(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-169187
(P2017-169187A)
(43)公開日　平成29年9月21日(2017.9.21)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/12	(2006.01)	H04L	9/00	631	5J104
H04L	9/08	(2006.01)	H04L	9/00	601B	
			H04L	9/00	601E	

審査請求 未請求　請求項の数 13　OL　（全 37 頁）

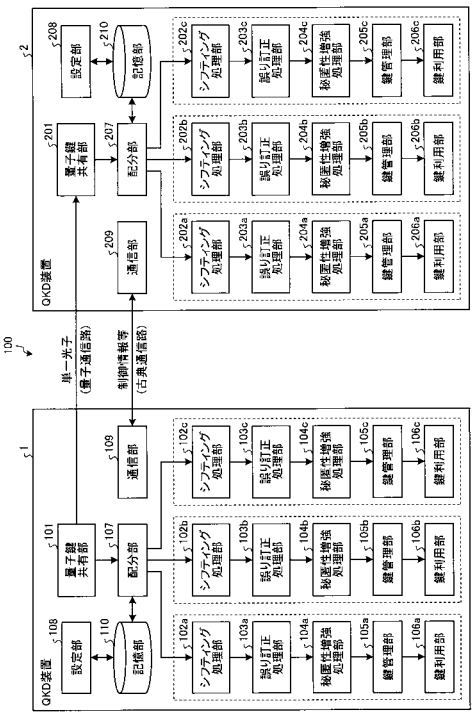
(21)出願番号　特願2016-179604 (P2016-179604)
(22)出願日　平成28年9月14日 (2016.9.14)
(31)優先権主張番号　特願2016-49754 (P2016-49754)
(32)優先日　平成28年3月14日 (2016.3.14)
(33)優先権主張国　日本国 (JP)

(71)出願人　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　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

Fターム(参考)　5J104 AA05　AA16　EA04　EA16　JA03
NA02　NA37

(54)【発明の名称】量子鍵配送装置、量子鍵配送システム、および量子鍵配送方法

(57)【要約】
【課題】暗号鍵を利用する対象が個別に要求するパラメータまたはバリエーションに応じた量子鍵配送および量子暗号技術のサービスの提供を実現することができる量子鍵配送装置、量子鍵配送システム、および量子鍵配送方法を提供する。
【解決手段】実施形態の量子鍵配送装置は、他の量子鍵配送装置と、量子通信路で接続され、暗号鍵を共有する量子鍵配送装置であって、共通処理部と、１以上の個別処理部と、配分部と、を備える。共通処理部は、量子通信路を介して他の量子鍵配送装置との間で光子列の送信または受信により取得したビット情報に基づいて中間データを出力する。個別処理部は、中間データに基づき暗号鍵を生成または提供する。配分部は、共通処理部で出力した中間データを１以上の個別処理部を含む２以上の配分先に配分する。
【選択図】図６



【特許請求の範囲】
【請求項１】
他の量子鍵配送装置と、量子通信路で接続され、暗号鍵を共有する量子鍵配送装置であって、
前記量子通信路を介して、前記他の量子鍵配送装置との間で光子列の送信または受信により取得したビット情報に基づいて、中間データを出力する共通処理部と、
前記中間データに基づき前記暗号鍵を生成または提供する１以上の個別処理部と、
前記共通処理部で出力した前記中間データを前記１以上の個別処理部を含む２以上の配分先に配分する配分部と、
を備えた量子鍵配送装置。
【請求項２】
前記共通処理部は、送信光子情報または検出光子情報を前記中間データとして出力する量子鍵共有部を含み、
前記１以上の個別処理部は、前記配分部により配分された前記中間データである前記送信光子情報または前記検出光子情報から、鍵蒸留処理によって前記暗号鍵を生成する鍵蒸留処理部をそれぞれ含む請求項１に記載の量子鍵配送装置。
【請求項３】
前記配分部は、２以上の前記個別処理部に対し、前記中間データを等分して配分する、
請求項１に記載の量子鍵配送装置。
【請求項４】
前記配分部は、２以上の前記個別処理部に対し、各個別処理部における要求内容に基づいて、前記中間データの配分方法を決定する、
請求項１に記載の量子鍵配送装置。
【請求項５】
前記配分部は、基底の偏り、デコイパルスとバキュームパルスとの割合、前記デコイパルスおよび前記バキュームパルスの分散、および、レーザ強度の分散のうち少なくともいずれかを規定する要求内容に応じて、前記中間データを前記鍵蒸留処理部にそれぞれ配分する請求項２に記載の量子鍵配送装置。
【請求項６】
前記配分部は、前記中間データの生成速度を規定する要求内容に応じて、前記中間データを前記個別処理部にそれぞれ配分する請求項１に記載の量子鍵配送装置。
【請求項７】
前記共通処理部は、
前記量子通信路を介して送信または受信した前記光子列に対応する光子ビット列を取得する量子鍵共有部と、
前記光子ビット列から、鍵蒸留処理の一部の処理を実行して前記中間データを出力する第１鍵蒸留処理部と、
を含み、
前記１以上の個別処理部は、前記配分部により配分された前記中間データから、前記鍵蒸留処理の前記一部の処理を除いた残りの処理を実行して、前記暗号鍵を生成する第２鍵蒸留処理部をそれぞれ含む請求項１に記載の量子鍵配送装置。
【請求項８】
前記第１鍵蒸留処理部は、前記中間データについての推定誤り率を算出し、
前記配分部は、前記中間データに対応する前記推定誤り率を規定する要求内容に応じて、前記中間データを前記第２鍵蒸留処理部にそれぞれ配分する請求項７に記載の量子鍵配送装置。
【請求項９】
前記第１鍵蒸留処理部は、前記中間データに対する前記鍵蒸留処理のうちの誤り訂正処理により該中間データの誤り率を取得し、
前記配分部は、前記中間データに対応する前記誤り率を規定する要求内容に応じて、前

記中間データを前記第２鍵蒸留処理部にそれぞれ配分する請求項７に記載の量子鍵配送装置。
【請求項１０】
前記共通処理部は、
前記量子通信路を介して送信または受信した前記光子列に対応する光子ビット列を取得する量子鍵共有部と、
前記光子ビット列から、鍵蒸留処理によって生成した前記暗号鍵を前記中間データとして出力する鍵蒸留処理部と、
を含み、
前記１以上の個別処理部は、前記配分部により配分された前記中間データである前記暗号鍵を、アプリケーションに提供する鍵管理部をそれぞれ含む請求項１に記載の量子鍵配送装置。
【請求項１１】
前記共通処理部は、２以上の前記量子鍵共有部を含む請求項２、７および１０のうちいずれか一項に記載の量子鍵配送装置。
【請求項１２】
複数の量子鍵配送装置が、量子通信路で接続され、暗号鍵を共有する量子鍵配送システムであって、
前記複数の量子鍵配送装置は、
前記量子通信路を介して、他の量子鍵配送装置との間で光子列の送信または受信により取得したビット情報基づいて、中間データを出力する共通処理部と、
前記中間データに基づき前記暗号鍵を生成または提供する１以上の個別処理部と、
前記共通処理部で出力した前記中間データを前記１以上の個別処理部を含む２以上の配分先に配分する配分部と、
をそれぞれ備えた量子鍵配送システム。
【請求項１３】
複数の量子鍵配送装置が、量子通信路で接続され、暗号鍵を共有する量子鍵配送システムの量子鍵配送方法であって、
前記量子通信路を介して、他の量子鍵配送装置との間で光子列の送信または受信により取得したビット情報に基づいて、中間データを出力する共通処理ステップと、
１以上の個別処理部が、前記中間データに基づき前記暗号鍵を生成または提供する個別処理ステップと、
前記共通処理ステップで出力した前記中間データを前記１以上の個別処理部を含む２以上の配分先に配分する配分ステップと、
を有する量子鍵配送方法。
【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、量子鍵配送システム、および量子鍵配送方法に関する。
【背景技術】
【０００２】
量子鍵配送システムは、送信ノードと、受信ノードと、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。送信ノードは、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、単一光子を連続的に受信ノードに送信する。その後、送信ノードと受信ノードとが相互に制御情報を交換することによって、送信ノードと受信ノードとの間で安全に暗号鍵を共有する。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】
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、送信ノード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ノードは、盗聴者に光子を観測されたことを検出することができる。この結果、送信ノードで得られた光子列、および受信ノードで検出された光子列を基にして、送信ノードと受信ノードとの相互間で制御情報を交換することにより、最終的に安全な暗号鍵が得られる。

【０００４】

２つのノード（例えば、上述の送信ノードおよび受信ノード）は、共有された上述の暗号鍵を使用して暗号化および復号化を行い、ワンタイムパッドと呼ばれる暗号通信方式を利用して暗号データ通信を行う。ワンタイムパッドとは、データ１バイトを暗号鍵１バイトで暗号化して送信し、受信時には同じ１バイトの暗号鍵を利用して復号化し、一度利用した暗号鍵は破棄する暗号通信方式である。このワンタイムパッド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。このように、量子鍵配送により共有された安全な暗号鍵を用いて暗号データ通信を行う技術を量子暗号技術という。量子鍵配送および量子暗号技術は、このように非常に高いセキュリティ機能を提供するものである。

【０００５】

一方、量子鍵配送を実現するためには、上述のように、単一の光子を連続的に送受信するための光学素子等を高精度で制御する技術が必要となるため、そのコストは高くなる。また、送信ノードと受信ノードとの間を接続する光ファイバの敷設も必要となり、そのコストも高くなる。このようにコストが高い装置および設備を、小規模なアプリケーションまたは、量子鍵配送サービスまたは量子暗号サービスの複数の利用者向けに個別に設置および敷設することは、コストの面から困難になる。これに対応するための技術として、一式の量子鍵配送装置を用いて、複数のアプリケーション向けに暗号鍵を提供する運用方式を採用した技術が提案されている。

【０００６】

しかしながら、上述の技術では、一式の量子鍵配送装置によって生成され蓄積された暗号鍵を、複数のアプリケーションに割り当てるのみである。従って、低コストで複数種類の量子鍵配送を提供したり、複数の利用者ごとに異なる量子鍵配送および量子暗号技術に関する各種パラメータまたはアルゴリズム等のバリエーションを用いてそれぞれ異なる量子鍵配送または量子暗号機能を提供したり、複数の利用者に対して、各利用者の要求に応じた量子鍵配送または量子暗号機能を提供したりすることができないという問題がある。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】米国特許第７６４６８７３号明細書

【特許文献２】特開２０１４－５３８１６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、暗号鍵を利用する対象が個別に要求するパラメータまたはバリエーションに応じた量子鍵配送および量子暗号技術のサービスの提供を実現することができる量子鍵配送装置、量子鍵配送システム、および量子鍵配送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】

【０００９】

実施形態の量子鍵配送装置は、他の量子鍵配送装置と、量子通信路で接続され、暗号鍵を共有する量子鍵配送装置であって、共通処理部と、１以上の個別処理部と、配分部と、を備える。共通処理部は、量子通信路を介して他の量子鍵配送装置との間で光子列の送信または受信により取得したビット情報に基づいて中間データを出力する。個別処理部は、

中間データに基づき暗号鍵を生成または提供する。配分部は、共通処理部で出力した中間データを１以上の個別処理部を含む２以上の配分先に配分する。

【図面の簡単な説明】

【００１０】

【図１】量子鍵配送システムの全体構成の一例を示す図である。

【図２】ＱＫＤ装置のハードウェア構成の一例を示す図である。

【図３】一般的なＱＫＤ装置の機能ブロックの構成を示す図である。

【図４】一般的な暗号鍵の共有動作を示すシーケンス図である。

【図５】仮想ＱＫＤ装置の構成を概念的に説明する図である。

【図６】第１の実施形態に係るＱＫＤ装置の機能ブロックの構成を示す図である。

【図７】第１の実施形態に係るＱＫＤ装置の機能ブロックの構成を示す図である。

【図８】第２の実施形態に係るＱＫＤ装置の機能ブロックの構成を示す図である。

【図９】第３の実施形態に係るＱＫＤ装置の機能ブロックの構成を示す図である。

【図１０】第４の実施形態に係るＱＫＤ装置の機能ブロックの構成を示す図である。

【図１１】第５の実施形態に係るＱＫＤ装置の機能ブロックの構成を示す図である。

【図１２】第６の実施形態に係るＱＫＤ装置の機能ブロックの構成を示す図である。

【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、量子鍵配送システム、および量子鍵配送方法を詳細に説明する。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】

（第１の実施形態）

図１は、量子鍵配送システムの全体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、ＱＫＤ装置１（量子鍵配送装置）と、ＱＫＤ装置２（量子鍵配送装置）と、光ファイバリンク３と、通信ケーブル４と、含んで構成されている。

【００１４】

ＱＫＤ装置１は、レーザにより発生した、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、ＱＫＤ装置２へ送信する送信機である。ＱＫＤ装置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、鍵蒸留処理の際、ＱＫＤ装置１は、ＱＫＤ装置２との間で、通信ケーブル４を介して制御情報（単一光子ではなく一般のデジタルデータであり、以下、「鍵蒸留処理データ」と称する場合がある）の交換を行う。ここで、鍵蒸留処理データの他、後述するようにアプリケーション（後述の図６に示す鍵利用部１０６ａ～１０６ｃ、２０６ａ～２０６ｃ）が通信するデータの通信経路となる通信ケーブル４を、「古典通信路」と称する場合がある。なお、鍵蒸留処理データは、通信ケーブル４ではなく、ＱＫＤ装置１とＱＫＤ装置２との間の光ファイバリンク３を介して転送されてもよく、または、これ以外の通信経路（例えば、一般のインターネット回線等）を用いて転送されてもよい。

【００１５】

ＱＫＤ装置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、ＱＫＤ装置１から受信する受信機である。ＱＫＤ装置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、ＱＫＤ装置１が生成した暗号鍵と同一の暗号鍵を生成する。また、鍵蒸留処理の際、ＱＫＤ装置２は、ＱＫＤ装置１との間で、通信ケーブル４を介して制御情報（鍵蒸留処理データ）の交換を行う。

【００１６】

光ファイバリンク３は、ＱＫＤ装置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。通信ケーブル４は、ＱＫＤ装置１とＱＫＤ装置２との間で、鍵蒸留処理データの他、後述するようにアプリケーションの通信データを通信するために古典通信路として機能するケーブルである。

【００１７】

このようなＱＫＤ装置１とＱＫＤ装置２とを含む量子鍵配送システム１００においては、ＱＫＤ装置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ＱＫＤ装置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。

【００１８】

また、ＱＫＤ装置１、２の上述の光子の送受信処理、鍵蒸留処理、ならびに、後述する鍵管理（暗号鍵の管理）および鍵利用（暗号鍵の利用）においては、設定項目等についての複数のパラメータ、または、アルゴリズムの選択等の動作についての複数のバリエーションが存在する。そして、それぞれのアプリケーションの要求、サービスレベルアグリーメント、またはアプリケーションの実施形態に応じて、これらのパラメータおよびバリエーションを適切に選択すべき場合がある。ここで、サービスレベルアグリーメントとは、物理的なＱＫＤ装置を保有し、量子鍵配送のサービスまたは量子暗号機能のサービスを提供する提供者の立場からは、サービスの利用者に対し、何らかの条件を持って提供するサービスの品質を定義するものをいう。例えば、可用性および利用料金等に関する規定等が代表的である。量子鍵配送のサービスまたは量子暗号機能のサービスの観点からは、鍵生成速度、提供する暗号鍵の中間データの誤り率、速度・誤り率・基底偏り・レーザ強度の分散等が挙げられる。これらに対する条件規定がサービスレベルアグリーメントとなり得る。一方、物理ＱＫＤ装置を保有せず、本実施形態の量子鍵配送のサービスまたは量子暗号機能のサービスの利用者の立場からは、あるサービスを利用する上で、様々な選択肢（パラメータおよびバリエーションの組み合わせ）があり得る。サービスの運用可能性および運用コスト等の観点から、量子鍵配送および量子暗号機能についてのパラメータ・バリエーションを選択することが考えられる。量子鍵配送および量子暗号機能の具体的な処理である光子の送受信処理、鍵蒸留処理、鍵管理および鍵利用におけるパラメータおよびバリエーションについての詳細は、後述する。

【００１９】

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２を参照しながら、ＱＫＤ装置１、２のハードウェア構成について説明する。なお、以下では、ＱＫＤ装置１を例にして説明をする。

【００２０】

図２に示すように、ＱＫＤ装置１は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）３０１と、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）３０２と、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）３０３と、通信Ｉ／Ｆ３０４と、補助記憶装置３０５と、光学処理装置３０６と、を備えている。

【００２１】

ＣＰＵ３０１は、ＱＫＤ装置１全体の動作を制御する演算装置である。ＲＯＭ３０２は、ＣＰＵ３０１が各機能を制御するために実行するＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ／Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）またはファームウェア等のプログラムを記憶する不揮発性記憶装置である。ＲＡＭ３０３は、ＣＰＵ３０１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。

【００２２】

通信Ｉ／Ｆ３０４は、古典通信路（通信ケーブル４等）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／Ｆ３０４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ってもよく、または、光ファイバ用インターフェースであってもよい。

【００２３】
補助記憶装置３０５は、ＣＰＵ３０１で実行される各種プログラム、ならびに暗号鍵の共有動作（量子鍵配送）の過程で生成した中間データおよび暗号鍵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３０５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。
【００２４】
光学処理装置３０６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。ＱＫＤ装置１の光学処理装置３０６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）を基に、例えば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、ＱＫＤ装置２の光学処理装置３０６に送信する。すなわち、ＱＫＤ装置１の光学処理装置３０６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。ＱＫＤ装置２の光学処理装置３０６は、量子通信路を介して、ＱＫＤ装置１の光学処理装置３０６から光子列を受信し、受信した光子列を、例えば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。
【００２５】
上述のＣＰＵ３０１、ＲＯＭ３０２、ＲＡＭ３０３、通信Ｉ／Ｆ３０４、補助記憶装置３０５、および光学処理装置３０６は、アドレスバスおよびデータバス等のバス３０７によって互いに通信可能に接続されている。
【００２６】
図３は、一般的な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、一般的な量子鍵配送システム（量子鍵配送システム５００）のＱＫＤ装置（ＱＫＤ装置１０、２０）の機能ブロックの構成について説明する。
【００２７】
図３に示すように、ＱＫＤ装置１０は、量子鍵共有部１１と、シフティング処理部１２と、誤り訂正処理部１３と、秘匿性増強処理部１４と、鍵管理部１５と、鍵利用部１６と、通信部１７と、記憶部１８と、を有する。
【００２８】
量子鍵共有部１１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を基に、例えばランダムに選択した基底により生成した基底情報（送信基底）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、ＱＫＤ装置２０の量子鍵共有部２１に送信する光子送信処理を行う機能部である。量子鍵共有部１１は、発生させた光子ビット列および送信基底（これらを含む情報を「送信光子情報」という場合がある）を記憶部１８に記憶させる。量子鍵共有部１１は、生成した送信基底および光子ビット列を、シフティング処理部１２に送る。なお、量子鍵共有部１１は、後述するように、古典通信路を介して、量子鍵共有部２１から受信した、量子鍵共有部２１が光子を検出した時刻を示す情報に基づいて、光子ビット列から検出した光子に対応するビット情報を抽出し、これを新たに光子ビット列とするものとしてもよい。
【００２９】
量子鍵共有部１１による単一光子の発生源として、レーザ光源を減衰させたものを用いることが可能である。この場合、光子送信処理において、レーザ光源の強度、減衰率、およびその分散等がパラメータとなる。また、量子鍵共有部１１による単一光子の発生源としてレーザ光源を用いる場合、送信基底により光子ビット列の情報を光子列にエンコードする際、厳密には単一光子ではなく、複数の光子が送出される場合がある。このような場合を排除し、量子鍵配送の安全性を保証するため、デコイ法と呼ばれる方法が用いられる。デコイ法では、レーザ光源の出力の強度を、常に一定とするのではなく、ある一定の確率で、通常のビットを送信するための出力の強度とは異なる強度のパルスで光子を送信する。この通常の出力の強度とは異なる強度で送信されるパルスとして、デコイパルスとバ

キュームパルスとが存在する。この場合、光子送信処理において、デコイパルスまたはバキュームパルスを送信する際のレーザの出力強度、および送信する頻度（確率）等もパラメータとなる。

【００３０】

さらに、量子鍵共有部１１による送信基底の選択、および後述する量子鍵共有部２１による受信基底の選択において、基本的には２種類の基底を５０：５０の割合でランダムに選択する方法があるが、より効率的に量子鍵配送を行うために、この割合に傾斜をつける「Ｅｆｆｉｃｉｅｎｔ　ＢＢ８４」という方法も知られている。この場合、光子送信処理において、どちらの基底を選択するかの割合もパラメータとなる。

【００３１】

シフティング処理部１２は、ＱＫＤ装置２０の量子鍵共有部２１が生成した基底情報（受信基底）を、ＱＫＤ装置２０から古典通信路を介して受信し、受信した受信基底と、記憶部１８に記憶された送信基底とを比較して、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。シフティング処理部１２は、生成した共有ビット列を、誤り訂正処理部１３に送る。

【００３２】

シフティング処理で生成された共有ビット列には、光子の送受信の際に、光ファイバ上のノイズ、ＱＫＤ装置２０の量子鍵共有部２１の光子検出器特性に起因するノイズ、または盗聴者による盗聴の痕跡等が含まれるため、シフティング処理部１２が生成する共有ビット列と、後述するシフティング処理部２２が生成する共有ビット列とは、一部ビットが異なっている場合がある。この共有ビット列が誤っている程度（確率）を誤り率と呼ぶ。誤り率は、例えば、光ファイバの振動または温度変化等によっても変動する。ここで、シフティング処理では、後述する誤り訂正処理で利用するために、推定誤り率を算出するものとしてもよい。推定誤り率とは、例えば、ＱＫＤ装置２０からＱＫＤ装置１０へ、共有ビット列の一部のビット情報を送信し、ＱＫＤ装置２０から受信したビット情報と、ＱＫＤ装置１０で生成した共有ビット列の対応するビット情報とを比較することにより、共有ビット列に含まれていると推定される誤りの程度を示す割合である。なお、共有ビット列の一部のビット情報は、ＱＫＤ装置１０からＱＫＤ装置２０へ送信するものとしてもよい。この場合、シフティング処理において、推定誤り率を算出するために利用する共有ビット列のうちのビット情報の量がパラメータとなる。

【００３３】

誤り訂正処理部１３は、古典通信路を介して、ＱＫＤ装置２０の誤り訂正処理部２３と誤り訂正用制御情報（ＥＣ（Ｅｒｒｏｒ　Ｃｏｒｒｅｃｔｉｏｎ：誤り訂正）情報）を交換することにより、生成し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機能部である。誤り訂正処理部１３は、生成した訂正後ビット列を、秘匿性増強処理部１４へ送る。この結果、誤り訂正処理部１３により生成された訂正後ビット列、および、後述する誤り訂正処理部２３による誤り訂正処理により生成された訂正後ビット列は、完全に一致するビット列となる。

【００３４】

誤り訂正処理を行うためには、ｃａｓｃａｄｅ、またはＬＤＰＣ（Ｌｏｗ　Ｄｅｎｓｉｔｙ　Ｐａｒｉｔｙ－Ｃｈｅｃｋ）等の様々なアルゴリズムのバリエーションがある。また、各バリエーションの誤り訂正処理において、入力される共有ビット列の処理単位、および選択する誤り訂正符号等のパラメータが存在する。

【００３５】

例えば、誤り訂正処理のアルゴリズムとしてＬＤＰＣを用いる場合、ＱＫＤ装置１０とＱＫＤ装置２０との間では、予め合意する誤り訂正符号を共有している。誤り訂正処理部１３は、訂正後ビット列から、誤り訂正符号を用いてシンドロームデータを誤り訂正用制御情報として生成し、これを古典通信路を介して、ＱＫＤ装置２０に送信する。後述するように、ＱＫＤ装置２０の誤り訂正処理部２３は、ＱＫＤ装置１０から受信した誤り訂正用制御情報を用いて、訂正後ビット列を生成する。

【００３６】
ここで、誤り訂正符号には、誤り訂正能力、および効率性というパラメータが存在する。誤り訂正能力が低い誤り訂正符号は、誤り率の低い共有ビット列を効率的に訂正することができる（効率性が良い）が、誤り率の高い共有ビット列については訂正することができず、誤り訂正処理に失敗し、この場合、誤り訂正処理の対象の共有ビット列を破棄することになる。一方、誤り訂正能力の高い誤り訂正符号は、誤り率の高い共有ビット列であっても訂正することが可能だが、通信するシンドロームデータサイズが大きくなり、最終的に得られる暗号鍵のサイズが小さくなってしまう（効率性が悪い）。このようなことから、誤り訂正処理においては、上述のシフティング処理において算出された共有ビット列についての推定誤り率を参照し、これに応じて誤り訂正符号を選択する方法を利用してもよい。ただし、多くの誤り訂正符号を切り替えて利用するためにはオーバヘッドがあり、同時に推定誤り率自体の精度も保証されない可能性がある。このように、誤り訂正処理の動作においては、どのような特性を持った誤り訂正符号を用いるか、どの程度までの誤り率を訂正できるようにするか、どの程度の確率の誤り訂正の失敗を許容するか、どの程度の効率性を重視するか、および、誤り訂正処理が失敗した場合にどのような動作を行うか等のバリエーションがある。

【００３７】
誤り訂正処理におけるその他のバリエーションとしては、どの程度の処理速度とするか（ソフトウェアのみで処理するか、専用のハードウェア等を搭載して高速に処理するか）、ＱＫＤ装置１０とＱＫＤ装置２０との間の通信方式およびフォーマットをどのようにするか（どのような通信プロトコルで通信するか、通信自体を暗号化するかどうか、どのような方法でデータ認証するか）等がある。

【００３８】
秘匿性増強処理部１４は、古典通信路を介して、ＱＫＤ装置２０の秘匿性増強処理部２４から制御情報（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、生成した訂正後ビット列に対して、誤り訂正処理により訂正した誤りの数から、光子送信処理、シフティング処理、および誤り訂正処理で理論上、漏洩して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。秘匿性増強処理部１４は、生成した暗号鍵を、記憶部１８に記憶させて蓄積させる。

【００３９】
秘匿性増強処理部１４は、秘匿性増強処理として、例えば、まず、公知の量子暗号理論に基づき、訂正後ビット列を何ビットの暗号鍵まで圧縮するかを計算する鍵長計算を行う。そして、秘匿性増強処理部１４は、鍵長計算によって求められたビット長の暗号鍵を生成するため鍵の圧縮を行い、暗号鍵を生成する。

【００４０】
秘匿性増強処理についても、量子暗号理論に基づく様々なアルゴリズムのバリエーションがある。例えば、ユニバーサルハッシュ関数を用いたハッシュ演算によるアルゴリズムもバリエーションの１つである。この場合、ハッシュ関数自体のパラメータも、秘匿性増強処理におけるパラメータとなる。このハッシュ関数自体のパラメータは、事前にＱＫＤ装置１０およびＱＫＤ装置２０に設定しておいてもよく、ＱＫＤ装置１０からＱＫＤ装置２０に、または、ＱＫＤ装置２０からＱＫＤ装置１０に送信してこれを更新するものとしてもよい。このようなハッシュ関数を用いた秘匿性増強処理において、どのようにハッシュ関数の更新をするかについてのバリエーションがあり、ハッシュ関数の更新期間はパラメータとなる。

【００４１】
秘匿性増強処理におけるその他のバリエーションとしては、どの程度の処理速度とするか（ソフトウェアのみで処理するか、専用のハードウェア等を搭載して高速に処理するか）、ＱＫＤ装置１０とＱＫＤ装置２０との間の通信方式およびフォーマットをどのようにするか（どのような通信プロトコルで通信するか、通信自体を暗号化するかどうか、どの

ような方法でデータ認証するか）等がある。

【００４２】

鍵管理部１５は、記憶部１８に記憶（蓄積）された暗号鍵の管理（鍵管理）を行う機能部である。また、鍵管理部１５は、記憶部１８に記憶された暗号鍵を、暗号データ通信を行うアプリケーション等である鍵利用部１６へ提供する。

【００４３】

どのような形態で鍵管理をするかについては、暗号鍵を蓄積する単位を所定の固定長とするか、秘匿性増強処理により生成されたままの長さとするか、これらの暗号鍵の蓄積単位毎にどのような鍵ＩＤを付与するのか、および、どのように暗号鍵の生成時刻を管理するか等のバリエーションがある。また、暗号鍵の蓄積（記憶）の実装形態については、暗号鍵をバイナリ形式とするかテキスト形式とするか、および、暗号鍵の記憶態様としてファイルシステムを利用するかデータベースを利用するか、のバリエーションがある。その他、どの程度の記憶容量のサイズとするか、および、暗号鍵が記憶できない場合はどのような挙動とするか等のバリエーションもある。

【００４４】

また、暗号鍵をワンタイムパッドで利用することを前提として、ＱＫＤ装置１０からＱＫＤ装置２０への暗号データ通信用の暗号鍵と、ＱＫＤ装置２０からＱＫＤ装置１０への暗号データ通信用の暗号鍵と、を分けて記憶するか否か、および、複数のアプリケーションが暗号鍵を利用する場合、これらのアプリケーション毎に分けて記憶するか否か等もバリエーションとして考えられる。また、暗号鍵の提供に関して、アプリケーションに対してどのようなインターフェースで暗号鍵を提供するかについても、様々なバリエーションが考えられる。例えば、アプリケーションに対して暗号鍵を提供するストリームインターフェースを提供する方法、専用言語のＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍ Ｉｎｔｅｒｆａｃｅ）を用意する方法、および、暗号鍵をレスポンスとして送信するＨＴＭＬ（ＨｙｐｅｒＴｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）ベースのＡＰＩを用意する方法等もバリエーションである。このとき、複数のアプリケーションに対する暗号鍵の提供をどのように実現するか、もしくは実現しないか、暗号鍵を提供するアプリケーションをどのように認証・認可・課金・ログ管理するか、ならびに、暗号鍵の生成が間に合わない場合の関連するフロー制御をどのように実現するか等もバリエーションである。

【００４５】

鍵利用部１６は、鍵管理部１５から提供された暗号鍵を利用（鍵利用）して、暗号データ通信を行うアプリケーション等である。

【００４６】

鍵利用部１６の暗号鍵の利用方法について、例えば、暗号鍵をワンタイムパッドの暗号化に利用するか、もしくはＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）の暗号化に利用するか等の暗号化のアルゴリズムに関するバリエーションがある。その他、データ認証機能を利用するか否か、および、どのような認証アルゴリズムを利用するか等のようなバリエーションもある。また、ＡＥＳのようなブロック暗号については、何ビットの鍵長を用いるか、および、どのような頻度で暗号鍵を更新するか等もバリエーションとなる。これらのバリエーションは、アプリケーションに求められるセキュリティの強度、または、セキュリティの機能（認証が必要か否か等）によって選択すべきものである。

【００４７】

なお、これらの鍵利用の機能は、アプリケーションそのものの一部として実装する方法に加え、これらの機能を提供するライブラリとして実装する方法もある。ライブラリとして実装する場合、どのような関数を上位プログラムに提供するか、および、どのような言語のプログラム向けに提供するか等のようなライブラリインタフェースのデザインについても複数のバリエーションが考えられる。

【００４８】

通信部１７は、古典通信路を介して、ＱＫＤ装置２０とデータを通信する機能部である

。
【００４９】
記憶部１８は、秘匿性増強処理部１４により生成された暗号鍵を蓄積（記憶）する機能部である。
【００５０】
図３に示すように、ＱＫＤ装置２０は、量子鍵共有部２１と、シフティング処理部２２と、誤り訂正処理部２３と、秘匿性増強処理部２４と、鍵管理部２５と、鍵利用部２６と、通信部２７と、記憶部２８と、を有する。
【００５１】
量子鍵共有部２１は、量子通信路を介して、ＱＫＤ装置１０の量子鍵共有部１１から光子列を検出する光子検出処理を行い、検出した光子列を、例えばランダムに選択した基底により生成した基底情報（受信基底）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。量子鍵共有部２１は、光子ビット列および受信基底（これらを含む情報を「検出光子情報」という場合がある）を記憶部２８に記憶させる。量子鍵共有部２１は、生成した受信情報および光子ビット列を、シフティング処理部２２に送る。なお、量子鍵共有部２１は、量子通信路を介して量子鍵共有部１１から送信された光子を検出した時刻を示す情報を、検出光子情報に含めるものとしてもよい。この場合、量子鍵共有部２１は、古典通信路を介して、この時刻を示す情報を量子鍵共有部１１に送信するものとしてもよい。また、上述の量子鍵共有部１１による光子送信処理、および量子鍵共有部２１による光子検出処理を総称して、以下「光子送受信処理」という場合があるものとする。
【００５２】
シフティング処理部２２は、ＱＫＤ装置１０の量子鍵共有部１１が生成した基底情報（送信基底）を、ＱＫＤ装置１０から古典通信路を介して受信し、受信した送信基底と、記憶部２８に記憶された受信基底とを比較して、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。シフティング処理部２２は、生成した共有ビット列を、誤り訂正処理部２３に送る。
【００５３】
誤り訂正処理部２３は、古典通信路を介して、ＱＫＤ装置１０の誤り訂正処理部１３と誤り訂正用制御情報（ＥＣ情報）を交換することにより、生成し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機能部である。誤り訂正処理部２３は、生成した訂正後ビット列を、秘匿性増強処理部２４へ送る。この結果、誤り訂正処理部２３により生成された訂正後ビット列、および、上述した誤り訂正処理部１３による誤り訂正処理により生成された訂正後ビット列は、完全に一致するビット列となる。
【００５４】
例えば、上述のように、誤り訂正処理のアルゴリズムとしてＬＤＰＣを用いる場合、誤り訂正処理部２３は、古典通信路を介してＱＫＤ装置１０から受信した誤り訂正用制御情報、および共有ビット列を基に、誤り訂正符号を用いて、訂正後ビット列を生成する。
【００５５】
秘匿性増強処理部２４は、古典通信路を介して、制御情報（ＰＡ情報）を生成してＱＫＤ装置１０の秘匿性増強処理部１４に送信し、このＰＡ情報に基づいて、生成した訂正後ビット列に対して、誤り訂正処理により訂正した誤りの数から、光子送信処理、シフティング処理、および誤り訂正処理で理論上、漏洩して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。秘匿性増強処理部２４は、生成した暗号鍵を、記憶部２８に記憶させて蓄積させる。秘匿性増強処理の具体的な処理内容は、上述の秘匿性増強処理部１４と同様である。
【００５６】
鍵管理部２５は、記憶部２８に記憶（蓄積）された暗号鍵を管理（鍵管理）する機能部である。また、鍵管理部２５は、記憶部２８に記憶された暗号鍵を、暗号データ通信を行

うアプリケーション等である鍵利用部２６へ提供する。
【００５７】
鍵利用部２６は、鍵管理部２５から提供された暗号鍵を利用（鍵利用）して、暗号データ通信を行うアプリケーション等である。
【００５８】
通信部２７は、古典通信路を介して、ＱＫＤ装置１０とデータを通信する機能部である。
【００５９】
記憶部２８は、秘匿性増強処理部２４により生成された暗号鍵を蓄積（記憶）する機能部である。
【００６０】
量子鍵共有部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、鍵管理部２５および鍵利用部２６の機能および動作についてのパラメータおよびバリエーションについては、ＱＫＤ装置１０について上述した通りである。
【００６１】
図４は、一般的な量子鍵配送システムの暗号鍵の共有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、一般的な暗号鍵の共有動作（量子鍵配送）を含めた量子暗号機能の動作の流れを総括的に説明する。
【００６２】
＜ステップＳ１１＞
量子鍵共有部１１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を基に、例えばランダムに選択した基底により生成した基底情報（送信基底）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、ＱＫＤ装置２０の量子鍵共有部２１に送信する光子送信処理を行う。量子鍵共有部１１は、発生させた光子ビット列および送信基底（送信光子情報）を記憶部１８に記憶させる。量子鍵共有部１１は、生成した送信基底および光子ビット列を、シフティング処理部１２に送る。
【００６３】
＜ステップＳ１２＞
量子鍵共有部２１は、量子通信路を介して、ＱＫＤ装置１０の量子鍵共有部１１から光子列を検出する光子検出処理を行い、検出した光子列を、例えばランダムに選択した基底により生成した基底情報（受信基底）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。量子鍵共有部２１は、光子ビット列および受信基底（検出光子情報）を記憶部２８に記憶させる。量子鍵共有部２１は、生成した受信情報および光子ビット列を、シフティング処理部２２に送る。
【００６４】
＜ステップＳ１３＞
シフティング処理部１２は、ＱＫＤ装置２０の量子鍵共有部２１が生成した基底情報（受信基底）を、ＱＫＤ装置２０から古典通信路を介して受信し、受信した受信基底と、記憶部１８に記憶された送信基底とを比較して、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１２は、生成した共有ビット列を、誤り訂正処理部１３に送る。
【００６５】
＜ステップＳ１４＞
シフティング処理部２２は、ＱＫＤ装置１０の量子鍵共有部１１が生成した基底情報（送信基底）を、ＱＫＤ装置１０から古典通信路を介して受信し、受信した送信基底と、記憶部２８に記憶された受信基底とを比較して、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２２は、生成した共有ビット列を、誤り訂正処理部２３に送る。
【００６６】

＜ステップＳ１５＞
誤り訂正処理部１３は、古典通信路を介して、ＱＫＤ装置２０の誤り訂正処理部２３と誤り訂正用制御情報（ＥＣ情報）を交換することにより、生成し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１３は、生成した訂正後ビット列を、秘匿性増強処理部１４へ送る。
【００６７】
＜ステップＳ１６＞
誤り訂正処理部２３は、古典通信路を介して、ＱＫＤ装置１０の誤り訂正処理部１３と誤り訂正用制御情報（ＥＣ情報）を交換することにより、生成し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２３は、生成した訂正後ビット列を、秘匿性増強処理部２４へ送る。この結果、誤り訂正処理部２３により生成された訂正後ビット列、および、上述した誤り訂正処理部１３による誤り訂正処理により生成された訂正後ビット列は、完全に一致するビット列となる。
【００６８】
＜ステップＳ１７＞
秘匿性増強処理部１４は、古典通信路を介して、ＱＫＤ装置２０の秘匿性増強処理部２４から制御情報（ＰＡ情報）を受信して、このＰＡ情報に基づいて、生成した訂正後ビット列に対して、誤り訂正処理により訂正した誤りの数から、光子送信処理、シフティング処理、および誤り訂正処理で理論上、漏洩して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１４は、生成した暗号鍵を、記憶部１８に記憶させて蓄積させる。
【００６９】
＜ステップＳ１８＞
秘匿性増強処理部２４は、古典通信路を介して、制御情報（ＰＡ情報）を生成してＱＫＤ装置１０の秘匿性増強処理部１４に送信し、このＰＡ情報に基づいて、生成した訂正後ビット列に対して、誤り訂正処理により訂正した誤りの数から、光子送信処理、シフティング処理、および誤り訂正処理で理論上、漏洩して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２４は、生成した暗号鍵を、記憶部２８に記憶させて蓄積させる。
【００７０】
＜ステップＳ１９＞
鍵管理部１５は、記憶部１８に記憶（蓄積）された暗号鍵の管理（鍵管理）を行う。また、鍵管理部１５は、記憶部１８に記憶された暗号鍵を、暗号データ通信を行うアプリケーション等である鍵利用部１６へ提供する。
【００７１】
＜ステップＳ２０＞
鍵管理部２５は、記憶部２８に記憶（蓄積）された暗号鍵を管理する。また、鍵管理部２５は、記憶部２８に記憶された暗号鍵を、暗号データ通信を行うアプリケーション等である鍵利用部２６へ提供する。
【００７２】
＜ステップＳ２１＞
鍵利用部１６は、鍵管理部１５から提供された暗号鍵を利用（鍵利用）して、暗号データ通信を行う。
【００７３】
＜ステップＳ２２＞
鍵利用部２６は、鍵管理部２５から提供された暗号鍵を利用（鍵利用）して、暗号データ通信を行う。
【００７４】
以上のような動作によって、ＱＫＤ装置１０およびＱＫＤ装置２０において、一致する暗号鍵が生成される。上述の動作を繰り返し実行することによって、相互に一致する暗号

鍵を連続して生成し続けることができる。

【００７５】

図５は、仮想ＱＫＤ装置の構成を概念的に説明する図である。図５を参照しながら、量子鍵配送および量子暗号機能の仮想化について説明する。

【００７６】

図５に示すように、２拠点（ＱＫＤ装置１およびＱＫＤ装置２がそれぞれ設置された拠点）を接続する１組のＱＫＤ装置が存在する。この１組のＱＫＤ装置を含む量子鍵配送システム１００は、一方の拠点に存在するＱＫＤ装置１（物理ＱＫＤ装置）と、他方の拠点に存在するＱＫＤ装置２（物理ＱＫＤ装置）と、２つの物理ＱＫＤ装置間を量子通信路として接続する光ファイバリンク３（図１参照）と、２つの物理ＱＫＤ装置間を古典通信路として接続する通信ケーブル４（図１参照）と、を含んで構成されている。ここで、物理的なＱＫＤ装置としては、１組（ＱＫＤ装置１、２）のみであるが、図５に示す例では、３つの異なる企業（企業Ａ～Ｃ）が、仮想的に専用のＱＫＤ装置の組を持っているかのように見せかけている。すなわち、１組のＱＫＤ装置を仮想化し、それぞれ３組のＱＫＤ装置（仮想ＱＫＤ装置）として各企業が仮想的に専有している状態である。具体的には、図５に示すように、企業Ａは、ＱＫＤ装置１を仮想化した仮想ＱＫＤ装置Ａ１と、ＱＫＤ装置２を仮想化した仮想ＱＫＤ装置Ａ２と、を専有している。また、企業Ｂは、ＱＫＤ装置１を仮想化した仮想ＱＫＤ装置Ｂ１と、ＱＫＤ装置２を仮想化した仮想ＱＫＤ装置Ｂ２と、を専有している。また、企業Ｃは、ＱＫＤ装置１を仮想化した仮想ＱＫＤ装置Ｃ１と、ＱＫＤ装置２を仮想化した仮想ＱＫＤ装置Ｃ２と、を専有している。

【００７７】

各企業は、それぞれの要求、ポリシー、またはＱＫＤ装置の提供者と合意するサービスレベルアグリーメント（以下、総括的に「要求内容」という場合がある）に応じて、仮想的に専有したＱＫＤ装置（仮想ＱＫＤ装置）を運用する。そして、各企業の仮想ＱＫＤ装置は、各要求内容に応じて異なるパラメータおよび異なるバリエーションによって、量子鍵配送および量子暗号機能に基づく動作を見かけ上実行する。

【００７８】

なお、図５に示す例では、仮想化されたＱＫＤ装置は、企業Ａ～Ｃの３つの企業に対して設定されているが、これに限定されるものではなく、その他の数の企業ごとにＱＫＤ装置を仮想化するものとしてもよい。以下、説明の簡略化のために、ＱＫＤ装置１、２が企業Ａ～Ｃの３つの企業に対して仮想化された場合について説明する。

【００７９】

図６は、第１の実施形態に係るＱＫＤ装置の機能ブロックの構成の一例を示す図である。図６を参照しながら、本実施形態に係るＱＫＤ装置（ＱＫＤ装置１、２）の機能ブロックの構成について説明する。なお、図３および４で説明した一般的なＱＫＤ装置の機能ブロック構成および暗号鍵の共有動作と相違する点を中心に説明する。

【００８０】

図６に示すように、量子鍵配送を含む量子暗号機能の動作における各処理のうち、光子送受信処理については、ＱＫＤ装置１、２は、物理的なＱＫＤ装置として通常通り実行する。一方、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）、鍵管理、および鍵利用については、ＱＫＤ装置１、２は、企業Ａ～Ｃに対してそれぞれ仮想化された仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２として、異なるパラメータおよび異なるバリエーションでそれぞれ独立に実行する。ここで、シフティング処理、誤り訂正処理、秘匿性増強処理、鍵管理、および鍵利用それぞれにおいて、どのようなパラメータおよびバリエーションがあるかについては、図３で上述した通りである。これらのパラメータおよびバリエーションは、仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２それぞれの運用者の要求内容に基づいて選択されている。

【００８１】

図６に示すように、ＱＫＤ装置１は、量子鍵共有部１０１と、シフティング処理部１０

２ａ～１０２ｃと、誤り訂正処理部１０３ａ～１０３ｃと、秘匿性増強処理部１０４ａ～１０４ｃと、鍵管理部１０５ａ～１０５ｃと、鍵利用部１０６ａ～１０６ｃと、配分部１０７と、設定部１０８と、通信部１０９と、記憶部１１０と、を有する。

【００８２】

量子鍵共有部１０１、通信部１０９および記憶部１１０は、それぞれ図３で上述した量子鍵共有部１１、通信部１７および記憶部１８と同様の機能を担う機能部である。量子鍵共有部１０１は、図２に示す光学処理装置３０６によって実現される。通信部１０９は、図２に示す通信Ｉ／Ｆ３０４によって実現される。記憶部１１０は、図２に示す補助記憶装置３０５によって実現される。

【００８３】

シフティング処理部１０２ａ～１０２ｃは、それぞれ、基本的なシフティング処理として、図３で上述したシフティング処理部１２と同様の機能を担う機能部である。シフティング処理部１０２ａ～１０２ｃは、それぞれ、企業Ａ～Ｃの要求内容に基づいて設定部１０８により設定されたシフティング処理用のパラメータおよびバリエーションに従って動作する。

【００８４】

誤り訂正処理部１０３ａ～１０３ｃは、それぞれ、基本的な誤り訂正処理として、図３で上述した誤り訂正処理部１３と同様の機能を担う機能部である。誤り訂正処理部１０３ａ～１０３ｃは、それぞれ、企業Ａ～Ｃの要求内容に基づいて設定部１０８により設定された誤り訂正処理用のパラメータおよびバリエーションに従って動作する。

【００８５】

秘匿性増強処理部１０４ａ～１０４ｃは、それぞれ、基本的な秘匿性増強処理として、図３で上述した秘匿性増強処理部１４と同様の機能を担う機能部である。秘匿性増強処理部１０４ａ～１０４ｃは、それぞれ、企業Ａ～Ｃの要求内容に基づいて設定部１０８により設定された秘匿性増強処理用のパラメータおよびバリエーションに従って動作する。

【００８６】

鍵管理部１０５ａ～１０５ｃは、それぞれ、図３で上述した鍵管理部１５と同様の鍵管理の機能を担う機能部である。鍵管理部１０５ａ～１０５ｃは、それぞれ、企業Ａ～Ｃの要求内容に基づいて設定部１０８により設定された鍵管理用のパラメータおよびバリエーションに従って動作する。

【００８７】

鍵利用部１０６ａ～１０６ｃは、それぞれ、図３で上述した鍵利用部１６と同様の鍵利用の機能を担う機能部である。鍵利用部１０６ａ～１０６ｃは、それぞれ、企業Ａ～Ｃの要求内容に基づいて設定部１０８により設定された鍵利用用のパラメータおよびバリエーションに従って動作する。

【００８８】

設定部１０８は、企業Ａ～Ｃそれぞれの要求内容に応じて、シフティング処理、誤り訂正処理、秘匿性増強処理、鍵管理および鍵利用のパラメータおよびバリエーションをそれぞれ設定する機能部である。

【００８９】

配分部１０７は、量子鍵共有部１０１および量子鍵共有部２０１による光子送受信処理により生成される中間データである送信光子情報（送信基底および光子ビット列）を、シフティング処理部１０２ａ～１０２ｃに配分する機能部である。配分部１０７は、企業Ａ～Ｃそれぞれの要求内容に応じて、シフティング処理部１０２ａ～１０２ｃそれぞれに配分する送信光子情報の配分量を決定する。

【００９０】

例えば、最も単純な送信光子情報の配分方法は、送信光子情報をシフティング処理部１０２ａ～１０２ｃそれぞれに等分する方法である。また、配分部１０７は、企業Ａ～Ｃそれぞれが要求する鍵生成速度（秘匿性増強処理部１４により暗号鍵が生成される速度）に応じて、傾斜をつけて送信光子情報を配分するものとしてもよい。例えば、企業Ａの鍵生

成速度に対する要求が、企業Ｂ、Ｃの要求の２倍である場合、配分部１０７は、送信光子情報の配分比が、企業Ａ：企業Ｂ：企業Ｃ＝２：１：１となるように配分するものとしてもよい。この場合、企業Ａ～Ｃそれぞれに関連付けられた優先度を考慮してもよい。

【００９１】

さらに、配分部１０７によるシフティング処理部１０２ａ～１０２ｃに対する送信光子情報の配分量の決定の基準としては、基底の偏り、デコイパルスおよびバキュームパルスの割合、それらの分散、およびレーザ強度の分散等がある。基底の偏りについては、仮想ＱＫＤ装置毎に企業等が要求する基底の偏りが異なることが考えられる。デコイパルスおよびバキュームパルスの割合については、仮想ＱＫＤ装置毎に企業等が要求するデコイパルスおよびバキュームパルスの割合が異なることが考えられる。デコイパルスおよびバキュームパルスの分散については、この分散に対する許容度が、企業等が専有する仮想ＱＫＤ装置毎に異なることが考えられる。レーザ強度の分散については、この分散に対する許容度が、企業等が専有する仮想ＱＫＤ装置毎に異なることが考えられる。

【００９２】

上述のシフティング処理部１０２ａ～１０２ｃ、誤り訂正処理部１０３ａ～１０３ｃ、秘匿性増強処理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、鍵利用部１０６ａ～１０６ｃ、配分部１０７、および設定部１０８は、図２に示すＣＰＵ３０１が補助記憶装置３０５等に記憶されたプログラムをＲＡＭ３０３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１０２ａ～１０２ｃ、誤り訂正処理部１０３ａ～１０３ｃ、秘匿性増強処理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、鍵利用部１０６ａ～１０６ｃ、配分部１０７、および設定部１０８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。

【００９３】

なお、図６に示す量子鍵共有部１０１、シフティング処理部１０２ａ～１０２ｃ、誤り訂正処理部１０３ａ～１０３ｃ、秘匿性増強処理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、鍵利用部１０６ａ～１０６ｃ、配分部１０７、設定部１０８、通信部１０９、および記憶部１１０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６に示すＱＫＤ装置１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６に示すＱＫＤ装置１で、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。

【００９４】

図６に示すように、ＱＫＤ装置２は、量子鍵共有部２０１と、シフティング処理部２０２ａ～２０２ｃと、誤り訂正処理部２０３ａ～２０３ｃと、秘匿性増強処理部２０４ａ～２０４ｃと、鍵管理部２０５ａ～２０５ｃと、鍵利用部２０６ａ～２０６ｃと、配分部２０７と、設定部２０８と、通信部２０９と、記憶部２１０と、を有する。

【００９５】

量子鍵共有部２０１、通信部２０９および記憶部２１０は、それぞれ図３で上述した量子鍵共有部２１、通信部２７および記憶部２８と同様の機能を担う機能部である。量子鍵共有部２０１は、図２に示す光学処理装置３０６によって実現される。通信部２０９は、図２に示す通信Ｉ／Ｆ３０４によって実現される。記憶部２１０は、図２に示す補助記憶装置３０５によって実現される。

【００９６】

シフティング処理部２０２ａ～２０２ｃは、それぞれ、基本的なシフティング処理として、図３で上述したシフティング処理部２２と同様の機能を担う機能部である。シフティング処理部２０２ａ～２０２ｃは、それぞれ、企業Ａ～Ｃの要求内容に基づいて設定部２０８により設定されたシフティング処理用のパラメータおよびバリエーションに従って動

作する。
【００９７】
誤り訂正処理部２０３ａ～２０３ｃは、それぞれ、基本的な誤り訂正処理として、図３で上述した誤り訂正処理部２３と同様の機能を担う機能部である。誤り訂正処理部２０３ａ～２０３ｃは、それぞれ、企業Ａ～Ｃの要求内容に基づいて設定部２０８により設定された誤り訂正処理用のパラメータおよびバリエーションに従って動作する。
【００９８】
秘匿性増強処理部２０４ａ～２０４ｃは、それぞれ、基本的な秘匿性増強処理として、図３で上述した秘匿性増強処理部２４と同様の機能を担う機能部である。秘匿性増強処理部２０４ａ～２０４ｃは、それぞれ、企業Ａ～Ｃの要求内容に基づいて設定部２０８により設定された秘匿性増強処理用のパラメータおよびバリエーションに従って動作する。
【００９９】
鍵管理部２０５ａ～２０５ｃは、それぞれ、図３で上述した鍵管理部２５と同様の鍵管理の機能を担う機能部である。鍵管理部２０５ａ～２０５ｃは、それぞれ、企業Ａ～Ｃの要求内容に基づいて設定部２０８により設定された鍵管理用のパラメータおよびバリエーションに従って動作する。
【０１００】
鍵利用部２０６ａ～２０６ｃは、それぞれ、図３で上述した鍵利用部２６と同様の鍵利用の機能を担う機能部である。鍵利用部２０６ａ～２０６ｃは、それぞれ、企業Ａ～Ｃの要求内容に基づいて設定部２０８により設定された鍵利用用のパラメータおよびバリエーションに従って動作する。
【０１０１】
設定部２０８は、企業Ａ～Ｃそれぞれの要求内容に応じて、シフティング処理、誤り訂正処理、秘匿性増強処理、鍵管理および鍵利用のパラメータおよびバリエーションをそれぞれ設定する機能部である。
【０１０２】
配分部２０７は、量子鍵共有部２０１および量子鍵共有部１０１による光子送受信処理により生成される中間データである検出光子情報（受信基底および光子ビット列）を、シフティング処理部２０２ａ～２０２ｃに配分する機能部である。配分部２０７は、企業Ａ～Ｃそれぞれの要求内容に応じて、シフティング処理部２０２ａ～２０２ｃそれぞれに配分する検出光子情報の配分量を決定する。配分部２０７による具体的な検出光子情報の配分方法は、上述した配分部１０７による送信光子情報の配分方法と同様である。
【０１０３】
上述のシフティング処理部２０２ａ～２０２ｃ、誤り訂正処理部２０３ａ～２０３ｃ、秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、鍵利用部２０６ａ～２０６ｃ、配分部２０７、および設定部２０８は、図２に示すＣＰＵ３０１が補助記憶装置３０５等に記憶されたプログラムをＲＡＭ３０３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２０２ａ～２０２ｃ、誤り訂正処理部２０３ａ～２０３ｃ、秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、鍵利用部２０６ａ～２０６ｃ、配分部２０７、および設定部２０８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、ＦＰＧＡ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。
【０１０４】
なお、図６に示す量子鍵共有部２０１、シフティング処理部２０２ａ～２０２ｃ、誤り訂正処理部２０３ａ～２０３ｃ、秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、鍵利用部２０６ａ～２０６ｃ、配分部２０７、設定部２０８、通信部２０９、および記憶部２１０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６に示すＱＫＤ装置２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６に示すＱＫＤ装置２

で、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。

【０１０５】

また、仮想ＱＫＤ装置毎に、最適と考えるデータのパルス、デコイパルス、およびバキュームパルスそれぞれのレーザ強度が異なる可能性も考えられる。この場合、仮想化されていない量子鍵共有部１０１（２０１）の設定により、各仮想ＱＫＤ装置向けに（企業Ａ～Ｃそれぞれの要求内容に応じて）、異なる強度のデータパルス、デコイパルス、およびバキュームパルスを送出するように設定することも原理上可能である。

【０１０６】

また、本実施形態において、本発明の「共通処理部」は、ＱＫＤ装置１において量子鍵共有部１０１に相当し、「個別処理部」は、シフティング処理部１０２ａ～１０２ｃ以降のそれぞれの処理部に相当する。これは、ＱＫＤ装置２についても同様である。また、本実施形態において、本発明の「鍵蒸留処理部」は、ＱＫＤ装置１においてシフティング処理部１０２ａ～１０２ｃ、誤り訂正処理部１０３ａ～１０３ｃ、および秘匿性増強処理部１０４ａ～１０４ｃのそれぞれの一連の処理部に相当する。これは、ＱＫＤ装置２についても同様である。

【０１０７】

以上のように、本実施形態では、物理的な１組のＱＫＤ装置を仮想化し、複数組のＱＫＤ装置（仮想ＱＫＤ装置）が存在するように見せかけ、これらを複数の利用者または利用組織（上述の実施形態の例では企業）がそれぞれ専有するものとしている。そして、複数の利用者または利用組織ごとに、異なるパラメータおよび異なるバリエーションによってそれぞれの利用者または利用組織が専有する仮想ＱＫＤ装置を動作させるものとしている。特に、本実施形態では、量子鍵配送および量子暗号機能の各処理のうち、シフティング処理以降の処理について、異なるパラメータおよび異なるバリエーションによって仮想ＱＫＤ装置を動作させるものとしている。これによって、複数の利用者および利用組織のそれぞれの要求内容に応じたシフティング処理以降の量子鍵配送および量子暗号機能を提供することができる。すなわち、１組の物理的なＱＫＤ装置によって、実際には異なる複数種類の量子鍵配送および量子暗号機能を提供することができる。これは、異なるパラメータおよび異なるバリエーションによる量子鍵配送または量子暗号機能を利用したい場合、利用者および利用組織ごとに専用の物理的なＱＫＤ装置を設置および敷設しなければならなかった従来の技術と比較して、量子鍵配送および量子暗号機能の利用コストを大幅に低減することが可能となる。さらに、ＱＫＤ装置の開発者および提供者の視点からは、１組のＱＫＤ装置では、従来では一種類の量子鍵配送または量子暗号機能しか提供できなかったが、本実施形態に係る量子鍵配送システム１００を用いることで、１組のＱＫＤ装置によって、複数種類の異なる量子鍵配送または量子暗号機能を提供することができるため、量子鍵配送または量子暗号機能の利用者および利用組織を拡大できる。

【０１０８】

また、量子鍵共有部１０１、２０１による光子送受信処理により生成された中間データ（送信光子情報、検出光子情報）を、利用者および利用組織の要求内容に応じて、配分量を決定することができる。これによって、利用者および利用組織の要求内容に応じた生成速度により暗号鍵を生成し、提供することができる。

【０１０９】

なお、図６では、１組のＱＫＤ装置を３組のＱＫＤ装置として仮想化するため、配分部１０７および２０７は３つの配分先に配分を行う様子を示した。ただし、配分部の配分先は３つに限らない。例えば２つであっても４つ以上であってもよい。また、配分先は、同一のＱＫＤ装置内で実行される「個別処理部」、すなわち、シフティング処理部でなくてもよい。すなわち、他の装置上で実行される「個別処理部」が存在し、その「個別処理部」に対して配分部が、中間データ（送信光子情報または検出光子情報）を配分する構成であってもよい。この場合、ＱＫＤ装置には、個別処理部は１以上存在し、配分部は、ＱＫＤ装置が実行する１以上の個別処理部を含む２以上の配分先に、中間データを配分するこ

ととなる。図７は、ＱＫＤ装置内部の１つの個別処理部と、ＱＫＤ装置の外部の１つの個別処理部と、の合計２つの個別処理部に対して配分部が配分する場合の構成を示す図である。以下の第２から第６の実施形態についても、同様の構成を適用できる。

【０１１０】

（第２の実施形態）

第２の実施形態に係る量子鍵配送システムについて、第１の実施形態に係る量子鍵配送システム１００と相違する点を中心に説明する。第１の実施形態では、量子鍵配送および量子暗号機能の処理のうち、シフティング処理以降の処理について、企業ごとに異なるパラメータおよび異なるバリエーションにより実行する動作について説明した。本実施形態では、量子鍵配送および量子暗号機能の処理のうち、誤り訂正処理以降の処理について、企業ごとに異なるパラメータおよび異なるバリエーションにより実行する動作について説明する。なお、本実施形態に係る量子鍵配送システムの全体構成、ＱＫＤ装置のハードウェア構成、および量子鍵配送および量子暗号機能の仮想化の態様については、第１の実施形態と同様である。

【０１１１】

図８は、第２の実施形態に係るＱＫＤ装置の機能ブロックの構成の一例を示す図である。図８を参照しながら、本実施形態に係るＱＫＤ装置（ＱＫＤ装置１ａ、２ａ）の機能ブロックの構成について説明する。なお、図３および４で説明した一般的なＱＫＤ装置の機能ブロック構成および暗号鍵の共有動作と相違する点を中心に説明する。

【０１１２】

図８に示すように、量子鍵配送を含む量子暗号機能の動作における各処理のうち、光子送受信処理およびシフティング処理については、ＱＫＤ装置１ａ、２ａは、物理的なＱＫＤ装置として通常通り実行する。一方、鍵蒸留処理の一部（誤り訂正処理および秘匿性増強処理）、鍵管理、および鍵利用については、ＱＫＤ装置１ａ、２ａは、企業Ａ～Ｃに対してそれぞれ仮想化された仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２として、異なるパラメータおよび異なるバリエーションでそれぞれ独立に実行する。ここで、誤り訂正処理、秘匿性増強処理、鍵管理、および鍵利用それぞれにおいて、どのようなパラメータおよびバリエーションがあるかについては、図３で上述した通りである。これらのパラメータおよびバリエーションは、仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２それぞれの運用者の要求内容に基づいて選択されている。

【０１１３】

図８に示すように、本実施形態に係る量子鍵配送システム１００ａのＱＫＤ装置１ａは、量子鍵共有部１０１と、シフティング処理部１０２と、誤り訂正処理部１０３ａ～１０３ｃと、秘匿性増強処理部１０４ａ～１０４ｃと、鍵管理部１０５ａ～１０５ｃと、鍵利用部１０６ａ～１０６ｃと、配分部１０７と、設定部１０８と、通信部１０９と、記憶部１１０と、を有する。

【０１１４】

量子鍵共有部１０１、通信部１０９および記憶部１１０の機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置１の量子鍵共有部１０１、通信部１０９および記憶部１１０の機能および構成と同様である。

【０１１５】

シフティング処理部１０２は、図３で上述したシフティング処理部１２と同様のシフティング処理を通常通り実行する機能部である。なお、シフティング処理において、上述の推定誤り率を算出した場合、生成される各共有ビット列に対して、対応する推定誤り率が関連付けられているものとする。

【０１１６】

誤り訂正処理部１０３ａ～１０３ｃ、秘匿性増強処理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、および鍵利用部１０６ａ～１０６ｃの機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置１の誤り訂正処理部１０３ａ～１０３ｃ、秘匿性増強処

理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、および鍵利用部１０６ａ～１０６ｃの機能および構成と同様である。すなわち、誤り訂正処理部１０３ａ～１０３ｃ、秘匿性増強処理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、および鍵利用部１０６ａ～１０６ｃは、企業Ａ～Ｃの要求内容に基づいて設定部１０８により設定されたパラメータおよびバリエーションに従ってそれぞれ動作する。

【０１１７】

設定部１０８は、企業Ａ～Ｃそれぞれの要求内容に応じて、誤り訂正処理、秘匿性増強処理、鍵管理および鍵利用のパラメータおよびバリエーションをそれぞれ設定する機能部である。

【０１１８】

配分部１０７は、シフティング処理部１０２によるシフティング処理により生成される中間データである共有ビット列を、誤り訂正処理部１０３ａ～１０３ｃに配分する機能部である。配分部１０７は、企業Ａ～Ｃそれぞれの要求内容に応じて、誤り訂正処理部１０３ａ～１０３ｃそれぞれへの共有ビット列の配分方法を決定する。この場合、企業Ａ～Ｃそれぞれに関連付けられた優先度を考慮してもよい。

【０１１９】

配分部１０７による誤り訂正処理部１０３ａ～１０３ｃに対する共有ビット列の配分方法の決定の基準としては、上述の第１の実施形態と同様のものを含んでもよい。ただし、共有ビット列は、一般的には、基底の偏り、デコイパルスおよびバキュームパルスの割合、それらの分散、およびレーザ強度の分散等のように光子送受信処理に直接関係するデータは除去され、ふるい処理であるシフティング処理が終了した後のビット列であることが一般的である。そのため、共有ビット列の配分方法の決定の基準として一般的に利用できるものは、鍵生成速度および推定誤り率である。鍵生成速度を基準とした配分については、上述の第１の実施形態で説明した通りである。ここでは、推定誤り率を基準とした配分について説明する。

【０１２０】

誤り訂正処理部１０３ａ～１０３ｃは、それぞれ用いる誤り訂正処理のアルゴリズムの差異により、共有ビット列について許容される誤り率の範囲が異なったり、秘匿性増強処理部１０４ａ～１０４ｃは、それぞれ用いる秘匿性増強処理の量子暗号理論に基づくアルゴリズムの差異により、暗号鍵の生成に有利となる共有ビット列の誤り率の範囲等が異なったりする。例えば、誤り訂正処理部１０３ａは、誤り率が２～５［％］が望ましく、かつ、１０［％］までを受け入れ可能であるのに対し、誤り訂正処理部１０３ｂは、誤り率が２．５～３．０［％］が望ましく、かつ、６［％］までを受け入れ可能である可能性がある。このような場合に、配分部１０７は、シフティング処理部１０２により算出された推定誤り率に基づいて、誤り訂正処理部１０３ａ～１０３ｃそれぞれに対し、どの共有ビット列を配分するかを決定する。この場合、企業Ａ～Ｃそれぞれに関連付けられた鍵生成速度の要求、または優先度を考慮してよい。

【０１２１】

なお、図８に示す量子鍵共有部１０１、シフティング処理部１０２、誤り訂正処理部１０３ａ～１０３ｃ、秘匿性増強処理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、鍵利用部１０６ａ～１０６ｃ、配分部１０７、設定部１０８、通信部１０９、および記憶部１１０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８に示すＱＫＤ装置１ａ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８に示すＱＫＤ装置１ａで、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。

【０１２２】

図８に示すように、本実施形態に係る量子鍵配送システム１００ａのＱＫＤ装置２ａは、量子鍵共有部２０１と、シフティング処理部２０２と、誤り訂正処理部２０３ａ～２０３ｃと、秘匿性増強処理部２０４ａ～２０４ｃと、鍵管理部２０５ａ～２０５ｃと、鍵利用部２０６ａ～２０６ｃと、配分部２０７と、設定部２０８と、通信部２０９と、記憶部

２１０と、を有する。

【０１２３】

量子鍵共有部２０１、通信部２０９および記憶部２１０の機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置２の量子鍵共有部２０１、通信部２０９および記憶部２１０の機能および構成と同様である。

【０１２４】

シフティング処理部２０２は、図３で上述したシフティング処理部２２と同様のシフティング処理を通常通り実行する機能部である。なお、シフティング処理において、上述の推定誤り率を算出した場合、生成される各共有ビット列に対して、対応する推定誤り率が関連付けられているものとする。

【０１２５】

誤り訂正処理部２０３ａ～２０３ｃ、秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、および鍵利用部２０６ａ～２０６ｃの機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置２の誤り訂正処理部２０３ａ～２０３ｃ、秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、および鍵利用部２０６ａ～２０６ｃの機能および構成と同様である。すなわち、誤り訂正処理部２０３ａ～２０３ｃ、秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、および鍵利用部２０６ａ～２０６ｃは、企業Ａ～Ｃの要求内容に基づいて設定部２０８により設定されたパラメータおよびバリエーションに従ってそれぞれ動作する。

【０１２６】

設定部２０８は、企業Ａ～Ｃそれぞれの要求内容に応じて、誤り訂正処理、秘匿性増強処理、鍵管理および鍵利用のパラメータおよびバリエーションをそれぞれ設定する機能部である。

【０１２７】

配分部２０７は、シフティング処理部２０２によるシフティング処理により生成される中間データである共有ビット列を、誤り訂正処理部２０３ａ～２０３ｃに配分する機能部である。配分部２０７は、企業Ａ～Ｃそれぞれの要求内容に応じて、誤り訂正処理部２０３ａ～２０３ｃそれぞれへの共有ビット列の配分方法を決定する。配分部２０７による具体的な共有ビット列の配分方法は、上述した配分部１０７による共有ビット列の配分方法と同様である。

【０１２８】

なお、図８に示す量子鍵共有部２０１、シフティング処理部２０２、誤り訂正処理部２０３ａ～２０３ｃ、秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、鍵利用部２０６ａ～２０６ｃ、配分部２０７、設定部２０８、通信部２０９、および記憶部２１０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８に示すＱＫＤ装置２ａ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８に示すＱＫＤ装置２ａで、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。

【０１２９】

また、本実施形態において、本発明の「共通処理部」は、ＱＫＤ装置１ａにおいて量子鍵共有部１０１およびシフティング処理部１０２に相当し、「個別処理部」は、誤り訂正処理部１０３ａ～１０３ｃ以降のそれぞれの処理部に相当する。これは、ＱＫＤ装置２ａについても同様である。また、本実施形態において、本発明の「第１鍵蒸留処理部」は、ＱＫＤ装置１ａにおいてシフティング処理部１０２に相当し、「第２鍵蒸留処理部」は、誤り訂正処理部１０３ａ～１０３ｃ、および秘匿性増強処理部１０４ａ～１０４ｃのそれぞれの一連の処理部に相当する。これは、ＱＫＤ装置２ａについても同様である。

【０１３０】

以上のように、本実施形態でも第１の実施形態と同様に、物理的な１組のＱＫＤ装置を仮想化し、複数組のＱＫＤ装置（仮想ＱＫＤ装置）が存在するように見せかけ、これらを複数の利用者または利用組織（上述の実施形態の例では企業）がそれぞれ専有するものと

している。そして、複数の利用者または利用組織の要求内容に応じて、異なるパラメータおよび異なるバリエーションによってそれぞれの利用者または利用組織が専有する仮想ＱＫＤ装置を動作させるものとしている。特に、本実施形態では、量子鍵配送および量子暗号機能の各処理のうち、誤り訂正処理以降の処理について、異なるパラメータおよび異なるバリエーションによって仮想ＱＫＤ装置を動作させるものとしている。これによって、複数の利用者および利用組織のそれぞれの要求内容に応じた誤り訂正処理以降の量子鍵配送および量子暗号機能を提供することができる。すなわち、１組の物理的なＱＫＤ装置によって、実際には異なる複数種類の量子鍵配送および量子暗号機能を提供することができる。本実施形態に係る量子鍵配送システム１００ａが有するその他の効果は、上述の第１の実施形態で説明した効果と同様である。

【０１３１】

（第３の実施形態）

第３の実施形態に係る量子鍵配送システムについて、第１の実施形態に係る量子鍵配送システム１００と相違する点を中心に説明する。本実施形態では、量子鍵配送および量子暗号機能の処理のうち、秘匿性増強処理以降の処理について、企業ごとに異なるパラメータおよび異なるバリエーションにより実行する動作について説明する。なお、本実施形態に係る量子鍵配送システムの全体構成、ＱＫＤ装置のハードウェア構成、および量子鍵配送および量子暗号機能の仮想化の態様については、第１の実施形態と同様である。

【０１３２】

図９は、第３の実施形態に係るＱＫＤ装置の機能ブロックの構成の一例を示す図である。図９を参照しながら、本実施形態に係るＱＫＤ装置（ＱＫＤ装置１ｂ、２ｂ）の機能ブロックの構成について説明する。なお、図３および４で説明した一般的なＱＫＤ装置の機能ブロック構成および暗号鍵の共有動作と相違する点を中心に説明する。

【０１３３】

図９に示すように、量子鍵配送を含む量子暗号機能の動作における各処理のうち、光子送受信処理、シフティング処理および誤り訂正処理については、ＱＫＤ装置１ｂ、２ｂは、物理的なＱＫＤ装置として通常通り実行する。一方、鍵蒸留処理のうちの秘匿性増強処理、鍵管理、および鍵利用については、ＱＫＤ装置１ｂ、２ｂは、企業Ａ～Ｃに対してそれぞれ仮想化された仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２として、異なるパラメータおよび異なるバリエーションでそれぞれ独立に実行する。ここで、秘匿性増強処理、鍵管理、および鍵利用それぞれにおいて、どのようなパラメータおよびバリエーションがあるかについては、図３で上述した通りである。これらのパラメータおよびバリエーションは、仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２それぞれの運用者の要求内容に基づいて選択されている。

【０１３４】

図９に示すように、本実施形態に係る量子鍵配送システム１００ｂのＱＫＤ装置１ｂは、量子鍵共有部１０１と、シフティング処理部１０２と、誤り訂正処理部１０３と、秘匿性増強処理部１０４ａ～１０４ｃと、鍵管理部１０５ａ～１０５ｃと、鍵利用部１０６ａ～１０６ｃと、配分部１０７と、設定部１０８と、通信部１０９と、記憶部１１０と、を有する。

【０１３５】

量子鍵共有部１０１、通信部１０９および記憶部１１０の機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置１の量子鍵共有部１０１、通信部１０９および記憶部１１０の機能および構成と同様である。

【０１３６】

シフティング処理部１０２は、図３で上述したシフティング処理部１２と同様のシフティング処理を通常通り実行する機能部である。なお、シフティング処理において、上述の推定誤り率を算出した場合、生成される各共有ビット列に対して、対応する推定誤り率が関連付けられているものとする。

【０１３７】
誤り訂正処理部１０３は、図３で上述した誤り訂正処理部１３と同様の誤り訂正処理を通常通り実行する機能部である。なお、誤り訂正処理の結果、生成される各訂正後ビット列に対して、誤りがどの程度含まれていたかを示す誤り率が関連付けられる。
【０１３８】
秘匿性増強処理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、および鍵利用部１０６ａ～１０６ｃの機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置１の秘匿性増強処理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、および鍵利用部１０６ａ～１０６ｃの機能および構成と同様である。すなわち、秘匿性増強処理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、および鍵利用部１０６ａ～１０６ｃは、企業Ａ～Ｃの要求内容に基づいて設定部１０８により設定されたパラメータおよびバリエーションに従ってそれぞれ動作する。
【０１３９】
設定部１０８は、企業Ａ～Ｃそれぞれの要求内容に応じて、秘匿性増強処理、鍵管理および鍵利用のパラメータおよびバリエーションをそれぞれ設定する機能部である。
【０１４０】
配分部１０７は、誤り訂正処理部１０３による誤り訂正処理により生成される中間データである訂正後ビット列を、秘匿性増強処理部１０４ａ～１０４ｃに配分する機能部である。配分部１０７は、企業Ａ～Ｃそれぞれの要求内容に応じて、秘匿性増強処理部１０４ａ～１０４ｃそれぞれへの訂正後ビット列の配分方法を決定する。この場合、企業Ａ～Ｃそれぞれに関連付けられた優先度を考慮してもよい。
【０１４１】
配分部１０７による秘匿性増強処理部１０４ａ～１０４ｃに対する訂正後ビット列の配分方法の決定の基準としては、上述の第１の実施形態と同様のものを含んでもよい。訂正後ビット列の配分方法の決定の基準として一般的に利用できるものは、鍵生成速度および誤り率である。鍵生成速度を基準とした配分については、上述の第１の実施形態で説明した通りである。また、誤り率を基準とした配分については、上述の第２の実施形態の推定誤り率を基準とした配分と同様である。ここで、推定誤り率は、推定値であるのに対し、誤り訂正処理の結果得られる誤り率は、厳密に共有ビット列に含まれていた誤りの数に基づいて求められている点が異なる。
【０１４２】
なお、図９に示す量子鍵共有部１０１、シフティング処理部１０２、誤り訂正処理部１０３、秘匿性増強処理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、鍵利用部１０６ａ～１０６ｃ、配分部１０７、設定部１０８、通信部１０９、および記憶部１１０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９に示すＱＫＤ装置１ｂ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９に示すＱＫＤ装置１ｂで、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。
【０１４３】
図９に示すように、本実施形態に係る量子鍵配送システム１００ｂのＱＫＤ装置２ｂは、量子鍵共有部２０１と、シフティング処理部２０２と、誤り訂正処理部２０３と、秘匿性増強処理部２０４ａ～２０４ｃと、鍵管理部２０５ａ～２０５ｃと、鍵利用部２０６ａ～２０６ｃと、配分部２０７と、設定部２０８と、通信部２０９と、記憶部２１０と、を有する。
【０１４４】
量子鍵共有部２０１、通信部２０９および記憶部２１０の機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置２の量子鍵共有部２０１、通信部２０９および記憶部２１０の機能および構成と同様である。
【０１４５】
シフティング処理部２０２は、図３で上述したシフティング処理部２２と同様のシフテ

ィング処理を通常通り実行する機能部である。なお、シフティング処理において、上述の推定誤り率を算出した場合、生成される各共有ビット列に対して、対応する推定誤り率が関連付けられているものとする。

【０１４６】

誤り訂正処理部２０３は、図３で上述した誤り訂正処理部２３と同様の誤り訂正処理を通常通り実行する機能部である。なお、誤り訂正処理の結果、生成される各訂正後ビット列に対して、誤りがどの程度含まれていたかを示す誤り率が関連付けられる。

【０１４７】

秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、および鍵利用部２０６ａ～２０６ｃの機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置２の秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、および鍵利用部２０６ａ～２０６ｃの機能および構成と同様である。すなわち、秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、および鍵利用部２０６ａ～２０６ｃは、企業Ａ～Ｃの要求内容に基づいて設定部２０８により設定されたパラメータおよびバリエーションに従ってそれぞれ動作する。

【０１４８】

設定部２０８は、企業Ａ～Ｃそれぞれの要求内容に応じて、秘匿性増強処理、鍵管理および鍵利用のパラメータおよびバリエーションをそれぞれ設定する機能部である。

【０１４９】

配分部２０７は、誤り訂正処理部２０３による誤り訂正処理により生成される中間データである訂正後ビット列を、秘匿性増強処理部２０４ａ～２０４ｃに配分する機能部である。配分部２０７は、企業Ａ～Ｃそれぞれの要求内容に応じて、秘匿性増強処理部２０４ａ～２０４ｃそれぞれへの訂正後ビット列の配分方法を決定する。配分部２０７による具体的な訂正後ビット列の配分方法は、上述した配分部１０７による訂正後ビット列の配分方法と同様である。

【０１５０】

なお、図９に示す量子鍵共有部２０１、シフティング処理部２０２、誤り訂正処理部２０３、秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、鍵利用部２０６ａ～２０６ｃ、配分部２０７、設定部２０８、通信部２０９、および記憶部２１０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９に示すＱＫＤ装置２ｂ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９に示すＱＫＤ装置２ｂで、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。

【０１５１】

また、本実施形態において、本発明の「共通処理部」は、ＱＫＤ装置１ｂにおいて量子鍵共有部１０１、シフティング処理部１０２および誤り訂正処理部１０３に相当し、「個別処理部」は、秘匿性増強処理部１０４ａ～１０４ｃ以降のそれぞれの処理部に相当する。これは、ＱＫＤ装置２ｂについても同様である。また、本実施形態において、本発明の「第１鍵蒸留処理部」は、ＱＫＤ装置１ｂにおいてシフティング処理部１０２および誤り訂正処理部１０３に相当し、「第２鍵蒸留処理部」は、秘匿性増強処理部１０４ａ～１０４ｃそれぞれに相当する。これは、ＱＫＤ装置２ｂについても同様である。

【０１５２】

以上のように、本実施形態でも第１の実施形態と同様に、物理的な１組のＱＫＤ装置を仮想化し、複数組のＱＫＤ装置（仮想ＱＫＤ装置）が存在するように見せかけ、これらを複数の利用者または利用組織（上述の実施形態の例では企業）がそれぞれ専有するものとしている。そして、複数の利用者または利用組織の要求内容に応じて、異なるパラメータおよび異なるバリエーションによってそれぞれの利用者または利用組織が専有する仮想ＱＫＤ装置を動作させるものとしている。特に、本実施形態では、量子鍵配送および量子暗号機能の各処理のうち、秘匿性増強処理以降の処理について、異なるパラメータおよび異なるバリエーションによって仮想ＱＫＤ装置を動作させるものとしている。これによって

、複数の利用者および利用組織のそれぞれの要求内容に応じた秘匿性増強処理以降の量子鍵配送および量子暗号機能を提供することができる。すなわち、１組の物理的なＱＫＤ装置によって、実際には異なる複数種類の量子鍵配送および量子暗号機能を提供することができる。本実施形態に係る量子鍵配送システム１００ｂが有するその他の効果は、上述の第１の実施形態で説明した効果と同様である。

【０１５３】

（第４の実施形態）

第４の実施形態に係る量子鍵配送システムについて、第１の実施形態に係る量子鍵配送システム１００と相違する点を中心に説明する。本実施形態では、量子暗号機能の処理のうち、鍵管理および鍵利用の処理について、企業ごとに異なるパラメータおよび異なるバリエーションにより実行する動作について説明する。なお、本実施形態に係る量子鍵配送システムの全体構成、ＱＫＤ装置のハードウェア構成、および量子鍵配送および量子暗号機能の仮想化の態様については、第１の実施形態と同様である。

【０１５４】

図１０は、第４の実施形態に係るＱＫＤ装置の機能ブロックの構成の一例を示す図である。図１０を参照しながら、本実施形態に係るＱＫＤ装置（ＱＫＤ装置１ｃ、２ｃ）の機能ブロックの構成について説明する。なお、図３および４で説明した一般的なＱＫＤ装置の機能ブロック構成および暗号鍵の共有動作と相違する点を中心に説明する。

【０１５５】

図１０に示すように、量子鍵配送を含む量子暗号機能の動作における各処理のうち、光子送受信処理、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ついては、ＱＫＤ装置１ｃ、２ｃは、物理的なＱＫＤ装置として通常通り実行する。一方、鍵管理および鍵利用については、ＱＫＤ装置１ｃ、２ｃは、企業Ａ～Ｃに対してそれぞれ仮想化された仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２として、異なるパラメータおよび異なるバリエーションでそれぞれ独立に実行する。ここで、鍵管理および鍵利用それぞれにおいて、どのようなパラメータおよびバリエーションがあるかについては、図３で上述した通りである。これらのパラメータおよびバリエーションは、仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２それぞれの運用者の要求内容に基づいて選択されている。

【０１５６】

図１０に示すように、本実施形態に係る量子鍵配送システム１００ｃのＱＫＤ装置１ｃは、量子鍵共有部１０１と、シフティング処理部１０２と、誤り訂正処理部１０３と、秘匿性増強処理部１０４と、鍵管理部１０５ａ～１０５ｃと、鍵利用部１０６ａ～１０６ｃと、配分部１０７と、設定部１０８と、通信部１０９と、記憶部１１０と、を有する。

【０１５７】

量子鍵共有部１０１、通信部１０９および記憶部１１０の機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置１の量子鍵共有部１０１、通信部１０９および記憶部１１０の機能および構成と同様である。

【０１５８】

シフティング処理部１０２は、図３で上述したシフティング処理部１２と同様のシフティング処理を通常通り実行する機能部である。なお、シフティング処理において、上述の推定誤り率を算出した場合、生成される各共有ビット列に対して、対応する推定誤り率が関連付けられているものとする。

【０１５９】

誤り訂正処理部１０３は、図３で上述した誤り訂正処理部１３と同様の誤り訂正処理を通常通り実行する機能部である。なお、誤り訂正処理の結果、生成される各訂正後ビット列に対して、誤りがどの程度含まれていたかを示す誤り率が関連付けられる。

【０１６０】

秘匿性増強処理部１０４は、図３で上述した秘匿性増強処理部１４と同様の秘匿性増強処理を通常通り実行する機能部である。

【０１６１】
鍵管理部１０５ａ～１０５ｃおよび鍵利用部１０６ａ～１０６ｃの機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置１の鍵管理部１０５ａ～１０５ｃおよび鍵利用部１０６ａ～１０６ｃの機能および構成と同様である。すなわち、鍵管理部１０５ａ～１０５ｃおよび鍵利用部１０６ａ～１０６ｃは、企業Ａ～Ｃの要求内容に基づいて設定部１０８により設定されたパラメータおよびバリエーションに従ってそれぞれ動作する。
【０１６２】
設定部１０８は、企業Ａ～Ｃそれぞれの要求内容に応じて、鍵管理および鍵利用のパラメータおよびバリエーションをそれぞれ設定する機能部である。
【０１６３】
配分部１０７は、秘匿性増強処理部１０４による秘匿性増強処理により生成される中間データである暗号鍵を、鍵管理部１０５ａ～１０５ｃに配分する機能部である。配分部１０７は、企業Ａ～Ｃそれぞれの要求内容に応じて、鍵管理部１０５ａ～１０５ｃそれぞれへの暗号鍵の配分方法を決定する。この場合、企業Ａ～Ｃそれぞれに関連付けられた優先度を考慮してもよい。
【０１６４】
配分部１０７による鍵管理部１０５ａ～１０５ｃに対する暗号鍵の配分方法の決定の基準としては、上述の第１の実施形態と同様のものを含んでもよい。暗号鍵の配分方法の決定の基準として一般的に利用できるものは、鍵生成速度および誤り率である。鍵生成速度を基準とした配分については、上述の第１の実施形態で説明した通りである。また、誤り率を基準とした配分については、上述の第３の実施形態で説明した通りである。
【０１６５】
なお、図１０に示す量子鍵共有部１０１、シフティング処理部１０２、誤り訂正処理部１０３、秘匿性増強処理部１０４、鍵管理部１０５ａ～１０５ｃ、鍵利用部１０６ａ～１０６ｃ、配分部１０７、設定部１０８、通信部１０９、および記憶部１１０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１０に示すＱＫＤ装置１ｃ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１０に示すＱＫＤ装置１ｃで、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。
【０１６６】
図１０に示すように、本実施形態に係る量子鍵配送システム１００ｃのＱＫＤ装置２ｃは、量子鍵共有部２０１と、シフティング処理部２０２と、誤り訂正処理部２０３と、秘匿性増強処理部２０４と、鍵管理部２０５ａ～２０５ｃと、鍵利用部２０６ａ～２０６ｃと、配分部２０７と、設定部２０８と、通信部２０９と、記憶部２１０と、を有する。
【０１６７】
量子鍵共有部２０１、通信部２０９および記憶部２１０の機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置２の量子鍵共有部２０１、通信部２０９および記憶部２１０の機能および構成と同様である。
【０１６８】
シフティング処理部２０２は、図３で上述したシフティング処理部２２と同様のシフティング処理を通常通り実行する機能部である。なお、シフティング処理において、上述の推定誤り率を算出した場合、生成される各共有ビット列に対して、対応する推定誤り率が関連付けられているものとする。
【０１６９】
誤り訂正処理部２０３は、図３で上述した誤り訂正処理部２３と同様の誤り訂正処理を通常通り実行する機能部である。なお、誤り訂正処理の結果、生成される各訂正後ビット列に対して、誤りがどの程度含まれていたかを示す誤り率が関連付けられる。
【０１７０】
秘匿性増強処理部２０４は、図３で上述した秘匿性増強処理部２４と同様の秘匿性増強処理を通常通り実行する機能部である。

【０１７１】
鍵管理部２０５ａ～２０５ｃおよび鍵利用部２０６ａ～２０６ｃの機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置２の鍵管理部２０５ａ～２０５ｃおよび鍵利用部２０６ａ～２０６ｃの機能および構成と同様である。すなわち、鍵管理部２０５ａ～２０５ｃおよび鍵利用部２０６ａ～２０６ｃは、企業Ａ～Ｃの要求内容に基づいて設定部２０８により設定されたパラメータおよびバリエーションに従ってそれぞれ動作する。
【０１７２】
設定部２０８は、企業Ａ～Ｃそれぞれの要求内容に応じて、鍵管理および鍵利用のパラメータおよびバリエーションをそれぞれ設定する機能部である。
【０１７３】
配分部２０７は、秘匿性増強処理部２０４による秘匿性増強処理により生成される暗号鍵を、鍵管理部２０５ａ～２０５ｃに配分する機能部である。配分部２０７は、企業Ａ～Ｃそれぞれの要求内容に応じて、鍵管理部２０５ａ～２０５ｃそれぞれへの暗号鍵の配分方法を決定する。配分部２０７による具体的な暗号鍵の配分方法は、上述した配分部１０７による暗号鍵の配分方法と同様である。
【０１７４】
なお、図１０に示す量子鍵共有部２０１、シフティング処理部２０２、誤り訂正処理部２０３、秘匿性増強処理部２０４、鍵管理部２０５ａ～２０５ｃ、鍵利用部２０６ａ～２０６ｃ、配分部２０７、設定部２０８、通信部２０９、および記憶部２１０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１０に示すＱＫＤ装置２ｃ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１０に示すＱＫＤ装置２ｃで、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。
【０１７５】
また、本実施形態において、本発明の「共通処理部」は、ＱＫＤ装置１ｃにおいて量子鍵共有部１０１、シフティング処理部１０２、誤り訂正処理部１０３および秘匿性増強処理部１０４に相当し、「個別処理部」は、鍵管理部１０５ａ～１０５ｃ以降のそれぞれの処理部に相当する。これは、ＱＫＤ装置２ｃについても同様である。また、本実施形態において、本発明の「鍵蒸留処理部」は、ＱＫＤ装置１ｃにおいてシフティング処理部１０２、誤り訂正処理部１０３および秘匿性増強処理部１０４に相当する。これは、ＱＫＤ装置２ｃについても同様である。
【０１７６】
以上のように、本実施形態でも第１の実施形態と同様に、物理的な１組のＱＫＤ装置を仮想化し、複数組のＱＫＤ装置（仮想ＱＫＤ装置）が存在するように見せかけ、これらを複数の利用者または利用組織（上述の実施形態の例では企業）がそれぞれ専有するものとしている。そして、複数の利用者または利用組織の要求内容に応じて、異なるパラメータおよび異なるバリエーションによってそれぞれの利用者または利用組織が専有する仮想ＱＫＤ装置を動作させるものとしている。特に、本実施形態では、量子暗号機能の各処理のうち、鍵管理および鍵利用の処理について、異なるパラメータおよび異なるバリエーションによって仮想ＱＫＤ装置を動作させるものとしている。これによって、複数の利用者および利用組織のそれぞれの要求内容に応じた鍵管理および鍵利用についての量子暗号機能を提供することができる。すなわち、１組の物理的なＱＫＤ装置によって、実際には異なる複数種類の量子鍵配送および量子暗号機能を提供することができる。本実施形態に係る量子鍵配送システム１００ｃが有するその他の効果は、上述の第１の実施形態で説明した効果と同様である。
【０１７７】
（第５の実施形態）
第５の実施形態に係る量子鍵配送システムについて、第１の実施形態に係る量子鍵配送システム１００と相違する点を中心に説明する。本実施形態では、量子暗号機能の処理のうち、鍵利用の処理について、企業ごとに異なるパラメータおよび異なるバリエーション

により実行する動作について説明する。なお、本実施形態に係る量子鍵配送システムの全体構成、ＱＫＤ装置のハードウェア構成、および量子鍵配送および量子暗号機能の仮想化の態様については、第１の実施形態と同様である。

【０１７８】

図１１は、第５の実施形態に係るＱＫＤ装置の機能ブロックの構成の一例を示す図である。図１１を参照しながら、本実施形態に係るＱＫＤ装置（ＱＫＤ装置１ｄ、２ｄ）の機能ブロックの構成について説明する。なお、図３および４で説明した一般的なＱＫＤ装置の機能ブロック構成および暗号鍵の共有動作と相違する点を中心に説明する。

【０１７９】

図１１に示すように、量子鍵配送を含む量子暗号機能の動作における各処理のうち、光子送受信処理、シフティング処理、誤り訂正処理、秘匿性増強処理および鍵管理については、ＱＫＤ装置１ｄ、２ｄは、物理的なＱＫＤ装置として通常通り実行する。一方、鍵利用については、ＱＫＤ装置１ｄ、２ｄは、企業Ａ～Ｃに対してそれぞれ仮想化された仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２として、異なるパラメータおよび異なるバリエーションでそれぞれ独立に実行する。ここで、鍵利用それぞれにおいて、どのようなパラメータおよびバリエーションがあるかについては、図３で上述した通りである。これらのパラメータおよびバリエーションは、仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２それぞれの運用者の要求内容に基づいて選択されている。

【０１８０】

図１１に示すように、本実施形態に係る量子鍵配送システム１００ｄのＱＫＤ装置１ｄは、量子鍵共有部１０１と、シフティング処理部１０２と、誤り訂正処理部１０３と、秘匿性増強処理部１０４と、鍵管理部１０５と、鍵利用部１０６ａ～１０６ｃと、配分部１０７と、設定部１０８と、通信部１０９と、記憶部１１０と、を有する。

【０１８１】

量子鍵共有部１０１、通信部１０９および記憶部１１０の機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置１の量子鍵共有部１０１、通信部１０９および記憶部１１０の機能および構成と同様である。

【０１８２】

シフティング処理部１０２は、図３で上述したシフティング処理部１２と同様のシフティング処理を通常通り実行する機能部である。なお、シフティング処理において、上述の推定誤り率を算出した場合、生成される各共有ビット列に対して、対応する推定誤り率が関連付けられているものとする。

【０１８３】

誤り訂正処理部１０３は、図３で上述した誤り訂正処理部１３と同様の誤り訂正処理を通常通り実行する機能部である。なお、誤り訂正処理の結果、生成される各訂正後ビット列に対して、誤りがどの程度含まれていたかを示す誤り率が関連付けられる。

【０１８４】

秘匿性増強処理部１０４は、図３で上述した秘匿性増強処理部１４と同様の秘匿性増強処理を通常通り実行する機能部である。

【０１８５】

鍵管理部１０５は、図３で上述した鍵管理部１５と同様に鍵管理を通常通り行う機能部である。

【０１８６】

鍵利用部１０６ａ～１０６ｃの機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置１の鍵利用部１０６ａ～１０６ｃの機能および構成と同様である。すなわち、鍵利用部１０６ａ～１０６ｃは、企業Ａ～Ｃの要求内容に基づいて設定部１０８により設定されたパラメータおよびバリエーションに従ってそれぞれ動作する。

【０１８７】

設定部１０８は、企業Ａ～Ｃそれぞれの要求内容に応じて、鍵利用のパラメータおよび

バリエーションをそれぞれ設定する機能部である。

【０１８８】

配分部１０７は、鍵管理部１０５により提供された中間データである暗号鍵を、鍵利用部１０６ａ～１０６ｃに配分する機能部である。配分部１０７は、企業Ａ～Ｃそれぞれの要求内容に応じて、鍵利用部１０６ａ～１０６ｃそれぞれへの暗号鍵の配分方法を決定する。この場合、企業Ａ～Ｃそれぞれに関連付けられた優先度を考慮してもよい。

【０１８９】

配分部１０７による鍵利用部１０６ａ～１０６ｃに対する暗号鍵の配分方法の決定の基準としては、上述の第４の実施形態と同様のものを含んでもよい。

【０１９０】

なお、図１１に示す量子鍵共有部１０１、シフティング処理部１０２、誤り訂正処理部１０３、秘匿性増強処理部１０４、鍵管理部１０５、鍵利用部１０６ａ～１０６ｃ、配分部１０７、設定部１０８、通信部１０９、および記憶部１１０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１１に示すＱＫＤ装置１ｄ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１１に示すＱＫＤ装置１ｄで、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。

【０１９１】

図１１に示すように、本実施形態に係る量子鍵配送システム１００ｄのＱＫＤ装置２ｄは、量子鍵共有部２０１と、シフティング処理部２０２と、誤り訂正処理部２０３と、秘匿性増強処理部２０４と、鍵管理部２０５と、鍵利用部２０６ａ～２０６ｃと、配分部２０７と、設定部２０８と、通信部２０９と、記憶部２１０と、を有する。

【０１９２】

量子鍵共有部２０１、通信部２０９および記憶部２１０の機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置２の量子鍵共有部２０１、通信部２０９および記憶部２１０の機能および構成と同様である。

【０１９３】

シフティング処理部２０２は、図３で上述したシフティング処理部２２と同様のシフティング処理を通常通り実行する機能部である。なお、シフティング処理において、上述の推定誤り率を算出した場合、生成される各共有ビット列に対して、対応する推定誤り率が関連付けられているものとする。

【０１９４】

誤り訂正処理部２０３は、図３で上述した誤り訂正処理部２３と同様の誤り訂正処理を通常通り実行する機能部である。なお、誤り訂正処理の結果、生成される各訂正後ビット列に対して、誤りがどの程度含まれていたかを示す誤り率が関連付けられる。

【０１９５】

秘匿性増強処理部２０４は、図３で上述した秘匿性増強処理部２４と同様の秘匿性増強処理を通常通り実行する機能部である。

【０１９６】

鍵管理部２０５は、図３で上述した鍵管理部２５と同様に鍵管理を通常通り行う機能部である。

【０１９７】

鍵利用部２０６ａ～２０６ｃの機能および構成は、それぞれ第１の実施形態に係るＱＫＤ装置２の鍵利用部２０６ａ～２０６ｃの機能および構成と同様である。すなわち、鍵利用部２０６ａ～２０６ｃは、企業Ａ～Ｃの要求内容に基づいて設定部２０８により設定されたパラメータおよびバリエーションに従ってそれぞれ動作する。

【０１９８】

設定部２０８は、企業Ａ～Ｃそれぞれの要求内容に応じて、鍵利用のパラメータおよびバリエーションをそれぞれ設定する機能部である。

【０１９９】

配分部２０７は、鍵管理部２０５により提供された暗号鍵を、鍵利用部２０６ａ～２０６ｃに配分する機能部である。配分部２０７は、企業Ａ～Ｃそれぞれの要求内容に応じて、鍵利用部２０６ａ～２０６ｃそれぞれへの暗号鍵の配分方法を決定する。配分部２０７による具体的な暗号鍵の配分方法は、上述した配分部１０７による暗号鍵の配分方法と同様である。

【０２００】

なお、図１１に示す量子鍵共有部２０１、シフティング処理部２０２、誤り訂正処理部２０３、秘匿性増強処理部２０４、鍵管理部２０５、鍵利用部２０６ａ～２０６ｃ、配分部２０７、設定部２０８、通信部２０９、および記憶部２１０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１１に示すＱＫＤ装置２ｄ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１１に示すＱＫＤ装置２ｄで、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。

【０２０１】

また、本実施形態において、本発明の「共通処理部」は、ＱＫＤ装置１ｄにおいて量子鍵共有部１０１、シフティング処理部１０２、誤り訂正処理部１０３、秘匿性増強処理部１０４および鍵管理部１０５に相当し、「個別処理部」は、鍵利用部１０６ａ～１０６ｃそれぞれに相当する。これは、ＱＫＤ装置２ｄについても同様である。

【０２０２】

以上のように、本実施形態でも第１の実施形態と同様に、物理的な１組のＱＫＤ装置を仮想化し、複数組のＱＫＤ装置（仮想ＱＫＤ装置）が存在するように見せかけ、これらを複数の利用者または利用組織（上述の実施形態の例では企業）がそれぞれ専有するものとしている。そして、複数の利用者または利用組織の要求内容に応じて、異なるパラメータおよび異なるバリエーションによってそれぞれの利用者または利用組織が専有する仮想ＱＫＤ装置を動作させるものとしている。特に、本実施形態では、量子暗号機能の各処理のうち鍵利用の処理について、異なるパラメータおよび異なるバリエーションによって仮想ＱＫＤ装置を動作させるものとしている。これによって、複数の利用者および利用組織のそれぞれの要求内容に応じた鍵利用についての量子暗号機能を提供することができる。すなわち、１組の物理的なＱＫＤ装置によって、実際には異なる複数種類の量子鍵配送および量子暗号機能を提供することができる。本実施形態に係る量子鍵配送システム１００ｄが有するその他の効果は、上述の第１の実施形態で説明した効果と同様である。

【０２０３】

（第６の実施形態）

第６の実施形態に係る量子鍵配送システムについて、第１の実施形態に係る量子鍵配送システム１００と相違する点を中心に説明する。第１の実施形態では、量子鍵配送および量子暗号機能の処理のうち、シフティング処理以降の処理について、各企業の要求内容に応じるために、仮想ＱＫＤ装置上で異なるパラメータおよび異なるバリエーションにより実行する動作について説明した。本実施形態では、仮想ＱＫＤ装置上の動作に対する企業等（運用者）の要求内容（企業等の要求、ポリシー、またはＱＫＤ装置の提供者と合意するサービスレベルアグリーメント等）を満たすように、物理的なＱＫＤ装置を構成する内容について説明する。なお、本実施形態に係る量子鍵配送システムの全体構成、ＱＫＤ装置のハードウェア構成、および量子鍵配送および量子暗号機能の仮想化の態様については、第１の実施形態と同様である。

【０２０４】

図１２は、第６の実施形態に係るＱＫＤ装置の機能ブロックの構成の一例を示す図である。図１２を参照しながら、本実施形態に係る量子鍵配送システム１００ｅのＱＫＤ装置（ＱＫＤ装置１ｅ、２ｅ）の機能ブロックの構成について説明する。なお、図３および４で説明した一般的なＱＫＤ装置の機能ブロック構成および暗号鍵の共有動作と相違する点を中心に説明する。

【０２０５】

図１２に示す例では、例えば、企業等の鍵生成速度についての要求内容に応じるために、光子を送信および検出する機能を増強した構成を示す。すなわち、ＱＫＤ装置１ｅ側では、物理的に２つの量子鍵共有部（量子鍵共有部１０１ａ、１０１ｂ）を有するものとし、ＱＫＤ装置２ｅ側では、物理的に２つの量子鍵共有部（量子鍵共有部２０１ａ、２０１ｂ）を有するものとしている。ＱＫＤ装置１ｅ、２ｅのその他の機能ブロックの構成は、図６に示す第１の実施形態に係るＱＫＤ装置１、２それぞれの構成と同様である。すなわち、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）、鍵管理、および鍵利用については、ＱＫＤ装置１ｅ、２ｅは、企業Ａ～Ｃの要求内容に応じてそれぞれ仮想化された仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２として、異なるパラメータおよび異なるバリエーションでそれぞれ独立に実行する。ここで、シフティング処理、誤り訂正処理、秘匿性増強処理、鍵管理、および鍵利用それぞれにおいて、どのようなパラメータおよびバリエーションがあるかについては、図３で上述した通りである。これらのパラメータおよびバリエーションは、仮想ＱＫＤ装置Ａ１、Ａ２、仮想ＱＫＤ装置Ｂ１、Ｂ２、および仮想ＱＫＤ装置Ｃ１、Ｃ２それぞれの運用者の要求内容に基づいて選択されている。また、ＱＫＤ装置１ｅ、２ｅの２つの量子鍵共有部は、図２に示す光学処理装置３０６を２台備えることによって実現される。

【０２０６】

図１２に示すように、物理的なハードウェア装置（量子鍵共有部１０１ａ、１０１ｂ、２０１ａ、２０１ｂ）を増強することによって、送信光子情報および検出光子情報の生成速度を増加させることが可能となる。そして、配分部１０７は、増加した送信光子情報を、シフティング処理部１０２ａ～１０２ｃに配分し、配分部２０７は、増加した検出光子情報を、シフティング処理部２０２ａ～２０２ｃに配分する。これによって、最終的な暗号鍵の生成速度（鍵生成速度）に関して、企業Ａ～Ｃの要求内容を満たすことができる。

【０２０７】

また、図１２に示す構成では、第１の実施形態と同様に、シフティング処理以降の処理を仮想化していることから、送信光子情報および検出光子情報の生成元となる物理的な量子鍵共有部（光学処理装置３０６）の台数を増加させても（または減少させても）、配分部１０７（２０７）により、送信光子情報および検出光子情報を適切に配分処理することによって、仮想ＱＫＤ装置としての動作部分への影響を小さく抑えることができる。

【０２０８】

なお、図１２に示す量子鍵共有部１０１ａ、１０１ｂ、シフティング処理部１０２ａ～１０２ｃ、誤り訂正処理部１０３ａ～１０３ｃ、秘匿性増強処理部１０４ａ～１０４ｃ、鍵管理部１０５ａ～１０５ｃ、鍵利用部１０６ａ～１０６ｃ、配分部１０７、設定部１０８、通信部１０９、および記憶部１１０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１２に示すＱＫＤ装置１ｅ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１２に示すＱＫＤ装置１ｅで、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。

【０２０９】

また、図１２に示す量子鍵共有部２０１ａ、２０１ｂ、シフティング処理部２０２ａ～２０２ｃ、誤り訂正処理部２０３ａ～２０３ｃ、秘匿性増強処理部２０４ａ～２０４ｃ、鍵管理部２０５ａ～２０５ｃ、鍵利用部２０６ａ～２０６ｃ、配分部２０７、設定部２０８、通信部２０９、および記憶部２１０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１２に示すＱＫＤ装置２ｅ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１２に示すＱＫＤ装置２ｅで、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。

【０２１０】

また、本実施形態において、本発明の「共通処理部」は、ＱＫＤ装置１ｅにおいて量子

鍵共有部１０１ａ、１０１ｂに相当し、「個別処理部」は、シフティング処理部１０２ａ～１０２ｃ以降のそれぞれの処理部に相当する。これは、ＱＫＤ装置２ｅについても同様である。

【０２１１】

以上のように、物理的なハードウェア装置（上述では量子鍵共有部）を増強することによって、例えば、物理的なＱＫＤ装置の故障対応または増強のために、物理的なＱＫＤ装置のハードウェアの追加または削除が発生しても、仮想ＱＫＤ装置に対しては鍵生成速度の劣化等の一部の影響のみに抑えて、量子鍵配送システム１００ｅの稼働を継続することが可能となる。その他、本実施形態に係る量子鍵配送システム１００ｅは、第１の実施形態で説明した効果を有することは言うまでもない。

【０２１２】

なお、上述のように物理的なハードウェア装置（図１２に示す例では量子鍵共有部１０１ａ、１０１ｂ、２０１ａ、２０１ｂ）を増強した構成は、上述の第２～５の実施形態に係る各量子鍵配送システムに対して適用することが可能である。

【０２１３】

また、図１２に示す例では、物理的なハードウェア装置を増強した構成を示したが、仮想ＱＫＤ装置上の動作に対する企業等（運用者）の要求内容を満たすために、現状の物理的な装置に対する設定の調整によって対応するようにしてもよい。例えば、全ての仮想ＱＫＤ装置に対して、送信光子情報・検出光子情報の配分ができるように、物理的な装置の設定等を調整するような対応を行ってもよい。他にも例えば、鍵生成速度に関連しても、仮想ＱＫＤ装置が要求する鍵生成速度がそれぞれある場合、それらの鍵生成速度の合計値以上の光子送受信処理が実現できるように、量子鍵共有部の調整（例えば、レーザ駆動速度の変更）をしたり、仮想ＱＫＤ装置の動作を実現する専用処理用のハードウェアを追加する等の対応も可能である。この場合、増強した一部の専用処理用のハードウェアは、一部の仮想ＱＫＤ装置にのみ利用させるといった構成も可能である。

【０２１４】

なお、上述の各実施形態に係るＱＫＤ装置で実行されるプログラムは、例えば、ＲＯＭ３０２等に予め組み込まれて提供されるものとしてもよい。

【０２１５】

また、上述の各実施形態に係る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。

【０２１６】

また、上述の各実施形態に係る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、上述の各実施形態に係る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。

【０２１７】

また、上述の各実施形態に係る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、ＣＰＵ３０１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。

【０２１８】

本発明の実施形態を説明したが、これらの実施形態は、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。これら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。これらの実施形態は、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。

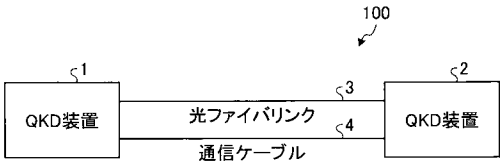
【符号の説明】

【０２１９】

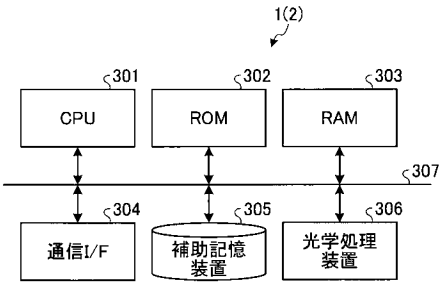
１、１ａ～１ｅ、２、２ａ～２ｅ　ＱＫＤ装置
３　光ファイバリンク
４　通信ケーブル
１０　ＱＫＤ装置
１１　量子鍵共有部
１２　シフティング処理部
１３　誤り訂正処理部
１４　秘匿性増強処理部
１５　鍵管理部
１６　鍵利用部
１７　通信部
１８　記憶部
２０　ＱＫＤ装置
２１　量子鍵共有部
２２　シフティング処理部
２３　誤り訂正処理部
２４　秘匿性増強処理部
２５　鍵管理部
２６　鍵利用部
２７　通信部
２８　記憶部
１００、１００ａ～１００ｅ　量子鍵配送システム
１０１、１０１ａ、１０１ｂ　量子鍵共有部
１０２、１０２ａ～１０２ｃ　シフティング処理部
１０３、１０３ａ～１０３ｃ　誤り訂正処理部
１０４、１０４ａ～１０４ｃ　秘匿性増強処理部
１０５、１０５ａ～１０５ｃ　鍵管理部
１０６ａ～１０６ｃ　鍵利用部
１０７　配分部
１０８　設定部
１０９　通信部
１１０　記憶部
２０１　量子鍵共有部
２０２、２０２ａ～２０２ｃ　シフティング処理部
２０３、２０３ａ～２０３ｃ　誤り訂正処理部
２０４、２０４ａ～２０４ｃ　秘匿性増強処理部
２０５、２０５ａ～２０５ｃ　鍵管理部
２０６ａ～２０６ｃ　鍵利用部
２０７　配分部
２０８　設定部
２０９　通信部
２１０　記憶部
３０１　ＣＰＵ
３０２　ＲＯＭ
３０３　ＲＡＭ
３０４　通信Ｉ／Ｆ

３０５　補助記憶装置
３０６　光学処理装置
３０７　バス
５００　量子鍵配送システム
Ａ１、Ａ２、Ｂ１、Ｂ２、Ｃ１、Ｃ２　仮想ＱＫＤ装置

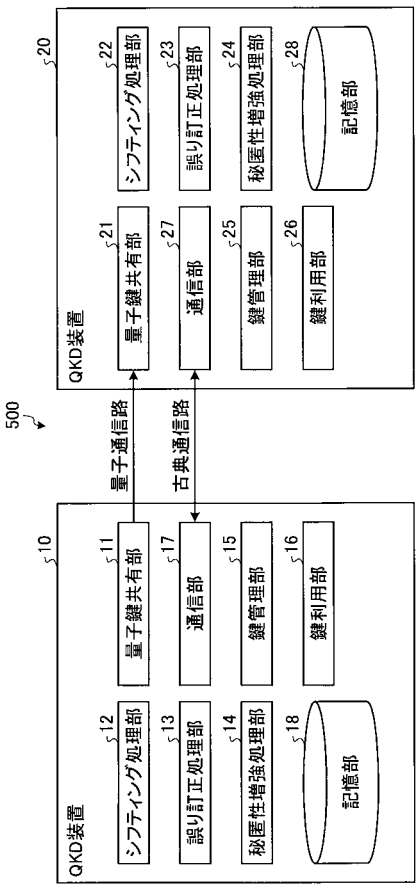
【図１】



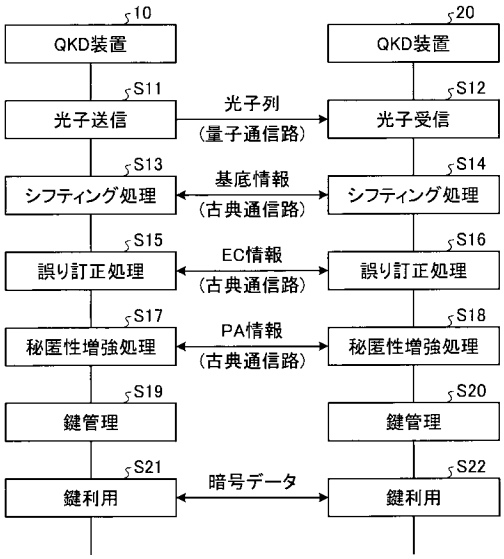
【図２】



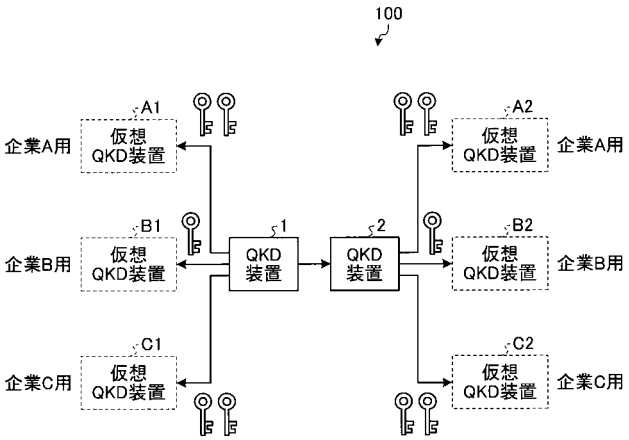
【図３】



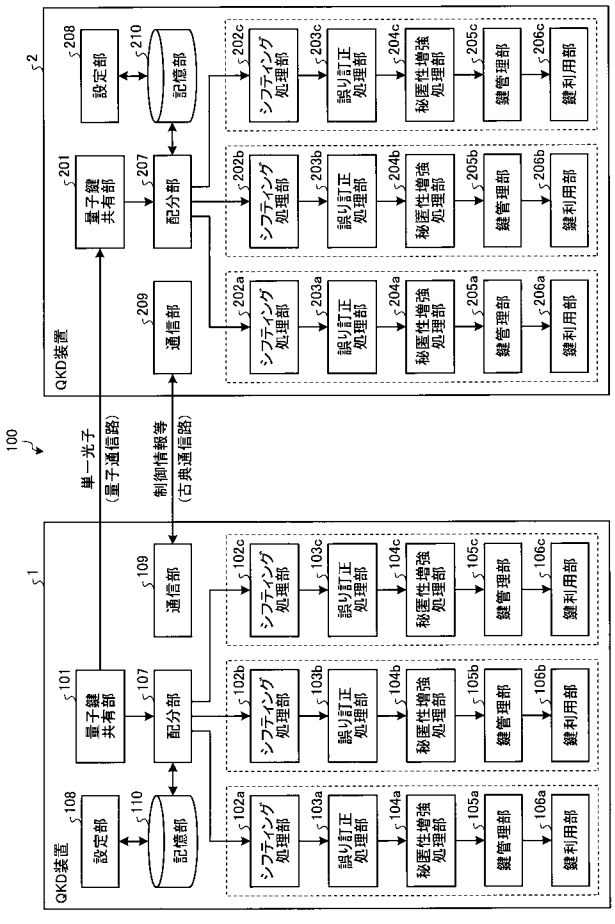
【図４】


10
QKD装置
20
QKD装置
S11
光子送信
光子列
（量子通信路）
S12
光子受信
S13
シフティング処理
基底情報
（古典通信路）
S14
シフティング処理
S15
誤り訂正処理
EC情報
（古典通信路）
S16
誤り訂正処理
S17
秘匿性増強処理
PA情報
（古典通信路）
S18
秘匿性増強処理
S19
鍵管理
S20
鍵管理
S21
鍵利用
暗号データ
S22
鍵利用

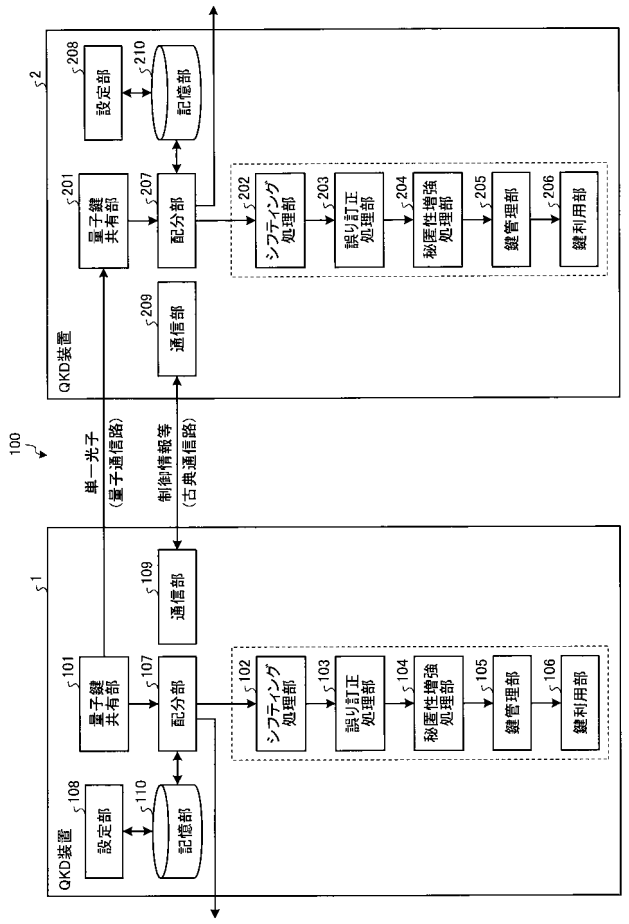
【図５】


100
企業A用
A1
仮想
QKD装置
A2
仮想
QKD装置
企業A用
企業B用
B1
仮想
QKD装置
1
QKD
装置
2
QKD
装置
B2
仮想
QKD装置
企業B用
企業C用
C1
仮想
QKD装置
C2
仮想
QKD装置
企業C用

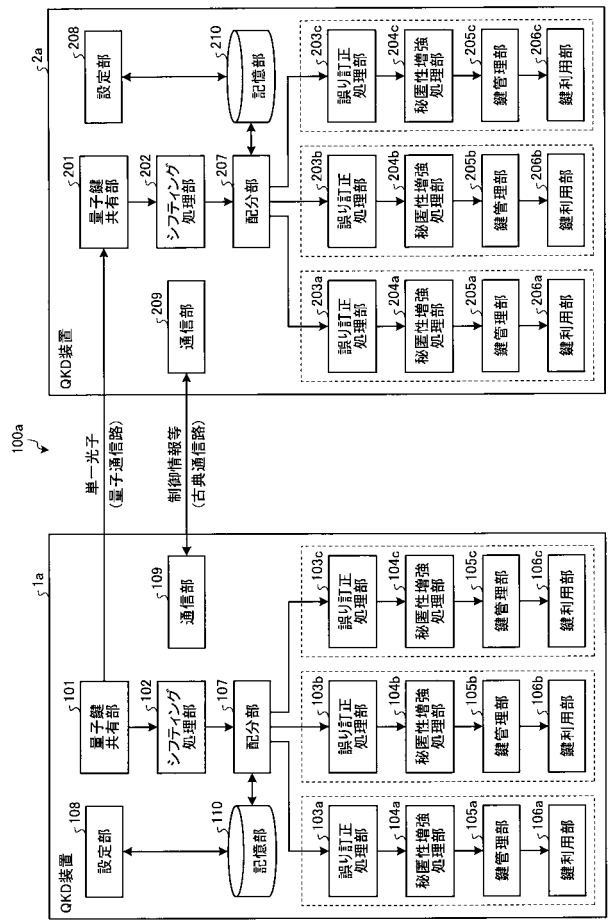
【図６】


100
単一光子
（量子通信路）
制御情報等
（古典通信路）
QKD装置
2
208 設定部
210 記憶部
201 量子鍵共有部
207 配分部
209 通信部
202c シフティング処理部
203c 誤り訂正処理部
204c 秘匿性増強処理部
205c 鍵管理部
206c 鍵利用部
202b シフティング処理部
203b 誤り訂正処理部
204b 秘匿性増強処理部
205b 鍵管理部
206b 鍵利用部
202a シフティング処理部
203a 誤り訂正処理部
204a 秘匿性増強処理部
205a 鍵管理部
206a 鍵利用部
1
109 通信部
101 量子鍵共有部
107 配分部
108 設定部
110 記憶部
102c シフティング処理部
103c 誤り訂正処理部
104c 秘匿性増強処理部
105c 鍵管理部
106c 鍵利用部
102b シフティング処理部
103b 誤り訂正処理部
104b 秘匿性増強処理部
105b 鍵管理部
106b 鍵利用部
102a シフティング処理部
103a 誤り訂正処理部
104a 秘匿性増強処理部
105a 鍵管理部
106a 鍵利用部

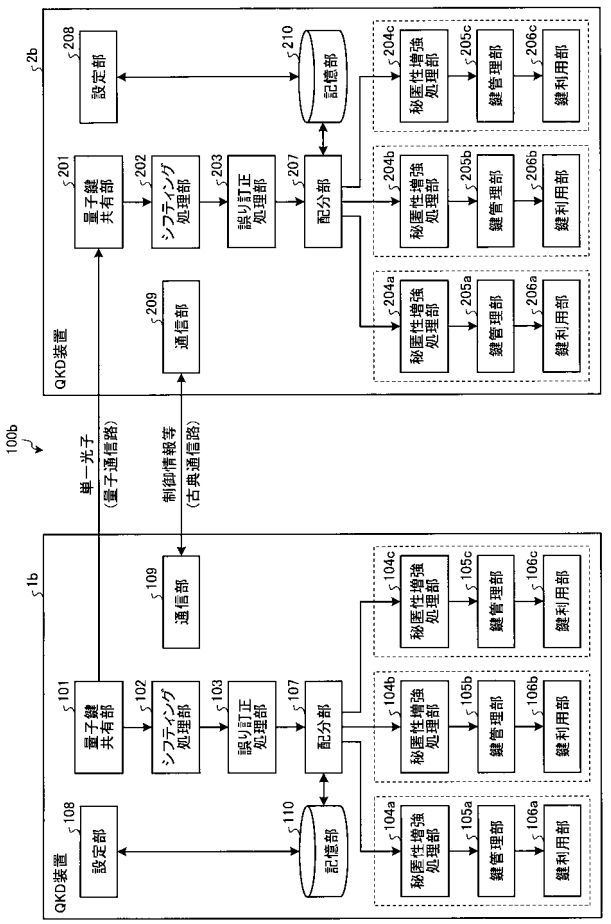
【図７】


100
単一光子
（量子通信路）
制御情報等
（古典通信路）
QKD装置
2
208 設定部
210 記憶部
201 量子鍵共有部
207 配分部
209 通信部
202 シフティング処理部
203 誤り訂正処理部
204 秘匿性増強処理部
205 鍵管理部
206 鍵利用部
1
109 通信部
101 量子鍵共有部
107 配分部
108 設定部
110 記憶部
102 シフティング処理部
103 誤り訂正処理部
104 秘匿性増強処理部
105 鍵管理部
106 鍵利用部

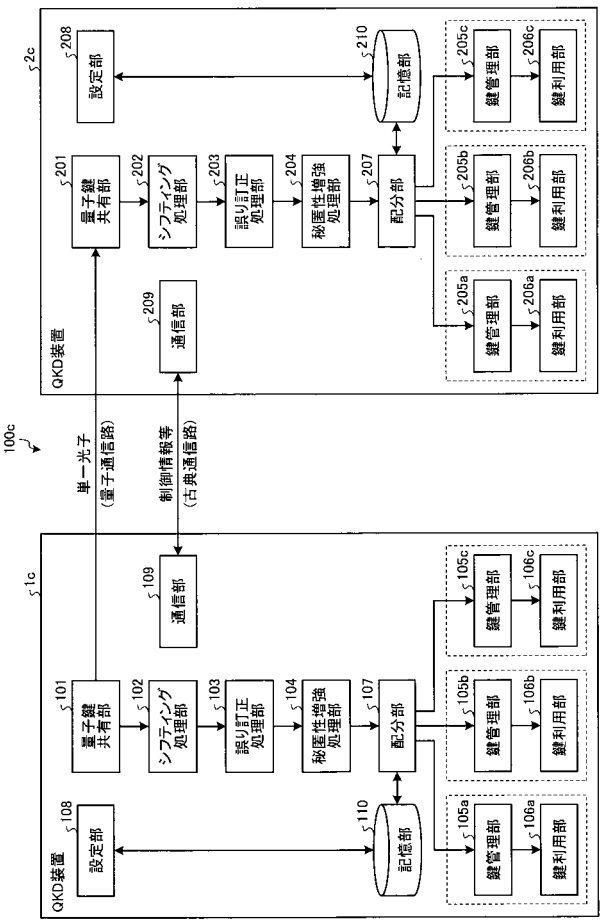
【図８】


100a
単一光子
(量子通信路)
制御情報等
(古典通信路)
QKD装置
1a
2a
量子鍵共有部
シフティング処理部
誤り訂正処理部
秘匿性増強処理部
鍵管理部
鍵利用部
配分部
通信部
設定部
記憶部

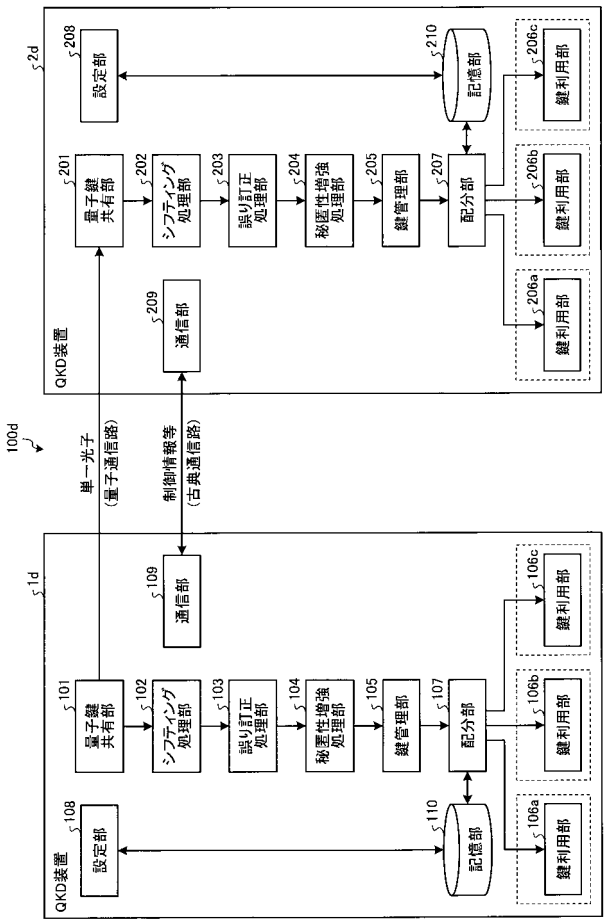
【図９】


100b
単一光子
(量子通信路)
制御情報等
(古典通信路)
QKD装置
1b
2b
量子鍵共有部
シフティング処理部
誤り訂正処理部
秘匿性増強処理部
鍵管理部
鍵利用部
配分部
通信部
設定部
記憶部

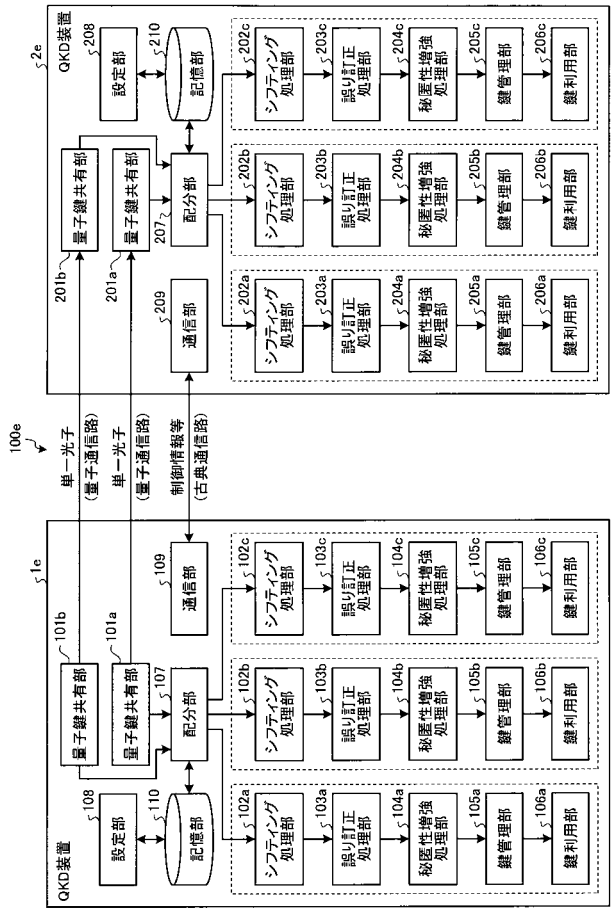
【図１０】


100c
単一光子
(量子通信路)
制御情報等
(古典通信路)
QKD装置
1c
2c
量子鍵共有部
シフティング処理部
誤り訂正処理部
秘匿性増強処理部
鍵管理部
鍵利用部
配分部
通信部
設定部
記憶部

【図１１】


100d
単一光子
(量子通信路)
制御情報等
(古典通信路)
QKD装置
1d
2d
量子鍵共有部
シフティング処理部
誤り訂正処理部
秘匿性増強処理部
鍵管理部
鍵利用部
配分部
通信部
設定部
記憶部

【図１２】


100e
単一光子
(量子通信路)
単一光子
(量子通信路)
制御情報等
(古典通信路)
1e
QKD装置
101b
101a
量子鍵共有部
量子鍵共有部
108
設定部
110
記憶部
107
配分部
109
通信部
102a
シフティング処理部
103a
誤り訂正処理部
104a
秘匿性増強処理部
105a
鍵管理部
106a
鍵利用部
102b
シフティング処理部
103b
誤り訂正処理部
104b
秘匿性増強処理部
105b
鍵管理部
106b
鍵利用部
102c
シフティング処理部
103c
誤り訂正処理部
104c
秘匿性増強処理部
105c
鍵管理部
106c
鍵利用部
2e
QKD装置
201b
201a
量子鍵共有部
量子鍵共有部
207
配分部
209
通信部
208
設定部
210
記憶部
202a
シフティング処理部
203a
誤り訂正処理部
204a
秘匿性増強処理部
205a
鍵管理部
206a
鍵利用部
202b
シフティング処理部
203b
誤り訂正処理部
204b
秘匿性増強処理部
205b
鍵管理部
206b
鍵利用部
202c
シフティング処理部
203c
誤り訂正処理部
204c
秘匿性増強処理部
205c
鍵管理部
206c
鍵利用部