

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2006-54638

(P2006-54638A)

(43) 公開日 平成18年2月23日(2006.2.23)

(51) Int. Cl.		F I		テーマコード (参考)
HO4L	9/12	(2006.01)	HO4L 9/00 631	5J104
HO4L	9/08	(2006.01)	HO4L 9/00 601C	
			HO4L 9/00 601E	

審査請求 有 請求項の数 8 O L (全 21 頁)

(21) 出願番号	特願2004-234258 (P2004-234258)	(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
(22) 出願日	平成16年8月11日(2004.8.11)	(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
		Fターム(参考)	5J104 AA05 AA16 EA04 EA15 EA16 JA03 NA02 NA37

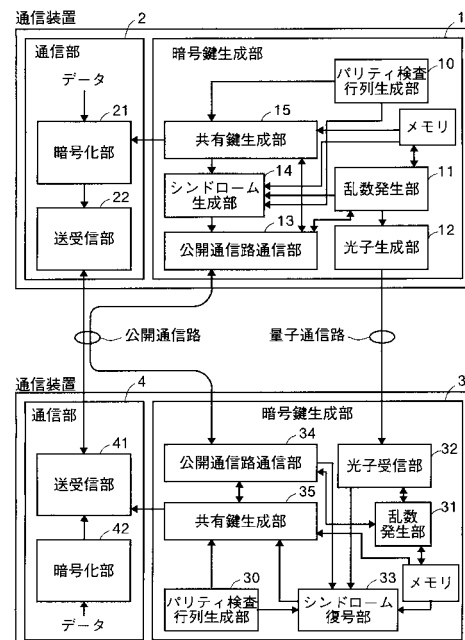
(54) 【発明の名称】 量子鍵配送方法および通信装置

(57) 【要約】

【課題】 高度に安全性の保証された共通鍵を効率良く生成可能な量子鍵配送方法を得ること。

【解決手段】 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。

【選択図】 図1



【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

10

20

30

40

50

、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、

10

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通信装置。

【請求項7】

20

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、

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、

40

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機能と、

50

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

10

20

30

40

50

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)。

【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, 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。

10

【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。

20

【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。

30

【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。

40

【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】

50

【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。

10

20

【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。

30

【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。

40

【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

50

)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。

10

【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。

20

30

【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。

40

50

【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

10

20

30

40

50

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 \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「Regular-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 $rate$ ($1 - \text{シンドローム長} / \text{鍵の長さ}$) 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 \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)。

【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 \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、

$B_1(x) = \{1\ 32\ 114\ 136\ 149\ 223\ 260\ 382\ 402\ 438\ 467\ 507\ 574\ 579\ 588\ 622\ 634\ 63$

10

20

30

40

50

7 638 676 717 728 790 851 861 879 947 954 971 977 979 998}

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、

$R_1(n) = \{1\ 114\ 574\ 637\ 851\ 879\ 977\ 979\}$

$R_2(n) = \{32\ 136\ 402\ 467\ 588\ 728\ 861\ 971\}$

$R_3(n) = \{149\ 260\ 382\ 438\ 579\ 638\ 717\ 998\}$

$R_4(n) = \{223\ 507\ 622\ 634\ 676\ 790\ 947\ 954\}$

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 \times k 行) を生成する。 10

【0038】

上記のように、パリティ検査行列 H 、生成行列 G 、 G^{-1} ($G^{-1} \cdot G = I$: 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) 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 20

【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 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)。

【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 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。 30

【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 40

【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 $m_A[C]$)。 50

【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 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 $m_A [C]$ 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 1 5 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。

10

【0044】

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 $m_B [C]$ 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、鍵長を長くすることができる。

【0045】

その後、共有鍵生成部 1 5 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 3 5 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。

20

【0046】

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 p^* を導入した。

30

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

【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 $P_r [P_E - P_T]$ の上限値 \hat{P}_r は、セキュリティパラメータ p^* を用いて、下記（2）式で与えられる。なお、下記上限値 \hat{P}_r 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 \hat{P}_0, \hat{P}_1 についても同様である。

$$\hat{P}_r = e \times p (- 2 n_R (p^*)^2) P_r [P_E - P_T] \quad \dots (2)$$

【0048】

また、共有鍵生成部 3 5 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、 \hat{P}_r を固定値とし、 \hat{P}_r 以下となるようなセキュリティパラメータ p^* を求めているが、これに限らず、 p^* を固定とし、エラー確率 P_E を満たすような \hat{P}_r を求めることとしてもよい。

40

【0049】

つぎに、送信側の通信装置では、シンドローム生成部 1 4 が、パリティ検査行列 $H (n \text{ 列} \times k \text{ 行})$ 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 S 5）。図 5 は、シンドローム生成部 1 4 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 $S_A (k \text{ ビット分の情報})$ 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 3 4 にて $m_A (n)$ のシンドローム S_A を受信し

50

、それをシンドローム復号部 33 に通知する (ステップ S 15)。

【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 S 16)。ここでは、

$$m_B(n) = m_A(n) + e \text{ (雑音等)} \quad \dots (3)$$

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。

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

【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 S 5 およびステップ S 15 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 S 17)。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 (5) 式により受信データ $m_B(n - k)'$ を生成する。

$$m_B(n - k)' = G^{-1} m_B(n)' \quad \dots (5)$$

【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 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 (6) 式により送信データ $m_A(n - k)$ を生成する。

$$m_A(n - k) = G^{-1} m_A(n) \quad \dots (6)$$

【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 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。

【0054】

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「 $M_{PC} G = 0$ 」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)。

【0055】

10

20

30

40

50

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 $m_A(n-k)$ 」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 $M_{PC} \times$ 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。

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

【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。

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

【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は、

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

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: $0^\circ, 45^\circ, 90^\circ, 135^\circ$)、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。

$$T = |m_A'| H_2(P_E) \\ H_2(P_E) = -P_E \log P_E - (1-P_E) \log (1-P_E) \quad \dots (10)$$

【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。

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

【0062】

10

20

30

40

50

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 $\rho_{00}, \rho_{01}, \rho_{10}, \rho_{11}$ と表す。この量子状態 $\rho_{00}, \rho_{01}, \rho_{10}, \rho_{11}$ 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 $\rho_{00}, \rho_{01}, \rho_{10}, \rho_{11}$ 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。

$$P_F^* = P_E + n_K T_r | \dots | / 2 = P_E + n_K T_r (\dots^T) / 2$$

$$= (\rho_{00} + \rho_{01} - \rho_{10} - \rho_{11}) / 2 \dots (12)$$

【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 ρ^* の計算式を下記(13)式と差し替える。

$$P_F^* = P_E + n_K T_r | \dots | / 4 = P_E + n_K T_r (\dots^T) / 4$$

$$\rho^* = 1 - (1 - \rho^*)^2$$

$$\rho^* = \exp (- n_R (\dots p^*)^2) \dots (13)$$

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： $S(\rho) = -T_r \log \dots$ を用いて、下記(14)式および(15)式により計算する。

$$C_0 = S(\rho_0) - (S(\rho_{00}) + S(\rho_{01})) / 2$$

$$\rho_0 = (\rho_{00} - \rho_{01}) / 2 \dots (14)$$

$$C_1 = S(\rho_1) - (S(\rho_{10}) + S(\rho_{11})) / 2$$

$$\rho_1 = (\rho_{10} - \rho_{11}) / 2 \dots (15)$$

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

10

20

30

40

50

/ 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。

$$P_{00} = P_{F10} + (1 - P_{F11}) = p_0 E_0 + (1 - p_0) (I - E_0) \quad \dots (16)$$

$$P_{00}' = P_{F11} + (1 - P_{F10}) = p_0' E_0' + (1 - p_0') (I - E_0') \quad \dots (17)$$

$$P_{10} = P_{F00} + (1 - P_{F01}) = p_1 E_1 + (1 - p_1) (I - E_1) \quad \dots (18)$$

$$P_{10}' = P_{F01} + (1 - P_{F00}) = p_1' E_1' + (1 - p_1') (I - E_1') \quad \dots (19)$$

10

【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 $|00\rangle, |01\rangle$ 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。

$$q_0 = \max \{ T_{r00} E_0, 1 - T_{r00} E_0, T_{r01} E_0, 1 - T_{r01} E_0 \} \quad \dots (20)$$

$$q_0' = \max \{ T_{r00} E_0', 1 - T_{r00} E_0', T_{r01} E_0', 1 - T_{r01} E_0' \} \quad \dots (21)$$

$$q_1 = \max \{ T_{r10} E_1, 1 - T_{r10} E_1, T_{r11} E_1, 1 - T_{r11} E_1 \} \quad \dots (22)$$

20

$$q_1' = \max \{ T_{r10} E_1', 1 - T_{r10} E_1', T_{r11} E_1', 1 - T_{r11} E_1' \} \quad \dots (23)$$

【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】

$$p(m_E | m_A) \leq 2^{n_K H_2(p_{\max} + \Delta p_0^*)} q_{\max}^{n_K} \quad \dots (24)$$

30

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

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

...

【0071】

ただし、 p_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 δ_0^* は、下記(25)式で与えられる。

40

$$\delta_0^* = \exp(-2 n_K (\delta_0^*)^2) \quad \dots (25)$$

【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。

$$H(m_E | m_A) \geq -\log \max p(m_E | m_A) = -n_K (H_2(p_{\max} + \delta_0^*) + \log q_{\max}) \quad \dots (26)$$

【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。

50

$$\begin{aligned}
I(m_A : m_E) &= H(m_E) - H(m_E | m_A) \\
&= n_K + n_K (H_2(p_{\max} + p_0^*) + \log_2 q_{\max}) \\
&= n_K (H_2(p_{\max} + p_0^*) + \log_2 q_{\max}) \\
&= I_{\max}(m_A : m_E) \quad \dots (27)
\end{aligned}$$

【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】

$$T = (1 - \epsilon_T^*) \max_{P_F \leq P_F^*} \{I_{\max}(m_A : m_E)\} + \epsilon_T^* (n_0 C_0 + n_1 C_1)$$

$$\epsilon_T^* = \epsilon^* + \epsilon_0^* + n_K \text{Tr}|\Delta|$$

... (28)

【0076】

なお、上記 ϵ_T^* は、生起確率がそれぞれ ϵ^* 、 ϵ_0^* 、 $n_K \text{Tr}|\Delta|$ 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 p_0^* 、 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。

$$T_0 = n_0 (H_2(p_0 + p_0^*) + \log_2 q_0) \quad \dots (29)$$

$$T_0' = n_0 (H_2(p_0' + p_0^*) + \log_2 q_0')$$

$$T_1 = n_1 (H_2(p_1 + p_1^*) + \log_2 q_1) \quad \dots (31)$$

$$T_1' = n_1 (H_2(p_1' + p_1^*) + \log_2 q_1') \quad \dots (32)$$

$$H_2(p) = -p \log p - (1-p) \log (1-p) \quad \dots (33)$$

【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】

$$T = (1 - \epsilon_T^*) \max_{P_F \leq P_F^*} \{ \max\{T_0, T_0'\} + \max\{T_1, T_1'\} \} + \epsilon_T^* (n_0 C_0 + n_1 C_1)$$

$$\epsilon_T^* = 1 - (1 - \epsilon^*) (1 - \epsilon_0^*) (1 - \epsilon_1^*) (1 - n_K \text{Tr}|\Delta|)$$

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

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

10

20

30

40

50

... (3 4)

【 0 0 8 0 】

なお、上記で用いたセキュリティパラメータ p^* , p_0^* , 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。

【 0 0 8 1 】

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。

【 0 0 8 2 】

【数 4】

$$S_0 = \{q_0^{w(x)}(1-q_0)^{n_0-w(x)} \mid x \in \{0,1\}^{n_0}\} \quad 20$$

... (3 5)

【 0 0 8 3 】

【数 5】

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

... (3 6)

【 0 0 8 4 】

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。

【 0 0 8 5 】

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 S 8 およびステップ S 19 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 S 9, ステップ S 20)。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。

【 0 0 8 6 】

具体的には、たとえば、共有鍵生成部 15 が、 $\{0,1\}^{n-k-s} \{0,1\}^{n-k-s-T-v}$ 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ることにより実現できる。そして、ハッシュ関数 H_u を、受信側の通信装置に対して公開通信路を介して送信する。なお、この処理は、受信側の通信装置の共有鍵生成部 35 にて行うこととしてもよい。

【 0 0 8 7 】

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。

$$r = H u m_A \quad \dots (37)$$

【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。

$$r = H u m_B \quad \dots (38)$$

【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 $(1 - \quad)$ 以上で、かつ盗聴者にもれる情報量が $(2^{-v} / 1n2)$ 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

10

20

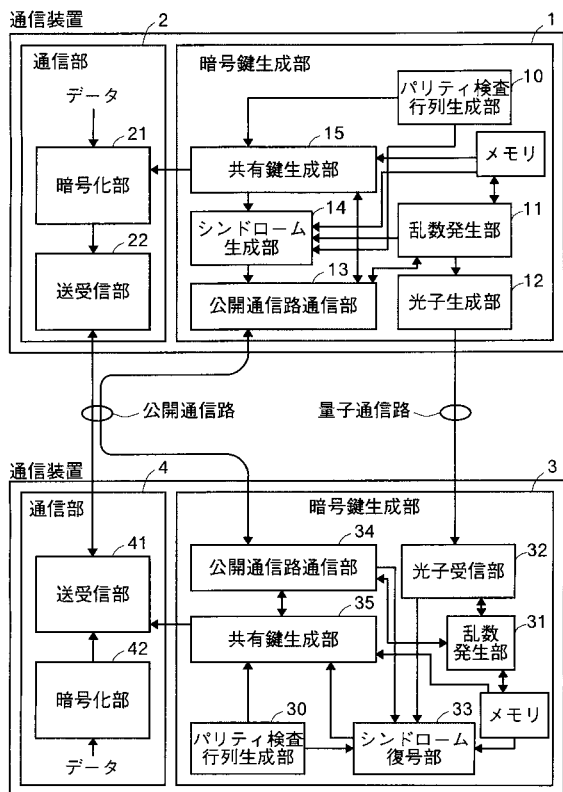
30

40

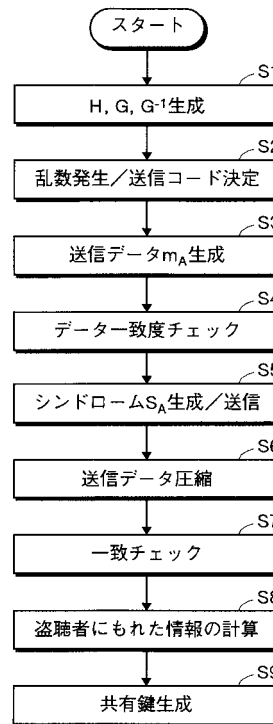
50

- 1 2 光子生成部
- 1 3 , 3 4 公開通信路通信部
- 1 4 シンドローム生成部
- 1 5 , 3 5 共有鍵生成部
- 2 1 , 4 2 暗号化部
- 2 2 , 4 1 送受信部
- 3 2 光子受信部
- 3 3 シンドローム復号部

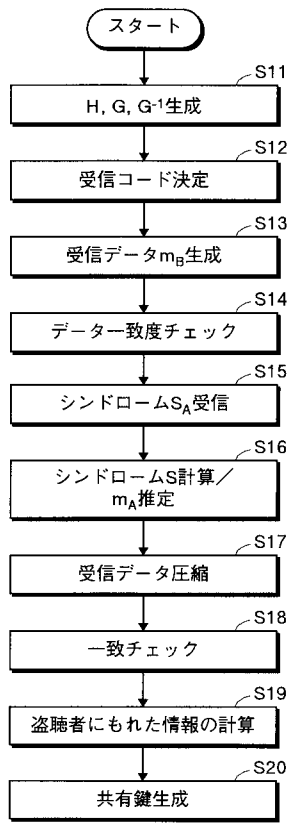
【 図 1 】



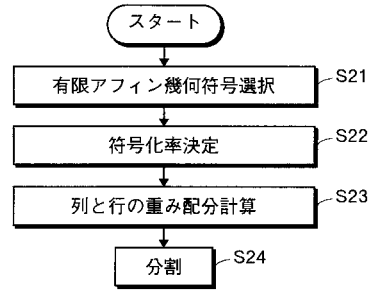
【 図 2 - 1 】



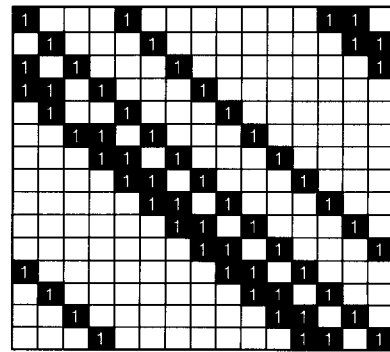
【 図 2 - 2 】



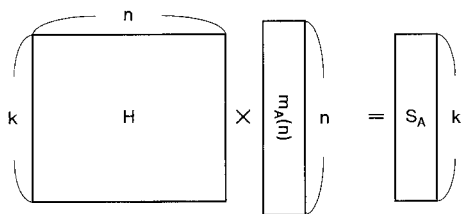
【 図 3 】



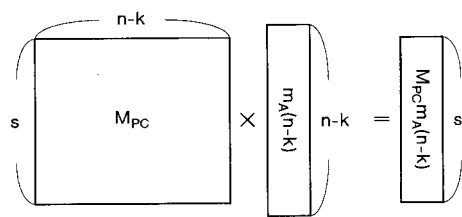
【 図 4 】



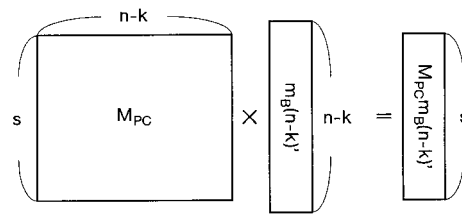
【 図 5 】



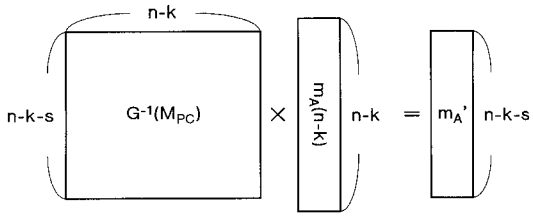
【 図 6 - 1 】



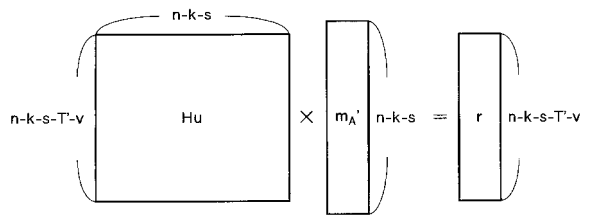
【 図 6 - 2 】



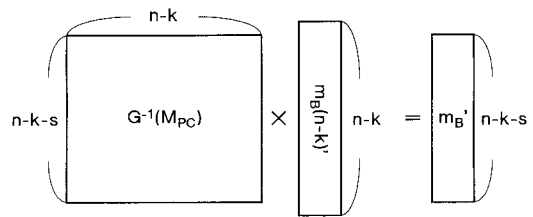
【 図 7 - 1 】



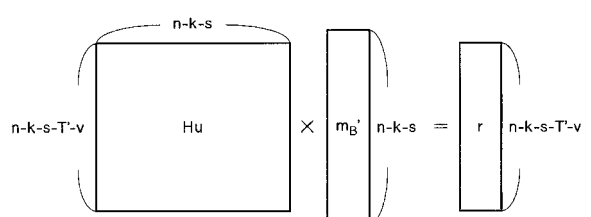
【 図 8 - 1 】



【 図 7 - 2 】



【 図 8 - 2 】



【 図 9 】

