

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6803620号
(P6803620)

(45) 発行日 令和2年12月23日(2020.12.23)

(24) 登録日 令和2年12月3日(2020.12.3)

(51) Int.Cl.		F I			
HO4L	9/12	(2006.01)	HO4L	9/00	631
HO4B	10/70	(2013.01)	HO4B	10/70	
GO2F	1/01	(2006.01)	GO2F	1/01	B

請求項の数 8 (全 16 頁)

(21) 出願番号	特願2018-537587 (P2018-537587)	(73) 特許権者	504173471
(86) (22) 出願日	平成29年9月4日(2017.9.4)		国立大学法人北海道大学
(86) 国際出願番号	PCT/JP2017/031800		北海道札幌市北区北8条西5丁目
(87) 国際公開番号	W02018/043742	(74) 代理人	100088155
(87) 国際公開日	平成30年3月8日(2018.3.8)		弁理士 長谷川 芳樹
審査請求日	令和2年8月31日(2020.8.31)	(74) 代理人	100124800
(31) 優先権主張番号	特願2016-173063 (P2016-173063)		弁理士 諏澤 勇司
(32) 優先日	平成28年9月5日(2016.9.5)	(74) 代理人	100195811
(33) 優先権主張国・地域又は機関	日本国(JP)		弁理士 秋元 達也
		(72) 発明者	富田 章久
(出願人による申告)平成23年度 国立研究開発法人			北海道札幌市北区北8条西5丁目 国立大
情報通信研究機構「高度通信・放送研究開発委託研究」		(72) 発明者	中田 賢佑
／「セキュアフォトニックネットワークの研究開発」課			北海道札幌市北区北8条西5丁目 国立大
題イ 量子暗号安全性評価理論」、産業技術力強化法第			大学法人北海道大学内
19条の適用を受ける特許出願			最終頁に続く

(54) 【発明の名称】 量子暗号鍵出力装置、量子暗号鍵通信システム及び量子暗号鍵出力方法

(57) 【特許請求の範囲】

【請求項1】

量子暗号鍵の生成に用いられる符号化されたパルスレーザ光を生成し、当該パルスレーザ光からなる光パルス列を量子暗号鍵入力装置に出力する量子暗号鍵出力装置であって、前記パルスレーザ光を繰り返し生成する光源と、

前記量子暗号鍵に基づいて前記パルスレーザ光を符号化するエンコーダと、

符号化された前記パルスレーザ光を第1光路及び第2光路に所定の光強度比となるように分岐させる光分岐部と、

前記第1光路に分岐された前記パルスレーザ光である第1パルスレーザ光の光子数が1以下の値である複数の候補値のうちの何れかとなるように、前記第1パルスレーザ光の光強度を減衰させる減衰部と、

前記減衰部によって光強度を減衰させられた前記第1パルスレーザ光を前記量子暗号鍵入力装置に出力する光出力部と、

前記第2光路に分岐された前記パルスレーザ光である第2パルスレーザ光の光強度が所定の範囲内にあるか否かを判定する光強度判定部と、

前記光強度判定部によって光強度が前記所定の範囲内ないと判定された前記第2パルスレーザ光に対応する前記第1パルスレーザ光を特定する特定情報を、前記量子暗号鍵入力装置に出力する情報出力部と、を備える、量子暗号鍵出力装置。

【請求項2】

前記光強度判定部は、

前記第 2 パルスレーザー光を入力し、入力された前記第 2 パルスレーザー光の光強度に応じた電気信号を出力する光電変換部と、

前記光電変換部によって出力された前記電気信号に基づいて、当該電気信号に係る前記第 2 パルスレーザー光の光強度が前記所定の範囲内にあるか否かを判定する比較部と、を有する、請求項 1 に記載の量子暗号鍵出力装置。

【請求項 3】

前記特定情報は、前記光源によって繰り返し生成される前記パルスレーザー光に係る前記第 1 パルスレーザー光のうち、前記光強度判定部によって光強度が前記所定の範囲内ないと判定された前記第 2 パルスレーザー光に対応する前記第 1 パルスレーザー光の順番に関する情報を含む、請求項 1 又は 2 に記載の量子暗号鍵出力装置。

10

【請求項 4】

前記特定情報は、前記光源によって繰り返し生成される前記パルスレーザー光に係る前記第 1 パルスレーザー光のうち、前記光強度判定部によって光強度が前記所定の範囲内にあると判定された前記第 2 パルスレーザー光に対応する前記第 1 パルスレーザー光の順番に関する情報を含む、請求項 1 ~ 3 の何れか一項に記載の量子暗号鍵出力装置。

【請求項 5】

前記エンコーダは、

前記パルスレーザー光を互いに干渉性を有する一対のパルスに分割する干渉計と、

前記パルスレーザー光の位相を変調する位相変調部と、

前記パルスレーザー光の光強度を変調する強度変調部と、を有し、

20

前記パルスレーザー光を、前記干渉計によって前記一対のパルスに分割すると共に、前記位相変調部によって当該パルスレーザー光の位相を変調し、且つ、前記強度変調部によって当該パルスレーザー光の光強度を変調することによって、当該パルスレーザー光を符号化する、請求項 1 ~ 4 の何れか一項に記載の量子暗号鍵出力装置。

【請求項 6】

前記位相変調部は、前記干渉計よりも後段に配置されている、請求項 5 に記載の量子暗号鍵出力装置。

【請求項 7】

請求項 1 ~ 6 の何れか一項に記載の量子暗号鍵出力装置と、

前記量子暗号鍵出力装置によって出力される前記光パルス列を入力する量子暗号鍵入力装置と、を具備し、

30

前記量子暗号鍵入力装置は、

前記光出力部によって出力された前記第 1 パルスレーザー光を入力する光入力部と、

前記情報出力部によって出力された前記特定情報を入力する情報入力部と、

前記光入力部によって入力された前記第 1 パルスレーザー光から、前記情報入力部によって入力された前記特定情報によって特定される前記第 1 パルスレーザー光を除外して、新たな量子暗号鍵とする鍵蒸留部と、を備える、量子暗号鍵通信システム。

【請求項 8】

量子暗号鍵の生成に用いられる符号化されたパルスレーザー光を生成し、当該パルスレーザー光からなる光パルス列を量子暗号鍵入力装置に出力する量子暗号鍵出力方法であって、

40

前記パルスレーザー光を繰り返し生成する発光工程と、

前記量子暗号鍵に基づいて前記パルスレーザー光を符号化する符号化工程と、

符号化された前記パルスレーザー光を第 1 光路及び第 2 光路に所定の光強度比となるように分岐させる光分岐工程と、

前記第 1 光路に分岐された前記パルスレーザー光である第 1 パルスレーザー光の光子数が 1 以下の値である複数の候補値のうちの何れかとなるように、前記第 1 パルスレーザー光の光強度を減衰させる減衰工程と、

光強度を減衰させられた前記第 1 パルスレーザー光を前記量子暗号鍵入力装置に出力する光出力工程と、

前記第 2 光路に分岐された前記パルスレーザー光である第 2 パルスレーザー光の光強度が所

50

定の範囲内にあるか否かを判定する光強度判定工程と、

光強度が前記所定の範囲内ないと判定された前記第2パルスレーザ光に対応する前記第1パルスレーザ光を特定する特定情報を、前記量子暗号鍵入力装置に出力する情報出力工程と、を備える、量子暗号鍵出力方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明の一態様は、量子暗号鍵出力装置、量子暗号鍵通信システム及び量子暗号鍵出力方法に関する。

【背景技術】

【0002】

情報理論的に安全に情報を伝送するための量子暗号鍵通信システムが知られている。量子暗号鍵通信システムでは、情報の送信者は、量子鍵配送(QKD: Quantum Key Distribution)によって、光子により構成される量子暗号鍵を受信者に伝送する。また、送信者は、受信者に伝送すべき情報を量子暗号鍵によって暗号化し、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。その後、受信者は、暗号化された情報を量子暗号鍵によって復号する。以上により、送信者から受信者に情報が伝送される。ここで、量子暗号鍵が送信者から受信者に伝送される際に量子暗号鍵が第三者によって盗聴されると、量子暗号鍵を構成する光子の量子状態が不確定性原理によって変化する。従って、盗聴された量子暗号鍵を構成する光子には必ず盗聴の痕跡が残ることとなり、送信者及び受信者は、量子暗号鍵の盗聴を確実に検知することができる。

【0003】

量子鍵配送では、送信者から受信者に伝送された量子暗号鍵に対して鍵蒸留処理が実行される。鍵蒸留処理は、例えば盗聴、雑音等に起因する量子暗号鍵の誤りを訂正する誤り訂正と、盗聴等により情報が漏洩した可能性のある量子暗号鍵から、情報が漏洩していないと見做すことができる量子暗号鍵を生成する秘匿性増強と、を含む。秘匿性増強では、情報が漏洩した可能性のある量子暗号鍵に関する情報の量(漏洩情報量)の上限を推定し、推定された漏洩情報量の上限に応じて量子暗号鍵に関する情報の量を減らすことにより、量子暗号鍵の安全性を向上させる。以上により、量子鍵配送では、情報理論的に安全に情報を伝送することが可能となる。

【0004】

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鍵通信システムとして、デコイBB84プロトコルを採用し、パルスレーザ光を繰り返し生成する光源と、パルスレーザ光を符号化して暗号鍵に関する情報を持った光パルスを生成するエンコーダと、パルスレーザ光の光子数が1以下の値である複数の候補値のうちの何れかとなるようにパルスレーザ光の光強度を減衰させる減衰部と、を備えるものが知られている(例えば、特許文献1参照)。

【先行技術文献】

【特許文献】

【0005】

【特許文献1】特開2016-46557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、このような量子暗号鍵通信システムでは、量子暗号鍵を構成するパルスレーザ光の平均光子数が候補値と一致するものとして、漏洩情報量の上限を推定している。しかしながら、量子暗号鍵を構成するパルスレーザ光の実際の光子数は、候補値に対して誤差を含んでいる。光子数の誤差の原因としては、例えば光源の出力強度の揺らぎ、エンコーダに供給される電圧の変動等が考えられる。ここで、情報の伝送における情報理論的な安全性を評価する際には、光子数の誤差の範囲で最も漏洩した情報量が大きくなるように

10

20

30

40

50

推定を行い、誤差があっても安全性が担保できるようにする。このため、光子数の誤差が大きいほど、漏洩情報量の上限が大きく推定され、秘匿性増強において減らすべき量子暗号鍵に関する情報の量が多くなる。その結果、量子暗号鍵の生成率が低下するという問題がある。

【 0 0 0 7 】

本発明の一態様は、上記課題に鑑みて為されたものであり、量子暗号鍵の生成率を向上させることができる量子暗号鍵出力装置、量子暗号鍵通信システム及び量子暗号鍵出力方法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】

【 0 0 0 8 】

本発明の一態様に係る量子暗号鍵出力装置は、量子暗号鍵の生成に用いられる符号化されたパルスレーザ光を生成し、当該パルスレーザ光からなる光パルス列を量子暗号鍵入力装置に出力する量子暗号鍵出力装置であって、パルスレーザ光を繰り返し生成する光源と、量子暗号鍵に基づいてパルスレーザ光を符号化するエンコーダと、符号化されたパルスレーザ光を第1光路及び第2光路に所定の光強度比となるように分岐させる光分岐部と、第1光路に分岐されたパルスレーザ光である第1パルスレーザ光の光子数が1以下の値である複数の候補値のうちの何れかとなるように、第1パルスレーザ光の光強度を減衰させる減衰部と、減衰部によって光強度を減衰させられた第1パルスレーザ光を量子暗号鍵入力装置に出力する光出力部と、第2光路に分岐されたパルスレーザ光である第2パルスレーザ光の光強度が所定の範囲内にあるか否かを判定する光強度判定部と、光強度判定部によって光強度が所定の範囲内ないと判定された第2パルスレーザ光に対応する第1パルスレーザ光を特定する特定情報を、量子暗号鍵入力装置に出力する情報出力部と、を備える。

【 0 0 0 9 】

或いは、本発明の一態様に係る量子暗号鍵通信システムは、上記の量子暗号鍵出力装置と、量子暗号鍵出力装置によって出力される光パルス列を入力する量子暗号鍵入力装置と、を具備し、量子暗号鍵入力装置は、光出力部によって出力された第1パルスレーザ光を入力する光入力部と、情報出力部によって出力された特定情報を入力する情報入力部と、光入力部によって入力された第1パルスレーザ光から、情報入力部によって入力された特定情報によって特定される第1パルスレーザ光を除外して、新たな量子暗号鍵とする鍵蒸留部と、を備える。

【 0 0 1 0 】

或いは、本発明の一態様に係る量子暗号鍵出力方法は、量子暗号鍵の生成に用いられる符号化されたパルスレーザ光を生成し、当該パルスレーザ光からなる光パルス列を量子暗号鍵入力装置に出力する量子暗号鍵出力方法であって、パルスレーザ光を繰り返し生成する発光工程と、量子暗号鍵に基づいてパルスレーザ光を符号化する符号化工程と、符号化されたパルスレーザ光を第1光路及び第2光路に所定の光強度比となるように分岐させる光分岐工程と、第1光路に分岐されたパルスレーザ光である第1パルスレーザ光の光子数が1以下の値である複数の候補値のうちの何れかとなるように、第1パルスレーザ光の光強度を減衰させる減衰工程と、光強度を減衰させられた第1パルスレーザ光を量子暗号鍵入力装置に出力する光出力工程と、第2光路に分岐されたパルスレーザ光である第2パルスレーザ光の光強度が所定の範囲内にあるか否かを判定する光強度判定工程と、光強度が所定の範囲内ないと判定された第2パルスレーザ光に対応する第1パルスレーザ光を特定する特定情報を、量子暗号鍵入力装置に出力する情報出力工程と、を備える。

【 0 0 1 1 】

このような量子暗号鍵出力装置、量子暗号鍵通信システム或いは量子暗号鍵出力方法の何れかでは、光源によって繰り返し生成されたパルスレーザ光を量子暗号鍵に基づいてエンコーダによって符号化し、当該パルスレーザ光を光分岐部によって第1光路及び第2光路に所定の光強度比となるように分岐させる。そして、第1光路に分岐されたパルスレーザ光である第1パルスレーザ光の光強度を減衰部によって減衰させて、当該第1パルスレ

10

20

30

40

50

ーザ光からなる光パルス列を光出力部によって量子暗号鍵入力装置に出力する。ここで、光強度判定部によって、第2光路に分岐されたパルスレーザ光である第2パルスレーザ光の光強度が所定の範囲内ないと判定された場合、情報出力部によって、当該第2パルスレーザ光に対応する第1パルスレーザ光を特定する特定情報が量子暗号鍵入力装置に出力される。第1パルスレーザ光と第2パルスレーザ光とは、同一のパルスレーザ光が光分岐部によって所定の光強度比となるように分岐されたものであるため、第2パルスレーザ光の光強度が所定の範囲内ないと判定された場合、当該第2パルスレーザ光に対応する第1パルスレーザ光の光子数の誤差が所定値よりも大きいと判定することができる。従って、光パルス列及び特定情報を入力した量子暗号鍵入力装置は、量子暗号鍵の生成に際し、誤差が所定値よりも大きい第1パルスレーザ光を特定情報により特定して除外することが可能となる。よって、量子暗号鍵の生成率を向上させることができる。

10

【発明の効果】

【0012】

本発明の一態様によれば、量子暗号鍵の生成率を向上させることができる量子暗号鍵出力装置、量子暗号鍵通信システム及び量子暗号鍵出力方法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鍵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、量子暗号鍵を構成するパルスレーザ光の実際の光子数の分布を示すシミュレーション結果のグラフである。

20

【図3】図3は、パルスレーザ光の実際の光子数の誤差に応じた暗号鍵の生成率の一例を伝送距離との関係で示すグラフである。

【図4】図4は、暗号鍵に対するパルス除外処理を示すフローチャートである。

【発明を実施するための形態】

【0014】

以下、図面を参照しつつ、本発明に係る量子暗号鍵出力装置、量子暗号鍵通信システム及び量子暗号鍵出力方法の好適な実施形態について詳細に説明する。なお、本実施形態において、「前段」とはパルスレーザ光の伝送方向とは反対側を意味し、「後段」とはパルスレーザ光の伝送方向側を意味する。

【0015】

30

図1は、本実施形態の量子暗号鍵通信システムの機能構成を示す概略図である。図1に示すように、量子暗号鍵通信システム100は、送信者側である量子暗号鍵出力装置1と、受信者側である量子暗号鍵入力装置2と、光ファイバ等を含む光伝送路3と、を備える。量子暗号鍵通信システム100は、量子暗号鍵出力装置1と量子暗号鍵入力装置2との間で、符号化されたパルスレーザ光Lを通信することにより、デジタルのビット列からなる暗号鍵に関する情報（以下、「暗号鍵情報」という）を第三者による盗聴に対して情報理論的に安全に共有するシステムである。量子暗号鍵出力装置1は、量子暗号鍵の生成に用いられる符号化されたパルスレーザ光Lを生成し、当該パルスレーザ光Lからなる光パルス列を量子暗号鍵入力装置2に光伝送路3を介して出力する。つまり、量子暗号鍵出力装置1は、光パルスを符号化し、符号化された光パルスを量子暗号鍵入力装置2に光伝送路3を介して出力する。量子暗号鍵入力装置2は、量子暗号鍵出力装置1によって出力されるパルスレーザ光Lからなる光パルス列を入力する。

40

【0016】

量子暗号鍵出力装置1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情報によってメッセージを暗号化する。また、量子暗号鍵出力装置1は、パルスレーザ光Lを符号化して暗号鍵情報を持たせ、当該パルスレーザ光Lを光伝送路3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鍵出力装置1から量子暗号鍵入力装置2に伝送される。光伝送路3は、量子暗号鍵出力装置1から量子暗号鍵入力装置2にパルスレーザ光Lを伝送する。量子暗号鍵入力装置2は、光伝送路3から入力されたパルスレーザ光Lが持つ暗号鍵情報から暗号鍵を取得

50

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。これにより、量子暗号鍵通信システム100によれば、量子暗号鍵出力装置1から量子暗号鍵入力装置2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】

まず、量子暗号鍵通信システム100の量子暗号鍵出力装置1について説明する。量子暗号鍵出力装置1は、半導体レーザ装置(光源)10と、エンコーダ11と、光分岐部12と、アッテネータ(減衰部)13と、光出力部14と、光強度判定部15と、情報出力部16と、乱数列生成部(不図示)と、を備える。乱数列生成部は、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。

10

【0018】

半導体レーザ装置10は、光ファイバ伝送に好適な波長(例えば1.55 μm)の光をパルス発振して、パルス毎の位相が乱雑なパルスレーザ光Lを繰り返し生成する。半導体レーザ装置10は、例えば、量子暗号鍵出力装置1と量子暗号鍵入力装置2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Lを繰り返し生成する。半導体レーザ装置10は、パルスレーザ光Lをエンコーダ11に入力する。

【0019】

エンコーダ11は、半導体レーザ装置10から繰り返し入力されるパルスレーザ光Lを量子暗号鍵に基づいて符号化する。エンコーダ11は、干渉計20と、位相変調部21と、強度変調部22と、を有する。位相変調部21は、干渉計20よりも後段に配置されており、強度変調部22は、位相変調部21よりも後段に配置されている。

20

【0020】

干渉計20は、各パルスレーザ光Lを互いに干渉性を有するダブルパルス(一对のパルス)に分割する。干渉計20は、非対称マツハツェンダ干渉計によって構成されている。干渉計20は、入力端20aと、出力端20bと、入力端20a及び出力端20bを接続する第1伝送路20c及び第2伝送路20dと、を有する。第1伝送路20cの伝送路長は、第2伝送路20dの伝送路長よりも長い。

【0021】

また、干渉計20は、入力端20a側に接続された第1ポート20eと、出力端20b側に接続された第2ポート20fと、を有する。第1ポート20eの前段には、半導体レーザ装置10が接続されている。一方、第2ポート20fの後段には、位相変調部21が接続されている。なお、干渉計20は、入力端20a側、出力端20b側のそれぞれに第1ポート20e、第2ポート20fとは別のポートを有するものの、これらのポートには何も接続されていない。

30

【0022】

半導体レーザ装置10により生成されたパルスレーザ光Lは、第1ポート20eを介して入力端20aに至り、第1伝送路20cを伝送するパルスと、第2伝送路20dを伝送するパルスと、からなるダブルパルスに分割される。ダブルパルスを構成する各パルスは、互いに干渉性を保ちつつ時間的及び空間的に分離されている。各パルスは、出力端20bに至り、第2ポート20fを介して位相変調部21に出力される。

40

【0023】

位相変調部21は、ダブルパルスを形成するパルスレーザ光Lの位相をランダムに変調させる。より具体的には、位相変調部21は、ダブルパルスを形成するパルスレーザ光Lが入力されると、乱数列生成部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、当該パルスレーザ光Lの位相を変調する。位相変調部21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。位相変調部21は、ダブルパルスを形成すると共に位相が変調されたパルスレーザ光Lを強度変調部22に出力する。

【0024】

ここで、ダブルパルスを形成するパルスレーザ光L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、ダブルパルスを形成するパルスレーザ光L

50

の内、先行して伝送するパルスの量子状態を $|0\rangle$ と記載し、遅れて伝送するパルスの量子状態を $|1\rangle$ と記載する。この場合、パルスレーザー光Lの量子状態は、下記の式(1)で表される。

【数1】

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

【0025】

ここでは、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しているため、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。

10

【数2】

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

【数3】

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

【数4】

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

20

【0026】

以上のように、位相変調部21は、パルスレーザー光L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。

【0027】

半導体レーザー装置10はパルスレーザー光Lを繰り返し生成している。このため、位相変調部21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。

【0028】

30

強度変調部22は、ダブルパルスを形成すると共に位相が変調されたパルスレーザー光Lの光強度(光子数)をランダムに変調させる。より具体的には、強度変調部22は、ダブルパルスを形成すると共に位相が変調されたパルスレーザー光Lが入力されると、乱数列生成部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、当該パルスレーザー光Lの光強度を変調する。なお、強度変調部22は、当該パルスレーザー光Lが光分岐部12及びアッテネータ13を更に通過することで、当該パルスレーザー光Lの光子数が1以下の値である複数の候補値のうちの何れかとなるように、光強度を変調する。強度変調部22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22は、ニオブ酸リチウム(LN: LiNbO₃)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22は、ダブルパルスを形成すると共に位相及び光強度が変調されたパルスレーザー光L(すなわち、量子暗号鍵に基づいて符号化されたパルスレーザー光L)を光分岐部12に出力する。

40

【0029】

光分岐部12は、符号化されたパルスレーザー光Lを第1光路P1及び第2光路P2に所定の光強度比となるように分岐させる。第1光路P1においては、光分岐部12の後段にアッテネータ13が接続されている。第2光路P2においては、光分岐部12の後段に光強度判定部15が接続されている。光分岐部12としては、例えば光ファイバカップラを用いることができる。ここでは、光分岐部12は、第1光路P1に分岐されたパルスレーザー光Lである第1パルスレーザー光L1と、第2光路P2に分岐されたパルスレーザー光Lである第2パルスレーザー光L2との光強度比が例えば1:9となるように、パルスレーザー光

50

Lを分岐させる。

【0030】

アッテネータ13は、第1パルスレーザ光L1の平均光子数が1以下の値である複数の候補値（例えば、0光子、0.1光子、及び、0.5光子）のうちの何れかとなるように、第1パルスレーザ光L1の光強度を減衰させる。ここでは、各候補値のうち、0.1光子がデコイパルスの平均光子数に該当し、0.5光子が信号パルスの平均光子数に該当する。アッテネータ13は、第1パルスレーザ光L1の光強度を、例えば強度変調部22を出した信号パルスの平均電力が0.32mWであるとき60dB程度減衰させる。ただし、アッテネータ13によって減衰させられた後の第1パルスレーザ光L1の平均光子数は、上述した複数の候補値の何れかに対して、例えば5%~10%程度の誤差を含んでいる場合がある。アッテネータ13としては、公知のアッテネータを適用可能であり、特定の構成に限定されない。アッテネータ13は、光強度を減衰させた第1パルスレーザ光L1を、光出力部14に出力する。

10

【0031】

光出力部14は、アッテネータ13によって入力された第1パルスレーザ光L1を、量子暗号鍵入力装置2に光伝送路3を介して出力する。光出力部14は、符号化された第1パルスレーザ光L1が量子暗号鍵出力装置1から後段に出力されるための構成であれば特定の構成に限定されず、例えば第1光路P1と光伝送路3との単なる接続箇所等であってもよい。

【0032】

光強度判定部15は、第2パルスレーザ光L2の光強度が所定の範囲内にあるか否かを判定する。ここで、所定の範囲とは、光分岐部12において当該第2パルスレーザ光L2に対し所定の光強度比となるように分岐された第1パルスレーザ光L1が、アッテネータ13によって更に減衰させられた場合に、当該第1パルスレーザ光L1の光子数が複数の候補値に対する所定の誤差範囲となるような範囲である。一例として、光強度判定部15は、第2パルスレーザ光L2の光強度が275μW以上300μW以下の範囲内にある場合に、第1パルスレーザ光L1の光子数が候補値0.5光子に対して5%の誤差範囲内であると判定する。一方、第2パルスレーザ光L2の光強度が所定の範囲内でない場合、当該第2パルスレーザ光L2に対応する第1パルスレーザ光L1のアッテネータ13よりも後段における光子数が、複数の候補値に対する所定の誤差範囲にないこととなる。

20

30

【0033】

ここで、複数の候補値に対する所定の誤差範囲について説明する。図2は、量子暗号鍵を構成するパルスレーザ光の実際の光子数の分布を示すグラフである。図2の横軸は、平均光子数の候補値に対する実際の光子数のばらつきを示しており、図2の縦軸は、実際の光子数毎の確率密度を示している。図2においては、量子暗号鍵を構成するパルスレーザ光の実際の光子数が略正規分布となる例が示されている。図中の線B1は、平均光子数の候補値に対して、光子数が少ない側に誤差が5%となる閾値を示している。また、図中の線B2は、平均光子数の候補値に対して、光子数が多い側に誤差が5%となる閾値を示している。図2に示すように、量子暗号鍵を構成するパルスレーザ光の実際の光子数には、5%以上の誤差が含まれている。

40

【0034】

図3は、パルスレーザ光の実際の光子数の誤差に応じた暗号鍵の生成率の一例を伝送距離との関係で示すシミュレーション結果のグラフである。図3の横軸は、暗号鍵情報の伝送距離を示しており、図3の縦軸は、1つのパルスレーザ光Lが量子暗号鍵出力装置1から量子暗号鍵入力装置2に伝送された場合に、安全性の保証された暗号鍵を生成可能なビット数（パルスあたりの鍵生成率）を示す。図3のグラフG1は、パルスレーザ光Lの実際の光子数の誤差を0%とした場合のシミュレーション結果を示している。図3のグラフG2は、パルスレーザ光Lの実際の光子数の誤差を5%とした場合のシミュレーション結果を示している。図3のグラフG3は、パルスレーザ光Lの実際の光子数の誤差を10%とした場合のシミュレーション結果を示している。グラフG1、G2を比較すると、例え

50

ば伝送距離が120 km程度以下の範囲では、誤差が5%であれば、誤差が0%の場合と比較して、暗号鍵の生成率は50%程度までにしか低下せず、また、最大伝送距離も150 km程度から130 km程度までにしか短縮しないことが分かる。一方、グラフG1, G3を比較すると、誤差が10%となると、誤差が0%の場合と比較して、暗号鍵の生成率が大幅に低下し、また、最大伝送距離も20 km程度まで大幅に短縮してしまうことが分かる。以上により、量子暗号鍵を構成するパルスレーザ光Lにおいて、実際の光子数の候補値に対する実際の光子数の誤差範囲は、5%以下であることが好ましいといえる。

【0035】

図1に戻り、光強度判定部15は、フォトダイオード(光電変換部)23と、コンパレータ(比較部)24と、を有する。フォトダイオード23は、第2パルスレーザ光L2を
10
入力し、入力された第2パルスレーザ光L2の光強度に応じた電気信号をコンパレータ24に出力する。フォトダイオード23としては、特に応答性に優れた高速フォトダイオードを用いることが好ましい。

【0036】

コンパレータ24は、フォトダイオード23によって出力された電気信号に基づいて、当該電気信号に係る第2パルスレーザ光L2の光強度が所定の範囲内にあるか否かを判定する。コンパレータ24は、第2パルスレーザ光L2の光強度が所定の範囲内
20
にない場合、半導体レーザ装置10によって繰り返し生成されるパルスレーザ光Lに係る第1パルスレーザ光L1のうち、光強度が所定の範囲内
にない
と判定された第2パルスレーザ光L2に対応する第1パルスレーザ光L1の順番に関する情報を含む情報である特定情報を情報出力部16に出力する。特定情報は、例えば、複数の第1パルスレーザ光L1のうち、光強度が所定の範囲内
にない
と判定された第2パルスレーザ光L2に対応する第1パルスレーザ光L1の位置に関する情報である。コンパレータ24としては、公知の比較器を適用可能であり、特定の構成に限定されない。

【0037】

情報出力部16は、特定情報を記憶するメモリ25と、メモリ25に記憶されている特定情報を量子暗号鍵入力装置2に出力する特定情報出力部26と、を備える。メモリ25は、特定情報を一時的に記憶可能であれば、特定の構成に限定されない。特定情報出力部26は、メモリ25から特定情報を引き出すと共に、メモリ25から引き出した特定情報を、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鍵入力装置2に伝送する
30
。特定情報出力部26は、特定の構成に限定されず、公知の装置を採用することができる。

【0038】

続いて、量子暗号鍵入力装置2について説明する。量子暗号鍵入力装置2は、光入力部30と、デコーダ31と、光子検出部32と、情報入力部33と、鍵蒸留部34と、を備える。

【0039】

光入力部30は、光出力部14によって出力された第1パルスレーザ光L1を入力する。光入力部30は、入力した第1パルスレーザ光L1をデコーダ31に出力する。デコーダ31は、入力された第1パルスレーザ光L1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32の各ポートに振り分ける。光子検出部32は、デコーダ31から入力されたパルスレーザ光に基づいて、0又は1の2値化された各ビットを生成する。なお、本実施形態において、「暗号鍵」とは、デジタルのビット列によって構成される鍵を意味している。
40

【0040】

情報入力部33は、情報出力部16の特定情報出力部26によって出力された特定情報を入力する。鍵蒸留部34は、光入力部30によって入力された第1パルスレーザ光L1から、情報入力部33によって入力された特定情報によって特定される第1パルスレーザ光L1を除外して、新たな暗号鍵とする(パルス除外処理)。また、鍵蒸留部34は、新たな暗号鍵に基づいて鍵蒸留処理を行う。光入力部30、デコーダ31、光子検出部32
50

、及び、情報入力部 33 は、特定の構成に限定されず、それぞれ公知の装置を採用することができる。

【0041】

量子暗号鍵通信システム 100 は、以下に説明するパルス除外処理を実行する。図 4 は、暗号鍵に対するパルス除外処理を示すフローチャートである。まず、ステップ S1 では、パルスレーザ光 L が半導体レーザ装置 10 によって繰り返し生成される（発光工程）。

【0042】

次に、ステップ S2 では、パルスレーザ光 L がエンコーダ 11 によって符号化され、暗号鍵情報を持ったパルスレーザ光 L が生成される（符号化工程）。次に、ステップ S3 では、符号化されたパルスレーザ光 L が、光分岐部 12 によって、第 1 光路 P1 及び第 2 光路 P2 に所定の光強度比となるように分岐させられる（光分岐工程）。

10

【0043】

次に、ステップ S4 では、第 1 パルスレーザ光 L1 の光子数が 1 以下の値である上述した複数の候補値のうちの何れかとなるように、第 1 パルスレーザ光 L1 の光強度がアッテナータ 13 によって減衰させられる（減衰工程）。次に、ステップ S5 では、光強度を減衰させられた第 1 パルスレーザ光 L1 が、光出力部 14 によって量子暗号鍵入力装置 2 に出力される（光出力工程）。

【0044】

次に、ステップ S6 では、第 2 パルスレーザ光 L2 の光強度が所定の範囲内にあるかが、光強度判定部 15 によって判定される（光強度判定工程）。第 2 パルスレーザ光 L2 の光強度が所定の範囲内ないと判定された場合、処理はステップ S7 に移行する。一方、第 2 パルスレーザ光 L2 の光強度が所定の範囲内にあると判定された場合、処理はステップ S10 に移行する。

20

【0045】

次に、ステップ S7 では、光強度が所定の範囲内ないと判定された第 2 パルスレーザ光 L2 に対応する第 1 パルスレーザ光 L1 を特定する特定情報が、情報出力部 16 によって取得される。続いて、ステップ S8 では、取得された特定情報が、情報出力部 16 によって量子暗号鍵入力装置 2 に出力される（情報出力工程）。以上が、量子暗号鍵出力装置 1 によって量子暗号鍵を生成し、当該量子暗号鍵を量子暗号鍵入力装置 2 に出力する量子暗号鍵出力方法である。

30

【0046】

引き続いて、ステップ S9 では、鍵蒸留部 34 によって、光入力工程にて入力された第 1 パルスレーザ光 L1 から、情報入力工程にて入力された特定情報により特定される第 1 パルスレーザ光 L1 が除外される。続いて、ステップ S10 では、この第 1 パルスレーザ光 L1 の符号化に用いられた量子暗号鍵に係る暗号鍵が、鍵蒸留部 34 によって、新たな暗号鍵として採用される。以上により、量子暗号鍵通信システム 100 におけるパルス除外処理が終了する。

【0047】

続いて、量子暗号鍵通信システム 100 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。量子暗号鍵出力装置 1 は、上述したパルス除外処理におけるステップ S1 ~ S5 によって、暗号鍵の元となるビット列を量子暗号鍵入力装置 2 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 L の一部のみが量子暗号鍵入力装置 2 に到達する。このため、量子暗号鍵入力装置 2 では、エンコーダ 11 において生成されたビット列の一部のみが再構築される。その後、量子暗号鍵入力装置 2 は、パルスレーザ光 L を検出した光子検出部 32 のポート（位置）を量子暗号鍵出力装置 1 に通知する。そして、量子暗号鍵入力装置 2 において再構築されたビット列が生鍵（暗号鍵）とされる。

40

【0048】

続いて、量子暗号鍵出力装置 1 は、基底照合を実行する。すなわち、量子暗号鍵出力装置 1 は、量子暗号鍵出力装置 1 において使用された基底（送信基底）と、量子暗号鍵入力装置 2 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

50

いに異なるビットを生鍵から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。

【 0 0 4 9 】

続いて、量子暗号鍵入力装置 2 は、シフト鍵の一部を量子暗号鍵出力装置 1 に対して公開する。量子暗号鍵出力装置 1 は、公開されたシフト鍵に基づいて、量子暗号鍵出力装置 1 が送信したビットに対して量子暗号鍵入力装置 2 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。

【 0 0 5 0 】

続いて、量子暗号鍵出力装置 1 及び量子暗号鍵入力装置 2 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。

10

【 0 0 5 1 】

続いて、量子暗号鍵出力装置 1 及び量子暗号鍵入力装置 2 は、秘匿性増強を実行する。まず、量子暗号鍵出力装置 1 及び量子暗号鍵入力装置 2 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、量子暗号鍵出力装置 1 及び量子暗号鍵入力装置 2 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。

【 0 0 5 2 】

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、乱数列生成部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。

20

【 0 0 5 3 】

以上のようにして取得された最終鍵を用いて、量子暗号鍵入力装置 2 は、暗号化されたメッセージを復号する。

【 0 0 5 4 】

以上説明したように、量子暗号鍵出力装置 1、量子暗号鍵通信システム 100 或いは量子暗号鍵出力方法の何れかでは、半導体レーザ装置 10 によって繰り返し生成されたパルスレーザ光 L を量子暗号鍵に基づいてエンコーダ 11 によって符号化し、当該パルスレーザ光 L を光分岐部 12 によって第 1 光路 P1 及び第 2 光路 P2 に所定の光強度比となるように分岐させる。そして、第 1 光路 P1 に分岐されたパルスレーザ光 L である第 1 パルスレーザ光 L1 の光強度をアッテネータ 13 によって減衰させて、当該第 1 パルスレーザ光 L1 からなる光パルス列を光出力部 14 によって量子暗号鍵入力装置 2 に出力する。ここで、光強度判定部 15 によって、第 2 光路 P2 に分岐されたパルスレーザ光 L である第 2 パルスレーザ光 L2 の光強度が所定の範囲内ないと判定された場合、情報出力部 16 によって、当該第 2 パルスレーザ光 L2 に対応する第 1 パルスレーザ光 L1 を特定する特定情報が量子暗号鍵入力装置 2 に出力される。第 1 パルスレーザ光 L1 と第 2 パルスレーザ光 L2 とは、同一のパルスレーザ光 L が光分岐部 12 によって所定の光強度比となるように分岐されたものであるため、第 2 パルスレーザ光 L2 の光強度が所定の範囲内ないと判定された場合、当該第 2 パルスレーザ光 L2 に対応する第 1 パルスレーザ光 L1 の平均光子数の誤差が所定値よりも大きいと判定することができる。従って、第 1 パルスレーザ光 L1 からなる光パルス列及び特定情報を入力した量子暗号鍵入力装置 2 は、量子暗号鍵の生成に際し、誤差が所定値よりも大きい第 1 パルスレーザ光 L1 を特定情報により特定して除外することが可能となる。よって、量子暗号鍵の生成率を向上させることができる。

30

40

【 0 0 5 5 】

また、量子暗号鍵出力装置 1 では、光強度判定部 15 は、第 2 パルスレーザ光 L2 を入力し、入力された第 2 パルスレーザ光 L2 の光強度に応じた電気信号を出力するフォトダイオード 23 と、フォトダイオード 23 によって出力された電気信号に基づいて、当該電

50

気信号に係る第2パルスレーザ光L2の光強度が所定の範囲内にあるか否かを判定するコンパレータ24と、を有している。このため、上記作用効果を好適に奏することができる。

【0056】

また、量子暗号鍵出力装置1では、特定情報は、半導体レーザ装置10によって繰り返し生成されるパルスレーザ光Lに係る第1パルスレーザ光L1のうち、光強度判定部15によって光強度が所定の範囲内ないと判定された第2パルスレーザ光L2に対応する第1パルスレーザ光L1の順番に関する情報を含んでいる。このため、第2パルスレーザ光L2のうち、光強度判定部15によって光強度が所定の範囲内ないと判定される第2パルスレーザ光L2の割合が、光強度判定部15によって光強度が所定の範囲内にあると判定される第2パルスレーザ光L2の割合よりも小さいとき、特定情報の情報量を低減させることができる。

10

【0057】

また、量子暗号鍵出力装置1では、エンコーダ11は、パルスレーザ光Lを互いに干渉性を有する一対のパルスに分割する干渉計20と、パルスレーザ光Lの位相を変調する位相変調部21と、パルスレーザ光Lの光強度を変調する強度変調部22と、を有し、パルスレーザ光Lを、干渉計20によって一対のパルスに分割すると共に、位相変調部21によって当該パルスレーザ光Lの位相を変調し、且つ、強度変調部22によって当該パルスレーザ光Lの光強度を変調することによって、当該パルスレーザ光Lを符号化する。このため、time-binエンコーディングの方式を採用して、上記作用効果を好適に奏することができる。

20

【0058】

また、量子暗号鍵出力装置1では、位相変調部21は、干渉計20よりも後段に配置されている。このため、上記作用効果を好適に奏することができる。

【0059】

以上の実施形態は、本発明に係る量子暗号鍵出力装置、量子暗号鍵通信システム及び量子暗号鍵出力方法の一実施形態について説明したものである。従って、本発明に係る量子暗号鍵出力装置、量子暗号鍵通信システム及び量子暗号鍵出力方法は、上記の量子暗号鍵出力装置1、量子暗号鍵通信システム100及び量子暗号鍵出力方法に限定されず、各請求項の要旨を変更しない範囲においてそれらを任意に変形したものとすることが可能である。

30

【0060】

例えば、特定情報は、半導体レーザ装置10によって繰り返し生成されるパルスレーザ光Lに係る第1パルスレーザ光L1のうち、光強度判定部15によって光強度が所定の範囲内にあると判定された第2パルスレーザ光L2に対応する第1パルスレーザ光L1の順番に関する情報を含んでいてもよい。この場合、第2パルスレーザ光L2のうち、光強度判定部15によって光強度が所定の範囲内ないと判定される第2パルスレーザ光L2の割合が、光強度判定部15によって光強度が所定の範囲内にあると判定される第2パルスレーザ光L2の割合よりも大きいとき、特定情報の情報量を低減させることができる。

【0061】

また、干渉計20、位相変調部21、強度変調部22、光分岐部12、及び、アッテネータ13の順序は、上記実施形態に係る順序に限定されない。より具体的には、これらの順序は、光分岐部12が強度変調部22よりも後段であると共にアッテネータ13よりも前段、且つ、位相変調部21が干渉計20よりも後段であればよく、それ以外の順序については変更可能である。

40

【0062】

また、上記実施形態では、エンコーダ11は、time-binエンコーディングの方式を採用している。しかし、エンコーダ11は、量子暗号鍵に基づいてパルスレーザ光Lを符号化することができる構成であればよく、上述した構成に限定されない。例えば、エンコーダ11は、偏光を用いたエンコーディングの方式を採用した構成であってもよい。

50

【 0 0 6 3 】

また、光伝送路 3 は光ファイバを含んでいなくてもよい。この場合、量子暗号鍵出力装置 1 と量子暗号鍵入力装置 2 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。また、干渉計 1 1 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。

【 0 0 6 4 】

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、乱数列生成部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、量子暗号鍵出力装置 1 及び量子暗号鍵入力装置 2 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、乱数列生成部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を選択を行ってもよい。

10

【 0 0 6 5 】

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 】

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

20

【 数 6 】

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

【 0 0 6 6 】

ここで、本発明の一態様に係る量子暗号鍵生成装置では、光強度判定部は、第 2 パルスレーザ光を入力し、入力された第 2 パルスレーザ光の光強度に応じた電気信号を出力する光電変換部と、光電変換部によって出力された電気信号に基づいて、当該電気信号に係る第 2 パルスレーザ光の光強度が所定の範囲内にあるか否かを判定する比較部と、を有していてもよい。この場合、上記作用効果を好適に奏することができる。

30

【 0 0 6 7 】

本発明の一態様に係る量子暗号鍵生成装置では、特定情報は、光源によって繰り返し生成されるパルスレーザ光に係る第 1 パルスレーザ光のうち、光強度判定部によって光強度が所定の範囲内ないと判定された第 2 パルスレーザ光に対応する第 1 パルスレーザ光の順番に関する情報を含んでいてもよい。この場合、第 2 パルスレーザ光のうち、光強度判定部によって光強度が所定の範囲内ないと判定される第 2 パルスレーザ光の割合が、光強度判定部によって光強度が所定の範囲内にあると判定される第 2 パルスレーザ光の割合よりも小さいとき、特定情報の情報量を低減させることができる。

40

【 0 0 6 8 】

本発明の一態様に係る量子暗号鍵生成装置では、特定情報は、光源によって繰り返し生成されるパルスレーザ光に係る第 1 パルスレーザ光のうち、光強度判定部によって光強度が所定の範囲内にあると判定された第 2 パルスレーザ光に対応する第 1 パルスレーザ光の順番に関する情報を含んでいてもよい。この場合、第 2 パルスレーザ光のうち、光強度判定部によって光強度が所定の範囲内ないと判定される第 2 パルスレーザ光の割合が、光強度判定部によって光強度が所定の範囲内にあると判定される第 2 パルスレーザ光の割合よりも大きいとき、特定情報の情報量を低減させることができる。

【 0 0 6 9 】

本発明の一態様に係る量子暗号鍵生成装置では、エンコーダは、パルスレーザ光を互い

50

に干渉性を有する一対のパルスに分割する干渉計と、パルスレーザー光の位相を変調する位相変調部と、パルスレーザー光の光強度を変調する強度変調部と、を有し、パルスレーザー光を、干渉計によって一対のパルスに分割すると共に、位相変調部によって当該パルスレーザー光の位相を変調し、且つ、強度変調部によって当該パルスレーザー光の光強度を変調することによって、当該パルスレーザー光を符号化してもよい。この場合、time-binエンコーディングの方式を採用して、上記作用効果を好適に奏することができる。

【0070】

本発明の一態様に係る量子暗号鍵生成装置では、位相変調部は、干渉計よりも後段に配置されていてもよい。この場合、上記作用効果を好適に奏することができる。

【産業上の利用可能性】

10

【0071】

量子暗号鍵の生成率を向上させることができる量子暗号鍵出力装置、量子暗号鍵通信システム及び量子暗号鍵出力方法を提供することができる。

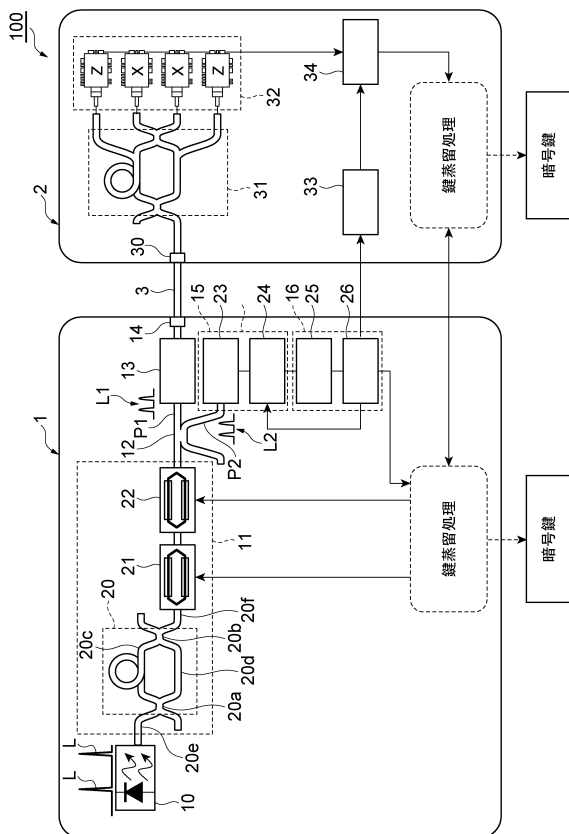
【符号の説明】

【0072】

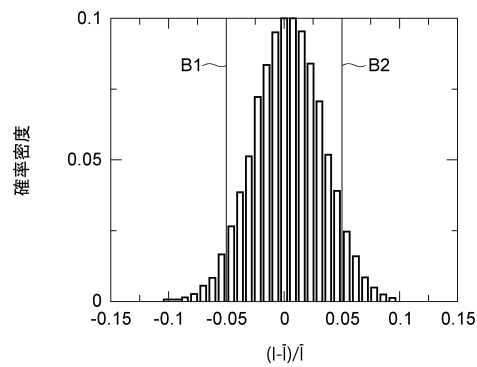
1...量子暗号鍵出力装置、2...量子暗号鍵入力装置、10...半導体レーザー装置(光源)、11...エンコーダ、12...光分岐部、13...アッテネータ(減衰部)、14...光出力部、15...光強度判定部、16...情報出力部、20...干渉計、21...位相変調部、22...強度変調部、23...フォトダイオード(光電変換部)、24...コンパレータ(比較部)、30...光入力部、33...情報入力部、34...鍵蒸留部、100...量子暗号鍵通信システム、L...パルスレーザー光、L1...第1パルスレーザー光、L2...第2パルスレーザー光、P1...第1光路、P2...第2光路。

20

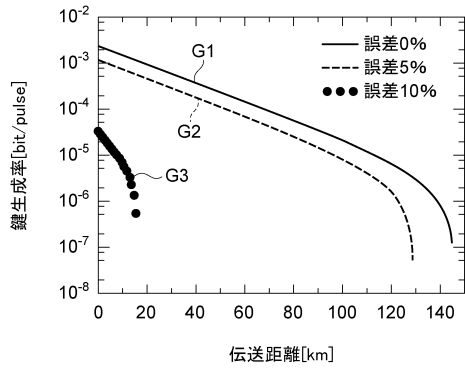
【図1】



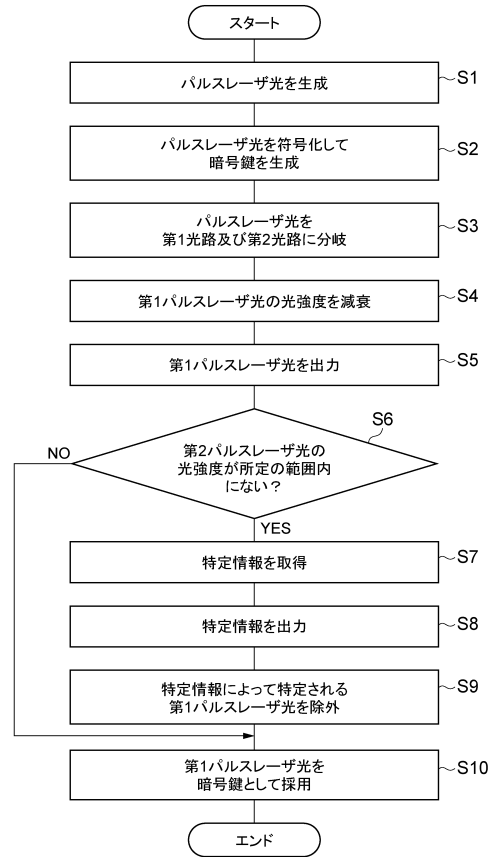
【図2】



【図3】



【図4】



フロントページの続き

早期審査対象出願

審査官 行田 悦資

- (56)参考文献 特表2009-515421(JP,A)
特開2009-194833(JP,A)
国際公開第2008/015758(WO,A1)
富田 章久, 量子暗号鍵配布システムの実際, 電子情報通信学会論文誌 A, 日本, 社団法人電子情報通信学会, 2007年 5月 1日, Vol. J90-A, No. 5, pp. 358-366

(58)調査した分野(Int.Cl., DB名)

H04L 9/12
G02F 1/01
H04B 10/70