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

特許第4231926号
(P4231926)

(45)発行日　平成21年3月4日(2009.3.4)　(24)登録日　平成20年12月19日(2008.12.19)

(51)Int.Cl.　F I
H04L 9/12 (2006.01)　H04L 9/00 631
H04L 9/08 (2006.01)　H04L 9/00 601C
H04L 9/00 601E

請求項の数 8　(全 22 頁)

(21)出願番号　特願2004-234258(P2004-234258)
(22)出願日　平成16年8月11日(2004.8.11)
(65)公開番号　特開2006-54638(P2006-54638A)
(43)公開日　平成18年2月23日(2006.2.23)
審査請求日　平成16年8月11日(2004.8.11)

(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
東京都港区南麻布四丁目６番７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２－１－２　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】量子鍵配送方法および通信装置

(57)【特許請求の範囲】
【請求項１】
乱数列と基底の組み合わせによって規定された量子状態で光子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光子の測定結果と基底の組み合わせによって規定されたデータを得る第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第１の受信データとし、当該第１の受信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鍵配送方法において、
各通信装置の共有鍵生成部が、前記第１の送信データおよび前記第１の受信データからそれぞれ所定数の同一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相互に通知し、その後、双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のエラー確率を推定するエラー確率推定ステップと、
前記各共有鍵生成部が、公開された部分データ以外の残りのデータをそれぞれ第２の送信データおよび第２の受信データとする第１のデータ圧縮ステップと、
前記第１の通信装置のシンドローム生成部が、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、前記第２の通信装置のシンドローム復号部が、前記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する誤り訂正ステップと、
公開された誤り訂正情報の量に応じて、前記第１の通信装置の共有鍵生成部が前記第２の送信データを、前記第２の通信装置の共有鍵生成部が前記誤り訂正後の第２の受信データを、それぞれ圧縮し、圧縮後のデータをそれぞれ第３の送信データおよび第３の受信データとする第２のデータ圧縮ステップと、

各共有鍵生成部が、前記第３の送信データと前記第３の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を、公開通信路を介して相互に通知し、さらに、前記判定情報に基づいて前記判定処理を行い、当該判定結果が不一致の場合、前記第３の送信データおよび前記第３の受信データを捨てる一致判定ステップと、

前記判定結果が一致の場合、公開された判定情報の量に応じて、前記第１の通信装置の共有鍵生成部が前記第３の送信データを、前記第２の通信装置の共有鍵生成部が前記第３の受信データを、それぞれ圧縮し、圧縮後のデータをそれぞれ第４の送信データおよび第４の受信データとする第３のデータ圧縮ステップと、

前記第１の通信装置の出力に誤差がない場合には、前記第１の通信装置の共有鍵生成部または前記各通信装置の共有鍵生成部のそれぞれが、前記エラー確率の推定値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、一方で、前記第１の通信装置の出力に誤差がある場合には、前記第１の通信装置の共有鍵生成部または前記各通信装置の共有鍵生成部のそれぞれが、前記エラー確率の推定値および前記誤差を反映させた量子状態に基づいて、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、

前記盗聴者にもれた情報量の推定値に基づいて、前記第１の通信装置の共有鍵生成部が前記第４の送信データを、前記第２の通信装置の共有鍵生成部が前記第４の受信データを、それぞれ圧縮し、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】

前記エラー確率推定ステップにおいては、予め規定された「エラー確率の推定値が真のエラー確率よりも小さく見積もられてしまう確率の上限値」を満たすように、エラー確率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】

前記一致判定ステップにて使用する前記判定情報は、システムが要求する安全性に応じて決定されるビット数分の情報とすることを特徴とする請求項１または２に記載の量子鍵配送方法。

【請求項４】

前記情報量推定ステップにおいては、前記送信状態を前記第２の通信装置に対して予め公開しておき、前記第１の通信装置と前記第２の通信装置の両方で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、２または３に記載の量子鍵配送方法。

【請求項５】

前記情報量推定ステップにおいては、前記第１の通信装置にて盗聴者にもれた情報量を推定し、当該推定値を、公開通信路を介して前記第２の通信装置に通知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６】

乱数列と基底の組み合わせによって規定された量子状態で光子を量子通信路上に送信し、光子受信側の通信装置において光子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光子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手段と、

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手段と、
自装置の出力に誤差がない場合には前記エラー確率の推定値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、自装置の出力に誤差がある場合には、前記エラー確率の推定値および自装置の誤差を反映させた量子状態（送信状態）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７】
量子通信路上の光子の測定結果と基底の組み合わせによって規定されたデータのうち、光子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光子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、
光子送信側の通信装置の出力に誤差がない場合には前記エラー確率の推定値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、光子送信側の通信装置の出力に誤差がある場合には、前記エラー確率の推定値および当該光子送信側通信装置の誤差を反映させた量子状態（送信状態）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８】
量子通信路上の光子の測定結果と基底の組み合わせによって規定されたデータのうち、光子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光子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、

請求項６に記載の光子送信側の通信装置が推定した「量子通信路を通して盗聴者にもれた情報量の推定値」を、公開通信路を介して受け取り、当該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、誤り訂正符号を用いてデータ誤りを訂正可能な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 and Coin Tossing, In Proceedings of IEEE Conference on Computers, System and Signal Processing, 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。
【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、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は、乱数列と基底の組み合わせによって規定された量子状態で光子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光子の測定結果と基底の組み合わせによって規定されたデータを得る第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第１の受信データとし、当該第１の受信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鍵配送方法であって、たとえば、各通信装置が、前記第１の送信データおよび前記第１の受信データからそれぞれ所定数の同一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相互に通知し、その後、双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のエラー確率を推定するエラー確率推定ステップと、公開された部分データ以外の残りのデータをそれぞれ第２の送信データおよび第２の受信データとする第１のデータ圧縮ステップと、前記第１の通信装置が、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、前記第２の通信装置が、前記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する誤り訂正ステップと、公開された誤り訂正情報の量に応じて前記第２の送信データおよび前記誤り訂正後の第２の受信データを圧縮し、圧縮後のデータをそれぞれ第３の送信データおよび第３の受信データとする第２のデータ圧縮ステップと、各通信装置が、前記第３の送信データと前記第３の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を、公開通信路を介して相互に通知し、さらに、前記判定情報に基づいて前記判定処理を行い、当該判定結果が不一致の場合、前記第３の送信データおよび前記第３の受信データを捨てる一致判定ステップと、前記判定結果が一致の場合、公開された判定情報の量に応じて前記第３の送信データおよび前記第３の受信データを圧縮し、圧縮後のデータをそれぞれ第４の送信データおよび第４の受信データとする第３のデータ圧縮ステップと、前記エラー確率推定値および前記第１の通信装置の出力の量子状態（送信状態）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、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の送信データおよび前記第４の受信データを圧縮し、圧縮後のデータを各通信装置間で共有の暗号鍵とする共有鍵生成ステップと、を含むことを特徴とする。

【００１６】

つぎの発明において、前記エラー確率推定ステップにあっては、予め規定された「エラー確率の推定値が真のエラー確率よりも小さく見積もられてしまう確率の上限値」を満たすように、エラー確率を推定することを特徴とする。

【００１７】

つぎの発明において、前記一致判定ステップにて使用する前記判定情報は、システムが要求する安全性に応じて決定されるビット数分の情報とすることを特徴とする。

【００１８】

つぎの発明において、前記情報量推定ステップにあっては、前記送信状態を前記第２の通信装置に対して予め公開しておき、前記第１の通信装置と前記第２の通信装置の両方で盗聴者にもれた情報量を推定することを特徴とする。

【００１９】

つぎの発明において、前記情報量推定ステップにあっては、前記第１の通信装置にて盗聴者にもれた情報量を推定し、当該推定値を、公開通信路を介して前記第２の通信装置に通知することを特徴とする。

【００２０】

つぎの発明において、乱数列と基底の組み合わせによって規定された量子状態で光子を量子通信路上に送信し、光子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光子送信側の通信装置にあっては、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、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。

【００２１】

つぎの発明において、量子通信路上の光子の測定結果と基底の組み合わせによって規定されたデータのうち、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光子受信側の通信装置にあっては、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、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。

【００２２】

つぎの発明において、量子通信路上の光子の測定結果と基底の組み合わせによって規定されたデータのうち、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光子受信側の通信装置にあっては、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から得られる「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】

【００２３】

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。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。

【発明を実施するための最良の形態】

【００２４】

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の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。

【実施例】

【００２５】

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、本実施の形態では、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。

【００２６】

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m_a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m_a、すなわち情報m_b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。

【００２７】

また、送信側の通信装置は、量子通信路を介して情報m_a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m_b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。

【００２８】

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。

【００２９】

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m_a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。

【００３０】

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、本実施の形態における量子鍵配送について詳細に説明する。図２は、本実施の形態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。

【００３１】
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）。本実施の形態では、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、本実施の形態では、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m_A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。

【００３２】
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、本実施の形態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。本実施の形態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。以降の実施の形態では、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。

【００３３】
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）。

【００３４】
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）。

【００３５】
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、本実施の形態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。

【００３６】
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。
【００３７】
このように、本実施の形態では、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。
【００３８】
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）。
【００３９】
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）。
【００４０】
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。
【００４１】
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）。
【００４２】
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m_A［Ｃ］および受信データm_B［Ｃ］）をメモリ等に保存する（m_B［Ｃ］は伝送路上で雑音等の影響を受けたm_A［Ｃ］。
【００４３】
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m_A［Ｃ］と上記受信データm_B［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m_A［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m_A［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m_A［Ｃ］の一部分、すなわち、送信データm_A［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。

【００４４】

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m_B［Ｃ］の一部分、すなわち、受信データm_B［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、その他のｎ（＝Ｃ－Ｒ）ビットに対応する送信データm_A（ｎ）および受信データm_B（ｎ）が共有鍵を生成するためのデータとなる。また、本実施の形態では、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。

【００４５】

その後、共有鍵生成部１５では、送信データm_A［Ｒ］と受信側から送られてきた受信データm_B［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_{C-R}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m_B［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m_B［Ｒ］と送信側から送られてきた送信データm_A［Ｒ］とを比較し、上記同様、受信データm_B［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。

【００４６】

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、エラー確率の推定値P_E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Δp^*を導入した。

$$P_E = n_e / n_R + \Delta p^* \quad \cdots (1)$$

【００４７】

このとき、エラー確率の推定値P_Eが真の値P_Tよりも小さく見積もられてしまう確率P_r［$P_E \leqq P_T$］の上限値ε^*は、セキュリティパラメータΔp^*を用いて、下記（２）式で与えられる。なお、下記上限値ε^*は、推定値P_Eが真の値P_T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_0^*，ε_1^*についても同様である。

$$\varepsilon^* = \exp(-2 n_R (\Delta p^*)^2) \geqq P_r [P_E \leqq P_T] \quad \cdots (2)$$

【００４８】

また、共有鍵生成部３５においても、同様の処理でエラー確率の推定値P_Eを求める。なお、上記では、ε^*を固定値とし、ε^*以下となるようなセキュリティパラメータΔp^*を求めているが、これに限らず、Δp^*を固定とし、エラー確率P_Eを満たすようなε^*を求めることとしてもよい。

【００４９】

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m_A（ｎ）を用いてm_A（ｎ）のシンドローム$S_A = H m_A$（ｎ）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、m_A（ｎ）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m_A（ｎ）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）。

【００５０】

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m_B（ｎ）を用いてm_B（ｎ）のシンドローム$S_B = H m_B$（ｎ）を計算し、さらに、m_A（ｎ）のシンドロームS_Aとm_B（ｎ）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m_A（ｎ）を推定する。すな

わち、誤り訂正後の受信データm_B（ｎ）′を求める（ステップＳ１６）。ここでは、

m_B（ｎ）＝m_A（ｎ）＋ｅ（雑音等）　…（３）

とし、下記（４）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、S_A＋S_B，m_A（ｎ）＋ｅの＋は排他的論理和を表す。

$$\begin{aligned} S &= S_A + S_B \\ &= Hm_A(n) + Hm_B(n) \\ &= H(m_A(n) + m_B(n)) \\ &= H(m_A(n) + m_A(n) + e) \\ &= He \end{aligned} \quad \cdots (4)$$

【００５１】

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m_B（ｎ）′の一部を捨てて、（ｎ－ｋ）ビット分の情報量を備えた受信データm_B（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（５）式により受信データm_B（ｎ－ｋ）′を生成する。

m_B（ｎ－ｋ）′＝$G^{-1}m_B$（ｎ）′　…（５）

【００５２】

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m_A（ｎ）の一部を捨てて、ｎ－ｋビット分の情報量を備えた送信データm_A（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（６）式により送信データm_A（ｎ－ｋ）を生成する。

m_A（ｎ－ｋ）＝$G^{-1}m_A$（ｎ）　…（６）

【００５３】

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m_A（ｎ－ｋ）と受信データm_B（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。

【００５４】

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「$M_{PC}G=0$」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）。

【００５５】

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m_A（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$M_{PC}m_A$（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$M_{PC}m_A$（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m_B（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$M_{PC}m_B$（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$M_{PC}m_B$（ｎ－ｋ

）′を示す図である。

【００５６】

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$M_{PC}m_B$（ｎ－ｋ）′と上記計算結果である情報$M_{PC}m_A$（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（７）式を計算し、送信データm_A（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m_A′を得る。図７－１は、送信データm_A′を示す図である。なお、一致しない場合は、送信データm_A（ｎ－ｋ）を捨てる。

$$m_A' = G^{-1}(M_{PC})\, m_A(n-k) \quad \cdots (7)$$

【００５７】

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$M_{PC}m_A$（ｎ－ｋ）と上記計算結果である情報$M_{PC}m_B$（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、受信データm_B（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m_B′を得る。図７－２は、受信データm_B′を示す図である。なお、一致しない場合は、受信データm_B（ｎ－ｋ）′を捨てる。

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

【００５８】

また、本実施の形態においては、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m_B（ｎ－ｋ）′と送信データm_A（ｎ－ｋ）が一致していない確率εは、

$$\varepsilon = 2^{-s} \quad \cdots (9)$$

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。

【００５９】

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Ｔ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Ｔ（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Ｔ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Ｔを計算する場合について説明する。

【００６０】

送信側の通信装置では、たとえば、送信機が理想的な場合（送信機の誤差がない場合：０°，４５°，９０°，１３５°）、共有鍵生成部１５が、上記送信データm_A′およびエラー確率の推定値P_Eに基づいて、下記（１０）式のように、盗聴者にもれた情報量Ｔを計算する。

$$T = |m_A'|\, H_2(P_E)$$

$$H_2(P_E) = -P_E \log P_E - (1-P_E) \log (1-P_E) \quad \cdots (10)$$

【００６１】

同様に、受信側の通信装置においては、共有鍵生成部３５が、上記受信データm_B′およびエラー確率の推定値P_Eに基づいて、下記（１１）式のように、盗聴者にもれた情報量Ｔを計算する。

$$T = |m_B'|\, H_2(P_E) \quad \cdots (11)$$

【００６２】

一方で、送信機が理想的でない場合（送信機誤差がある場合）、送信側の通信装置では、共有鍵生成部１５が、下記のように、盗聴者にもれた情報量Ｔを計算する。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Ｔ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。

【００６３】

この状態で、共有鍵生成部１５では、送信側で用いた基底と上記ビット位置の部分集合Ｒで一致し、さらに、鍵生成のために用いるデータ（送信データm_A'および受信データm_B'に相当）のビット位置の集合Ｋにおいて反転した基底を用いて受信側が観測した場合の、エラー確率P_Fの上限値P_F^*を、下記（１２）式により計算する。ただし、集合Ｋの個数をn_Kとし、上付き文字のＴは複素共役転置を表す。

$$P_F^* = P_E + n_K T_r |\Delta| / 2 = P_E + n_K T_r (\sqrt{\Delta^T \Delta}) / 2$$
$$\Delta = (\rho_{00} + \rho_{01} - \rho_{10} - \rho_{11}) / 2 \quad \cdots (12)$$

【００６４】

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_F^*およびε^*の計算式を下記（１３）式と差し替える。

$$P_F^* = P_E + n_K T_r |\Delta| / 4 = P_E + n_K T_r (\sqrt{\Delta^T \Delta}) / 4$$
$$\varepsilon^* = 1 - (1 - \varepsilon')^2$$
$$\varepsilon' = \exp(-n_R (\Delta p^*)^2) \quad \cdots (13)$$

ただし、Ｒ＝Ｋ、$n_R = n_K$である。

【００６５】

また、送信側で０°，９０°基底を用いた場合のホレボ（Ｈｏｌｅｖｏ）容量をC_0とし、４５°，１３５°基底を用いた場合のホレボ（Ｈｏｌｅｖｏ）容量をC_1とし、C_0およびC_1を、フォン・ノイマンエントロピー：「$S(\rho) = -T_r \rho \log \rho$」を用いて、下記（１４）式および（１５）式により計算する。

$$C_0 = S(\rho_0) - (S(\rho_{00}) + S(\rho_{01}))/2$$
$$\rho_0 = (\rho_{00} - \rho_{01})/2 \quad \cdots (14)$$
$$C_1 = S(\rho_1) - (S(\rho_{10}) + S(\rho_{11}))/2$$
$$\rho_1 = (\rho_{10} - \rho_{11})/2 \quad \cdots (15)$$

【００６６】

また、上記エラー確率P_Fについての条件は、盗聴者による送信量子状態に対する操作についての条件と考えることができる。これにより、以下の手順に従って盗聴者にもれた情報量を見積もることができる。まず、上記と同様に、受信側がデータ部で送信側と反対の基底を用いて測定した場合を考え、その測定値を固定する。さらに、その測定値とエラー確率がP_Fとなる関係にある送信量子状態の混合状態を考える。この混合状態を高い確率で保存する（射影の前後で状態が一致する）ような射影演算子を導入し、この射影演算子を送信状態に作用させることによって、送信状態（送信データ）を固定した場合の盗聴者の測定値に関する条件付き確率の上限値を求める。この上限値から、送信データを条件とした場合の盗聴者の測定値の条件付き情報量（条件付きエントロピー）を見積もることができ、これにより、送信データと盗聴者の測定値の相互情報量も見積もることができる。これを、「$P_F \leqq P_F^*$」という条件の下で送信状態および受信側の測定値に関して最大化することによって盗聴者にもれた情報量の上限値が求まる。以下に、上記手順の実装例を示す。

【００６７】

ここで、共有鍵生成部１５では、上記エラー確率P_Fおよび量子状態ρ_{00}，ρ_{01}，ρ_{10}，ρ_{11}を用いて、４つの混合状態P_0，P_0'，P_1，P_1'を、それぞれ下記（１６）式～（１９）式のように求める。ただし、上記各式の最右辺は、p_0，p_0'，p_1，p_1'が１／２以下となるような各状態のスペクトル分解を表しているものとする。なお、E_0，E_0'，E_1，E_1'は射影演算子になっている。

$$P_0 = P_F \rho_{10} + (1 - P_F) \rho_{11} = p_0 E_0 + (1 - p_0)(I - E_0) \quad \cdots (16)$$
$$P_0' = P_F \rho_{11} + (1 - P_F) \rho_{10} = p_0' E_0' + (1 - p_0')(I - E_0') \quad \cdots (17)$$

$P_1 = P_F\rho_{00} + (1-P_F)\rho_{01} = p_1E_1 + (1-p_1)(I-E_1)$ …（１８）

$P_1' = P_F\rho_{01} + (1-P_F)\rho_{00} = p_1'E_1' + (1-p_1')(I-E_1')$ …（１９）

【００６８】

また、P_0を対角化する正規直交基底を用いて量子状態ρ_{00}，ρ_{01}を表したときの対角成分の最大値をq_0と定義し、同様にq_0'，q_1，q_1'を定義した場合、q_0，q_0'，q_1，q_1'は、下記（２０）式～（２３）式により与えられる。

$q_0 = max\{T_r\rho_{00}E_0,\ 1-T_r\rho_{00}E_0,\ T_r\rho_{01}E_0,\ 1-T_r\rho_{01}E_0\}$ …（２０）

$q_0' = max\{T_r\rho_{00}E_0',\ 1-T_r\rho_{00}E_0',\ T_r\rho_{01}E_0',\ 1-T_r\rho_{01}E_0'\}$ …（２１）

$q_1 = max\{T_r\rho_{10}E_1,\ 1-T_r\rho_{10}E_1,\ T_r\rho_{11}E_1,\ 1-T_r\rho_{11}E_1\}$ …（２２）

$q_1' = max\{T_r\rho_{10}E_1',\ 1-T_r\rho_{10}E_1',\ T_r\rho_{11}E_1',\ 1-T_r\rho_{11}E_1'\}$ …（２３）

【００６９】

これにより、送信データm_Aを固定した場合の盗聴者の測定値m_Eに関する条件付き確率$p(m_E|m_A)$は、下記（２４）式のように見積もることができる。

【００７０】

【数１】

$$p(m_E|m_A) \le 2^{n_K H_2(p_{max}+\Delta p_0^*)} q_{max}^{n_K}$$

$$p_{max} = \max\{p_0, p_0', p_1, p_1'\}$$

$$q_{max} = \max\{q_0, q_0', q_1, q_1'\}$$

…（２４）

【００７１】

ただし、Δp_0^*はセキュリティパラメータであり、この見積もりが失敗する確率の上限値ε_0^*は、下記（２５）式で与えられる。

$\varepsilon_0^* = exp(-2n_K(\Delta p_0^*)^2)$ …（２５）

【００７２】

このとき、送信データm_Aを条件とした場合の盗聴者の測定値m_Eの条件付き情報量$H(m_E|m_A)$は、下記（２６）式の不等式を満たす。

$H(m_E|m_A) \geqq -log\,max\,p(m_E|m_A)$
$= -n_K(H_2(p_{max}+\Delta p_0^*) + log\,q_{max})$ …（２６）

【００７３】

したがって、m_Aとm_Eの相互情報量$I(m_A:m_E)$は、下記（２７）式のように見積もることができる。

$I(m_A:m_E) = H(m_E) - H(m_E|m_A)$
$\leqq n_K + n_K(H_2(p_{max}+\Delta p_0^*) + log\,2q_{max})$
$= n_K(H_2(p_{max}+\Delta p_0^*) + log\,2q_{max})$
$= I_{max}(m_A:m_E)$ …（２７）

【００７４】

最終的に、盗聴者にもれた情報量Tは、下記（２８）式のように見積もることができる

。ただし、鍵生成のために用いるデータのビット位置の集合Ｋにおいて０°，９０°基底が用いられたビットの数をn_0、４５°，１３５°基底が用いられたビットの数をn_1とした。

【００７５】

【数２】

$$T=\left(1-\epsilon_T^*\right)\max_{p_F\le p_F^*}\left\{I_{max}\left(m_A:m_E\right)\right\}+\epsilon_T^*\left(n_0C_0+n_1C_1\right)$$

$$\epsilon_T^*=\epsilon^*+\epsilon_0^*+n_KTr\left|\Delta\right|$$

…（２８）

【００７６】

なお、上記$\varepsilon_T{}^*$は、生起確率がそれぞれε^*，$\varepsilon_0{}^*$，$n_KT_r|\Delta|$であるような事象のうち、少なくともいずれか１つが起こる確率の上限値となっていればよく、その形は上記（２８）式に限定されない。

【００７７】

上記Ｔは、たとえば、以下のようにして計算することもできる。まず、鍵生成のために用いるデータのビット位置の集合Ｋにおいて０°，９０°基底が用いられたビットの数n_0、同じく集合Ｋにおいて４５°，１３５°基底が用いられたビットの数n_1、２つのセキュリティパラメータ$\Delta p_0{}^*$，$\Delta p_1{}^*$、および上記p_0，p_0'，p_1，p_1'，q_0，q_0'，q_1，q_1'を用いて、下記（２９）式～（３３）式により情報量T_0，T_0'，T_1，T_1'を計算する。

$T_0=n_0(H_2(p_0+\Delta p_0{}^*)+\log_2 q_0)$ …（２９）

$T_0'=n_0(H_2(p_0'+\Delta p_0{}^*)+\log_2 q_0')$ …（３０）

$T_1=n_1(H_2(p_1+\Delta p_1{}^*)+\log_2 q_1)$ …（３１）

$T_1'=n_1(H_2(p_1'+\Delta p_1{}^*)+\log_2 q_1')$ …（３２）

$H_2(p)=-p\log p-(1-p)\log(1-p)$ …（３３）

【００７８】

そして、上記で求めた情報量T_0，T_0'，T_1，T_1'を用いて、下記（３４）式のように、盗聴者にもれた情報量Ｔを計算する。

【００７９】

【数３】

$$T=\left(1-\epsilon_T^*\right)\max_{p_F\le p_F^*}\left\{\max\left\{T_0,T'_0\right\}+\max\left\{T_1,T'_1\right\}\right\}+\epsilon_T^*\left(n_0C_0+n_1C_1\right)$$

$$\epsilon_T^*=1-\left(1-\epsilon^*\right)\left(1-\epsilon_0^*\right)\left(1-\epsilon_1^*\right)\left(1-n_KTr\left|\Delta\right|\right)$$

$$\epsilon_0^*=\exp\left(-2n_0\left(\Delta p_0^*\right)^2\right)$$

$$\epsilon_1^*=\exp\left(-2n_1\left(\Delta p_1^*\right)^2\right)$$

…（３４）

【００８０】

なお、上記で用いたセキュリティパラメータΔp^*，$\Delta p_0{}^*$，$\Delta p_1{}^*$は、システムのパフォーマンスの観点からは、盗聴者にもれた情報量Ｔを最小化するように決定するのが望ましい。しかしながら、何らかの理由により最小化ができない場合であっても、送信側と受信側でパラメータが共有できていれば、それを用いることによってシステムの安全性は

保証される。送信側または受信側のいずれか一方が公開することにより、上記パラメータを共有できる。

【００８１】

また、上記情報量T_0，T_0'，T_1，T_1'は、下記の処理で計算することとしてもよい。たとえば、q_0または$1-q_0$のどちらかをn_0回選択し、選択したすべてを掛け合わせてできる実数の集合をS_0とする。すなわち、ビット列ｘに対してｗ（ｘ）によりｘの重み（１の数）を表すと、S_0は、下記（３５）式にて定義することができ、そして、T_0は、下記（３６）式で表すことができる。以降、上記情報量T_0'，T_1，T_1'についても同様に計算する。この計算により、盗聴者にもれた情報量Ｔを小さく見積もることができる。

【００８２】

【数４】

$$S_0 = \left\{ q_0^{w(x)} (1-q_0)^{n_0 - w(x)} \mid x \in \{0,1\}^{n_0} \right\}$$

…（３５）

【００８３】

【数５】

$$T_0 = \max_{\#S_0 = 2^{H_2\left(p_0 + \Delta p_0^*\right)}} \sum_{x \in S_0} q_0^{w(x)} (1-q_0)^{n_0 - w(x)}$$

…（３６）

【００８４】

なお、本実施の形態では、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Ｔを計算する。

【００８５】

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Ｔに基づいて、送信データm_A'および受信データm_B'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Ｔ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Ｔ以上の整数を表す。

【００８６】

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Ｈｕを選ぶ。これは、たとえば、Ｈｕとしてフルランク（ｒａｎｋＨｕ＝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Ｈｕ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。

【００８７】

そして、共有鍵生成部１５では、上記Ｈｕを用いて下記（３７）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。

$r = Hu m_A'$　　…（３７）

【００８８】

一方、共有鍵生成部３５では、上記Ｈｕを用いて下記（３８）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。

$r = Hum_B'$ …（３８）

【００８９】

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Ｈｕを生成し、その後、上記（３７）式および（３８）式を実行することとしてもよい。

【００９０】

このように、本実施の形態おいては、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－ε）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。

【産業上の利用可能性】

【００９１】

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。

【図面の簡単な説明】

【００９２】

【図１】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】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】本発明の量子鍵配送を示すフローチャートである。

【図３】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】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】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】情報$M_{PC}m_A$（ｎ－ｋ）を示す図である。

【図６－２】情報$M_{PC}m_B$（ｎ－ｋ）′を示す図である。

【図７－１】送信データm_A'を示す図である。

【図７－２】受信データm_B'を示す図である。

【図８－１】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】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】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。

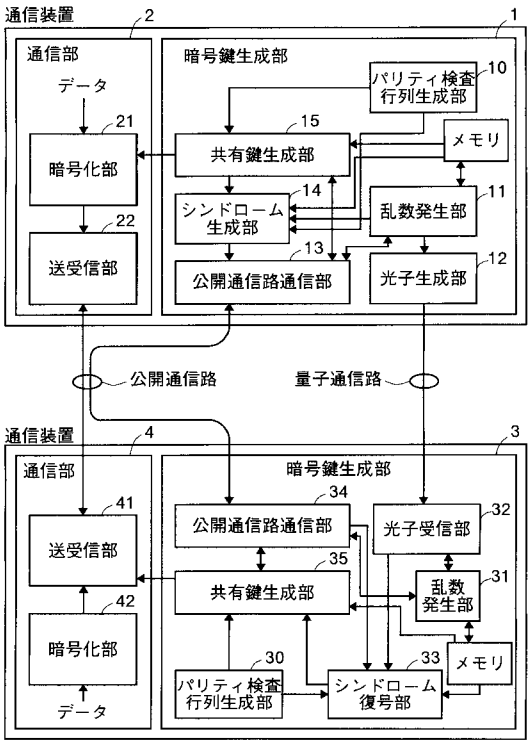
【符号の説明】

【００９３】

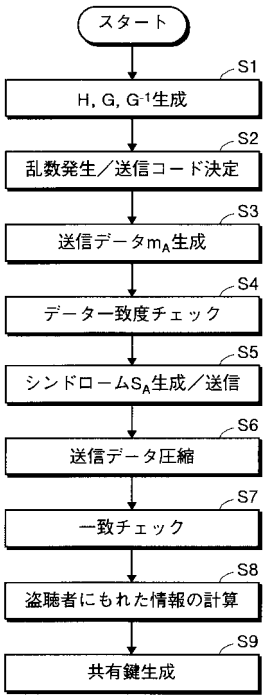
１，３　暗号鍵生成部
２，４　通信部
１０，３０　パリティ検査行列生成部
１１，３１　乱数発生部
１２　光子生成部
１３，３４　公開通信路通信部
１４　シンドローム生成部
１５，３５　共有鍵生成部
２１，４２　暗号化部
２２，４１　送受信部

３２　光子受信部
３３　シンドローム復号部

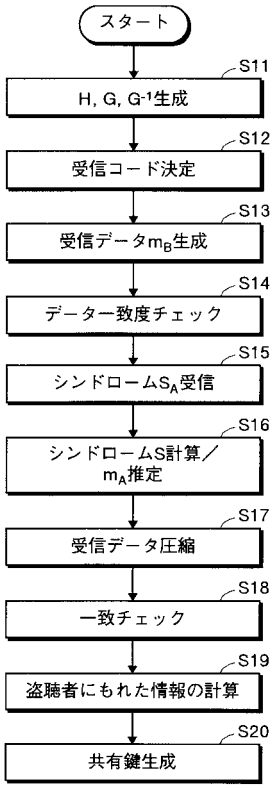
【図１】



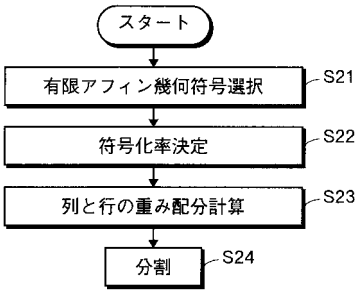
【図２－１】



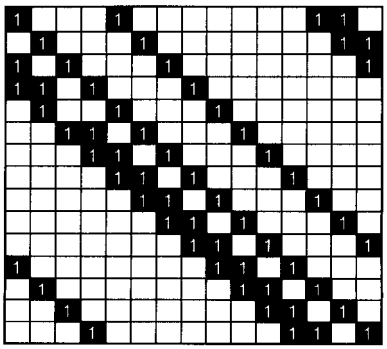
【図２－２】



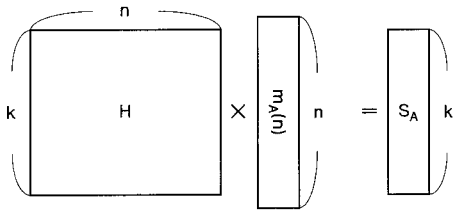
【図３】



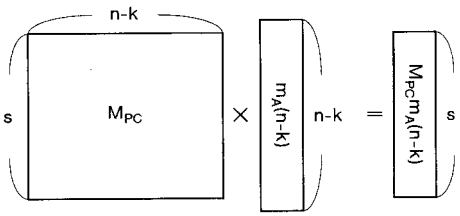
【図４】



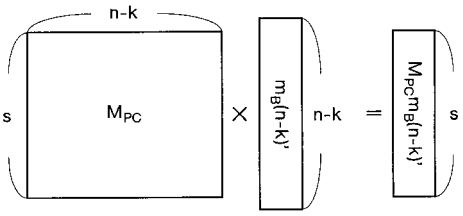
【図５】



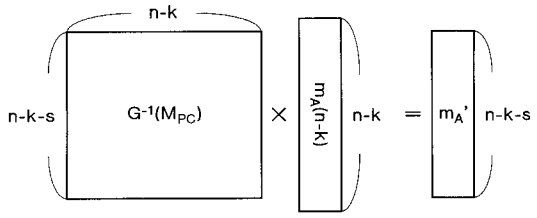
【図６－１】



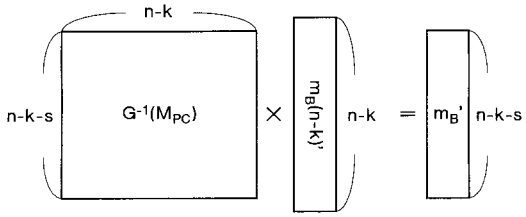
【図６－２】



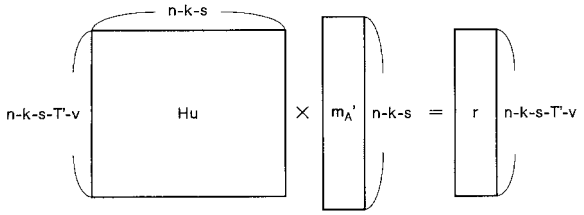
【図７－１】



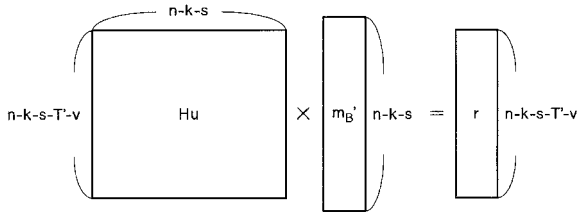
【図７－２】



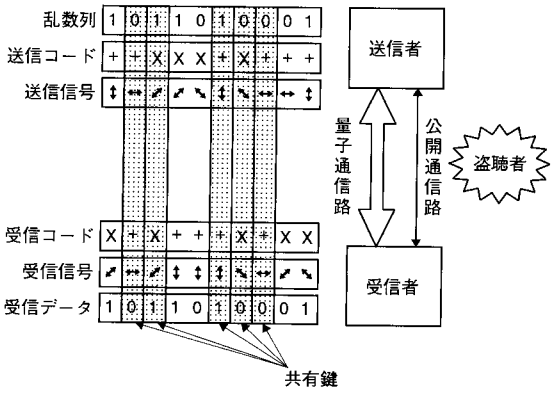
【図８－１】



【図８－２】



【図９】



フロントページの続き

(56)参考文献 特開２００４－１１２２７８（ＪＰ，Ａ）
富田 章久，量子情報処理パラダイム，経営の科学 オペレーションズ・リサーチ 第４７巻第５号 Communications of the Operations Research Society of Japan，日本，社団法人日本オペレーションズ・リサーチ学会，第47巻，３２２頁－３２７頁

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ 9／１２
Ｈ０４Ｌ 9／０８