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

特許第6681081号
(P6681081)

(45)発行日　令和2年4月15日(2020.4.15)　(24)登録日　令和2年3月25日(2020.3.25)

(51)Int.Cl.			F I		
G09C	1/00	(2006.01)	G09C	1/00	650B
H04L	9/12	(2006.01)	H04L	9/00	631
G06F	7/58	(2006.01)	G06F	7/58	680
H04B	10/70	(2013.01)	H04B	10/70	
H04B	10/85	(2013.01)	H04B	10/85	

請求項の数 5　(全 16 頁)　最終頁に続く

(21)出願番号　特願2017-565666(P2017-565666)
(86)(22)出願日　平成29年2月3日(2017.2.3)
(86)国際出願番号　PCT/JP2017/004081
(87)国際公開番号　WO2017/135444
(87)国際公開日　平成29年8月10日(2017.8.10)
審査請求日　令和2年1月31日(2020.1.31)
(31)優先権主張番号　特願2016-19552(P2016-19552)
(32)優先日　平成28年2月4日(2016.2.4)
(33)優先権主張国・地域又は機関
日本国(JP)

(出願人による申告)平成２３年度、独立行政法人情報通信研究機構「高度通信・放送研究開発委託研究／「セキュアフォトニックネットワーク技術の研究開発」課題イ　量子暗号安全性評価理論」産業技術力強化法第１９条の適用を受ける特許出願

(73)特許権者　504173471
国立大学法人北海道大学
北海道札幌市北区北８条西５丁目
(74)代理人　100088155
弁理士　長谷川　芳樹
(74)代理人　100124800
弁理士　諏澤　勇司
(74)代理人　100195811
弁理士　秋元　達也
(72)発明者　富田　章久
北海道札幌市北区北８条西５丁目　国立大学法人北海道大学内
(72)発明者　中田　賢佑
北海道札幌市北区北８条西５丁目　国立大学法人北海道大学内

最終頁に続く

(54)【発明の名称】乱数列生成装置、量子暗号送信機及び量子暗号通信システム

(57)【特許請求の範囲】

【請求項１】

パルス発振して、パルス毎の位相が乱雑なパルスレーザ光を繰り返し生成する半導体レーザ装置と、

互いに異なる伝送路長を有する第１伝送路及び第２伝送路と、前記第１伝送路及び前記第２伝送路の入力端側に接続され、前記パルスレーザ光が入力される第１ポートと、前記第１伝送路及び前記第２伝送路の出力端側に接続され、前記第１ポートに入力されて前記第１伝送路又は前記第２伝送路を経由した前記パルスレーザ光のそれぞれを出力する第２ポートと、前記入力端側に接続された第３ポートと、を有する干渉計と、

前記第２ポートに接続され、前記第２ポートから出力される前記パルスレーザ光を反射して前記第２ポートに再び入力する光反射部と、

前記第３ポートに接続され、前記光反射部により前記第２ポートに入力されて前記第１伝送路又は前記第２伝送路を経由した前記パルスレーザ光の干渉光が入力されると共に、前記干渉光が入力されたことに応じて電気信号を出力するフォトダイオードと、

前記電気信号の信号強度と予め設定された閾値との大小関係に基づいて乱数列を生成するＡＤ変換部と、を備える、乱数列生成装置。

【請求項２】

前記ＡＤ変換部において生成された前記乱数列を記憶する乱数列記憶部を更に備える、請求項１記載の乱数列生成装置。

【請求項３】

前記ＡＤ変換部において生成された前記乱数列に対して乱数性の検証を実行し、前記検証に適合した前記乱数列を前記乱数列記憶部に出力する乱数性検定部を更に備える、請求項２記載の乱数列生成装置。

【請求項４】

請求項２又は３記載の乱数列生成装置を備える量子暗号送信機であって、

前記干渉計は、前記出力端側に接続され、前記第１ポートに入力されて前記第１伝送路又は前記第２伝送路を経由した前記パルスレーザ光のそれぞれを出力する第４ポートを更に有し、

前記第４ポートから出力される前記パルスレーザ光の光強度及び位相を前記乱数列記憶部に記憶された前記乱数列に基づいて変調する変調部を備える、量子暗号送信機。

【請求項５】

請求項４記載の量子暗号送信機を備える量子暗号通信システムであって、

前記変調部によって光強度及び位相を変調された前記パルスレーザ光を前記量子暗号送信機との間で量子通信する量子暗号受信機を備える、量子暗号通信システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明の一形態は、乱数列生成装置、量子暗号送信機及び量子暗号通信システムに関する。

【背景技術】

【０００２】

従来、情報理論的に安全に情報を伝送するための量子暗号通信システムが知られている。量子暗号通信システムにおいて、情報の送信者は、受信者に対して、光子による量子鍵配送（QKD: Quantum Key Distribution）によって暗号鍵を伝送する。これにより、送信者及び受信者は、暗号鍵に関する情報を第三者によって取得（盗聴）されずに共有することができる。送信者は、受信者に伝送すべき情報を暗号鍵を用いて暗号化する。そして、送信者は、暗号化された情報を任意の通信手段によって受信者に伝送する。受信者は、暗号化された情報を暗号鍵を用いて復号する。

【０００３】

暗号鍵は、乱数列に基づいて取得される。このような乱数列として、情報理論的に予測不可能な物理乱数を用いる必要があり、アルゴリズムに基づいて生成される疑似乱数を用いることはできない。また、情報通信の高速化に対応するため、乱数列には、例えば数Gb/s以上の生成速度が要求される場合がある。

【０００４】

量子鍵配送では、第三者が光子から暗号鍵に関する情報を盗聴すると、不確定性原理によって光子の量子状態が変化し、盗聴の痕跡が残る。このため、送信者及び受信者は、盗聴を確実に検知することができる。このような量子鍵配送を実行することができる量子暗号通信システムとして、例えば特許文献１には、半導体レーザ装置と、干渉計と、乱数源と、を備える量子暗号送信機を有するシステムが記載されている。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２０１０－２３３１２３号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

ところで、特許文献１に記載された量子暗号通信システムでは、量子鍵配送を行うために用いられる半導体レーザ装置及び干渉計等とは別に、乱数列を生成するための乱数源が独立して設けられている。ここで、情報理論的に予測不可能な物理乱数を生成可能、且つ、例えば数Gb/s以上の生成速度で乱数列を生成可能な乱数源では、装置構成が複雑になる

場合がある。このような乱数源を用いる場合、量子暗号通信システム全体としての装置構成が複雑化する。

【０００７】

本発明の一形態は、上記課題に鑑みて為されたものであり、簡素な構成により、情報理論的に安全な乱数列を高速で生成することができる乱数列生成装置、量子暗号送信機及び量子暗号通信システムを提供することを目的とする。

【課題を解決するための手段】

【０００８】

上記課題を解決するため、本発明の一形態の乱数列生成装置は、パルス発振して、パルス毎の位相が乱雑なパルスレーザ光を繰り返し生成する半導体レーザ装置と、互いに異なる伝送路長を有する第１伝送路及び第２伝送路と、第１伝送路及び第２伝送路の入力端側に接続され、パルスレーザ光が入力される第１ポートと、第１伝送路及び第２伝送路の出力端側に接続され、第１ポートに入力されて第１伝送路又は第２伝送路を経由したパルスレーザ光のそれぞれを出力する第２ポートと、入力端側に接続された第３ポートと、を有する干渉計と、第２ポートに接続され、第２ポートから出力されるパルスレーザ光を反射して第２ポートに再び入力する光反射部と、第３ポートに接続され、光反射部により第２ポートに入力されて第１伝送路又は第２伝送路を経由したパルスレーザ光の干渉光が入力されると共に、干渉光が入力されたことに応じて電気信号を出力するフォトダイオードと、電気信号の信号強度と予め設定された閾値との大小関係に基づいて乱数列を生成するＡＤ変換部と、を備える。

【０００９】

このような乱数列生成装置では、パルスレーザ光は、第１ポートから第１伝送路又は第２伝送路を伝送されて第２ポートに至り、光反射部によって反射された後に、第２ポートから第１伝送路又は第２伝送路を伝送されて第３ポートに至る。第１伝送路及び第２伝送路は互いに異なる伝送路長を有する。このため、パルスレーザ光が、干渉計の第１ポートから第２ポートに伝送されるとき、及び、第２ポートから第３ポートに伝送されるときのそれぞれにおいて、１つのパルスが、干渉性を保った２つのパルス（ダブルパルス）に分離される。ダブルパルスを形成する２つのパルスの内、伝送路長のより長い方の伝送路を伝送されたパルスは、伝送先のポートへの到着が他方のパルスよりも遅延する。このため、第１伝送路及び第２伝送路の伝送路長の差が適切に設定されると、半導体レーザ装置によって互いに異なるタイミングで生成された２つのパルスレーザ光から分離されたパルスが第３ポートに略同時に到着し、第３ポートにおいて互いに干渉して干渉光を生成する。ここで、パルスレーザ光はパルス毎の位相が乱雑であるため、干渉光の干渉ピークの光強度は乱雑な値となる。この干渉光がフォトダイオードに入力されると、フォトダイオードは、干渉ピークに対応するピークの信号強度が乱雑な電気信号を出力する。この電気信号がＡＤ変換部に入力されると、ＡＤ変換部は、電気信号のピークの信号強度と予め設定された閾値との大小関係に基づいて、２値化された乱数列を出力する。よって、簡素な構成により、情報理論的に安全な乱数列を高速で生成することができる。

【００１０】

本発明の一形態の量子暗号送信機は、上述した乱数列生成装置を備え、干渉計は、出力端側に接続され、第１ポートに入力されて第１伝送路又は第２伝送路を経由したパルスレーザ光のそれぞれを出力する第４ポートを更に有し、第４ポートから出力されるパルスレーザ光の光強度及び位相を乱数列記憶部に記憶された乱数列に基づいて変調する変調部を備えてもよい。この場合、量子暗号送信機が備えている半導体レーザ装置及び干渉計を、乱数列生成装置の半導体レーザ装置及び干渉計としても利用するため、構成を簡素化することができる。

【００１１】

本発明の一形態の量子暗号通信システムは、上述した量子暗号送信機を備え、変調部によって光強度及び位相を変調されたパルスレーザ光を量子暗号送信機との間で量子通信する量子暗号受信機を備えてもよい。この場合、量子暗号送信機が備えている半導体レーザ

装置及び干渉計を、乱数列生成装置の半導体レーザ装置及び干渉計としても利用するため、構成を簡素化することができる。

【発明の効果】

【００１２】

本発明の一形態によれば、簡素な構成により、情報理論的に安全な乱数列を高速で生成することができる乱数列生成装置、量子暗号送信機及び量子暗号通信システムを提供することができる。

【図面の簡単な説明】

【００１３】

【図１】図１は、本実施形態の量子暗号通信システムの機能構成を示す概略図である。

【図２】図２は、図１の干渉計の構成を示す図である。

【図３】図３は、パルスレーザ光の干渉を説明するための図である。

【図４】図４は、干渉光が入力されたことに応じてフォトダイオードが出力する電気信号の一例を示す図である。

【図５】図５は、乱数性の検証の有無に応じた暗号鍵情報の伝送距離と暗号鍵生成レートとの関係を示すグラフである。

【図６】図６は、前提構成の量子暗号通信システムの機能構成を示す概略図である。

【図７】図７は、図６の干渉計の構成を示す図である。

【発明を実施するための形態】

【００１４】

以下、図面を参照しつつ、本発明に係る乱数列生成装置、量子暗号送信機及び量子暗号通信システムの好適な実施形態について詳細に説明する。なお、図面の説明において、同一又は相当部分には同一符号を付し、重複する説明を省略する。

【００１５】

［前提の構成］

最初に、本実施形態の前提となる量子暗号通信システムの構成について説明する。

【００１６】

図６は、前提構成の量子暗号通信システム２００の機能構成を示す概略図である。図６に示すように、量子暗号通信システム２００は、量子暗号送信機２１０と、光ファイバ等を含む光伝送路８０と、量子暗号受信機９０と、を備える。量子暗号通信システム２００は、量子暗号送信機２１０と量子暗号受信機９０との間で、第三者によって盗聴されずに暗号鍵に関する情報（以下、「暗号鍵情報」という）を共有するシステムである。すなわち、量子暗号通信システム２００によれば、量子暗号送信機２１０から量子暗号受信機９０に伝送すべき情報（以下、「メッセージ」という）を情報理論的に安全に伝送することができる。

【００１７】

量子暗号送信機２１０は、乱数列を生成し、生成した乱数列に基づいて取得される暗号鍵によってメッセージを暗号化する。また、量子暗号送信機２１０は、光子に暗号鍵情報を持たせ、当該光子を光伝送路８０に出力する。なお、暗号化されたメッセージは、例えばインターネット等の任意の通信手段によって量子暗号送信機２１０から量子暗号受信機９０に伝送される。光伝送路８０は、量子暗号送信機２１０から量子暗号受信機９０に光子を伝送する。量子暗号受信機９０は、光伝送路８０から入力された光子が持つ暗号鍵情報から暗号鍵を取得すると共に、暗号化されたメッセージを暗号鍵により復号する。

【００１８】

量子暗号送信機２１０は、半導体レーザ装置１１と、干渉計１２と、変調部１３と、乱数源４０と、を備える。乱数源４０は、情報理論的に予測不可能な物理乱数を生成可能、且つ、例えば数Gb/s以上の生成速度で乱数列を生成可能であれば、特定の構成には限定されない。なお、乱数源４０は、半導体レーザ装置１１及び干渉計１２とは独立して設けられている。

【００１９】

半導体レーザ装置１１は、パルス発振して、パルス毎の位相が乱雑なパルスレーザ光を繰り返し生成する。半導体レーザ装置１１は、例えば、量子暗号送信機２１０と量子暗号受信機９０とによって共有される同期信号のクロック周波数にて、パルスレーザ光を繰り返し生成する。図中には、１クロック分だけ互いに異なるタイミングで生成されたパルスレーザ光Ｌ１，Ｌ２が例示されている。半導体レーザ装置１１は、パルスレーザ光Ｌ１，Ｌ２を干渉計１２に入力する。

【００２０】

図７は、図６の干渉計１２の構成を示す図である。図７に示すように、干渉計１２は、非対称マッハツェンダ干渉計である。干渉計１２は、入力端２０と、出力端２１と、入力端２０及び出力端２１を接続する第１伝送路２２及び第２伝送路２３と、入力端２０側に接続された第１ポート２４及び第３ポート２６と、出力端２１側に接続された第２ポート２５及び第４ポート２７と、を有する。各ポートは、干渉計１２においてパルスレーザ光Ｌ１，Ｌ２の入出力を行うためのものである。第１ポート２４には、半導体レーザ装置１１が接続されている。半導体レーザ装置１１は、生成したパルスレーザ光Ｌ１，Ｌ２を、第１ポート２４を介して干渉計１２に入力する。

【００２１】

入力端２０には、第１ビームスプリッタ２８が配置されている。例えば半導体レーザ装置１１により生成されたパルスレーザ光Ｌ１は、第１ビームスプリッタ２８によって反射光と透過光とに分離される。パルスレーザ光Ｌ１の内、第１ビームスプリッタ２８により反射されたパルスレーザ光の成分を第１パルスＰ１とする。また、パルスレーザ光Ｌ１の内、第１ビームスプリッタ２８を透過したパルスレーザ光の成分を第２パルスＰ２とする。第１パルスＰ１と第２パルスＰ２とは、干渉性を保ちつつ時間的及び空間的に分離されたダブルパルスを形成する。

【００２２】

第１伝送路２２は、入力端２０から出力端２１まで第１パルスＰ１が伝送される伝送路である。第１伝送路２２は、その途中にミラー２９，３０を含んでいる。一方、第２伝送路２３は、入力端２０から出力端２１まで第２パルスＰ２が伝送される伝送路である。第１伝送路２２及び第２伝送路２３は、互いに異なる伝送路長を有する。ここでは、第１伝送路２２の伝送路長の方が、第２伝送路２３の伝送路長よりも長い。

【００２３】

出力端２１には、第２ビームスプリッタ３１が配置されている。第１伝送路２２を経由した第１パルスＰ１は、第２ビームスプリッタ３１によって反射光と透過光とに分離される。第１パルスＰ１の内、第２ビームスプリッタ３１により反射されたパルスレーザ光の成分を第３パルスＰ３とする。また、第１パルスＰ１の内、第２ビームスプリッタ３１を透過したパルスレーザ光の成分を第４パルスＰ４とする。第３パルスＰ３と第４パルスＰ４とは、干渉性を保ちつつ時間的及び空間的に分離されたダブルパルスを形成する。

【００２４】

また、第２伝送路２３を経由した第２パルスＰ２は、第２ビームスプリッタ３１によって反射光と透過光とに分離される。第２パルスＰ２の内、第２ビームスプリッタ３１により反射されたパルスレーザ光の成分を第５パルスＰ５とする。また、第２パルスＰ２の内、第２ビームスプリッタ３１を透過したパルスレーザ光の成分を第６パルスＰ６とする。第５パルスＰ５と第６パルスＰ６とは、干渉性を保ちつつ時間的及び空間的に分離されたダブルパルスを形成する。

【００２５】

このようにして、第１ポート２４に入力された１つのパルスからなるパルスレーザ光Ｌ１は、干渉性を保ちつつ時間的及び空間的に分離されたダブルパルスである第３パルスＰ３及び第６パルスＰ６として、第４ポート２７から出力される。

【００２６】

図６に示すように、第４ポート２７には変調部１３が接続されている。変調部１３は、強度変調部３２と、状態生成部３３と、減衰部（減衰器）３４と、を有している。変調部

１３は、ダブルパルスを形成するパルスレーザ光の光強度（すなわち、平均光子数）及び位相をランダムに変調させて送信用パルスレーザ光を生成する。変調部１３は、生成した送信用パルスレーザ光を光伝送路８０に出力する。なお、第２ポート２５及び第３ポート２６には何も接続されていない。

【００２７】

強度変調部３２としては、通常の光通信において用いられる公知の変調器を適用することができる。例えば、強度変調部３２は、ニオブ酸リチウム（LN: $LiNbO_3$）結晶を用いたマッハツェンダ型変調器であってもよい。強度変調部３２は、第３パルスＰ３及び第６パルスＰ６が入力されると、乱数源４０において生成された乱数に基づいてランダムに選択される所望の平均光子数となるように、光強度を変調する。なお、強度変調部３２は、減衰部３４によって光強度が減衰される減衰量と合わせて上述した所望の平均光子数となるように、光強度を変調する。

【００２８】

状態生成部３３としては、例えば公知の位相変調器を適用することができる。状態生成部３３は、第３パルスＰ３及び第６パルスＰ６が入力されると、乱数源４０において生成された乱数に基づいてランダムに選択される量子状態となるように、第３パルスＰ３及び第６パルスＰ６の位相を変調する。

【００２９】

ここで、第３パルスＰ３及び第６パルスＰ６の量子状態を記述するための基底は、以下のように選択すると好適である。まず、第３パルスＰ３及び第６パルスＰ６の内、先行して伝送する第６パルスＰ６の量子状態を|0>と記載し、遅れて伝送する第３パルスＰ３の量子状態を|1>と記載する。この場合、ダブルパルスの量子状態は、下記の式（１）で表される。

【数１】

$$\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right) \quad \cdots(1)$$

【００３０】

量子鍵配送においてデコイＢＢ８４プロトコルを用いることを前提とする場合には、基底としてＸ基底及びＺ基底を採用してもよい。このとき、デコイＢＢ８４プロトコルに必要な４つの状態は下記の式（２）、式（３）、式（４）で表される。

【数２】

$$\frac{1}{\sqrt{2}}\left(|0\rangle\pm|1\rangle\right) \quad \cdots(2)$$

【数３】

$$|0\rangle \quad \cdots(3)$$

【数４】

$$|1\rangle \quad \cdots(4)$$

【００３１】

以上のように、変調部１３は、パルスレーザ光の量子状態をランダムに変調して、０又は１の２値化されたビットを割り当てる。このとき、各ビットはＸ基底又はＺ基底の何れかランダムに選択された基底によって記述されている。

【００３２】

半導体レーザ装置１１はパルスレーザ光を繰り返し生成している。このため、変調部１３は、０又は１の２値化された各ビットがランダムに並んだビット列を生成する。このビット列が暗号鍵の元となる。

【００３３】

量子暗号通信システム２００は、暗号鍵に対して、以下に説明する鍵蒸留処理を実行する。

【００３４】

量子暗号送信機２１０は、暗号鍵の元となるビット列を量子暗号受信機９０に伝送する。伝送中の損失のため、送信されたパルスレーザ光の一部のみが量子暗号受信機９０に到達する。量子暗号受信機９０は、デコーダ９１と、光子検出部９２と、を備える。デコーダ９１は、受信した送信用パルスレーザ光に基づいて、暗号鍵の元となるビット列の各ビットを構成するパルスレーザ光を、Ｘ基底又はＺ基底に対応する光子検出部９２の各ポートに振り分ける。その結果、光子検出部９２において０又は１の２値化された各ビットが生成される。すなわち、変調部１３において生成されたビット列の一部が、量子暗号受信機９０において再生される。その後、量子暗号受信機９０は、パルスレーザ光を検出した光子検出部９２のポート（位置）を量子暗号送信機２１０に通知する。そして、量子暗号受信機９０において再生されたビット列が生鍵とされる。

【００３５】

続いて、量子暗号送信機２１０は、基底照合を実行する。すなわち、量子暗号送信機２１０は、量子暗号送信機２１０において使用された基底（送信基底）と、量子暗号受信機９０において使用された基底（受信基底）と、を照合する。送信基底と受信基底とが互いに異なるビットを除いた他のビットからなるビット列がシフト鍵とされる。

【００３６】

続いて、量子暗号受信機９０は、シフト鍵の一部を量子暗号送信機２１０に対して公開する。量子暗号送信機２１０は、公開されたシフト鍵に基づいて、量子暗号送信機２１０が送信したビットに対して量子暗号受信機９０が誤ったビットを受信した割合である誤り率を推定する。

【００３７】

続いて、量子暗号送信機２１０及び量子暗号受信機９０は、誤り訂正を実行する。誤り訂正としては、通常の通信において実行されている方法と同様の手法を用いることができる。

【００３８】

続いて、量子暗号送信機２１０及び量子暗号受信機９０は、秘匿性増強を実行する。まず、量子暗号送信機２１０及び量子暗号受信機９０は、推定された誤り率に基づいて、Ｎビットのシフト鍵の内の第三者に盗聴された可能性のあるビット数（漏洩情報量）の上限値Ｍを推定する。そして、量子暗号送信機２１０及び量子暗号受信機９０は、Ｎビットのシフト鍵から、上限値Ｍに定数ｓを加えたＭ＋ｓビットをランダムに捨てて、残りを最終鍵とする。その結果、盗聴者が最終鍵を取得することができる確率を2^{-s}以下に低減することができる。

【００３９】

ところで、シフト鍵からランダムに捨てられるビットは、ユニバーサルハッシュ関数を用いて選択される。ユニバーサルハッシュ関数としては、乱数源４０によって生成された乱数に基づいて、各成分の値（０，１）がランダムに選択された行列を用いることができる。

【００４０】

なお、秘匿性増強において推定される漏洩情報量は、半導体レーザ装置１１によって繰り返し生成されるパルスレーザ光同士の位相相関によって異なる。位相相関がないと仮定される場合に比較して、位相相関があると仮定される場合においては、漏洩情報量は大きな値であると推定される。

【００４１】

以上のようにして取得された最終鍵を用いて、量子暗号受信機９０は、暗号化されたメッセージを復号する。

【００４２】

［本実施形態の構成］

次に、本実施形態の乱数列生成装置１、量子暗号送信機１０及び量子暗号通信システム１００の構成について説明する。

【００４３】

図１は、本実施形態の量子暗号通信システム１００の機能構成を示す概略図である。図１に示すように、量子暗号通信システム１００の量子暗号送信機１０は、図６の量子暗号通信システム２００の量子暗号送信機２１０に対して、乱数源４０を備えていない点、及び、ファラディミラー（光反射部）５０、フォトダイオード５１、処理回路５２を備えている点で異なっている。なお、量子暗号送信機１０に含まれて構成される乱数列生成装置１は、半導体レーザ装置１１と、干渉計１２と、ファラディミラー５０と、フォトダイオード５１と、処理回路５２と、を含む。

【００４４】

図２は、干渉計１２の構成を示す概略図である。図２に示すように、干渉計１２の第２ポート２５にはファラディミラー５０が接続されている。また、第３ポート２６には、フォトダイオード５１が接続されている。

【００４５】

量子暗号通信システム１００において、上述した第４パルスＰ４及び第５パルスＰ５は、第２ポート２５からファラディミラー５０に出力され、ファラディミラー５０により反射される。ファラディミラー５０によって反射された第４パルスＰ４及び第５パルスＰ５は、第２ポート２５に再び入力する。

【００４６】

第２ポート２５に再び入力した第４パルスＰ４は、第２ビームスプリッタ３１によって反射光と透過光とに分離される。第４パルスＰ４の内、第２ビームスプリッタ３１により反射されたパルスレーザ光の成分を第６パルスＰ６とする。また、第４パルスＰ４の内、第２ビームスプリッタ３１を透過したパルスレーザ光の成分を第７パルスＰ７とする。第６パルスＰ６と第７パルスＰ７とは、干渉性を保ちつつ時間的及び空間的に分離されたダブルパルスを形成する。

【００４７】

また、第２ポート２５に再び入力した第５パルスＰ５は、第２ビームスプリッタ３１によって反射光と透過光とに分離される。第５パルスＰ５の内、第２ビームスプリッタ３１により反射されたパルスレーザ光の成分を第８パルスＰ８とする。また、第５パルスＰ５の内、第２ビームスプリッタ３１を透過したパルスレーザ光の成分を第９パルスＰ９とする。第８パルスＰ８と第９パルスＰ９とは、干渉性を保ちつつ時間的及び空間的に分離されたダブルパルスを形成する。

【００４８】

第７パルスＰ７は、第１伝送路２２を伝送して第１ビームスプリッタ２８に至り、第１ビームスプリッタ２８によって透過光と反射光とに分離される。第７パルスＰ７の内、第１ビームスプリッタ２８を透過したパルスレーザ光の成分を第１０パルスＰ１０とする。第１０パルスＰ１０は、第３ポート２６からフォトダイオード５１に出力される。

【００４９】

また、第８パルスＰ８は、第２伝送路２３を伝送して第１ビームスプリッタ２８に至り、第１ビームスプリッタ２８によって透過光と反射光とに分離される。第８パルスＰ８の内、第１ビームスプリッタ２８により反射されたパルスレーザ光の成分を第１１パルスＰ１１とする。第１１パルスＰ１１は、第３ポート２６からフォトダイオード５１に出力される。

【００５０】

第１０パルスＰ１０と第１１パルスＰ１１は、干渉性を保ちつつ時間的及び空間的に分離されたダブルパルスを形成する。第１０パルスＰ１０は、第１１パルスＰ１１よりも遅延して第３ポート２６に到着する。ここで、第１０パルスＰ１０が第１１パルスＰ１１よりも遅延する時間は、第１伝送路２２と第２伝送路２３との伝送路長の差によって決まる。

【００５１】
以上、半導体レーザ装置１１によって生成されたパルスレーザ光Ｌ１がファラディミラー５０によって反射されて、フォトダイオード５１に到着するまでのパルスの挙動について説明した。同様に、半導体レーザ装置１１によってパルスレーザ光Ｌ１よりも１クロック遅れて生成されたパルスレーザ光Ｌ２においても、パルスは上述した挙動をする。ここで、パルスレーザ光Ｌ２において、パルスレーザ光Ｌ１の第１０パルスＰ１０に相当するパルス（すなわち、パルスレーザ光Ｌ２から分離されたパルスの内、第１ポート２４から第１伝送路２２を経由して第２ポート２５に至り、ファラディミラー５０によって反射された後、第１伝送路２２を経由して第３ポート２６に至ったパルス）を第１２パルスＰ１２とする。また、パルスレーザ光Ｌ２において、パルスレーザ光Ｌ１の第１１パルスＰ１１に相当するパルス（すなわち、パルスレーザ光Ｌ２から分離されたパルスの内、第１ポート２４から第２伝送路２３を経由して第２ポート２５に至り、ファラディミラー５０によって反射された後、第２伝送路２３を経由して第３ポート２６に至ったパルス）を第１３パルスＰ１３とする。

【００５２】
図３は、パルスレーザ光の干渉を説明するための図である。図３の状態Ａは、それぞれ第３ポート２６からフォトダイオード５１に各パルスレーザ光が出力されるタイミングの一例を示している。なお、図３では、第１０パルスＰ１０、第１１パルスＰ１１、第１２パルスＰ１２、第１３パルスＰ１３以外のパルスは省略されている。

【００５３】
ここで、第１伝送路２２及び第２伝送路２３の伝送路長の差を適切に設定すると、第１０パルスＰ１０、第１１パルスＰ１１、第１２パルスＰ１２、第１３パルスＰ１３は、図３の状態Ｂに示すようなタイミングで第３ポート２６からフォトダイオード５１に出力される。状態Ｂでは、パルスレーザ光Ｌ１から分離された第１０パルスＰ１０と、パルスレーザ光Ｌ２から分離された第１３パルスＰ１３と、が第３ポート２６からフォトダイオード５１に略同時に出力されている。このため、図３の状態Ｃに示すように、フォトダイオード５１に入力されるときに、第１０パルスＰ１０と第１３パルスＰ１３とが互いに干渉して第１４パルスＰ１４（干渉光）が生成される。

【００５４】
フォトダイオード５１は、干渉光が入力されたことに応じて電気信号を処理回路５２に出力する。フォトダイオード５１としては、特に応答性に優れたフォトダイオードを用いることが好ましい。

【００５５】
半導体レーザ装置１１によって生成されるパルスレーザ光は、パルス毎の位相が乱雑である。このため、第１４パルスＰ１４の光強度は乱雑な値となる。図４は、干渉光が入力されたことに応じてフォトダイオード５１が出力する電気信号の一例を示す図である。図４に示すように、第１４パルスＰ１４がフォトダイオード５１に入力されると、フォトダイオード５１は、第１４パルスＰ１４の光強度に対応して、信号強度が乱雑な電気信号を出力する。

【００５６】
処理回路５２は、フォトダイオード５１から出力された電気信号を処理して乱数列を取得する回路である。処理回路５２は、ＡＤ変換部５３と、乱数抽出部５４と、乱数性検定部５５と、乱数列記憶部５６と、を有する。

【００５７】
ＡＤ変換部５３は、電気信号をアナログ値からデジタル値に変換する。ＡＤ変換部５３は、予め設定された閾値を記憶している。ＡＤ変換部５３は、電気信号のピークにおける信号強度と閾値とを比較し、これらの大小関係に基づいて２値化された乱数を出力する。なお、１個の電気信号のピークからｎビットの乱数列を取得する場合には、閾値T_0，T_1，…，T_u（ただし、$u=2^n-2$）が予め設定され、電気信号のピークにおける信号強度ＶがT_{i-1}以上T_i未満であるときに、２進法で表したｉの値がｎビットの乱数列

とされる。なお、信号強度ＶがＴ$_{u}$以上であるときには、２進法で表したｕの値がｎビットの乱数列とされる。また、信号強度ＶがＴ$_{0}$未満であるときには、０が乱数の値とされる。閾値Ｔ$_{0}$，Ｔ$_{1}$，…，Ｔ$_{u}$は、各乱数の値がほぼ等確率で出現するように設定されてもよく、これにより、一様乱数を取得したい場合においては乱数の生成効率を向上させることができる。

【００５８】

乱数抽出部５４は、ｍ個の電気信号のピークから取得されたｍ×ｎビットの乱数列におけるｍｉｎ－エントロピーＨ$_{min}$を算出する。ここで、ｍｉｎ－エントロピーＨ$_{min}$とは、乱数列としてＩ（ただし、Ｉは２進法で表したｉの値）が出現する確率Ｐ（Ｉ）の内の最も高い確率をＰ$_{max}$＝ｍａｘＰ（Ｉ）としたときに、Ｈ$_{min}$＝－ｌｏｇ$_{2}$Ｐ$_{max}$で表される値である。乱数抽出部５４は、ユニバーサルハッシュ関数を用いて、ｍ×ｎビットの乱数列からＨ$_{min}$ビットの乱数列をランダムに取り出して出力する。また、乱数抽出部５４は、Ｈ$_{min}$と乱数列との大きさの比Ｒ＝Ｈ$_{min}$／ｍｎを出力する。

【００５９】

乱数性検定部５５は、乱数抽出部５４によって取得された乱数列を規定量（例えば、１Ｍビット）だけ集めた乱数列を作り、例えば「ブロック単位の頻度検定」等の複数のテストを実行して乱数性の検証を行う。乱数性の検証では、複数の乱数列に対して各テストを実行し、全ての乱数列が全てのテストに適合したときに１（適合）を出力し、それ以外の場合に０（不適合）を出力する。また、乱数性検定部５５は、Ｈ$_{min}$と乱数列との大きさの比Ｒが、各プロトコルにおいて要求される乱雑性に対応するｍｉｎ－エントロピーＨ$_{min}$と乱数列との大きさの比Ｒ$_{c}$よりも大きい場合に１（適合）を出力し、それ以外の場合に０（不適合）を出力する。乱数性検定部５５は、乱数性の検証に適合した乱数列を乱数列記憶部５６に出力する。

【００６０】

乱数列記憶部５６は、乱数性検定部５５から入力される乱数列を記憶する。そして、乱数列記憶部５６は、量子鍵配送における各プロセスにおいて乱数列が必要になったときに、記憶している乱数列を出力する。例えば、乱数列記憶部５６は、強度変調部３２における光強度の選択、状態生成部３３における光パルスの状態の選択、秘匿性増強においてシフト鍵から捨てられるビットの選択等のために、乱数列を出力する。

【００６１】

以上説明したように、実施形態に係る乱数列生成装置１によれば、パルスレーザ光Ｌ１，Ｌ２は、第１ポート２４から第１伝送路２２又は第２伝送路２３を伝送されて第２ポート２５に至り、ファラディミラー５０によって反射された後に、第２ポート２５から第１伝送路２２又は第２伝送路２３を伝送されて第３ポート２６に至る。第１伝送路２２及び第２伝送路２３は互いに異なる伝送路長を有する。このため、パルスレーザ光Ｌ１，Ｌ２が、干渉計１２の第１ポート２４から第２ポート２５に伝送されるとき、及び、第２ポート２５から第３ポート２６に伝送されるときのそれぞれにおいて、１つのパルスが、干渉性を保った２つのパルス（ダブルパルス）に分離される。ダブルパルスを形成する２つのパルスの内、伝送路長のより長い第１伝送路２２を伝送されたパルスは、伝送先のポートへの到着が第２伝送路２３を伝送されたパルスよりも遅延する。このため、第１伝送路２２及び第２伝送路２３の伝送路長の差が適切に設定されると、半導体レーザ装置１１によって互いに異なるタイミングで生成された２つのパルスレーザ光Ｌ１，Ｌ２から分離されたパルスが第３ポート２６に略同時に到着し、第３ポート２６において互いに干渉して干渉光を生成する。ここで、パルスレーザ光Ｌ１，Ｌ２はパルス毎の位相が乱雑であるため、干渉光の干渉ピークの光強度は乱雑な値となる。この干渉光がフォトダイオード５１に入力されると、フォトダイオード５１は、干渉ピークに対応するピークの信号強度が乱雑な電気信号を出力する。この電気信号がＡＤ変換部５３に入力されると、ＡＤ変換部５３は、電気信号のピークの信号強度と予め設定された閾値との大小関係に基づいて、２値化された乱数列を出力する。よって、簡素な構成により、情報理論的に安全な乱数列を高速で生成することができる。

【００６２】
また、乱数列生成装置１は、ＡＤ変換部５３において生成された乱数列を記憶する乱数列記憶部５６を更に備える。このため、乱数列が必要となったときに直ちに乱数列を出力することができる。
【００６３】
また、乱数列生成装置１は、ＡＤ変換部５３において生成された乱数列に対して乱数性の検証を実行し、検証に適合した乱数列を乱数列記憶部５６に出力する乱数性検定部５５を更に備える。このため、半導体レーザ装置１１によって生成されるパルスレーザ光Ｌ１，Ｌ２同士に位相相関がないことを保証することができる。
【００６４】
図５は、乱数性の検証の有無に応じた暗号鍵情報の伝送距離と暗号鍵生成レートとの関係を示すグラフである。図５において、横軸は暗号鍵情報の伝送距離、縦軸は１つのパルスレーザ光が量子暗号送信機１０から量子暗号受信機９０に送信された場合において、安全性の保証された暗号鍵の生成可能なビット数（パルスあたり鍵生成レート）を示す。図５は、乱数性が検証された乱数列、及び、乱数性が検証されていない乱数列のそれぞれにおける、暗号鍵情報の伝送距離とパルスあたり鍵生成レートとの関係を示している。ここで、「乱数性が検証された乱数列」とは、乱数性検定部５５において乱数性の検証が実行され、検証に適合した乱数列を意味する。一方、「乱数性が検証されていない乱数列」とは、乱数性検定部５５において乱数性の検証が実行されていない乱数列を意味する。量子鍵配送では、伝送距離が長くなると、伝送路において光強度が減衰するため、量子暗号受信機９０によって検出される光子の割合が低下する。また、伝送距離が長くなると、伝送路における雑音の影響が大きくなるため、誤り率が増大する。これらにより、伝送距離が長くなることに応じてパルスあたりの暗号鍵が生成されるレートが低下することから、伝送距離に制限が生じる。
【００６５】
ここで、乱数列生成装置１では、半導体レーザ装置１１によって繰り返し生成されるパルスレーザ光同士に位相相関がない場合には、フォトダイオード５１において繰り返し生成される干渉光の干渉ピークの光強度は乱雑な値となる。一方、位相相関がある場合には、この乱雑性は失われている。以上により、取得された乱数列の乱数性を検証することにより、パルスレーザ光同士の位相相関の有無を検証していることになる。位相相関がないことが保証された場合には、誤り率に対して漏洩情報量を少なく見積もることができる。よって、伝送距離をより長くすることができる。
【００６６】
また、実施形態に係る量子暗号送信機１０によれば、乱数列生成装置１を備え、干渉計１２は、出力端２１側に接続され、第１ポート２４に入力されて第１伝送路２２又は第２伝送路２３を経由したパルスレーザ光のそれぞれを出力する第４ポート２７を更に有し、第４ポート２７から出力されるパルスレーザ光の光強度及び位相を乱数列記憶部５６に記憶された乱数列に基づいて変調する変調部１３を備える。このため、量子暗号送信機１０が備えている半導体レーザ装置１１及び干渉計１２を、乱数列生成装置１の半導体レーザ装置１１及び干渉計１２としても利用するため、構成を簡素化することができる。
【００６７】
また、実施形態に係る量子暗号通信システム１００によれば、量子暗号送信機１０を備え、変調部１３によって光強度及び位相を変調されたパルスレーザ光を量子暗号送信機１０との間で量子通信する量子暗号受信機９０を備える。このため、量子暗号送信機１０が備えている半導体レーザ装置１１及び干渉計１２を、乱数列生成装置１の半導体レーザ装置１１及び干渉計１２としても利用するため、構成を簡素化することができる。
【００６８】
なお、本発明は、上記実施形態に限定されない。例えば、上記実施形態では、量子暗号通信システム１００は光ファイバ等を含む光伝送路８０を備えることとした。このため、量子暗号送信機１０と量子暗号受信機９０とは、光ファイバを介して暗号鍵情報を持つ光

子を伝送する。しかし、光伝送路８０は光ファイバを含んでいなくてもよく、この場合、量子暗号送信機１０と量子暗号受信機９０とは、例えば空間を介して暗号鍵情報を持つ光子を伝送してもよい。

【００６９】

また、上記実施形態では、乱数列生成装置１は処理回路５２を備えるとしたが、乱数列生成装置１は、処理回路５２の内の少なくともＡＤ変換部５３を備えていればよい。

【００７０】

また、上記実施形態では、干渉計１２は非対称マッハツェンダ干渉計であるとしたが、干渉計１２は、例えば非対称なマイケルソン干渉計等の他の種類の干渉計であってもよい。干渉計１２として非対称なマイケルソン干渉計を利用する場合には、干渉計１２の出力の一部を反射させるためのビームスプリッタ等の光学部品を追加する必要がある。

【００７１】

また、上記実施形態では、第２ポート２５にはファラディミラー５０が接続されているとしたが、第２ポート２５には通常のミラーが接続されていてもよい。

【００７２】

また、上記実施形態では、変調部１３は、ダブルパルスを形成するパルスレーザ光の光強度及び位相をランダムに変調させるとした。しかし、変調部１３は、各パルスレーザ光の位相に限らず、ダブルパルス間の振幅比及び位相差（すなわち、ダブルパルスの状態）を変調してもよい。具体的には、変調部１３の内の状態生成部３３が、ダブルパルス間の振幅比及び位相差を変調してもよい。なお、この場合、状態生成部３３は、公知の位相変調器と公知の強度変調器との組み合わせ、又はニオブ酸リチウム結晶を用いた２電極型マッハツェンダ型変調器を用いてもよい。特に、デコイＢＢ８４プロトコルの状態においては、変調部１３は、ダブルパルス間の振幅比及び位相差を変調する。

【００７３】

また、上記実施形態では、秘匿性増強において、シフト鍵からランダムに捨てられるビットの選択においては、乱数源４０によって生成された乱数に基づいて、各成分の値（０，１）がランダムに選択された行列を用いたユニバーサルハッシュ関数が用いられるとした。しかし、シフト鍵からランダムに捨てられるビットの選択においては、量子暗号送信機１０及び量子暗号受信機９０に予め複数のユニバーサルハッシュ関数を記憶させておき、乱数源４０によって生成された乱数に基づいて、何れのユニバーサルハッシュ関数を適用するかの選択を行ってもよい。

【００７４】

また、上記実施形態では、ダブルパルスの量子状態の基底としてＸ基底及びＺ基底を採用したが、ダブルパルスの量子状態の基底としてＸ基底及びＹ基底を採用してもよい。このとき、デコイＢＢ８４プロトコルに必要な４つの状態は下記の式（５）及び式（６）で表される。

【数５】

$$\frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right) \quad \cdots(5)$$

【数６】

$$\frac{1}{\sqrt{2}}\left(|0\rangle \pm i|1\rangle\right) \quad \cdots(6)$$

【００７５】

ここで、乱数列生成装置は、ＡＤ変換部において生成された乱数列を記憶する乱数列記憶部を更に備えてもよい。この場合、乱数列が必要となったときに直ちに乱数列を出力することができる。

【００７６】

また、乱数列生成装置は、ＡＤ変換部において生成された乱数列に対して乱数性の検証

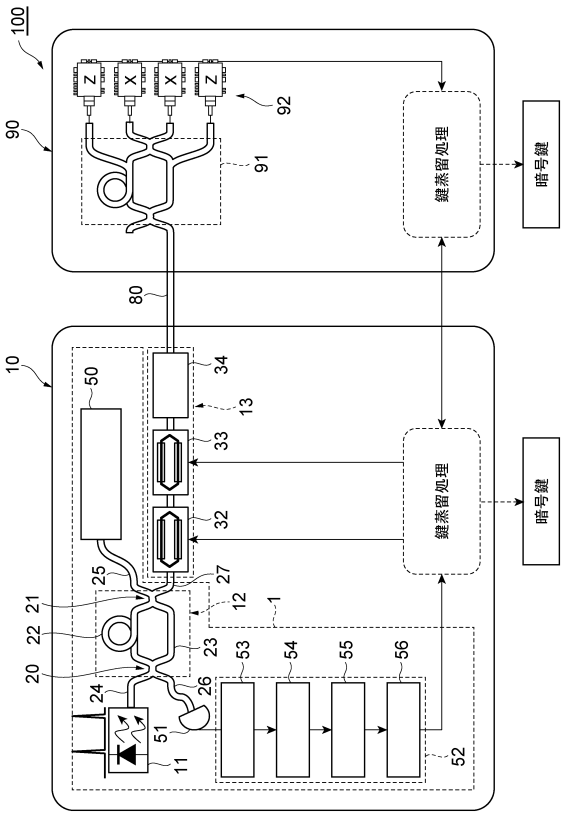
を実行し、検証に適合した乱数列を乱数列記憶部に出力する乱数性検定部を更に備えてもよい。この場合、半導体レーザ装置によって生成されるパルスレーザ光同士に位相相関がないことを保証することができる。

【符号の説明】

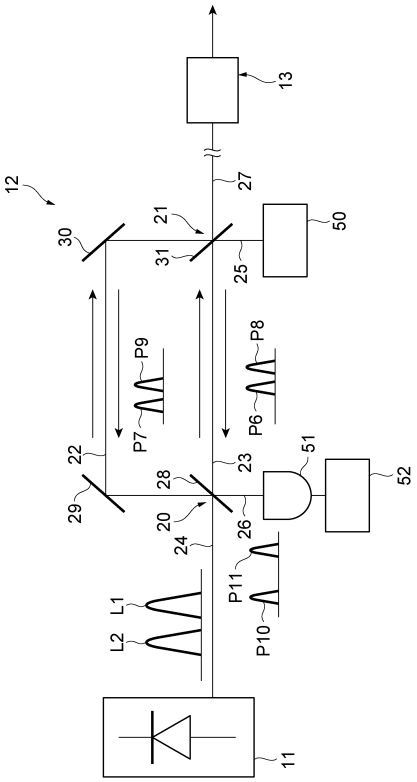
【００７７】

１…乱数列生成装置、１０…量子暗号送信機、１１…半導体レーザ装置、１２…干渉計、１３…変調部、２０…入力端、２１…出力端、２２…第１伝送路、２３…第２伝送路、２４…第１ポート、２５…第２ポート、２６…第３ポート、２７…第４ポート、５０…ファラディミラー（光反射部）、５１…フォトダイオード、５３…ＡＤ変換部、５５…乱数性検定部、５６…乱数列記憶部、９０…量子暗号受信機、１００…量子暗号通信システム、Ｌ１，Ｌ２…パルスレーザ光。

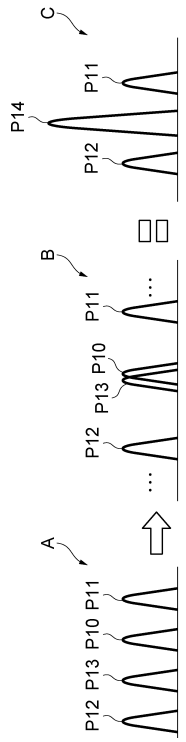
【図１】



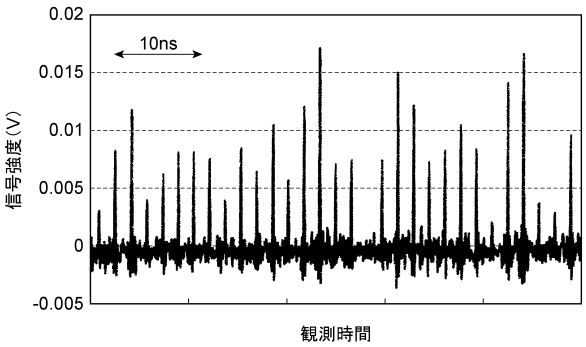
【図２】



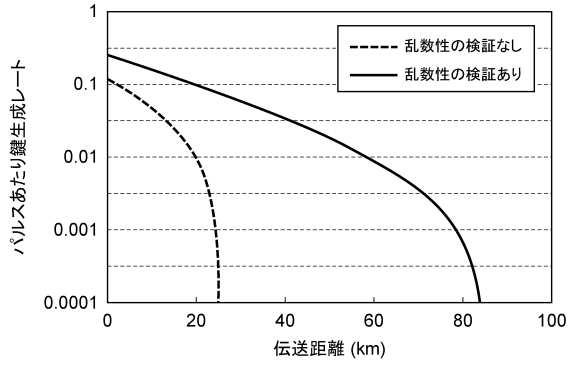
【図３】


A
P11
P10
P13
P12
B
P11
P10
P13
P12
C
P11
P14
P12

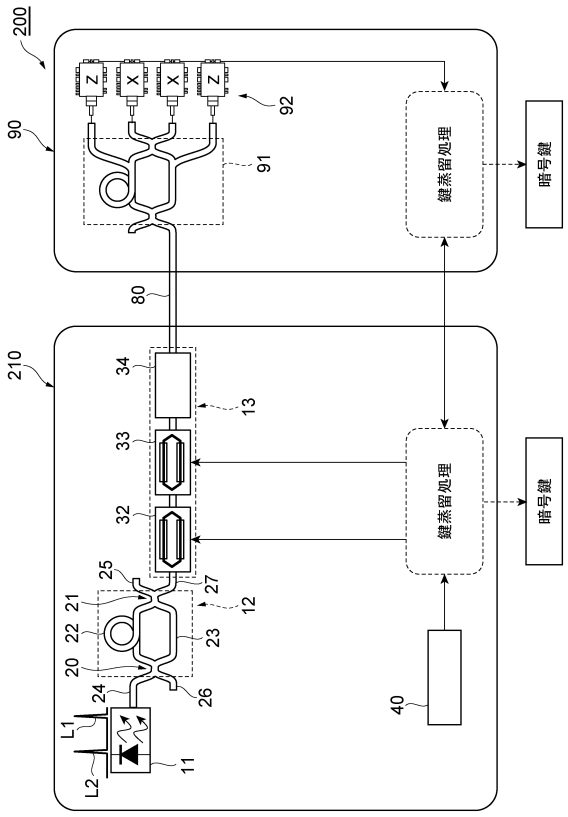
【図４】


10ns
0.02
0.015
0.01
0.005
0
-0.005
信号強度(V)
観測時間

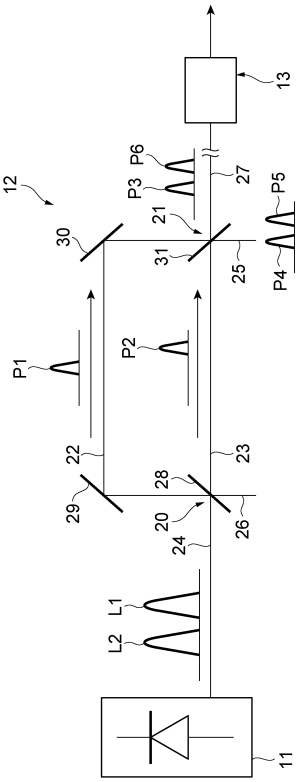
【図５】


乱数性の検証なし
乱数性の検証あり
1
0.1
0.01
0.001
0.0001
パルスあたり鍵生成レート
0
20
40
60
80
100
伝送距離 (km)

【図６】


200
90
Z
X
X
Z
92
91
鍵蒸留処理
暗号鍵
80
210
34
13
33
32
25
27
12
21
22
23
20
24
26
L1
L2
11
40
鍵蒸留処理
暗号鍵

【図７】



フロントページの続き

(51)Int.Cl.			FI	
H04B	*10/516*	*(2013.01)*	H04B	10/516
G02F	*1/225*	*(2006.01)*	G02F	1/225
G02F	*3/00*	*(2006.01)*	G02F	3/00

早期審査対象出願

審査官　金沢　史明

(56)参考文献　特開２０１６－６６２９（ＪＰ，Ａ）
米国特許出願公開第２０１３／００３６１４５（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)

Ｇ０９Ｃ	１／００
Ｇ０２Ｆ	１／２１－　１／２２５
Ｇ０２Ｆ	３／００
Ｇ０６Ｆ	７／５８
Ｈ０４Ｂ	１０／５１６
Ｈ０４Ｂ	１０／７０
Ｈ０４Ｂ	１０／８５
Ｈ０４Ｌ	９／１２