

(19) 日本国特許庁(JP)

再公表特許(A1)

(11) 国際公開番号

W02006/078033

発行日 平成20年6月19日(2008.6.19)

(43) 国際公開日 平成18年7月27日(2006.7.27)

(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 予備審査請求 未請求 (全 41 頁)

出願番号	特願2006-553998 (P2006-553998)	(71) 出願人	504202472 大学共同利用機関法人情報・システム研究 機構 東京都港区南麻布四丁目6番7号
(21) 国際出願番号	PCT/JP2006/301039	(74) 代理人	100089118 弁理士 酒井 宏明
(22) 国際出願日	平成18年1月24日(2006.1.24)	(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
(31) 優先権主張番号	特願2005-15466 (P2005-15466)	Fターム(参考)	5J104 AA05 AA16 EA16 EA21 PA07
(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)		

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) 【要約】

本発明にかかる量子鍵配送方法は、送信データと受信データのエラー確率を推定するエラー確率推定ステップと、誤り訂正情報に基づいて受信データの誤りを訂正する誤り訂正ステップと、送信データと誤り訂正後の受信データが一致しているかどうかを判定する一致判定ステップと、量子通信路を通して盗聴者にもれた情報量を推定する情報量推定ステップと、を含み、さらに、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基づいてデータを圧縮し、圧縮後のデータを装置間で共有の暗号鍵とする。

【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量子通信路上に送信する第 1 の通信装置、および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、にて実行され、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を受信データとし、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方法において、

前記送信データおよび前記受信データからそれぞれ所定数の同一位置のデータを抽出し、抽出後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エラー確率推定ステップと、

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する情報量推定ステップと、

を含み、

各通信装置は、前記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および受信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量子鍵配送方法。

【請求項 2】

前記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および第 2 の通信装置が持つ受信データをそれぞれ所定の数に分割し、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 の通信装置が、前記所定の判定情報として、「所定のランダム行列 × 第 1 の通信装置が持つ送信データ」の計算により特定ビット長の第 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、「所定のランダム行列 × 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

10

20

30

40

50

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。

10

【請求項6】

2準位の量子系を前提とした場合、

前記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、

20

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、

30

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)、

40

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。

50

【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、

10

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、

20

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。

30

【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 の共有鍵生成手段が、前記所定の判定情報として、「所定のランダム行列 × 第 1 の通信装置が持つ送信データ」の計算により特定ビット長の第 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、

40

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、「所定のランダム行列 × 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。

50

【請求項 1 3】

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機能と、

10

所定の誤り訂正情報を、公開通信路を介して前記第2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機能と、

前記第3の送信データと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機能と、

前記推定エラー確率および送信機または受信機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機能と、

20

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機能と、

を有することを特徴とする通信装置。

【請求項 1 4】

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、量子状態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光子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機能と、

30

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機能と、

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機能と、

40

前記推定エラー確率および送信機または受信機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機能と、

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機能と、

を有することを特徴とする通信装置。

【請求項 1 5】

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送信側の通信装置におい

50

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機能と、

所定の誤り訂正情報を、公開通信路を介して前記第2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機能と、

前記第3の送信データと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機能と、

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機能と、

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機能と、

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、量子状態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光子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機能と、

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機能と、

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機能と、

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機能と、

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機能と、

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

10

20

30

40

50

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機能と、

所定の誤り訂正情報を、公開通信路を介して前記第2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機能と、

前記第3の送信データと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、
10 圧縮後のデータを第4の送信データとする一致判定機能と、

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機能と、

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機能と、

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、
20

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光子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機能と、

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機能と、
30

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機能と、

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機能と、

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機能と、
40

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】

10

20

30

40

50

【 0 0 0 2 】

以下、従来 of 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。

【 0 0 0 3 】

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。

10

【 0 0 0 4 】

図9は、従来 of 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。

【 0 0 0 5 】

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。

20

【 0 0 0 6 】

図9に示す従来 of 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。

【 0 0 0 7 】

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, x : 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xの組み合わせで45°方向に偏光された光を、1とx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)。

30

【 0 0 0 8 】

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, x : 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xの組み合わせで0を、135°方向に偏光された光とxの組み合わせで1を、それぞれ得る。

40

【 0 0 0 9 】

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

50

。

【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。

10

【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】

20

【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。

30

【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おいては、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量子通信路上に送信する第1の通信装置、および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、にて実行され、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を受信データとし、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方法において、前記送信データおよび前記受信データからそれぞれ所定数の同一位置のデータを抽出し、抽出後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エラー確率推定ステップと、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する情報量推定ステップと、を含み、各通信装置は、前記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および受信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。

40

【0016】

つぎの発明にかかる量子鍵配送方法において、前記情報量推定ステップでは、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

50

が備える量子状態測定器の特性と、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。

【0017】

つぎの発明にかかる量子鍵配送方法において、前記情報量推定ステップでは、第1の通信装置が持つ送信データおよび第2の通信装置が持つ受信データをそれぞれ所定の数に分割し、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。

【0018】

つぎの発明にかかる量子鍵配送方法においては、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の通信装置が、前記所定の判定情報として、「所定のランダム行列×第1の通信装置が持つ送信データ」の計算により特定ビット長の第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、「所定のランダム行列×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。

10

20

【0019】

つぎの発明にかかる量子鍵配送方法において、2準位の量子系を前提とした場合、前記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。

30

【0020】

つぎの発明にかかる量子鍵配送方法において、2準位の量子系を前提とした場合、前記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に対応する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。

40

50

【 0 0 2 1 】

つぎの発明にかかる量子鍵配送方法において、前記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。

【 0 0 2 2 】

つぎの発明にかかる量子鍵配送方法において、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。

【 0 0 2 3 】

つぎの発明にかかる量子鍵配送方法は、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。

【 0 0 2 4 】

つぎの発明にかかる通信システムは、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。

【 0 0 2 5 】

つぎの発明にかかる通信システムにおいて、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。

【 0 0 2 6 】

つぎの発明にかかる通信システムにおいて、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 の共有鍵生成手段が、前記所定の判定情報として、「所定のランダム行列 × 第 1 の通信装置が持つ送信データ」の計算により特定ビット長の第 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、「所定のランダム行列 × 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。

10

【 0 0 2 7 】

つぎの発明にかかる通信装置にあつては、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量子通信路上に送信し、当該量子状態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送信側の通信装置であつて、たとえば、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機能と、所定の誤り訂正情報を、公開通信路を介して前記第 2 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機能と、前記第 3 の送信データと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機能と、前記推定エラー確率および送信機または受信機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機能と、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機能と、を有することを特徴とする。

20

30

【 0 0 2 8 】

つぎの発明にかかる通信装置にあつては、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、量子状態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を第 1 の受信データとする量子状態受信側の通信装置であつて、たとえば、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光子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機能と、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機能と、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

40

50

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機能と、前記推定エラー確率および送信機または受信機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機能と、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機能と、を有することを特徴とする。

【0029】

つぎの発明にかかる通信装置にあつては、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量子通信路上に送信し、当該量子状態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送信側の通信装置であつて、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機能と、所定の誤り訂正情報を、公開通信路を介して前記第2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機能と、前記第3の送信データと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機能と、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機能と、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機能と、を有することを特徴とする。

【0030】

つぎの発明にかかる通信装置にあつては、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、量子状態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を第1の受信データとする量子状態受信側の通信装置であつて、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光子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機能と、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機能と、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機能と、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機能と、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機能と、を有することを特徴とする。

【0031】

つぎの発明にかかる通信装置にあつては、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、当該量子状態受信側の通信装置における測定結果と一

10

20

30

40

50

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送信側の通信装置にあって、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機能と、所定の誤り訂正情報を、公開通信路を介して前記第2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機能と、前記第3の送信データと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機能と、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機能と、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機能と、を有することを特徴とする。

10

20

30

40

50

【0032】

つぎの発明にかかる通信装置にあっては、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あって、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光子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機能と、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機能と、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機能と、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機能と、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機能と、を有することを特徴とする。

【発明の効果】

【0033】

この発明によれば、上記エラー確率推定ステップと誤り訂正ステップと一致判定ステップと情報量推定ステップとを実行し、さらに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基づいてデータを圧縮し、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。特に、量子通信路を通して盗聴者にもれた情報量に関しては、送信機および受信機の特性に基づいて推定することとした。これにより、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 $M_{PC} \times (n - k)$ 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。

10

【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、従来の特許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

20

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】

30

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】

40

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

50

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 4 2 が暗号鍵に基づいて暗号化したデータを、送受信部 4 1 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。

【 0 0 4 0 】

また、上記暗号鍵生成部 1 は、パリティ検査行列生成部 1 0 と、乱数発生部 1 1 と、光子生成部 1 2 と、公開通信路通信部 1 3 と、シンドローム生成部 1 4 と、共有鍵生成部 1 5 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 3 0 と、乱数発生部 3 1 と、光子受信部 3 2 と、シンドローム復号部 3 3 と、公開通信路通信部 3 4 と、共有鍵生成部 3 5 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。

10

【 0 0 4 1 】

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。

20

【 0 0 4 2 】

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。

【 0 0 4 3 】

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 1 0、3 0 が、特定の線形符号のパリティ検査行列 H （ n 列 \times 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 \times n 行）を求め、さらに、 $G^{-1} \cdot G = I$ （単位行列）となる G の逆行列 G^{-1} （ n 列 \times $(n - k)$ 行）を求める（ステップ S 1、ステップ S 1 1）。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。

30

【 0 0 4 4 】

ここで、上記パリティ検査行列生成部 1 0 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 S 1 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 3 0 については、パリティ検査行列生成部 1 0 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 1 0 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 1 0 で検査行列生成処理を実行

40

50

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 \times 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)。

10

【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 \times 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、 $B_1(x) = \{1\ 32\ 114\ 136\ 149\ 223\ 260\ 382\ 402\ 438\ 467\ 507\ 574\ 579\ 588\ 622\ 634\ 637\ 638\ 676\ 717\ 728\ 790\ 851\ 861\ 879\ 947\ 954\ 971\ 977\ 979\ 998\}$ の場合、分割後の行列における1~4列目 $R_m(n)$ は、 $B_1(x)$ から「1」の番号がランダムに抽出され、たとえば、

20

$R_1(n) = \{1\ 114\ 574\ 637\ 851\ 879\ 977\ 979\}$
 $R_2(n) = \{32\ 136\ 402\ 467\ 588\ 728\ 861\ 971\}$
 $R_3(n) = \{149\ 260\ 382\ 438\ 579\ 638\ 717\ 998\}$
 $R_4(n) = \{223\ 507\ 622\ 634\ 676\ 790\ 947\ 954\}$
 となる。

30

【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 \times 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} ($G^{-1} \cdot G = I$: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, x: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, x: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)。

40

【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xの組み合わせで 45° 方向に偏光された光を、1とx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】

50

光子生成部 1 2 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 3 2 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 S 1 3）。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 \times の組み合わせで 0 を、 135° 方向に偏光された光と \times の組み合わせで 1 を、それぞれ得る。

【 0 0 5 3 】

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 3 1 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 S 1 3）。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 1 1 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 S 3）。

10

【 0 0 5 4 】

そして、受信側の通信装置では、乱数発生部 3 1 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 S 1 3）。また、送信側の通信装置においても、乱数発生部 1 1 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 S 3）。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 $x[C]$ ）。

20

【 0 0 5 5 】

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 S 4, S 1 4）。具体的には、まず、共有鍵生成部 1 5 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 1 5 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。

30

【 0 0 5 6 】

一方、受信側の通信装置の共有鍵生成部 3 5 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、鍵長を長くすることができる。

40

【 0 0 5 7 】

その後、共有鍵生成部 1 5 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 3 5 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。

【 0 0 5 8 】

そして、共有鍵生成部 1 5 では、一致度チェックの最終的な結果として、たとえば、上

50

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 ρ を導入した。

$$P^+ = P_R + (n_R + n_K) \rho / n_K \quad \dots (1)$$

【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 $Pr [P^+ < P_K]$ の上限値 ρ は、セキュリティパラメータ ρ を用いて、下記 (2) 式で与えられる。なお、下記上限値 ρ 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 ρ についても同様である。

$$\rho = \exp(-2 n_R (\rho)^2) Pr [P^+ < P_K] \quad \dots (2)$$

【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 ρ の計算式を下記 (3) 式と差し替える。

$$\begin{aligned} P^+ &= P_R \\ \rho &= 0 \end{aligned} \quad \dots (3)$$

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 \times k 行) と送信データ $x [K]$ を用いて $x [K]$ のシンドローム $S_A = H \times [K]$ 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 $S_B = H y [K]$ 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、

$$y [K] = x [K] + e \text{ (雑音等)} \quad \dots (4)$$

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。

$$\begin{aligned} S &= S_A + S_B \\ &= H x [K] + H y [K] \\ &= H (x [K] + y [K]) \\ &= H (x [K] + x [K] + e) \\ &= H e \end{aligned} \quad \dots (5)$$

【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} ($n \times (n - k)$) を用いて下記 (6) 式により受信データ $y (n - k)'$ を生成する。

$$y (n - k) ' = G^{-1} y [K] ' \quad \dots (6)$$

【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

10

20

30

40

50

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 S 6)。すなわち、共有鍵生成部 15 では、先に計算しておいた $G^{-1}(n \times (n - k))$ を用いて下記 (7) 式により送信データ $x(n - k)$ を生成する。

$$x(n - k) = G^{-1} x [K] \quad \dots (7)$$

【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 S 7, ステップ S 18)。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。

10

【0066】

たとえば、どちらか一方の共有鍵生成部が、 $(n - k)$ 列 $\times s$ 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「 $M_{PC} \cdot G(M_{PC}) = 0$ 」を満たす $(n - k - s)$ 列 $\times (n - k)$ 行の生成行列 $G(M_{PC})$ を求め、さらに、 $G^{-1}(M_{PC}) \cdot G(M_{PC}) = I$ (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 $\times (n - k - s)$ 行の行列)。

20

【0067】

そして、たとえば、共有鍵生成部 15 では、「ランダム行列 $M_{PC} \times$ 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 $M_{PC} \times$ 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。

30

【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。

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

【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。

40

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

【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 c は、

$$c = 2^{-s} \quad \dots (10)$$

50

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 $0^\circ, 90^\circ, 45^\circ, 135^\circ$ 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 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ と表す。この量子状態 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ 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 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ を公開する必要はない。

【0074】

送信機において、基底0($0^\circ, 90^\circ$ 基底)および1($45^\circ, 135^\circ$ 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 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ として、下記(11)式を満たし、かつ、下記(12)式中の $|0\rangle$ および $|1\rangle$ 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。

$$\begin{aligned}
(|00\rangle)^2 &= |00\rangle, & (|01\rangle)^2 &= |01\rangle, & |00\rangle + |01\rangle &= I \\
(|10\rangle)^2 &= |10\rangle, & (|11\rangle)^2 &= |11\rangle, & |10\rangle + |11\rangle &= I \quad \dots (11) \\
|0\rangle &= d\left(\left(\frac{1}{2}\right)|00\rangle - \left(\frac{1}{2}\right)|00\rangle + d\left(\left(\frac{1}{2}\right)|01\rangle - \left(\frac{1}{2}\right)|01\rangle\right)\right) \\
|1\rangle &= d\left(\left(\frac{1}{2}\right)|10\rangle - \left(\frac{1}{2}\right)|10\rangle + d\left(\left(\frac{1}{2}\right)|11\rangle - \left(\frac{1}{2}\right)|11\rangle\right)\right) \quad \dots (12)
\end{aligned}$$

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。

$$d(A) = \text{Tr}\left(\left(A^*A\right)\right) \quad \dots (13)$$

【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 $|0\rangle$ および $|1\rangle$ を用いて、量子状態 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ の代わりに量子状態 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

10

20

30

40

50

$0, 1$ を用いた場合の測定結果の差(変動距離)の上限値 κ 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、 K 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。

$$\kappa = n_0 \cdot 0 + n_1 \cdot 1 + \kappa \quad \dots (14)$$

【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 $00, 01, 10, 11$ の代わりに量子状態 $00, 01, 10, 11$ 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_κ よりも小さく見積もられてしまう確率の上限値 κ を、下記(15)式により計算する。

$$\kappa = 2 \cdot \kappa p_b (a) / p_b (a') \quad \dots (15)$$

【0078】

また、送信機から出力される基底 $0 (0^\circ, 90^\circ \text{基底})$ に対応する平均量子状態 ρ_0 、および基底 $1 (45^\circ, 135^\circ \text{基底})$ 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。

$$\rho_0 = p_x (0) \cdot 00 + p_x (1) \cdot 01 \quad \dots (16)$$

$$\rho_1 = p_x (0) \cdot 10 + p_x (1) \cdot 11 \quad \dots (17)$$

【0079】

さらに、量子状態 $00, 01, 10, 11$ 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。

$$q = \max \{ \text{Tr} \rho_0 \rho_1, \text{Tr} \rho_0 \rho_1 \} \quad \dots (18)$$

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 κ を下記(19)式により計算する。

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

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。

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

【0080】

量子状態 $00, 01, 10, 11$ 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。

$$I_Q = n_\kappa + (1 - 1/c) (\log(\kappa) - 2 \log(1 - (c/\kappa))) \quad \dots (21)$$

【0081】

さらに、量子状態 $00, 01, 10, 11$ 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。

$$I_E = I_Q + \kappa (3 n_\kappa - 2 \log \kappa) \quad \dots (22)$$

【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 $00, 01, 10, 11, p_b(0), p_b(1), p_x(0), p_x(1)$ 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 e_s を用いて、パラメータ e^+ を下記(24)式により計算する。

$$e^+ = e_s + \dots (24)$$

10

20

30

40

50

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ふ確率の上限 ϵ_s は、下記 (25) 式で計算できる。

$$\epsilon_s = \exp(-2n_K(\epsilon_s)^2) \Pr[n^+ \leq n_s] \quad \dots (25)$$

【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 中の 0 の数、 m_1 は、 a_L 中の 1 の数を表す。また、 ϵ_L 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。

$$\epsilon_L = m_0 \epsilon_0 + m_1 \epsilon_1 \quad \dots (26)$$

【0085】

(15) 式および (19) 式の代わりに、 ϵ_L および ϵ_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。

$$\epsilon_L = \max_L \{ 2^{-n_L} p_b(a_L) / p_b(a_L') \} \quad \dots (27)$$

$$\epsilon_L = 2^{-n_L (h((n_K/n_L)P^+) + \log(q))} \quad \dots (28)$$

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どうかと独立な場合は、入力を「 $P_{R^+}(n_R/n_L)P/n_L$ 」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。

$$I_Q' = n_L + (1 - 1/c) (\log(\epsilon_L) - 2 \log(1 - (c \epsilon_L))) \quad \dots (29)$$

$$I_E' = I_Q' + \epsilon_L (3n_L - 2 \log \epsilon_L) \quad \dots (30)$$

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。

$$I_E = I_E' + I_M' \quad \dots (31)$$

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

10

20

30

40

50

限を、それぞれ ρ_0 および ρ_1 と表す。すなわち、 ρ_0 および ρ_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。

$$d(\rho_0 - (1/2)I) = \rho_0 \quad \dots (32)$$

$$d(\rho_1 - (1/2)I) = \rho_1 \quad \dots (33)$$

【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 ρ_0 および ρ_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。

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

$$(F_{10})^2 = F_{10}, (F_{11})^2 = F_{11}, F_{10} + F_{11} = I \quad \dots (34)$$

$$\rho_0 = d((1/2)E_{00} - (1/2)F_{00}) + d((1/2)E_{01} - (1/2)F_{01})$$

$$\rho_1 = d((1/2)E_{10} - (1/2)F_{10}) + d((1/2)E_{11} - (1/2)F_{11})$$

$$\dots (35)$$

【0091】

特に、上記 ρ_0 および ρ_1 が 0 の場合は、前記 ρ_0 および ρ_1 として、下記 (36) 式を満たす ρ_p を用いることができる。すなわち、 $\rho_0 = \rho_1 = 0$ の場合は、下記 (36) 式中の ρ_p を用いて、 $\rho_0 = \rho_1 = \rho_p$ とすることができる。

$$d(\rho_0 - \rho_1) = \rho_p \quad \dots (36)$$

【0092】

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

$$n_k = n_0(\rho_0 + \rho_1) + n_1(\rho_1 + \rho_1) + n_k \quad \dots (37)$$

$$q = \max\{\text{Tr} F_{00} F_{10}, \text{Tr} F_{00} F_{11}\} \quad \dots (38)$$

$$L = m_0(\rho_0 + \rho_1) + m_1(\rho_1 + \rho_1) + L \quad \dots (39)$$

上記 n_k, q および 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、 $\{0, 1\}^{n-k-s} \{0, 1\}^{n-k-s-T-v}$

10

20

30

40

50

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 ($\text{rank}(H_u) = n - k - s - T - v$) のランダム行列をとてく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。

$$r = H_u x \quad \dots (40)$$

10

【0098】

一方、共有鍵生成部 35 では、上記 H_u 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。

$$r = H_u y \quad \dots (41)$$

【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、 $\{0, 1\}^{n-k-s} \{0, 1\}^{n-k-s-T-v-k}$ 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。

20

【0100】

このように、本実施例においては、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 $(1 - p_p)(1 - p_s)(1 - p_c)$ 以上で、かつ盗聴者にもれる情報量が $(2^{-v} / \ln 2)$ 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、 $p_s = 0$ とする。

30

【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。

40

【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 00 , 01 , 10 , 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 00 , 01 , 10 , 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。

50

【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。

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

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。

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

【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 $\rho_{ij}^{(1)}$ を出力するものとする。

【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、

$$\rho_x^{(0)} = \sum_{k_x} p_{k_x} \rho_x(k_x) |k_x\rangle \langle k_x| \quad \dots (44)$$

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、 $|k_x\rangle$ 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。

$$G_{xy} = \sum_{k_x} p_{k_x} \langle k_x | \rho_{xy} | k_x \rangle \quad (\rho_x(k_x) \quad \rho_y(k_{xy})) \quad \dots (45)$$

ただし、 $k_{xy} = \mu_{xy}(k_x)$ である。 μ_{xy} および $|k_x\rangle$ 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。

$$G = C^* C \quad \dots (46)$$

【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 ρ_x' ($X = 00, 01, 10$ または 11) を下記 (47) 式により定義する。

$$\rho_x' = |C_x\rangle \langle C_x| \quad \dots (47)$$

ただし、 C_x は行列 C の第 X 列を表すものとする。この ρ_x' の構成法より、 ρ_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 ρ_x' が出力されるものとする。

【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。 ρ_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。

$$\rho_{00} + \rho_{01} = I, \quad \rho_{10} + \rho_{11} = I \quad \dots (48)$$

【0110】

ヒルベルト空間 H_2 および量子状態 ρ_x は、下記 (49) 式で定義される ρ_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、 $d(\rho, \sigma)$ は ρ と σ のトレース距離をあらわすものとする。

$$\rho_x = d(\rho_x', \rho_x) \quad \dots (49)$$

10

20

30

40

50

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 $p_{X|k} = \sum_{k'} \binom{\mu}{k'} \exp(-\mu) |k\rangle\langle k'|$ （ 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。

$$\begin{aligned} p_X^{(0)} &= \sum_{k=0}^{\infty} p_{X|k} = \sum_{k=0}^{\infty} \binom{\mu}{k} \exp(-\mu) = 1 \\ p_X^{(0)} &= \mu \exp(-\mu) \\ \mu_{XY}(|k\rangle\langle k|; X) &= \sum_{k'} \binom{\mu}{k'} \exp(-\mu) \dots (50) \end{aligned}$$

【0111】

部分 K のうち、 $p_{ij}^{(0)}$ が出力されている部分を L 、 $p_{ij}^{(1)}$ 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（の下限值） $R_{X[M]}^m$ 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 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、 p_{iM}^i ($i = 0, 1$) を適当な正数とし、部分 M の長さの上限値 n_{M+}^i ($i = 0, 1$) を下記（51）式により見積もる。

$$\begin{aligned} p_i^{(1)} &= (p_{i0} p_{i0}^{(1)} + p_{i1} p_{i1}^{(1)}) / (p_{i0} + p_{i1}) \\ p_{iM}^i &= (n_{M+}^i / n_{iA}^i) - p_{iM}^i / (p_i^{(1)} n_{iK}^i / n_{iD}^i) \\ n_{M+}^i &= \max_M \{ n_{iM}^i \} \dots (51) \end{aligned}$$

ただし、 n_{iK}^i ($i = 0, 1$) は $a[K]$ における i ($= 0$ もしくは 1) の数を表す。 n_{iA}^i , n_{iD}^i , n_{iM}^i も同様とする。なお、 \max_M は $p_{iM}^i = 1$ 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_{iD}^i を n_{iC}^i 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_M^i 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。

$$\epsilon_M^i = \sum_{k=0}^{n_{M+}^i} \binom{n_{M+}^i}{k} \exp(-n_{iA}^i D(B(n_{iM}^i / n_{iA}^i) | (B(n_{iM}^i / n_{iA}^i) - p_{iM}^i))) \dots (52)$$

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。

$$0 \leq T_{ij}, T_{i0} + T_{i1} \leq I \dots (53)$$

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 $p_{i0}^{(1)}$ であるか $p_{i1}^{(1)}$ 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_{iM}^i を下記（54）式で計算する。

$$\begin{aligned} p_{ij}^{(M)} &= p_{ij} p_{ij}^{(1)} / (p_{i0} p_{i0}^{(1)} + p_{i1} p_{i1}^{(1)}) \\ s_{iM}^i &= \sup_T \{ \sum_{j=0,1} \text{Tr} p_{ij}^{(M)} T_{ij} / (\sum_{k=0,1} \text{Tr} p_{ik}^{(M)} T_{ik}) \} \dots (54) \end{aligned}$$

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。

$$\sum_{j=0,1} \text{Tr} p_{ij}^{(M)} T_{ij} \leq p_{iM}^i \dots (55)$$

【0115】

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

$$R_{X[M]}^m = -n_{M+}^0 \log s_{M+}^0 - n_{M+}^1 \log s_{M+}^1 \dots (56)$$

【0116】

10

20

30

40

50

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。 p_e 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。

$$P^+ = (n_K P_R + n_C p_e - n_M^0 (1 - s_M^0) - n_M^1 (1 - s_M^1)) / n_L \quad \dots (57)$$

【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 p_e は、下記（58）式で与えられる。なお、下記上限値 p_e 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。

$$p_e = n_R \exp(-n_R D(B(P_R) | (B(P_R + p_e)))) \quad Pr [P_L > P^+] \quad \dots (58)$$

10

【0118】

量子状態 ρ_x の代わりに量子状態 ρ_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 $a_{\sim[L]}$ 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、 ρ_0 および ρ_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。

$$\begin{aligned} \rho_0 &= (\rho_{00} + \rho_{01}) / 2 \\ \rho_1 &= (\rho_{10} + \rho_{11}) / 2 \quad \dots (59) \end{aligned}$$

20

【0119】

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

$$d(\rho_{a_{[L]}}, \rho_{a_{\sim[L]}}) \quad \dots (60)$$

【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。

$$Pr [P_L > P^+] \leq p_e + \epsilon \quad \dots (61)$$

30

【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 f_x を計算する。

$$f_x = (1 / 2^{n_L}) d(\rho_{a_{\sim[L], x_{[L]}}}, \rho_{a_{\sim[L], x_{[L]}}}) \quad \dots (62)$$

【0122】

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

$$\begin{aligned} f_x &= f(\rho_x, \rho_x) \\ f_0 &= \min\{f_{00}, f_{01}\} \\ f_1 &= \min\{f_{10}, f_{11}\} \\ &= (1 - (f_0)^{2n_0} (f_1)^{2n_1}) \quad \dots (63) \end{aligned}$$

40

ただし、 n_0 、 n_1 は、ビット列 $a_{\sim[L]}$ 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 $a_{\sim[L]}$ 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。

$$Pr [P^+ < P_K] \leq p_e + \epsilon \quad \dots (64)$$

【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

50

により計算する。

$$\begin{aligned}
P_{00} &= \{ \rho_{00} - \rho_{01} > 0 \} \\
P_{01} &= \{ \rho_{01} - \rho_{00} > 0 \} \\
P_{10} &= \{ \rho_{10} - \rho_{11} > 0 \} \\
P_{11} &= \{ \rho_{11} - \rho_{10} > 0 \} \quad \dots (65)
\end{aligned}$$

【0125】

さらに、量子状態 ρ_{00} および ρ_{01} の識別に成功する確率の最大値 s_0 、量子状態 ρ_{10} および ρ_{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。

$$\begin{aligned}
s_0 &= 1 / 2 + d(\rho_{00}, \rho_{01}) \\
s_1 &= 1 / 2 + d(\rho_{10}, \rho_{11}) \quad \dots (66)
\end{aligned}$$

【0126】

いま、量子状態 $\rho_{a-[L], x[L]}$ 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 s_k とする。 s_k は、たとえば、下記 (67) 式により計算することができる。

$$\begin{aligned}
s_k &= (2^{nL} - 2^{nLh(k/nL)}) / 2 / n_L (s_0)^{n_0} (s_1)^{n_1} ((1 - s_m) / s_m)^k \\
s_m &= \min\{s_0, s_1\} \quad \dots (67)
\end{aligned}$$

【0127】

これらの値を用いて、パラメータ L を下記 (68) 式により計算する。

$$L = p^+ + \dots + k 2^{nLh(P^+)} \quad \dots (68)$$

【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。

$$\begin{aligned}
L &= p^+ + E^+ + \dots \\
k &= 0 \quad \dots (69)
\end{aligned}$$

【0129】

パラメータ q_0, q_1 を下記 (70) 式により計算する。

$$\begin{aligned}
q_0 &= \max\{\text{Tr } \rho_{00} P_{10}, \text{Tr } \rho_{00} P_{11}, \text{Tr } \rho_{01} P_{10}, \text{Tr } \rho_{01} P_{11}\} \\
q_1 &= \max\{\text{Tr } \rho_{10} P_{00}, \text{Tr } \rho_{10} P_{01}, \text{Tr } \rho_{11} P_{00}, \text{Tr } \rho_{11} P_{01}\} \quad \dots (70)
\end{aligned}$$

【0130】

これを用いて、パラメータ L を下記 (71) 式により計算する。

$$\begin{aligned}
L &= 2^{nLh(P^*) + n_0 \log(q_0) + n_1 \log(q_1)} \\
P^* &= P^+ + (k / n_L) \quad \dots (71)
\end{aligned}$$

【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。

$$\begin{aligned}
Pr [p_{x|yz} > L] &= (1 / c) \\
L &= L / (1 - (c L))^2 \quad \dots (72)
\end{aligned}$$

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 $R_{x[L]}^m$ および 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。

$$Pr [R_{x[L]} > R_{x[L]}^m] \quad \dots (73)$$

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

$$\begin{aligned}
R_{x[L]}^m &= - \log L \\
L &= 1 / c \quad \dots (74)
\end{aligned}$$

。

10

20

30

40

50

【 0 1 3 3 】

さらに、部分 K のもつ情報量の下限値を下記 (7 5) 式により計算する。

$$R_x = R_{x[K]} = \min_M (R_{x[L]}^m + R_{x[M]}^m) \quad \dots (7 5)$$

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

【 0 1 3 4 】

つぎに、受信機側の装置の特性を用いて鍵のもつ情報量 R_x を計算する手順を示す (ステップ S 8 , ステップ S 1 9 に相当) 。実際に送信機から出力される $0^\circ, 90^\circ, 45^\circ, 135^\circ$ 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 $_{00}, _{01}, _{10}, _{11}$ 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 $0^\circ, 90^\circ, 45^\circ, 135^\circ$ 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 $_{00}, _{01}, _{10}, _{11}$ 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。

10

【 0 1 3 5 】

送信側の通信装置では、量子状態 $_{ij} (i, j \text{ は } 0 \text{ もしくは } 1)$ を下記 (7 6) 式のように分解する。

20

$$_{ij} = p_{ij}^{(0)} \rho_{ij}^{(0)} + p_{ij}^{(1)} \rho_{ij}^{(1)} \quad \dots (7 6)$$

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 (7 7) 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。

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

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

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

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

$$\dim H_{ij}^{(0)} = 2 \quad \dots (7 7)$$

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 $\rho_{ij}^{(1)}$ を出力するものとする。

30

【 0 1 3 6 】

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 (7 8) 式により定義する。

$$F_X' = P_X^{(0)} E_X P_X^{(0)} \quad \dots (7 8)$$

【 0 1 3 7 】

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。 $F_X (X = 00, 01, 10 \text{ または } 11)$ をヒルベルト空間 H_2 上の演算子で下記 (7 9) 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。

40

$$F_{00} + F_{01} = I$$

$$F_{10} + F_{11} = I \quad \dots (7 9)$$

【 0 1 3 8 】

ヒルベルト空間 H_2 および演算子 F_X は、下記 (8 0) 式で定義される $\rho_X (X = 00, 01, 10 \text{ または } 11)$ あるいはその上限を最小化するものを選ぶ。

$$\rho_X = d (F_X', F_X) \quad \dots (8 0)$$

【 0 1 3 9 】

いま、 $\rho_0^{(0)}$ および $\rho_1^{(0)}$ を下記 (8 1) 式で与えられる基底に関する平均量子状態とする。

50

$$\begin{aligned} \rho_0^{(0)} &= (\rho_{00}^{(0)} + \rho_{01}^{(0)}) / 2 \\ \rho_1^{(0)} &= (\rho_{10}^{(0)} + \rho_{11}^{(0)}) / 2 \end{aligned} \quad \dots (81)$$

【0140】

さらに、 $\rho_0^{(0)}$ 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 $a_{\sim[L]}$ 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、 $\rho_0^{(0)}$ は下記(82)式をみたすものとする。

$$d(\rho_{a_{[L]}}^{(0)}, \rho_{a_{\sim[L]}}^{(0)}) \leq 1 \quad \dots (82)$$

【0141】

以下、 $\rho_0^{(0)}$ を E に、 $\rho_1^{(0)}$ 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。

10

【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($0^\circ, 90^\circ$)の偏光を識別可能な測定器を、ビット1に斜め方向($45^\circ, 135^\circ$)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。

20

【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。

30

【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 $0^\circ, 45^\circ$ 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。

40

【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。

$$\begin{aligned} \rho_i &= p_i^{(0)} \rho_i^{(0)} + p_i^{(1)} \rho_i^{(1)} \\ 0 &< p_i^{(0)} \leq \min\{p_i\} \end{aligned}$$

50

$$\begin{aligned} p_i^{(0)} &= p^{(0)} / p_i \\ p_i^{(0)} + p_i^{(1)} &= 1 \end{aligned} \quad \dots (83)$$

【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、 $d(p_0^{(1)}, p_1^{(1)})$ 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 $i^{(0)}$ を出力し、確率 $p_i^{(1)}$ で $i^{(1)}$ を出力するものとする。

【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

$$\rho_X^{(0)} = \sum_{k_X} p_{k_X} |k_X\rangle \langle k_X| \quad \dots (84)$$

10

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、 $|k_X\rangle$ 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。

$$G_{XY} = \sum_{k_X} p_{k_X} |k_X\rangle \langle k_X| \quad \dots (85)$$

ただし、 $k_{XY} = \mu_{XY}(k_X)$ である。 μ_{XY} および $|k_X\rangle$ 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。

$$G = C^* C \quad \dots (86)$$

20

【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 $\rho_{00}, \rho_{01}, \rho_{10}, \rho_{11}$ 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。

$$\begin{aligned} \rho_{00} &= |C_0\rangle \langle C_0| \\ \rho_{01} &= I - \rho_{00} \\ \rho_{11} &= |C_1\rangle \langle C_1| \\ \rho_{10} &= I - \rho_{11} \end{aligned} \quad \dots (87)$$

30

【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 C_X の構成法より、 C_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 C_X が出力されるものとする。

【0153】

部分 K のうち、 $i^{(0)}$ が出力されている部分を L 、 $i^{(1)}$ 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 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、 ϵ 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。

40

$$\begin{aligned} p^{(1)} &= p_0 p_0^{(1)} + p_1 p_1^{(1)} \\ p_M &= (n_M / n_A) - \epsilon / (p^{(1)} n_K / n_C) \\ n_{M+} &= \max_M \{n_M\} \end{aligned} \quad \dots (88)$$

なお、 \max_M は $p_M = 1$ 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。

$$\epsilon = n_A e^{-x p} (n_A D(B(n_M / n_A) | (B(n_M / n_A) - \epsilon))) \quad \dots (89)$$

【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

50

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。

$$0 \leq T_i, T_0 + T_1 \leq I \quad \dots (90)$$

これにより、T_i は部分 M において、送信量子状態が ρ₀⁽¹⁾ であるか ρ₁⁽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。

$$p_i^{(M)} = p_i p_i^{(1)} / (p_0 p_0^{(1)} + p_1 p_1^{(1)})$$
$$s_M = \max_T \{ (\sum_i \text{Tr} p_i^{(M)} \rho_i^{(1)} T_i) / (\sum_{i,j} \text{Tr} p_i^{(M)} \rho_i^{(1)} T_j) \} \quad \dots (91)$$

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。

$$(\sum_{i,j} \text{Tr} p_i^{(M)} \rho_i^{(1)} T_j) \leq p_M \quad \dots (92)$$

【0156】

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

$$R_{x[M]} = -n_M \log s_M \quad \dots (93)$$

【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值 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。

$$\rho_{00}' = \rho_{00}, \rho_{01}' = \rho_{01}, \rho_{10}' = \rho_{10}, \rho_{11}' = \rho_{11}$$
$$x = 0, \alpha = 0, \beta = 0, \gamma_k = 0, \delta_k = 0 \quad \dots (94)$$

【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 ρ₀, ρ₁ と表す。また、各量子状態はそれぞれ確率 p₀, p₁ 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 E₀, E₁ 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 E₀, E₁ 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 ρ₀, ρ₁ 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。

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

ただし、ρ_i⁽⁰⁾, ρ_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。

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

【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 ρ_i⁽⁰⁾ を出力し、確率 p_i⁽¹⁾ で ρ_i⁽¹⁾ を出力するものとする。

【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。

$$F_x = P_x^{(0)} E_x P_x^{(0)} \quad \dots (97)$$

【0162】

以下、ρ₀ を E に、ρ₁ を F に置き換えて、上記 (57) 式から (75) 式までを計算し、

10

20

30

40

50

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、本実施例においては、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 $1 - e^{-p-k-c}$ 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。

10

【産業上の利用可能性】

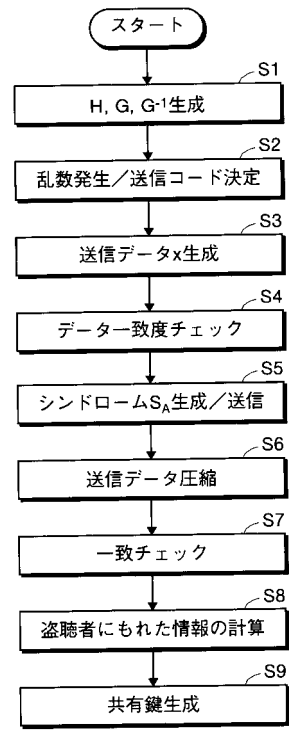
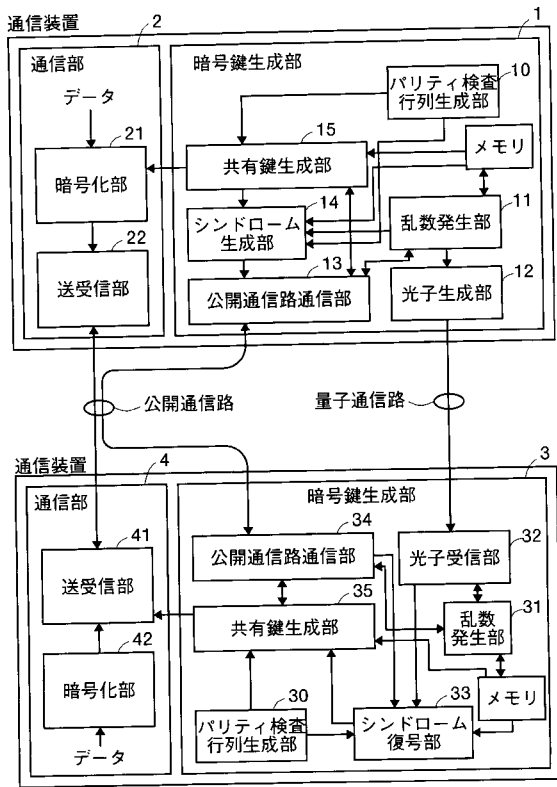
【0166】

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。

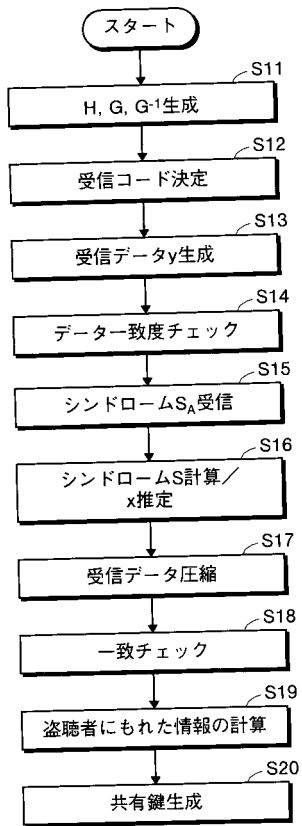
20

【図1】

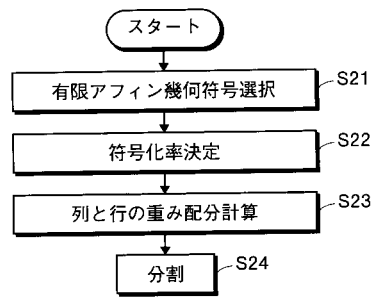
【図2-1】



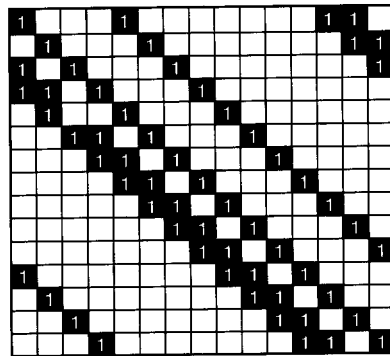
【 図 2 - 2 】



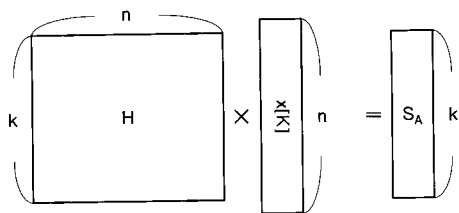
【 図 3 】



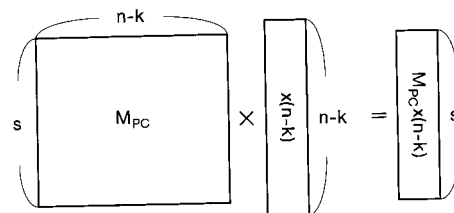
【 図 4 】



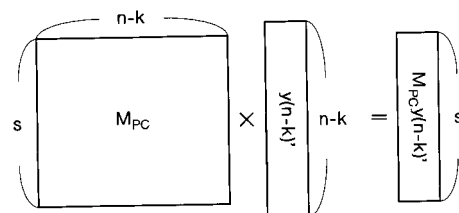
【 図 5 】



【 図 6 - 1 】



【 図 6 - 2 】



【 国際調査報告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP2006/301039
A. CLASSIFICATION OF SUBJECT MATTER H04L9/12(2006.01) , H04L9/08(2006.01)		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04L9/12(2006.01) , H04L9/08(2006.01)		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006 Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Yodai WATANABE, Ayumu MATSUMOTO, Hideki IMAI, "Tei Mitsudo Parity Kensa Gyoretsu o Mochiita Ryoshi Kagi Haiso no tameno Ayamari Teisei Gijutsu", 2003 Nen Anko to Joho Security Symposium Yokoshu, Vol.2 of 2, 26 January, 2003 (26.01.03), pages 1219 to 1224	1-18
A	DOMINIC MAYERS, "Unconditional Security in Quantum Cryptography", Journal of the ACM, Vol.48, No.3, 2001.05, p.351-406 (Quantum Physics, abstract quant-ph/9802025 http://arxiv.org/abs/quant-ph/9802025)	1-18
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 30 March, 2006 (30.03.06)		Date of mailing of the international search report 11 April, 2006 (11.04.06)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2006/301039

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Masato Koashi and John Preskill, "Secure quantum key distribution with an uncharacterized source", arXiv:quant-ph/020815v2, 2002.12.21, http://arxiv.org/abs/quant-ph/0208155 , pages 1 to 4	1-18
A	Daniel Gottesman, Hoi-Kwong Lo, Norbert Lutkenhaus, and John Preskill, "Security of Quantum key distribution with imperfect devices", arXiv:quant-ph/0212066v3, 2004.09.03, http://arxiv.org/abs/quant-ph/0212066 , pages 1-22	1-18
P,X	Yodai WATANABE, "Ryoshi Kagi Haiso Hoshiki no Hanzensei ni tsuite", 2005 Nen Ango to Joho Security Symposium Yokoshu, Vol.2 of 4; 25 January, 2005 (25.01.05), pages 523 to 526	1-18

国際調査報告		国際出願番号 PCT/JP2006/301039									
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. H04L9/12(2006.01), H04L9/08(2006.01)											
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int.Cl. H04L9/12(2006.01), H04L9/08(2006.01)											
最小限資料以外の資料で調査を行った分野に含まれるもの <table border="0" style="width: 100%;"> <tr> <td>日本国実用新案公報</td> <td>1922-1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971-2006年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2006年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2006年</td> </tr> </table>				日本国実用新案公報	1922-1996年	日本国公開実用新案公報	1971-2006年	日本国実用新案登録公報	1996-2006年	日本国登録実用新案公報	1994-2006年
日本国実用新案公報	1922-1996年										
日本国公開実用新案公報	1971-2006年										
日本国実用新案登録公報	1996-2006年										
日本国登録実用新案公報	1994-2006年										
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)											
C. 関連すると認められる文献											
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号									
A	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”, 2003年暗号と情報セキュリティシンポジウム予稿集, Volume 2 of 2, 2003.01.26, p.1219-1224	1-18									
A	DOMINIC MAYERS, “Unconditional Security in Quantum Cryptography”, Journal of the ACM, Vol.48, No.3, 2001.05, p.351-406 (Quantum Physics, abstract quant-ph/9802025 http://arxiv.org/abs/quant-ph/9802025)	1-18									
☞ C欄の続きにも文献が列挙されている。		☞ パテントファミリーに関する別紙を参照。									
* 引用文献のカテゴリー 「A」特に関連のある文献ではなく、一般的技術水準を示すもの 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」口頭による開示、使用、展示等に言及する文献 「P」国際出願日前で、かつ優先権の主張の基礎となる出願		の日の後に公表された文献 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」同一パテントファミリー文献									
国際調査を完了した日 30.03.2006		国際調査報告の発送日 11.04.2006									
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 青木 重徳	5S 4229								
		電話番号 03-3581-1101	内線 3546								

国際調査報告

国際出願番号 PCT/J P 2 0 0 6 / 3 0 1 0 3 9

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	Masato Koashi and John Preskill, "Secure quantum key distribution with an uncharacterized source", arXiv:quant-ph/020815v2, 2002.12.21, http://arxiv.org/abs/quant-ph/0208155 , p.1-4	1-18
A	Daniel Gottesman, Hoi-Kwong Lo, Norbert Lutkenhaus, and John Preskill, "Security of Quantum key distribution with imperfect devices", arXiv:quant-ph/0212066v3, 2004.09.03, http://arxiv.org/abs/quant-ph/0212066 , p.1-22	1-18
P, X	渡辺曜大, "量子鍵配送方式の安全性について", 2005年暗号と情報セキュリティシンポジウム予稿集, Volume 2 of 4, 2005.01.25, p.523-526	1-18

様式PCT/ISA/210 (第2ページの続き) (2005年4月)

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(注)この公表は、国際事務局(WIPO)により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願(日本語実用新案登録出願)の国際公開の効果は、特許法第184条の10第1項(実用新案法第48条の13第2項)により生ずるものであり、本掲載とは関係ありません。