(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2018-148503
(P2018-148503A)
(43)公開日　平成30年9月20日(2018.9.20)

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

審査請求 未請求　請求項の数 10　OL　（全 16 頁）

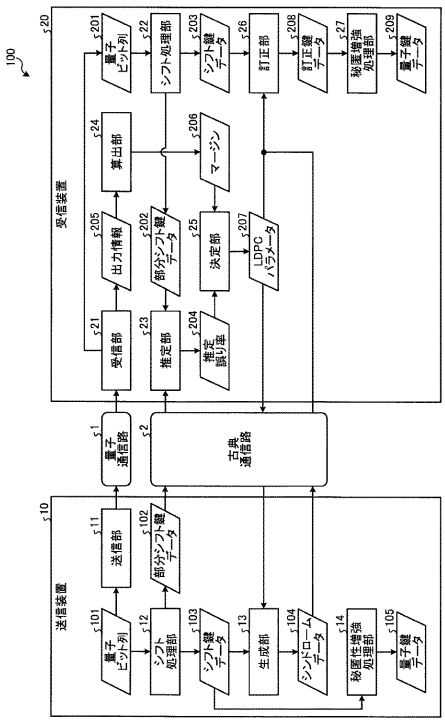
(21)出願番号　特願2017-44373(P2017-44373)
(22)出願日　平成29年3月8日(2017.3.8)

(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　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
(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　AA28　AA29　EA16

(54)【発明の名称】量子通信装置、量子通信システム及び量子通信方法

(57)【要約】
【課題】誤り訂正処理の設定情報をより適切に決定する。
【解決手段】実施形態の量子通信装置は、受信部とシフト処理部と決定部と生成部とを備える。受信部は、光子の量子状態を利用した複数の基底のうち一の基底により表現された量子ビットを、送信装置から量子通信路を介して受信し、受信した複数の量子ビットから成る量子ビット列を取得する。シフト処理部は、複数の基底からランダムに選択した参照基底により、所定のビット列単位で量子ビット列を参照して第１シフト鍵データを取得するシフト処理を行う。決定部は、第１シフト鍵データの推定誤り率と、推定誤り率のマージンとから、第１シフト鍵データの誤り訂正処理の設定情報を決定する。訂正部は、設定情報を使用して、誤り訂正処理を行うことにより、訂正鍵データを生成する。
【選択図】図２



【特許請求の範囲】
【請求項１】
光子の量子状態を利用した複数の基底のうち一の基底により表現された量子ビットを、送信装置から量子通信路を介して受信し、受信した複数の前記量子ビットから成る量子ビット列を取得する受信部と、
前記複数の基底からランダムに選択した参照基底により、所定のビット列単位で前記量子ビット列を参照して第１シフト鍵データを取得するシフト処理を行うシフト処理部と、
前記第１シフト鍵データの推定誤り率と、前記推定誤り率のマージンとから、前記第１シフト鍵データの誤り訂正処理の設定情報を決定する決定部と、
前記設定情報を使用して、前記誤り訂正処理を行うことにより、訂正鍵データを生成する訂正部と、
を備える量子通信装置。
【請求項２】
前記第１シフト鍵データに含まれる第１部分シフト鍵データと、前記送信装置の前記シフト処理により得られた第２シフト鍵データに含まれる第２部分シフト鍵データとを比較することにより得られた誤り率により、前記推定誤り率を推定する推定部、
を更に備える請求項１に記載の量子通信装置。
【請求項３】
前記訂正部は、前記第１シフト鍵データに含まれる第１部分シフト鍵データに、前記誤り訂正処理を行うことにより、部分訂正鍵データを生成し、
前記部分訂正鍵データと、前記第１部分シフト鍵データとを比較することにより得られた誤り率により、前記推定誤り率を推定する推定部、
を更に備える請求項１に記載の量子通信装置。
【請求項４】
前回の前記シフト処理により取得された前記第１シフト鍵データと、前回の前記誤り訂正処理により生成された前記訂正鍵データとを比較することにより得られた誤り率により、前記推定誤り率を推定する推定部、
を更に備える請求項１に記載の量子通信装置。
【請求項５】
前記決定部は、前記受信部に使用される光学系機器の出力情報に基づいて前記マージンを決定する、
請求項１に記載の量子通信装置。
【請求項６】
前記光学系機器は、偏光調整器であり、
前記偏光調整器の出力電圧の変動量に基づいて前記マージンを算出する算出部、
を更に備える請求項５に記載の量子通信装置。
【請求項７】
前記光学系機器は、ファイバーストレッチャーであり、
前記ファイバーストレッチャーの出力電圧の変動量に基づいて前記マージンを算出する算出部、
を更に備える請求項５に記載の量子通信装置。
【請求項８】
前記光学系機器は、光学検出器であり、
前記光学検出器の検出ゲート調整信号の変動量に基づいて前記マージンを算出する算出部、
を更に備える請求項５に記載の量子通信装置。
【請求項９】
送信装置と受信装置とが量子通信路を介して接続された量子通信システムであって、
前記受信装置は、
光子の量子状態を利用した複数の基底のうち一の基底により表現された量子ビットを、

前記送信装置から前記量子通信路を介して受信し、受信した複数の前記量子ビットから成る量子ビット列を取得する受信部と、
前記複数の基底からランダムに選択した参照基底により、所定のビット列単位で前記量子ビット列を参照して第１シフト鍵データを取得するシフト処理を行うシフト処理部と、
前記第１シフト鍵データの推定誤り率と、前記推定誤り率のマージンとから、前記第１シフト鍵データの誤り訂正処理の設定情報を決定する決定部と、
前記設定情報を使用して、前記誤り訂正処理を行うことにより、訂正鍵データを生成する訂正部と、
を備える量子通信システム。
【請求項１０】
光子の量子状態を利用した複数の基底のうち一の基底により表現された量子ビットを、送信装置から量子通信路を介して受信し、受信した複数の前記量子ビットから成る量子ビット列を取得するステップと、
前記複数の基底からランダムに選択した参照基底により、所定のビット列単位で前記量子ビット列を参照して第１シフト鍵データを取得するシフト処理を行うステップと、
前記第１シフト鍵データの推定誤り率と、前記推定誤り率のマージンとから、前記第１シフト鍵データの誤り訂正処理の設定情報を決定するステップと、
前記設定情報を使用して、前記誤り訂正処理を行うことにより、訂正鍵データを生成するステップと、
を含む量子通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は量子通信装置、量子通信システム及び量子通信方法に関する。
【背景技術】
【０００２】
ＬＤＰＣ（Ｌｏｗ Ｄｅｎｓｉｔｙ Ｐａｒｉｔｙ Ｃｈｅｃｋ）符号は、情報伝送レートの理論上の限界値であるシャノン限界に非常に近い誤り訂正能力を持つ誤り訂正符号として注目を集めている。そのため、通信及びストレージシステム等の分野では、ＬＤＰＣ復号器をハードウェアとして実装すること等の検討が盛んに行われている。
【先行技術文献】
【非特許文献】
【０００３】
【非特許文献１】"Ｈｉｇｈ ｓｐｅｅｄ ａｎｄ ａｄａｐｔａｂｌｅ ｅｒｒｏｒ ｃｏｒｒｅｃｔｉｏｎ ｆｏｒ ｍｅｇａｂｉｔ／ｓ ｒａｔｅ ｑｕａｎｔｕｍ ｋｅｙ ｄｉｓｔｒｉｂｕｔｉｏｎ", Ａ．Ｒ．Ｄｉｘｏｎ ｅｔ ａｌ, Ｓｃｉｅｎｔｉｆｉｃ Ｒｅｐｏｒｔｓ ４, ２０１４
【非特許文献２】"Ｃｏｎｔｉｎｕｏｕｓ ｏｐｅｒａｔｉｏｎ ｏｆ ｈｉｇｈ ｂｉｔ ｒａｔｅ ｑｕａｎｔｕｍ ｋｅｙ ｄｉｓｔｒｉｂｕｔｉｏｎ", Ａ．Ｒ．Ｄｉｘｏｎ ｅｔ ａｌ, ＡＰＰＬＩＥＤ ＰＨＹＳＩＣＳ ＬＥＴＥＲＳ ９６, １６１１０２（２０１０）
【非特許文献３】"Ｓｔａｂｉｌｉｔｙ ｏｆ ｈｉｇｈ ｂｉｔ ｒａｔｅ ｑｕａｎｔｕｍ ｋｅｙ ｄｉｓｔｒｉｂｕｔｉｏｎ ｏｎ ｉｎｓｔａｌｌｅｄ ｆｉｂｅｒ", Ａ．Ｒ．Ｄｉｘｏｎ ｅｔ ａｌ, ＯＰＴＩＣＳ ＥＸＰＲＥＳＳ １６３３９ Ｖｏｌ．２０, Ｎｏ．１５（２０１２）
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら従来の技術では、誤り訂正処理の設定情報をより適切に決定することが難しかった。本発明が解決しようとする課題は、誤り訂正処理の設定情報をより適切に決定

することができる量子通信装置、量子通信システム及び量子通信方法を提供することである。

【課題を解決するための手段】

【０００５】

実施形態の量子通信装置は、受信部とシフト処理部と決定部と生成部とを備える。受信部は、光子の量子状態を利用した複数の基底のうち一の基底により表現された量子ビットを、送信装置から量子通信路を介して受信し、受信した複数の前記量子ビットから成る量子ビット列を取得する。シフト処理部は、前記複数の基底からランダムに選択した参照基底により、所定のビット列単位で前記量子ビット列を参照して第１シフト鍵データを取得するシフト処理を行う。決定部は、前記第１シフト鍵データの推定誤り率と、前記推定誤り率のマージンとから、前記第１シフト鍵データの誤り訂正処理の設定情報を決定する。訂正部は、前記設定情報を使用して、前記誤り訂正処理を行うことにより、訂正鍵データを生成する。

【図面の簡単な説明】

【０００６】

【図１】第１実施形態の量子通信システムの装置構成の例を示す図。

【図２】第１実施形態の量子通信システムの機能構成の例を示す図。

【図３】第１実施形態の受信部のハードウェア構成の例を示す図。

【図４】第１実施形態の算出部の機能構成の例を示す図。

【図５】第１実施形態のＬＤＰＣパラメータの例を示す図。

【図６】第２実施形態の量子通信システムの機能構成の例を示す図。

【図７】第３実施形態の量子通信システムの機能構成の例を示す図。

【図８】第１～第３実施形態の送信装置及び受信装置の主要部のハードウェア構成の例を示す図。

【発明を実施するための形態】

【０００７】

以下に添付図面を参照して、量子通信装置、量子通信システム及び量子通信方法の実施形態を詳細に説明する。

【０００８】

（第１実施形態）

はじめに第１実施形態について説明する。

【０００９】

［装置構成の例］

図１は第１実施形態の量子通信システム１００の装置構成の例を示す図である。第１実施形態の量子通信システム１００は、２つの量子通信装置（送信装置１０及び受信装置２０）を備える。送信装置１０は、量子ビットを示す光子を連続的に受信装置２０に送信する。なお第１実施形態では、説明の便宜上、光子を送信する側の装置を送信装置１０と呼ぶが、送信装置１０が光子を受信する機能を有していてもよい。同様に、受信装置２０が光子を送信する機能を有していてもよい。

【００１０】

送信装置１０及び受信装置２０は、量子鍵データを使用して、暗号データを送受信する。量子鍵データの生成方法の詳細については、図２を参照して説明する。

【００１１】

［機能構成の例］

図２は第１実施形態の量子通信システム１００の機能構成の例を示す図である。第１実施形態の量子通信システム１００は、送信装置１０及び受信装置２０を備える。

【００１２】

送信装置１０及び受信装置２０は、量子通信路１を介して接続されている。量子通信路１は、量子ビットを示す光子を送受信する光ファイバーである。量子通信路１は、１光子という非常に微弱な光を送受信するため、外乱の影響を受けやすい。

【００１３】
　また、送信装置１０及び受信装置２０は、古典通信路２を介して接続されている。古典通信路２は、量子鍵データ１０５（２０９）を生成するための制御情報を送受信する。図２の例では、制御情報は、例えば部分シフト鍵データ１０２、ＬＤＰＣパラメータ２０７及びシンドロームデータ１０４等である。古典通信路２は、有線であっても無線であってもよく、また有線及び無線を組み合わせて実現してもよい。
【００１４】
　送信装置１０は、送信部１１、シフト処理部１２、生成部１３及び秘匿性増強処理部１４を備える。
【００１５】
　受信装置２０は、受信部２１、シフト処理部２２、推定部２３、算出部２４、決定部２５、訂正部２６及び秘匿性増強処理部２７を備える。
【００１６】
　送信部１１は、量子ビット列１０１を、量子通信路１を介して、受信部２１に送信する。量子ビット列１０１を構成する量子ビットは、光子の量子状態を利用した複数の基底のうち一の基底により表現される。基底には、例えば光子の偏光及び位相等が利用される。
【００１７】
　受信部２１は、量子ビット列１０１を、送信部１１から量子通信路１を介して受信することにより、量子ビット列２０１を取得する。また、受信部２１は、量子ビット列２０１の取得処理に使用された光学系機器の出力情報２０５を、算出部２４に入力する。出力情報２０５の詳細は、図３を参照して後述する。
【００１８】
　シフト（Ｓｉｆｔ）処理部２２は、複数の基底からランダムに選択した参照基底により、所定のビット列単位で量子ビット列２０１を参照してシフト鍵データ２０３（第１シフト鍵データ）を取得するシフト処理を行う。そしてシフト処理部２２は、シフト鍵データ２０３を訂正部２６に入力する。また、シフト処理部２２は、シフト鍵データ２０３に含まれる部分シフト鍵データ２０２を、推定部２３に入力する。部分シフト鍵データ２０２は、シフト鍵データ２０３に含まれる所定の長さのビット列である。
【００１９】
　一方、送信装置１０のシフト処理部１２は、量子ビット列１０１にシフト処理を行うことにより、シフト鍵データ１０３を取得する。そしてシフト処理部１２は、シフト鍵データ１０３を生成部１３及び秘匿性増強処理部１４に入力する。また、シフト処理部１２は、シフト鍵データ１０３に含まれる部分シフト鍵データ１０２（第２部分シフト鍵データ）を、古典通信路２を介して、推定部２３に送信する。部分シフト鍵データ１０２は、シフト鍵データ１０３に含まれる所定の長さのビット列である。
【００２０】
　推定部２３は、送信装置１０のシフト処理部１２から、部分シフト鍵データ１０２を受信し、シフト処理部２２から、部分シフト鍵データ２０２を受け付ける。推定部２３は、部分シフト鍵データ１０２と部分シフト鍵データ２０２とを比較することにより、部分シフト鍵データ２０２の誤りビットの位置情報を特定する。推定部２３は、誤りビットの位置情報と、部分シフト鍵データ２０２のビット数から得られた部分シフト鍵データ２０２の誤り率により、シフト鍵データ２０３の推定誤り率２０４を推定する。そして推定部２３は、推定誤り率２０４を決定部２５に入力する。
【００２１】
　また、算出部２４は、受信部２１から出力情報２０５を受け付けると、当該出力情報２０５に応じて、推定誤り率２０４のマージン２０６を算出する。マージン２０６の算出処理の詳細は、図４を参照して後述する。算出部２４は、マージン２０６を決定部２５に入力する。
【００２２】
　決定部２５は、推定部２３から推定誤り率２０４を受け付け、算出部２４からマージン

２０６を受け付ける。決定部２５は、推定誤り率２０４とマージン２０６とから、シフト鍵データ２０３の誤り訂正処理の設定情報を決定する。設定情報は任意でよい。第１実施形態の説明では、設定情報はＬＤＰＣパラメータ２０７である。ＬＤＰＣパラメータ２０７の例、及び、ＬＤＰＣパラメータ２０７の決定方法の詳細は、図５を参照して後述する。決定部２５は、ＬＤＰＣパラメータ２０７を訂正部２６に入力する。また決定部２５は、ＬＤＰＣパラメータ２０７を、古典通信路２を介して、送信装置１０の生成部１３に送信する。

【００２３】

送信装置１０の生成部１３は、受信装置２０の決定部２５からＬＤＰＣパラメータ２０７を受信し、シフト処理部１２からシフト鍵データ１０３を受け付ける。生成部１３は、ＬＤＰＣパラメータ２０７を使用して、シフト鍵データ１０３からシンドロームデータ１０４を生成する。そして生成部１３は、シンドロームデータ１０４を、古典通信路２を介して、受信装置２０の訂正部２６に送信する。

【００２４】

受信装置２０の訂正部２６は、送信装置１０の生成部１３から、シンドロームデータ１０４を受信し、決定部２５から、ＬＤＰＣパラメータ２０７を受け付け、シフト処理部２２から、シフト鍵データ２０３を受け付ける。訂正部２６は、シンドロームデータ１０４及びＬＤＰＣパラメータ２０７を使用して、シフト鍵データ２０３に誤り訂正処理を行うことにより、訂正鍵データ２０８を生成する。そして訂正部２６は、訂正鍵データ２０８を秘匿性増強処理部２７に入力する。

【００２５】

秘匿性増強処理部２７は、訂正部２６から、訂正鍵データ２０８を受け付けると、当該訂正鍵データ２０８に秘匿性増強処理を行うことにより、量子鍵データ２０９を生成する。秘匿性増強処理は、訂正鍵データ２０８を圧縮して、量子鍵データ２０９を生成することにより、当該量子鍵データ２０９の秘匿性を高める処理である。

【００２６】

一方、送信装置１０の秘匿性増強処理部１４は、シフト処理部１２から、シフト鍵データ１０３を受け付けると、当該シフト鍵データ１０３に秘匿性増強処理を行うことにより、量子鍵データ２０９と同一の量子鍵データ１０５を生成する。

【００２７】

次に図３を参照して、受信部２１に使用される光学系機器の出力情報２０５の詳細について説明する。

【００２８】

図３は第１実施形態の受信部２１のハードウェア構成の例を示す図である。第１実施形態の受信部２１は、偏光調整器２２１、マッハツェンダ干渉計２２２及び光学検出器２２３により実現される。マッハツェンダ干渉計２２２は、ファイバーストレッチャー２２４及び位相変調器２２５を備える。

【００２９】

量子暗号通信が不安定になる要因として、送信装置１０と受信装置２０とをつなぐ光ファイバー（量子通信路１）の偏光特性の変化、位相特性の変化、及び、光子の到着時間のずれの３つが考えられる。偏光特性の変化、及び、光子の到着時間のずれは、光ファイバー敷設区間の温度等の外的環境の変化によって引き起こされる。位相特性の変化は、光ファイバーのパス長の変化によって引き起こされる。光ファイバーのパス長の変化は、送信装置１０及び受信装置２０が設置されている部屋の温度等の変化により生じる。光ファイバーの偏光特性の変化、光ファイバーの位相特性の変化、及び、光子の到着時間のずれが生じると、量子通信路１の誤り率が上昇する。

【００３０】

偏光調整器２２１は、光ファイバーの偏光特性の変化を補償するため、光ファイバーの偏光を調整する。ファイバーストレッチャー２２４は、光ファイバーの位相特性の変化を補償するため、光ファイバーのパス長を調整する。位相変調器２２５は、送信装置１０で

変調された光子の位相を復調する。光学検出器２２３は、光子の検出ゲートを調整して光子の到着時間のずれを補償しながら、光子を検出し、複数の量子ビット列２０１を取得する。

【００３１】

出力情報２０５は、偏光調整器２２１の出力電圧２３１、ファイバーストレッチャー２２４の出力電圧２３２、及び、検出ゲート調整信号２３３を含む。偏光調整器２２１の出力電圧２３１は、光ファイバーの偏光を調整する制御に使用された電圧である。ファイバーストレッチャー２２４の出力電圧２３２は、光ファイバーのパス長を調整する制御に使用された電圧である。検出ゲート調整信号２２３は、光子の検出ゲートを調整する制御に使用された電圧である。

【００３２】

次に図４を参照して、マージン２０６の算出処理の詳細について説明する。

【００３３】

図４は第１実施形態の算出部２４の機能構成の例を示す図である。第１実施形態の算出部２４は、変動量算出部２４１及びマージン決定部２４２を備える。

【００３４】

偏光調整器２２１の出力電圧２３１の変動、及び、検出ゲート調整信号２３３の変動は、光ファイバー（量子通信路１）の偏光特性の変動、及び、光子の到着時間のずれの変動に対応している。よって、偏光調整器２２１の出力電圧２３１の変動、及び、検出ゲート調整信号２３３の変動が大きいほど、量子通信路１は不安定な状態になっている。

【００３５】

また、ファイバーストレッチャー２２４の出力電圧２３２の変動は、光ファイバー（量子通信路１）の位相特性の変動に対応している。ファイバーストレッチャー２２４の出力電圧２３２の変動が大きいほど、量子通信路１は不安定な状態になっている。

【００３６】

まとめると、出力情報２０５（出力電圧２３１、出力電圧２３２及び検出ゲート調整信号２３３）の変動が大きいほど、量子通信路１の状態は不安定になっている。

【００３７】

変動量算出部２４１は、受信部２１から、出力情報２０５を受け付けると、出力情報２０５に含まれる出力電圧２３１、出力電圧２３２及び検出ゲート調整信号２３３それぞれの変動量２３４を算出する。変動量２３４は、例えば単位時間あたりの変動の絶対値を累積した量である。変動量算出部２４１は、変動量２３４をマージン決定部２４２に入力する。

【００３８】

マージン決定部２４２は、変動量算出部２４１から変動量２３４を受け付けると、当該変動量２３４に基づいてマージン２０６を決定する。

【００３９】

マージン決定部２４２は、例えば変動量２３４が、偏光調整器２２１の出力電圧２３１の変動量である場合、変動量２３４と、偏光調整器２２１で定められている電圧の最大変動幅との割合に応じて、マージン２０６を決定する。具体的には、マージン決定部２４２は、例えば１分あたりの変動量２３４が最大変動幅の５％以下の場合、マージン２０６を５％に決定する。また例えば、マージン決定部２４２は、１分あたりの変動量２３４が最大変動幅の５％～１０％の場合、マージン２０６を１０％に決定する。また例えば、マージン決定部２４２は、１分あたりの変動量２３４が最大変動幅の１０％～１５％の場合、マージン２０６を１５％に決定する。また例えば、マージン決定部２４２は、１分あたりの変動量２３４が最大変動幅の２０％を超える場合、マージン２０６を２０％に決定する。

【００４０】

また例えば、マージン決定部２４２は、変動量２３４が、ファイバーストレッチャー２２４の出力電圧２３２の変動量である場合、変動量２３４と、ファイバーストレッチャー

２２４で定められている電圧の最大変動幅との割合に応じて、マージン２０６を決定する。

【００４１】

また例えば、マージン決定部２４２は、変動量２３４が、検出ゲート調整信号２３３の変動量である場合、変動量２３４と光学検出器２２３の検出ゲート信号の駆動周期との割合に応じてマージン２０６を決定する。

【００４２】

次に図５を参照して、ＬＤＰＣパラメータ２０７の例、及び、ＬＤＰＣパラメータ２０７の決定方法の詳細について説明する。

【００４３】

図５は第１実施形態のＬＤＰＣパラメータ２０７の例を示す図である。図５の例は、ＬＤＰＣパラメータ２０７が、ＬＤＰＣ符号の符号化率である場合を示す。決定部２５は、設定誤り率に応じて符号化率（ＬＤＰＣパラメータ２０７）を決定する。設定誤り率は、推定誤り率２０４及びマージン２０６から算出される。決定部２５は、例えば推定誤り率２０４が２％であり、マージン２０６が２０％である場合、設定誤り率を２．４％（＝２×１．２）に決定する。決定部２５は、例えば図５に示すテーブル情報を使用して、設定誤り率から、符号化率（ＬＤＰＣパラメータ２０７）を決定する。

【００４４】

以上、説明したように、第１実施形態の受信装置２０（量子通信装置）では、受信部２１が、光子の量子状態を利用した複数の基底のうち一の基底により表現された量子ビットを、送信装置１０から量子通信路１を介して受信し、受信した複数の量子ビットから成る量子ビット列２０１を取得する。シフト処理部２２が、複数の基底からランダムに選択した参照基底により、所定のビット列単位で量子ビット列２０１を参照してシフト鍵データ２０３（第１シフト鍵データ）を取得するシフト処理を行う。決定部２５が、シフト鍵データ２０３の推定誤り率２０４と、推定誤り率２０４のマージン２０６とから、シフト鍵データ２０３の誤り訂正処理の設定情報（ＬＤＰＣパラメータ２０７）を決定する。そして訂正部２６が、設定情報を使用して、誤り訂正処理を行うことにより、訂正鍵データ２０８を生成する。

【００４５】

量子暗号通信の誤り訂正処理では、シンドロームデータ１０４を古典通信路２経由で転送する必要がある。シンドロームデータ１０４はシフト鍵データ１０３に関連する情報であるため、古典通信路２に潜んでいる可能性のある盗聴者にできるだけ知られないようにする必要がある。よって、シフト鍵データ２０３の訂正が可能であり、かつ、シンドロームデータ１０４の転送量が最小となるＬＤＰＣパラメータ２０７を決定することが理想である。しかしながら、シフト鍵データ２０３の誤り率に影響を及ぼす量子通信路１は、外乱の影響を受けやすいので、量子通信路１の状態は不安定である。また、訂正対象となるシフト鍵データ２０３の誤り率の真値（正しい誤り率）は、実際に訂正処理をする前はわからない。訂正対象となるシフト鍵データ２０３の誤り率の真値に対応したＬＤＰＣパラメータ２０７を決定することが理想である。

【００４６】

第１実施形態の受信装置２０（量子通信装置）では、算出部２４が、光学系機器の振る舞いを示す出力情報２０５からマージン２０６を算出する。すなわち、第１実施形態の受信装置２０（量子通信装置）は、出力情報２０５から算出されたマージン２０６により、量子通信路１の状態を予測する。そして決定部２５が、当該マージン２０６と推定誤り率２０４とを考慮して設定情報（ＬＤＰＣパラメータ２０７）を決定する。これにより第１実施形態の量子通信システム１００によれば、誤り訂正処理の設定情報をより適切に決定することができる。

【００４７】

（第２実施形態）

次に第２実施形態について説明する。第２実施形態の説明では、第１実施形態と同様の

説明については省略し、第１実施形態と異なる箇所について説明する。第２実施形態では、推定誤り率２０４の推定方法が第１実施形態と異なる。

【００４８】

［機能構成の例］

図６は第２実施形態の量子通信システム１００の機能構成の例を示す図である。第２実施形態の量子通信システム１００は、送信装置１０及び受信装置２０を備える。

【００４９】

送信装置１０は、送信部１１、シフト処理部１２、生成部１３ａ、生成部１３ｂ及び秘匿性増強処理部１４を備える。

【００５０】

受信装置２０は、受信部２１、シフト処理部２２、推定部２３、算出部２４、決定部２５、訂正部２６ａ、訂正部２６ｂ及び秘匿性増強処理部２７を備える。

【００５１】

送信装置１０のシフト処理部１２は、第１実施形態と同様にして、量子ビット列１０１から、部分シフト鍵データ１０２及びシフト鍵データ１０３を取得する。シフト処理部１２は、部分シフト鍵データ１０２を生成部１３ａに入力し、シフト鍵データ１０３を生成部１３ｂに入力する。

【００５２】

なお第２実施形態では、部分シフト鍵データ１０２は、受信装置２０に送信されない。そのため部分シフト鍵データ１０２を、秘匿性増強処理の対象として使用されるシフト鍵データ１０３に含めてもよい。

【００５３】

生成部１３ａは、シフト処理部１２から、部分シフト鍵データ１０２を受け付けると、当該部分シフト鍵データ１０２から部分シンドロームデータ１０６を生成する。そして生成部１３ａは、部分シンドロームデータ１０６を、古典通信路２を介して、受信装置２０の訂正部２６ａに送信する。

【００５４】

生成部１３ｂの動作は、第１実施形態の生成部１３と同じなので、説明を省略する。

【００５５】

受信装置２０の訂正部２６ａは、送信装置１０の生成部１３ａから、部分シンドロームデータ１０６を受信し、シフト処理部２２から部分シフト鍵データ２０２を受け付ける。訂正部２６ａは、部分シンドロームデータ１０６を使用して、部分シフト鍵データ２０２（第１部分シフト鍵データ）に、誤り訂正処理を行うことにより、部分訂正鍵データ２１０を生成する。そして訂正部２６ａは、部分訂正鍵データ２１０を推定部２３に入力する。

【００５６】

なお第２実施形態では、部分シフト鍵データ１０２は、受信装置２０に送信されない。そのため部分シフト鍵データ１０２に対応する部分シフト鍵データ２０２から生成された部分訂正鍵データ２１０を、秘匿性増強処理の対象として使用される訂正鍵データ２０８に含めてもよい。

【００５７】

推定部２３は、シフト処理部２２から、部分シフト鍵データ２０２を受け付け、訂正部２６ａから、部分訂正鍵データ２１０を受け付ける。推定部２３は、部分訂正鍵データ２１０と、部分シフト鍵データ２０２（第１部分シフト鍵データ）とを比較することにより得られた誤りビットの位置情報に基づいて、シフト鍵データ２０３の推定誤り率２０４を推定する。

【００５８】

訂正部２６ｂの動作は、第１実施形態の訂正部２６と同じなので、説明を省略する。

【００５９】

なお上述の生成部１３ａ及び１３ｂは、１つの生成部として実現されていてもよい。同

様に、上述の訂正部２６ａ及び２６ｂは、１つの訂正部として実現されていてもよい。
【００６０】
以上、説明したように、第２実施形態の量子通信システム１００によれば、第１実施形態の場合と同様に、誤り訂正処理の設定情報をより適切に決定することができる。
【００６１】
（第３実施形態）
次に第３実施形態について説明する。第３実施形態の説明では、第１実施形態と同様の説明については省略し、第１実施形態と異なる箇所について説明する。第３実施形態では、推定誤り率２０４の推定方法が第１実施形態と異なる。
【００６２】
［機能構成の例］
図７は第３実施形態の量子通信システム１００の機能構成の例を示す図である。第３実施形態の量子通信システム１００は、送信装置１０及び受信装置２０を備える。
【００６３】
送信装置１０は、送信部１１、シフト処理部１２、生成部１３及び秘匿性増強処理部１４を備える。
【００６４】
受信装置２０は、受信部２１、シフト処理部２２、推定部２３、算出部２４、決定部２５、訂正部２６及び秘匿性増強処理部２７を備える。
【００６５】
推定部２３は、前回のシフト処理により取得されたシフト鍵データ２０３（第１シフト鍵データ）と、前回の誤り訂正処理により生成された訂正鍵データ２０８とを比較することにより得られた誤りビットの位置情報に基づいて、推定誤り率２０４を推定する。すなわち推定部２３は、前回のシフト処理によって取得されたシフト鍵データ２０３の誤り率により、次に誤り訂正処理の対象にするシフト鍵データ２０３の推定誤り率２０４を推定する。
【００６６】
なお、ひとつ前の誤り訂正処理が失敗した場合、決定部２５が、例えば使用可能なＬＤＰＣパラメータ２０７の中で、訂正能力が一番高いＬＤＰＣパラメータ２０７を、誤り訂正処理に使用するＬＤＰＣパラメータ２０７に決定してもよい。また例えば、推定部２３が、最後に訂正が成功した時のシフト鍵データ２０３の誤り率により、推定誤り率２０４を推定してもよい。
【００６７】
以上、説明したように、第３実施形態の量子通信システム１００によれば、第１実施形態の場合と同様に、誤り訂正処理の設定情報をより適切に決定することができる。
【００６８】
最後に、第１～第３実施形態の送信装置１０及び受信装置２０のハードウェア構成の例について説明する。
【００６９】
［ハードウェア構成の例］
図８は第１～第３実施形態の送信装置１０及び受信装置２０の主要部の構成の例を示す図である。第１～第３実施形態の送信装置１０及び受信装置２０は、制御装置３０１、主記憶装置３０２、補助記憶装置３０３、表示装置３０４、入力装置３０５、量子通信ＩＦ（Ｉｎｔｅｒｆａｃｅ）３０６及び古典通信ＩＦ３０７を備える。
【００７０】
制御装置３０１、主記憶装置３０２、補助記憶装置３０３、表示装置３０４、入力装置３０５、量子通信ＩＦ３０６及び古典通信ＩＦ３０７は、バス３１０を介して接続されている。
【００７１】
制御装置３０１は、補助記憶装置３０３から主記憶装置３０２に読み出されたプログラ

ムを実行する。主記憶装置３０２は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）及びＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等のメモリである。補助記憶装置３０３は、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）及びメモリカード等である。

【００７２】

表示装置３０４は、送信装置１０及び受信装置２０の状態等を表示する。入力装置３０５はユーザーからの入力を受け付ける。

【００７３】

量子通信ＩＦ３０６は、量子通信路１に接続するためのインターフェースである。受信装置２０の量子通信ＩＦ３０６は、上述の受信部２１のハードウェア構成（図３参照）を含む。古典通信ＩＦ３０７は、古典通信路２に接続するためのインターフェースである。

【００７４】

第１～第３実施形態の送信装置１０及び受信装置２０は、図８のハードウェア構成を備えていれば、汎用のコンピュータ等を含む任意の装置により実現可能である。

【００７５】

第１～第３実施形態の送信装置１０及び受信装置２０で実行されるプログラムは、インストール可能な形式又は実行可能な形式のファイルでＣＤ－ＲＯＭ、メモリカード、ＣＤ－Ｒ、及び、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）等のコンピュータで読み取り可能な記憶媒体に記憶されてコンピュータ・プログラム・プロダクトとして提供される。

【００７６】

また第１～第３実施形態の送信装置１０及び受信装置２０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。

【００７７】

また第１～第３実施形態の送信装置１０及び受信装置２０が実行するプログラムを、ダウンロードさせずにインターネット等のネットワーク経由で提供するように構成してもよい。

【００７８】

また第１～第３実施形態の送信装置１０及び受信装置２０で実行されるプログラムを、ＲＯＭ等に予め組み込んで提供するように構成してもよい。

【００７９】

第１～第３実施形態の送信装置１０及び受信装置２０で実行されるプログラムは、第１～第３実施形態の送信装置１０及び受信装置２０の機能構成のうち、プログラムにより実現可能な機能を含むモジュール構成となっている。

【００８０】

プログラムにより実現される機能は、制御装置３０１が補助記憶装置３０３等の記憶媒体からプログラムを読み出して実行することにより、主記憶装置３０２にロードされる。すなわちプログラムにより実現される機能は、主記憶装置３０２上に生成される。

【００８１】

なお第１～第３実施形態の送信装置１０及び受信装置２０の機能の一部又は全部を、ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）等のハードウェアにより実現してもよい。ＩＣは、例えば専用の処理を実行するプロセッサである。

【００８２】

また複数のプロセッサを用いて各機能を実現する場合、各プロセッサは、各機能のうち１つを実現してもよいし、各機能のうち２つ以上を実現してもよい。

【００８３】

また第１～第３実施形態の送信装置１０及び受信装置２０の動作形態は任意でよい。第１～第３実施形態の送信装置１０及び受信装置２０を、例えばネットワーク上のクラウドシステムを構成する装置として動作させてもよい。

【００８４】

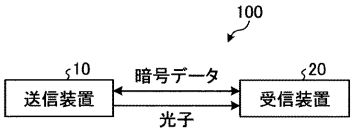
本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

【符号の説明】

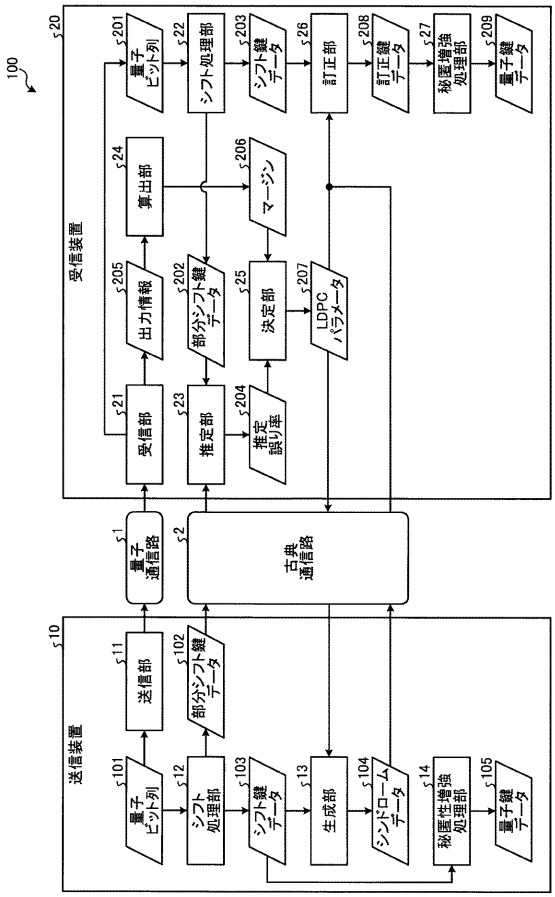
【００８５】

１０　送信装置
１１　送信部
１２　シフト処理部
１３　生成部
１４　秘匿性増強処理部
２０　受信装置
２１　受信部
２２　シフト処理部
２３　推定部
２４　算出部
２５　決定部
２６　訂正部
２７　秘匿性増強処理部
１００　量子通信システム
２２１　偏光調整器
２２２　マッハツェンダ干渉計
２２３　光学検出器
２２４　ファイバーストレッチャー
２２５　位相変調器
２４１　変動量算出部
２４２　マージン決定部
３０１　制御装置
３０２　主記憶装置
３０３　補助記憶装置
３０４　表示装置
３０５　入力装置
３０６　量子通信ＩＦ
３０７　古典通信ＩＦ
３１０　バス

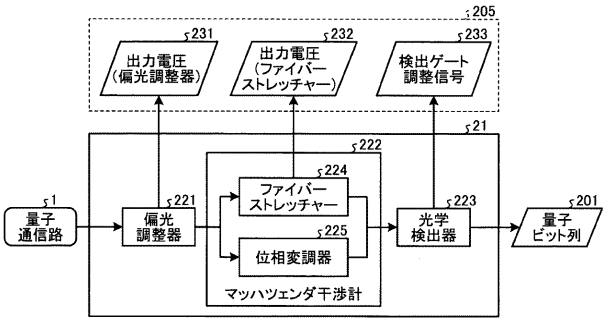
【図１】



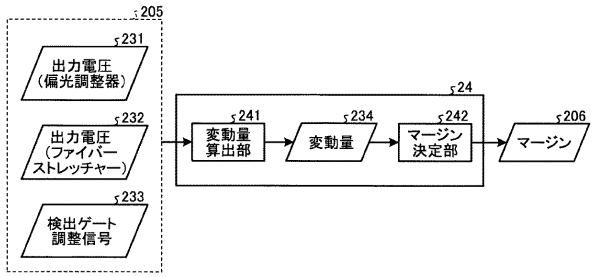
【図２】



【図３】



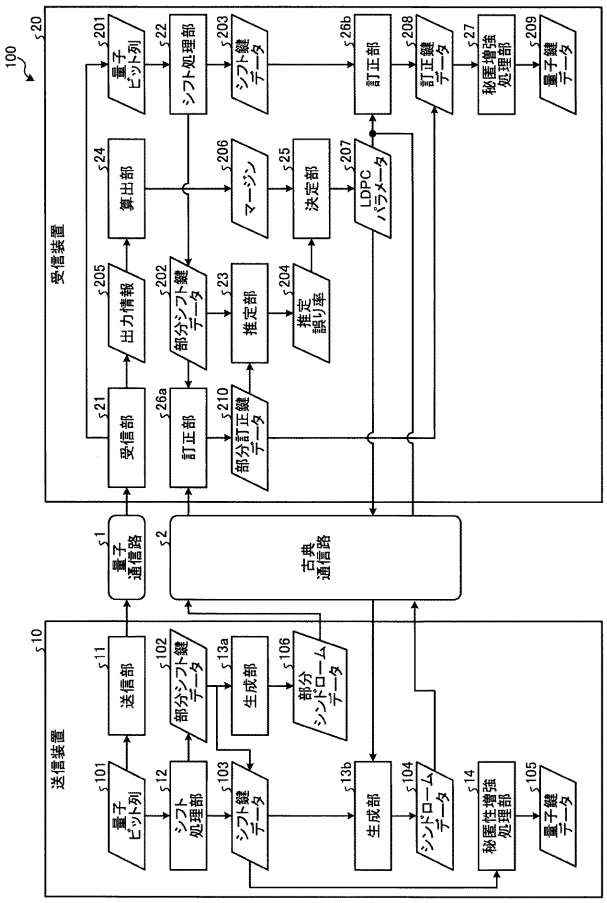
【図４】



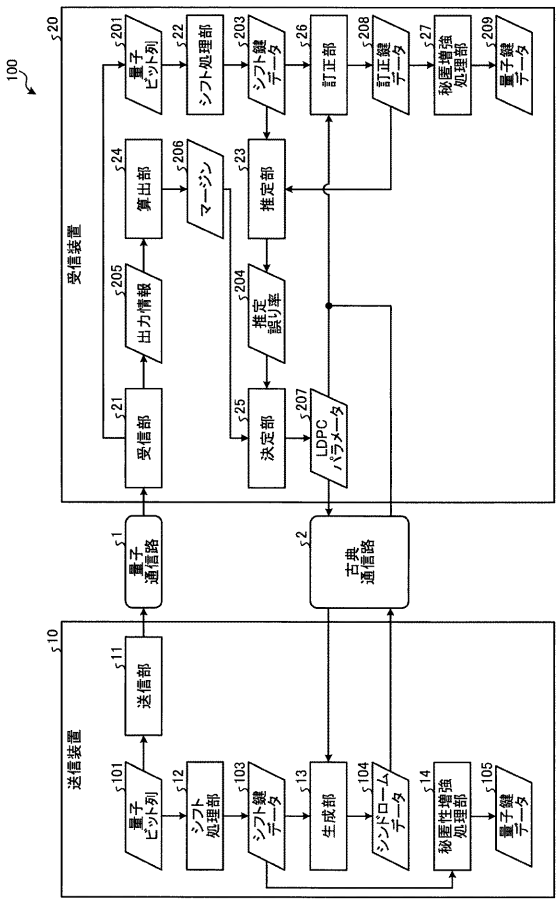
【図５】

設定誤り率	符号化率
2.00%	0.837
2.01%	0.837
2.02%	0.836
…	…
5.00%	0.671
5.01%	0.670
…	…
8.98%	0.499
8.99%	0.498
9.00%	0.498

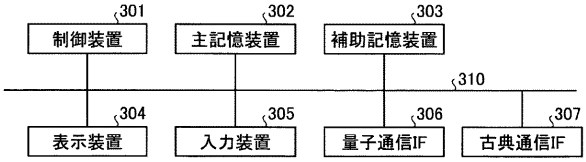
【図６】


100
受信装置
20
送信装置
10
量子通信路
1
古典通信路
2
量子ビット列
201
シフト処理部
22
シフト鍵データ
203
訂正部
26b
訂正鍵データ
208
秘匿増強処理部
27
量子鍵データ
209
算出部
24
マージン
206
決定部
25
LDPCパラメータ
207
出力情報
205
部分シフト鍵データ
202
推定部
23
推定誤り率
204
受信部
21
訂正部
26a
部分訂正鍵データ
210
送信部
11
部分シフト鍵データ
102
生成部
13a
部分シンドロームデータ
106
量子ビット列
101
シフト処理部
12
シフト鍵データ
103
生成部
13b
シンドロームデータ
104
秘匿性増強処理部
14
量子鍵データ
105

【図７】


100
受信装置
20
送信装置
10
量子通信路
1
古典通信路
2
量子ビット列
201
シフト処理部
22
シフト鍵データ
203
訂正部
26
訂正鍵データ
208
秘匿増強処理部
27
量子鍵データ
209
算出部
24
マージン
206
推定部
23
推定誤り率
204
受信部
21
決定部
25
LDPCパラメータ
207
出力情報
205
送信部
11
量子ビット列
101
シフト処理部
12
シフト鍵データ
103
生成部
13
シンドロームデータ
104
秘匿性増強処理部
14
量子鍵データ
105

【図８】


301
制御装置
302
主記憶装置
303
補助記憶装置
310
304
表示装置
305
入力装置
306
量子通信IF
307
古典通信IF

【手続補正書】
【提出日】平成29年8月30日(2017.8.30)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
送信装置から量子通信路を介して受信された量子ビット列にシフト処理を行うことにより得られた第１シフト鍵データを訂正する量子通信装置であって、
前記第１シフト鍵データの推定誤り率と、前記推定誤り率のマージンとから、前記第１シフト鍵データの誤り訂正処理の設定情報を決定する決定部と、
前記設定情報を使用して、前記誤り訂正処理を行うことにより、訂正鍵データを生成する訂正部と、
を備える量子通信装置。
【請求項２】
前記第１シフト鍵データに含まれる第１部分シフト鍵データと、前記送信装置の前記シフト処理により得られた第２シフト鍵データに含まれる第２部分シフト鍵データとを比較することにより、前記推定誤り率を推定する推定部、
を更に備える請求項１に記載の量子通信装置。
【請求項３】
前記訂正部は、前記第１シフト鍵データに含まれる第１部分シフト鍵データに、前記誤り訂正処理を行うことにより、部分訂正鍵データを生成し、
前記部分訂正鍵データと、前記第１部分シフト鍵データとを比較することにより、前記推定誤り率を推定する推定部、
を更に備える請求項１に記載の量子通信装置。
【請求項４】
前回の前記シフト処理により取得された前記第１シフト鍵データと、前回の前記誤り訂正処理により生成された前記訂正鍵データとを比較することにより、前記推定誤り率を推定する推定部、
を更に備える請求項１に記載の量子通信装置。
【請求項５】
前記量子ビット列の受信に使用される光学系機器の出力情報に基づいて前記マージンを算出する算出部、
を更に備える請求項１に記載の量子通信装置。
【請求項６】
前記光学系機器は、偏光調整器であり、
前記算出部は、前記偏光調整器の出力電圧の変動量に基づいて前記マージンを算出する、
請求項５に記載の量子通信装置。
【請求項７】
前記光学系機器は、ファイバーストレッチャーであり、
前記算出部は、前記ファイバーストレッチャーの出力電圧の変動量に基づいて前記マージンを算出する、
請求項５に記載の量子通信装置。
【請求項８】
前記光学系機器は、光学検出器であり、
前記算出部は、前記光学検出器の検出ゲート調整信号の変動量に基づいて前記マージンを算出する、

請求項５に記載の量子通信装置。
【請求項９】
送信装置と、前記送信装置から量子通信路を介して受信された量子ビット列にシフト処理を行うことにより得られた第１シフト鍵データを訂正する受信装置とを備える量子通信システムであって、
前記受信装置は、
前記第１シフト鍵データの推定誤り率と、前記推定誤り率のマージンとから、前記第１シフト鍵データの誤り訂正処理の設定情報を決定する決定部と、
前記設定情報を使用して、前記誤り訂正処理を行うことにより、訂正鍵データを生成する訂正部と、
を備える量子通信システム。
【請求項１０】
送信装置から量子通信路を介して受信された量子ビット列にシフト処理を行うことにより得られた第１シフト鍵データを訂正する量子通信装置の量子通信方法であって、
前記第１シフト鍵データの推定誤り率と、前記推定誤り率のマージンとから、前記第１シフト鍵データの誤り訂正処理の設定情報を決定するステップと、
前記設定情報を使用して、前記誤り訂正処理を行うことにより、訂正鍵データを生成するステップと、
を含む量子通信方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００５
【補正方法】変更
【補正の内容】
【０００５】
実施形態の量子通信装置は、送信装置から量子通信路を介して受信された量子ビット列にシフト処理を行うことにより得られた第１シフト鍵データを訂正する量子通信装置であって、決定部と訂正部とを備える。決定部は、前記第１シフト鍵データの推定誤り率と、前記推定誤り率のマージンとから、前記第１シフト鍵データの誤り訂正処理の設定情報を決定する。訂正部は、前記設定情報を使用して、前記誤り訂正処理を行うことにより、訂正鍵データを生成する。