明したように、各スロットにおける干渉の仕方に依存する。真ん中の時間スロット(図2のマル印で示す)では、4つのパルスの全部が干渉するので、盗聴者200の意図した検出器で光子が検出される。一方、その他の時間スロットでは、干渉するパルス数が3または2、または干渉相手がないので、盗聴者200の意図とは関係なく、検出器に関しランダムに光子が検出されることになる。したがって、受信機100がこれらの時間スロットで光子を検出し、それから前述の手順(4)にしたがって秘密鍵ビットを生成すると、その秘密鍵ビットは送信機10の生成した鍵ビットと一致しない場合が生じる。その結果、その後のテストビットの照合により、盗聴行為を発見することができる。

30

【0045】

真ん中の時間スロットで光子を検出する確率は1/4、その他の時間スロットで光子検出する確率は $1 - 1/4 = 3/4$ である。後者のうちの半分以上がビット不一致となるので、ビット不一致率は3/8となる。一方、図4で説明した従来システムにおけるなりすまし盗聴によるビット不一致率は1/4である。すなわち、本発明は、なりすまし盗聴によるビット不一致率が、従来システムよりもはるかに高いものとなっている。

40

【0046】

このように、本発明によれば、なりすまし盗聴で生成された正しい位相を有するパルス合波の検出確率が低下し、同時にビット不一致率が増加する。その結果、テストビットにおける不一致検出確率が増加し、盗聴を検出する確率が高くなる。

【0047】

以上説明したように、本実施形態により、なりすまし盗聴によるビット不一致率を高め

50

た量子鍵配送が実現されるが、そのために生じる欠点としては、秘密鍵ビットの生成率が低くなることが挙げられる。本実施形態では、確定的光子検出事象から鍵（秘密鍵）を生成し、その他の光子検出は無視する。これに対し、従来システムでは検出した光子は全て鍵ビット生成に寄与するので、本実施形態は従来システムよりも鍵生成率が低くなる。通常一般に行なわれているように、各パルス位相が{0、 }で無作為に変調された場合は、表1に示した16の位相組み合わせパターンは等確率で発生する。この場合、光子が検出される確率は表1に示した確率振幅の2乗で与えられる。表1に示した光子検出パターンの検出確率を全て足し合わせると128という数字になる。このうち、確定的光子検出について足し合わせると64になる。すなわち、鍵ビット生成率は50%となる。

【0048】

しかし、以下に説明するように、この鍵生成率は、位相変調パターンに条件を課すと高めることができる。例えば、送信機10において、連続パルス列を4つずつにブロック化し、各ブロックに{0-0- -0}か{ - - -0}かのいずれかのパターンを無作為（ランダム）に割り当て、これに従い各パルスを位相変調器12で位相変調する。ここで便宜上、前者の{0-0- -0}をパターンA、後者の{ - - -0}をパターンBと呼ぶこととする。

【0049】

その位相変調の結果、受信機100は、パルス列からランダムに選ばれた4連続パルスの位相状態にしたがって、光子を検出することになる。この場合、4連続パルスがちょうどブロック単位で選ばれるとは限らず、ブロックにまたがった4パルスが選ばれる。今、ブロックのパターンはA、Bの2種類なので、選ばれる位相パターンは、連続する2ブロックがA-A、A-B、B-A、B-Bである場合について考察すれば十分である。各組み合わせの中から選ばれた連続4パルスと、光子を検出し得る検出器の関係は下記の表2のようになる。

【0050】

10

20

【表 2】

表 2 : 位相変調をブロック化した場合の 4 連続パルスと光子検出器との関係

A-A

0	0	π	0	0	0	π	0	検出器
○	○	○	○					1
	○	○	○	○				—
		○	○	○	○			—
			○	○	○	○		2
				○	○	○	○	1

10

A-B

0	0	π	0	π	π	π	0	検出器
○	○	○	○					1
	○	○	○	○				1、2
		○	○	○	○			—
			○	○	○	○		—
				○	○	○	○	2

20

B-A

π	π	π	0	0	0	π	0	検出器
○	○	○	○					1
	○	○	○	○				1、2
		○	○	○	○			—
			○	○	○	○		2
				○	○	○	○	1

B-B

π	π	π	0	π	π	π	0	検出器
○	○	○	○					2
	○	○	○	○				1
		○	○	○	○			—
			○	○	○	○		—
				○	○	○	○	2

30

【0051】

表 2 中、「1」または「2」と記入されているのは確定的光子検出、「1、2」と記入されているのは確率的光子検出である。確定的光子検出の場合の | 確率振幅 |² は 1/6、確率的光子検出の場合は $2 \times 2 + 2 \times 2 = 8$ である。表 2 から、光子を検出した場合（検出器の欄が「1」以外）にそれが確定的である割合（検出器の欄が「1」又は「2」で確定的である場合は 1/6、「1、2」で不確定的の場合は 8/8 である。）は、92%（11/12%）となる。このように、位相変調パターンの条件を課すと秘密鍵ビット生成率を高くすることができる。

40

【0052】

（他の実施の形態）

上記では、本発明の好適な実施形態を例示して説明したが、本発明の実施形態は上記例

50

示に限定されるものではなく、特許請求の範囲に記載の範囲内であれば、その構成部材等の置換、変更、追加、個数の増減、形状の設計変更等の各種変形は、全て本発明の実施形態に含まれる。

【0053】

例えば、図1の受信機構成は、1段目の分岐・合波回路で遅延時間Tを与え、2段目の分岐・合波回路で遅延時間2Tを与えるものとしたが、順序を入れ替えて、1段目の分岐・合波回路で遅延時間2T、2段目の分岐・合波回路で遅延時間Tの時間遅延を与えるものとしてもよい。

【図面の簡単な説明】

【0054】

10

【図1】本発明の一実施形態における量子暗号通信システムの構成を示すブロック図である。

【図2】本発明の一実施形態における量子暗号通信システムに対するなりすまし盗聴の説明をするためのブロック図である。

【図3】従来技術の差動位相シフト量子鍵配送システムの基本構成を示すブロック図である。

【図4】従来技術の差動位相シフト量子鍵配送システムに対するなりすまし盗聴の説明をするためのブロック図である。

【符号の説明】

【0055】

10 送信機（送信者）

20

11 光源

12 位相変調器

13 光減衰手段

14 制御部

15 光伝送路

17 通信路

100 受信機（受信者）

101 光分岐手段（光分波器）

102, 103 2×2光カップラー（光合波器）

104, 105 光子検出器

30

106 制御部

107, 109 遅延経路（長経路）

108, 110 短経路

200 盗聴者（盗聴機）

201 光分岐手段（光分波器）

202, 203 2×2光カップラー（光合波器）

204, 205 光子検出器

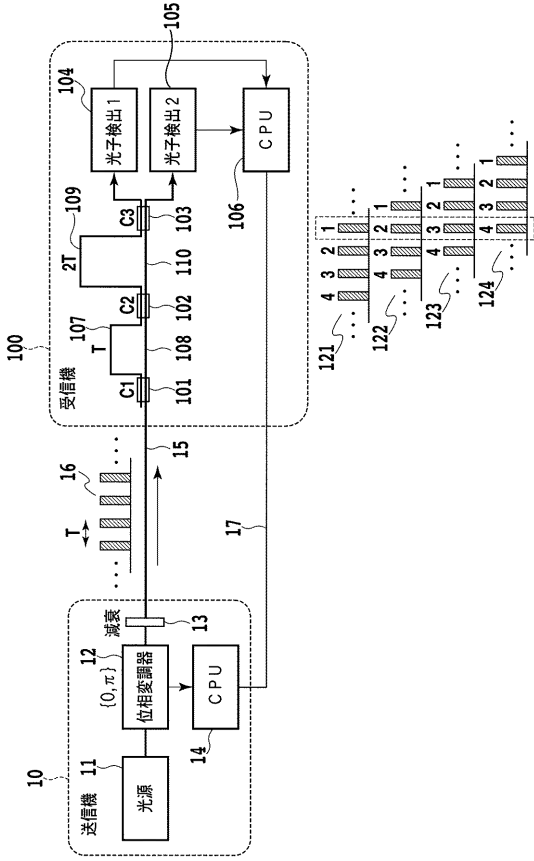
207, 209 遅延経路（長経路）

208, 210 短経路

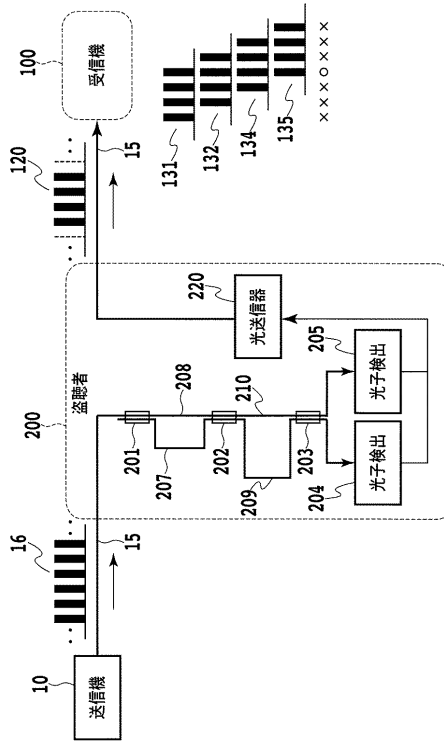
220 光送信器

40

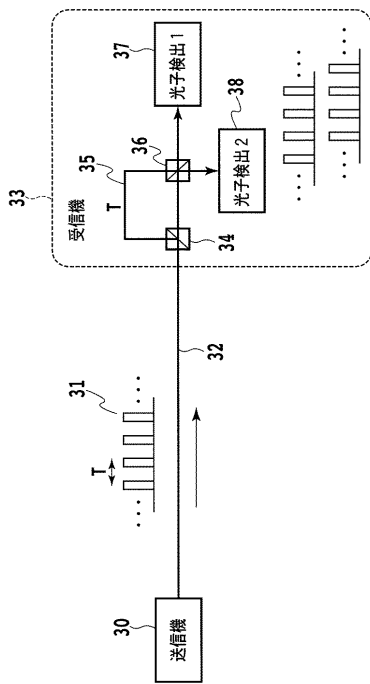
【 図 1 】



【 図 2 】



【 図 3 】



【 図 4 】

