(19)日本国特許庁(JP)

再公表特許(A1)

(11)国際公開番号
WO2018/043742

発行日　令和1年6月24日(2019.6.24)

(43)国際公開日　平成30年3月8日(2018.3.8)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/12	(2006.01)	H04L	9/00	631	2K102
H04B 10/70	(2013.01)	H04B	10/70		5J104
G02F 1/01	(2006.01)	G02F	1/01	B	5K102

審査請求 未請求　予備審査請求 未請求　（全 22 頁）

出願番号　特願2018-537587 (P2018-537587)
(21)国際出願番号　PCT/JP2017/031800
(22)国際出願日　平成29年9月4日(2017.9.4)
(31)優先権主張番号　特願2016-173063 (P2016-173063)
(32)優先日　平成28年9月5日(2016.9.5)
(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】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)【要約】
量子暗号鍵出力装置１は、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１１と、パルスレーザ光Ｌを分岐させる光分岐部１２と、第１パルスレーザ光Ｌ１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Ｌ１の光強度を減衰させるアッテネータ１３と、を備える。また、量子暗号鍵出力装置１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光強度判定部１５と、光強度が所定の範囲内にない第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を、量子暗号鍵入力装置２に出力する情報出力部１６と、を備える。

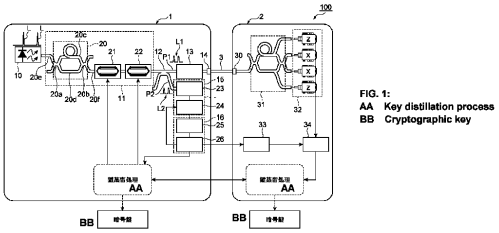


FIG. 1:
AA Key distillation process
BB Cryptographic key

【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に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パルスレーザ光を入力し、入力された前記第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、
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光に係る前記第１パルスレーザ光のうち、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。
【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光に係る前記第１パルスレーザ光のうち、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パルスレーザ光に対応する前記第１パルスレーザ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、
前記パルスレーザ光の位相を変調する位相変調部と、
前記パルスレーザ光の光強度を変調する強度変調部と、を有し、
前記パルスレーザ光を、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光の光強度を変調することによって、当該パルスレーザ光を符号化する、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、
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、
前記パルスレーザ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工程と、
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工程と、
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工程と、
光強度が前記所定の範囲内に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。
【０００７】
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】
【０００８】
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に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。
【０００９】
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。

【００１０】

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に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。

【００１１】

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に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に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。

【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。

【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】

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。

【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。

【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１．５５μｍ）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。

【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（一対のパルス）に分割する。干渉計２０は、非対称マッ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。

【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。

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

【数１】

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

【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。

【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】

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

【００２６】

以上のように、位相変調部２１は、パルスレーザ光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】

半導体レーザ装置１０はパルスレーザ光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】

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: $LiNbO_3$）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光Ｌ）を光分岐部１２に出力する。

【００２９】

光分岐部１２は、符号化されたパルスレーザ光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光Ｌである第１パルスレーザ光Ｌ１と、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との光強度比が例えば１：９となるように、パルスレーザ光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。

【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％の誤差範囲内にあると判定する。一方、第２パルスレーザ光Ｌ２の光強度が所定の範囲内にない場合、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。

【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。

【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、例えば伝送距離が１２０ｋｍ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１５０ｋｍ程度から１３０ｋｍ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２０ｋｍ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にないと判定した場合、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

。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。

【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、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）。

【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の光強度がアッテネータ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否かが、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に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。

【００４５】

次に、ステップＳ７では、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。

【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。

【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。

【００４９】
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。

【００５０】
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。

【００５１】
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。

【００５２】
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。

【００５３】
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。

【００５４】
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に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に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。

【００５５】

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に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。

【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。

【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。

【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に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。

【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。

【００６３】

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１１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。

【００６４】

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の選択を行ってもよい。

【００６５】

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】

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

【００６６】

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。

【００６７】

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に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。

【００６８】

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に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。

【００６９】

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、パルスレーザ光の位相を変調する位相変調部と、パルスレーザ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光の光強度を変調することによって、当該パルスレーザ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】

【００７１】

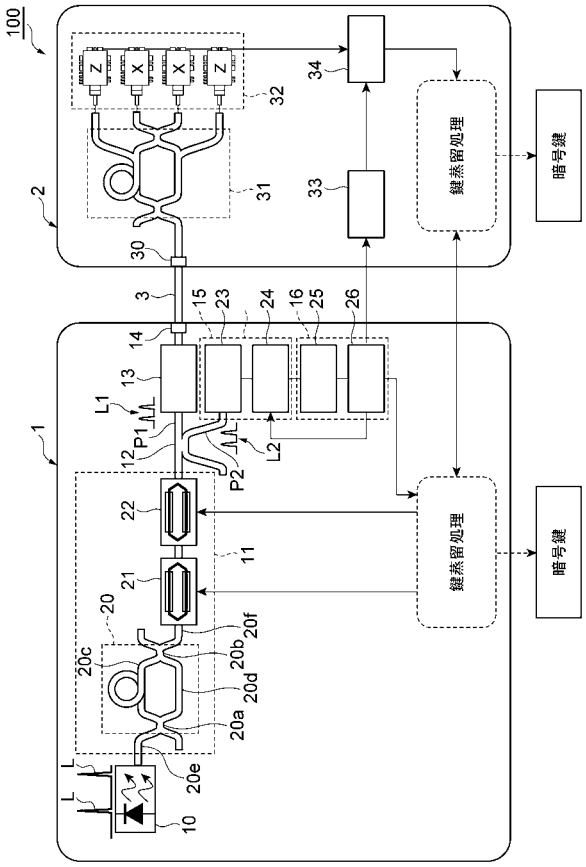
量子暗号鍵の生成率を向上させることができる量子暗号鍵出力装置、量子暗号鍵通信システム及び量子暗号鍵出力方法を提供することができる。

【符号の説明】

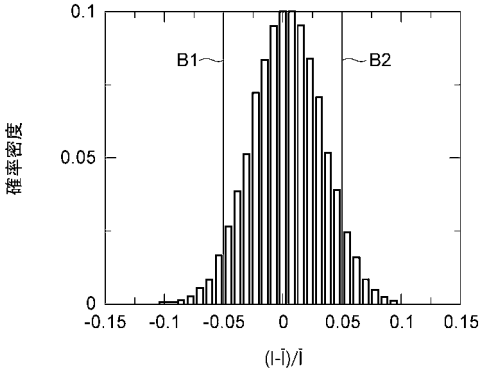
【００７２】

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…パルスレーザ光、Ｌ１…第１パルスレーザ光、Ｌ２…第２パルスレーザ光、Ｐ１…第１光路、Ｐ２…第２光路。

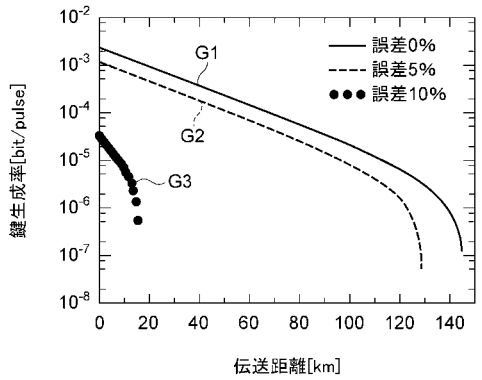
【図１】


100
2
1
3
Z
X
X
Z
32
34
31
33
30
鍵蒸留処理
暗号鍵
15
23
24
16
25
26
14
13
L1
P1
12
L2
P2
22
11
21
20
20f
20b
20c
20d
20a
20e
L
10

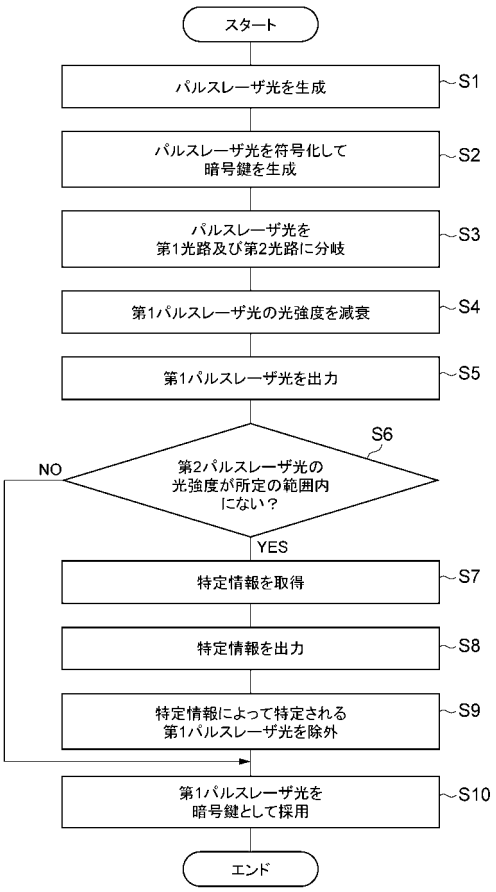
【図２】


0.1
0.05
0
確率密度
B1
B2
-0.15
-0.1
-0.05
0
0.05
0.1
0.15
(I-Ī)/Ī

【図３】


鍵生成率[bit/pulse]
伝送距離[km]
G1
G2
G3
誤差0%
誤差5%
誤差10%
0
20
40
60
80
100
120
140

【図４】


スタート
パルスレーザ光を生成
S1
パルスレーザ光を符号化して
暗号鍵を生成
S2
パルスレーザ光を
第1光路及び第2光路に分岐
S3
第1パルスレーザ光の光強度を減衰
S4
第1パルスレーザ光を出力
S5
S6
第2パルスレーザ光の
光強度が所定の範囲内
にない？
NO
YES
特定情報を取得
S7
特定情報を出力
S8
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
S9
第1パルスレーザ光を
暗号鍵として採用
S10
エンド

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/031800

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/12(2006.01)i, *G02F1/035*(2006.01)i, *G02F1/21*(2006.01)i, *H04B10/70*(2013.01)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)
H04L9/12, G02F1/035, G02F1/21, H04B10/70

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2017
Kokai Jitsuyo Shinan Koho 1971-2017 Toroku Jitsuyo Shinan Koho 1994-2017

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	WO 2008/015758 A1 (Mitsubishi Electric Corp.), 07 February 2008 (07.02.2008), paragraphs [0027] to [0064]; fig. 1 to 6 & US 2010/0226659 A1 paragraphs [0064] to [0101]; fig. 1 to 6 & EP 2051411 A1	1-8
A	JP 2009-515421 A (The Board of Trustees of the Leland Stanford Junior University), 09 April 2009 (09.04.2009), paragraphs [0032], [0035]; fig. 3 & US 2010/0034390 A1 paragraphs [0030], [0033]; fig. 3 & WO 2007/055683 A2	1-8

☒ Further documents are listed in the continuation of Box C. ☐ 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	Date of mailing of the international search report
02 November 2017 (02.11.17)	14 November 2017 (14.11.17)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/031800

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2009-194833 A (NEC Corp.), 27 August 2009 (27.08.2009), paragraphs [0037] to [0038]; fig. 2 (Family: none)	1-8
A	Akihisa TOMITA, "Implementation of Quantum Key Distribution Systems", The Transactions of the Institute of Electronics, Information and Communication Engineers A, 01 May 2007 (01.05.2007), vol.J90-A, no.5, pages 358 to 366	1-8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/031800

Object to be covered by this search:
The "encoder for encoding the pulse laser light on the basis of said quantum cryptographic key", comprised by "a quantum cryptographic key output apparatus that generates an encoded pulse laser light to be used for the generation of a quantum cryptographic key and that outputs an optical pulse sequence consisting of the pulse laser light to a quantum cryptographic key input apparatus" recited in claim 1, and the "process of encoding the pulse laser light on the basis of said quantum cryptographic key", comprised by "a quantum cryptographic key output method that generates an encoded pulse laser light to be used for the generation of a quantum cryptographic key and that outputs an optical pulse sequence consisting of the pulse laser light to a quantum cryptographic key input apparatus" recited in claim 8, each use "said quantum cryptographic key" so as to generate the "quantum cryptographic key", and hence the search has been done by reading "said quantum cryptographic key" as "a random number".

国際調査報告	国際出願番号 PCT／JP2017／031800

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04L9/12(2006.01)i, G02F1/035(2006.01)i, G02F1/21(2006.01)i, H04B10/70(2013.01)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. H04L9/12, G02F1/035, G02F1/21, H04B10/70

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	WO 2008/015758 A1（三菱電機株式会社）2008.02.07, 段落［0027］－［0064］、［図1］－［図6］ & US 2010/0226659 A1,段落［0064］－［0101］、Fig. 1－6 & EP 2051411 A1	1－8
A	JP 2009-515421 A（サ・ボード・オブ・トラスティーズ・オブ・ザ・レランド・スタンフォード・ジュニア・ユニバーシティ）2009.04.09, 段落［0032］、［0035］、［図3］ & US 2010/0034390 A1, ［0030］、［0033］、Fig. 3 & WO 2007/055683 A2	1－8

☑ C欄の続きにも文献が列挙されている。　☐ 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の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
02. 11. 2017	14. 11. 2017

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5S	4229
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	青木 重徳 電話番号 03－3581－1101 内線 3546		

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２０１７／０３１８００

Ｃ（続き）． 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 2009-194833 A（日本電気株式会社）2009.08.27, 段落［００３７］－［００３８］、［図２］（ファミリーなし）	１－８
Ａ	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，2007.05.01，Ｖｏｌ．Ｊ９０－Ａ，Ｎｏ．５， ｐｐ．３５８－３６６	１－８

様式ＰＣＴ／ＩＳＡ／２１０（第２ページの続き）（２０１５年１月）

＜調査の対象について＞

請求項１に記載された、「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」が備える「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」や、請求項８に記載された、「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」が備える「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工程」は、それぞれ「量子暗号鍵」の生成に「前記量子暗号鍵」を用いているため、「前記量子暗号鍵」を「乱数」と読み替えて調査を行った。

フロントページの続き

(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,JO,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

（出願人による申告）平成２３年度　国立研究開発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 AA21 BA02 BA14 BB01 BB04 BB10 BC04 BD04 DA04 DB04
DC07 DD05 EA21 EB20 EB22
5J104 AA05 AA16 EA04 EA16 NA02 NA37
5K102 AA61 AB11 AH02 AH26 AH27 AH29 PB20 PH02 PH31 PH42
RD02

（注）この公表は、国際事務局（ＷＩＰＯ）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。