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

特許第4862159号
(P4862159)

(45)発行日　平成24年1月25日(2012.1.25)　(24)登録日　平成23年11月18日(2011.11.18)

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

請求項の数 18 (全 33 頁)

(21)出願番号	特願2006-553998 (P2006-553998)
(86)(22)出願日	平成18年1月24日 (2006.1.24)
(86)国際出願番号	PCT/JP2006/301039
(87)国際公開番号	WO2006/078033
(87)国際公開日	平成18年7月27日 (2006.7.27)
審査請求日	平成20年11月27日 (2008.11.27)
(31)優先権主張番号	特願2005-15466 (P2005-15466)
(32)優先日	平成17年1月24日 (2005.1.24)
(33)優先権主張国	日本国 (JP)
(31)優先権主張番号	特願2005-188865 (P2005-188865)
(32)優先日	平成17年6月28日 (2005.6.28)
(33)優先権主張国	日本国 (JP)

(73)特許権者　504202472
大学共同利用機関法人情報・システム研究機構
東京都立川市緑町１０番３号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　渡辺　曜大
東京都千代田区一ツ橋２丁目１番２号　学術総合センター内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】量子鍵配送方法、通信システムおよび通信装置

(57)【特許請求の範囲】

【請求項１】

基底およびデータに対応する２つの乱数列によって規定された量子状態を生成する量子状態生成器を備え当該量子状態を量子通信路上に送信する第１の通信装置と、当該量子通信路上の量子状態を乱数列により規定された基底を用いて測定することによりデータを得る第２の通信装置と、から構成され、前記第２の通信装置が、前記第１の通信装置と同一の基底を用いた測定により得られたデータを受信データとし、前記第１の通信装置が、当該受信データに対応する乱数列を送信データとする量子鍵配送を実現する通信システムであって、前記量子状態を知らない盗聴者が任意に基底を選択して量子通信路上の量子状態を測定可能な通信システムによる、量子鍵配送方法において、

前記第１の通信装置が、前記送信データから所定数の第１の部分データを抽出し、一方で、前記第２の通信装置から前記第１の部分データと同一位置の第２の部分データ（前記受信データから抽出された部分データ）を受信し、両方の部分データの一致度（エラー確率）に基づいて、鍵生成に用いるデータにおけるエラー確率を推定する第１のエラー確率推定ステップと、

前記第２の通信装置が、前記第１の通信装置から前記第１の部分データを受信し、当該第１の部分データと前記第２の部分データとの一致度（エラー確率）に基づいて、鍵生成に用いるデータにおけるエラー確率を推定する第２のエラー確率推定ステップと、

前記第１の通信装置が、前記第１のエラー確率推定ステップにより得られたエラー確率推定値と、前記量子状態生成器の特性に関する情報とに基づいて、量子通信路を通して盗

聴者にもれた情報量を推定する第１の情報量推定ステップと、
前記第２の通信装置が、前記第２のエラー確率推定ステップにより得られたエラー確率推定値と前記第１の通信装置が備える量子状態生成器の特性に関する情報とに基づいて、量子通信路を通して盗聴者にもれた情報量を推定する第２の情報量推定ステップと、
前記第１の通信装置が、前記第１の情報量推定ステップにより得られた盗聴者にもれた情報量の推定値に基づいて圧縮した後の送信データを、各通信装置間で共有の暗号鍵とする第１の共有鍵生成ステップと、
前記第２の通信装置が、前記第２の情報量推定ステップにより得られた盗聴者にもれた情報量の推定値に基づいて圧縮した後の受信データを、各通信装置間で共有の暗号鍵とする第２の共有鍵生成ステップと、
を含むことを特徴とする量子鍵配送方法。

【請求項２】
前記第１および第２の情報量推定ステップにおいては、前記エラー確率推定値と、前記第１の通信装置が備える量子状態生成器および前記第２の通信装置が備える量子状態測定器の特性に関する情報、に基づいて、量子通信路を通して盗聴者にもれた情報量を推定することを特徴とする請求項１に記載の量子鍵配送方法。

【請求項３】
前記第１の情報量推定ステップにおいては、第１の通信装置が持つ送信データを所定の数に分割し、当該分割データのそれぞれに対して盗聴者にもれた情報量を推定し、
前記第２の情報量推定ステップにおいては、第２の通信装置が持つ受信データを前記所定の数に分割し、当該分割データのそれぞれに対して盗聴者にもれた情報量を推定する、
ことを特徴とする請求項２に記載の量子鍵配送方法。

【請求項４】
さらに、第１の通信装置が持つ送信データと第２の通信装置が持つ受信データが一致しているかどうかを判定するための所定の判定情報に基づいて判定処理を行い、当該判定結果が不一致の場合、前記各通信装置が持つデータを捨てる一致判定ステップ、
を含み、
前記一致判定ステップでは、
前記第１の通信装置および前記第２の通信装置が、前記所定の判定情報のビット長α（αは前記送信データおよび前記受信データのビット長βよりも短いビット長）を決定し、いずれか一方の通信装置が、β列×α行のランダム行列を生成し、当該ランダム行列を、公開通信路を介して他方の通信装置に送信し、
前記第１の通信装置が、前記所定の判定情報として、「前記ランダム行列×第１の通信装置が持つ送信データ」の計算によりビット長αの第１の判定情報を求め、当該第１の判定情報を、公開通信路を介して前記第２の通信装置に送信し、
前記第２の通信装置が、前記所定の判定情報として、「前記ランダム行列×第２の通信装置が持つ受信データ」の計算により前記第１の判定情報と同一ビット長の第２の判定情報を求め、当該第２の判定情報を、公開通信路を介して前記第１の通信装置に送信し、
その後、前記第１の通信装置が、前記判定処理として、前記第１の判定情報と前記第２の通信装置から得られた第２の判定情報とが一致しているかどうかを判定し、
一方、前記第２の通信装置が、前記判定処理として、前記第２の判定情報と前記第１の通信装置から得られた第１の判定情報とが一致しているかどうかを判定することを特徴とする請求項１、２または３に記載の量子鍵配送方法。

【請求項５】
２準位の量子系を前提とした場合、
前記第１および第２の情報量推定ステップでは、
解析の比較的容易な近似プロトコル（性質のよい量子状態を用いたプロトコル）と現実のプロトコル（現実の状況における送信誤差を含む量子状態を用いたプロトコル）の変動距離の上限値を計算する第１の工程と、
前記近似プロトコルにおいて、現実とは反対の基底を用いた場合に、前記エラー確率推

定値が真の値よりも小さく見積もられてしまう確率の上限値を計算する第２の工程と、
送信データを条件とした場合の受信データおよび盗聴情報の条件付確率の上限値を計算する第３の工程と、
前記第２の工程にて得られる前記エラー確率推定値が真の値よりも小さく見積もられてしまう確率の上限値、および前記第３の工程にて得られる条件付確率の上限値に基づいて、前記近似プロトコルにおける盗聴量を計算する第４の工程と、
前記近似プロトコルにおける盗聴量、および前記第１の工程にて得られる変動距離の上限値に基づいて、現実のプロトコルにおける盗聴量を計算し、その結果を、前記量子通信路を通して盗聴者にもれた情報量とする第５の工程と、
を含むことを特徴とする請求項１に記載の量子鍵配送方法。

【請求項６】
２準位の量子系を前提とした場合、
前記第１および第２の情報量推定ステップでは、
解析の比較的容易な近似プロトコル（性質のよい演算子を用いたプロトコル）と現実のプロトコル（現実の状況における受信誤差を含む測定演算子を用いたプロトコル）の変動距離の上限値を計算する第１の工程と、
前記近似プロトコルにおいて、現実とは反対の基底を用いた場合に、前記エラー確率推定値が真の値よりも小さく見積もられてしまう確率の上限値を計算する第２の工程と、
送信データを条件とした場合の受信データおよび盗聴情報の条件付確率の上限値を計算する第３の工程と、
前記第２の工程にて得られる前記エラー確率推定値が真の値よりも小さく見積もられてしまう確率の上限値、および前記第３の工程にて得られる条件付確率の上限値に基づいて、前記近似プロトコルにおける盗聴量を計算する第４の工程と、
前記近似プロトコルにおける盗聴量、および前記第１の工程にて得られる変動距離の上限値に基づいて、現実のプロトコルにおける盗聴量を計算し、その結果を、前記量子通信路を通して盗聴者にもれた情報量とする第５の工程と、
を含むことを特徴とする請求項２に記載の量子鍵配送方法。

【請求項７】
前記第１および第２の情報量推定ステップでは、前記第１の通信装置が備える量子状態生成器の特性に基づいて、または、前記第１の通信装置が備える量子状態生成器および前記第２の通信装置が備える量子状態測定器の特性に基づいて、鍵の持つ情報量を推定し、
各通信装置は、前記鍵の持つ情報量の推定値に基づいてそれぞれが持つデータを圧縮し、圧縮後のデータを各通信装置間で共有の暗号鍵とすることを特徴とする請求項１に記載の量子鍵配送方法。

【請求項８】
必ずしも２準位とは限らない量子系を前提とし、前記第２の通信装置の観測値として「０」、「１」の他に「非検出」という結果を想定し、さらに、全送信データをｘ［Ａ］とし、当該ｘ［Ａ］のうち第２の通信装置で検出できたデータ部分をｘ［Ｄ］とし、当該ｘ［Ｄ］のうち送信側と受信側で用いた基底が一致した部分をｘ［Ｃ］とし、前記各エラー確率推定ステップにて用いた部分データをｘ［Ｒ］とし、共有鍵生成用の部分データ（ｘ［Ｃ］－ｘ［Ｒ］）をｘ［Ｋ］とした場合（Ａ、Ｄ、Ｃ、Ｋ、Ｒはビット位置を示す部分集合に相当）、
量子状態を、鍵の持つ情報量ができるだけ大きく見積もれるように、ヒルベルト空間上の第１の密度演算子を含む部分（部分集合Ｋのうちの部分Ｌに相当）、第２の密度演算子を含む部分（部分集合Ｋのうちの部分Ｍ（＝Ｋ－Ｌ）に相当）に分解する第１の工程と、
前記部分Ｍの持つ情報量を見積もる第２の工程と、
前記部分Ｌの持つ情報量を見積もる第３の工程と、
前記部分Ｍの持つ情報量と前記部分Ｌの持つ情報量とを用いて前記部分Ｋの持つ情報量を計算する第４の工程と、
を含むことを特徴とする請求項７に記載の量子鍵配送方法。

【請求項９】
２つの非直交量子状態を用いる量子鍵配送方式に対して適用可能とすることを特徴とする請求項８に記載の量子鍵配送方法。
【請求項１０】
基底およびデータに対応する２つの乱数列によって規定された量子状態を量子通信路上に送信する第１の通信装置と、当該量子通信路上の量子状態を乱数列により規定された基底を用いて測定することによりデータを得る第２の通信装置と、から構成され、前記第２の通信装置が、前記第１の通信装置と同一の基底を用いた測定により得られたデータを受信データとし、前記第１の通信装置が、当該受信データに対応する乱数列を送信データとする量子鍵配送を実現する通信システムにおいて、
前記第１の通信装置は、
前記送信データから所定数の第１の部分データを抽出し、一方で、前記第２の通信装置から前記第１の部分データと同一位置の第２の部分データ（前記受信データから抽出された部分データ）を受信し、両方の部分データの一致度（エラー確率）に基づいて、鍵生成に用いるデータにおけるエラー確率を推定し、その後、前記エラー確率推定値と自装置が備える量子状態生成器の特性に関する情報に基づいて、量子通信路を通して盗聴者にもれた情報量を推定し、そして、当該盗聴者にもれた情報量の推定値に基づいて圧縮した後の送信データを各通信装置間で共有の暗号鍵とする第１の共有鍵生成手段、
を備え、
前記第２の通信装置は、
前記第２の部分データと前記第１の通信装置から受信した前記第１の部分データとの一致度（エラー確率）に基づいて、鍵生成に用いるデータにおけるエラー確率を推定し、その後、前記エラー確率推定値と前記第１の通信装置が備える量子状態生成器の特性に関する情報に基づいて、量子通信路を通して盗聴者にもれた情報量を推定し、そして、当該盗聴者にもれた情報量の推定値に基づいて圧縮した後の受信データを各通信装置間で共有の暗号鍵とする第２の共有鍵生成手段、
を備えることを特徴とする通信システム。
【請求項１１】
前記第１および第２の共有鍵生成手段は、前記エラー確率推定値と、前記第１の通信装置が備える量子状態生成器および前記第２の通信装置が備える量子状態測定器の特性に関する情報、に基づいて、量子通信路を通して盗聴者にもれた情報量を推定することを特徴とする請求項１０に記載の通信システム。
【請求項１２】
前記第１および第２の共有鍵生成手段は、
さらに、第１の通信装置が持つ送信データと第２の通信装置が持つ受信データが一致しているかどうかを判定するための所定の判定情報に基づいて判定処理を行い、当該判定結果が不一致の場合、前記各通信装置が持つデータを捨てる処理を実行し、
前記判定処理では、
前記第１の共有鍵生成手段および前記第２の共有鍵生成手段が、前記所定の判定情報のビット長α（αは前記送信データおよび前記受信データのビット長βよりも短いビット長）を決定し、いずれか一方の共有鍵生成手段が、β列×α行のランダム行列を生成し、当該ランダム行列を、公開通信路を介して他方の共有鍵生成手段に送信し、
前記第１の共有鍵生成手段が、前記所定の判定情報として、「前記ランダム行列×第１の通信装置が持つ送信データ」の計算によりビット長αの第１の判定情報を求め、当該第１の判定情報を、公開通信路を介して前記第２の通信装置に送信し、
前記第２の共有鍵生成手段が、前記所定の判定情報として、「前記ランダム行列×第２の通信装置が持つ受信データ」の計算により前記第１の判定情報と同一ビット長の第２の判定情報を求め、当該第２の判定情報を、公開通信路を介して前記第１の通信装置に送信し、
その後、前記第１の共有鍵生成手段が、前記第１の判定情報と前記第２の通信装置から

得られた第２の判定情報とが一致しているかどうかを判定し、
一方、前記第２の共有鍵生成手段が、前記第２の判定情報と前記第１の通信装置から得られた第１の判定情報とが一致しているかどうかを判定することを特徴とする請求項１０または１１に記載の通信システム。
【請求項１３】
基底およびデータに対応する２つの乱数列によって規定された量子状態を量子通信路上に送信し、当該量子状態の受信側の通信装置において送信側と同一の基底を用いた測定により得られたデータ、に対応する乱数列を第１の送信データとする量子状態送信側の通信装置において、
前記第１の送信データから所定数のビット位置のデータを抽出し、抽出後の部分データを、公開通信路を介して前記受信側の通信装置に通知し、その後、前記受信側の通信装置から得られる同一ビット位置の部分データとの一致度（エラー確率）に基づいて、鍵生成に用いるデータのエラー確率を推定し、さらに、公開した部分データ以外の残りのデータを第２の送信データとするエラー確率推定手段と、
所定の誤り訂正情報を、公開通信路を介して前記受信側の通信装置に通知し、公開した誤り訂正情報の量に応じて前記第２の送信データを圧縮し、圧縮後のデータを第３の送信データとする誤り訂正手段と、
前記第３の送信データと前記受信側の通信装置から得られるデータとが一致しているかどうかを判定するための判定情報を、公開通信路を介して前記受信側の通信装置に通知し、前記判定情報に基づく判定結果が不一致の場合、前記第３の送信データを捨て、一方、前記判定結果が一致の場合、公開した判定情報の量に応じて前記第３の送信データを圧縮し、圧縮後のデータを第４の送信データとする一致判定手段と、
前記推定エラー確率および送信機または受信機の特性に関する情報から量子通信路を通して盗聴者にもれた情報量を推定する推定手段と、
前記盗聴者にもれた情報量の推定値に基づいて前記第４の送信データを圧縮し、圧縮後のデータを装置間で共有の暗号鍵とする共有鍵生成手段と、
を有することを特徴とする通信装置。
【請求項１４】
量子通信路上の量子状態に対して乱数列により規定された基底を用いて測定することにより得られたデータのうち、当該量子状態の送信側の通信装置と同一の基底を用いた測定により得られたデータを第１の受信データとする量子状態受信側の通信装置において、
前記第１の受信データから所定数のビット位置のデータを抽出し、抽出後の部分データを、公開通信路を介して前記送信側の通信装置に通知し、その後、前記送信側の通信装置から得られる同一ビット位置の部分データとの一致度（エラー確率）に基づいて、鍵生成に用いるデータのエラー確率を推定し、さらに、公開した部分データ以外の残りのデータを第２の受信データとするエラー確率推定手段と、
前記送信側の通信装置から得られる誤り訂正情報に基づいて前記第２の受信データの誤りを訂正し、前記送信側の通信装置により公開された誤り訂正情報の量に応じて前記誤り訂正後の第２の受信データを圧縮し、圧縮後のデータを第３の受信データとする誤り訂正手段と、
前記第３の受信データと前記送信側の通信装置から得られるデータとが一致しているかどうかを判定するための判定情報を、公開通信路を介して前記送信側の通信装置に通知し、前記判定情報に基づく判定結果が不一致の場合、前記第３の受信データを捨て、一方、前記判定結果が一致の場合、公開した判定情報の量に応じて前記第３の受信データを圧縮し、圧縮後のデータを第４の受信データとする一致判定手段と、
前記推定エラー確率および送信機または受信機の特性に関する情報から量子通信路を通して盗聴者にもれた情報量を推定する推定手段と、
前記盗聴者にもれた情報量の推定値に基づいて前記第４の受信データを圧縮し、圧縮後のデータを装置間で共有の暗号鍵とする共有鍵生成手段と、
を有することを特徴とする通信装置。

【請求項１５】
基底およびデータに対応する２つの乱数列によって規定された量子状態を量子通信路上に送信し、当該量子状態の受信側の通信装置において送信側と同一の基底を用いた測定により得られたデータ、に対応する乱数列を第１の送信データとする量子状態送信側の通信装置において、
前記第１の送信データから所定数のビット位置のデータを抽出し、抽出後の部分データを、公開通信路を介して前記受信側の通信装置に通知し、その後、前記受信側の通信装置から得られる同一ビット位置の部分データとの一致度（エラー確率）に基づいて、鍵生成に用いるデータのエラー確率を推定し、さらに、公開した部分データ以外の残りのデータを第２の送信データとするエラー確率推定手段と、
所定の誤り訂正情報を、公開通信路を介して前記受信側の通信装置に通知し、公開した誤り訂正情報の量に応じて前記第２の送信データを圧縮し、圧縮後のデータを第３の送信データとする誤り訂正手段と、
前記第３の送信データと前記受信側の通信装置から得られるデータとが一致しているかどうかを判定するための判定情報を、公開通信路を介して前記受信側の通信装置に通知し、前記判定情報に基づく判定結果が不一致の場合、前記第３の送信データを捨て、一方、前記判定結果が一致の場合、公開した判定情報の量に応じて前記第３の送信データを圧縮し、圧縮後のデータを第４の送信データとする一致判定手段と、
自装置が備える量子状態生成器の特性に基づいて、または、当該量子状態生成器および前記受信側の通信装置が備える量子状態測定器の特性に基づいて、鍵の持つ情報量を推定する推定手段と、
前記鍵の持つ情報量の推定値に基づいて前記第４の送信データを圧縮し、圧縮後のデータを装置間で共有の暗号鍵とする共有鍵生成手段と、
を有することを特徴とする通信装置。
【請求項１６】
量子通信路上の量子状態に対して乱数列により規定された基底を用いて測定することにより得られたデータのうち、当該量子状態の送信側の通信装置と同一の基底を用いた測定により得られたデータを第１の受信データとする量子状態受信側の通信装置において、
前記第１の受信データから所定数のビット位置のデータを抽出し、抽出後の部分データを、公開通信路を介して前記送信側の通信装置に通知し、その後、前記送信側の通信装置から得られる同一ビット位置の部分データとの一致度（エラー確率）に基づいて、鍵生成に用いるデータのエラー確率を推定し、さらに、公開した部分データ以外の残りのデータを第２の受信データとするエラー確率推定手段と、
前記送信側の通信装置から得られる誤り訂正情報に基づいて前記第２の受信データの誤りを訂正し、前記送信側の通信装置により公開された誤り訂正情報の量に応じて前記誤り訂正後の第２の受信データを圧縮し、圧縮後のデータを第３の受信データとする誤り訂正手段と、
前記第３の受信データと前記送信側の通信装置から得られるデータとが一致しているかどうかを判定するための判定情報を、公開通信路を介して前記送信側の通信装置に通知し、前記判定情報に基づく判定結果が不一致の場合、前記第３の受信データを捨て、一方、前記判定結果が一致の場合、公開した判定情報の量に応じて前記第３の受信データを圧縮し、圧縮後のデータを第４の受信データとする一致判定手段と、
前記送信側の通信装置が備える量子状態生成器の特性に基づいて、または、当該量子状態生成器および自装置が備える量子状態測定器の特性に基づいて、鍵の持つ情報量を推定する推定手段と、
前記鍵の持つ情報量の推定値に基づいて前記第４の受信データを圧縮し、圧縮後のデータを装置間で共有の暗号鍵とする共有鍵生成手段と、
を有することを特徴とする通信装置。
【請求項１７】
データに対応する乱数列によって規定された量子状態を量子通信路上に送信し、当該量

子状態の受信側の通信装置における測定結果と一致も直交もしない量子状態、に対応する乱数列を第１の送信データとする量子状態送信側の通信装置において、
前記第１の送信データから所定数のビット位置のデータを抽出し、抽出後の部分データを、公開通信路を介して前記受信側の通信装置に通知し、その後、前記受信側の通信装置から得られる同一ビット位置の部分データとの一致度（エラー確率）に基づいて、鍵生成に用いるデータのエラー確率を推定し、さらに、公開した部分データ以外の残りのデータを第２の送信データとするエラー確率推定手段と、
所定の誤り訂正情報を、公開通信路を介して前記受信側の通信装置に通知し、公開した誤り訂正情報の量に応じて前記第２の送信データを圧縮し、圧縮後のデータを第３の送信データとする誤り訂正手段と、
前記第３の送信データと前記受信側の通信装置から得られるデータとが一致しているかどうかを判定するための判定情報を、公開通信路を介して前記受信側の通信装置に通知し、前記判定情報に基づく判定結果が不一致の場合、前記第３の送信データを捨て、一方、前記判定結果が一致の場合、公開した判定情報の量に応じて前記第３の送信データを圧縮し、圧縮後のデータを第４の送信データとする一致判定手段と、
自装置が備える量子状態生成器の特性に基づいて、または、当該量子状態生成器および前記受信側の通信装置が備える量子状態測定器の特性に基づいて、鍵の持つ情報量を推定する推定手段と、
前記鍵の持つ情報量の推定値に基づいて前記第４の送信データを圧縮し、圧縮後のデータを装置間で共有の暗号鍵とする共有鍵生成手段と、
を有することを特徴とする通信装置。
【請求項１８】
量子通信路上の量子状態に対して乱数列により規定された基底を用いて測定することにより得られたデータのうち、送信側の量子状態と一致も直交もしない測定結果、に対応するデータを第１の受信データとする量子状態受信側の通信装置において、
前記第１の受信データから所定数のビット位置のデータを抽出し、抽出後の部分データを、公開通信路を介して前記量子状態の送信側の通信装置に通知し、その後、前記送信側の通信装置から得られる同一ビット位置の部分データとの一致度（エラー確率）に基づいて、鍵生成に用いるデータのエラー確率を推定し、さらに、公開した部分データ以外の残りのデータを第２の受信データとするエラー確率推定手段と、
前記送信側の通信装置から得られる誤り訂正情報に基づいて前記第２の受信データの誤りを訂正し、前記送信側の通信装置により公開された誤り訂正情報の量に応じて前記誤り訂正後の第２の受信データを圧縮し、圧縮後のデータを第３の受信データとする誤り訂正手段と、
前記第３の受信データと前記送信側の通信装置から得られるデータとが一致しているかどうかを判定するための判定情報を、公開通信路を介して前記送信側の通信装置に通知し、前記判定情報に基づく判定結果が不一致の場合、前記第３の受信データを捨て、一方、前記判定結果が一致の場合、公開した判定情報の量に応じて前記第３の受信データを圧縮し、圧縮後のデータを第４の受信データとする一致判定手段と、
前記送信側の通信装置が備える量子状態生成器の特性に基づいて、または、当該量子状態生成器および自装置が備える量子状態測定器の特性に基づいて、鍵の持つ情報量を推定する推定手段と、
前記鍵の持つ情報量の推定値に基づいて前記第４の受信データを圧縮し、圧縮後のデータを装置間で共有の暗号鍵とする共有鍵生成手段と、
を有することを特徴とする通信装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法に関するものであり、特に、誤り訂正技術および秘匿性増強技術を適用することによって、

量子状態について送信機および受信機に誤差があるような現実的な実装においても安全性を保証することのできる量子鍵配送方法および当該量子鍵配送を実現可能な通信装置に関するものである。

【背景技術】

【０００２】

以下、従来の量子暗号システムについて説明する。近年、高速大容量の通信技術として光通信が広く利用されているが、このような光通信システムでは、光のオン／オフで通信が行われ、オンのときに大量の光子が送信されているため、量子効果が直接現れる通信系にはなっていない。

【０００３】

一方、量子暗号システムでは、通信媒体として光子を用い、不確定性原理等の量子効果が生じるように１個の光子で１ビットの情報を伝送する。このとき、盗聴者が、その偏光，位相等の量子状態を知らずに適当に基底を選んで光子を測定すると、その量子状態に変化が生じる。したがって、受信側では、この光子の量子状態の変化を確認することによって、伝送データが盗聴されたかどうかを認識することができる。

【０００４】

図９は、従来の偏光を利用した量子鍵配送の概要を示す図である。たとえば、水平垂直方向の偏光を識別可能な測定器では、量子通信路上の、水平方向（０°）に偏光された光と垂直方向（９０°）に偏光された光とを正しく識別する。一方、斜め方向（４５°，１３５°）の偏光を識別可能な測定器では、量子通信路上の、４５°方向に偏光された光と１３５°方向に偏光された光とを正しく識別する。

【０００５】

このように、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（０°，９０°）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ５０％の確率でランダムに識別することになる。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

【０００６】

図９に示す従来の量子鍵配送では、上記不確定性（ランダム性）を利用して、盗聴者に知られずに送信者と受信者との間で鍵を共有する（たとえば、非特許文献１参照）。なお、送信者および受信者は、量子通信路以外に公開通信路を使用することができる。

【０００７】

ここで、鍵の共有手順について説明する。まず、送信者は、乱数列（１，０の列：送信データ）を発生し、さらに送信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応，×：斜め方向に偏光された光を識別可能な測定器に対応）をランダムに決定する。その乱数列と送信コードの組み合わせで、送信する光の偏光方向が自動的に決まる。ここでは、０と＋の組み合わせで水平方向に偏光された光を、１と＋の組み合わせで垂直方向に偏光された光を、０と×の組み合わせで４５°方向に偏光された光を、１と×の組み合わせで１３５°方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。

【０００８】

つぎに、受信者は、受信コード（＋：水平垂直方向に偏光された光を識別可能な測定器，×：斜め方向に偏光された光を識別可能な測定器）をランダムに決定し、量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組み合わせによって受信データを得る。ここでは、受信データとして、水平方向に偏光された光と＋の組み合わせで０を、垂直方向に偏光された光と＋の組み合わせで１を、４５°方向に偏光された光と×の組み合わせで０を、１３５°方向に偏光された光と×の組み合わせで１を、それぞれ得る。

【０００９】

つぎに、受信者は、自身の測定が送信側と同一の基底を用いた測定かどうか、すなわち、正しい測定器で行われたものかどうかを調べるために、受信コードを、公開通信路を介して送信者に対して送信する。受信コードを受け取った送信者は、測定が正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信者に対して返信する。

【００１０】

つぎに、受信者は、正しい測定器で受信した受信信号に対応する受信データだけを残し、その他を捨てる。この時点で、残された受信データは送信者と受信者との間で共有できている。

【００１１】

つぎに、送信者と受信者は、それぞれの通信相手に対して、共有データから選択した所定数のデータを、公開通信路を経由して送信する。そして、受け取ったデータが自身の持つデータと一致しているかどうかを確認する。たとえば、確認したデータの中に一致しないデータが１つでもあれば、盗聴者がいるものと判断して共有データを捨て、再度、鍵の共有手順を最初からやり直す。一方、確認したデータがすべて一致した場合には、盗聴者がいないと判断し、確認に使用したデータを捨て、残った共有データを送信者と受信者の共有鍵とする。

【００１２】

【非特許文献１】Bennett,C.H. and Brassard,G. : Quantum Cryptography : Public Key Distribution andCoin Tossing, In Proceedings of IEEE Conference on Computers, System and SignalProcessing, Bangalore, India, pp.175-179(DEC.1984).

【発明の開示】

【発明が解決しようとする課題】

【００１３】

しかしながら、上記図９に示す従来の量子鍵配送においては、誤り通信路を想定していないため、誤りがある場合には盗聴行為が存在したものとして上記共通データ（共通鍵）を捨てることとなり、伝送路によっては共通鍵の生成効率が非常に悪くなる、という問題があった。また、送信機または受信機のどちらか一方に誤差が存在するような場合には、安全性が保証されない、という問題もあった。

【００１４】

本発明は、上記に鑑みてなされたものであって、極めて高い特性を持つ誤り訂正符号を用いて伝送路上におけるデータ誤りを訂正することにより高い鍵生成効率を達成しつつ、さらに、送信機または受信機の特性に関する情報を考慮して盗聴者に漏れた情報量を見積もることにより、送信機および受信機に誤差があるような現実的な実装においても高度に安全性の保証された量子鍵配送方法を得ることを目的とする。

【課題を解決するための手段】

【００１５】

上述した課題を解決し、目的を達成するために、本発明にかかる量子鍵配送方法にあっては、基底およびデータに対応する２つの乱数列によって規定された量子状態を生成する量子状態生成器を備え当該量子状態を量子通信路上に送信する第１の通信装置と、当該量子通信路上の量子状態を乱数列により規定された基底を用いて測定することによりデータを得る第２の通信装置と、から構成され、前記第２の通信装置が、前記第１の通信装置と同一の基底を用いた測定により得られたデータを受信データとし、前記第１の通信装置が、当該受信データに対応する乱数列を送信データとする量子鍵配送を実現する通信システムであって、前記量子状態を知らない盗聴者が任意に基底を選択して量子通信路上の量子状態を測定可能な通信システムによる、量子鍵配送方法において、前記第１の通信装置が、前記送信データから所定数の第１の部分データを抽出し、一方で、前記第２の通信装置から前記第１の部分データと同一位置の第２の部分データ（前記受信データから抽出された部分データ）を受信し、両方の部分データの一致度（エラー確率）に基づいて、鍵生成

に用いるデータにおけるエラー確率を推定する第１のエラー確率推定ステップと、前記第２の通信装置が、前記第１の通信装置から前記第１の部分データを受信し、当該第１の部分データと前記第２の部分データとの一致度（エラー確率）に基づいて、鍵生成に用いるデータにおけるエラー確率を推定する第２のエラー確率推定ステップと、前記第１の通信装置が、前記第１のエラー確率推定ステップにより得られたエラー確率推定値と、前記量子状態生成器の特性に関する情報とに基づいて、量子通信路を通して盗聴者にもれた情報量を推定する第１の情報量推定ステップと、前記第２の通信装置が、前記第２のエラー確率推定ステップにより得られたエラー確率推定値と前記第１の通信装置が備える量子状態生成器の特性に関する情報とに基づいて、量子通信路を通して盗聴者にもれた情報量を推定する第２の情報量推定ステップと、前記第１の通信装置が、前記第１の情報量推定ステップにより得られた盗聴者にもれた情報量の推定値に基づいて圧縮した後の送信データを、各通信装置間で共有の暗号鍵とする第１の共有鍵生成ステップと、前記第２の通信装置が、前記第２の情報量推定ステップにより得られた盗聴者にもれた情報量の推定値に基づいて圧縮した後の受信データを、各通信装置間で共有の暗号鍵とする第２の共有鍵生成ステップと、を含むことを特徴とする。

【発明の効果】

【００３３】

この発明によれば、現実的な実装においても、高度に安全性の保証された共通鍵を効率良く生成することができる、という効果を奏する。

【図面の簡単な説明】

【００３４】

【図１】図１は、本発明にかかる量子暗号システムにおける通信装置の構成を示す図である。

【図２－１】図２－１は、本発明の量子鍵配送を示すフローチャートである。

【図２－２】図２－２は、本発明の量子鍵配送を示すフローチャートである。

【図３】図３は、有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法の一例を示すフローチャートである。

【図４】図４は、有限アフィン幾何符号ＡＧ（２，２^{2}）のマトリクスを示す図である。

【図５】図５は、シンドローム生成部にて生成した$Ｓ_{Ａ}$を示す図である。

【図６－１】図６－１は、情報$Ｍ_{ＰＣ}$ｘ（ｎ－ｋ）を示す図である。

【図６－２】図６－２は、情報$Ｍ_{ＰＣ}$ｙ（ｎ－ｋ）′を示す図である。

【図７－１】図７－１は、送信データｘ′を示す図である。

【図７－２】図７－２は、受信データｙ′を示す図である。

【図８－１】図８－１は、送信側の通信装置にて生成した暗号鍵ｒを示す図である。

【図８－２】図８－２は、受信側の通信装置にて生成した暗号鍵ｒを示す図である。

【図９】図９は、従来の偏光を利用した量子鍵配送の概要を示す図である。

【符号の説明】

【００３５】

１，３　暗号鍵生成部
２，４　通信部
１０，３０　パリティ検査行列生成部
１１，３１　乱数発生部
１２　光子生成部
１３，３４　公開通信路通信部
１４　シンドローム生成部
１５，３５　共有鍵生成部
２１，４２　暗号化部
２２，４１　送受信部
３２　光子受信部
３３　シンドローム復号部

【発明を実施するための最良の形態】
【００３６】
以下に、本発明にかかる量子鍵配送方法および通信装置の実施例を図面に基づいて詳細に説明する。なお、この実施例によりこの発明が限定されるものではない。
【実施例１】
【００３７】
量子鍵配送は、盗聴者の計算能力によらず、安全性の保証された鍵配送方式であるが、たとえば、より効率よく共有鍵を生成するためには、伝送路を通ることによって発生するデータの誤りを取り除く必要がある。そこで、本実施例では、極めて高い特性をもつことが知られている低密度パリティ検査（ＬＤＰＣ：Low-Density Parity-Check）符号を用いて誤り訂正を行う場合の量子鍵配送について説明する。
【００３８】
図１は、本発明にかかる量子暗号システムにおける通信装置（送信機，受信機）の構成を示す図である。この量子暗号システムは、情報ｘを送信する機能を備えた送信側の通信装置と、伝送路上で雑音等の影響を受けた情報ｘ、すなわち、情報ｙを受信する機能を備えた受信側の通信装置と、を備えている。
【００３９】
また、送信側の通信装置は、量子通信路を介して情報ｘを送信し、さらに公開通信路を介して送受信する情報および盗聴者にもれた情報量（見積もり量）に基づいて暗号鍵（受信側との共通鍵）を生成する暗号鍵生成部１と、暗号化部２１が暗号鍵に基づいて暗号化したデータを、送受信部２２が公開通信路を介してやりとりする通信部２と、を備え、受信側の通信装置は、量子通信路を介して情報ｙを受信し、さらに公開通信路を介して送受信する情報および盗聴者にもれた情報量（見積もり値）に基づいて暗号鍵（送信側との共通鍵）を生成する暗号鍵生成部３と、暗号化部４２が暗号鍵に基づいて暗号化したデータを、送受信部４１が公開通信路を介してやりとりする通信部４と、を備えている。
【００４０】
また、上記暗号鍵生成部１は、パリティ検査行列生成部１０と、乱数発生部１１と、光子生成部１２と、公開通信路通信部１３と、シンドローム生成部１４と、共有鍵生成部１５と、を備え、上記暗号鍵生成部３は、パリティ検査行列生成部３０と、乱数発生部３１と、光子受信部３２と、シンドローム復号部３３と、公開通信路通信部３４と、共有鍵生成部３５と、を備えている。なお、上記暗号鍵生成部１および３において用いる量子状態は、光子の偏光に限定する必要はなく、２準位の量子系であればどのようなものを用いてもよい。
【００４１】
上記送信側の通信装置では、量子通信路上に送信する情報ｘとして、偏光フィルターを用いて所定の方向に偏光させた光（図９参照）を、受信側の通信装置に対して送信する。一方、受信側の通信装置では、水平垂直方向（０°，９０°）の偏光を識別可能な測定器と斜め方向（４５°，１３５°）の偏光を識別可能な測定器とを用いて、量子通信路上の、水平方向（０°）に偏光された光と垂直方向（９０°）に偏光された光と４５°方向に偏光された光と１３５°方向に偏光された光とを識別する。なお、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（０°，９０°）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ５０％の確率でランダムに識別することになる。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。
【００４２】
以下、上記量子暗号システムにおける各通信装置の動作、すなわち、本実施例における量子鍵配送について詳細に説明する。図２は、本実施例の量子鍵配送を示すフローチャートであり、詳細には、図２－１は送信側の通信装置の処理を示し、図２－２は受信側の通信装置の処理を示す。

【００４３】
まず、上記送信側の通信装置および受信側の通信装置では、パリティ検査行列生成部１０，３０が、特定の線形符号のパリティ検査行列Ｈ（ｎ列×ｋ行）を求め、このパリティ検査行列Ｈから「ＨＧ＝０」を満たす生成行列Ｇ（（ｎ－ｋ）列×ｎ行）を求め、さらに、G^{-1}・Ｇ＝Ｉ（単位行列）となるＧの逆行列G^{-1}（ｎ列×（ｎ－ｋ）行）を求める（ステップＳ１，ステップＳ１１）。本実施例では、上記特定の線形符号として、シャノン限界に極めて近い優れた特性をもつＬＤＰＣ符号を用いた場合の量子鍵配送について説明する。なお、本実施例では、誤り訂正方式としてＬＤＰＣ符号を用いることとしたが、これに限らず、たとえば、ターボ符号等の他の線形符号を用いることとしてもよい。また、たとえば、後述する誤り訂正情報（シンドローム）と情報ｘの線形性が確保されるのであれば、どのような行列Ｈを用いてもよい。

【００４４】
ここで、上記パリティ検査行列生成部１０におけるＬＤＰＣ符号の構成法について、詳細には、有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法（図２ステップＳ１の一例）について説明する。図３は、有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法の一例を示すフローチャートである。なお、パリティ検査行列生成部３０については、パリティ検査行列生成部１０と同様の処理を行うのでその説明を省略する。また、本実施例における検査行列生成処理は、たとえば、設定されるパラメータに応じてパリティ検査行列生成部１０で実行する構成としてもよいし、通信装置外部の他の制御装置（計算機等）で実行することとしてもよい。本実施例における検査行列生成処理が通信装置外部で実行される場合は、生成済みの検査行列が通信装置に格納される。以降の実施例では、パリティ検査行列生成部１０で検査行列生成処理を実行する場合について説明する。

【００４５】
まず、パリティ検査行列生成部１０では、「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用の検査行列のベースとなる有限アフィン幾何符号ＡＧ（２，2^s）を選択する（図３、ステップＳ２１）。ここでは、行の重みと列の重みがそれぞれ2^sとなる。図４は、たとえば、有限アフィン幾何符号ＡＧ（２，2^2）のマトリクスを示す図（空白は０を表す）である。つぎに、パリティ検査行列生成部１０では、符号化率ｒａｔｅ（１－シンドローム長／鍵の長さ）を決定する（ステップＳ２２）。

【００４６】
つぎに、パリティ検査行列生成部１０では、ガウス近似法（Gaussian Approximation）による最適化を用いて、符号化率ｒａｔｅに基づく、分割後（ｎ列×ｋ行への分割）の列の重み配分と行の重み配分とを求める（ステップＳ２３）。

【００４７】
最後に、パリティ検査行列生成部１０では、上記で求めた重み配分に基づいて、有限アフィン幾何における行および列を分割して（ステップＳ２４）、ｎ列×ｋ行のパリティ検査行列Ｈを生成する。このとき、本実施例における有限アフィン幾何符号の分割処理は、規則的に分割するのではなく、各行または各列から「１」の番号をランダムに抽出することにより分割する。なお、この抽出処理は、ランダム性が保持されるのであればどのような方法を用いてもよい。

【００４８】
たとえば、ＡＧ（２，2^5）における１列中の「１」の行番号が、
B_l（ｘ）＝{1 32 114 136 149 223 260 382 402 438 467 507 574 579 588 622 634 637 638 676 717 728 790 851 861 879 947 954 971 977 979 998}
の場合、分割後の行列における１～４列目R_m（ｎ）は、B_l（ｘ）から「１」の番号がランダムに抽出され、たとえば、
R_1（ｎ）＝{1 114 574 637 851 879 977 979}
R_2（ｎ）＝{32 136 402 467 588 728 861 971}
R_3（ｎ）＝{149 260 382 438 579 638 717 998}

R_4（ｎ）＝｛223 507 622 634 676 790 947 954｝
となる。
【００４９】
このように、本実施例では、図３に示す上記有限アフィン幾何に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法を実行することによって、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用の検査行列Ｈ（ｎ列×ｋ行）を生成する。
【００５０】
上記のように、パリティ検査行列Ｈ，生成行列Ｇ，G^{-1}（G^{-1}・Ｇ＝Ｉ：単位行列）を生成後、つぎに、送信側の通信装置では、乱数発生部１１が、乱数列（１，０の列：送信データ）を発生し、さらに送信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応したコード，×：斜め方向に偏光された光を識別可能な測定器に対応したコード）をランダムに決定する（ステップＳ２）。一方、受信側の通信装置では、乱数発生部３１が、受信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応したコード，×：斜め方向に偏光された光を識別可能な測定器に対応したコード）をランダムに決定する（ステップＳ１２）。
【００５１】
つぎに、送信側の通信装置では、光子生成部１２が、上記乱数列と送信コードの組み合わせで自動的に決まる偏光方向で光子を送信する（ステップＳ３）。たとえば、０と＋の組み合わせで水平方向に偏光された光を、１と＋の組み合わせで垂直方向に偏光された光を、０と×の組み合わせで４５°方向に偏光された光を、１と×の組み合わせで１３５°方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。
【００５２】
光子生成部１２により生成した光信号を受け取った受信側の通信装置の光子受信部３２では、量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組み合わせによって自動的に決まる受信データを得る（ステップＳ１３）。ここでは、受信データとして、水平方向に偏光された光と＋の組み合わせで０を、垂直方向に偏光された光と＋の組み合わせで１を、４５°方向に偏光された光と×の組み合わせで０を、１３５°方向に偏光された光と×の組み合わせで１を、それぞれ得る。
【００５３】
つぎに、受信側の通信装置では、上記測定が送信側と同一の基底を用いた測定かどうか、すなわち、正しい測定器で行われたものかどうかを調べるために、乱数発生部３１が、上記受信データに対応する受信コード（基底）および光子が検出できなかった位置を、公開通信路を介して送信側の通信装置に対して送信する（ステップＳ１３）。受信コードを受け取った送信側の通信装置では、乱数発生部１１が、受信側にて光子を検出できた位置における測定が正しい測定器で行われたものかどうかを調べ、その調査結果を、公開通信路を介して受信側の通信装置に対して送信する（ステップＳ３）。
【００５４】
そして、受信側の通信装置では、乱数発生部３１が、上記調査結果に基づいて正しい測定器で測定された受信データだけを残し、その他を捨てる（ステップＳ１３）。また、送信側の通信装置においても、乱数発生部１１が、受信側にて正しい測定器で測定された受信データに対応する送信データだけを残し、その他を捨てる（ステップＳ３）。その後、残ったビットの位置の集合：Ｃに対応するデータ（送信データｘ［Ｃ］および受信データｙ［Ｃ］）をメモリ等に保存する（ｙ［Ｃ］は伝送路上で雑音等の影響を受けたｘ［Ｃ］）。
【００５５】
つぎに、受信側の通信装置および送信側の通信装置では、上記送信データｘ［Ｃ］と上記受信データｙ［Ｃ］の一致度をチェックする（ステップＳ４，Ｓ１４）。具体的には、まず、共有鍵生成部１５が、送信データｘ［Ｃ］を読み出し、一致度チェックに用いるビット位置（送信データｘ［Ｃ］のビット位置の集合：Ｃからランダムに抽出したビット位置の部分集合：Ｒ）を、公開通信路を介して受信側の通信装置に対して送信する。なお、

上記部分集合Ｒの公開は、受信側の通信装置で行うこととしてもよい。この時点で、部分集合Ｒが送信側と受信側で共有できている。そして、共有鍵生成部１５では、部分集合Ｒに対応する送信データｘ［Ｃ］の一部分、すなわち、送信データｘ［Ｒ］を、公開通信路を介して受信側の通信装置に対して送信する。

【００５６】

一方、受信側の通信装置の共有鍵生成部３５では、部分集合Ｒに対応する受信データｙ［Ｃ］の一部分、すなわち、受信データｙ［Ｒ］を、公開通信路を介して送信側の通信装置に対して送信する。なお、部分集合：Ｒが公開されているので、残りの部分集合：Ｋ（＝Ｃ－Ｒ）に対応する送信データｘ［Ｋ］および受信データｙ［Ｋ］が共有鍵を生成するためのデータとなる。また、本実施例では、たとえば、部分集合Ｒを大きくとると、一致度チェックの精度は向上するが、鍵長が短くなり、逆に、部分集合：Ｒを小さくとると、一致度チェックの精度は低下するが、鍵長を長くとることができる。

【００５７】

その後、共有鍵生成部１５では、送信データｘ［Ｒ］と受信側から送られてきた受信データｙ［Ｒ］とを比較する。たとえば、部分集合Ｒの個数をn_Rとし（残りのビット位置の集合の個数をn_Kとする）、比較した結果一致しなかったデータ数（エラー数）をn_eとした場合の、受信データｙ［Ｒ］のエラー確率$P_R=n_e/n_R$を求める。一方、共有鍵生成部３５では、受信データｙ［Ｒ］と送信側から送られてきた送信データｘ［Ｒ］とを比較し、上記同様、受信データｙ［Ｒ］のエラー確率$P_R=n_e/n_R$を求める。この時点では、エラー確率P_Rが送信側と受信側で共有できている。

【００５８】

そして、共有鍵生成部１５では、一致度チェックの最終的な結果として、たとえば、上記エラー確率P_Rに基づいて、部分集合Ｋにおけるエラー確率P_Kの推定値P^+を下記（１）式により計算する。ここでは、セキュリティパラメータδ_pを導入した。

$$P^+=P_R+(n_R+n_K)\delta_p/n_K \quad \cdots(1)$$

【００５９】

このとき、エラー確率の推定値P^+が真の値P_Kよりも小さく見積もられてしまう確率$Pr[P^+\leqq P_K]$の上限値ε_pは、セキュリティパラメータδ_pを用いて、下記（２）式で与えられる。なお、下記上限値ε_pは、推定値P^+が真の値P_Kよりも小さく見積もられてしまう確率の上限値となっていればよく、その形は下記（２）式に限定しない。また、以下のε_sについても同様である。

$$\varepsilon_p=\exp(-2n_R(\delta_p)^2)\geqq Pr[P^+\leqq P_K] \quad \cdots(2)$$

【００６０】

なお、エラー推定と誤り訂正を同時に行う場合は、たとえば、適切な線形符号の族を構成し、追加シンドローム処理による適応的な復号を行う。このような場合、P^+およびε_pの計算式を下記（３）式と差し替える。

$$P^+=P_R$$
$$\varepsilon_p=0 \quad \cdots(3)$$

ただし、Ｒ＝Ｋ＝Ｃ、$n_R=n_K$である。

【００６１】

つぎに、送信側の通信装置では、シンドローム生成部１４が、パリティ検査行列Ｈ（ｎ列×ｋ行）と送信データｘ［Ｋ］を用いてｘ［Ｋ］のシンドローム$S_A=Hx[K]$を計算し、その結果を、公開通信路を介して受信側の通信装置に通知する（ステップＳ５）。図５は、シンドローム生成部１４にて生成したS_Aを示す図である。この段階で、ｘ［Ｋ］のシンドロームS_A（ｋビット分の情報）は盗聴者に知られる可能性がある。一方、受信側の通信装置では、公開通信路通信部３４にてｘ［Ｋ］のシンドロームS_Aを受信し、それをシンドローム復号部３３に通知する（ステップＳ１５）。

【００６２】

シンドローム復号部３３では、予め生成しておいたパリティ検査行列Ｈと受信データｙ［Ｋ］を用いてｙ［Ｋ］のシンドローム$S_B=Hy[K]$を計算し、さらに、ｘ［Ｋ］の

シンドロームS$_A$とy［K］のシンドロームS$_B$を用いてシンドロームS＝S$_A$＋S$_B$を計算する。そして、シンドロームSに基づいて送信データx［K］を推定する。すなわち、誤り訂正後の受信データy［K］′を求める（ステップS１６）。ここでは、

y［K］＝x［K］＋e（雑音等）　…（４）

とし、下記（５）式に示すようにシンドロームSを変形した後、シンドローム復号によりeを求め、送信データを推定する。なお、下記（５）式中の＋は排他的論理和を表す。

S＝S$_A$＋S$_B$
＝Hx［K］＋Hy［K］
＝H（x［K］＋y［K］）
＝H（x［K］＋x［K］＋e）
＝He　…（５）

【００６３】

つぎに、受信側の通信装置では、共有鍵生成部３５が、上記ステップS５およびステップS１５の処理で公開された誤り訂正情報（盗聴された可能性のある上記kビット分の情報：S$_A$）に応じて受信データy［K］′の一部を捨てて、（n－k）ビットの長さをもつ受信データy（n－k）′を生成する（ステップS１７）。すなわち、共有鍵生成部３５では、先に計算しておいたG^{-1}（n×（n－k））を用いて下記（６）式により受信データy（n－k）′を生成する。

y（n－k）′＝G^{-1}y［K］′　…（６）

【００６４】

一方、送信側の通信装置においても、共有鍵生成部１５が、公開された誤り訂正情報（盗聴された可能性のある上記kビット分の情報：S$_A$）に応じて送信データx［K］の一部を捨てて、n－kビットの長さを持つ送信データx（n－k）を生成する（ステップS６）。すなわち、共有鍵生成部１５では、先に計算しておいたG^{-1}（n×（n－k））を用いて下記（７）式により送信データx（n－k）を生成する。

x（n－k）＝G^{-1}x［K］　…（７）

【００６５】

つぎに、送信側の通信装置および受信側の通信装置では、それぞれ送信データx（n－k）と受信データy（n－k）′とが一致しているかどうかをチェックする（ステップS７，ステップS１８）。具体的には、まず、共有鍵生成部１５および３５が、セキュリティパラメータ：sを決定する。このセキュリティパラメータs（このステップで公開するビット長に相当）は、システムが要求する安全性に応じて決定される値であり、固定値であれば、両者が予め保存しておき、可変値であれば、その都度どちらか一方が他方に公開することになる。このセキュリティパラメータsが大きい場合には、鍵長が短くなるが安全性が向上し、逆に、小さい場合には、安全性が低下するが鍵長を長くすることができる。

【００６６】

たとえば、どちらか一方の共有鍵生成部が、（n－k）列×s行のランダム行列M$_{PC}$を生成し、そのランダム行列M$_{PC}$を、公開通信路を介して他方の通信装置に送信する。この時点で、ランダム行列M$_{PC}$が送信側と受信側で共有できている。さらに、各共有鍵生成部では、それぞれ、ランダム行列M$_{PC}$から「M$_{PC}$・G（M$_{PC}$）＝０」を満たす（n－k－s）列×（n－k）行の生成行列G（M$_{PC}$）を求め、さらに、G^{-1}（M$_{PC}$）・G（M$_{PC}$）＝I（単位行列）を満たすG（M$_{PC}$）の逆行列G^{-1}（M$_{PC}$）を求める（G^{-1}（M$_{PC}$）は（n－k）列×（n－k－s）行の行列）。

【００６７】

そして、たとえば、共有鍵生成部１５では、「ランダム行列M$_{PC}$×送信データx（n－k）」を計算し、セキュリティパラメータsビット分の情報M$_{PC}$x（n－k）を、公開通信路を介して受信側の通信装置に送信する。図６－１は、情報M$_{PC}$x（n－k）を示す図である。一方、共有鍵生成部３５では、「ランダム行列M$_{PC}$×受信データy（n－k）′」を計算し、セキュリティパラメータsビット分の情報M$_{PC}$y（n－k）′を、公開通信

路を介して送信側の通信装置に送信する。図６－２は、情報$M_{PC}y$（ｎ－ｋ）′を示す図である。

【００６８】

その後、共有鍵生成部１５では、受信側の通信装置から得られた情報$M_{PC}y$（ｎ－ｋ）′と上記計算結果である情報$M_{PC}x$（ｎ－ｋ）とが一致しているかどうかをチェックする。そして、一致している場合は、下記（８）式を計算し、送信データｘ（ｎ－ｋ）を圧縮する。すなわち、圧縮後の（ｎ－ｋ－ｓ）ビットの送信データｘ′を得る。図７－１は、送信データｘ′を示す図である。なお、一致しない場合は、送信データｘ（ｎ－ｋ）を捨てる。

$$x' = G^{-1}(M_{PC})\,x(n-k) \quad \cdots (8)$$

【００６９】

また、共有鍵生成部３５では、送信側の通信装置から得られた情報$M_{PC}x$（ｎ－ｋ）と上記計算結果である情報$M_{PC}y$（ｎ－ｋ）′とが一致しているかどうかをチェックする。そして、一致している場合は、下記（９）式を計算し、受信データｙ（ｎ－ｋ）′を圧縮する。すなわち、圧縮後の（ｎ－ｋ－ｓ）ビットの受信データｙ′を得る。図７－２は、受信データｙ′を示す図である。なお、一致しない場合は、受信データｙ（ｎ－ｋ）′を捨てる。

$$y' = G^{-1}(M_{PC})\,y(n-k)' \quad \cdots (9)$$

【００７０】

また、本実施例においては、上記チェックで一致しているにもかかわらず、誤り訂正後の受信データｙ（ｎ－ｋ）′と送信データｘ（ｎ－ｋ）が一致していない確率ε_cは、

$$\varepsilon_c = 2^{-s} \quad \cdots (10)$$

で表すことができ、ｓが大きい場合には上記確率が下がり、ｓが小さい場合には上記確率が上がる。

【００７１】

つぎに、送信側の通信装置および受信側の通信装置では、量子通信路を通して盗聴者にもれた情報量（の上限値）I_Eを推定する（ステップＳ８，ステップＳ１９）。ここでは、送信側の通信装置と受信側の通信装置の両方で盗聴者にもれた情報量I_E（量子通信路を通してもれた情報量の見積もり値）を計算することとしてもよいし、または、送信側の通信装置でI_Eを計算し、その結果を受信側に公開することとしてもよい。以下では、特に、両方でI_Eを計算する場合について説明する。

【００７２】

送信側の通信装置では、共有鍵生成部１５が、下記のように、前記エラー確率推定値と送信側の通信装置が備える量子状態生成器の特性に関する情報に基づいて、量子通信路を通して盗聴者にもれた情報量を計算する。まず、解析の比較的容易な近似プロトコル（性質のよい量子状態が送信機から出力されるプロトコル）を考え、現実のプロトコルと近似プロトコルの測定結果の差（変動距離）の上限値を計算する。さらに、近似プロトコルにおいて、部分集合Ｋに対応する位置に関して現実とは反対の基底を用いた場合に、エラー確率の推定値が真の値よりも小さく見積もられてしまう確率の上限値を計算する。加えて、部分集合Ｋに対応する位置に関して、送信データを条件とした場合の、受信データおよび盗聴情報の条件付確率の上限値を計算する。これらの値を用いて、最終的に盗聴者にもれた情報量の上限値を計算する。

【００７３】

ここで、量子通信路を通して盗聴者にもれた情報量の計算処理について説明する。まず、実際に送信機から出力される０°，９０°，４５°，１３５°方向に偏光された光子の量子状態（送信機誤差を含む送信状態）をρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}と表す。この量子状態ρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}は予め受信側の通信装置に対して公開しておく。ただし、送信側の通信装置でI_Eを計算し、その結果を受信側に公開する場合には、量子状態ρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}を公開する必要はない。

【００７４】

送信機において、基底０（０°，９０°基底）および１（４５°，１３５°基底）が選択される確率をそれぞれp_b（０），p_b（１）と表す。また、送信機において、データ０および１が選択される確率をそれぞれp_x（０），p_x（１）と表す。送信機が理想的な場合、これら４つの値はすべて１／２となる。

【００７５】

量子状態σ_{00}，σ_{01}，σ_{10}，σ_{11}として、下記（１１）式を満たし、かつ、下記（１２）式中のΔ_0およびΔ_1を最小化するものを選ぶ。ただし、Ｉは２次元ヒルベルト空間上の単位演算子を表す。

$$(\sigma_{00})^2=\sigma_{00},\ (\sigma_{01})^2=\sigma_{01},\ \sigma_{00}+\sigma_{01}=I$$
$$(\sigma_{10})^2=\sigma_{10},\ (\sigma_{11})^2=\sigma_{11},\ \sigma_{10}+\sigma_{11}=I \quad \cdots(11)$$

$$\Delta_0=d((1/2)\rho_{00}-(1/2)\sigma_{00})+d((1/2)\rho_{01}-(1/2)\sigma_{01})$$

$$\Delta_1=d((1/2)\rho_{10}-(1/2)\sigma_{10})+d((1/2)\rho_{11}-(1/2)\sigma_{11})$$

$$\cdots(12)$$

なお、上記（１１）式における$d(A)$は、演算子Ａのトレースノルムを表している。すなわち、$d(A)$は下記（１３）式で計算する。ただし、上付き文字の＊は複素共役転置を表す。

$$d(A)=Tr(\sqrt{(A^*A)}) \quad \cdots(13)$$

【００７６】

部分集合Ｋにおいて用いられた基底に対応するn_Kビットの乱数をａと表す。上記Δ_0およびΔ_1を用いて、量子状態ρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}の代わりに量子状態σ_{00}，σ_{01}，σ_{10}，σ_{11}を用いた場合の測定結果の差（変動距離）の上限値ε_Kを下記（１４）式で計算する。ただし、n_0は、ａの中の０の数、n_1は、ａの中の１の数を表す。また、ΔＫはビット列ｘ［Ｋ］を生成する確率分布p_X（ｘ［Ｋ］）と一様分布との変動距離の上限値を表す。

$$\varepsilon_K=n_0\Delta_0+n_1\Delta_1+\Delta_K \quad \cdots(14)$$

【００７７】

前記ビット列ａをビットごとに反転させたものをａ´と表す。確率分布p_bにしたがってビット列ａが生成される確率をp_b（ａ）、ビット列ａ´が生成される確率をp_b（ａ´）と表す。量子状態ρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}の代わりに量子状態σ_{00}，σ_{01}，σ_{10}，σ_{11}を用い、さらに、基底ａの代わりに反転基底ａ´を用いた場合に、対応するエラー確率の推定値P^+が真の値P_Kよりも小さく見積もられてしまう確率の上限値ω_Kを、下記（１５）式により計算する。

$$\omega_K=2\varepsilon_K p_b(a)/p_b(a') \quad \cdots(15)$$

【００７８】

また、送信機から出力される基底０（０°，９０°基底）に対応する平均量子状態ρ_0、および基底１（４５°，１３５°基底）に対応する平均量子状態ρ_1を、下記（１６）式および（１７）式により計算する。

$$\rho_0=p_x(0)\rho_{00}+p_x(1)\rho_{01} \quad \cdots(16)$$
$$\rho_1=p_x(0)\rho_{10}+p_x(1)\rho_{11} \quad \cdots(17)$$

【００７９】

さらに、量子状態σ_{00}，σ_{01}，σ_{10}，σ_{11}によって定まるパラメータｑを下記（１８）式により計算する。

$$q=max\{Tr\sigma_{00}\sigma_{10},\ Tr\sigma_{00}\sigma_{11}\} \quad \cdots(18)$$

これを用いて、部分集合Ｋに対応する位置に関して、送信データを条件とした場合の、受信データおよび盗聴情報の条件付確率の上限値π_Kを下記（１９）式により計算する。

$$\pi_K=2^{nK(h(P+)+\log(q))} \quad \cdots(19)$$

ただし、上記（１９）式の中のｌｏｇは底が２の対数関数を表し、ｈ（ｐ）は、下記（２０）式で計算する。

$$h(p)=-p\log(p)-(1-p)\log(1-p) \quad \cdots(20)$$

【００８０】

量子状態σ_{00}，σ_{01}，σ_{10}，σ_{11}を用いたと仮定した場合の盗聴者にもれる盗聴量I_Qを下記（２０）式により計算する。ただし、ｃは０より大きな実数で、下記（２１）式ができるだけ小さくなるものを選ぶものとする。

$$I_Q=n_K+(1-1/c)(\log(\pi_K)-2\log(1-(\sqrt{(c\omega_K)})))) \quad \cdots(21)$$

【００８１】

さらに、量子状態ρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}を用いた現実の状況において盗聴者にもれる盗聴量I_Eを下記（２２）式により計算する。

$$I_E=I_Q+\varepsilon_K(3n_K-2\log\varepsilon_K) \quad \cdots(22)$$

【００８２】

上記（２２）式は、近似プロトコルにおいて盗聴者に漏れる盗聴量をI_Qとした場合の、現実のプロトコルにおける盗聴量の上限になっていればよく、上記の形に限定しない。

【００８３】

現実の実装においては、送信機の特性が確率１で特定できるとは限らない。たとえば、送信機が常に単一光子を出力できるとは限らない。そこで、送信機の特性を表すパラメータの組ρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}，$p_b(0)$，$p_b(1)$，$p_x(0)$，$p_x(1)$に注目し、$1-e_s$以上の確率でこれらのパラメータの組が集合Ｓに含まれる状況を想定する。ここで、セキュリティパラメータδ_sを用いて、パラメータe^+を下記（２４）式により計算する。

$$e^+=e_s+\delta_s \quad \cdots(24)$$

このとき、部分集合Ｋにおいて、送信機が想定外の状態を送信してしまう回数n_sが、$n^+=e^+n_K$よりも小さくなってしまう確率の上限ε_sは、下記（２５）式で計算できる。

$$\varepsilon_s=\exp(-2n_K(\delta_s)^2)\geqq Pr[n^+\leqq n_s] \quad \cdots(25)$$

【００８４】

部分集合Ｋにおいて、送信機が想定外の状態を送信してしまう回数が、上記n^+であると仮定する。このとき、部分集合Ｋにおいて送信機が想定どおりの状態を送信している位置に相当する部分集合をＬとする。部分集合Ｌの長さは$n_L=n_K-n^+$である。さらに、部分集合Ｌにおいて用いられた基底に対応するn_Lビットの乱数をa_Lと表し、これをビット毎に反転させたものをa_L'を表す。（１４）式のε_Kと同様に、ε_Lを下記（２６）式により計算する。ただし、m_0は、a_Lの中の０の数、m_1は、a_Lの中の１の数を表す。また、ΔＬは部分集合Ｌにおけるビット列ｘ［Ｌ］を生成する確率分布p_X（ｘ［Ｌ］）と一様分布との変動距離の上限値を表す。

$$\varepsilon_L=m_0\Delta_0+m_1\Delta_1+\Delta_L \quad \cdots(26)$$

【００８５】

（１５）式および（１９）式の代わりに、ω_Lおよびπ_Lを下記（２７）式および（２８）式により計算する。ただし、max_Lは、長さn_Lを固定した状況における、部分集合Ｌに関する最大化を表す。

$$\omega_L=max_L\{2\varepsilon_L p_b(a_L)/p_b(a_L')\} \quad \cdots(27)$$

$$\pi_L=2^{nL(h((nK/nL)P+)+\log(q))} \quad \cdots(28)$$

なお、上記Ｌに関する最大化の計算が困難な場合は、最大値の代わりに上限値を用いることとしてもよい。また、上記（２８）式の中の関数ｈへの入力「$(n_K/n_L)P^+$」に関しては、部分集合Ｌにおけるエラー確率の上限値になっていればよく、上記の形に限定しない。たとえば、部分集合Ｋにおけるエラーの発生が、送信機が想定どおりに動作するか否かと独立な場合は、入力を「$P_R+(n_R/n_L)\delta_P/n_L$」で置き換えてもよい。

【００８６】

（２１）式および（２２）式の代わりに、I_Q'およびI_E'を下記（２９）式および（３０）式により計算する。

$$I_Q'=n_L+(1-1/c)(\log(\pi_L)-2\log(1-(\sqrt{(c\omega_L)})))$$

…（２９）

$I_E' = I_Q' + \varepsilon_L(3n_L - 2\log\varepsilon_L)$ …（３０）

なお、上記（３０）式は、部分集合Ｌに関して、近似プロトコルの盗聴量の上限値がI_Q'であるときの現実のプロトコルにおける盗聴量の上限になっていればよく、上記の形に限定しない。

【００８７】

さらに、盗聴者にもれる盗聴量I_Eを下記（３１）式により計算する。ただし、$I_M' = n^+$である。

$I_E = I_E' + I_M'$ …（３１）

なお、I_M'は想定外の送信量子状態から盗聴者が得ることのできる情報量の上限になっていればよい。

【００８８】

最後に、上記（３１）式の盗聴量I_Eを集合Ｓに関して最大化し、得られた最大値を求める盗聴量とする。なお、上記Ｓに関する最大化の計算が困難な場合は、最大値の代わりに上限値を用いることとしてもよい。

【００８９】

つぎに、前記エラー確率推定値と送信側の通信装置が備える量子状態生成器および受信側の通信装置が備える量子状態測定器の特性に関する情報に基づいて、量子通信路を通して盗聴者にもれた情報量を推定する場合について、以下に記す。まず、受信機が行う０°，９０°，４５°，１３５°方向の測定（受信機誤差を含む測定）に対応する演算子をE_{00}，E_{01}，E_{10}，E_{11}と表す。また、送信機から出力される基底０に対応する平均量子状態および基底１に対応する平均量子状態の完全混合状態からの差異のトレースノルムの上限を、それぞれ∇_0および∇_1と表す。すなわち、∇_0および∇_1に関して、下記（３２）式および（３３）式が成り立っているものとする。

$d(\rho_0 - (1/2)I) \leqq \nabla_0$ …（３２）

$d(\rho_1 - (1/2)I) \leqq \nabla_1$ …（３３）

【００９０】

さらに、測定に対応する演算子F_{00}，F_{01}，F_{10}，F_{11}として、下記（３４）式を満たし、かつ、下記（３５）式中のΔ_0およびΔ_1を最小化するものを選ぶ。ただし、Ｉは２次元ヒルベルト空間上の単位演算子を表す。

$(F_{00})^2 = F_{00}$，$(F_{01})^2 = F_{01}$，$F_{00} + F_{01} = I$

$(F_{10})^2 = F_{10}$，$(F_{11})^2 = F_{11}$，$F_{10} + F_{11} = I$ …（３４）

$\Delta_0 = d((1/2)E_{00} - (1/2)F_{00}) + d((1/2)E_{01} - (1/2)F_{01})$

$\Delta_1 = d((1/2)E_{10} - (1/2)F_{10}) + d((1/2)E_{11} - (1/2)F_{11})$

…（３５）

【００９１】

特に、上記Δ_0およびΔ_1が０の場合は、前記∇_0および∇_1として、下記（３６）式を満たすΔ_pを用いることができる。すなわち、$\Delta_0 = \Delta_1 = 0$の場合は、下記（３６）式中のΔ_pを用いて、$\nabla_0 = \nabla_1 = \Delta_p$とすることができる。

$d(\rho_0 - \rho_1) \leqq \Delta_p$ …（３６）

【００９２】

（１４）式、（１８）式および（２６）式の代わりに、ε_K、ｑおよびε_Lを、下記（３７）式、（３８）式および（３９）式により計算する。

$\varepsilon_K = n_0(\Delta_0 + \nabla_0) + n_1(\Delta_1 + \nabla_1) + \Delta_K$ …（３７）

$q = \max\{\mathrm{Tr}F_{00}F_{10}, \mathrm{Tr}F_{00}F_{11}\}$ …（３８）

$\varepsilon_L = m_0(\Delta_0 + \nabla_0) + m_1(\Delta_1 + \nabla_1) + \Delta_L$ …（３９）

上記ε_K、ｑおよびε_Lを用いて、（２２）式もしくは（３１）式と同様に盗聴量I_Eを計算する。

【００９３】
一般に、誤り訂正の特性は、符号長（本実施例においてはn_K）が長ければ長いほどよい。一方、盗聴量I_Eは、必ずしもn_Kが長ければよいというわけではない。そこで、誤り訂正のための符号長と盗聴量I_Eの推定のためのビット列の長さを変えることによって、より特性の高い量子鍵配送法を構成できる。すなわち、部分集合Ｋを所定の数に分割し、分割された部分集合それぞれに対して盗聴量I_Eを計算するものとする。ここで、分割数は、各分割部分集合に対する盗聴量I_Eの合計ができるだけ小さくなるように選ぶ。
【００９４】
なお、本実施例では、受信側の通信装置においても、上記と同様の処理で盗聴者にもれた情報量I_Eを計算する。
【００９５】
つぎに、送信側の通信装置および受信側の通信装置では、上記ステップＳ８およびステップＳ１９の処理で計算した情報量I_Eに基づいて、送信データｘ´および受信データｙ´の一部を捨てて、（ｎ－ｋ－ｓ－Ｔ－ｖ）ビット分の情報量を備えた暗号鍵ｒを生成する（ステップＳ９，ステップＳ２０）。なお、共有鍵生成部１５および３５は、上記情報量I_Eのマージンとして、セキュリティパラメータ：ｖを決定する。このセキュリティパラメータｖは、システムが要求する安全性に応じて決定される値である。このセキュリティパラメータｖが大きい場合には、鍵長が短くなるが安全性が向上し、逆に、小さい場合には、安全性が低下するが鍵長を長くすることができる。また、上記Ｔは、上記で求めた盗聴者にもれた情報量I_E以上の整数で最小のものを表す。
【００９６】
具体的には、たとえば、共有鍵生成部１５が、$\{0,1\}^{n-k-s} \rightarrow \{0,1\}^{n-k-s-T-v}$となるユニバーサル・ハッシュ関数の族からランダムに元H_uを選ぶ。これは、たとえば、H_uとしてフルランク（ｒａｎｋ（H_u）＝ｎ－ｋ－ｓ－Ｔ－ｖ）のランダム行列をとってくることにより実現できる。そして、ハッシュ関数H_uを、受信側の通信装置に対して公開通信路を介して送信する。なお、この処理は、受信側の通信装置の共有鍵生成部３５にて行うこととしてもよい。
【００９７】
そして、共有鍵生成部１５では、上記H_uを用いて下記（４０）式により暗号鍵ｒを生成する。図８－１は、共有鍵生成部１５にて生成した暗号鍵ｒを示す図である。送信側の通信装置は、この暗号鍵ｒを受信側の通信装置との共有鍵とする。

$$r = H_u x' \quad \cdots (40)$$

【００９８】
一方、共有鍵生成部３５では、上記Ｈｕを用いて下記（４１）式により暗号鍵ｒを生成する。図８－２は、共有鍵生成部３５にて生成した暗号鍵ｒを示す図である。受信側の通信装置は、この暗号鍵ｒを送信側の通信装置との共有鍵とする。

$$r = H_u y' \quad \cdots (41)$$

【００９９】
なお、上記では、ステップＳ６，Ｓ１７による圧縮およびステップＳ９，Ｓ２０による圧縮を個別に行っているが、これに限らず、たとえば、$\{0,1\}^{n-k-s} \rightarrow \{0,1\}^{n-k-s-T-v-k}$となるランダム行列$H_u$を生成し、その後、上記（４０）式および（４１）式を実行することとしてもよい。
【０１００】
このように、本実施例おいては、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正しつつ、上記ステップＳ４およびＳ１４、ステップＳ７およびＳ１８、ステップＳ８およびＳ１９、を実行し、さらに、上記処理の過程で公開通信路を介して公開した情報量および量子通信路を通して盗聴者にもれた情報量の推定値に応じてデータを圧縮し、圧縮後のデータを装置間で共有の暗号鍵とすることとした。これにより、高度に安全性の保証された共通鍵を効率良く生成することができる。すなわち、成功確率が（$1-\varepsilon_p$）（$1-\varepsilon_s$）（$1-\varepsilon_c$）以

上で、かつ盗聴者にもれる情報量が（2^{-v}／ｌｎ２）以下の、量子鍵配送方法が実現できる。ただし、想定外の送信状態を考えない場合は、$\varepsilon_s=0$とする。

【実施例２】

【０１０１】

つづいて、実施例２について説明する。実施例２では、用いる量子状態を２準位系に限定せず、受信側の通信装置の観測値として「０」，「１」の他に「非検出」という結果もありうる状況を考える。そこで、全送信データをｘ［Ａ］とし、そのうち、受信側で検出できたデータ部分をｘ［Ｄ］とする。ｘ［Ｃ］，ｘ［Ｒ］，ｘ［Ｋ］は、これまでと同様とする。送信側の通信装置および受信側の通信装置では、量子通信路を通して盗聴者にもれた情報を考慮した上での鍵（送信データｘ［Ｋ］）の持つ情報量（の下限値）R_xを推定する（ステップＳ８，ステップＳ１９に相当）。ここでは、送信側の通信装置と受信側の通信装置の両方で鍵の持つ情報量R_xを計算することとしてもよいし、または、送信側の通信装置でR_xを計算し、その結果を受信側に公開することとしてもよい。以下では、特に、両方でR_xを計算する場合について説明する。

【０１０２】

実際に送信機から出力される０°，９０°，４５°，１３５°方向に偏光された光子の量子状態（送信機誤差を含む送信状態）をρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}と表す。ここで、各量子状態はヒルベルト空間Ｈ上の密度演算子になっているものとする。また、各量子状態は、それぞれ確率p_{00}，p_{01}，p_{10}，p_{11}で出力されるものとする。この量子状態ρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}は、予め受信側の通信装置に対して公開しておく。ただし、送信側の通信装置でR_xを計算し、その結果を受信側に公開する場合には、これらの値を公開する必要はない。

【０１０３】

送信側の通信装置では、量子状態ρ_{ij}（ｉ，ｊは０もしくは１）を下記（４２）式のように分解する。

$$\rho_{ij}=p_{ij}^{(0)}\rho_{ij}^{(0)}+p_{ij}^{(1)}\rho_{ij}^{(1)} \quad \cdots(42)$$

ただし、$\rho_{ij}^{(0)}$，$\rho_{ij}^{(1)}$はヒルベルト空間Ｈ上の密度演算子であり、下記（４３）式をみたすものとする。

$$0<p^{(0)}\leqq \min\{p_{ij}\},\ p_{ij}^{(0)}=p^{(0)}/p_{ij},\ p_{ij}^{(0)}+p_{ij}^{(1)}=1 \quad \cdots(43)$$

【０１０４】

この分解は、鍵のもつ情報量（レニーエントロピー）R_xができるだけ大きく、あるいは、最終的な（圧縮後の）鍵のもつ情報量（相互情報量）ができるだけ小さく見積もれるように決定する。たとえば、$\rho_{ij}^{(0)}$はできるだけ２準位の量子状態に近く、$p_{ij}^{(0)}$はできるだけ大きくなるように選ぶと、一般にR_xを大きく見積もることができる。以下、送信機は、確率$p_{ij}^{(0)}$で$\rho_{ij}^{(0)}$を出力し、確率$p_{ij}^{(1)}$で$\rho_{ij}^{(1)}$を出力するものと考える。

【０１０５】

Ｘ，Ｙは、００，０１，１０，１１の４つの値をとるものとする。上記量子状態$\rho_x^{(0)}$のスペクトル分解を、

$$\rho_x^{(0)}=\Sigma_{kX}\lambda_X(k_X)\,|k_X\rangle\langle k_X| \quad \cdots(44)$$

とし、μ_{XY}を集合$\{k_X\}$から集合$\{k_Y\}$への写像とする。

【０１０６】

さらに、$|\phi_{kX}\rangle$を適当なヒルベルト空間の元とする。ここで、４行４列のグラム行列Ｇを下記（４５）式により計算する。

$$G_{XY}=\Sigma_{kX}\langle k_X|k_{XY}\rangle\langle\phi_{kX}|\phi_{kXY}\rangle\sqrt{(\lambda_X(k_X)\lambda_Y(k_{XY}))} \quad \cdots(45)$$

ただし、$k_{XY}=\mu_{XY}(k_X)$である。μ_{XY}および$|\phi_{kX}\rangle$は、鍵のもつ情報量R_xができるだけ大きく見積もれるように選ぶ。

【０１０７】
グラム行列Ｇは、半正定値であるから４次の正方行列Ｃが存在して下記（４６）式が成り立つ。
$$G = C^{*}C \qquad \cdots (46)$$
【０１０８】
さらに、Ｇの対角成分は１であるから、行列Ｃの列ベクトルは４次元ヒルベルト空間H_4上の長さ１の元とみなすことができる。そこで、H_4上の量子状態σ_X'（Ｘ＝００，０１，１０または１１）を下記（４７）式により定義する。
$$\sigma_X' = |C_X\rangle\langle C_X| \qquad \cdots (47)$$
ただし、C_Xは行列Ｃの第Ｘ列を表すものとする。このσ_X'の構成法より、σ_X'から$\rho_X^{(0)}$への完全正写像の存在が保証される。そこで、以下、$\rho_X^{(0)}$の代わりにσ_X'が出力されるものと考える。
【０１０９】
４次元ヒルベルト空間H_4の２次元部分ヒルベルト空間をH_2とする。σ_X（Ｘ＝００，０１，１０または１１）をヒルベルト空間H_2上の量子状態で下記（４８）式を満たすものとする。ただし、Ｉはヒルベルト空間H_2上の単位演算子を表す。
$$\sigma_{00}+\sigma_{01}=I,\ \sigma_{10}+\sigma_{11}=I \qquad \cdots (48)$$
【０１１０】
ヒルベルト空間H_2および量子状態σ_Xは、下記（４９）式で定義されるΔ_X（Ｘ＝００，０１，１０または１１）あるいはその上限を最小化するものを選ぶ。ただし、ｄ（ρ，σ）はρとσのトレース距離をあらわすものとする。
$$\Delta_X = d(\sigma_X', \sigma_X) \qquad \cdots (49)$$
なお、上式ではトレース距離を最小化することを考えたが、信頼度（フィデリティ）を最大化するものとしてもよい。また、たとえば$\rho_X=\Sigma_k(\mu^k/k!)\exp(-\mu)|k;X\rangle\langle k;X|$（ｋは自然数）で与えられるとき、前記パラメータは下記（５０）式のように選ぶことができる。
$$\rho_X^{(0)}=\sigma_X'=\sigma_X=|1;X\rangle\langle 1;X|$$
$$p_X^{(0)}=\mu\exp(-\mu)$$
$$\mu_{XY}(|k;X\rangle\langle k;X|)=|k;Y\rangle\langle k;Y|$$
$$|\phi_{kX}\rangle=|\phi\rangle \qquad \cdots (50)$$
【０１１１】
部分Ｋのうち、$\rho_{ij}^{(0)}$が出力されている部分をＬ、$\rho_{ij}^{(1)}$が出力されている部分をＭ、とする。部分Ｍの長さの上限値n_{M+}、部分Ｍのもつ情報量（の下限値）$R^{m}{}_{x[M]}$を見積もり、これらの見積もりが誤ってしまう確率（の上限値）ε_Eを計算する。この計算は、たとえば、以下のようにして行うことができる。
【０１１２】
まず、δ^{i}_{M}（ｉ＝０，１）を適当な正数とし、部分Ｍの長さの上限値n^{i}_{M+}（ｉ＝０，１）を下記（５１）式により見積もる。
$$p_i^{(1)}=(p_{i0}p_{i0}^{(1)}+p_{i1}p_{i1}^{(1)})/(p_{i0}+p_{i1})$$
$$p^{i}_{M}=((n^{i}_{M}/n^{i}_{A})-\delta^{i}_{M})/(p_i^{(1)}n^{i}_{K}/n^{i}_{D})$$
$$n^{i}_{M+}=\max_M\{n^{i}_{M}\} \qquad \cdots (51)$$
ただし、n^{i}_{K}（ｉ＝０，１）はａ［Ｋ］におけるｉ（＝０もしくは１）の数を表す。n^{i}_{A}，n^{i}_{D}，n^{i}_{M}も同様とする。なお、$\max_M$は$p^{i}_{M}\leqq 1$という条件のもとで、Ｍに関して最大化するものとする。また、受信者が攻撃者に取り込まれてしまっているような場合も想定して、前記（５１）式中のn^{i}_{D}をn^{i}_{C}で置き換えることによって、さらに強い安全性を保証することが可能となる。
【０１１３】
この見積もりが誤ってしまう確率の上限値を、下記（５２）式で計算する。なお、下記上限値ε^{i}_{M}は、この見積もりが誤ってしまう確率の上限値となっていればよく、その形は下式に限定しない。

$\varepsilon_E = \varepsilon^0_M + \varepsilon^1_M$
$\varepsilon^i_M = n^i_A \exp(-n^i_A D(B(n^i_M/n^i_A) \mid (B(n^i_M/n^i_A - \delta^i_M))))$
…（５２）

ただし、ｅｘｐは２のべき乗関数、Ｄは相対エントロピー、Ｂはベルヌーイ分布を表している。

【０１１４】

T_{ij}（ｉ，ｊは０もしくは１）をヒルベルト空間Ｈ上の演算子で、下記（５３）式を満たすものとする。ただし、Ｉはヒルベルト空間Ｈ上の単位演算子を表す。

$0 \leqq T_{ij},\ T_{i0} + T_{i1} \leqq I$ …（５３）

これにより、T_{ij}は部分Ｍにおいて基底がｉ（＝０もしくは１）の場合に、送信量子状態が$\rho_{i0}^{(1)}$であるか$\rho_{i1}^{(1)}$であるかを識別するための測定演算子と考えることができる。この識別が成功する確率の最大値s^i_Mを下記（５４）式で計算する。

$p_{ij}^{(M)} = p_{ij} p_{ij}^{(1)} / (p_{i0} p_{i0}^{(1)} + p_{i1} p_{i1}^{(1)})$
$s^i_{M,} = \sup_T \{ (\Sigma_j Trp_{ij}^{(M)} \rho_{ij}^{(1)} T_{ij}) / (\Sigma_{k,l} Trp_{ik}^{(M)} \rho_{ik}^{(1)} T_{il}) \}$
…（５４）

ただし、$\sup_T$は下記（５５）式を満たすという条件のもとでＴに関して最大化するものとする。

$(\Sigma_{jl} Trp_{ij}^{(M)} \rho_{ij}^{(1)} T_{il}) \geqq p^i_M$ …（５５）

【０１１５】

部分Ｍのもつ情報量の下限値$R_{x[M]}$を下記（５６）式により計算する。

$R^m_{x[M]} = -n^0_M \log s^0_M - n^1_M \log s^1_M$ …（５６）

【０１１６】

つぎに、部分Ｌのもつ情報量（レニー・エントロピー）を見積もる。そのために、まず、部分Ｌにおけるエラー確率を推定する。δ_pをセキュリティパラメータとし、推定値P^+として下記（５７）式を用いる。

$P^+ = (n_K P_R + n_C \delta_p - n^0_M (1 - s^0_M) - n^1_M (1 - s^1_M)) / n_L$ …（５７）

【０１１７】

このとき、エラー確率の推定値P^+が真の値P_Lよりも小さく見積もられてしまう確率$Pr[P_L > P^+]$の上限値ε_pは、下記（５８）式で与えられる。なお、下記上限値ε_pは、推定値P^+が真の値P_Lよりも小さく見積もられてしまう確率の上限値となっていればよく、その形は下式に限定しない。

$\varepsilon_p = n_R \exp(-n_R D(B(P_R) \mid (B(P_R + \delta_p)))) \geqq Pr[P_L > P^+]$
…（５８）

【０１１８】

量子状態σ_X'の代わりに量子状態σ_Xを用いる近似プロトコルを考える。この近似プロトコルにおいて、部分Ｌのもつ情報量を見積もる。そのため、まず部分Ｌにおいて基底ａ［Ｌ］の代わりにその反転基底ａ~［Ｌ］を用いた場合に、上記推定値P^+が真の値P_Kよりも小さく見積もられてしまう確率を見積もる。いま、σ_0'およびσ_1'を下記（５９）式で与えられる基底に関する平均量子状態とする。

$\sigma_0' = (\sigma_{00}' + \sigma_{01}') / 2$
$\sigma_1' = (\sigma_{10}' + \sigma_{11}') / 2$ …（５９）

【０１１９】

さらに、υを基底ａ［Ｌ］に対応する平均量子状態$\sigma_{a[L]}'$と反転基底ａ~［Ｌ］に対応する平均量子状態$\sigma_{a\sim[L]}'$の間のトレース距離の上限値とする。すなわち、υは下記（６０）式を満たすものとする。

$d(\sigma_{a[L]}', \sigma_{a\sim[L]}') \leqq \upsilon$ …（６０）

【０１２０】

これを用いて、上記推定値P^+が真の値P_Kよりも小さく見積もられてしまう確率の上限値は下記（６１）式のように計算できる。

$$Pr[P_L > P^+] \leqq \varepsilon_p + \varepsilon_E + \upsilon \quad \cdots(61)$$

【0121】

正規プロトコルにおいて送信，受信，盗聴情報の従う確率分布と、近似プロトコルにおいて送信，受信，盗聴情報の従う確率分布と、の変動距離を見積もる。そのため、下記（62）式をみたす上限値τを計算する。

$$\Sigma_{x[L]} (1/2^{nL}) d(\sigma_{a\sim[L],x[L]}', \sigma_{a\sim[L],x[L]}) \leqq \tau \quad \cdots(62)$$

【0122】

上限値τは、たとえば、fを量子状態の間の信頼度（フィデリティ）とするとき、下記（63）式により計算することができる。

$$f_X = f(\sigma_X', \sigma_X)$$
$$f_0 = \min\{f_{00}, f_{01}\}$$
$$f_1 = \min\{f_{10}, f_{11}\}$$
$$\tau = \sqrt{(1-(f_0)^{2n0}(f_1)^{2n1})} \quad \cdots(63)$$

ただし、n_0，n_1は、ビット列a~［L］における0の数、1の数をそれぞれ表している。

【0123】

近似プロトコルにおいて、反転基底a~［L］を用いた場合に上記推定値P^+が真の値P_Kよりも小さく見積もられてしまう確率の上限値は、下記（64）式のように計算できる。

$$Pr[P^+ \leqq P_K] \leqq \varepsilon_p + \varepsilon_E + \upsilon + \tau \quad \cdots(64)$$

【0124】

つぎに、ヒルベルト空間H_2上の射影演算子P_{00}，P_{01}，P_{10}，P_{11}を下記（65）式により計算する。

$$P_{00} = \{\sigma_{00} - \sigma_{01} > 0\}$$
$$P_{01} = \{\sigma_{01} - \sigma_{00} > 0\}$$
$$P_{10} = \{\sigma_{10} - \sigma_{11} > 0\}$$
$$P_{11} = \{\sigma_{11} - \sigma_{10} > 0\} \quad \cdots(65)$$

【0125】

さらに、量子状態σ_{00}およびσ_{01}の識別に成功する確率の最大値s_0，量子状態σ_{10}およびσ_{11}の識別に成功する確率の最大値s_1を下記（66）式により計算する。

$$s_0 = 1/2 + d(\sigma_{00}, \sigma_{01})$$
$$s_1 = 1/2 + d(\sigma_{10}, \sigma_{11}) \quad \cdots(66)$$

【0126】

いま、量子状態$\sigma_{a\sim[L],x[L]}$が与えられ、x［L］を上記射影演算子を用いて推定することを考える。推定値（x［L］に対応するビット列）にkビットの誤りを許すことにした場合の推定誤り確率の上限値をε_kとする。ε_kは、たとえば、下記（67）式により計算することができる。

$$\varepsilon_k = (2^{nL} - 2^{nLh(k/nL)}/2/\sqrt{n_L})(s_0)^{n0}(s_1)^{n1}((1-s_m)/s_m)^k$$
$$s_m = \min\{s_0, s_1\} \quad \cdots(67)$$

【0127】

これらの値を用いて、パラメータω_Lを下記（68）式により計算する。

$$\omega_L = \varepsilon_p + \upsilon + \tau + \varepsilon_k 2^{nLh(P+)} \quad \cdots(68)$$

【0128】

もし、s_mが0の場合は、下記（69）式の値を用いて以下の計算を行う。

$$\omega_L = \varepsilon_p + \varepsilon_E + \upsilon + \tau$$
$$k = 0 \quad \cdots(69)$$

【0129】

パラメータq_0，q_1を下記（70）式により計算する。

$$q_0 = \max\{Tr\sigma_{00}P_{10}, Tr\sigma_{00}P_{11}, Tr\sigma_{01}P_{10}, Tr\sigma_{01}P_{11}\}$$
$$q_1 = \max\{Tr\sigma_{10}P_{00}, Tr\sigma_{10}P_{01}, Tr\sigma_{11}P_{00}, Tr\sigma_{11}P_{01}\} \quad \cdots($$

７０）

【０１３０】

これを用いて、パラメータπ_Lを下記（７１）式により計算する。

$$\pi_L = 2^{nLh(P^*)+n0\log(q0)+n1\log(q1))}$$

$$P^* = P^+ + (k/n_L) \quad \cdots (71)$$

【０１３１】

ｃを正数とすれば、反対基底を用いた場合の受信データおよび盗聴情報を条件とした場合の送信データの条件付確率$p_{x|yz}$に関して、マルコフの不等式より下記（７２）式が成り立つ。

$$Pr[p_{x|yz} > \Pi_L] \leqq (1/c)$$

$$\Pi_L = \pi_L / (1 - \sqrt{(c\omega_L)})^2 \quad \cdots (72)$$

ここで正数ｃは、鍵のもつ情報量（レニーエントロピー）R_xができるだけ大きく、あるいは、最終的な（圧縮後の）鍵のもつ情報量（相互情報量）ができるだけ小さく見積もれるように決定する。

【０１３２】

前記（６２）式および（７２）式を用いて、適当に$R^m_{x[L]}$およびε_Lを選ぶことによって、部分Ｌのもつ情報量$R_{x[L]}$に関する下記（７３）式の形の条件式を導出する。

$$Pr[R_{x[L]} > R^m_{x[L]}] \leqq \varepsilon_L \quad \cdots (73)$$

たとえば、$\tau = 0$の場合、$R^m_{x[L]}$およびε_Lは下記（７４）式のようにとることができる。

$$R^m_{x[L]} = -\log \Pi_L$$

$$\varepsilon_L = 1/c \quad \cdots (74)$$

【０１３３】

さらに、部分Ｋのもつ情報量の下限値を下記（７５）式により計算する。

$$R_x = R_{x[K]} = \min_M (R^m_{x[L]} + R^m_{x[M]}) \quad \cdots (75)$$

ただし、$\min_M$は$n^i_M \leqq n^i_{M+}$（ｉ＝０，１）という条件のもとでＭに関して最小化するものとする。

【０１３４】

つぎに、受信機側の装置の特性を用いて鍵の持つ情報量R_xを計算する手順を示す（ステップＳ８，ステップＳ１９に相当）。実際に送信機から出力される０°，９０°，４５°，１３５°方向に偏光された光子の量子状態（送信機誤差を含む送信状態）をρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}と表す。また、各量子状態は、それぞれ確率p_{00}，p_{01}，p_{10}，p_{11}で出力されるものとする。さらに、実際に受信機が行う０°，９０°，４５°，１３５°方向の測定（受信機誤差を含む測定）に対応する演算子をE_{00}，E_{01}，E_{10}，E_{11}と表す。ここで、各演算子は、ヒルベルト空間Ｈ上の密度演算子になっているものとする。この演算子E_{00}，E_{01}，E_{10}，E_{11}は、予め送信側の通信装置に対して公開しておく。また、量子状態ρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}は、予め受信側の通信装置に対して公開しておく。ただし、送信側の通信装置でR_xを計算し、その結果を受信側に公開する場合には、これらの値（量子状態）を公開する必要はない。

【０１３５】

送信側の通信装置では、量子状態ρ_{ij}（ｉ，ｊは０もしくは１）を下記（７６）式のように分解する。

$$\rho_{ij} = p_{ij}^{(0)} \rho_{ij}^{(0)} + p_{ij}^{(1)} \rho_{ij}^{(1)} \quad \cdots (76)$$

ただし、$\rho_{ij}^{(0)}$，$\rho_{ij}^{(1)}$はヒルベルト空間Ｈ上の密度演算子であり、下記（７７）式をみたすものとする。ただし、ヒルベルト空間Ｈに対して、Ｓ（Ｈ）はＨ上の量子状態からなる集合を表すものとする。

$$0 < p^{(0)} \leqq \min\{p_{ij}\}$$

$$p_{ij}^{(0)} = p^{(0)} / p_{ij}$$

$$p_{ij}^{(0)} + p_{ij}^{(1)} = 1$$

$$\rho_{ij}^{(0)} \in S(H_{ij}^{(0)})$$

$$\dim H_{ij}^{(0)} = 2 \qquad \cdots (77)$$

この分解は、鍵のもつ情報量R_xができるだけ大きく、あるいは、最終的な（圧縮後の）鍵のもつ情報量ができるだけ小さく見積もれるように決定する。以下、送信機は、確率$p_{ij}^{(0)}$で$\rho_{ij}^{(0)}$を出力し、確率$p_{ij}^{(1)}$で$\rho_{ij}^{(1)}$を出力するものと考える。

【０１３６】

上記と同様に、Ｘは００，０１，１０，１１の４つの値をとるものとする。$P_X^{(0)}$を$H_X^{(0)}$への射影演算子とする。これを用いて$H_X^{(0)}$上の演算子F_X'を下記（７８）式により定義する。

$$F_X' = P_X^{(0)} E_X P_X^{(0)} \qquad \cdots (78)$$

【０１３７】

さらに、ヒルベルト空間Ｈの２次元部分ヒルベルト空間をH_2とする。F_X（Ｘ＝００，０１，１０または１１）をヒルベルト空間H_2上の演算子で下記（７９）式を満たすものとする。ただし、Ｉはヒルベルト空間H_2上の単位演算子を表す。

$$F_{00} + F_{01} = I$$
$$F_{10} + F_{11} = I \qquad \cdots (79)$$

【０１３８】

ヒルベルト空間H_2および演算子F_Xは、下記（８０）式で定義されるΔ_X（Ｘ＝００，０１，１０または１１）あるいはその上限を最小化するものを選ぶ。

$$\Delta_X = d(F_X', F_X) \qquad \cdots (80)$$

【０１３９】

いま、$\rho_0^{(0)}$および$\rho_1^{(0)}$を下記（８１）式で与えられる基底に関する平均量子状態とする。

$$\rho_0^{(0)} = (\rho_{00}^{(0)} + \rho_{01}^{(0)}) / 2$$
$$\rho_1^{(0)} = (\rho_{10}^{(0)} + \rho_{11}^{(0)}) / 2 \qquad \cdots (81)$$

【０１４０】

さらに、υを基底ａ［Ｌ］に対応する平均量子状態$\rho_{a[L]}^{(0)}$と反転基底ａ~［Ｌ］に対応する平均量子状態$\rho_{a\sim[L]}^{(0)}$の間のトレース距離の上限値とする。すなわち、υは下記（８２）式をみたすものとする。

$$d(\rho_{a[L]}^{(0)}, \rho_{a\sim[L]}^{(0)}) \leqq \upsilon \qquad \cdots (82)$$

【０１４１】

以下、ρをＥに、σをＦに置き換えて、上記（６３）式から（７５）式までを計算し、部分Ｋのもつ情報量の下限値R_xを求める。

【０１４２】

つぎに、２つの非直交量子状態をもちいる量子鍵配送方式（Ｂ９２プロトコル）を考える。このプロトコルでは、ステップＳ２，ステップＳ３，ステップＳ１２，ステップＳ１３を以下で置き換える。まず、送信機側では、長さn_Aのランダムなビット列ｘ［Ａ］を用意し、ビット０に０°に偏光された光を、ビット１に４５°に偏光された光を、対応させる（ステップＳ２）。この対応関係に基づいて、送信機側は受信側に光子を送信する（ステップＳ３）。受信機側でも、長さn_Aのランダムなビット列ａ［Ａ］を用意し、ビット０に水平垂直方向（０°，９０°）の偏光を識別可能な測定器を、ビット１に斜め方向（４５°，１３５°）の偏光を識別可能な測定器を、対応させる（ステップＳ１２）。この対応関係に基づいて、受信機側は、受信側から送られてきた光子を測定する（ステップＳ１３）。なお、鍵生成の効率をよくするため、本実施例では、４５°偏光を用いたが、０°と直交しない偏光であればよい。

【０１４３】

受信側で検出できた部分をＤとする。受信側で９０°もしくは１３５°の結果が得られた場合、受信データをそれぞれ１，０とする。それ以外の場合、データを捨てる。Ｄのうち、捨てられずに残った部分をＣとする。受信側で得られたデータをｙ［Ｃ］とする（ステップＳ１３）。部分Ｃの位置に対応する送信データをｘ［Ｃ］とする（ステップＳ３）。

【０１４４】
ステップＳ４からステップＳ７まで、ステップＳ１４からステップＳ１８までは、これまでと同様に行う。
【０１４５】
送信側の通信装置および受信側の通信装置では、量子通信路を通して盗聴者にもれた情報を考慮した上での鍵（送信データｘ［Ｋ］）のもつ情報量（の下限値）R_xを推定する（ステップＳ８，ステップＳ１９に相当）。ここでは、送信側の通信装置と受信側の通信装置の両方で鍵のもつ情報量R_xを計算することとしてもよいし、または、送信側の通信装置でR_xを計算し、その結果を受信側に公開することとしてもよい。以下では、特に、両方でR_xを計算する場合について説明する。
【０１４６】
実際に送信機から出力される０°，４５°方向に偏光された光子の量子状態（送信機誤差を含む送信状態）をρ_0，ρ_1と表す。ここで、各量子状態は、ヒルベルト空間Ｈ上の密度演算子になっているものとする。また、各量子状態は、それぞれ確率p_0，p_1で出力されるものとする。この量子状態ρ_0，ρ_1は、予め受信側の通信装置に対して公開しておく。ただし、送信側の通信装置でR_xを計算し、その結果を受信側に公開する場合には、これらの値を公開する必要はない。
【０１４７】
送信側の通信装置では、量子状態ρ_i（ｉは０もしくは１）を下記（８３）式のように分解する。

$$\rho_i = p_i^{(0)} \rho_i^{(0)} + p_i^{(1)} \rho_i^{(1)}$$
$$0 < p^{(0)} \leqq \min \{p_i\}$$
$$p_i^{(0)} = p^{(0)} / p_i$$
$$p_i^{(0)} + p_i^{(1)} = 1 \qquad \cdots (83)$$

【０１４８】
この分解は、鍵のもつ情報量R_xができるだけ大きく見積もれるように決定する。たとえば、$d(p_0^{(1)}\rho_0^{(1)}, p_1^{(1)}\rho_1^{(1)})$はできるだけ小さく、$p_0^{(1)} + p_1^{(1)}$はできるだけ大きくなるように選ぶと、一般に$R_x$を大きく見積もることができる。以下、送信機は、確率$p_i^{(0)}$で$\rho_i^{(0)}$を出力し、確率$p_i^{(1)}$で$\rho_i^{(1)}$を出力するものと考える。
【０１４９】
Ｘ，Ｙは０，１の２つの値をとるものとする。上記量子状態$\rho_X^{(0)}$のスペクトル分解を

$$\rho_X^{(0)} = \Sigma_{kX} \lambda_X(k_X) \, |k_X\rangle \langle k_X| \qquad \cdots (84)$$

とし、μ_{XY}を集合$\{k_X\}$から集合$\{k_Y\}$への写像とする。さらに、$|\phi_{kX}\rangle$を適当なヒルベルト空間の元とする。ここで、２行２列のグラム行列Ｇを下記（８５）式により計算する。

$$G_{XY} = \Sigma_{kX} \langle k_X | k_{XY} \rangle \langle \phi_{kX} | \phi_{kXY} \rangle \sqrt{(\lambda_X(k_X) \lambda_Y(k_{XY}))} \qquad \cdots (85)$$

ただし、$k_{XY} = \mu_{XY}(k_X)$である。μ_{XY}および$|\phi_{kX}\rangle$は、鍵のもつ情報量R_xができるだけ大きく見積もれるように選ぶ。
【０１５０】
グラム行列Ｇは、半正定値であるから２次の正方行列Ｃが存在して下記（８６）式が成り立つ。

$$G = C^* C \qquad \cdots (86)$$

【０１５１】
さらに、Ｇの対角成分は１であるから、行列Ｃの列ベクトルは２次元ヒルベルト空間H_2上の長さ１の元とみなすことができる。そこで、H_2上の量子状態σ_{00}，σ_{01}，σ_{10}，σ_{11}を下記（８７）式により定義する。ただし、Ｉはヒルベルト空間H_2上の単位演算子を表す。

$$\sigma_{00} = |C_0\rangle \langle C_0|$$
$$\sigma_{01} = I - \sigma_{00}$$

$\sigma_{11}=|C_1\rangle\langle C_1|$
$\sigma_{10}=I-\sigma_{11}$ …（８７）

【０１５２】
ここで、C_Xは行列Ｃの第Ｘ列をあらわすものとする。このσ_{XY}の構成法より、σ_{XX}から$\rho_X^{(0)}$への完全正写像の存在が保証される。そこで、以下、$\rho_X^{(0)}$の代わりにσ_{XX}が出力されるものと考える。

【０１５３】
部分Ｋのうち、$\rho_i^{(0)}$が出力されている部分をＬ、$\rho_i^{(1)}$が出力されている部分をＭ、とする。部分Ｍの長さの上限値n_{M+}，部分Ｍのもつ情報量（の下限値）$R_{x[M]}$を見積もり、これらの見積もりが誤ってしまう確率（の上限値）ε_Eを計算する。この計算は、たとえば、以下のようにして行うことができる。まず、δ_Lを適当な正数とし、部分Ｍの長さの上限値n_{M+}を下記（８８）式により見積もる。

$p^{(1)}=p_0p_0^{(1)}+p_1p_1^{(1)}$
$p_M=((n_M/n_A)-\delta_M)/(p^{(1)}n_K/n_C)$
$n_{M+}=max_M\{n_M\}$ …（８８）

なお、max_Mは$p_M\leqq 1$という条件のもとで、Ｍに関して最大化するものとする。

【０１５４】
この見積もりが誤ってしまう確率の上限値を、下記（８９）式で計算する。

$\varepsilon_E=n_A\exp(-n_AD(B(n_M/n_A)|(B(n_M/n_A-\delta_M))))$ …（８９）

【０１５５】
T_i（ｉは０もしくは１）をヒルベルト空間Ｈ上の演算子で、下記（９０）式を満たすものとする。ただし、Ｉはヒルベルト空間Ｈ上の単位演算子を表す。

$0\leqq T_i,\ T_0+T_1\leqq I$ …（９０）

これにより、T_iは部分Ｍにおいて、送信量子状態が$\rho_0^{(1)}$であるか$\rho_1^{(1)}$であるかを識別するための測定演算子と考えることができる。この識別が成功する確率の最大値を下記（９１）式で計算する。

$p_i^{(M)}=p_ip_i^{(1)}/(p_0p_0^{(1)}+p_1p_1^{(1)})$
$s_{M,}=max_T\{(\Sigma_i Trp_i^{(M)}\rho_i^{(1)}T_i)/(\Sigma_{i,j}Trp_i^{(M)}\rho_i^{(1)}T_j)\}$ …（９１）

ただし、max_Tは下記（９２）式を満たすという条件のもとでＴに関して最大化するものとする。

$(\Sigma_{ij}Trp_i^{(M)}\rho_i^{(1)}T_j)\geqq p_M$ …（９２）

【０１５６】
これを用いて、部分Ｍのもつ情報量の下限値$R_{x[M]}$を下記（９３）式により計算する。

$R_{x[M]}=-n_M\log s_M$ …（９３）

【０１５７】
上記（５７）式から（７５）式までを計算し、部分Ｋのもつ情報量の下限値R_xを求める。ただし、下記（９４）式中のパラメータに関しては同式中の値を用いるものとする。

$\sigma_{00}'=\sigma_{00}$，$\sigma_{01}'=\sigma_{01}$，$\sigma_{10}'=\sigma_{10}$，$\sigma_{11}'=\sigma_{11}$
$\Delta_X=0$，$\upsilon=0$，$\tau=0$，$\varepsilon_k=0$，$k=0$ …（９４）

【０１５８】
つぎに、２つの非直交量子状態をもちいる量子鍵配送方式（Ｂ９２プロトコル）において、受信機側の装置の特性を用いて鍵の持つ情報量R_xを計算する手順を示す（ステップＳ８，ステップＳ１９に相当）。実際に送信機から出力される０°，４５°方向に偏光された光子の量子状態（送信機誤差を含む送信状態）をρ_0，ρ_1と表す。また、各量子状態はそれぞれ確率p_0，p_1で出力されるものとする。さらに、実際に受信機が行う０°，４５°方向の測定（受信機誤差を含む測定）に対応する演算子をE_0，E_1と表す。ここで、各演算子は、ヒルベルト空間Ｈ上の密度演算子になっているものとする。この演算子E_0，E_1は、予め送信側の通信装置に対して公開しておく。また、量子状態ρ_0，ρ_1は、予

め受信側の通信装置に対して公開しておく。ただし、送信側の通信装置でR_xを計算し、その結果を受信側に公開する場合には、これらの値（量子状態）を公開する必要はない。

【０１５９】

送信側の通信装置では、量子状態ρ_{ij}（ｉは０もしくは１）を下記（９５）式のように分解する。

$$\rho_i = p_i^{(0)} \rho_i^{(0)} + p_i^{(1)} \rho_i^{(1)} \quad \cdots (95)$$

ただし、$\rho_i^{(0)}$，$\rho_i^{(1)}$はヒルベルト空間Ｈ上の密度演算子であり、下記（９６）式をみたすものとする。ただし、ヒルベルト空間Ｈに対して、Ｓ（Ｈ）はＨ上の量子状態からなる集合を表すものとする。

$$0 < p^{(0)} \leqq \min \{p_{ij}\}$$
$$p_{ij}^{(0)} = p^{(0)} / p_{ij}$$
$$p_{ij}^{(0)} + p_{ij}^{(1)} = 1$$
$$\rho_i^{(0)} \in S(H_i^{(0)}) \quad \cdots (96)$$

【０１６０】

この分解は、鍵のもつ情報量R_xができるだけ大きく見積もれるように決定する。以下、送信機は確率$p_i^{(0)}$で$\rho_i^{(0)}$を出力し、確率$p_i^{(1)}$で$\rho_i^{(1)}$を出力するものと考える。

【０１６１】

Ｘは０，１の２つの値をとるものとする。$P_X^{(0)}$を$H_X^{(0)}$への射影演算子とする。これを用いて$H_X^{(0)}$上の演算子F_Xを下記（９７）式により定義する。

$$F_X = P_X^{(0)} E_X P_X^{(0)} \quad \cdots (97)$$

【０１６２】

以下、ρをＥに、σをＦに置き換えて、上記（５７）式から（７５）式までを計算し、部分Ｋのもつ情報量の下限値R_xを求める。ただし、上記（８８）式から（９４）式までの中に記されるパラメータに関しては当該式中の値を用いるものとする。

【０１６３】

なお、本実施例では、受信側の通信装置においても、上記ステップＳ８と同様の処理で鍵の持つ情報量R_xを計算する。

【０１６４】

情報量I_Eの代わりに情報量（$n_K - R_x$）を用いて、上記ステップＳ９，ステップＳ２０と同様の手順で鍵を圧縮する。

【０１６５】

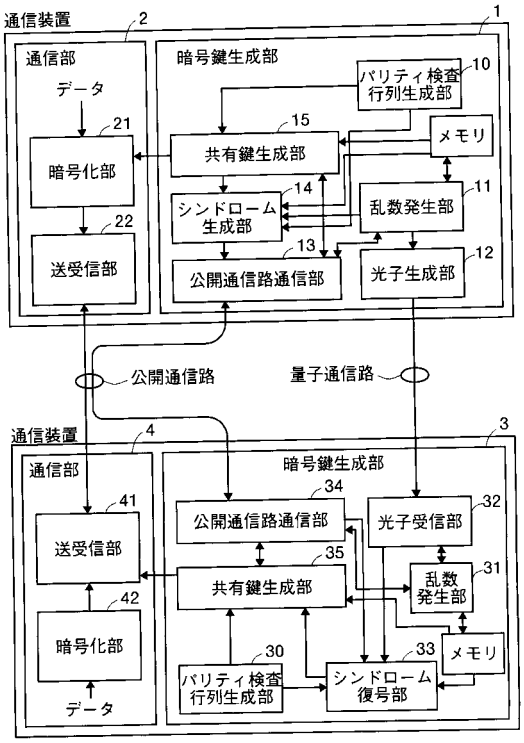
このように、本実施例おいては、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正しつつ、上記ステップＳ４およびＳ１４、ステップＳ７およびＳ１８、ステップＳ８およびＳ１９、を実行し、さらに、上記処理の過程で公開通信路を介して公開した情報量および量子通信路を通して盗聴者にもれた情報量の推定値に応じてデータを圧縮し、圧縮後のデータを装置間で共有の暗号鍵とすることとした。これにより、高度に安全性の保証された共通鍵を効率良く生成することができる。すなわち、成功確率が$1 - \varepsilon_E - \varepsilon_p - \varepsilon_k - \varepsilon_c$以上で、かつ盗聴者にもれる情報量が$(2^{-v} / \ln 2) + n_L e_L$以下の、量子鍵配送方法が実現できる。なお、ｌｎは、底が自然対数ｅの対数関数を表している。

【産業上の利用可能性】

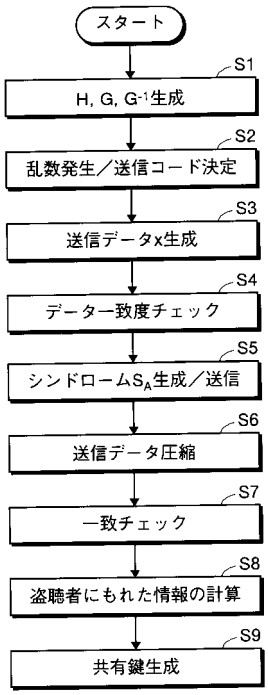
【０１６６】

以上のように、本発明にかかる量子鍵配送方法および通信装置は、高度に安全性の保証された共通鍵を生成する技術として有用であり、特に、盗聴者が存在する可能性のある伝送路上の通信に適している。

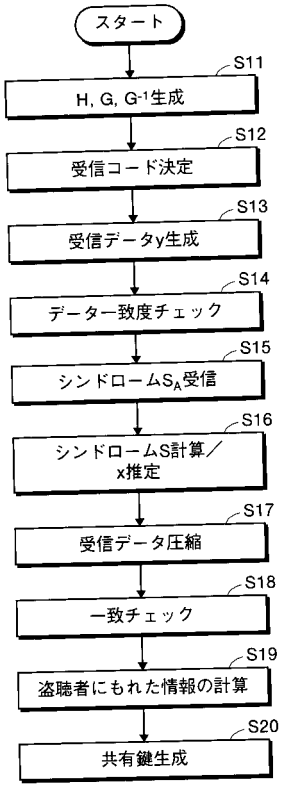
【図１】



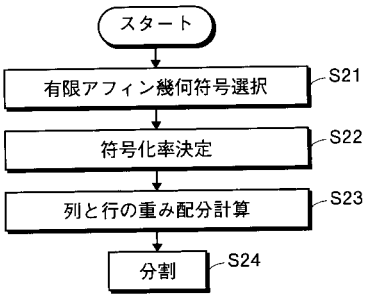
【図２－１】



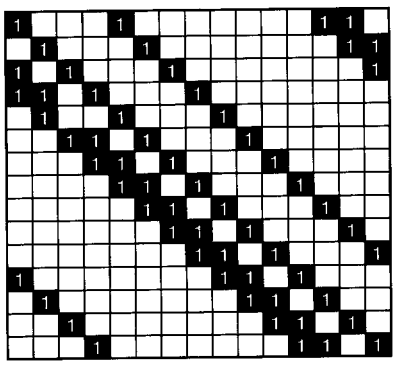
【図２－２】



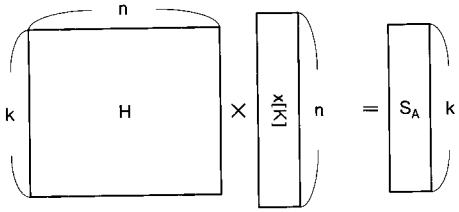
【図３】



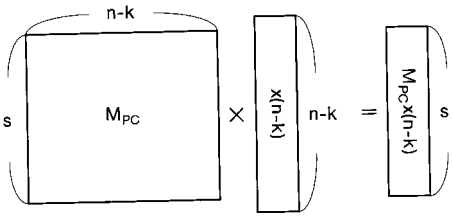
【図４】



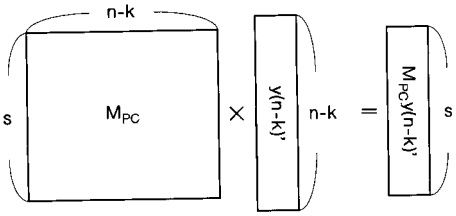
【図５】



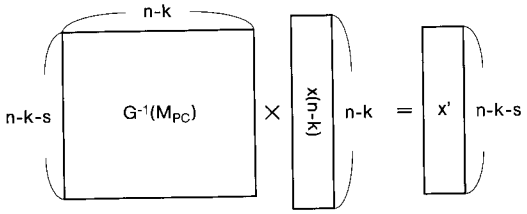
【図６－１】



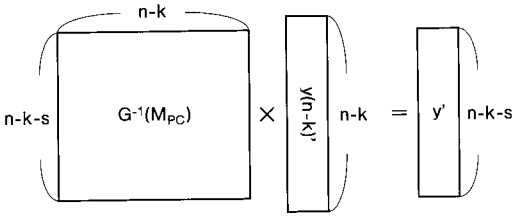
【図６－２】



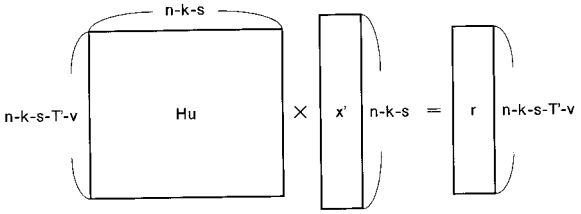
【図７－１】



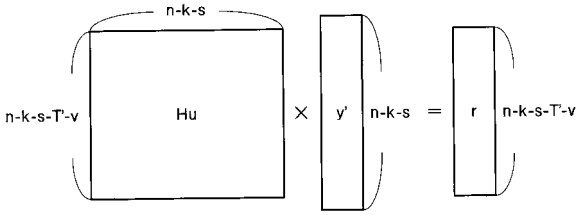
【図７－２】



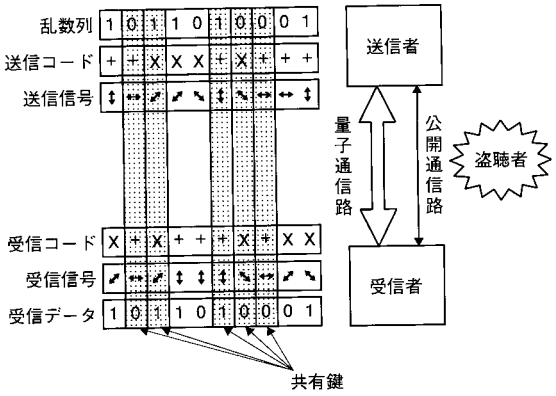
【図８－１】



【図８－２】



【図９】



フロントページの続き

(56)参考文献 特開２００４－１７９８８９（ＪＰ，Ａ）
特開２００４－２７４４５９（ＪＰ，Ａ）
国際公開第２００４／０３０２７０（WO，Ａ１）
Masato Koashi and John Preskill, “Secure quantum key distribution with an uncharacterized source”, Quantum Physics (quant-ph), [online], ２００２年１２月２１日, arXiv:quant-ph/0208155v2, p.1-4, [retrieved on 2011-07-01]. Retrieved from the Internet, ＵＲＬ, <http://arxiv.org/PS_cache/quant-ph/pdf/0208/0208155v2.pdf>
Daniel Gottesman, Hoi-Kwong Lo, Norbert Luetkenhaus, and John Preskill, “Security of quantum key distribution with imperfect devices”, Quantum Physics (quant-ph), [online], ２００４年 ９月 ３日, arXiv:quant-ph/0212066v3, p.1-22, [retrieved on 2011-07-01]. Retrieved from the Internet, ＵＲＬ, <http://arxiv.org/PS_cache/quant-ph/pdf/0212/0212066v3.pdf>
DOMINIC MAYERS, “Unconditional Security in Quantum Cryptography”, Quantum Physics (quant-ph), [online], ２００４年 ９月２９日, arXiv:quant-ph/9802025v5, [retrieved on 2011-07-01]. Retrieved from the Internet, ＵＲＬ, <http://arxiv.org/ftp/quant-ph/papers/9802/9802025.pdf>
渡辺曜大，松本渉，今井秀樹，“低密度パリティ検査行列を用いた量子鍵配送のための誤り訂正技術”，暗号と情報セキュリティシンポジウム（ＳＣＩＳ２００３）講演論文集ＣＤ－ＲＯＭ，日本，２００３年 １月２６日，１５Ｄ 量子システム（２），１５Ｄ－１

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/12