

(19) 日本国特許庁(JP)

再公表特許(A1)

(11) 国際公開番号

W02017/135444

発行日 平成30年12月20日 (2018.12.20)

(43) 国際公開日 平成29年8月10日 (2017.8.10)

(51) Int.Cl.			F I			テーマコード (参考)	
G09C	1/00	(2006.01)	G09C	1/00	650B	2K102	
H04L	9/12	(2006.01)	H04L	9/00	631	5J104	
G06F	7/58	(2006.01)	G06F	7/58	680	5K102	
H04B	10/70	(2013.01)	H04B	10/70			
H04B	10/85	(2013.01)	H04B	10/85			

審査請求 未請求 予備審査請求 未請求 (全 18 頁) 最終頁に続く

出願番号 特願2017-565666 (P2017-565666)
 (21) 国際出願番号 PCT/JP2017/004081
 (22) 国際出願日 平成29年2月3日 (2017.2.3)
 (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 日本国 (JP)

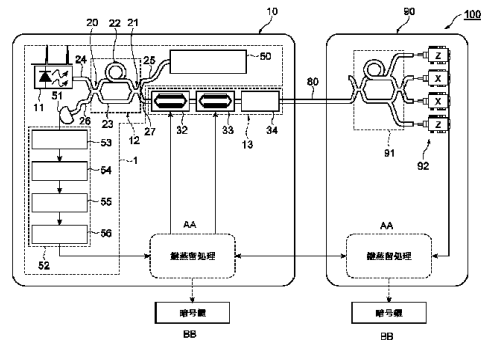
(71) 出願人 504173471
 国立大学法人北海道大学
 北海道札幌市北区北8条西5丁目
 (74) 代理人 100088155
 弁理士 長谷川 芳樹
 (74) 代理人 100124800
 弁理士 諏澤 勇司
 (74) 代理人 100195811
 弁理士 秋元 達也
 (72) 発明者 富田 章久
 北海道札幌市北区北8条西5丁目 国立大
 学法人北海道大学内
 (72) 発明者 中田 賢佑
 北海道札幌市北区北8条西5丁目 国立大
 学法人北海道大学内

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) 【要約】

乱数列生成装置 1 は、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 1 1 と、互いに異なる伝送路長を有する第 1 伝送路 2 2 及び第 2 伝送路 2 3 と、入力端 2 0 側に接続され、パルスレーザ光が入力される第 1 ポート 2 4 と、出力端 2 1 側に接続され、何れかの伝送路を経由したパルスレーザ光を出力する第 2 ポート 2 5 と、入力端 2 0 側に接続された第 3 ポート 2 6 と、を有する干渉計 1 2 と、第 2 ポート 2 5 に接続され、パルスレーザ光を反射するファラディミラー 5 0 と、第 3 ポート 2 6 に接続され、ファラディミラー 5 0 によって反射され、何れかの伝送路を経由したパルスレーザ光の干渉光に応じて電気信号を出力するフォトダイオード 5 1 と、電気信号の信号強度と閾値との大小関係に基づき乱数列を生成する A/D 変換部 5 3 と、を備える。



AA Key distillation
 BB Encryption key

【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 A/D 変換部と、を備える、乱数列生成装置。

【請求項 2】

前記 A/D 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 A/D 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

10

20

30

40

50

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にそれぞれにおいて、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

10

20

30

40

50

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。

10

【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。

20

【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。

30

【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】

40

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

50

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。

10

【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。

20

【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。

30

【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、非対称マツ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。

40

【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】

50

出力端 2 1 には、第 2 ビームスプリッタ 3 1 が配置されている。第 1 伝送路 2 2 を経由した第 1 パルス P 1 は、第 2 ビームスプリッタ 3 1 によって反射光と透過光とに分離される。第 1 パルス P 1 の内、第 2 ビームスプリッタ 3 1 により反射されたパルスレーザ光の成分を第 3 パルス P 3 とする。また、第 1 パルス P 1 の内、第 2 ビームスプリッタ 3 1 を透過したパルスレーザ光の成分を第 4 パルス P 4 とする。第 3 パルス P 3 と第 4 パルス P 4 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。

【 0 0 2 4 】

また、第 2 伝送路 2 3 を経由した第 2 パルス P 2 は、第 2 ビームスプリッタ 3 1 によって反射光と透過光とに分離される。第 2 パルス P 2 の内、第 2 ビームスプリッタ 3 1 により反射されたパルスレーザ光の成分を第 5 パルス P 5 とする。また、第 2 パルス P 2 の内、第 2 ビームスプリッタ 3 1 を透過したパルスレーザ光の成分を第 6 パルス P 6 とする。第 5 パルス P 5 と第 6 パルス P 6 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。

10

【 0 0 2 5 】

このようにして、第 1 ポート 2 4 に入力された 1 つのパルスからなるパルスレーザ光 L 1 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 P 3 及び第 6 パルス P 6 として、第 4 ポート 2 7 から出力される。

【 0 0 2 6 】

図 6 に示すように、第 4 ポート 2 7 には変調部 1 3 が接続されている。変調部 1 3 は、強度変調部 3 2 と、状態生成部 3 3 と、減衰部（減衰器）3 4 と、を有している。変調部 1 3 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 1 3 は、生成した送信用パルスレーザ光を光伝送路 8 0 に出力する。なお、第 2 ポート 2 5 及び第 3 ポート 2 6 には何も接続されていない。

20

【 0 0 2 7 】

強度変調部 3 2 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 3 2 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 3 2 は、第 3 パルス P 3 及び第 6 パルス P 6 が入力されると、乱数源 4 0 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 3 2 は、減衰部 3 4 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。

30

【 0 0 2 8 】

状態生成部 3 3 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 3 3 は、第 3 パルス P 3 及び第 6 パルス P 6 が入力されると、乱数源 4 0 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 P 3 及び第 6 パルス P 6 の位相を変調する。

【 0 0 2 9 】

ここで、第 3 パルス P 3 及び第 6 パルス P 6 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 P 3 及び第 6 パルス P 6 の内、先行して伝送する第 6 パルス P 6 の量子状態を $|0\rangle$ と記載し、遅れて伝送する第 3 パルス P 3 の量子状態を $|1\rangle$ 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。

40

【 数 1 】

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \dots(1)$$

【 0 0 3 0 】

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

50

要な 4 つの状態は下記の式 (2)、式 (3)、式 (4) で表される。

【数 2】

$$\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \quad \dots(2)$$

【数 3】

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

【数 4】

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

10

【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 基底のど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。

20

【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。

30

【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。

40

【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

50

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。

10

【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]

20

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。

30

【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 P_4 及び第 5 パルス P_5 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 P_4 及び第 5 パルス P_5 は、第 2 ポート 25 に再び入力する。

【0046】

40

第 2 ポート 25 に再び入力した第 4 パルス P_4 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 P_4 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 P_6 とする。また、第 4 パルス P_4 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 P_7 とする。第 6 パルス P_6 と第 7 パルス P_7 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 P_5 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 P_5 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 P_8 とする。また、第 5 パルス P_5

50

の内、第2ビームスプリッタ31を透過したパルスレーザー光の成分を第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ー光の成分を第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ー光の成分を第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、半導体レーザー装置11によって生成されたパルスレーザー光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、半導体レーザー装置11によってパルスレーザー光L1よりも1クロック遅れて生成されたパルスレーザー光L2においても、パルスは上述した挙動をする。ここで、パルスレーザー光L2において、パルスレーザー光L1の第10パルスP10に相当するパルス(すなわち、パルスレーザー光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、パルスレーザー光L2において、パルスレーザー光L1の第11パルスP11に相当するパルス(すなわち、パルスレーザー光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、パルスレーザー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に各パルスレーザー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、パルスレーザー光L1から分離された第10パルスP10と、パルスレーザー光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

10

20

30

40

50

出力する。フォトダイオード 5 1 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。

【 0 0 5 5 】

半導体レーザ装置 1 1 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 1 4 パルス P 1 4 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 5 1 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 1 4 パルス P 1 4 がフォトダイオード 5 1 に入力されると、フォトダイオード 5 1 は、第 1 4 パルス P 1 4 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。

【 0 0 5 6 】

処理回路 5 2 は、フォトダイオード 5 1 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 5 2 は、A D 変換部 5 3 と、乱数抽出部 5 4 と、乱数性検定部 5 5 と、乱数列記憶部 5 6 と、を有する。

【 0 0 5 7 】

A D 変換部 5 3 は、電気信号をアナログ値からデジタル値に変換する。A D 変換部 5 3 は、予め設定された閾値を記憶している。A D 変換部 5 3 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, \dots, 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, \dots, 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。

【 0 0 5 8 】

乱数抽出部 5 4 は、 m 個の電気信号のピークから取得された $m \times n$ ビットの乱数列における $m i n$ - エントロピー $H_{m i n}$ を算出する。ここで、 $m i n$ - エントロピー $H_{m i n}$ 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 $P_{m a x} = \max P(I)$ としたときに、 $H_{m i n} = -\log_2 P_{m a x}$ で表される値である。乱数抽出部 5 4 は、ユニバーサルハッシュ関数を用いて、 $m \times n$ ビットの乱数列から $H_{m i n}$ 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 5 4 は、 $H_{m i n}$ と乱数列との大きさの比 $R = H_{m i n} / m n$ を出力する。

【 0 0 5 9 】

乱数性検定部 5 5 は、乱数抽出部 5 4 によって取得された乱数列を規定量 (例えば、1 M 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 5 5 は、 $H_{m i n}$ 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 $m i n$ - エントロピー $H_{m i n}$ 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 5 5 は、乱数性の検証に適合した乱数列を乱数列記憶部 5 6 に出力する。

【 0 0 6 0 】

乱数列記憶部 5 6 は、乱数性検定部 5 5 から入力される乱数列を記憶する。そして、乱数列記憶部 5 6 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 5 6 は、強度変調部 3 2 における光強度の選択、状態生成部 3 3 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。

【 0 0 6 1 】

10

20

30

40

50

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 L 1 , L 2 は、第 1 ポート 2 4 から第 1 伝送路 2 2 又は第 2 伝送路 2 3 を伝送されて第 2 ポート 2 5 に至り、ファラディミラー 5 0 によって反射された後に、第 2 ポート 2 5 から第 1 伝送路 2 2 又は第 2 伝送路 2 3 を伝送されて第 3 ポート 2 6 に至る。第 1 伝送路 2 2 及び第 2 伝送路 2 3 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 L 1 , L 2 が、干渉計 1 2 の第 1 ポート 2 4 から第 2 ポート 2 5 に伝送されるとき、及び、第 2 ポート 2 5 から第 3 ポート 2 6 に伝送されるときにそれぞれにおいて、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 2 2 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 2 3 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 2 2 及び第 2 伝送路 2 3 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 1 1 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 L 1 , L 2 から分離されたパルスが第 3 ポート 2 6 に略同時に到着し、第 3 ポート 2 6 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 L 1 , L 2 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 5 1 に入力されると、フォトダイオード 5 1 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 A D 変換部 5 3 に入力されると、A D 変換部 5 3 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。

10

20

【 0 0 6 2 】

また、乱数列生成装置 1 は、A D 変換部 5 3 において生成された乱数列を記憶する乱数列記憶部 5 6 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。

【 0 0 6 3 】

また、乱数列生成装置 1 は、A D 変換部 5 3 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 5 6 に出力する乱数性検定部 5 5 を更に備える。このため、半導体レーザ装置 1 1 によって生成されるパルスレーザ光 L 1 , L 2 同士に位相相関がないことを保証することができる。

30

【 0 0 6 4 】

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 1 0 から量子暗号受信機 9 0 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 5 5 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 5 5 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 9 0 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伴っ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。

40

【 0 0 6 5 】

ここで、乱数列生成装置 1 では、半導体レーザ装置 1 1 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 5 1 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

50

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を經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。

10

【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。

20

【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。

30

【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。

40

【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

50

用するかの選択を行ってもよい。

【 0 0 7 4 】

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 】

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

10

【 数 6 】

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

【 0 0 7 5 】

ここで、乱数列生成装置は、A D 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。

【 0 0 7 6 】

また、乱数列生成装置は、A D 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。

20

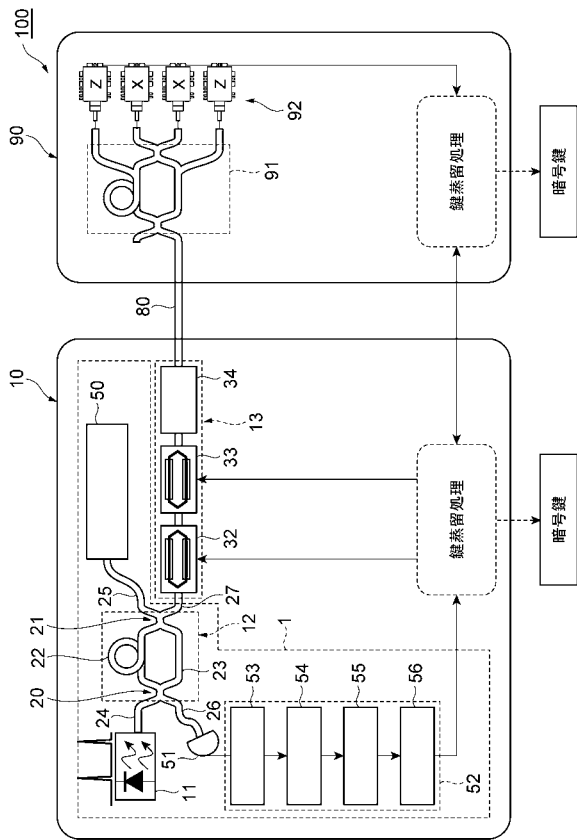
【 符号の説明 】

【 0 0 7 7 】

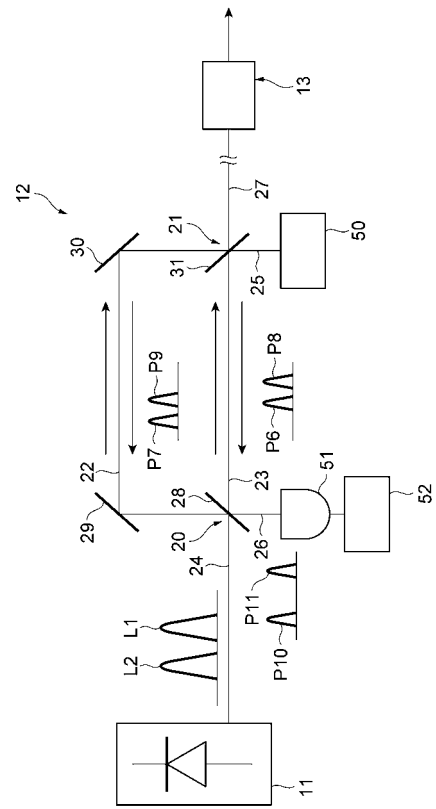
1 ... 乱数列生成装置、 1 0 ... 量子暗号送信機、 1 1 ... 半導体レーザ装置、 1 2 ... 干渉計、 1 3 ... 変調部、 2 0 ... 入力端、 2 1 ... 出力端、 2 2 ... 第 1 伝送路、 2 3 ... 第 2 伝送路、 2 4 ... 第 1 ポート、 2 5 ... 第 2 ポート、 2 6 ... 第 3 ポート、 2 7 ... 第 4 ポート、 5 0 ... フアラディミラー（光反射部）、 5 1 ... フォトダイオード、 5 3 ... A D 変換部、 5 5 ... 乱数性検定部、 5 6 ... 乱数列記憶部、 9 0 ... 量子暗号受信機、 1 0 0 ... 量子暗号通信システム、 L 1 , L 2 ... パルスレーザ光。

30

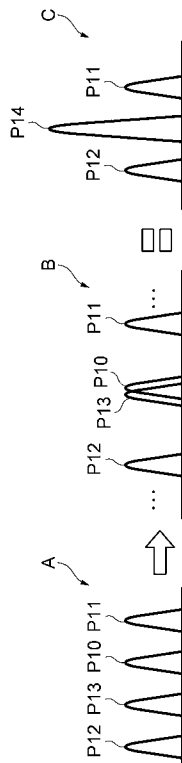
【 図 1 】



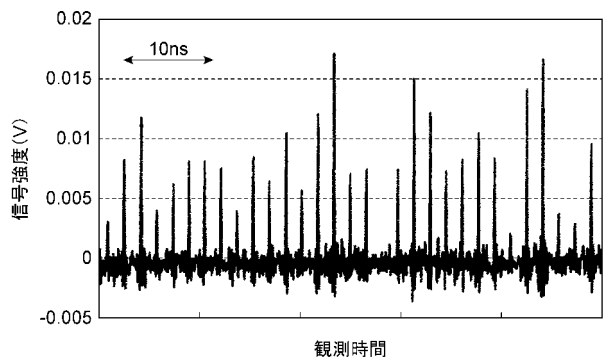
【 図 2 】



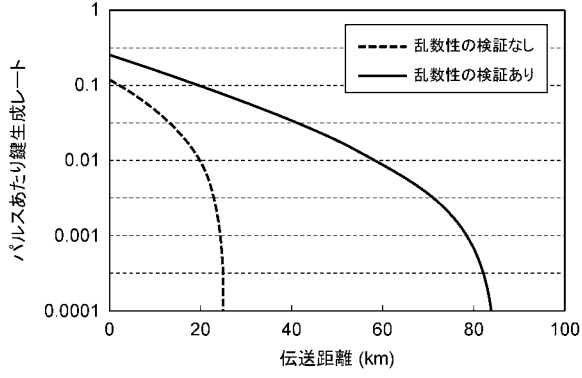
【 図 3 】



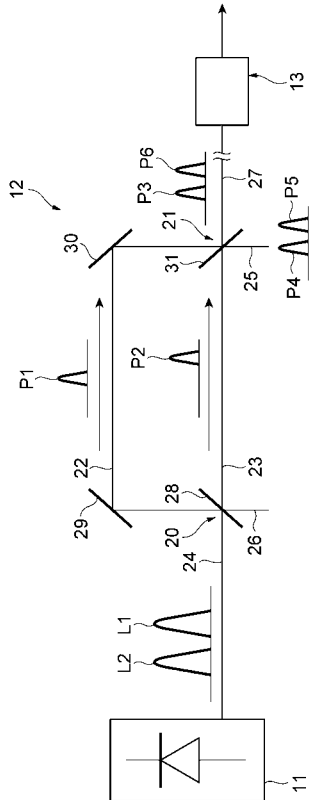
【 図 4 】



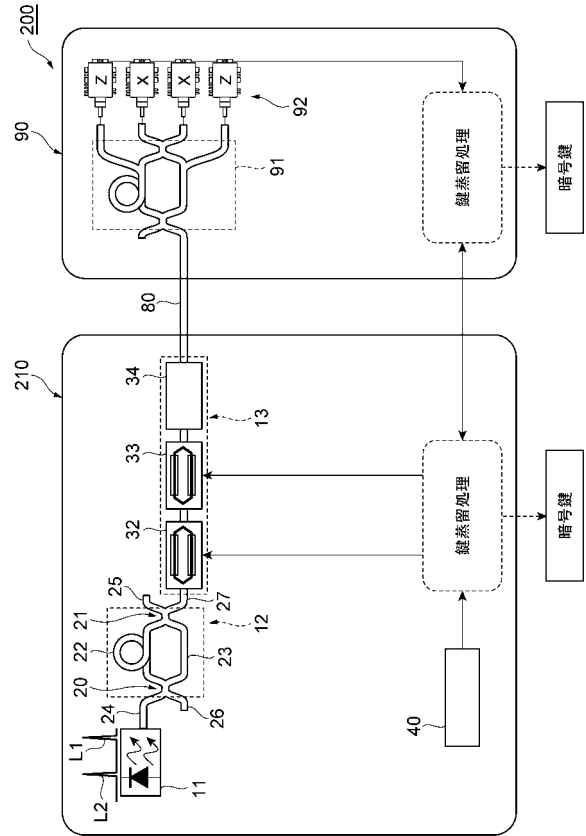
【 図 5 】



【 図 7 】



【 図 6 】



【 国際調査報告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP2017/004081
A. CLASSIFICATION OF SUBJECT MATTER <i>G09C1/00(2006.01)i, G02F1/21(2006.01)i, G02F3/00(2006.01)i, G06F7/58(2006.01)i, H04B10/70(2013.01)i, H04B10/85(2013.01)i, H04L9/12(2006.01)i</i>		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) <i>G09C1/00, G02F1/21, G02F3/00, G06F7/58, H04B10/70, H04B10/85, H04L9/12</i>		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched <i>Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2017</i> <i>Kokai Jitsuyo Shinan Koho 1971-2017 Toroku Jitsuyo Shinan Koho 1994-2017</i>		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2016-6629 A (Toshiba Corp.), 14 January 2016 (14.01.2016), & US 2015/0331672 A1 & GB 2526288 A	1-5
A	US 2013/0036145 A1 (PRUNERI, Valerio et al.), 07 February 2013 (07.02.2013), & US 2013/0036145 A1 & CH 705137 A2	1-5
<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 20 April 2017 (20.04.17)		Date of mailing of the international search report 09 May 2017 (09.05.17)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan		Authorized officer Telephone No.

国際調査報告		国際出願番号 PCT/J P 2 0 1 7 / 0 0 4 0 8 1	
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. G09C1/00(2006.01)i, G02F1/21(2006.01)i, G02F3/00(2006.01)i, G06F7/58(2006.01)i, H04B10/70(2013.01)i, H04B10/85(2013.01)i, H04L9/12(2006.01)i			
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int.Cl. G09C1/00, G02F1/21, G02F3/00, G06F7/58, H04B10/70, H04B10/85, H04L9/12			
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2017年 日本国実用新案登録公報 1996-2017年 日本国登録実用新案公報 1994-2017年			
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号	
A	JP 2016-6629 A (株式会社東芝) 2016.01.14, & US 2015/0331672 A1 & GB 2526288 A	1-5	
A	US 2013/0036145 A1 (PRUNERI, Valerio et al.) 2013.02.07, & US 2013/0036145 A1 & CH 705137 A2	1-5	
<input type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的な技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願			
国際調査を完了した日 20.04.2017		国際調査報告の発送日 09.05.2017	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 金沢 史明	5 S 4 5 3 8 電話番号 03-3581-1101 内線 3546

フロントページの続き

(51) Int.Cl.			F I			テーマコード (参考)
H 0 4 B	10/516	(2013.01)	H 0 4 B	10/516		
G 0 2 F	1/225	(2006.01)	G 0 2 F	1/225		
G 0 2 F	3/00	(2006.01)	G 0 2 F	3/00		

(81) 指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ

(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 / 「セキュアフォトリ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

F ターム(参考) 2K102 BB01 BB04 BB10 BC04 BD04 CA20 DA04 DB04 DC07 DD05
EA02 EA21 EB22
5J104 AA05 FA10
5K102 AA15 AA61 AB11 AH02 PB20 PH02 PH31 RB02 RD26 RD28

(注) この公表は、国際事務局 (W I P O) により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願 (日本語実用新案登録出願) の国際公開の効果は、特許法第 184 条の 10 第 1 項 (実用新案法第 48 条の 13 第 2 項) により生ずるものであり、本掲載とは関係ありません。