(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6400441号
(P6400441)

(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
H04B 10/70	(2013.01)	H04B	9/00	370

請求項の数 7　(全 25 頁)

(21)出願番号　特願2014-234947(P2014-234947)
(22)出願日　平成26年11月19日(2014.11.19)
(65)公開番号　特開2016-100693(P2016-100693A)
(43)公開日　平成28年5月30日(2016.5.30)
審査請求日　平成29年9月8日(2017.9.8)

(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　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
(72)発明者　佐藤　英昭
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　土井　一右
東京都港区芝浦一丁目１番１号　株式会社東芝内

最終頁に続く

(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)【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、同一の暗号鍵を生成して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た前記他の量子鍵配送装置との量子鍵配送により生成された光子ビット列に対するシフティング処理を含む鍵蒸留処理のうち少なくとも一部の処理である第１処理を実行し、前記第１処理の少なくとも一部を実行するハードウェア回路を含む第１処理手段と、
前記第１処理以外の前記鍵蒸留処理である第２処理を実行し、前記第２処理の少なくとも一部を実行するハードウェア回路を含む第２処理手段と、
前記第１処理手段および前記第２処理手段の動作を制御する制御手段と、
を備え、
前記第１処理手段は、前記第１処理により生成した中間データを記憶手段に記憶させ、
前記第２処理手段は、前記記憶手段に記憶された前記中間データから、前記第２処理によって前記暗号鍵を生成し、
前記第１処理手段および前記第２処理手段は、前記鍵蒸留処理の処理結果を含む実行ログを前記記憶手段に記憶させ、
前記制御手段は、前記実行ログ、前記第１処理による前記中間データの生成速度、前記第２処理による前記暗号鍵の生成速度、前記中間データのサイズまたは蓄積量、および前記記憶手段のデータ記憶量の少なくともいずれかに基づいて、前記第１処理手段および前

記第２処理手段の動作パラメータ、前記鍵蒸留処理の実行タイミング、および前記記憶手段の利用可能な記憶領域の少なくともいずれかを変更することにより、前記第１処理による前記中間データの生成速度、および前記第２処理による前記暗号鍵の生成速度を調整する量子鍵配送装置。

【請求項２】

前記第１処理手段および前記第２処理手段は、双方全体として、

前記光子ビット列から、前記シフティング処理により共有ビット列を生成し、前記共有ビット列を前記記憶手段に記憶させる第１鍵蒸留処理手段と、

前記記憶手段に記憶された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して、訂正後ビット列を生成し、前記訂正後ビット列を前記記憶手段に記憶させる第２鍵蒸留処理手段と、

前記記憶手段に記憶された前記訂正後ビット列から、秘匿性増強処理により暗号鍵を生成する第３鍵蒸留処理手段と、

を含む請求項１に記載の量子鍵配送装置。

【請求項３】

前記制御手段は、前記実行ログ、前記第１処理による前記中間データの生成速度、前記第２処理による前記暗号鍵の生成速度、前記中間データのサイズまたは蓄積量、および前記記憶手段のデータ記憶量の少なくともいずれかに基づいて、前記第１処理により生成される前記中間データを蓄積することが可能な記憶領域のサイズ、および前記第２処理により生成される前記暗号鍵を蓄積することが可能な記憶領域のサイズのうち少なくともいずれか１つを変更する請求項１に記載の量子鍵配送装置。

【請求項４】

前記第１処理手段による前記第１処理、および前記第２処理手段による前記第２処理の実行の際に必要となる制御データを前記他の量子鍵配送装置と通信する１つの通信手段を、さらに備え、

前記制御手段は、前記通信手段の前記制御データの通信動作を制御する請求項１に記載の量子鍵配送装置。

【請求項５】

前記制御手段は、前記第１処理による前記中間データの生成速度、および前記第２処理による前記暗号鍵の生成速度の調整とは別に、前記通信手段の通信帯域を観測し、前記通信帯域に応じて、前記第１処理および前記第２処理のアルゴリズムを変更して、前記制御データの通信量を調整する請求項４に記載の量子鍵配送装置。

【請求項６】

請求項１～５のいずれか一項に記載の量子鍵配送装置を複数備え、

前記複数の量子鍵配送装置は、前記量子通信路によって接続され、該量子通信路を介した前記量子鍵配送、および前記鍵蒸留処理により、同一の前記暗号鍵を生成する量子鍵配送システム。

【請求項７】

他の量子鍵配送装置と量子通信路で接続され、同一の暗号鍵を生成して共有する量子鍵配送装置の量子鍵配送方法であって、

前記量子通信路を介した前記他の量子鍵配送装置との量子鍵配送により生成された光子ビット列に対するシフティング処理を含む鍵蒸留処理のうち少なくとも一部の処理である第１処理を実行し、かつ、前記第１処理の少なくとも一部を集積回路により実行させる第１処理ステップと、

前記第１処理以外の前記鍵蒸留処理である第２処理を実行し、かつ、前記第２処理の少なくとも一部を集積回路により実行させる第２処理ステップと、

前記第１処理により生成した中間データを記憶手段に記憶させる記憶ステップと、

前記記憶手段に記憶された前記中間データから、前記第２処理によって前記暗号鍵を生成する生成ステップと、

前記鍵蒸留処理の処理結果を含む実行ログを前記記憶手段に記憶させるステップと、

前記実行ログ、前記第１処理による前記中間データの生成速度、前記第２処理による前記暗号鍵の生成速度、前記中間データのサイズまたは蓄積量、および前記記憶手段のデータ記憶量の少なくともいずれかに基づいて、前記第１処理および前記第２処理の動作パラメータ、前記鍵蒸留処理の実行タイミング、および前記記憶手段の利用可能な記憶領域の少なくともいずれかを変更することにより、前記第１処理による前記中間データの生成速度、および前記第２処理による前記暗号鍵の生成速度を調整するステップと、

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、光ファイバリンク（量子通信路）を介して、光子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。共有される暗号鍵の単位時間あたりの生成量をセキュア鍵レートという。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、セキュア鍵レートが高いほど高性能な量子鍵配送システムであると言える。

【０００４】

このような量子鍵配送システムにおいて、量子鍵配送のための光学処理装置、高速信号処理部、およびＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）が直列に接続され、相手の通信装置との通信内容に応じて、高速信号処理部に鍵蒸留処理を実行させるのか、ＣＰＵに鍵蒸留処理を実行させるのかを切り替えるものがある。このように、鍵蒸留処理に必要な処理負荷および通信負荷の分散をして、処理の高速化を図っている。

【０００５】

しかし、上述のような量子鍵配送システムにおいては、光学処理装置、高速信号処理部、およびＣＰＵが直列に接続されて、順次、データを受け渡す処理のため、一部の処理モジュール（例えば、高速信号処理部）が停止すると、その前段または後段の処理が停止するという問題点がある。さらに、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の複数の異なるアルゴリズムを含むため、単一の高速信号処理モジュールのみで構成するものとした場合、鍵蒸留処理ごとに最適な構成の高速信号処理部を実現することができないという問題点もある。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】特開２０１１－１６６２９２号公報

【発明の概要】

【発明が解決しようとする課題】

【０００７】

本発明は、上記に鑑みてなされたものであって、鍵蒸留処理を構成する各処理の一部が停止しても他の処理の動作が継続可能で、かつ、鍵蒸留処理を高速化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】
【０００８】
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、同一の暗号鍵を生成して共有する量子鍵配送装置であって、第１処理手段と、第２処理手段と、制御手段と、を備える。第１処理手段は、量子通信路を介した他の量子鍵配送装置との量子鍵配送により生成された光子ビット列に対するシフティング処理を含む鍵蒸留処理のうち少なくとも一部の処理である第１処理を実行し、第１処理の少なくとも一部を実行するハードウェア回路を含み、第１処理により生成した中間データを記憶手段に記憶させる。第２処理手段は、第１処理以外の鍵蒸留処理である第２処理を実行し、第２処理の少なくとも一部を実行するハードウェア回路を含み、記憶手段に記憶された中間データから、第２処理によって暗号鍵を生成する。第１処理手段および第２処理手段は、鍵蒸留処理の処理結果を含む実行ログを記憶手段に記憶させる。制御手段は、第１処理手段および第２処理手段の動作を制御し、実行ログ、第１処理による中間データの生成速度、第２処理による暗号鍵の生成速度、中間データのサイズまたは蓄積量、および記憶手段のデータ記憶量の少なくともいずれかに基づいて、第１処理手段および第２処理手段の動作パラメータ、鍵蒸留処理の実行タイミング、および記憶手段の利用可能な記憶領域の少なくともいずれかを変更することにより、第１処理による中間データの生成速度、および第２処理による暗号鍵の生成速度を調整する。
【図面の簡単な説明】
【０００９】
【図１】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２】図２は、量子鍵配送システムの全体構成の別の一例を示す図である。
【図３】図３は、ＱＫＤ装置のハードウェア構成の一例を示す図である。
【図４】図４は、ＱＫＤ受信機の機能ブロック構成の一例を示す図である。
【図５】図５は、ＱＫＤ送信機の機能ブロック構成の一例を示す図である。
【図６】図６は、ＱＫＤ受信機およびＱＫＤ送信機の動作を示すシーケンス図である。
【図７】図７は、ＱＫＤ受信機におけるデータの流れを模式的に示す図である。
【図８】図８は、秘匿性増強処理を説明する図である。
【発明を実施するための形態】
【００１０】
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。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。
【００１１】
（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２は、量子鍵配送システムの全体構成の別の一例を示す図である。図１および２を参照しながら、量子鍵配送システム５００の全体構成について説明する。
【００１２】
図１に示すように、量子鍵配送システム５００は、例えば、１つのＱＫＤ受信機に対して、複数のＱＫＤ受信機（図１の場合、３つのＱＫＤ受信機）が接続されたＱＡＮ（Ｑｕａｎｔｕｍ　Ａｃｃｅｓｓ　Ｎｅｔｗｏｒｋ：量子アクセスネットワーク）であるものとして説明する。なお、このＱＡＮは、量子鍵配送システムの一例であり、この構成に限定されるものではない。量子鍵配送システム５００は、ＱＫＤ受信機１と、ＱＫＤ送信機２ａ～２ｃと、光学機器４と、を含んで構成されている。ＱＫＤ受信機１は、量子通信路となる光ファイバリンク３ｄによって、光学機器４に接続されている。ＱＫＤ送信機２ａ～２ｃも、それぞれ量子通信路となる光ファイバリンク３ａ～３ｃによって、光学機器４に接続されている。なお、以下、ＱＫＤ送信機２ａ～２ｃを区別なく呼称する場合、または

総称する場合、単に「ＱＫＤ送信機２」というものとする。また、図１に示す量子鍵配送システム５００では、ＱＫＤ送信機２が３つである場合を示しているが、これに限定されるものではなく、その他の数のＱＫＤ送信機２を含むものとしてもよい。ここで、ＱＫＤ送信機２が１つである場合、光学機器４を介する必要はなく、直接、ＱＫＤ受信機１と接続するものとすればよい。

【００１３】

ＱＫＤ送信機２ａ～２ｃは、例えば、乱数によって発生させたビット列（以下、ＱＫＤ送信機２側における「光子ビット列」という）に基づいて発生させた、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、それぞれ光学機器４を介して、ＱＫＤ受信機１へ送信する装置である。ＱＫＤ送信機２ａ～２ｃは、それぞれ光子ビット列を基に、シフティング処理、誤り訂正処理（ＥＣ（Ｅｒｒｏｒ　Ｃｏｒｒｅｃｔｉｏｎ）処理）および秘匿性増強処理（ＰＡ（Ｐｒｉｖａｃｙ　Ａｍｐｌｉｆｉｃａｔｉｏｎ）処理）を実行して、暗号鍵を生成する。なお、シフティング処理、ＥＣ処理およびＰＡ処理の動作の詳細は後述する。また、シフティング処理、ＥＣ処理およびＰＡ処理の少なくともいずれかを示す場合、または総称する場合、「鍵蒸留処理」というものとする。

【００１４】

ＱＫＤ受信機１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、光学機器４を介して、ＱＫＤ送信機２ａ～２ｃそれぞれから受信する装置である。ＱＫＤ受信機１は、受信した光子列を読み取ることによって得た光子ビット列を基に、シフティング処理、ＥＣ処理およびＰＡ処理等を実行して、ＱＫＤ送信機２ａ～２ｃがそれぞれ生成した暗号鍵と同一の暗号鍵を生成する。すなわち、ＱＫＤ受信機１は、ＱＫＤ送信機２ａとの間で同一の暗号鍵を共有し、ＱＫＤ送信機２ｂとの間で同一の暗号鍵を共有し、さらに、ＱＫＤ送信機２ｃとの間で同一の暗号鍵を共有する。

【００１５】

光ファイバリンク３ａ～３ｄは、ＱＫＤ受信機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。

【００１６】

光学機器４は、ＱＫＤ送信機２ａ～２ｃから出力された単一光子から構成される光子列を、ＱＫＤ受信機１に中継する機器である。

【００１７】

このようなＱＫＤ受信機１とＱＫＤ送信機２とを含む量子鍵配送システム５００において、ＱＫＤ送信機２が送信した単一光子を量子通信路である光ファイバリンク３ａ～３ｄ上で盗聴者が観測すると、光子の物理的変化が発生し、光子を受信したＱＫＤ受信機１は、盗聴者に光子を観測されたことを知ることができる。

【００１８】

なお、図示していないが、ＱＫＤ受信機１とＱＫＤ送信機２ａ～２ｃとは、光ファイバリンク３ａ～３ｄの量子通信路以外に、通常の「０」と「１」と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。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。また、上述のように光ファイバリンク３ａ～３ｄの量子通信路と、デジタルデータを通信する古典通信路とは、別体であることに限定されるものではない。すなわち、同一の光ファイバにおいてＷＤＭ（Ｗａｖｅｌｅｎｇｔｈ　Ｄｉｖｉｓｉｏｎ　Ｍｕｌｔｉｐｌｅｘ：光波長多重化）技術により、単一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を形成するものとしてもよい。この場合、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。

【００１９】

また、ＱＫＤ受信機１およびＱＫＤ送信機２を総称する場合、「ＱＫＤ装置」というものとする。

【００２０】

また、図１に示す量子鍵配送システム５００は、１つのＱＫＤ受信機に対して、複数の

ＱＫＤ送信機が接続されたＱＡＮ（量子アクセスネットワーク）を構成するものとしたが、上述のように量子鍵配送システムの一例であって、これに限定されるものではない。例えば、ＱＫＤ受信機１を複数とし、１つのＱＫＤ送信機２に接続される量子鍵配送システムであってもよい。さらに、図１に示す量子鍵配送システム５００のように複数のＱＫＤ送信機２が光学機器４を介して１つのＱＫＤ受信機１に接続されるのではなく、図２に示す量子鍵配送システム５００ａのように１つのＱＫＤ受信機１が、直接、１つのＱＫＤ送信機２に接続される基本構成であってもよい。

【００２１】

図３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を参照しながら、ＱＫＤ受信機１およびＱＫＤ送信機２のハードウェア構成について説明する。

【００２２】

図３に示すように、ＱＫＤ受信機１は、ＣＰＵ１００と、第１鍵蒸留処理装置１０１と、第２鍵蒸留処理装置１０２と、第３鍵蒸留処理装置１０３と、光学処理装置１０４と、ＲＯＭ１０５と、ＲＡＭ１０６と、記憶装置１０７と、各部を接続するバス１１０と、を備えている。

【００２３】

ＣＰＵ１００は、ＱＫＤ受信機１全体の動作を制御する演算装置である。

【００２４】

第１鍵蒸留処理装置１０１は、光学処理装置１０４より受信した光子ビット列から、後述する共有ビット列を生成するシフティング処理を実行する専用のハードウェア装置である。第１鍵蒸留処理装置１０１は、生成した共有ビット列を記憶装置１０７に記憶させる。第１鍵蒸留処理装置１０１は、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構成される。また、このハードウェア回路は、コプロセッサもしくはＧＰＵ（Ｇｒａｐｈｉｃ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）等であっても、またはそれらを含む構成であってもよい。

【００２５】

第２鍵蒸留処理装置１０２は、第１鍵蒸留処理装置１０１により生成され記憶装置１０７に記憶された共有ビット列のビット誤りを訂正して、訂正後のビット列である訂正後ビット列を生成するＥＣ処理を実行する専用のハードウェア装置である。第２鍵蒸留処理装置１０２は、生成した訂正後ビット列を記憶装置１０７に記憶させる。第２鍵蒸留処理装置１０２は、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構成される。また、このハードウェア回路は、コプロセッサもしくはＧＰＵ等であっても、またはそれらを含む構成であってもよい。

【００２６】

第３鍵蒸留処理装置１０３は、第２鍵蒸留処理装置１０２により生成され記憶装置１０７に記憶された訂正後ビット列に対して、第２鍵蒸留処理装置１０２により訂正した誤りの数から、シフティング処理およびＥＣ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取り除いて鍵ビット列（暗号鍵）を生成するＰＡ処理を実行する専用のハードウェア装置である。第３鍵蒸留処理装置１０３は、生成した暗号鍵を記憶装置１０７に記憶させる。第３鍵蒸留処理装置１０３は、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構成される。また、このハードウェア回路は、コプロセッサもしくはＧＰＵ等であっても、またはそれらを含む構成であってもよい。

【００２７】

光学処理装置１０４は、量子通信路を介して、ＱＫＤ送信機２から光子列を受信する光学装置である。光学処理装置１０４は、受信した光子列を、ランダムに発生させた基底情報に基づいて読み取ることによって光子ビット列を得る。光学処理装置１０４は、光子ビット列および基底情報を第１鍵蒸留処理装置１０１に送信するため、第１鍵蒸留処理装置１０１に電気的に接続されている。

【００２８】
ＲＯＭ１０５は、ＣＰＵ１００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。ＲＡＭ１０６は、ＣＰＵ１００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。
【００２９】
記憶装置１０７は、ＣＰＵ１００で実行される各種プログラム、ならびに第１鍵蒸留処理装置１０１、第２鍵蒸留処理装置１０２および第３鍵蒸留処理装置１０３がそれぞれ生成した共有ビット列、訂正後ビット列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。記憶装置１０７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。
【００３０】
通信Ｉ／Ｆ１０８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、ＱＫＤ送信機２と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／Ｆ１０８は、例えば、１０Ｂａｓｅ－Ｔ、１００Ｂａｓｅ－ＴＸもしくは１０００Ｂａｓｅ－Ｔ等のＥｔｈｅｒｎｅｔ（登録商標）に対応した有線ネットワークのインターフェースである。
【００３１】
なお、図３では、光学処理装置１０４は、第１鍵蒸留処理装置１０１に接続されているものとしているが、これに限定されるものではない。すなわち、光学処理装置１０４は、バス１１０に接続されるものとし、光子ビット列を、バス１１０を介して、第１鍵蒸留処理装置１０１に送信される構成としてもよい。
【００３２】
また、図３では、第１鍵蒸留処理装置１０１、第２鍵蒸留処理装置１０２および第３鍵蒸留処理装置１０３は、それぞれ独立したハードウェア装置として示したが、これに限定されるものではない。例えば、第１鍵蒸留処理装置１０１と第２鍵蒸留処理装置１０２とを１つのハードウェア装置とし、または、第２鍵蒸留処理装置１０２と第３鍵蒸留処理装置１０３とを１つのハードウェア装置として、全体として２つのハードウェア装置として構成するものとしてもよい。例えば、第１鍵蒸留処理装置１０１と第２鍵蒸留処理装置１０２とを１つのハードウェア装置とした場合、この１つのハードウェア装置とした第１鍵蒸留処理装置１０１および第２鍵蒸留処理装置１０２が「第１処理手段」に相当し、鍵蒸留処理のうちシフティング処理およびＥＣ処理が「第１処理」に相当する。また、残りの第３鍵蒸留処理装置１０３が「第２処理手段」に相当し、鍵蒸留処理のうちＰＡ処理が「第２処理」に相当する。
【００３３】
図３に示すように、ＱＫＤ送信機２は、ＣＰＵ２００と、第１鍵蒸留処理装置２０１と、第２鍵蒸留処理装置２０２と、第３鍵蒸留処理装置２０３と、光学処理装置２０４と、ＲＯＭ２０５と、ＲＡＭ２０６と、記憶装置２０７と、通信Ｉ／Ｆ２０８と、各部を接続するバス２１０と、を備えている。
【００３４】
ＣＰＵ２００は、ＱＫＤ送信機２全体の動作を制御する演算装置である。
【００３５】
第１鍵蒸留処理装置２０１は、光学処理装置２０４より受信した光子ビット列から、共有ビット列を生成するシフティング処理を実行する専用のハードウェア装置である。第１鍵蒸留処理装置２０１は、生成した共有ビット列を記憶装置２０７に記憶させる。第１鍵蒸留処理装置２０１は、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構成される。また、このハードウェア回路は、コプロセッサもしくはＧＰＵ等であっても、またはそれらを含む構成であってもよい。
【００３６】
第２鍵蒸留処理装置２０２は、第１鍵蒸留処理装置２０１により生成され記憶装置２０

７に記憶された共有ビット列のビット誤りを訂正して、訂正後のビット列である訂正後ビット列を生成するＥＣ処理を実行する専用のハードウェア装置である。第２鍵蒸留処理装置２０２は、生成した訂正後ビット列を記憶装置２０７に記憶させる。第２鍵蒸留処理装置２０２は、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構成される。また、このハードウェア回路は、コプロセッサもしくはＧＰＵ等であっても、またはそれらを含む構成であってもよい。

【００３７】

第３鍵蒸留処理装置２０３は、第２鍵蒸留処理装置２０２により生成され記憶装置２０７に記憶された訂正後ビット列に対して、第２鍵蒸留処理装置２０２により訂正した誤りの数から、シフティング処理およびＥＣ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取り除いて鍵ビット列（暗号鍵）を生成するＰＡ処理を実行する専用のハードウェア装置である。第３鍵蒸留処理装置２０３は、生成した暗号鍵を記憶装置２０７に記憶させる。第３鍵蒸留処理装置２０３は、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構成される。また、このハードウェア回路は、コプロセッサもしくはＧＰＵ等であっても、またはそれらを含む構成であってもよい。

【００３８】

光学処理装置２０４は、例えば、乱数によって発生させたビット列（光子ビット列）に対して、ランダムに発生させた基底情報に基づく状態と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受信機１に送信する光学装置である。光学処理装置２０４は、発生させた光子ビット列および基底情報を第１鍵蒸留処理装置２０１に送信するため、第１鍵蒸留処理装置２０１に電気的に接続されている。

【００３９】

ＲＯＭ２０５は、ＣＰＵ２００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。ＲＡＭ２０６は、ＣＰＵ２００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。

【００４０】

記憶装置２０７は、ＣＰＵ２００で実行される各種プログラム、ならびに第１鍵蒸留処理装置２０１、第２鍵蒸留処理装置２０２および第３鍵蒸留処理装置２０３がそれぞれ生成した共有ビット列、訂正後ビット列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。記憶装置２０７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。

【００４１】

通信Ｉ／Ｆ２０８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、ＱＫＤ受信機１と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／Ｆ２０８は、例えば、１０Ｂａｓｅ－Ｔ、１００Ｂａｓｅ－ＴＸもしくは１０００Ｂａｓｅ－Ｔ等のＥｔｈｅｒｎｅｔに対応した有線ネットワークのインターフェースである。

【００４２】

なお、図３では、光学処理装置２０４は、第１鍵蒸留処理装置２０１に接続されているものとしているが、これに限定されるものではない。すなわち、光学処理装置２０４は、バス２１０に接続されるものとし、光子ビット列を、バス２１０を介して、第１鍵蒸留処理装置２０１に送信される構成としてもよい。

【００４３】

また、図３では、第１鍵蒸留処理装置２０１、第２鍵蒸留処理装置２０２および第３鍵蒸留処理装置２０３は、それぞれ独立したハードウェア装置として示したが、これに限定されるものではない。例えば、第１鍵蒸留処理装置２０１と第２鍵蒸留処理装置２０２とを１つのハードウェア装置とし、または、第２鍵蒸留処理装置２０２と第３鍵蒸留処理装置２０３とを１つのハードウェア装置として、全体として２つのハードウェア装置として構成するものとしてもよい。例えば、第１鍵蒸留処理装置２０１と第２鍵蒸留処理装置２

０２とを１つのハードウェア装置とした場合、この１つのハードウェア装置とした第１鍵蒸留処理装置２０１および第２鍵蒸留処理装置２０２が「第１処理手段」に相当し、鍵蒸留処理のうちシフティング処理およびＥＣ処理が「第１処理」に相当する。また、残りの第３鍵蒸留処理装置２０３が「第２処理手段」に相当し、鍵蒸留処理のうちＰＡ処理が「第２処理」に相当する。

【００４４】

以上のように、ＱＫＤ受信機１およびＱＫＤ送信機２において、シフティング処理、ＥＣ処理、およびＰＡ処理の各処理ごとに専用のハードウェア装置によって構成するものとしている。例えば、上述の一連の鍵蒸留処理を専用の１つのハードウェア装置で構成するものとすると、そのような処理が可能な市販のハードウェア装置は存在しないので、設計・実装が必要になりコストが高くなる。これは、例えば、ＰＡ処理において、量子暗号の安全性を踏まえた効率的な処理を実行するためには、入力となる訂正後ビット列のサイズを非常に大きくする必要があり（例えば、１００［Ｍｂｉｔ］等）、単一のハードウェア装置で実装することが困難な回路規模となる可能性があり、さらに、各鍵蒸留処理によってハードウェア特性が異なるためである。一方、図３に示したように、鍵蒸留処理ごとに専用のハードウェア装置により構成した場合、個々のハードウェア装置のサイズを小さくすることができ、市販のハードウェア装置を利用することもできるので低コスト化を実現することができる。さらに、各鍵蒸留処理について最適なハードウェア装置を選定することができ、鍵蒸留処理の高速化を図ることができる。

【００４５】

図４は、ＱＫＤ受信機の機能ブロック構成の一例を示す図である。図４を参照しながら、ＱＫＤ受信機１の機能ブロック構成について説明する。

【００４６】

図４に示すように、ＱＫＤ受信機１は、制御部１０（制御手段）と、第１鍵蒸留処理部１１（第１鍵蒸留処理手段）と、第２鍵蒸留処理部１２（第２鍵蒸留処理手段）と、第３鍵蒸留処理部１３（第３鍵蒸留処理手段）と、光学処理部１４と、蓄積部１５（記憶手段）と、通信部１６（通信手段）と、を有する。

【００４７】

第１鍵蒸留処理部１１は、光学処理部１４から光子ビット列および基底情報を受信する機能部である。次に、第１鍵蒸留処理部１１は、ＱＫＤ送信機２（光学処理部２４）が光子列を送信するためにランダムに発生させた基底情報を、通信部１６および古典通信路を介して受信する。また、第１鍵蒸留処理部１１は、光学処理部１４から受信した基底情報と、第１鍵蒸留処理部２１から受信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。そして、第１鍵蒸留処理部１１は、蓄積部１５に、シフティング処理により生成した共有ビット列を第１中間データ６１ａとして記憶させると共に、シフティング処理により得られるパラメータ等を含むログデータ（例えば、シフティング処理における量子ビット誤り率の情報）を第１実行ログ７１ａとして記憶させる。第１鍵蒸留処理部１１は、図３に示す第１鍵蒸留処理装置１０１によって実現される。ここで、共有ビット列の長さは、光学処理部２４および第１鍵蒸留処理部１１がランダムに発生させた基底情報に基づいて定まるので、基底情報の選択が真にランダムである場合、統計上、光子ビット列の略１／２の長さとなる。なお、ここで説明したシフティング処理は一例であり、これ以外の方法であってもよい。

【００４８】

第２鍵蒸留処理部１２は、通信部１６および古典通信路を介して、第２鍵蒸留処理部２２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、訂正後のビット列である訂正後ビット列を生成するＥＣ処理を実行する機能部である。第２鍵蒸留処理部１２は、蓄積部１５に、ＥＣ処理により生成した訂正後ビット列を第２中間データ６２ａとして記憶させると共に、ＥＣ処理により得られるパラメータ等を含むログデータ（例えば、ＥＣ処理において訂正を行った結果得られた誤り率の情報）を第

２実行ログ７２ａとして記憶させる。第２鍵蒸留処理部１２は、図３に示す第２鍵蒸留処理装置１０２によって実現される。この第２鍵蒸留処理部１２が生成した訂正後ビット列は、後述する第２鍵蒸留処理部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。

【００４９】

第３鍵蒸留処理部１３は、通信部１６および古典通信路を介して、第３鍵蒸留処理部２３と制御データ（ＰＡ情報）を送信し、第２鍵蒸留処理部１２により訂正した誤りの数から、シフティング処理およびＥＣ処理の際に盗聴者に盗聴された可能性のあるビットを取り除いて鍵ビット列（暗号鍵）を生成するＰＡ処理を実行する機能部である。第３鍵蒸留処理部１３は、蓄積部１５に、ＰＡ処理により生成した暗号鍵を鍵データ６３ａとして記憶させると共に、ＰＡ処理により得られるパラメータ等を含むログデータを第３実行ログ７３ａとして記憶させる。第３鍵蒸留処理部１３は、図３に示す第３鍵蒸留処理装置１０３によって実現される。なお、ここで説明したＰＡ処理は一例であり、これ以外の方法であってもよい。

【００５０】

なお、第１鍵蒸留処理部１１、第２鍵蒸留処理部１２および第３鍵蒸留処理部１３を、鍵蒸留処理を実行する機能部として区別なく呼称する場合、または総称する場合、以下、単に「鍵蒸留処理部」という場合があるものとする。

【００５１】

光学処理部１４は、量子通信路を介して、ＱＫＤ送信機２（光学処理部２４）から光子列を受信する機能部である。光学処理部１４は、受信した光子列を、ランダムに発生させた基底情報に基づいて読み取ることによって光子ビット列を得る。光学処理部１４は、光子ビット列および基底情報を第１鍵蒸留処理部１１に送る。光学処理部１４は、図３に示す光学処理装置１０４によって実現される。

【００５２】

蓄積部１５は、各種データを記憶する機能部である。蓄積部１５が記憶するデータの例として、図４に示すように、第１中間データ６１ａ、第２中間データ６２ａ、鍵データ６３ａ、第１実行ログ７１ａ、第２実行ログ７２ａ、および第３実行ログ７３ａがある。蓄積部１５は、図３に示す記憶装置１０７によって実現される。なお、蓄積部１５は、記憶装置１０７により実現されることに限定されるものではなく、ＲＡＭ１０６のような揮発性記憶装置によって実現されるものとしてもよい。また、ＱＫＤ受信機１において、第１中間データ６１ａおよび第２中間データ６２ａを区別なく呼称する場合、または総称する場合、単に「中間データ」というものとする。また、ＱＫＤ受信機１において、第１実行ログ７１ａ、第２実行ログ７２ａおよび第３実行ログ７３ａを区別なく呼称する場合、または総称する場合、単に「実行ログ」というものとする。

【００５３】

第１中間データ６１ａは、上述のように、第１鍵蒸留処理部１１のシフティング処理により生成された共有ビット列である。第２中間データ６２ａは、上述のように、第２鍵蒸留処理部１２のＥＣ処理により生成された訂正後ビット列である。鍵データ６３ａは、上述のように、第３鍵蒸留処理部１３のＰＡ処理により生成された暗号鍵である。

【００５４】

第１実行ログ７１ａは、第１鍵蒸留処理部１１のシフティング処理により得られるパラメータ等を含むログデータ等である。第１実行ログ７１ａは、例えば、シフティング処理における量子ビット誤り率の情報、または、後段の第２鍵蒸留処理部１２のＥＣ処理のために利用されるシフティング処理の際の付属的な情報を含む。

【００５５】

第２実行ログ７２ａは、第２鍵蒸留処理部１２のＥＣ処理により得られるパラメータ等を含むログデータ等である。第２実行ログ７２ａは、例えば、ＥＣ処理におけるビット誤り率の情報、または、後段の第３鍵蒸留処理部１３のＰＡ処理のために利用されるＥＣ処

理の際の付属的な情報を含む。

【００５６】

第３実行ログ７３ａは、第３鍵蒸留処理部１３のＰＡ処理により得られるパラメータ等を含むログデータ等である。

【００５７】

なお、蓄積部１５に記憶される上述の中間データ、鍵データ６３ａ、および実行ログの記憶方式は、どのような方式であってもよい。例えば、中間データ、鍵データ６３ａおよび実行ログを、それぞれファイルシステム上のファイルとして記憶する方式が考えられる。ファイルシステムは、メディアの種類に依存せず利用可能であり、例えば、蓄積部１５がＲＡＭ１０６上にファイルシステムを構築することによって、高速アクセス可能なファイルシステムとすることもできる。

【００５８】

通信部１６は、制御部１０の制御に従って、各鍵蒸留処理部がＱＫＤ送信機２と制御データを送受信するための古典通信路を形成するための通信インターフェースとして機能する機能部である。通信部１６は、図３に示す通信Ｉ／Ｆ１０８によって実現される。なお、通信部１６は、有線通信用または無線通信用のいずれのインターフェースであってもよい。

【００５９】

制御部１０は、鍵蒸留処理の動作全体を制御する機能部である。制御部１０は、図４に示すように、中央制御部５０ａと、シフティング制御部５１ａと、ＥＣ制御部５２ａと、ＰＡ制御部５３ａと、を有する。制御部１０は、図３に示すＣＰＵ１００によって実現される。

【００６０】

中央制御部５０ａは、各鍵蒸留処理部の処理結果（実行ログ）、処理速度、動作パラメータ、中間データ、および鍵データ６３ａ等をモニタリングする機能部である。中央制御部５０ａは、モニタリングの結果に基づいて、シフティング制御部５１ａ、ＥＣ制御部５２ａおよびＰＡ制御部５３ａそれぞれに、各鍵蒸留処理の実行タイミングまたは動作パラメータ等の指示または変更を行う。中央制御部５０ａは、図３に示すＣＰＵ１００により実行されるプログラムによって実現される。

【００６１】

中央制御部５０ａは、例えば、蓄積部１５に記憶された実行ログ、中間データまたは鍵データ６３ａのサイズに基づいて、シフティング制御部５１ａに対して共有ビット列のサイズの変更を指示し、第１鍵蒸留処理部１１が利用する蓄積部１５の記憶領域のサイズを調整させる。また、中央制御部５０ａは、例えば、蓄積部１５に記憶された第１鍵蒸留処理部１１の実行ログである第１中間データ６１ａに含まれる量子ビット誤り率に基づいて、ＥＣ制御部５２ａに対して、第２鍵蒸留処理部１２によるＥＣ処理で用いるアルゴリズムのパラメータの修正を指示し、ＥＣ処理の効率を向上させる。また、中央制御部５０ａは、例えば、蓄積部１５に記憶された実行ログ、中間データまたは鍵データ６３ａのサイズに基づいて、ＰＡ制御部５３ａに対して、第３鍵蒸留処理部１３に実行させるＰＡ処理の実行タイミングを変更し、第２中間データ６２ａのために利用される蓄積部１５の記憶領域のサイズを縮小し、結果として、最終的な鍵データ６３ａ（暗号鍵）が生成される総合的な速度を向上させる。

【００６２】

このように、中央制御部５０ａは、各鍵蒸留処理部の処理結果（実行ログ）、処理速度、動作パラメータ、中間データおよび暗号鍵等を把握することができ、それらによって、各鍵蒸留処理部の動作を総合的に制御している。また、各鍵蒸留処理部の間で速度差があったり、蓄積部１５において利用できる記憶領域が上限に近づくことにより、複数の鍵蒸留処理部のうち一部がボトルネックとなり総合的な動作速度が十分に向上しない場合がある。このような場合に、中央制御部５０ａは、各鍵蒸留処理部の動作パラメータもしくは実行タイミング、または利用可能な記憶領域等を変更することにより、各鍵蒸留処理部間

の処理速度のバランスを調整し、総合的な量子鍵配送速度を向上させることができる。

【００６３】

また、中央制御部５０ａは、古典通信路を利用してデータ通信をする場合、単一の通信部１６を制御してデータ通信を行う。これによって、各鍵蒸留処理の順序制御の実現が可能となる。

【００６４】

また、中央制御部５０ａは、蓄積部１５のデータ記憶量および通信部１６をモニタリングする。これによって、例えば、中央制御部５０ａは、蓄積部１５における空き領域が逼迫した場合、シフティング制御部５１ａ、ＥＣ制御部５２ａおよびＰＡ制御部５３ａに指示して、各鍵蒸留処理において出力される中間データおよび暗号鍵のサイズを調整して、蓄積部１５の空き容量の逼迫状態を回避することができる。また、例えば、中央制御部５０ａは、通信部１６における通信帯域が逼迫した場合、シフティング制御部５１ａ、ＥＣ制御部５２ａおよびＰＡ制御部５３ａに指示して、各鍵蒸留処理に対してデータ通信量の少ないアルゴリズム（処理内容）に変更して、通信部１６における通信帯域の逼迫状態を回避することができる。一方、通信帯域に余裕がある場合、中央制御部５０ａは、各鍵蒸留処理に対してデータ通信量を大きくするアルゴリズムに変更するものとしてもよい。

【００６５】

シフティング制御部５１ａは、第１鍵蒸留処理装置１０１を動作制御するドライバとして機能する機能部である。また、シフティング制御部５１ａは、中央制御部５０ａからの動作パラメータまたは実行タイミングの指示および変更に従って、第１鍵蒸留処理部１１にシフティング処理を実行させる。また、シフティング制御部５１ａは、第１鍵蒸留処理部１１がシフティング処理を実行するために利用する基底情報をＱＫＤ送信機２と通信するために、通信部１６の通信制御を実行する。シフティング制御部５１ａは、図３に示すＣＰＵ１００により実行されるプログラムによって実現される。なお、上述のように、第１鍵蒸留処理部１１によってシフティング処理が実行されるものとしたが、シフティング処理の一部が、シフティング制御部５１ａにより実行されるものとしてもよい。この場合、第１鍵蒸留処理部１１、およびシフティング処理の一部を実行するシフティング制御部５１ａが「第１鍵蒸留処理手段」を構成する。

【００６６】

ＥＣ制御部５２ａは、第２鍵蒸留処理装置１０２を動作制御するドライバとして機能する機能部である。また、ＥＣ制御部５２ａは、中央制御部５０ａからの動作パラメータまたは実行タイミングの指示および変更に従って、第２鍵蒸留処理部１２にＥＣ処理を実行させる。また、ＥＣ制御部５２ａは、第２鍵蒸留処理部１２がＥＣ処理を実行するために利用するＥＣ情報をＱＫＤ送信機２と通信するために、通信部１６の通信制御を実行する。ＥＣ制御部５２ａは、図３に示すＣＰＵ１００により実行させるプログラムによって実現される。なお、上述のように、第２鍵蒸留処理部１２によってＥＣ処理が実行されるものとしたが、ＥＣ処理の一部が、ＥＣ制御部５２ａにより実行されるものとしてもよい。この場合、第２鍵蒸留処理部１２、およびＥＣ処理の一部を実行するＥＣ制御部５２ａが「第２鍵蒸留処理手段」を構成する。

【００６７】

ＰＡ制御部５３ａは、第３鍵蒸留処理装置１０３を動作制御するドライバとして機能する機能部である。また、ＰＡ制御部５３ａは、中央制御部５０ａからの動作パラメータまたは実行タイミングの指示および変更に従って、第３鍵蒸留処理部１３にＰＡ処理を実行させる。また、ＰＡ制御部５３ａは、第３鍵蒸留処理部１３がＰＡ処理を実行するために利用するＰＡ情報をＱＫＤ送信機２に送信するために、通信部１６の通信制御を実行する。ＰＡ制御部５３ａは、図３に示すＣＰＵ１００により実行させるプログラムによって実現される。なお、上述のように、第３鍵蒸留処理部１３によってＰＡ処理が実行されるものとしたが、ＰＡ処理の一部が、ＰＡ制御部５３ａにより実行されるものとしてもよい。この場合、第３鍵蒸留処理部１３、およびＰＡ処理の一部を実行するＰＡ制御部５３ａが「第３鍵蒸留処理手段」を構成する。

【００６８】
なお、上述の中央制御部５０ａ、シフティング制御部５１ａ、ＥＣ制御部５２ａおよびＰＡ制御部５３ａは、それぞれＣＰＵ１００で実行されるプログラムによって実現されるものとしたが、これに限定されるものではなく、少なくとも一部の機能が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。
【００６９】
また、制御部１０の中央制御部５０ａ、シフティング制御部５１ａ、ＥＣ制御部５２ａおよびＰＡ制御部５３ａ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。
【００７０】
図５は、ＱＫＤ送信機の機能ブロック構成の一例を示す図である。図５を参照しながら、ＱＫＤ送信機２の機能ブロック構成について説明する。
【００７１】
図５に示すように、ＱＫＤ送信機２は、制御部２０（制御手段）と、第１鍵蒸留処理部２１（第１鍵蒸留処理手段）と、第２鍵蒸留処理部２２（第２鍵蒸留処理手段）と、第３鍵蒸留処理部２３（第３鍵蒸留処理手段）と、光学処理部２４と、蓄積部２５（記憶手段）と、通信部２６（通信手段）と、を有する。
【００７２】
第１鍵蒸留処理部２１は、光学処理部２４から光子ビット列および基底情報を受信する機能部である。次に、第１鍵蒸留処理部２１は、ＱＫＤ受信機１（光学処理部１４）が光子列を読み取るためにランダムに発生させた基底情報を、通信部２６および古典通信路を介して受信する。また、第１鍵蒸留処理部２１は、光学処理部２４から受信した基底情報と、第１鍵蒸留処理部１１から受信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。そして、第１鍵蒸留処理部２１は、蓄積部２５に、シフティング処理により生成した共有ビット列を第１中間データ６１ｂとして記憶させると共に、シフティング処理により得られるパラメータ等を含むログデータ（例えば、シフティング処理における量子ビット誤り率の情報）を第１実行ログ７１ｂとして記憶させる。第１鍵蒸留処理部２１は、図３に示す第１鍵蒸留処理装置２０１によって実現される。ここで、共有ビット列の長さは、光学処理部２４および第１鍵蒸留処理部１１がランダムに発生させた基底情報に基づいて定まるので、基底情報の選択が真にランダムである場合、統計上、光子ビット列の略１／２の長さとなる。なお、ここで説明したシフティング処理は一例であり、これ以外の方法であってもよい。
【００７３】
第２鍵蒸留処理部２２は、通信部２６および古典通信路を介して、第２鍵蒸留処理部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、訂正後のビット列である訂正後ビット列を生成するＥＣ処理を実行する機能部である。第２鍵蒸留処理部２２は、蓄積部２５に、ＥＣ処理により生成した訂正後ビット列を第２中間データ６２ｂとして記憶させると共に、ＥＣ処理により得られるパラメータ等を含むログデータ（例えば、ＥＣ処理において訂正を行った結果得られた誤り率の情報）を第２実行ログ７２ｂとして記憶させる。第２鍵蒸留処理部２２は、図３に示す第２鍵蒸留処理装置２０２によって実現される。この第２鍵蒸留処理部２２が生成した訂正後ビット列は、第２鍵蒸留処理部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。
【００７４】
第３鍵蒸留処理部２３は、通信部２６および古典通信路を介して、第３鍵蒸留処理部１３から制御データ（ＰＡ情報）を受信し、第２鍵蒸留処理部２２により訂正した誤りの数から、シフティング処理およびＥＣ処理の際に盗聴者に盗聴された可能性のあるビットを取り除いて鍵ビット列（暗号鍵）を生成するＰＡ処理を実行する機能部である。第３鍵蒸

留処理部２３は、蓄積部２５に、ＰＡ処理により生成した暗号鍵を鍵データ６３ｂとして記憶させると共に、ＰＡ処理により得られるパラメータ等を含むログデータを第３実行ログ７３ｂとして記憶させる。第３鍵蒸留処理部２３は、図３に示す第３鍵蒸留処理装置２０３によって実現される。なお、ここで説明したＰＡ処理は一例であり、これ以外の方法であってもよい。

【００７５】

なお、第１鍵蒸留処理部２１、第２鍵蒸留処理部２２および第３鍵蒸留処理部２３を、鍵蒸留処理を実行する機能部として区別なく呼称する場合、または総称する場合、以下、単に「鍵蒸留処理部」という場合があるものとする。

【００７６】

光学処理部２４は、例えば、乱数によって発生させたビット列（光子ビット列）に対して、ランダムに発生させた基底情報に基づく状態とした単一光子から構成される光子列を生成する機能部である。光学処理部２４は、生成した光子列を、量子通信路を介して、ＱＫＤ受信機１（光学処理部１４）に送信する。また、光学処理部２４は、発生させた光子ビット列および基底情報を第１鍵蒸留処理部２１に送る。光学処理部２４は、図３に示す光学処理装置２０４によって実現される。

【００７７】

蓄積部２５は、各種データを記憶する機能部である。蓄積部２５が記憶するデータの例として、図５に示すように、第１中間データ６１ｂ、第２中間データ６２ｂ、鍵データ６３ｂ、第１実行ログ７１ｂ、第２実行ログ７２ｂ、および第３実行ログ７３ｂがある。第１中間データ６１ｂ、第２中間データ６２ｂ、鍵データ６３ｂ、第１実行ログ７１ｂ、第２実行ログ７２ｂ、および第３実行ログ７３ｂの内容は、それぞれ上述の第１中間データ６１ａ、第２中間データ６２ａ、鍵データ６３ａ、第１実行ログ７１ａ、第２実行ログ７２ａ、および第３実行ログ７３ａと同様であるので説明を省略する。蓄積部２５は、図３に示す記憶装置２０７によって実現される。なお、蓄積部２５は、記憶装置２０７により実現されることに限定されるものではなく、ＲＡＭ２０６のような揮発性記憶装置によって実現されるものとしてもよい。また、ＱＫＤ送信機２において、第１中間データ６１ｂおよび第２中間データ６２ｂを区別なく呼称する場合、または総称する場合、単に「中間データ」というものとする。また、ＱＫＤ送信機２において、第１実行ログ７１ｂ、第２実行ログ７２ｂおよび第３実行ログ７３ｂを区別なく呼称する場合、または総称する場合、単に「実行ログ」というものとする。

【００７８】

通信部２６は、制御部２０の制御に従って、各鍵蒸留処理部がＱＫＤ受信機１と制御データを送受信するための古典通信路を形成するための通信インターフェースとして機能する機能部である。通信部２６は、図３に示す通信Ｉ／Ｆ２０８によって実現される。なお、通信部２６は、有線通信用または無線通信用のいずれのインターフェースであってもよい。

【００７９】

制御部２０は、鍵蒸留処理の動作全体を制御する機能部である。制御部２０は、図５に示すように、中央制御部５０ｂと、シフティング制御部５１ｂと、ＥＣ制御部５２ｂと、ＰＡ制御部５３ｂと、を有する。制御部２０は、図３に示すＣＰＵ２００によって実現される。

【００８０】

中央制御部５０ｂは、各鍵蒸留処理部の処理結果（実行ログ）、処理速度、動作パラメータ、中間データ、および鍵データ６３ａ等をモニタリングする機能部である。中央制御部５０ｂは、モニタリングの結果に基づいて、シフティング制御部５１ｂ、ＥＣ制御部５２ｂおよびＰＡ制御部５３ｂそれぞれに、各鍵蒸留処理の実行タイミングまたは動作パラメータ等の指示または変更を行う。中央制御部５０ｂは、図３に示すＣＰＵ２００により実行されるプログラムによって実現される。

【００８１】

中央制御部５０ｂは、例えば、蓄積部２５に記憶された実行ログ、中間データまたは鍵データ６３ｂのサイズに基づいて、シフティング制御部５１ｂに対して共有ビット列のサイズの変更を指示し、第１鍵蒸留処理部２１が利用する蓄積部２５の記憶領域のサイズを調整させる。また、中央制御部５０ｂは、例えば、蓄積部２５に記憶された第１鍵蒸留処理部２１の実行ログである第１中間データ６１ｂに含まれる量子ビット誤り率に基づいて、ＥＣ制御部５２ｂに対して、第２鍵蒸留処理部２２によるＥＣ処理で用いるアルゴリズムのパラメータの修正を指示し、ＥＣ処理の効率を向上させる。また、中央制御部５０ｂは、例えば、蓄積部２５に記憶された実行ログ、中間データまたは鍵データ６３ｂのサイズに基づいて、ＰＡ制御部５３ｂに対して、第３鍵蒸留処理部２３に実行させるＰＡ処理の実行タイミングを変更し、第２中間データ６２ｂのために利用される蓄積部２５の記憶領域のサイズを縮小し、結果として、最終的な鍵データ６３ｂ（暗号鍵）が生成される総合的な速度を向上させる。

【００８２】

このように、中央制御部５０ｂは、各鍵蒸留処理部の処理結果（実行ログ）、処理速度、動作パラメータ、中間データおよび暗号鍵等を把握することができ、それらによって、各鍵蒸留処理部の動作を総合的に制御している。また、各鍵蒸留処理部の間で速度差があったり、蓄積部２５において利用できる記憶領域が上限に近づくことにより、複数の鍵蒸留処理部のうち一部がボトルネックとなり総合的な動作速度が十分に向上しない場合がある。このような場合に、中央制御部５０ｂは、各鍵蒸留処理部の動作パラメータもしくは実行タイミング、または利用可能な記憶領域等を変更することにより、各鍵蒸留処理部間の処理速度のバランスを調整し、総合的な量子鍵配送速度を向上させることができる。

【００８３】

また、中央制御部５０ｂは、古典通信路を利用してデータ通信する場合、単一の通信部２６を制御してデータ通信を行う。これによって、各鍵蒸留処理の順序制御の実現が可能となる。

【００８４】

また、中央制御部５０ｂは、蓄積部２５のデータ記憶量および通信部２６をモニタリングする。これによって、例えば、中央制御部５０ｂは、蓄積部２５における空き領域が逼迫した場合、シフティング制御部５１ｂ、ＥＣ制御部５２ｂおよびＰＡ制御部５３ｂに指示して、各鍵蒸留処理において出力される中間データおよび暗号鍵のサイズを調整して、蓄積部１５の空き容量の逼迫状態を回避することができる。また、例えば、中央制御部５０ｂは、通信部２６における通信帯域が逼迫した場合、シフティング制御部５１ｂ、ＥＣ制御部５２ｂおよびＰＡ制御部５３ｂに指示して、各鍵蒸留処理に対してデータ通信量の少ないアルゴリズム（処理内容）に変更して、通信部２６における通信帯域の逼迫状態を回避することができる。一方、通信帯域に余裕がある場合、中央制御部５０ｂは、各鍵蒸留処理に対してデータ通信量を大きくするアルゴリズムに変更するものとしてもよい。

【００８５】

シフティング制御部５１ｂは、第１鍵蒸留処理装置２０１を動作制御するドライバとしての機能する機能部である。また、シフティング制御部５１ｂは、中央制御部５０ｂからの動作パラメータまたは実行タイミングの指示および変更に従って、第１鍵蒸留処理部２１にシフティング処理を実行させる。また、シフティング制御部５１ｂは、第１鍵蒸留処理部２１がシフティング処理を実行するために利用する基底情報をＱＫＤ受信機１と通信するために、通信部２６の通信制御を実行する。シフティング制御部５１ｂは、図３に示すＣＰＵ２００により実行されるプログラムによって実現される。なお、上述のように、第１鍵蒸留処理部２１によってシフティング処理が実行されるものとしたが、シフティング処理の一部が、シフティング制御部５１ｂにより実行されるものとしてもよい。この場合、第１鍵蒸留処理部２１、およびシフティング処理の一部を実行するシフティング制御部５１ｂが「第１鍵蒸留処理手段」を構成する。

【００８６】

ＥＣ制御部５２ｂは、第２鍵蒸留処理装置２０２を動作制御するドライバとして機能す

る機能部である。また、ＥＣ制御部５２ｂは、中央制御部５０ｂからの動作パラメータまたは実行タイミングの指示および変更に従って、第２鍵蒸留処理部２２にＥＣ処理を実行させる。また、ＥＣ制御部５２ｂは、第２鍵蒸留処理部２２がＥＣ処理を実行するために利用するＥＣ情報をＱＫＤ受信機１と通信するために、通信部２６の通信制御を実行する。ＥＣ制御部５２ｂは、図３に示すＣＰＵ２００により実行させるプログラムによって実現される。なお、上述のように、第２鍵蒸留処理部２２によってＥＣ処理が実行されるものとしたが、ＥＣ処理の一部が、ＥＣ制御部５２ｂにより実行されるものとしてもよい。この場合、第２鍵蒸留処理部２２、およびＥＣ処理の一部を実行するＥＣ制御部５２ｂが「第２鍵蒸留処理手段」を構成する。

【００８７】

ＰＡ制御部５３ｂは、第３鍵蒸留処理装置２０３を動作制御するドライバとして機能する機能部である。また、ＰＡ制御部５３ｂは、中央制御部５０ｂからの動作パラメータまたは実行タイミングの指示および変更に従って、第３鍵蒸留処理部２３にＰＡ処理を実行させる。また、ＰＡ制御部５３ｂは、第３鍵蒸留処理部２３がＰＡ処理を実行するために利用するＰＡ情報をＱＫＤ受信機１から受信するために、通信部２６の通信制御を実行する。ＰＡ制御部５３ｂは、図３に示すＣＰＵ２００により実行させるプログラムによって実現される。なお、上述のように、第３鍵蒸留処理部２３によってＰＡ処理が実行されるものとしたが、ＰＡ処理の一部が、ＰＡ制御部５３ｂにより実行されるものとしてもよい。この場合、第３鍵蒸留処理部２３、およびＰＡ処理の一部を実行するＰＡ制御部５３ｂが「第３鍵蒸留処理手段」を構成する。

【００８８】

なお、上述の中央制御部５０ｂ、シフティング制御部５１ｂ、ＥＣ制御部５２ｂおよびＰＡ制御部５３ｂは、それぞれＣＰＵ２００で実行されるプログラムによって実現されるものとしたが、これに限定されるものではなく、少なくとも一部の機能が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。

【００８９】

また、制御部２０の中央制御部５０ｂ、シフティング制御部５１ｂ、ＥＣ制御部５２ｂおよびＰＡ制御部５３ｂ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。

【００９０】

図６は、ＱＫＤ受信機およびＱＫＤ送信機の動作を示すシーケンス図である。図７は、ＱＫＤ受信機におけるデータの流れを模式的に示す図である。図８は、秘匿性増強処理を説明する図である。図６～８を参照しながら、ＱＫＤ受信機１およびＱＫＤ送信機２による鍵蒸留処理を含めた暗号鍵の生成動作の一連の流れ説明する。なお、ＱＫＤ受信機１におけるデータの流れを図７に模式的に示したが、ＱＫＤ送信機２におけるデータの流れについても同様である。

【００９１】

＜ステップＳ１１＞

ＱＫＤ送信機２の光学処理部２４は、例えば、乱数によって発生させたビット列（光子ビット列）に対して、ランダムに発生させた基底情報に基づく状態とした単一光子から構成される光子列を生成する。光学処理部２４は、生成した光子列を、量子通信路を介して、ＱＫＤ受信機１の光学処理部１４に送信する。また、光学処理部２４は、発生させた光子ビット列および基底情報を第１鍵蒸留処理部２１に送る。

【００９２】

ＱＫＤ受信機１の光学処理部１４は、量子通信路を介して、ＱＫＤ送信機２の光学処理部２４から光子列を受信する。光学処理部１４は、受信した光子列を、ランダムに発生させた基底情報に基づいて読み取ることによって光子ビット列を得る。光学処理部１４は、光子ビット列および基底情報をＱＫＤ受信機１の第１鍵蒸留処理部１１に送る。

【００９３】

＜ステップＳ１２＞

第１鍵蒸留処理部１１は、光学処理部２４が光子列を送信するためにランダムに発生させた基底情報を、通信部１６および古典通信路を介して受信する。第１鍵蒸留処理部２１は、第１鍵蒸留処理部１１が光子列を読み取るためにランダムに発生させた基底情報を、通信部２６および古典通信路を介して受信する。

【００９４】

＜ステップＳ１３＞

ＱＫＤ受信機１のシフティング制御部５１ａは、ＱＫＤ受信機１の中央制御部５０ａからの動作パラメータまたは実行タイミングの指示および変更に従って、第１鍵蒸留処理部１１にシフティング処理を実行させる。第１鍵蒸留処理部１１は、光学処理部１４から受信した基底情報と、第１鍵蒸留処理部２１から受信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。第１鍵蒸留処理部１１は、図７に示すように、蓄積部１５に、シフティング処理により生成した共有ビット列を第１中間データ６１ａとして記憶させると共に、シフティング処理により得られるパラメータ等を含むログデータを第１実行ログ７１ａとして記憶させる。

【００９５】

＜ステップＳ１４＞

ＱＫＤ送信機２のシフティング制御部５１ｂは、ＱＫＤ送信機２の中央制御部５０ｂからの動作パラメータまたは実行タイミングの指示および変更に従って、第１鍵蒸留処理部２１にシフティング処理を実行させる。第１鍵蒸留処理部２１は、光学処理部２４から受信した基底情報と、第１鍵蒸留処理部１１から受信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。第１鍵蒸留処理部２１は、蓄積部２５に、シフティング処理により生成した共有ビット列を第１中間データ６１ｂとして記憶させると共に、シフティング処理により得られるパラメータ等を含むログデータを第１実行ログ７１ｂとして記憶させる。

【００９６】

＜ステップＳ１５＞

ＱＫＤ受信機１の第２鍵蒸留処理部１２、およびＱＫＤ送信機２の第２鍵蒸留処理部２２は、古典通信路を介して、共有ビット列の誤りを訂正するための制御データであるＥＣ情報を交換する。

【００９７】

＜ステップＳ１６＞

ＱＫＤ受信機１のＥＣ制御部５２ａは、中央制御部５０ａからの動作パラメータまたは実行タイミングの指示および変更に従って、第２鍵蒸留処理部１２にＥＣ処理を実行させる。第２鍵蒸留処理部１２は、蓄積部１５に記憶された第１中間データ６１ａである共有ビット列を読み出す。第２鍵蒸留処理部１２は、古典通信路を介して第２鍵蒸留処理部２２と交換したＥＣ情報に基づいて、読み出した共有ビット列のビット誤りを訂正して、訂正後のビット列である訂正後ビット列を生成するＥＣ処理を実行する。第２鍵蒸留処理部１２は、図７に示すように、蓄積部１５に、ＥＣ処理により生成した訂正後ビット列を第２中間データ６２ａとして記憶させると共に、ＥＣ処理により得られるパラメータ等を含むログデータを第２実行ログ７２ａとして記憶させる。この第２鍵蒸留処理部１２が生成した訂正後ビット列は、ＱＫＤ送信機２の第２鍵蒸留処理部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。

【００９８】

＜ステップＳ１７＞

ＱＫＤ送信機２のＥＣ制御部５２ｂは、中央制御部５０ｂからの動作パラメータまたは実行タイミングの指示および変更に従って、第２鍵蒸留処理部２２にＥＣ処理を実行させる。第２鍵蒸留処理部２２は、蓄積部２５に記憶された第１中間データ６１ｂである共有ビット列を読み出す。第２鍵蒸留処理部２２は、古典通信路を介して第２鍵蒸留処理部１２と交換したＥＣ情報に基づいて、読み出した共有ビット列のビット誤りを訂正して、訂

正後のビット列である訂正後ビット列を生成するＥＣ処理を実行する。第２鍵蒸留処理部２２は、蓄積部２５に、ＥＣ処理により生成した訂正後ビット列を第２中間データ６２ｂとして記憶させると共に、ＥＣ処理により得られるパラメータ等を含むログデータを第２実行ログ７２ｂとして記憶させる。この第２鍵蒸留処理部２２が生成した訂正後ビット列は、第２鍵蒸留処理部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。

【００９９】

＜ステップＳ１８＞

ＱＫＤ受信機１の第３鍵蒸留処理部１３は、古典通信路を介して、ＱＫＤ送信機２の第３鍵蒸留処理部２３にＰＡ情報（乱数および暗号鍵の長さ情報等）を送信し、第３鍵蒸留処理部２３は、古典通信路を介して、第３鍵蒸留処理部１３からＰＡ情報を受信する。

【０１００】

＜ステップＳ１９＞

ＱＫＤ受信機１のＰＡ制御部５３ａは、中央制御部５０ａからの動作パラメータまたは実行タイミングの指示および変更に従って、第３鍵蒸留処理部１３にＰＡ処理を実行させる。第３鍵蒸留処理部１３は、蓄積部１５に記憶された第２中間データ６２ａである訂正後ビット列を読み出す。第３鍵蒸留処理部１３は、古典通信路を介して第３鍵蒸留処理部２３に送信したＰＡ情報に基づいて、第２鍵蒸留処理部１２により訂正した誤りの数から、シフティング処理およびＥＣ処理の際に盗聴者に盗聴された可能性のあるビットを取り除いて鍵ビット列（暗号鍵）を生成するＰＡ処理を実行する。

【０１０１】

具体的には、ＰＡ処理として、第３鍵蒸留処理部１３は、図８に示すように、第２鍵蒸留処理部１２により生成され、蓄積部１５から読み出した訂正後ビット列の長さｎと、ＰＡ情報に含まれる乱数ｒと、暗号鍵の長さｓとから、ｎ×ｓの行列であり乱数ｒによりランダムに構成されたハッシュ関数を生成する。そして、第３鍵蒸留処理部１３は、訂正後ビット列にハッシュ関数を乗じることによって、長さｓの暗号鍵（鍵ビット列）を生成する。なお、ＰＡ処理の方法は、上述のようなハッシュ関数を用いたものに限定されるものではなく、その他の方法によって実現するものとしてもよい。

【０１０２】

＜ステップＳ２０＞

ＱＫＤ送信機２のＰＡ制御部５３ｂは、中央制御部５０ｂからの動作パラメータまたは実行タイミングの指示および変更に従って、第３鍵蒸留処理部２３にＰＡ処理を実行させる。第３鍵蒸留処理部２３は、蓄積部２５に記憶された第２中間データ６２ｂである訂正後ビット列を読み出す。第３鍵蒸留処理部２３は、古典通信路を介して第３鍵蒸留処理部１３から受信したＰＡ情報に基づいて、第２鍵蒸留処理部２２により訂正した誤りの数から、シフティング処理およびＥＣ処理の際に盗聴者に盗聴された可能性のあるビットを取り除いて鍵ビット列（暗号鍵）を生成するＰＡ処理を実行する。第３鍵蒸留処理部２３による具体的なＰＡ処理の方法は、上述した第３鍵蒸留処理部１３によるＰＡ処理と方法と同様である。

【０１０３】

＜ステップＳ２１＞

第３鍵蒸留処理部１３は、図７に示すように、蓄積部１５に、ＰＡ処理により生成した暗号鍵を鍵データ６３ａとして記憶させ、管理させると共に、ＰＡ処理により得られるパラメータ等を含むログデータを第３実行ログ７３ａとして記憶させる。蓄積部１５に記憶（管理）された暗号鍵は、必要に応じて、外部のアプリケーションに提供される。

【０１０４】

＜ステップＳ２２＞

第３鍵蒸留処理部２３は、蓄積部２５に、ＰＡ処理により生成した暗号鍵を鍵データ６３ｂとして記憶させ、管理させると共に、ＰＡ処理により得られるパラメータ等を含むログデータを第３実行ログ７３ｂとして記憶させる。蓄積部２５に記憶（管理）された暗号

鍵は、必要に応じて、外部のアプリケーションに提供される。

【０１０５】

以上のような動作によって、ＱＫＤ受信機１およびＱＫＤ送信機２において、同一の暗号鍵が生成される。ただし、上述のステップは、それぞれ並行に実行可能であり、例えば、ステップＳ１６およびＳ１７のＥＣ処理が実行されるのと並行して、ステップＳ１３およびＳ１４のシフティング処理が、別のビット列に対して実行されるものとしてもよい。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。

【０１０６】

以上のように、本実施形態のＱＫＤ受信機１では、第１鍵蒸留処理装置１０１（第１鍵蒸留処理部１１）、第２鍵蒸留処理装置１０２（第２鍵蒸留処理部１２）および第３鍵蒸留処理装置１０３（第３鍵蒸留処理部１３）は、それぞれ蓄積部１５を介して中間データをやり取りするものとしている。具体的には、第１鍵蒸留処理装置１０１は、シフティング処理により生成した共有ビット列を、第２鍵蒸留処理装置１０２に送らずに、蓄積部１５に記憶させるものとしている。そして、第２鍵蒸留処理装置１０２は、蓄積部１５に記憶された共有ビット列を読み出し、ＥＣ処理により生成した訂正後ビット列を、第３鍵蒸留処理装置１０３に送らずに、蓄積部１５に記憶させるものとしている。さらに、第３鍵蒸留処理装置１０３は、蓄積部１５に記憶された訂正後ビット列を読み出し、ＰＡ処理により生成した暗号鍵を、外部のアプリケーション等に直接提供することなく、蓄積部１５に記憶させるものとしている。したがって、各鍵蒸留処理装置の処理速度に差があったり、一部が停止または故障した場合であっても、その他の部分は、鍵蒸留処理に必要な中間データが蓄積部１５に記憶されていれば、鍵蒸留処理を継続することができる。よって、各鍵蒸留処理装置の一部が故障した場合、他の鍵蒸留処理装置が動作中においても、故障した着脱可能な鍵蒸留処理装置を取り外して交換する等の対応が可能となる。同様に、各鍵蒸留処理装置の独立性が高いため、システム納入先の要件（動作速度要件等）に応じて、鍵蒸留処理装置を容易に入れ替え、最適な量子鍵配送システム５００を構成することも可能となる。

【０１０７】

そもそも、各鍵蒸留処理装置が生成する中間データおよび暗号鍵のブロックサイズはそれぞれ異なるため、中間データおよび暗号鍵を蓄積部１５にバッファリングすることは必須である。例えば、ＰＡ処理であれば、ブロックサイズは常に大きくした方が生成される暗号鍵のサイズを大きくすることができる一方、ＥＣ処理では、ブロックサイズに関連するアルゴリズム上の差異は存在しないため、単純に処理速度が最も高速化できるようにブロックサイズを決定することができることになる。また、鍵蒸留処理の動作パラメータ（例えば、量子ビット誤り率等）に応じて、ＥＣ処理で用いるべき参照データ（符号データ）が変化したり、ＰＡ処理における暗号鍵のサイズを決定する別のパラメータがシステム運用中に変化する場合がある。このため、各鍵蒸留処理装置が生成する中間データまたは暗号鍵を蓄積部１５にバッファリングするために必要な記憶領域は変動し得る。よって、各鍵蒸留処理部で必要な蓄積部１５の記憶領域を事前に設計することは難しいため、共通の記憶装置である蓄積部１５において全ての中間データおよび暗号鍵をバッファリングし、各鍵蒸留処理装置によって利用できる記憶領域のサイズをシステム運用中にも変更できるように構成することにメリットがある。以上のような点から、各鍵蒸留処理装置が、生成した中間データおよび暗号鍵を、共通の記憶装置である蓄積部１５にバッファリングすることによって、システムの可用性が高まるという効果がある。上述の内容は、ＱＫＤ受信機１だけでなく、ＱＫＤ送信機２についても同様である。

【０１０８】

また、本実施形態のＱＫＤ受信機１およびＱＫＤ送信機２では、鍵蒸留処理の各ステップ（シフティング処理、ＥＣ処理およびＰＡ処理）をそれぞれ異なるハードウェアである鍵蒸留処理装置が実行する。これによって、シフティング処理、ＥＣ処理、およびＰＡ処理の各鍵蒸留処理において、高速に実行する場合に要求されるハードウェア特性がそれぞ

れ異なっていても、それぞれ種類の異なる専用のハードウェア装置を用いることで、それぞれ個別に高速化が可能なハードウェア装置を選定および利用することができる。例えば、ＥＣ処理およびＰＡ処理は、それぞれ用いるアルゴリズムによって、ハードウェアに対する要求スペック（処理並列度、および必要なハードウェア演算器の種類等）が異なる可能性がある。以上のように、鍵蒸留処理の各ステップをそれぞれ異なるハードウェアである鍵蒸留処理装置が実行することによって、各ステップにそれぞれ最適なハードウェア装置を選定および利用することができ、量子鍵配送システム５００全体として高速な鍵蒸留処理（量子鍵配送）が実現できる。

【０１０９】

また、本実施形態では、制御部（制御部１０、２０）が、蓄積部（蓄積部１５、２５）に記憶された中間データおよび暗号鍵をモニタリングする。このため、制御部が、各高速鍵蒸留処理装置への入力および出力を個別に直接モニタリングすることが可能となり、メインテナンス性を向上させることができる。また、制御部（ＣＰＵ１００、２００）は、各鍵蒸留処理装置と、バス（バス１１０、２１０）を介して直接アクセスすることが可能であるため、各鍵蒸留処理装置の動作を直接モニタリング、アップグレード、デバッグおよび調整を行うことが容易となる。例えば、蓄積部（蓄積部１５、２５）に記憶されている各高速鍵蒸留処理装置の設定ファイルを修正したり、各鍵蒸留処理装置のレジスタに直接アクセスしたりすることが容易となる。

【０１１０】

また、本実施形態では、中間データおよび暗号鍵を共通の蓄積部（蓄積部１５、２５）に記憶させることによって、データの一貫性の保持が実現される。

【０１１１】

なお、ＱＫＤ受信機１およびＱＫＤ送信機２のいずれにおいても、各鍵蒸留処理装置がハードウェア装置によって構成していなければならないわけではない。例えば、図１に示す量子鍵配送システム５００では、ＱＫＤ送信機２が３つであるのに対し、ＱＫＤ受信機１は１つである。したがって、ＱＫＤ受信機１における鍵蒸留処理の負荷がＱＫＤ送信機２と比較して大きくなる。よって、量子鍵配送システム５００のような構成の場合、ＱＫＤ受信機１が、ハードウェア装置である各鍵蒸留処理装置を備えるものとして、鍵蒸留処理の動作を高速化させるものとしてもよい。

【０１１２】

また、各鍵蒸留処理部は、生成した中間データまたは暗号鍵を蓄積部に記憶させる場合、ＣＰＵである制御部を介して記憶させるものとしてもよく、ＤＭＡ（Ｄｉｒｅｃｔ Ｍｅｍｏｒｙ Ａｃｃｅｓｓ）方式によって、直接、蓄積部に記憶させるものとしてもよい。

【０１１３】

本実施形態に係るＱＫＤ装置で実行されるプログラムは、ＲＯＭ（ＲＯＭ１０５、２０５）等に予め組み込まれて提供される。

【０１１４】

なお、本実施形態に係る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。

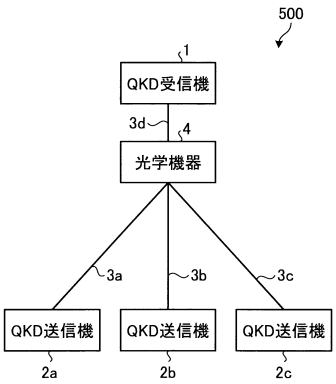
【０１１５】

さらに、本実施形態に係る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、本実施形態および変形例に係る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。

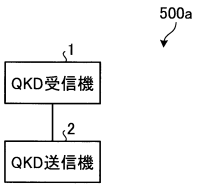
【０１１６】
本実施形態に係るＱＫＤ装置で実行されるプログラムは、コンピュータを上述したＱＫＤ装置の各機能部（中央制御部５０ａ、５０ｂ、シフティング制御部５１ａ、５１ｂ、ＥＣ制御部５２ａ、５２ｂ、およびＰＡ制御部５３ａ、５３ｂ）として機能させ得る。このコンピュータは、ＣＰＵ１００、２００がコンピュータ読取可能な記憶媒体からプログラムを主記憶装置上に読み出して実行することができる。
【０１１７】
本発明の実施形態を説明したが、この実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。この新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、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】
【０１１８】
１　ＱＫＤ受信機
２、２ａ～２ｃ　ＱＫＤ送信機
３、３ａ～３ｄ　光ファイバリンク
４　光学機器
１０　制御部
１１　第１鍵蒸留処理部
１２　第２鍵蒸留処理部
１３　第３鍵蒸留処理部
１４　光学処理部
１５　蓄積部
１６　通信部
２０　制御部
２１　第１鍵蒸留処理部
２２　第２鍵蒸留処理部
２３　第３鍵蒸留処理部
２４　光学処理部
２５　蓄積部
２６　通信部
５０ａ、５０ｂ　中央制御部
５１ａ、５１ｂ　シフティング制御部
５２ａ、５２ｂ　ＥＣ制御部
５３ａ、５３ｂ　ＰＡ制御部
６１ａ、６１ｂ　第１中間データ
６２ａ、６２ｂ　第２中間データ
６３ａ、６３ｂ　鍵データ
７１ａ、７１ｂ　第１実行ログ
７２ａ、７２ｂ　第２実行ログ
７３ａ、７３ｂ　第３実行ログ
１００　ＣＰＵ
１０１　第１鍵蒸留処理装置
１０２　第２鍵蒸留処理装置
１０３　第３鍵蒸留処理装置
１０４　光学処理装置
１０５　ＲＯＭ
１０６　ＲＡＭ
１０７　記憶装置

１０８　通信Ｉ／Ｆ
１１０　バス
２００　ＣＰＵ
２０１　第１鍵蒸留処理装置
２０２　第２鍵蒸留処理装置
２０３　第３鍵蒸留処理装置
２０４　光学処理装置
２０５　ＲＯＭ
２０６　ＲＡＭ
２０７　記憶装置
２０８　通信Ｉ／Ｆ
２１０　バス
５００、５００ａ　量子鍵配送システム

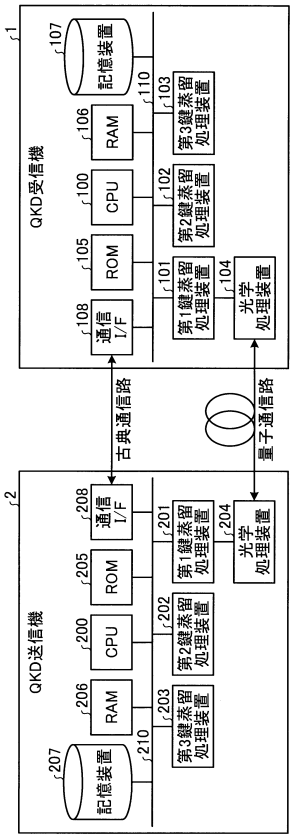
【図１】



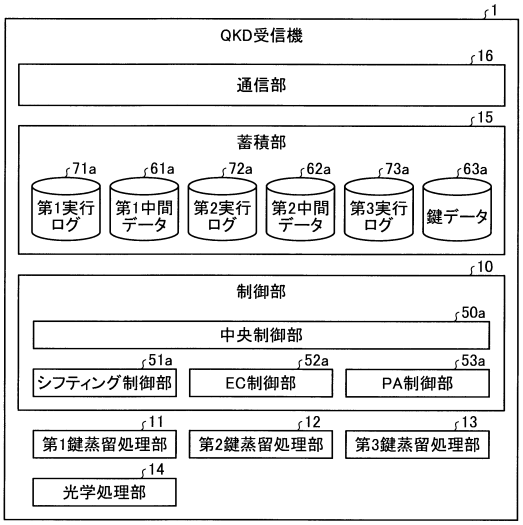
【図２】



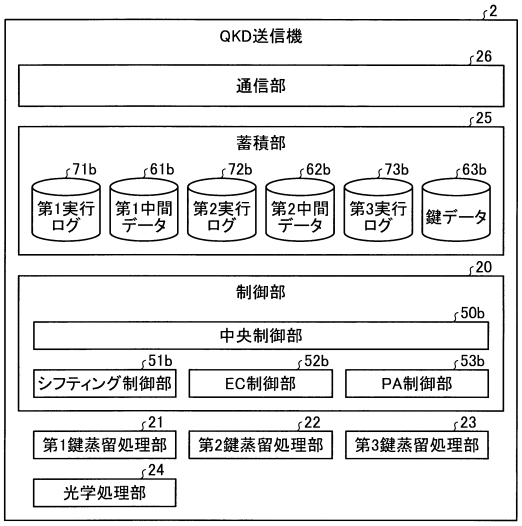
【図３】


1
QKD受信機
107
記憶装置
110
103
第3鍵蒸留処理装置
106
RAM
102
第2鍵蒸留処理装置
100
CPU
101
第1鍵蒸留処理装置
105
ROM
104
光学処理装置
108
通信I/F
古典通信路
量子通信路
2
QKD送信機
208
通信I/F
201
第1鍵蒸留処理装置
204
光学処理装置
205
ROM
202
第2鍵蒸留処理装置
200
CPU
203
第3鍵蒸留処理装置
206
RAM
210
207
記憶装置

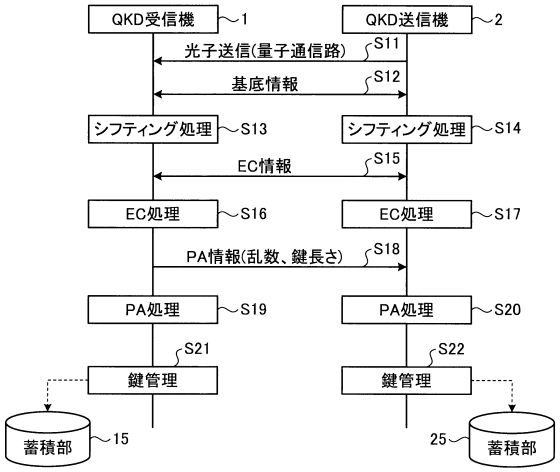
【図４】


1
QKD受信機
16
通信部
15
蓄積部
71a
第1実行ログ
61a
第1中間データ
72a
第2実行ログ
62a
第2中間データ
73a
第3実行ログ
63a
鍵データ
10
制御部
50a
中央制御部
51a
シフティング制御部
52a
EC制御部
53a
PA制御部
11
第1鍵蒸留処理部
12
第2鍵蒸留処理部
13
第3鍵蒸留処理部
14
光学処理部

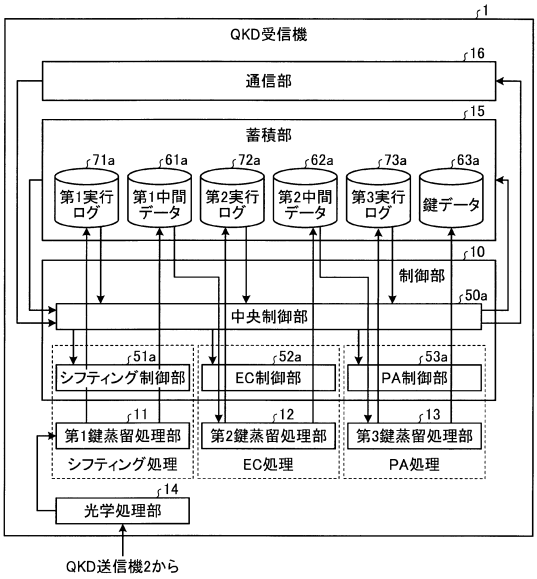
【図５】


2
QKD送信機
26
通信部
25
蓄積部
71b
第1実行ログ
61b
第1中間データ
72b
第2実行ログ
62b
第2中間データ
73b
第3実行ログ
63b
鍵データ
20
制御部
50b
中央制御部
51b
シフティング制御部
52b
EC制御部
53b
PA制御部
21
第1鍵蒸留処理部
22
第2鍵蒸留処理部
23
第3鍵蒸留処理部
24
光学処理部

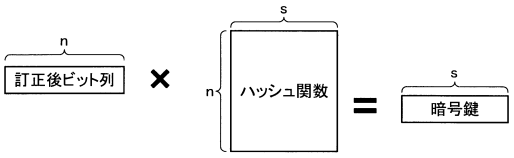
【図６】


QKD受信機
1
QKD送信機
2
光子送信(量子通信路)
S11
基底情報
S12
シフティング処理
S13
シフティング処理
S14
EC情報
S15
EC処理
S16
EC処理
S17
PA情報(乱数、鍵長さ)
S18
PA処理
S19
PA処理
S20
S21
S22
鍵管理
鍵管理
蓄積部
15
25
蓄積部

【図７】


1
QKD受信機
16
通信部
15
蓄積部
71a
第1実行ログ
61a
第1中間データ
72a
第2実行ログ
62a
第2中間データ
73a
第3実行ログ
63a
鍵データ
10
制御部
50a
中央制御部
51a
シフティング制御部
52a
EC制御部
53a
PA制御部
11
第1鍵蒸留処理部
12
第2鍵蒸留処理部
13
第3鍵蒸留処理部
シフティング処理
EC処理
PA処理
14
光学処理部
QKD送信機2から

【図８】


n
訂正後ビット列
×
s
n
ハッシュ関数
=
s
暗号鍵

フロントページの続き

(72)発明者　高橋　莉里香
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　村上　明
東京都港区芝浦一丁目１番１号　株式会社東芝内

審査官　金木　陽一

(56)参考文献　特開２００７－５３５９０（ＪＰ，Ａ）
特開２００９－２１００２（ＪＰ，Ａ）
特表２０１０－５０６４３２（ＪＰ，Ａ）
特開２０１１－４４７６８（ＪＰ，Ａ）
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，２０１１年　1月２０日，Vol. 110，No. 392，pp. 25-30，OCS2010-103

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１２