(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6400513号
(P6400513)
(45)発行日　平成30年10月3日(2018.10.3)　(24)登録日　平成30年9月14日(2018.9.14)

(51)Int.Cl.　F I
H04L 9/12 (2006.01)　H04L 9/00 631

請求項の数 11 (全 26 頁)

(21)出願番号　特願2015-55322(P2015-55322)
(22)出願日　平成27年3月18日(2015.3.18)
(65)公開番号　特開2016-178381(P2016-178381A)
(43)公開日　平成28年10月6日(2016.10.6)
審査請求日　平成29年11月22日(2017.11.22)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　村上　明
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　谷澤　佳道
東京都港区芝浦一丁目１番１号　株式会社東芝内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】量子鍵配送装置、量子鍵配送方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
光子に対する量子通信路を介した量子鍵配送によって、他の量子鍵配送装置と光子列を共有する光子共有処理を実行し、生成した基底情報に基づいて前記光子列に対応した光子ビット列を取得する量子鍵共有手段と、
前記光子ビット列から、前記量子鍵共有手段および前記他の量子鍵配送装置の基底情報に基づいたシフティング処理によって共有ビット列を生成するシフティング手段と、
前記共有ビット列に含まれる誤りを誤り訂正処理により訂正することによって訂正後ビット列を生成する訂正手段と、
前記誤りの数に基づいて、前記訂正後ビット列を圧縮する秘匿性増強処理によって暗号鍵を生成する秘匿性増強手段と、
前記光子共有処理、前記シフティング処理、前記誤り訂正処理、および前記秘匿性増強処理の各処理の実行段階で、前記各処理のうち実行されている処理で出力される出力値、および、前記各処理のうち実行されていない処理の出力値に対応する所定値に基づいて、単位時間あたりの前記暗号鍵の生成量を示す暗号鍵生成速度を推定する推定手段と、
を備えた量子鍵配送装置。
【請求項２】
前記量子鍵共有手段は、前記光子共有処理の実行によって、共有した前記光子列の光子数を前記出力値として出力し、
前記訂正手段は、前記誤り訂正処理の実行によって、前記誤りの数から前記量子通信路

での誤り率を算出し、前記誤り率を前記出力値として出力し、
前記秘匿性増強手段は、前記秘匿性増強処理の実行によって、前記光子列に基づいて前記暗号鍵が生成されるまでの処理時間を前記出力値として出力する請求項１に記載の量子鍵配送装置。
【請求項３】
前記シフティング手段は、前記シフティング処理の実行によって生成した前記共有ビット列の一部のビット情報に基づいて、前記量子通信路での仮誤り率を算出し、前記仮誤り率を前記出力値として出力する請求項２に記載の量子鍵配送装置。
【請求項４】
前記推定手段により推定された前記暗号鍵生成速度の推定値に関する情報を表示する表示手段を、さらに備えた請求項１に記載の量子鍵配送装置。
【請求項５】
前記推定手段により推定された前記暗号鍵生成速度の推定値と、前記各処理がすべて実行されていない場合の該各処理に対応する前記所定値に基づいて求まる前記暗号鍵生成速度の値との差分に基づいて、前記各処理のうち前記推定手段により前記推定値が推定された際に実行されている処理であり、かつ、後段側の処理の動作の調整を行う制御手段を、さらに備えた請求項１に記載の量子鍵配送装置。
【請求項６】
操作入力を受け付ける入力手段と、
前記推定手段により推定された前記推定値に関する情報を表示する表示手段と、
をさらに備え、
前記制御手段は、前記表示手段に表示された前記推定値に関する情報に基づいて前記入力手段により受け付けられた操作入力に従って、前記調整を行う請求項５に記載の量子鍵配送装置。
【請求項７】
前記所定値は、対応する前記出力値のうち過去の出力値に基づいて定められた値である請求項１に記載の量子鍵配送装置。
【請求項８】
前記表示手段は、前記推定値に関する情報として、前記推定値の時系列の推移を示す情報を表示する請求項４または６に記載の量子鍵配送装置。
【請求項９】
前記推定値が所定の条件を満たすか否かを判定する判定手段と、
前記判定手段によって前記推定値が前記所定の条件を満たすと判定された場合、その旨を報知する報知手段と、
をさらに備えた請求項６に記載の量子鍵配送装置。
【請求項１０】
光子に対する量子通信路を介した量子鍵配送によって、他の量子鍵配送装置と光子列を共有する光子共有処理を実行し、生成した基底情報に基づいて前記光子列に対応した光子ビット列を取得する量子鍵共有ステップと、
前記光子ビット列から、前記量子鍵共有ステップの基底情報および前記他の量子鍵配送装置の基底情報に基づいたシフティング処理によって共有ビット列を生成するシフティングステップと、
前記共有ビット列に含まれる誤りを誤り訂正処理により訂正することによって訂正後ビット列を生成する訂正ステップと、
前記誤りの数に基づいて、前記訂正後ビット列を圧縮する秘匿性増強処理によって暗号鍵を生成する秘匿性増強ステップと、
前記光子共有処理、前記シフティング処理、前記誤り訂正処理、および前記秘匿性増強処理の各処理の実行段階で、前記各処理のうち実行されている処理で出力される出力値、および、前記各処理のうち実行されていない処理の出力値に対応する所定値に基づいて、単位時間あたりの前記暗号鍵の生成量を示す暗号鍵生成速度を推定する推定ステップと、

を有する量子鍵配送方法。
【請求項１１】
コンピュータを、
光子に対する量子通信路を介した量子鍵配送によって、他の量子鍵配送装置と光子列を共有する光子共有処理を実行し、生成した基底情報に基づいて前記光子列に対応した光子ビット列を取得する量子鍵共有手段と、
前記光子ビット列から、前記量子鍵共有手段および前記他の量子鍵配送装置の基底情報に基づいたシフティング処理によって共有ビット列を生成するシフティング手段と、
前記共有ビット列に含まれる誤りを誤り訂正処理により訂正することによって訂正後ビット列を生成する訂正手段と、
前記誤りの数に基づいて、前記訂正後ビット列を圧縮する秘匿性増強処理によって暗号鍵を生成する秘匿性増強手段と、
前記光子共有処理、前記シフティング処理、前記誤り訂正処理、および前記秘匿性増強処理の各処理の実行段階で、前記各処理のうち実行されている処理で出力される出力値、および、前記各処理のうち実行されていない処理の出力値に対応する所定値に基づいて、単位時間あたりの前記暗号鍵の生成量を示す暗号鍵生成速度を推定する推定手段と、
して機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、量子鍵配送装置、量子鍵配送方法およびプログラムに関する。
【背景技術】
【０００２】
量子鍵配送システムは、送信機、受信機と、それを接続する光ファイバリンクとを含んで構成される。送信機は、光ファイバの通信路である光ファイバリンク（量子通信路）を介して、単一光子の列を受信機に送信する。その後、送信機と受信機が相互に制御情報を交換することによって、送信機と受信機との間で暗号鍵を共有する。この技術は、一般に量子鍵配送（ＱＫＤ：Ｑｕａｎｔｕｍ　Ｋｅｙ　Ｄｉｓｔｒｉｂｕｔｉｏｎ）と呼ばれる技術により実現される。
【０００３】
量子鍵配送により送信機と受信機との間で暗号鍵を共有するためには、送信機および受信機それぞれにおいて鍵蒸留処理を実行する必要がある。鍵蒸留処理は、シフティング処理、誤り訂正処理、および秘匿性増強処理によって構成される。この鍵蒸留処理によって、送信機および受信機は暗号鍵を共有する。共有された暗号鍵は、送信機と受信機との間、または、それぞれの装置に接続されたアプリケーション間で暗号データ通信を行う際に、ワンタイムパッドの鍵として利用される。ワンタイムパッドの暗号鍵による暗号データ通信では、いかなる知識を有する盗聴者によっても解読できないことが情報理論により保証されている。
【０００４】
また、量子鍵配送では、暗号鍵を共有するために利用される光子は、観測されることで物理的な状態が変化するという量子力学の基本原理の一つである不確定性原理を有する。この原理により、送信機が送信した暗号鍵の情報を含む光子を量子通信路上で盗聴者が観測すると、光子の物理的な状態が変化し、光子を受け取った受信機は、盗聴者に光子を観測されたことを知ることができる。その際、光子の物理的な状態の変化は送信機と受信機との間のリンク（量子通信路）の量子ビット誤り率（Ｑｕａｎｔｕｍ　Ｂｉｔ　Ｅｒｒｏｒ　Ｒａｔｅ、ＱＢＥＲ）として現れる。盗聴者が光子を盗聴しようとすると、光子の物理的な状態が変化し、ＱＢＥＲが大きくなるため、受信機および送信機は盗聴者の存在を知ることができる。
【０００５】
また、単位時間あたりに共有される暗号鍵の生成量をセキュアキーレート（暗号鍵生成

速度）という。多くの暗号鍵を利用できる方が、より高速かつ安全な暗号データ通信が可能となるため、セキュアキーレートが高いほど高性能な量子鍵配送システムを実現できる。量子鍵配送システムでは、装置起動時または故障復帰時等でのメインテナンス作業の一環として、セキュアキーレートを向上させるために、送信機および受信機での暗号鍵生成動作のうちの各処理の調整項目を設定する必要がある。このような量子鍵配送システムとして、暗号鍵生成動作のうち、送信機から受信機に量子通信路を介して光子を送信する動作について調整を行うものがある。

【０００６】

しかし、セキュアキーレートの算出に必要な情報は、暗号鍵生成動作における全処理が終了した後でないと正確な値が判明しない。暗号鍵生成動作の途中の段階では、現在の設定内容が最終的に求まるセキュアキーレートにどのような影響を与えるかを即座に判断するのは容易ではない。上述のシステムでは、光子を送信する動作について調整を行うものであるが、暗号鍵生成動作におけるその他の処理における調整項目を設定するものではないので、セキュアキーレートの向上には不十分である。したがって、調整項目をどのように変更するべきかは、過去の調整作業の経験を参考に試行錯誤で行う必要があるため、メインテナンス作業には時間がかかり、システム保守のためのコストが増大するという問題がある。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】特許第４９５７９５２号公報

【発明の概要】

【発明が解決しようとする課題】

【０００８】

本発明は、上記に鑑みてなされたものであって、容易にセキュアキーレートを向上させることができる量子鍵配送装置、量子鍵配送方法およびプログラ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】

【０００９】

実施形態の量子鍵配送装置は、量子鍵共有手段と、シフティング手段と、訂正手段と、秘匿性増強手段と、推定手段と、を備える。量子鍵共有手段は、光子に対する量子通信路を介した量子鍵配送によって、他の量子鍵配送装置と光子列を共有する光子共有処理を実行し、生成した基底情報に基づいて光子列に対応した光子ビット列を取得する。シフティング手段は、光子ビット列から、量子鍵共有手段および他の量子鍵配送装置の基底情報に基づいたシフティング処理によって共有ビット列を生成する。訂正手段は、共有ビット列に含まれる誤りを誤り訂正処理により訂正することによって訂正後ビット列を生成する。秘匿性増強手段は、誤りの数に基づいて、訂正後ビット列を圧縮する秘匿性増強処理によって暗号鍵を生成する。推定手段は、光子共有処理、シフティング処理、誤り訂正処理、および秘匿性増強処理の各処理の実行段階で、各処理のうち実行されている処理で出力される出力値、および、各処理のうち実行されていない処理の出力値に対応する所定値に基づいて、単位時間あたりの暗号鍵の生成量を示す暗号鍵生成速度を推定する。

【図面の簡単な説明】

【００１０】

【図１】図１は、量子鍵配送システムの構成の一例を示す図である。

【図２】図２は、ＱＫＤ装置のハードウェア構成の一例を示す図である。

【図３】図３は、ＱＫＤ装置の機能ブロックの構成の一例を示す図である。

【図４】図４は、ＱＫＤ装置の暗号鍵生成動作の一例を示すシーケンス図である。

【図５】図５は、各処理における推定値を求めるための情報を示す図である。

【図６】図６は、２値エントロピー関数を示す図である。

【図７】図７は、変形例１のＱＫＤ装置の機能ブロックの構成の一例を示す図である。

【図８】図８は、推定値の表示例を示す図である。
【図９】図９は、棒グラフによる推定値の表示例を示す図である。
【図１０】図１０は、推定値の時系列のグラフによる表示例を示す図である。
【図１１】図１１は、推定値の時系列のグラフによる表示例を示す図である。
【図１２】図１２は、変形例２のＱＫＤ装置の機能ブロックの構成の一例を示す図である。
【発明を実施するための形態】
【００１１】
以下に、図面を参照しながら、本発明の実施形態に係る量子鍵配送装置、量子鍵配送方法およびプログラムを詳細に説明する。また、以下の図面において、同一の部分には同一の符号が付してある。ただし、図面は模式的なものであるため、具体的な構成は以下の説明を参酌して判断すべきものである。
【００１２】
（実施形態）
図１は、実施形態の量子鍵配送システムの構成の一例を示す図である。図１を参照しながら、量子鍵配送システム１００の構成について説明する。
【００１３】
図１に示すように、量子鍵配送システム１００は、送信機１と、受信機２と、光ファイバリンク３と、を含んで構成されている。なお、以下においては、図１に示すように、送信機１と受信機２とがそれぞれ１つで構成された量子鍵配送システム１００について説明するが、受信機２が１台で、光学機器を介して複数の送信機１が接続された、いわゆる量子アクセスネットワーク（ＱＡＮ：Ｑｕａｎｔｕｍ　Ａｃｃｅｓｓ　Ｎｅｔｗｏｒｋ）が量子鍵配送システムに統合された構成であってもよい。また、受信機２が複数の光ファイバ通信のインターフェースを有し、それらのインターフェースを介して、複数の送信機１が接続された量子鍵配送システムであってもよい。また、これらのシステムにおいて、送信機１と受信機２とが逆となっている構成でもよい。
【００１４】
送信機１は、レーザにより発生させた、暗号鍵を生成する基となる単一光子から構成される光子列を、光ファイバリンク３を介して、受信機２へ送信する装置である。送信機１は、送信した光子列を基に、後述する鍵蒸留処理（シフティング処理、誤り訂正処理および秘匿性増強処理）等を実行して、暗号鍵を生成する。また、送信機１は、光ファイバリンク３により実現される量子通信路以外の、Ｅｔｈｅｒｎｅｔ（登録商標）ケーブル等の通信ケーブルで実現される古典通信路を介して、受信機２との間でデータ通信を行う。なお、古典通信路を介して通信されるデータとしては、上述の鍵蒸留処理で必要な制御データであってもよく、これ以外の一般的なデータであってもよい。
【００１５】
受信機２は、暗号鍵を生成する基となる単一光子から構成される光子列を、光ファイバリンク３を介して、送信機１から受信する装置である。受信機２は、受信した光子列を基に、後述する鍵蒸留処理（シフティング処理、誤り訂正処理および秘匿性増強処理）等を実行して、送信機１が生成した暗号鍵と同一の暗号鍵を生成する。すなわち、送信機１および受信機２は、同一の暗号鍵を生成して共有することになる。また、受信機２は、光ファイバリンク３により実現される量子通信路以外の、Ｅｔｈｅｒｎｅｔケーブル等の通信ケーブルで実現される古典通信路を介して、送信機１との間でデータ通信を行う。
【００１６】
光ファイバリンク３は、送信機１が出力した単一光子の送信路となる量子通信路として機能する光ファイバケーブルである。なお、図示していないが、送信機１と受信機２とは、光ファイバリンク３の量子通信路以外に、通常の「０」および「１」のデジタルデータを通信する通信ケーブル（古典通信路）で接続されている。また、古典通信路は、有線である必要はなく無線であってもよい。
【００１７】

なお、光ファイバリンク３が量子通信路として機能し、図示しないＥｔｈｅｒｎｅｔケーブル等の通信ケーブルが古典通信路として機能するものとしたが、これに限定されるものではない。例えば、光ファイバリンク３は、ＷＤＭ（Ｗａｖｅｌｅｎｇｔｈ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅｘ：光波長多重化）技術により、光子の送受信をするための光子通信チャネルと、光データ通信を行うための光データ通信チャネルとが形成されるものとしてもよい。すなわち、この場合、光ファイバリンク３の光子通信チャネルが量子通信路として機能し、光データ通信チャネルが古典通信路として機能する。

【００１８】

このような送信機１と受信機２とを含む量子鍵配送システム１００によって、送信機１が送信した光子列を光ファイバリンク３上で盗聴者が観測すると、光子の物理的状態が変化し、光子を受信した受信機２は、盗聴者に光子を観測されたことを認識することができる。

【００１９】

なお、送信機１および受信機２を総称する場合、「ＱＫＤ装置」（量子鍵配送装置）というものとする。

【００２０】

図２は、実施形態に係るＱＫＤ装置のハードウェア構成の一例を示す図である。図２を参照しながら、ＱＫＤ装置（送信機１、受信機２）のハードウェア構成について説明する。

【００２１】

図２に示すように、ＱＫＤ装置は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）８０と、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）８１と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）８２と、入力装置８３と、表示装置８４と、通信Ｉ／Ｆ８５と、補助記憶装置８６と、光学処理装置８７と、スピーカ８８と、を備えている。

【００２２】

ＣＰＵ８０は、ＱＫＤ装置全体の動作を制御する演算装置である。ＲＯＭ８１は、ＣＰＵ８０が各機能を制御するために実行するプログラムを記憶する不揮発性記憶装置である。ＲＡＭ８２は、ＣＰＵ８０のワークメモリ等として機能する揮発性記憶装置である。

【００２３】

入力装置８３は、文字、数字、各種指示の選択、および設定情報の設定等を行うマウスおよびキーボード等の装置である。

【００２４】

表示装置８４は、カーソル、メニュー、ウィンドウ、文字もしくは画像等の各種情報を表示する表示装置である。表示装置８４は、例えば、ＣＲＴ（Ｃａｔｈｏｄｅ Ｒａｙ Ｔｕｂｅ）ディスプレイ、液晶ディスプレイ、プラズマディスプレイまたは有機ＥＬ（Ｅｌｅｃｔｒｏｌｕｍｉｎｅｓｃｅｎｃｅ）ディスプレイ等である。なお、表示装置８４は、例えば、ＱＫＤ装置の本体に対して、ＶＧＡケーブルまたはＨＤＭＩ（登録商標）（Ｈｉｇｈ－Ｄｅｆｉｎｉｔｉｏｎ Ｍｕｌｔｉｍｅｄｉａ Ｉｎｔｅｒｆａｃｅ）ケーブル等によって接続される。

【００２５】

通信Ｉ／Ｆ８５は、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）等のネットワークまたは無線ネットワーク等の古典通信路を介してデータ通信を行うためのインターフェースである。通信Ｉ／Ｆ８５は、例えば、１０Ｂａｓｅ－Ｔ、１００Ｂａｓｅ－ＴＸもしくは１０００Ｂａｓｅ－Ｔ等のＥｔｈｅｒｎｅｔ（登録商標）に対応したインターフェースである。

【００２６】

補助記憶装置８６は、ＣＰＵ８０で実行される各種プログラム、および暗号鍵生成動作の過程で生成したデータ等を記憶して蓄積する不揮発性記憶装置である。補助記憶装置８６は、ＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）、ＳＳＤ（Ｓｏｌｉｄ Ｓｔａｔｅ

Ｄｒｉｖｅ）、フラッシュメモリまたは光ディスク等の電気的、磁気的または光学的に記憶可能な記憶装置である。

【００２７】

光学処理装置８７は、量子通信路を介して、光子列を送信または受信する光学装置である。送信機１の光学処理装置８７は、例えば、乱数によって発生させたビット情報であるビット列（光子ビット列）に対して、ランダムに選択した基底により生成した基底情報に基づく偏光状態となるように生成した単一光子から構成される光子列を、量子通信路（図１に示す光ファイバリンク３）を介して、受信機２の光学処理装置８７に送信する。すなわち、送信機１の光学処理装置８７により発生された光子列の各光子は、「０」か「１」かの１ビットの情報を有する。なお、光子列は、基底情報に基づく偏光状態になるように生成した単一光子から構成されるものとしたが、これに限定されるものではなく、基底情報に基づく位相状態となるように生成した単一光子から構成されるものとしてもよい。受信機２の光学処理装置８７は、量子通信路を介して、送信機１の光学処理装置８７から光子列を受信し、受信した光子列を、ランダムに選択した基底により生成した基底情報に基づいて読み取ることによってビット情報である光子ビット列を得る。

【００２８】

スピーカ８８は、ＣＰＵ８０の指令に従って音声を出力する装置である。

【００２９】

上述のＣＰＵ８０、ＲＯＭ８１、ＲＡＭ８２、入力装置８３、表示装置８４、通信Ｉ／Ｆ８５、補助記憶装置８６、光学処理装置８７、およびスピーカ８８は、アドレスバスおよびデータバス等のバス８９によって互いに通信可能に接続されている。

【００３０】

なお、図２に示したＱＫＤ装置の各装置は、一例を示したものであり、すべてを備えていなければならないわけではない。例えば、情報を表示する必要がなければ、表示装置８４は備えられなくてもよく、音声を出力する必要がなければ、スピーカ８８は備えられなくてもよい。

【００３１】

図３は、実施形態に係るＱＫＤ装置の機能ブロックの構成の一例を示す図である。図３を参照しながら、ＱＫＤ装置（送信機１、受信機２）の機能ブロックの構成について説明する。

【００３２】

図３に示すように、送信機１は、光子送信部１０（量子鍵共有手段）と、シフティング処理部１１（シフティング手段）と、誤り訂正処理部１２（訂正手段）と、秘匿性増強処理部１３（秘匿性増強手段）と、制御部１４（制御手段）と、推定部１５（推定手段）と、入力部１６（入力手段）と、記憶部１７と、を有する。

【００３３】

光子送信部１０は、例えば、乱数によって発生させたビット情報である光子ビット列に対して、ランダムに選択した基底により生成した基底情報に基づく偏光状態となるように生成した単一光子から構成される光子列を、量子通信路を介して、受信機２の光子受信部２０に送信して光子列を光子受信部２０と共有する機能部である。光子送信部１０は、図２に示す光学処理装置８７によって実現される。

【００３４】

シフティング処理部１１は、受信機２の光子受信部２０が生成した基底情報を、受信機２のシフティング処理部２１から古典通信路を介して受信し、受信した基底情報と、光子送信部１０が生成した基底情報とを比較して、一致する部分に対応するビットを光子ビット列から抽出して、共有ビット列を生成するシフティング処理を実行する機能部である。また、シフティング処理部１１は、ＱＢＥＲがどれくらいの値となるかを見積もるために、共有ビット列の一部のビット情報を利用して、仮のＱＢＥＲであるサンプルＱＢＥＲ（仮誤り率の一例）を算出する。なお、ここで説明したシフティング処理は一例であり、これ以外の方法を採用してもよい。

【００３５】
誤り訂正処理部１２は、古典通信路を介して、受信機２の誤り訂正処理部２２と制御データ（ＥＣ（Ｅｒｒｏｒ　Ｃｏｒｒｅｃｔｉｏｎ）情報）を交換することにより、共有ビット列のビット誤りを訂正して訂正後ビット列を生成する誤り訂正処理を実行する機能部である。誤り訂正処理に成功した場合、誤り訂正処理部１２が生成した訂正後ビット列は、後述する受信機２の誤り訂正処理部２２が、共有ビット列を訂正して生成した訂正後ビット列と一致する。また、訂正後ビット列は、共有ビット列のビット誤りを訂正したビット列なので、共有ビット列および訂正後ビット列の長さは同一である。
【００３６】
また、誤り訂正処理部１２は、訂正後ビット列を生成する誤り訂正処理において訂正した誤りのビット数、および訂正後ビット列のビット数に基づいて、ＱＢＥＲを算出する。さらに、誤り訂正処理部１２は、上述のように、共有ビット列のビット誤りを訂正して訂正後ビット列を生成するために、誤り訂正処理部２２と交換したＥＣ情報の情報量に基づいて、漏洩したビット情報の量である情報漏洩量を算出する。この漏洩ビット数が大きいほど、盗聴の可能性が高くなり、また、盗聴された情報量も大きい可能性があることを示す。
【００３７】
秘匿性増強処理部１３は、古典通信路を介して、後述する受信機２の秘匿性増強処理部２３から制御データ（ＰＡ（Ｐｒｉｖａｃｙ　Ａｍｐｌｉｆｉｃａｔｉｏｎ：秘匿性増強）情報）を受信して、このＰＡ情報に基づいて、訂正後ビット列に対して、誤り訂正処理部１２により訂正した誤りの数から、光子送信部１０および誤り訂正処理部１２の処理の際に盗聴者により盗聴された可能性のあるビットを打ち消すための鍵圧縮処理（秘匿性増強処理）を行って暗号鍵を生成する機能部である。秘匿性増強処理に成功した場合、秘匿性増強処理部１３により生成された暗号鍵は、受信機２の秘匿性増強処理部２３により生成された暗号鍵と一致するものであり、同一の暗号鍵を共有することになる。これらの共有された暗号鍵は、送信機１と受信機２との間、または、それぞれの装置に接続されたアプリケーション間で暗号データ通信を行う際に利用される。
【００３８】
制御部１４は、上述の光子送信部１０、シフティング処理部１１、誤り訂正処理部１２、および秘匿性増強処理部１３の動作を制御する機能部である。また、制御部１４は、光子送信部１０、シフティング処理部１１、誤り訂正処理部１２および秘匿性増強処理部１３の各処理で求まる測定値（出力値）を取得し、推定部１５に送る。また、制御部１４は、入力部１６から操作入力された初期値を、予め記憶部１７に記憶させる。ここで、初期値とは、光子送信部１０、シフティング処理部１１、誤り訂正処理部１２、および秘匿性増強処理部１３の各処理で求まる測定値に対応する初期値（所定値の一例）である。初期値としては、例えば、過去に各処理の測定値に基づいて定められた値、または送信機１および受信機２の特定、設置環境およびＱＫＤの方式等から期待される値とすればよい。光子送信部１０の光子列の共有処理（以下、「光子共有処理」という）で出力される測定値は、光子列の光子の数（以下、単に「光子数」という）である。シフティング処理部１１のシフティング処理で出力される測定値は、上述のサンプルＱＢＥＲである。誤り訂正処理部１２の誤り訂正処理で出力される測定値は、上述のＱＢＥＲおよび情報漏洩量である。秘匿性増強処理部１３の秘匿性増強処理で出力される測定値は、１つの暗号鍵が生成されるまでの処理時間、すなわち、光子共有処理から秘匿性増強処理の終了までに必要とする処理時間である。
【００３９】
推定部１５は、セキュアキーレートの推定動作を行う機能部である。具体的には、推定部１５は、送信機１における起動時、光子共有処理時、シフティング処理時、誤り訂正処理時、および秘匿性増強処理時の各タイミングで、取得が可能な測定値、および取得できない測定値に対応する初期値を用いて、セキュアキーレートを推定する。このとき、推定部１５は、セキュアキーレートを推定するために用いる初期値については、予め記憶され

ている記憶部１７から取得する。なお、推定部１５によるセキュアキーレートの推定動作の詳細は、図５で後述する。

【００４０】

入力部１６は、初期値等の操作入力を受け付ける機能部である。入力部１６は、図２に示す入力装置８３によって実現される。

【００４１】

記憶部１７は、入力部１６から操作入力された初期値を記憶する機能部である。記憶部１７は、図２に示す補助記憶装置８６によって実現される。

【００４２】

上述のシフティング処理部１１、誤り訂正処理部１２、秘匿性増強処理部１３、制御部１４、および推定部１５は、図２に示すＣＰＵ８０が補助記憶装置８６等に記憶されたプログラムをＲＡＭ８２に読み出して実行することによって実現される。なお、シフティング処理部１１、誤り訂正処理部１２、秘匿性増強処理部１３、制御部１４、および推定部１５のすべてがプログラムの実行により実現されることに限定されるものではなく、少なくともいずれかが、例えば、ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）、ＦＰＧＡ（Ｆｉｅｌｄ－Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）またはその他の集積回路等のハードウェア回路によって実現されるものとしてもよい。

【００４３】

なお、図３に示す光子送信部１０、シフティング処理部１１、誤り訂正処理部１２、秘匿性増強処理部１３、制御部１４、推定部１５、入力部１６、および記憶部１７は、機能を概念的に示したものであって、このような構成に限定されるものではない。例えば、図３で独立した機能部として図示した複数の機能部を、１つの機能部として構成してもよい。一方、図３の１つの機能部が有する機能を複数に分割し、複数の機能部として構成するものとしてもよい。

【００４４】

図３に示すように、受信機２は、光子受信部２０（量子鍵共有手段）と、シフティング処理部２１（シフティング手段）と、誤り訂正処理部２２（訂正手段）と、秘匿性増強処理部２３（秘匿性増強手段）と、制御部２４（制御手段）と、推定部２５（推定手段）と、入力部２６（入力手段）と、記憶部２７と、を有する。

【００４５】

光子受信部２０は、量子通信路を介して、送信機１の光子送信部１０から光子列を受信して光子列を光子送信部１０と共有し、受信した光子列を、ランダムに選択した基底により生成した基底情報に基づいて読み取ることによってビット情報である光子ビット列を得る機能部である。光子受信部２０は、図２に示す光学処理装置８７によって実現される。

【００４６】

シフティング処理部２１は、送信機１の光子送信部１０が生成した基底情報を、送信機１のシフティング処理部１１から古典通信路を介して受信し、受信した基底情報と、光子受信部２０が生成した基底情報とを比較して、一致する部分に対応するビットを光子ビット列から抽出して、共有ビット列を生成するシフティング処理を実行する機能部である。また、シフティング処理部２１は、ＱＢＥＲがどれくらいの値となるかを見積もるために、共有ビット列の一部のビット情報を利用して、仮のＱＢＥＲであるサンプルＱＢＥＲを算出する。なお、ここで説明したシフティング処理は一例であり、これ以外の方法を採用してもよい。

【００４７】

誤り訂正処理部２２は、古典通信路を介して、送信機１の誤り訂正処理部１２と制御データ（ＥＣ情報）を交換することにより、共有ビット列のビット誤りを訂正して訂正後ビット列を生成する誤り訂正処理を実行する機能部である。誤り訂正処理に成功した場合、誤り訂正処理部２２が生成した訂正後ビット列は、送信機１の誤り訂正処理部１２が、共有ビット列を訂正して生成した訂正後ビット列と一致する。また、訂正後ビット列は、共

有ビット列のビット誤りを訂正したビット列なので、共有ビット列および訂正後ビット列の長さは同一である。

【００４８】

また、誤り訂正処理部２２は、訂正後ビット列を生成する誤り訂正処理において訂正した誤りのビット数、および訂正後ビット列のビット数に基づいて、ＱＢＥＲを算出する。さらに、誤り訂正処理部２２は、上述のように、共有ビット列のビット誤りを訂正して訂正後ビット列を生成するために、誤り訂正処理部１２と交換したＥＣ情報の情報量に基づいて、漏洩したビット情報の量である情報漏洩量を算出する。この漏洩ビット数が大きいほど、盗聴の可能性が高くなり、また、盗聴された情報量も大きい可能性があることを示す。

【００４９】

秘匿性増強処理部２３は、古典通信路を介して、制御データ（ＰＡ情報）を生成して送信機１の秘匿性増強処理部１３に送信し、このＰＡ情報に基づいて、訂正後ビット列に対して、誤り訂正処理部２２により訂正した誤りの数から、光子受信部２０および誤り訂正処理部２２の処理の際に盗聴者により盗聴された可能性のあるビットを打ち消すための鍵圧縮処理（秘匿性増強処理）を行って暗号鍵を生成する機能部である。秘匿性増強処理に成功した場合、秘匿性増強処理部２３により生成された暗号鍵は、送信機１の秘匿性増強処理部１３により生成された暗号鍵と一致するものであり、同一の暗号鍵を共有することになる。これらの共有された暗号鍵は、送信機１と受信機２との間、または、それぞれの装置に接続されたアプリケーション間で暗号データ通信を行う際に利用される。

【００５０】

制御部２４は、上述の光子受信部２０、シフティング処理部２１、誤り訂正処理部２２、および秘匿性増強処理部２３の動作を制御する機能部である。また、制御部２４は、光子受信部２０、シフティング処理部２１、誤り訂正処理部２２および秘匿性増強処理部２３の各処理で求まる測定値を取得し、推定部２５に送る。また、制御部２４は、入力部２６から操作入力された初期値を、予め記憶部２７に記憶させる。ここで、初期値および測定値については、上述の制御部１４の説明した内容に準じる。

【００５１】

推定部２５は、セキュアキーレートの推定動作を行う機能部である。具体的には、推定部２５は、受信機２における起動時、光子共有処理時、シフティング処理時、誤り訂正処理時、および秘匿性増強処理時の各タイミングで、取得が可能な測定値、および取得できない測定値に対応する初期値を用いて、セキュアキーレートを推定する。このとき、推定部２５は、セキュアキーレートを推定するために用いる初期値については、予め記憶されている記憶部２７から取得する。なお、推定部２５によるセキュアキーレートの推定動作の詳細は、図５で後述する。

【００５２】

入力部２６は、初期値等の操作入力を受け付ける機能部である。入力部２６は、図２に示す入力装置８３によって実現される。

【００５３】

記憶部２７は、入力部２６から操作入力された初期値を記憶する機能部である。記憶部２７は、図２に示す補助記憶装置８６によって実現される。

【００５４】

上述のシフティング処理部２１、誤り訂正処理部２２、秘匿性増強処理部２３、制御部２４、および推定部２５は、図２に示すＣＰＵ８０が補助記憶装置８６等に記憶されたプログラムをＲＡＭ８２に読み出して実行することによって実現される。なお、シフティング処理部２１、誤り訂正処理部２２、秘匿性増強処理部２３、制御部２４、および推定部２５のすべてがプログラムの実行により実現されることに限定されるものではなく、少なくともいずれかが、例えば、ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）、ＦＰＧＡ（Ｆｉｅｌｄ－Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）またはその他の集積回路等のハードウェア回路によって実

現されるものとしてもよい。

【００５５】

なお、図３に示す光子受信部２０、シフティング処理部２１、誤り訂正処理部２２、秘匿性増強処理部２３、制御部２４、推定部２５、入力部２６、および記憶部２７は、機能を概念的に示したものであって、このような構成に限定されるものではない。例えば、図３で独立した機能部として図示した複数の機能部を、１つの機能部として構成してもよい。一方、図３の１つの機能部が有する機能を複数に分割し、複数の機能部として構成するものとしてもよい。

【００５６】

図４は、実施形態に係るＱＫＤ装置の暗号鍵生成動作の一例を示すシーケンス図である。図４を参照しながら、暗号鍵生成動作の流れを説明する。

【００５７】

＜ステップＳ１１＞

光子送信部１０は、例えば、乱数によって発生させたビット情報である光子ビット列に対して、ランダムに選択した基底により生成した基底情報に基づく偏光状態となるように生成した単一光子から構成される光子列を、量子通信路を介して、受信機２の光子受信部２０に送信して光子列を光子受信部２０と共有する。光子送信部１０は、生成した基底情報および光子ビット列をシフティング処理部１１に送る。なお、光子送信部１０は、生成した基底情報および光子ビット列を、記憶部１７に記憶させるものとしてもよい。

【００５８】

＜ステップＳ１２＞

光子受信部２０は、量子通信路を介して、送信機１の光子送信部１０から光子列を受信して光子列を光子送信部１０と共有し、受信した光子列を、ランダムに選択した基底により生成した基底情報に基づいて読み取ることによってビット情報である光子ビット列を得る。光子受信部２０は、生成した基底情報および光子ビット列をシフティング処理部２１に送る。なお、光子受信部２０は、生成した基底情報および光子ビット列を、記憶部２７に記憶させるものとしてもよい。

【００５９】

＜ステップＳ１３＞

シフティング処理部１１は、受信機２の光子受信部２０が生成した基底情報を、受信機２のシフティング処理部２１から古典通信路を介して受信し、受信した基底情報と、光子送信部１０が生成した基底情報とを比較して、一致する部分に対応するビットを光子ビット列から抽出して、共有ビット列を生成するシフティング処理を実行する。シフティング処理部１１は、生成した共有ビット列を誤り訂正処理部１２に送る。なお、シフティング処理部１１は、生成した共有ビット列を、記憶部１７に記憶させるものとしてもよい。

【００６０】

＜ステップＳ１４＞

シフティング処理部２１は、送信機１の光子送信部１０が生成した基底情報を、送信機１のシフティング処理部１１から古典通信路を介して受信し、受信した基底情報と、光子受信部２０が生成した基底情報とを比較して、一致する部分に対応するビットを光子ビット列から抽出して、共有ビット列を生成するシフティング処理を実行する。シフティング処理部２１は、生成した共有ビット列を誤り訂正処理部２２に送る。なお、シフティング処理部２１は、生成した共有ビット列を、記憶部２７に記憶させるものとしてもよい。

【００６１】

＜ステップＳ１５＞

誤り訂正処理部１２は、古典通信路を介して、受信機２の誤り訂正処理部２２と制御データ（ＥＣ情報）を交換することにより、シフティング処理部１１により生成された共有ビット列のビット誤りを訂正して訂正後ビット列を生成する誤り訂正処理を実行する。誤り訂正処理部１２は、生成した訂正後ビット列を秘匿性増強処理部１３に送る。なお、誤り訂正処理部１２は、生成した訂正後ビット列を、記憶部１７に記憶させるものとしても

よい。
【００６２】
＜ステップＳ１６＞
誤り訂正処理部２２は、古典通信路を介して、送信機１の誤り訂正処理部１２と制御データ（ＥＣ情報）を交換することにより、シフティング処理部２１により生成された共有ビット列のビット誤りを訂正して訂正後ビット列を生成する誤り訂正処理を実行する。誤り訂正処理部２２は、生成した訂正後ビット列を秘匿性増強処理部２３に送る。なお、誤り訂正処理部２２は、生成した訂正後ビット列を、記憶部２７に記憶させるものとしてもよい。
【００６３】
＜ステップＳ１７＞
秘匿性増強処理部１３は、古典通信路を介して、受信機２の秘匿性増強処理部２３から制御データ（ＰＡ情報）を受信して、このＰＡ情報に基づいて、誤り訂正処理部１２により生成された訂正後ビット列に対して、誤り訂正処理部１２により訂正した誤りの数から、光子送信部１０および誤り訂正処理部１２の処理の際に盗聴者により盗聴された可能性のあるビットを打ち消すための鍵圧縮処理（秘匿性増強処理）を行って暗号鍵を生成する。秘匿性増強処理部１３は、生成した暗号鍵を、記憶部１７に記憶（蓄積）させる。
【００６４】
＜ステップＳ１８＞
秘匿性増強処理部２３は、古典通信路を介して、制御データ（ＰＡ情報）を生成して送信機１の秘匿性増強処理部１３に送信し、このＰＡ情報に基づいて、誤り訂正処理部２２により生成された訂正後ビット列に対して、誤り訂正処理部２２により訂正した誤りの数から、光子受信部２０および誤り訂正処理部２２の処理の際に盗聴者により盗聴された可能性のあるビットを打ち消すための鍵圧縮処理（秘匿性増強処理）を行って暗号鍵を生成する。秘匿性増強処理部２３は、生成した暗号鍵を、記憶部２７に記憶（蓄積）させる。
【００６５】
以上のような動作によって、送信機１および受信機２において、同一の暗号鍵が生成される。上述の動作によって生成された暗号鍵は、一度しか使用しないいわゆるワンタイムパッドの鍵であるので、上述の動作によって、異なる暗号鍵が繰り返し生成される。なお、上述の動作は、ワンタイムパッド方式の暗号鍵の生成に限定されるものではなく、他の方式の暗号鍵、例えば、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）に代表される共通鍵暗号方式の鍵の生成に適用するものとしてもよい。
【００６６】
なお、図３の各機能部が生成したビット列を、次工程の機能部に直接送っているが、記憶部１７および記憶部２７を経由させるものとしてもよい。例えば、シフティング処理部１１は、上述では、生成した共有ビット列を、直接誤り訂正処理部１２に送るものとしている。これに代えて、シフティング処理部１１は、共有ビット列を記憶部１７に記憶させ、誤り訂正処理部１２は、記憶部１７から共有ビット列を読み出して、誤り訂正処理を実行するものとしてもよい。
【００６７】
図５は、各処理における推定値を求めるための情報を示す図である。図６は、２値エントロピー関数を示す図である。図５および６を参照しながら、セキュアキーレートの推定動作、および、暗号鍵生成動作での各処理の調整をする動作について説明する。
【００６８】
図５に示すように、暗号鍵生成動作は、（１）装置起動、（２）光子共有処理、（３）シフティング処理、（４）誤り訂正処理、（５）秘匿性増強処理、の順で実行される。（２）～（５）の各処理の動作内容の概要は、図４で上述した通りである。
【００６９】
秘匿性増強処理部１３、２３で生成される暗号鍵の長さは、光子送信部１０および光子受信部２０の光子共有処理で共有された光子列の光子数、ならびに、誤り訂正処理部１２

、２２の誤り訂正処理で算出されるＱＢＥＲおよび情報漏洩量に基づいて算出できる。ここで、例えば、情報理論によって暗号通信の安全性を証明している暗号鍵の長さＲ$_{secure}$は、下記の（式１）によって表される。

【数１】

$$R_{secure}=\frac{1}{2}Q\left\{1-\left(1+f_{EC}(E)\right)*H_2(E)\right\} \quad \cdots(式1)$$

$$\left(\begin{array}{l} R_{secure}:暗号鍵の長さ \\ E:QBER(量子通信路での誤り率) \\ Q:共有した光子数 \\ \frac{1}{2}:共有した光子数の中、シフティング処理で残る割合 \\ f_{EC}(E):EC効率 \\ H_2(E):2値エントロピー関数 \end{array}\right)$$

【００７０】

（式１）のＥＣ効率ｆ$_{EC}$とは、あるビット列の誤り訂正を行うためにどの程度の情報量が盗聴者に漏れるかの割合であり、ＱＢＥＲおよび情報漏洩量に依存する値である。また、Ｈ$_2$（Ｅ）は、図６に示すようなエラー率Ｅの関数である２値エントロピー関数である。このように、暗号鍵の長さＲ$_{secure}$は、共有した光子数、ＱＢＥＲ、および情報漏洩量によって求められるので、Ｒ$_{secure}$＝ｆ（共有した光子数，ＱＢＥＲ，情報漏洩量）とし、この関数ｆと、秘匿性増強処理部１３、２３の秘匿性増強処理の終了時に求まる処理時間とを用いて、セキュアキーレートは、下記の（式２）で求められる。

【００７１】

（セキュアキーレート）＝ｆ（共有した光子数，ＱＢＥＲ，情報漏洩量）／（処理時間）　・・・（式２）

【００７２】

このセキュアキーレートは、上述の（式１）および（式２）に示すように、共有した光子数、ＱＢＥＲ、情報漏洩量、および処理時間が測定されていなければ正確な値を求めることができない。また、共有した光子数、ＱＢＥＲ、情報漏洩量、および処理時間は、上述の（５）の段階である秘匿性増強処理部１３、２３の秘匿性増強処理が終了した時にすべてが測定値として明らかになる。ここで、セキュアキーレートを向上させるためには、上述の（１）～（４）の段階で、予想されるセキュアキーレートが求まっていると、光子共有処理、シフティング処理、および誤り訂正処理の調整動作が容易になる。また、（５）の段階では、正確なセキュアキーレートが求まるので、秘匿性増強処理の調整動作が容易になる。以下、図５を参照しながら、推定部１５、２５による上述の（１）～（５）の各段階においてセキュアキーレートの推定動作について説明する。なお、ここでは、推定部１５を例に説明するが、推定部２５についても同様の動作となる。

【００７３】

図５における（１）装置起動の時には、共有した光子数、ＱＢＥＲ、情報漏洩量、および処理時間は、いずれも測定されてないので、推定部１５は、記憶部１７に記憶された、共有した光子数、ＱＢＥＲ、情報漏洩量、および処理時間の初期値を取得する。そして、推定部１５は、図５に示すように、共有した光子数、ＱＢＥＲ、情報漏洩量、および処理時間の初期値を用いて、上述の（式１）および（式２）により、セキュアキーレートの推定値を算出する。ここで、推定部１５により算出されるセキュアキーレートの推定値は、共有した光子数、ＱＢＥＲ、情報漏洩量、および処理時間のすべてについて初期値を用いて算出されるので、セキュアキーレートの初期値と称するものとする。上述のように、共有した光子数、ＱＢＥＲ、情報漏洩量、および処理時間の初期値は、それぞれ、過去に各処理の測定値に基づいて算出された値としているので、セキュアキーレートの初期値は、

ＱＫＤ装置（ここでは、送信機１）の特性、ＱＫＤ装置の設置環境、およびＱＫＤの方式等から期待されるセキュアキーレートの理想値としてとらえることができる。推定部１５は、算出したセキュアキーレートの初期値を、記憶部１７に記憶させる。なお、セキュアキーレートの理想値としては、共有した光子数、ＱＢＥＲ、情報漏洩量、および処理時間の各初期値として装置特性等から期待される値を設定した場合のセキュアキーレートの推定値、すなわち、装置特性等から期待されるセキュアキーレートの値を採用してもよい。また、セキュアキーレートの理想値として、共有した光子数、ＱＢＥＲ、情報漏洩量、および処理時間の各値の過去の測定値の中で、最適または好適な値を用いた場合のセキュアキーレートの推定値、すなわち、過去における最適または好適なセキュアキーレートの実績値を採用してもよい。

【００７４】

図５における（２）光子共有処理の実行時には、ＱＢＥＲ、情報漏洩量、および処理時間が、それぞれ測定されていないので、推定部１５は、記憶部１７に記憶されたＱＢＥＲ、情報漏洩量、および処理時間の初期値を取得する。また、推定部１５は、光子送信部１０の光子共有処理により出力される共有した光子数の測定値を、制御部１４を介して受け取る。そして、推定部１５は、図５に示すように、共有した光子数の測定値、ならびに、ＱＢＥＲ、情報漏洩量、および処理時間の初期値を用いて、上述の（式１）および（式２）により、セキュアキーレートの推定値を算出する。さらに、制御部１４は、記憶部１７に記憶されたセキュアキーレートの初期値と、推定部１５により算出されたセキュアキーレートの推定値との差分に基づいて、光子送信部１０による光子共有処理の動作を調整する。例えば、制御部１４は、光子共有処理によって共有させる光子数を増加させるように調整する。すなわち、シフティング処理の実行前の段階、すなわち、光子共有処理のみの実行時の段階で、推定部１５の推定値から十分なセキュアキーレートが得られていない場合、制御部１４は、光子送信部１０の光子共有処理の動作のみの調整を行うことによって、セキュアキーレートの改善効果が期待できることになる。なお、制御部１４による光子共有処理の動作の調整は、セキュアキーレートの初期値と、セキュアキーレートの推定値との差分に基づいて、自動で調整するものとしてもよく、または、入力部１６により受け付けられた作業者の操作入力に基づいて調整されるものとしてもよい。入力部１６により受け付けられた作業者の操作入力に基づいて調整される動作については、後述の変形例１において詳述する。

【００７５】

図５における（３）シフティング処理の実行時には、ＱＢＥＲ、情報漏洩量、および処理時間が、それぞれ測定されていない。ただし、シフティング処理部１１は、上述のように、シフティング処理によって、仮のＱＢＥＲであるサンプルＱＢＥＲを算出する。したがって、推定部１５は、上述の（式１）および（式２）におけるＱＢＥＲとして、シフティング処理部１１により算出されたサンプルＱＢＥＲを、ＱＢＥＲの測定値として用いる。また、推定部１５は、記憶部１７に記憶された情報漏洩量、および処理時間の初期値を取得する。また、推定部１５は、光子送信部１０の光子共有処理により出力される共有した光子数、およびシフティング処理部１１のシフティング処理により出力されるサンプルＱＢＥＲの測定値を、制御部１４を介して受け取る。そして、推定部１５は、図５に示すように、共有した光子数、およびサンプルＱＢＥＲの測定値、ならびに、情報漏洩量、および処理時間の初期値を用いて、上述の（式１）および（式２）により、セキュアキーレートの推定値を算出する。さらに、制御部１４は、記憶部１７に記憶されたセキュアキーレートの初期値と、推定部１５により算出されたセキュアキーレートの推定値との差分に基づいて、光子送信部１０によるシフティング処理の動作を調整する。すなわち、光子共有処理およびシフティング処理の実行時の段階で、推定部１５の推定値から十分なセキュアキーレートが得られていない場合、制御部１４は、光子共有処理の調整は終了しているので、シフティング処理部１１のシフティング処理の動作のみの調整を行うことによって、セキュアキーレートの改善効果が期待できることになる。なお、制御部１４によるシフティング処理の動作の調整は、セキュアキーレートの初期値と、セキュアキーレートの推

定値との差分に基づいて、自動で調整するものとしてもよく、または、入力部１６により受け付けられた作業者の操作入力に基づいて調整されるものとしてもよい。入力部１６により受け付けられた作業者の操作入力に基づいて調整される動作については、後述の変形例１において詳述する。

【００７６】

図５における（４）誤り訂正処理の実行時には、処理時間のみが測定されていないので、推定部１５は、記憶部１７に記憶された処理時間の初期値を取得する。また、推定部１５は、光子送信部１０の光子共有処理により出力される共有した光子数、ならびに、誤り訂正処理部１２の誤り訂正処理により出力されるＱＢＥＲおよび漏洩情報量の測定値を、制御部１４を介して受け取る。そして、推定部１５は、図５に示すように、共有した光子数、ＱＢＥＲ、および情報漏洩量の測定値、ならびに、処理時間の初期値を用いて、上述の（式１）および（式２）により、セキュアキーレートの推定値を算出する。例えば、記憶部１７に予め記憶されているＱＢＥＲの初期値が５［％］であるものとし、（１）装置起動の段階で、推定部１５によるセキュアキーレートの推定値が１００［ｋｂｐｓ］であるものとする。その後の誤り訂正処理部１２による誤り訂正処理の実行段階で、誤り訂正処理部１２によりＱＢＥＲが６［％］と算出された場合、推定部１５は、セキュアキーレートの推定値を算出するために、ＱＢＥＲの初期値である５［％］ではなく、算出された測定値である６［％］を利用する。上述の（式１）および（式２）から、ＱＢＥＲについて５［％］から６［％］の変化は、セキュアキーレートについて２４［％］の減少効果があるため、推定部１５によって、セキュアキーレートは７６［ｋｂｐｓ］と推定される。なお、この例では、簡単のためＥＣ効率を１．２としている。

【００７７】

さらに、制御部１４は、記憶部１７に記憶されたセキュアキーレートの初期値と、推定部１５により算出されたセキュアキーレートの推定値との差分に基づいて、光子送信部１０による誤り訂正処理の動作を調整する。すなわち、光子共有処理、シフティング処理および誤り訂正処理の実行時の段階で、推定部１５の推定値から十分なセキュアキーレートが得られていない場合、制御部１４は、光子共有処理およびシフティング処理の調整は終了しているので、誤り訂正処理部１２の誤り訂正処理の動作のみの調整を行うことによって、セキュアキーレートの改善効果が期待できることになる。例えば、制御部１４による誤り訂正処理の調整の結果、誤り訂正処理部１２による誤り訂正処理で算出されるＱＢＥＲがサンプル値である６［％］から、ＱＢＥＲとして正確な４［％］が得られる。これを基に、上述の（式１）および（式２）から、セキュアキーレートについてより正確な値を求めることができ、推定部１５によって、セキュアキーレートは１２７［ｋｂｐｓ］と推定される。

【００７８】

なお、制御部１４による誤り訂正処理の動作の調整は、セキュアキーレートの初期値と、セキュアキーレートの推定値との差分に基づいて、自動で調整するものとしてもよく、または、入力部１６により受け付けられた作業者の操作入力に基づいて調整されるものとしてもよい。入力部１６により受け付けられた作業者の操作入力に基づいて調整される動作については、後述の変形例１において詳述する。

【００７９】

図５における（５）秘匿性増強処理の実行時には、共有した光子数、ＱＢＥＲ、情報漏洩量、および処理時間はすべて測定されている。したがって、推定部１５は、光子送信部１０の光子共有処理により出力される共有した光子数、誤り訂正処理部１２の誤り訂正処理により出力されるＱＢＥＲおよび漏洩情報量、ならびに、秘匿性増強処理部１３の秘匿性増強処理により出力される処理時間の測定値を、制御部１４を介して受け取る。そして、推定部１５は、図５に示すように、共有した光子数、ＱＢＥＲ、情報漏洩量、および処理時間の測定値を用いて、上述の（式１）および（式２）により、セキュアキーレートの推定値を算出する。ここで、推定部１５により算出されたセキュアキーレートの推定値は、すべて測定値を用いて算出されているので、セキュアキーレートの実際の値となる。さ

らに、制御部１４は、記憶部１７に記憶されたセキュアキーレートの初期値と、推定部１５により算出されたセキュアキーレートの推定値との差分に基づいて、光子送信部１０による秘匿性増強処理の動作を調整する。すなわち、光子共有処理、シフティング処理、誤り訂正処理および秘匿性増強処理の実行時の段階で、推定部１５の推定値から十分なセキュアキーレートが得られていない場合、制御部１４は、光子共有処理、シフティング処理および誤り訂正処理の調整は終了しているので、誤り訂正処理部１２の秘匿性増強処理の動作のみの調整を行うことによって、セキュアキーレートの改善効果が期待できることになる。なお、制御部１４による秘匿性増強処理の動作の調整は、セキュアキーレートの初期値と、セキュアキーレートの推定値との差分に基づいて、自動で調整するものとしてもよく、または、入力部１６により受け付けられた作業者の操作入力に基づいて調整されるものとしてもよい。入力部１６により受け付けられた作業者の操作入力に基づいて調整される動作については、後述の変形例１において詳述する。

【００８０】

以上のように、暗号鍵生成動作での光子共有処理、シフティング処理、誤り訂正処理および秘匿性増強処理の各段階において、セキュアキーレートを算出するためのパラメータのうち、測定されているものは測定値を利用し、測定されていないものは初期値を利用して、セキュアキーレートを推定するものとしている。これによって、暗号鍵生成動作の各段階でのセキュアキーレートの推定値を認識することができ、各段階で動作している処理を調整することによって、セキュアキーレートを理想値に近づけることができ、容易にセキュアキーレートを向上させることができる。

【００８１】

なお、上述のように、推定部１５（２５）は、光子共有処理、シフティング処理、誤り訂正処理および秘匿性増強処理における各測定値（共有した光子数、サンプルＱＢＥＲ、ＱＢＥＲ、情報漏洩量および処理時間）を、制御部１４（２４）を介して受け取るものとしているが、これに限定されるものではなく、制御部１４（２４）を介さずに直接受け取るものとしてもよい。

【００８２】

また、セキュアキーレートの推定に用いる上述の（式１）の計算式は、ＱＫＤの方式に応じて変更が可能である。例えば、光子送信部１０および光子受信部２０は、基底をランダムに選択するものとしているが、例えば、基底の選択確率に偏りを持たせる方式の場合、シフティング処理で破棄されるビット数も変化するため、（式１）の計算式も変更するものとすればよい。この場合、基底の選択確率の偏りに合わせて、（式１）の係数「１／２」を変更するものとすればよい。

【００８３】

また、上述の図３に示すように、送信機１および受信機２の双方が推定部（推定部１５、２５）を備えるものとしているが、これに限定されるものではなく、送信機１および受信機２のいずれかが推定部を備えるものとしてもよい。

【００８４】

また、推定部１５、２５による推定動作は、各段階で取得できる測定値が更新されるたびに実行されるものとしてもよく、または、所定時間ごとに実行されるものとしてもよい。

【００８５】

＜変形例１＞

本変形例に係るＱＫＤ装置について、上述の実施形態に係るＱＫＤ装置（送信機１および受信機２）と相違する点を中心に説明する。本変形例に係るＱＫＤ装置は、上述の実施形態に係るＱＫＤ装置が備える各機能部に加えて、さらに表示部を備えるものである。

【００８６】

図７は、変形例１に係るＱＫＤ装置の機能ブロックの構成の一例を示す図である。図７を参照しながら、本変形例に係るＱＫＤ装置（送信機１ａ、受信機２ａ）の機能ブロック構成について説明する。

【００８７】
図７に示すように、送信機１ａは、光子送信部１０（量子鍵共有手段）と、シフティング処理部１１（シフティング手段）と、誤り訂正処理部１２（訂正手段）と、秘匿性増強処理部１３（秘匿性増強手段）と、制御部１４（制御手段）と、推定部１５（推定手段）と、入力部１６（入力手段）と、記憶部１７と、表示部１８（表示手段）と、を有する。
【００８８】
制御部１４は、上述の光子送信部１０、シフティング処理部１１、誤り訂正処理部１２、および秘匿性増強処理部１３の動作を制御する機能部である。また、制御部１４は、光子送信部１０、シフティング処理部１１、誤り訂正処理部１２および秘匿性増強処理部１３の各処理で求まる測定値を取得し、推定部１５に送る。また、制御部１４は、入力部１６から操作入力された初期値を、予め記憶部１７に記憶させる。また、制御部１４は、入力部１６により受け付けられた操作入力に基づいて、上述の（１）～（５）の各段階を進める動作、および、光子送信部１０、シフティング処理部１１、誤り訂正処理部１２および秘匿性増強処理部１３の各処理の調整動作を行う。
【００８９】
入力部１６は、初期値の操作入力、上述の（１）～（５）の各段階を進める操作入力、および、光子送信部１０、シフティング処理部１１、誤り訂正処理部１２および秘匿性増強処理部１３の各処理の調整動作を制御部１４に行わせるための操作入力等を受け付ける機能部である。
【００９０】
表示部１８は、推定部１５により算出されたセキュアキーレートの推定値に関する情報を表示する装置である。表示部１８は、図２に示す表示装置８４によって実現される。
【００９１】
図７に示すように、受信機２ａは、光子受信部２０（量子鍵共有手段）と、シフティング処理部２１（シフティング手段）と、誤り訂正処理部２２（訂正手段）と、秘匿性増強処理部２３（秘匿性増強手段）と、制御部２４（制御手段）と、推定部２５（推定手段）と、入力部２６（入力手段）と、記憶部２７と、表示部２８（表示手段）と、を有する。
【００９２】
制御部２４は、上述の光子受信部２０、シフティング処理部２１、誤り訂正処理部２２、および秘匿性増強処理部２３の動作を制御する機能部である。また、制御部２４は、光子受信部２０、シフティング処理部２１、誤り訂正処理部２２および秘匿性増強処理部２３の各処理で求まる測定値を取得し、推定部２５に送る。また、制御部２４は、入力部２６から操作入力された初期値を、予め記憶部２７に記憶させる。また、制御部２４は、入力部２６により受け付けられた操作入力に基づいて、上述の（１）～（５）の各段階を進める動作、および、光子受信部２０、シフティング処理部２１、誤り訂正処理部２２および秘匿性増強処理部２３の各処理の調整動作を行う。
【００９３】
図８は、推定値の表示例を示す図である。図９は、棒グラフによる推定値の表示例を示す図である。図１０は、推定値の時系列のグラフによる表示例を示す図である。図１１は、推定値の時系列のグラフによる表示例を示す図である。図８～１１、および上述の図５を参照しながら、セキュアキーレートの推定動作、推定値に関する情報を表示する動作、および暗号鍵生成動作での各処理の調整をする動作について説明する。
【００９４】
まず、セキュアキーレートを向上させるための作業を行う作業者は、ＱＫＤ装置（送信機１および受信機２）を起動させる。図５における（１）装置起動の時における、推定部１５によるセキュアキーレートの推定動作は、上述した通りである。また、制御部１４は、推定部１５からセキュアキーレートの推定値を受け取り、例えば、図８に示すように、受け取った推定値、およびセキュアキーレートの初期値を表示部１８に表示させる。ただし、ここでは、セキュアキーレートの推定値と初期値とは、同一の値となる。そして、作業者は、入力部１６に対して、次の段階である光子送信部１０に光子共有処理を実行させ

る段階に進める操作入力を行う。

【００９５】

制御部１４は、入力部１６から光子送信部１０に光子共有処理を実行させるための操作情報を受信すると、光子送信部１０に光子共有処理を開始させる。図５における（２）光子共有処理の実行時における、推定部１５によるセキュアキーレートの推定動作は、上述した通りである。光子送信部１０は、生成した光子ビット列を、記憶部１７に記憶（蓄積）させる。また、推定部１５は、算出したセキュアキーレートの推定値を、記憶部１７に記憶させる。また、制御部１４は、推定部１５からセキュアキーレートの推定値を受け取り、例えば、図８に示すように、受け取った推定値、およびセキュアキーレートの初期値を表示部１８に表示させる。作業者は、表示部１８に表示されたセキュアキーレートの推定値および初期値を確認し、光子共有処理のみの実行時の段階で、推定部１５の推定値から十分なセキュアキーレートが得られていないと判断した場合、光子送信部１０の光学共有処理を調整するための操作入力を入力部１６に対して行う。制御部１４は、入力部１６により受け付けられた調整のための操作入力に基づいて、光子送信部１０による光子共有処理の動作を調整する。このように、光子送信部１０の光子共有処理の動作のみの調整が行われることによって、セキュアキーレートの改善効果が期待できることになる。そして、作業者は、光子共有処理の動作を調整した後、入力部１６に対して、次の段階であるシフティング処理部１１のシフティング処理を実行させる段階に進める操作入力を行う。

【００９６】

制御部１４は、入力部１６からシフティング処理部１１にシフティング処理を実行させるための操作情報を受信すると、シフティング処理部１１にシフティング処理を開始させる。シフティング処理部１１は、記憶部１７に蓄積された光子ビット列を用いて、シフティング処理を実行する。図５における（３）シフティング処理の実行時における、推定部１５によるセキュアキーレートの推定動作は、上述した通りである。シフティング処理部１１は、生成した共有ビット列を、記憶部１７に記憶（蓄積）させる。また、推定部１５は、算出したセキュアキーレートの推定値を、記憶部１７に記憶させる。また、制御部１４は、推定部１５からセキュアキーレートの推定値を受け取り、例えば、図８に示すように、受け取った推定値、およびセキュアキーレートの初期値を表示部１８に表示させる。作業者は、表示部１８に表示されたセキュアキーレートの推定値および初期値を確認し、光子共有処理およびシフティング処理の実行時の段階で、推定部１５の推定値から十分なセキュアキーレートが得られていないと判断した場合、光子共有処理の調整は終了しているので、シフティング処理部１１のシフティング処理を調整するための操作入力を入力部１６に対して行う。制御部１４は、入力部１６により受け付けられた調整のための操作入力に基づいて、シフティング処理部１１によるシフティング処理の動作を調整する。このように、シフティング処理部１１のシフティング処理の動作のみの調整が行われることによって、セキュアキーレートの改善効果が期待できることになる。そして、作業者は、シフティング処理の動作を調整した後、入力部１６に対して、次の段階である誤り訂正処理部１２の誤り訂正処理を実行させる段階に進める操作入力を行う。

【００９７】

制御部１４は、入力部１６から誤り訂正処理部１２に誤り訂正処理を実行させるための操作情報を受信すると、誤り訂正処理部１２に誤り訂正処理を開始させる。誤り訂正処理部１２は、記憶部１７に蓄積された共有ビット列を用いて、誤り訂正処理を実行する。図５における（４）誤り訂正処理の実行時における、推定部１５によるセキュアキーレートの推定動作は、上述した通りである。誤り訂正処理部１２は、生成した訂正後ビット列を、記憶部１７に記憶（蓄積）させる。また、推定部１５は、算出したセキュアキーレートの推定値を、記憶部１７に記憶させる。また、制御部１４は、推定部１５からセキュアキーレートの推定値を受け取り、例えば、図８に示すように、受け取った推定値、およびセキュアキーレートの初期値を表示部１８に表示させる。作業者は、表示部１８に表示されたセキュアキーレートの推定値および初期値を確認し、光子共有処理、シフティング処理および誤り訂正処理の実行時の段階で、推定部１５の推定値から十分なセキュアキーレー

トが得られていないと判断した場合、光子共有処理およびシフティング処理の調整は終了しているので、誤り訂正処理部１２の誤り訂正処理を調整するための操作入力を入力部１６に対して行う。制御部１４は、入力部１６により受け付けられた調整のための操作入力に基づいて、誤り訂正処理部１２による誤り訂正処理の動作を調整する。このように、誤り訂正処理部１２の誤り訂正処理の動作のみの調整が行われることによって、セキュアキーレートの改善効果が期待できることになる。そして、作業者は、誤り訂正処理の動作を調整した後、入力部１６に対して、次の段階である秘匿性増強処理部１３の秘匿性増強処理を実行させる段階に進める操作入力を行う。

【００９８】

制御部１４は、入力部１６から秘匿性増強処理部１３に秘匿性増強処理を実行させるための操作情報を受信すると、秘匿性増強処理部１３に秘匿性増強処理を開始させる。秘匿性増強処理部１３は、記憶部１７に蓄積された訂正後ビット列を用いて、秘匿性増強処理を実行する。図５における（５）秘匿性増強処理の実行時における、推定部１５によるセキュアキーレートの推定動作は、上述した通りである。秘匿性増強処理部１３は、生成した暗号鍵を、記憶部１７に記憶（蓄積）させる。また、推定部１５は、算出したセキュアキーレートの推定値を、記憶部１７に記憶させる。また、制御部１４は、推定部１５からセキュアキーレートの推定値（セキュアキーレートの実際の値）を受け取り、例えば、図８に示すように、受け取った推定値、およびセキュアキーレートの初期値を表示部１８に表示させる。作業者は、表示部１８に表示されたセキュアキーレートの推定値および初期値を確認し、光子共有処理、シフティング処理、誤り訂正処理および秘匿性増強処理の実行時の段階で、推定部１５の推定値から十分なセキュアキーレートが得られていないと判断した場合、光子共有処理、シフティング処理および秘匿性増強処理の調整は終了しているので、秘匿性増強処理部１３の秘匿性増強処理を調整するための操作入力を入力部１６に対して行う。制御部１４は、入力部１６により受け付けられた調整のための操作入力に基づいて、秘匿性増強処理部１３による秘匿性増強処理の動作を調整する。このように、秘匿性増強処理部１３の秘匿性増強処理の動作のみの調整が行われることによって、セキュアキーレートの改善効果が期待できることになる。

【００９９】

以上の手順によって、作業者は、各段階で算出される推定値と初期値とを比較しながら、セキュアキーレートを向上させるための調整作業を行う。

【０１００】

以上のように、作業者は、上述の（１）～（５）の各段階において、推定部１５（２５）によって算出されるセキュアキーレートの推定値と、セキュアキーレートの理想値（例えば、初期値）とを比較しながら、各段階での処理の調整作業を行うことができる。このように、推定部１５（２５）により算出される推定値および初期値が、表示部１８（２８）に表示されるので、作業者はセキュアキーレートを向上させるための調整作業を容易に行うことができ、セキュアキーレートを容易に向上させることができる。

【０１０１】

なお、図８に示すように、表示部１８（２８）に現在表示されている推定値と、前回、推定部１５（２５）により算出された推定値との変化率を、表示部１８（２８）に表示させるものとしてもよい。この場合、推定部１５（２５）は、セキュアキーレートの推定値を算出すると共に、記憶部１７（２７）に記憶されている前回の推定値を取得して変化率を算出し、制御部１４（２４）は、図８に示すように、推定部１５（２５）により算出された最新の推定値と変化率とを、表示部１８（２８）に表示させるものとすればよい。このように変化率を表示させることによって、調整前の推定値と、調整後の推定値との変化率を把握することができ、調整の目安とすることができる。

【０１０２】

また、図８に示すように、表示部１８（２８）は、推定部１５（２５）により算出された推定値と共に、セキュアキーレートの初期値を表示するものとしているが、これに限定されるものではなく、セキュアキーレートの初期値は表示しないものとしてもよい。この

場合、作業者は、セキュアキーレートの理想値を予め把握しており、この理想値に、表示部１８（２８）に表示された推定値が近づくように、各処理に対する調整作業を行えばよい。

【０１０３】

また、表示部１８（２８）は、図９に示すように、制御部１４（２４）から受信したセキュアキーレートの推定値と初期値とを、棒グラフによって表示するものとしてもよい。これによって、作業者は、セキュアキーレートの推定値と初期値との差分を視覚的に即座に認識することができる。

【０１０４】

また、表示部１８（２８）は、図１０に示すように、推定値を時系列にプロットしたグラフを表示するものとしてもよい。この場合、グラフと共に、セキュアキーレートの初期値の線を併せて表示させることによって、作業者は、セキュアキーレートの調整の目安を視覚的に確認することができると共に、上述の（１）～（５）の各段階でのセキュアキーレートについての調整作業の効果を把握することができる。

【０１０５】

また、表示部１８（２８）は、図１１に示すように、推定値を時系列にプロットしたグラフと併せて、運用可能レベルの線を表示させるものとしてもよい。ここで、運用可能レベルとは、例えば、暗号データ通信を一定の品質で行い得るだけの暗号鍵を生成できるセキュアキーレートをいう。これによっても、作業者は、セキュアキーレートの調整の目安を視覚的に確認することができると共に、上述の（１）～（５）の各段階でのセキュアキーレートについての調整作業の効果を把握することができる。

【０１０６】

また、表示部１８（２８）は、例えば、図８の表示項目に併せて、各処理の測定値（共有した光子数、サンプルＱＢＥＲ、ＱＢＥＲ、情報漏洩量、および処理時間）の少なくともいずれかを表示するものとしてもよい。また、表示部１８（２８）は、これらの測定値と併せて、各測定値に対応する初期値を表示するものとしてもよい。また、表示部１８（２８）は、これらの測定値についても、図１０と同様に、時系列にプロットしたグラフを表示するものとしてもよく、これに併せて、各測定値の初期値の線を併せて表示するものとしてもよい。

【０１０７】

また、上述の図７に示すように、送信機１ａおよび受信機２ａの双方が表示部（表示部１８、２８）を備えるものとしているが、これに限定されるものではなく、送信機１ａおよび受信機２ａのいずれかが表示部を備えるものとしてもよい。例えば、送信機１ａおよび受信機２ａの双方が表示部を備え、送信機１ａおよび受信機２ａのいずれかのみが推定部を備える場合、その推定部は、算出したセキュアキーレートの推定値を、古典通信路を介して、推定部を備えないＱＫＤ装置に送信するものとすればよい。

【０１０８】

＜変形例２＞

本変形例に係るＱＫＤ装置について、上述の変形例１に係るＱＫＤ装置（送信機１ａおよび受信機２ａ）と相違する点を中心に説明する。本変形例に係るＱＫＤ装置は、上述の変形例１に係るＱＫＤ装置が備える各機能部に加えて、さらに判定部および報知部を備えるものである。

【０１０９】

図１２は、変形例２に係るＱＫＤ装置の機能ブロックの構成の一例を示す図である。図１２を参照しながら、本変形例に係るＱＫＤ装置（送信機１ｂ、受信機２ｂ）の機能ブロック構成について説明する。

【０１１０】

図１２に示すように、送信機１ｂは、光子送信部１０（量子鍵共有手段）と、シフティング処理部１１（シフティング手段）と、誤り訂正処理部１２（訂正手段）と、秘匿性増強処理部１３（秘匿性増強手段）と、制御部１４（制御手段）と、推定部１５（推定手段

）と、入力部１６（入力手段）と、記憶部１７と、表示部１８（表示手段）と、判定部１９ａ（判定手段）と、報知部１９ｂ（報知手段）と、を有する。

【０１１１】

判定部１９ａは、推定部１５によって算出されたセキュアキーレートの推定値に対して、所定の条件を満たすか否かの判定を行う機能部である。また、判定部１９ａは、所定の条件を満たす場合、報知部１９ｂに報知させる。例えば、判定部１９ａは、所定の条件として、セキュアキーレートの推定値が運用可能レベルに達したか否かを判定するものとし、推定値が運用可能レベル以上となった場合、報知部１９ｂにその旨を報知させる。または、判定部１９ａは、所定の条件として、セキュアキーレートの推定値が運用不可能となるレベルを下回ったか否かを判定するものとし、推定値が運用不可能となるレベル未満となった場合、報知部１９ｂにその旨を報知させるものとしてもよい。判定部１９ａは、図２に示すＣＰＵ８０が補助記憶装置８６等に記憶されたプログラムをＲＡＭ８２に読み出して実行することによって実現される。なお、判定部１９ａは、ハードウェア回路によって実現されるものとしてもよい。

【０１１２】

報知部１９ｂは、判定部１９ａによってセキュアキーレートの推定値が所定の条件を満たすと判定された場合、判定部１９ａの指令に基づいて、所定の条件を満たす旨を音声出力等で報知する機能部である。報知部１９ｂは、図２に示すスピーカ８８によって実現される。

【０１１３】

図１２に示すように、受信機２ｂは、光子受信部２０（量子鍵共有手段）と、シフティング処理部２１（シフティング手段）と、誤り訂正処理部２２（訂正手段）と、秘匿性増強処理部２３（秘匿性増強手段）と、制御部２４（制御手段）と、推定部２５（推定手段）と、入力部２６（入力手段）と、記憶部２７と、表示部２８（表示手段）と、判定部２９ａ（判定手段）と、報知部２９ｂ（報知手段）と、を有する。

【０１１４】

判定部２９ａは、推定部２５によって算出されたセキュアキーレートの推定値に対して、所定の条件を満たすか否かの判定を行う機能部である。また、判定部２９ａは、所定の条件を満たす場合、報知部２９ｂに報知させる。判定部２９ａは、図２に示すＣＰＵ８０が補助記憶装置８６等に記憶されたプログラムをＲＡＭ８２に読み出して実行することによって実現される。なお、判定部２９ａは、ハードウェア回路によって実現されるものとしてもよい。

【０１１５】

報知部２９ｂは、判定部２９ａによってセキュアキーレートの推定値が所定の条件を満たすと判定された場合、判定部２９ａの指令に基づいて、所定の条件を満たす旨を音声出力等で報知する機能部である。報知部２９ｂは、図２に示すスピーカ８８によって実現される。

【０１１６】

なお、報知部１９ｂ、２９ｂは、音声を出力するものに限定されるものではなく、例えば、ランプ表示等によって報知するものとしてもよい。また、セキュアキーレートの推定値が所定の条件を満たす場合、表示部１８、２８において、セキュアキーレートの推定値の表示形式（文字色、棒グラフの色等）を変化させたり、または、所定の条件を満たした旨のメッセージを表示させるものとしてもよい。このように表示部１８、２８における表示を変化させる機能は、報知部１９ｂ、２９ｂによる報知機能と同様の機能を担うものである。

【０１１７】

以上のように、作業者は、表示部１８（２８）でセキュアキーレートの推定値を確認しながら、各段階での処理の調整を行うことに加え、判定部１９ａ（２９ａ）により推定値が所定の条件を満たすと判定された場合、報知部１９ｂ（２９ｂ）はその旨を報知するものとしている。これによって、作業者は、視覚的に推定値を確認するだけでなく、聴覚的

に所定の条件を満たしていること（例えば、推定値が運用可能レベル以上になったこと）を認識することができるので、セキュアキーレートを向上させるための調整作業をさらに容易に行うことができる。

【０１１８】

なお、上述の実施形態および各変形例に係るＱＫＤ装置で実行されるプログラムは、例えば、ＲＯＭ８１等に予め組み込まれて提供されるものとしてもよい。

【０１１９】

また、上述の実施形態および各変形例に係るＱＫＤ装置で実行されるプログラムは、インストール可能な形式または実行可能な形式のファイルでＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｋ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、フレキシブルディスク（ＦＤ）、ＣＤ－Ｒ（Ｃｏｍｐａｃｔ Ｄｉｓｋ Ｒｅｃｏｒｄａｂｌｅ）、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ）等のコンピュータで読み取り可能な記録媒体に記録してコンピュータプログラムプロダクトとして提供されるように構成してもよい。

【０１２０】

さらに、上述の実施形態および各変形例に係るＱＫＤ装置で実行されるプログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成してもよい。また、上述の実施形態および各変形例に係るＱＫＤ装置で実行されるプログラムをインターネット等のネットワーク経由で提供または配布するように構成してもよい。

【０１２１】

また、上述の実施形態および各変形例に係るＱＫＤ装置で実行されるプログラムは、コンピュータを上述したＱＫＤ装置の各機能部として機能させ得る。このコンピュータは、ＣＰＵ８０がコンピュータ読取可能な記憶媒体からプログラムを主記憶装置上に読み出して実行することができる。

【０１２２】

本発明の実施形態およびその変形例を説明したが、この実施形態および変形例は、例として提示したものであり、発明の範囲を限定することは意図していない。この新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、および変更を行うことができる。この実施形態および変形例は、発明の範囲および要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

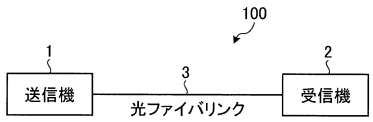
【符号の説明】

【０１２３】

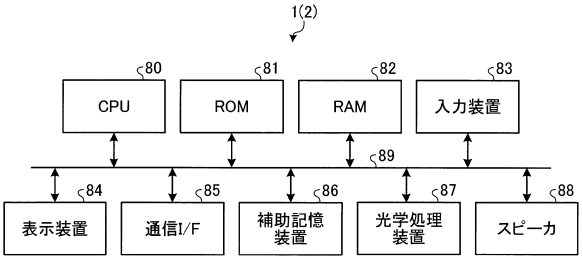
１、１ａ、１ｂ　送信機
２、２ａ、２ｂ　受信機
３　光ファイバリンク
１０　光子送信部
１１　シフティング処理部
１２　誤り訂正処理部
１３　秘匿性増強処理部
１４　制御部
１５　推定部
１６　入力部
１７　記憶部
１８　表示部
１９ａ　判定部
１９ｂ　報知部
２０　光子受信部
２１　シフティング処理部
２２　誤り訂正処理部

２３　秘匿性増強処理部
２４　制御部
２５　推定部
２６　入力部
２７　記憶部
２８　表示部
２９ａ　判定部
２９ｂ　報知部
８０　ＣＰＵ
８１　ＲＯＭ
８２　ＲＡＭ
８３　入力装置
８４　表示装置
８５　通信Ｉ／Ｆ
８６　補助記憶装置
８７　光学処理装置
８８　スピーカ
８９　バス
１００　量子鍵配送システム

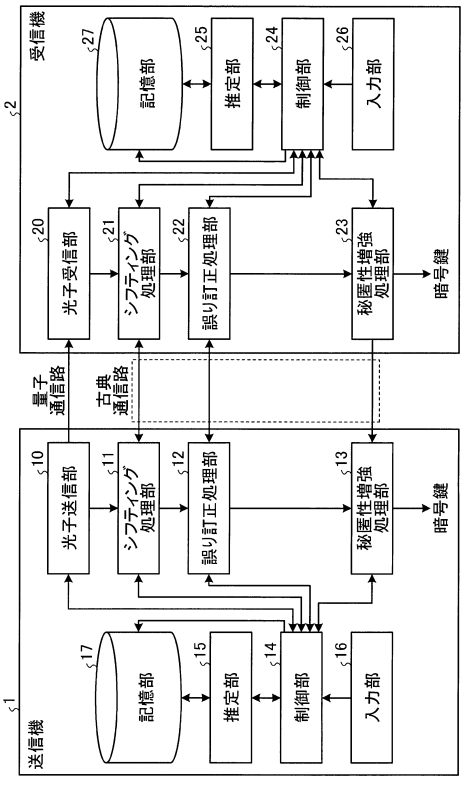
【図１】



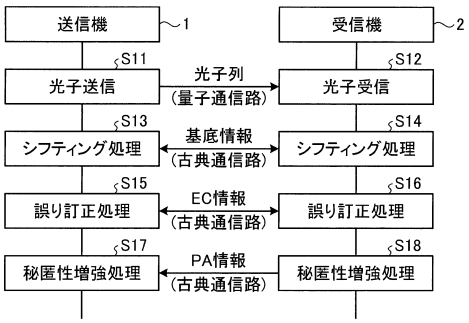
【図２】



【図３】



【図４】

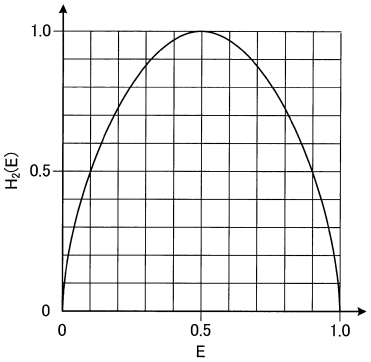


【図５】

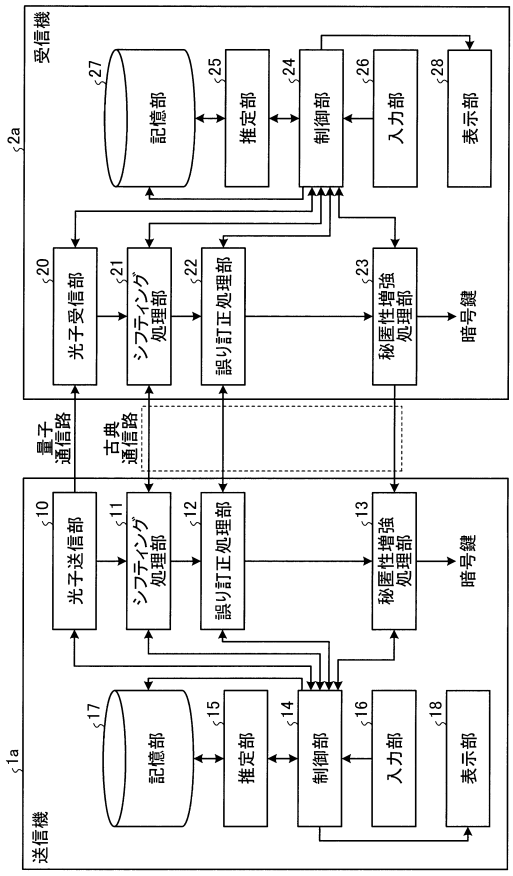
暗号鍵生成手順	光子数	QBER	情報漏洩量	処理時間	セキュアキーレート
(1)装置起動	初期値	初期値	初期値	初期値	すべて初期値から算出
(2)光子共有処理	測定値	初期値	初期値	初期値	初期値と測定値とから算出
(3)シフティング処理	測定値	測定値（サンプルQBER）	初期値	初期値	
(4)誤り訂正処理	測定値	測定値	測定値	初期値	
(5)秘匿性増強処理	測定値	測定値	測定値	測定値	すべて測定値から算出

時間

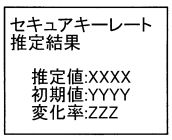
【図６】



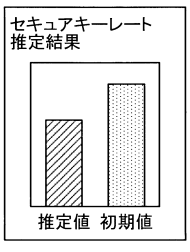
【図７】



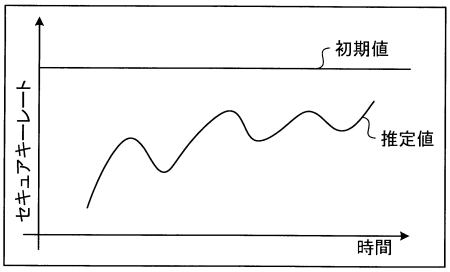
【図８】



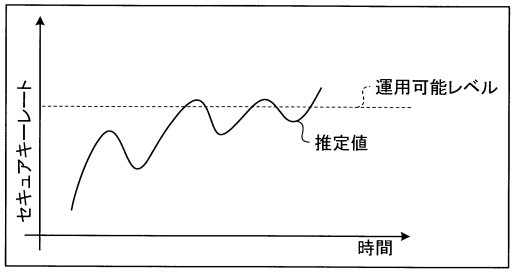
【図９】



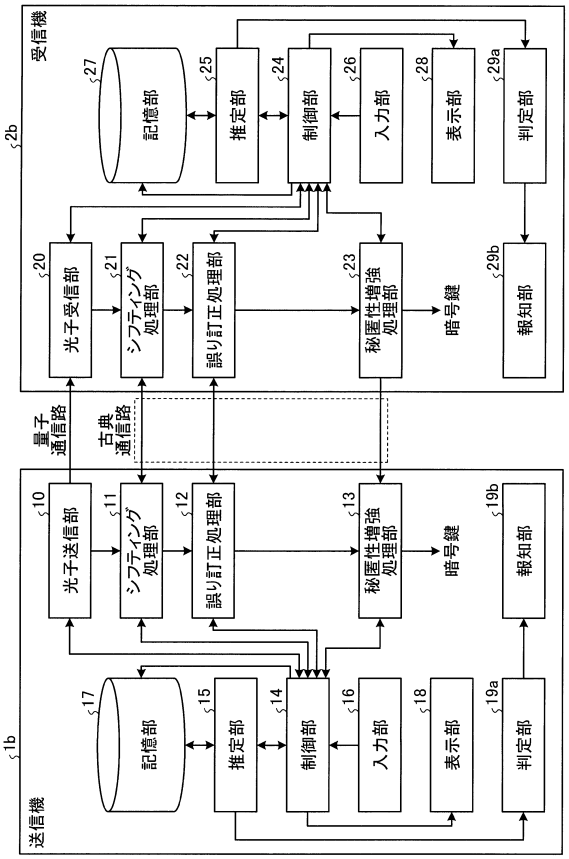
【図１０】


初期値
推定値
セキュアキーレート
時間

【図１１】


運用可能レベル
推定値
セキュアキーレート
時間

【図１２】


受信機
2b
27 記憶部
25 推定部
24 制御部
26 入力部
28 表示部
29a 判定部
20 光子受信部
21 シフティング処理部
22 誤り訂正処理部
23 秘匿性増強処理部
暗号鍵
29b 報知部
量子通信路
古典通信路
送信機
1b
10 光子送信部
11 シフティング処理部
12 誤り訂正処理部
13 秘匿性増強処理部
暗号鍵
19b 報知部
17 記憶部
15 推定部
14 制御部
16 入力部
18 表示部
19a 判定部

フロントページの続き

(56)参考文献 特開２０１５－１３０６２８（ＪＰ，Ａ）
特表２０１０－５０６４３２（ＪＰ，Ａ）
国際公開第２０１４／１１５１１８（WO，Ａ２）
田中 聡寛 ほか，量子鍵配送技術の高速化の為の鍵抽出高速化エンジンの開発，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２０１１年 1月２０日，第110巻 第392号，pp.25-30
Xiongfeng Ma, et al., Alternative schemes for measurement-device-independent quantum key distribution, Cornell University Library, ［オンライン］, ２０１２年１２月２４日, arXiv:1204.4856v2 [quant-ph], pp. 1-30, ［検索日 平成３０年７月２７日］、インターネット，ＵＲＬ，<https://arxiv.org/pdf/1204.4856.pdf>

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／１２