

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4662040号
(P4662040)

(45) 発行日 平成23年3月30日 (2011.3.30)

(24) 登録日 平成23年1月14日 (2011.1.14)

(51) Int.Cl.		F I			
H O 4 L	7/08	(2006.01)	H O 4 L	7/08	Z
H O 4 L	9/12	(2006.01)	H O 4 L	9/00	6 3 1
H O 4 L	9/08	(2006.01)	H O 4 L	9/00	6 O 1 C
			H O 4 L	9/00	6 O 1 E

請求項の数 13 (全 25 頁)

(21) 出願番号	特願2005-200974 (P2005-200974)	(73) 特許権者	000004237
(22) 出願日	平成17年7月8日 (2005.7.8)		日本電気株式会社
(65) 公開番号	特開2007-20013 (P2007-20013A)		東京都港区芝五丁目7番1号
(43) 公開日	平成19年1月25日 (2007.1.25)	(74) 代理人	100097157
審査請求日	平成20年6月11日 (2008.6.11)		弁理士 桂木 雄二
(出願人による申告) 国等の委託研究の成果に係る特許出願 (平成17年度N I C T高度通信・放送研究開発における委託研究) は産業再生法第30条の適用を受けるもの		(72) 発明者	田中 聡寛
			東京都港区芝五丁目7番1号 日本電気株式会社社内
		(72) 発明者	田島 章雄
			東京都港区芝五丁目7番1号 日本電気株式会社社内
		(72) 発明者	高橋 成五
			東京都港区芝五丁目7番1号 日本電気株式会社社内

最終頁に続く

(54) 【発明の名称】 通信システムおよびその同期制御方法

(57) 【特許請求の範囲】

【請求項1】

複数の通信チャネルにより接続された第1通信器と第2通信器との間で共有すべきデータのビット対応を確立する同期制御方法において、

a) 前記第1通信器は、それぞれビットタイミングが相対的に定められた複数のビット列からなる第1データを一の通信チャネルを通して前記第2通信器へ送信し、前記第2通信器は前記一の通信チャネルを通して前記第1通信器から受信した第2データを保存し、

b) 前記第1通信器と前記第2通信器との間のビットタイミング差である第1同期ずれと、前記第2通信器内のビットタイミング差である第2同期ずれと、を仮設定し、

c) 仮設定された前記第1同期ずれおよび前記第2同期ずれを所定調整範囲内で順次変更しながら、前記第2データの一部とそれに対応する前記第1データとを照合し、

d) 前記照合結果に基づいて前記第1同期ずれおよび前記第2同期ずれを確定する、ことを特徴とする同期制御方法。

【請求項2】

前記c)は、

c. 1) 仮設定された前記第1同期ずれおよび仮設定された前記第2同期ずれを用いて、前記第2データの一部のビットタイミングにそれぞれ対応する前記第1データのビットタイミングを決定し、

c. 2) 前記第2データの前記一部の値とそれらに対応する前記第1データの値とを照合し、

10

20

c. 3) 仮設定された前記第1同期ずれおよび仮設定された前記第2同期ずれの少なくとも一方を所定ステップ変化させ、

c. 4) 前記c. 1)～c. 3)を前記所定調整範囲内で繰り返す、
ことを特徴とする請求項1に記載の同期制御方法。

【請求項3】

前記d)は、前記照合結果のうち最も良好な照合結果をもたらす仮設定された第1同期ずれおよび第2同期ずれを同期確立された前記第1同期ずれおよび前記第2同期ずれとして決定する、ことを特徴とする請求項1または2に記載の同期制御方法。

【請求項4】

前記c)は、

c. 1) 仮設定された前記第1同期ずれおよび仮設定された前記第2同期ずれを用いて、前記第2データの一部のビットタイミングにそれぞれ対応する前記第1データのビットタイミングを決定し、

c. 2) 前記第2データの前記一部の値とそれらに対応する前記第1データの値とを照合し、

c. 3) 前記照合結果が所定の閾値より良好でない場合には、仮設定された前記第1同期ずれおよび仮設定された前記第2同期ずれの少なくとも一方を所定ステップ変化させ、

c. 4) 前記c. 1)～c. 3)を前記所定調整範囲内で繰り返し、

前記d)は、

前記c. 2)で得られた前記照合結果が前記所定の閾値より良好である場合には、当該照合結果をもたらす仮設定された第1同期ずれおよび第2同期ずれを同期確立された前記第1同期ずれおよび前記第2同期ずれとして決定する、

ことを特徴とする請求項1に記載の同期制御方法。

【請求項5】

前記所定調整範囲内で、前記c. 2)で得られた前記照合結果が前記所定の閾値より良好にならなかった場合には処理を中断することを特徴とする請求項4に記載の同期制御方法。

【請求項6】

前記c)およびd)は、

e. 1) 仮設定された前記第1同期ずれおよび仮設定された前記第2同期ずれを用いて、前記第2データの一部のビットタイミングにそれぞれ対応する前記第1データのビットタイミングを決定し、

e. 2) 前記第2データの前記一部の値とそれらに対応する前記第1データの値とを照合し、

e. 3) 前記照合結果が第1閾値より良好でない場合には、仮設定された前記第1同期ずれを所定ステップ変化させ、

e. 4) 前記e. 1)～e. 3)を前記第1同期ずれの所定調整範囲内で繰り返し、

e. 5) 前記e. 2)で得られた前記照合結果が前記第1閾値より良好である場合には、当該照合結果をもたらす仮設定された第1同期ずれを同期確立された前記第1同期ずれとして決定し、

e. 6) 前記e. 2)で得られた前記照合結果が前記第1閾値より良好で、かつ、第2閾値より良好でない場合には、仮設定された前記第2同期ずれを所定ステップ変化させ、

e. 7) 前記第2データの前記一部の値とそれらに対応する前記第1データの値とを照合し、

e. 8) 前記e. 7)で得られた前記照合結果が前記第2閾値より良好でない場合には、前記e. 6)～e. 7)を前記第2同期ずれの所定調整範囲内で繰り返し、

e. 9) 前記e. 7)で得られた前記照合結果が前記第2閾値より良好である場合には、当該照合結果をもたらす仮設定された第2同期ずれを同期確立された前記第2同期ずれとして決定する、

ことを特徴とする請求項1に記載の同期制御方法。

10

20

30

40

50

【請求項 7】

前記第 1 同期ずれの所定調整範囲内で前記 e. 2) で得られた前記照合結果が前記第 1 閾値より良好にならなかった場合、あるいは、前記第 2 同期ずれの所定調整範囲内で前記 e. 7) で得られた前記照合結果が前記第 2 閾値より良好にならなかった場合には処理を中断することを特徴とする請求項 6 に記載の同期制御方法。

【請求項 8】

複数の通信チャネルにより接続された第 1 通信器と第 2 通信器との間で共有すべきデータのビット対応を確立する同期制御方法において、

前記第 1 通信器は、

それぞれビットタイミングが相対的に定められた複数のビット列からなる第 1 データを一の通信チャネルを通して前記第 2 通信器へ送信し、

前記第 1 通信器と前記第 2 通信器との間のビットタイミング差である第 1 同期ずれを仮設定し、

前記第 2 通信器は、

前記一の通信チャネルを通して前記第 1 通信器から受信した第 2 データを保存し、

前記第 2 通信器内のビットタイミング差である第 2 同期ずれを仮設定し、

仮設定された第 2 同期ずれが所定調整範囲で変化した場合の前記第 2 データの一部を前記第 1 通信器へ送信し、

前記第 1 通信器は、

仮設定された第 1 同期ずれを所定調整範囲内で変化させながら、前記第 2 通信器から受信した前記第 2 データの一部とそれに対応する前記第 1 データとを照合し、

前記照合結果に基づいて前記第 1 同期ずれおよび前記第 2 同期ずれを確定する、

ことを特徴とする同期制御方法。

【請求項 9】

複数の通信チャネルにより接続された第 1 通信器と第 2 通信器との間で共有すべきデータのビット対応を確立する同期制御システムにおいて、

前記第 2 通信器は、

それぞれビットタイミングが相対的に定められた複数のビット列からなる第 1 データを一の通信チャネルを通して前記第 1 通信器から受信する受信手段と、

受信したデータを第 2 データを格納する格納手段と、

前記第 2 通信器内のビットタイミング差である第 2 同期ずれを仮設定し、仮設定された第 2 同期ずれが所定調整範囲で変化した場合の前記第 2 データの一部を生成する生成手段と、

前記第 2 データの一部を前記第 1 通信器へ送信する送信手段と、

を有し、

前記第 1 通信器は、前記第 1 通信器と前記第 2 通信器との間のビットタイミング差である第 1 同期ずれを仮設定し、仮設定された第 1 同期ずれを所定調整範囲内で変化させながら、前記第 2 通信器から受信した前記第 2 データの一部とそれに対応する前記第 1 データとを照合し、前記照合結果に基づいて前記第 1 同期ずれおよび前記第 2 同期ずれを確定する制御手段を有する、

ことを特徴とする同期制御システム。

【請求項 10】

送信器と受信器とが光伝送路を介して接続され、複数の通信チャネルにより通信を行う通信システムにおいて、

前記送信器は、

それぞれビットタイミングが相対的に定められた複数のビット列からなる第 1 データおよび第 2 データを格納する第 1 格納手段と、

前記第 1 および第 2 データに従って光信号を変調する第 1 変調手段と、

変調された光信号を一の通信チャネルを通して前記受信器へ送信する第 1 通信手段と

、

前記受信器との間で他の通信チャネルを通してデータ通信を行うための第1送受信手段と、

を有し、

前記受信器は、

第3データを格納する第2格納手段と、

前記一の通信チャネルを通して前記送信器から光信号を受信する第2通信手段と、

前記受信した光信号を前記第3データに従って変調する第2変調手段と、

前記受信した光信号と前記第2変調手段により変調された光信号とに基づいて第4データを検出する光検出手段と、

前記第4データを格納する第3格納手段と、

10

前記送信器との間で前記他の通信チャネルを通してデータ通信を行うための第2送受信手段と、

前記第2変調手段と前記光検出手段との間のビットタイミング差である第2同期ずれを仮設定し、仮設定された第2同期ずれが所定調整範囲で変化した場合の前記第3データおよび第4データの一部を前記送信器へ送信する受信側制御手段と、

を有し、

前記送信器は、さらに、

前記第1変調手段と前記光検出手段との間のビットタイミング差である第1同期ずれを仮設定し、仮設定された第1同期ずれを所定調整範囲内で変化させながら、前記受信器から受信した前記第3データおよび前記第4データの一部と、それに対応する前記第1データおよび前記第2データと、を照合し、前記照合結果に基づいて前記第1同期ずれおよび前記第2同期ずれを確定する送信側制御手段を有する、

20

ことを特徴とする通信システム。

【請求項11】

請求項10に記載の通信システムにおける送信器。

【請求項12】

請求項10に記載の通信システムにおける受信器。

【請求項13】

コンピュータに、複数の通信チャネルにより接続された第1通信器と第2通信器との間で共有すべきデータのビット対応を確立する同期制御を実行させるためのプログラムにおいて、

30

それぞれビットタイミングが相対的に定められた複数のビット列からなる第1データを一の通信チャネルを通して第1通信器から第2通信器へ送信することで前記第2通信器が受信したデータを第2データとして保存するステップと、

前記第1通信器と前記第2通信器との間のビットタイミング差である第1同期ずれと、前記第2通信器内のビットタイミング差である第2同期ずれと、を仮設定するステップと、

仮設定された前記第1同期ずれおよび前記第2同期ずれを所定調整範囲内で順次変更しながら、前記第2データの一部とそれに対応する前記第1データとを照合するステップと、

40

前記照合結果に基づいて前記第1同期ずれおよび前記第2同期ずれを確定するステップと、

を有することを特徴とする同期制御プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は送信器から受信器へ伝送路を通してデータを送信する通信システムにかかり、特に送信器と受信器との間で送受信データのビット対応を確立するための同期制御方法およびシステムに関する。

50

【背景技術】

【0002】

急激な成長を続けるインターネットは、便利である反面、その安全性に大きな不安を抱えており、通信の秘密保持の為に暗号技術の必要性が高まっている。現在一般的に用いられている暗号方式は、DES(Data Encryption Standard)やTriple DESといった秘密鍵暗号と、RSA(Rivest Shamir Adleman)や楕円曲線暗号の様な公開鍵暗号に分類される。しかしこれらは「計算の複雑性」を元にその安全性を保証する暗号通信方法であり、膨大な計算量や暗号解読アルゴリズムの出現によって解読されてしまう危険性を常に孕んでいる。こういった背景の下、量子暗号鍵配布システム(QKD)は、「絶対に盗聴されない」暗号鍵配布技術として注目されている。

10

【0003】

QKDでは一般に通信媒体として光子を使用し、その偏光、位相等の量子状態に情報を載せて伝送を行う。伝送路の盗聴者は伝送中の光子をタッピングする等して情報を盗み見るが、Heisenbergの不確定性原理により、1度観測されてしまった光子を完全に観測前の量子状態に戻すことは不可能となり、このことによって正規の受信者が検出する受信データの統計値に変化が生じる。この変化を検出することにより受信者は伝送路における盗聴の有無を検出することができる。

【0004】

光子の位相を利用した量子暗号鍵配布方法の場合、送信者および受信者（以下、通例に従ってそれぞれ「Alice」および「Bob」称する。）で光学干渉計を組織し、各々の光子にAliceおよびBobでそれぞれランダムに位相変調を施す。この変調位相深さの差によって出力0あるいは1が得られ、その後、出力データを測定したときの条件の一部分をAliceとBobとで照合することによって最終的にAlice-Bob間で同一ビット列を共有することができる。次に、BB84プロトコルと呼ばれる最も代表的な量子暗号鍵配送アルゴリズムについて簡単に説明する（非特許文献1参照）。

20

【0005】

図11はBB84プロトコルによる量子暗号鍵配布方法の概念を示す模式図である。ここではAlice141とBob143とが光伝送路142で接続されているものとする。

【0006】

この方法では、Alice141が乱数源を2つ持ち、片側(乱数1)で0/1の暗号鍵データを表し、もう一方(乱数2)で乱数1の情報をコーディングする方法を決定する。光子の位相を利用した量子暗号鍵配布方法では、位相0が暗号鍵“0”、位相 π が暗号鍵“1”の組を表すコーディングセット（以下、「+基底」と称する。）と、位相 $\pi/2$ が暗号鍵“0”、位相 $3\pi/2$ が暗号鍵“1”を表すコーディングセット（以下、「×基底」と称する。）と、の2組の基底を乱数2で選択する。つまり1つの光子に対して、0、 $\pi/2$ 、 π 、 $3\pi/2$ の4通りの変調をランダムに施してBobへと送信する。

30

【0007】

一方、Bob143では基底に対応する乱数源（乱数3）を持ち、Alice141より送られてきた光子に対してデコードを行う。乱数3の値が“0”である場合、光子に対して位相0（+基底）の変調を、“1”である時には位相 $\pi/2$ （×基底）の変調を施す。ここで光学干渉計出力として得られた乱数を乱数4とする。

40

【0008】

Alice/Bob両者が施した変調の基底が同一である場合（乱数2＝乱数3）、乱数1の値をBobは正しく検出することができ（乱数1＝乱数4）、異なる場合（乱数2≠乱数3）には乱数1の値に依らずBobは乱数4として0/1の値をランダムに得る。乱数1/2/3は共に1ビット毎に変化する乱数であるから、基底が一致する確率と不一致である確率は共に50%となるが、後段の基底照合(Basis Reconciliation)によって基底が不一致となるビットを削除するから、Alice141とBob143は乱数1に対応する0/1ビット列を共有することができる。

50

【0009】

しかしながら、上記のようにして共有したビット列には伝送路142や受信器に起因する誤りが含まれており、この誤りを訂正する誤り訂正処理が必要となる。加えて伝送路途中に存在する盗聴者が光子情報を覗き見た場合にも共有ビット列に誤りが発生する。したがって、最終的に使用する暗号鍵を共有するためには、誤りを訂正する誤り訂正処理だけでなく、誤りの頻度（誤り率）に基づいて、盗聴されたと想定し得る情報量を削減する秘匿増強処理が必要となる。なお「盗聴されたと想定し得る情報量」を推定する方法は、非特許文献2および3に記載されている。

【0010】

図12は、一般的な量子暗号鍵生成の流れを示すフローチャートである。Aliceより送られた暗号鍵の元乱数（鍵の素）は、量子暗号鍵配布（単一光子伝送）S1によって大部分の情報量が失われる。この段階でAliceとBobで共有されている鍵を生鍵(Raw Key)と呼び、上述した基底照合S2を行った後で半減した暗号鍵を選別鍵(Sifted Key)と呼ぶ。この後、量子鍵配布段階で混入した誤りを訂正する誤り訂正(Error Correction)S3過程と、盗聴者に漏れていると想定され得る情報量を削ぎ落とす秘匿増強(Privacy Amplification)S4とを経て、残りが実際に暗号鍵として使用される最終鍵となる。このような量子暗号鍵を共有する技術がいくつか提案されている。

【0011】

たとえば、特開2000-174747号公報（特許文献1）には、量子チャネルと古典チャネルとを用いて送信側および受信側で秘密鍵を共有する量子暗号装置が開示されている。具体的には、送信者側で乱数表からビット値を取り出し、それによって光パルスを微小変調し、量子チャネルを通して送信する。受信者側は、別途乱数表からビット値を取り出し、それによって受信した光パルスを再変調し、光子が検出されたか否かを古典チャネルを通して送信者側へ通知する。送信者側では、受信者側で光子が検出されたビット値のみを用いて乱数表を構成する。これによって、送信者および受信者に共通の乱数表が記憶されたこととなる。さらに、盗聴の有無を確認するために、共通乱数表から適当な割合で照合ビットを抽出し、それらを古典チャネルを通して照合し、十分な数のビットが一致すれば、照合ビットを除いたビット列を共有の秘密鍵として使用する（明細書段落0036～0039参照）。

【0012】

特開2004-112278号公報（特許文献2）には、量子通信路（量子チャネル）を通ることによって発生するデータ誤りを除去することで、共通鍵の生成効率を向上させる量子鍵配送方法が開示されている。より詳しくは、送信側は、乱数列（送信データ）およびランダムに決定された基底（送信コード）により規定された量子状態で光子を量子通信路を通して送信する。受信側では、受信した光子を測定し、その測定結果とランダムに決定された基底（受信コード）とにより規定された受信データを得る。そして、公開通信路を通した手順で基底の一致したビットのみを残すことで、送信側および受信側に共有情報が記憶される。続いて、送信側はパリティ検査行列および送信データから生成される所定ビット数の誤り訂正情報を公開通信路を通して送信する。受信側は、受信した誤り訂正情報、上記受信データおよび同一のパリティ検査行列を用いて、受信データの誤りを訂正する。誤り訂正で公開された情報に応じて、訂正後の共有情報の一部が捨てられ、残りの情報を共有の暗号鍵として生成する（明細書段落0016～0020、図1、図2、図9参照）。

【0013】

【特許文献1】特開2000-174747号公報（明細書段落0036～0039参照）

【特許文献2】特開2004-112278号公報（明細書段落0016～0020、図1、図2、図9参照）

【非特許文献1】"IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, India, p.175", Bennett, Brassard

10

20

30

40

50

【非特許文献 2】"Estimates for practical quantum cryptography", Physical Review A, Vol.59, No.5, pp.3301, N. Lutkenhaus

【非特許文献 3】"Eavesdropping on practical quantum cryptography" quantum-ph / 0211155, M. Williamson

【非特許文献 4】"Automated 'plug & play' quantum key distribution", Electronics Letters, Vol.34, No.22, pp2116-2117, G. Ribordy

【非特許文献 5】"Balanced, gated-mode photon detector for quantum-bit discrimination at 1550nm" Optics letters, vol. 27 (2002) pp1827-1829, A. Tomita

【非特許文献 6】"High-Speed QKD System Synchronized by Automatic Phase-Alignment Mechanism", OFC2005, OWI4, W. Maeda

【非特許文献 7】"Temperature independent QKD system using alternative-shifted phase modulation method", ECOC2004, Tu4.5.3, A. Tanaka

【発明の開示】

【発明が解決しようとする課題】

【0014】

しかしながら、上述した量子暗号鍵配布を現実世界で実現しようとする、様々な原因によって上記誤り率が上昇することがある。具体的には、単一光子に情報を載せて伝送するので伝送途中で消失するビットが多く、Alice-Bob間でのビット対応の誤認識が生じやすい。この誤認識によって誤り率が劣化し、暗号鍵の生成が行えなくなる。以下、送信側と受信側との間でビット位置の同期が取れていること、すなわちビット対応の正しい認識が成立している状態を「フレーム同期」、ビット対応が誤認識されている状態を「フレーム同期ずれ」、フレーム同期ずれをフレーム同期状態に正しく合わせる処理を「フレーム同期処理」と称す。

【0015】

上述したように、送信側と受信側で情報を共有するためには、どのビットが正しく検出され、どのビットが検出されなかったかを、送信器および受信器の双方で特定できなければならない。言い換えれば、量子暗号鍵配布システムでは送信器と受信器とでビット位置の同期を確立することが必要である。鍵生成フローにおいて、ビット位置の同期確立は大前提であり、同期が確立していないと最終鍵は生成できない。

【0016】

しかしながら、上記従来の方法では、伝送路の伸縮や装置内の処理のずれによって、フレーム同期が外れる可能性が残されている。実際の運用において同期がはずれた場合、特許文献 1 に記載された鍵生成フローでは、照合ビットが十分一致しないために、盗聴者を検出したとみなし、再度ビット位置の同期を確立し直して鍵生成を実行することとなる。これでは、それまでに量子通信で生成した鍵は無駄となり、共通鍵の生成効率がきわめて悪くなる。同様に、特許文献 2 に記載された方法においても、ビット位置の同期が外れた場合には受信データの誤り率が非常に大きくなり、共通鍵を生成できなくなる。特許文献 2 では、誤り率が大きい場合の処理については全く考慮されていない。

【0017】

特に、本発明者等は、フレーム同期ずれの原因が伝送路の伸縮などの装置間の処理ずれだけでなく受信器側の装置内の処理ずれも関係していることに注目し、正確なフレーム同期を迅速に確立する同期制御方法を提案する。

【課題を解決するための手段】

【0018】

上記目的を達成するために、本発明によれば、複数の通信チャネルにより接続された第 1 通信器と第 2 通信器との間で共有すべきデータのビット対応を確立する同期制御方法において、a) 前記第 1 通信器は、それぞれビットタイミングが相対的に定められた複数のビット列からなる第 1 データを一の通信チャネルを通して前記第 2 通信器へ送信し、前記第 2 通信器は前記一の通信チャネルを通して前記第 1 通信器から受信した第 2 データを保存し、b) 前記第 1 通信器と前記第 2 通信器との間のビットタイミング差である第 1 同期

ずれと、前記第2通信器内のビットタイミング差である第2同期ずれと、を仮設定し、c) 仮設定された前記第1同期ずれおよび前記第2同期ずれを所定調整範囲内で順次変更しながら、前記第2データの一部とそれに対応する前記第1データとを照合し、d) 前記照合結果に基づいて前記第1同期ずれおよび前記第2同期ずれを確定する、ことを特徴とする。

【0019】

本発明の一実施例によれば、前記c)は、c. 1) 仮設定された前記第1同期ずれおよび仮設定された前記第2同期ずれを用いて、前記第2データの一部のビットタイミングにそれぞれ対応する前記第1データのビットタイミングを決定し、c. 2) 前記第2データの
10 前記一部の値とそれらに対応する前記第1データの値とを照合し、c. 3) 仮設定された前記第1同期ずれおよび仮設定された前記第2同期ずれの少なくとも一方を所定ステップ変化させ、c. 4) 前記c. 1)～c. 3)を前記所定調整範囲内で繰り返す。前記d)は、前記照合結果のうち最も良好な照合結果をもたらす仮設定された第1同期ずれおよび第2同期ずれを同期確立された前記第1同期ずれおよび前記第2同期ずれとして決定する。

【0020】

本発明の他の実施例によれば、前記c)は、c. 1) 仮設定された前記第1同期ずれおよび仮設定された前記第2同期ずれを用いて、前記第2データの一部のビットタイミングにそれぞれ対応する前記第1データのビットタイミングを決定し、c. 2) 前記第2データの
20 前記一部の値とそれらに対応する前記第1データの値とを照合し、c. 3) 前記照合結果が所定の閾値より良好でない場合には、仮設定された前記第1同期ずれおよび仮設定された前記第2同期ずれの少なくとも一方を所定ステップ変化させ、c. 4) 前記c. 1)～c. 3)を前記所定調整範囲内で繰り返し、前記d)は、前記c. 2)で得られた前記照合結果が前記所定の閾値より良好である場合には、当該照合結果をもたらす仮設定された第1同期ずれおよび第2同期ずれを同期確立された前記第1同期ずれおよび前記第2同期ずれとして決定する。

【0021】

本発明の更に別の実施例によれば、前記c)およびd)は、e. 1) 仮設定された前記第1同期ずれおよび仮設定された前記第2同期ずれを用いて、前記第2データの一部のビットタイミングにそれぞれ対応する前記第1データのビットタイミングを決定し、e. 2) 前記第2データの
30 前記一部の値とそれらに対応する前記第1データの値とを照合し、e. 3) 前記照合結果が第1閾値より良好でない場合には、仮設定された前記第1同期ずれを所定ステップ変化させ、e. 4) 前記e. 1)～e. 3)を前記第1同期ずれの所定調整範囲内で繰り返し、e. 5) 前記e. 2)で得られた前記照合結果が前記第1閾値より良好である場合には、当該照合結果をもたらす仮設定された第1同期ずれを同期確立された前記第1同期ずれとして決定し、e. 6) 前記e. 2)で得られた前記照合結果が前記第1閾値より良好で、かつ、第2閾値より良好でない場合には、仮設定された前記第2同期ずれを所定ステップ変化させ、e. 7) 前記第2データの
40 前記一部の値とそれらに対応する前記第1データの値とを照合し、e. 8) 前記e. 7)で得られた前記照合結果が前記第2閾値より良好でない場合には、前記e. 6)～e. 7)を前記第2同期ずれの所定調整範囲内で繰り返し、e. 9) 前記e. 7)で得られた前記照合結果が前記第2閾値より良好である場合には、当該照合結果をもたらす仮設定された第2同期ずれを同期確立された前記第2同期ずれとして決定する。

【発明の効果】

【0022】

本発明によれば、第1同期ずれおよび第2同期ずれを所定調整範囲内で順次変更しながら、受信側の第2データの一部とそれに対応する送信側の第1データとを照合し、その照合結果に基づいて第1同期ずれおよび第2同期ずれを確定する。したがって、第1通信器
50 および第2通信器の間の処理ずれだけでなく第2通信器内の処理ずれも考慮するので、正確なフレーム同期を迅速に確立することができ、安定した信頼性の高い通信システムを実

現できる。

【0023】

特に、本発明を量子暗号鍵配布システムに適用した場合、暗号鍵の生成を安定して行うことができる。従来の量子暗号鍵配布技術では誤り率(QBER)の劣化は盗聴者の存在を意味していたが、本発明では暗号鍵生成を中断する前に復旧処理を施すことができ、環境変化や通信エラー等に起因する誤り率劣化を盗聴行為の存在と誤認識することが無くなる。従って従来であれば鍵生成を中断していたところが、暗号鍵の生成を再開することができるので暗号鍵生成の長時間に渡る安定動作を実現できる。

【発明を実施するための最良の形態】

【0024】

本発明は、送信側および受信側でデータの同期を必要とする通信システムに広く適用可能であるが、その望ましい実施形態として、ここでは量子暗号鍵配布システムについて説明する。特にPlug & Play方式は、光ファイバ伝送路における偏光の揺らぎを補償することができるため、偏光に敏感な量子暗号鍵配布システムを実用化するための方式として期待されている（非特許文献4および6を参照）。

【0025】

1. システム構成

図1は本発明の一実施形態によるPlug & Play方式の量子暗号鍵配布システムの構成を示すブロック図である。本実施形態による量子暗号鍵配布システムでは、送信器(Alice)10と受信器(Bob)20とが光ファイバ伝送路30を介して接続されている。

【0026】

1. 1) 送信器(Alice)

送信器10の量子ユニットは、位相変調器101および偏光ビームスプリッタ(PBS)102から構成されるPBSループと可変光減衰器103とを有する。位相変調器101は、位相制御部104から供給される位相制御信号に従って、通過する光パルス列に対して位相変調を行う。位相変調の深さは、ここでは基底(+/-)を示す乱数および鍵の素データを示す乱数(0/1)の4通りの組み合わせにそれぞれ対応する4通りの深さ(0、 $\pi/2$ 、 π 、 $3\pi/2$)となる。位相制御信号は変調の深さに対応した電圧であり、光パルスが位相変調器101を通過するタイミングで位相変調器101に印加され、当該光パルスの位相変調が行われる。位相制御部104は、光受信器105により受信した同期クロックに従って位相制御信号を位相変調器101へ印加するが、後述するように、その印加タイミングと印加電圧は制御部107により制御される。

【0027】

PBSループはファラデーミラーと同様の機能を有し、PBS102に受信器側から入射した光の偏光状態が90度回転して送出される（詳しくは、本出願人により平成16年11月19日に出願された特願2004-335228号の明細書、非特許文献7を参照）。受信器20から入射した量子ユニットの光信号は、光可変減衰器103を通してPBSループで上述したように折り返され、光可変減衰器103を通して受信器20へ送出される。光可変減衰器103は、量子ユニットの同期を取るためのトレーニングモード時には小さい減衰量に設定され、鍵生成のための量子モード時には単一光子伝送となるように大きい減衰量に設定される。

【0028】

また、送信器10は2個の乱数発生器（図示せず）を有し、制御部107は一方の乱数発生器で暗号鍵の素データ(0/1)を、もう一方の乱数発生器で基底情報(+/-)をそれぞれ生成してメモリ109に順次格納する。後述するように、格納された乱数のビット番号はメモリ109のアドレスを用いて管理される。メモリ109としては、高速アクセスが実現できるメモリが望ましく、ここではSDRAMを使用する。

【0029】

鍵生成フローが開始されると、制御部107は光可変減衰器103の減衰量を大きくし

10

20

30

40

50

、メモリ109から素データおよび基底を1組ずつ順次読み出して位相制御部104へ出力する。位相制御部104は、素データおよび基底の組に対応した位相制御信号を同期クロックに従って位相変調器101へ出力することで、位相変調器101を通過する光パルスに対して4通りの深さ(0、 $\pi/2$ 、 π 、 $3\pi/2$)の変調が施される。

【0030】

位相制御部104に供給される同期クロックは、受信器20から光ファイバ伝送路30を通して受信した基準クロックを用いる。基準クロックは光受信器105により電気信号に変換され位相制御部104へ出力される。同時に、この基準クロックは光送信器106へも出力され、基準クロックとして受信器20へ折り返される。また、制御部107は、光送受信器108を通して鍵生成、同期処理や補正処理などに必要なデータおよび制御信号を受信器20の制御部211との間でやり取りする。

10

【0031】

本実施形態では波長分割多重伝送が用いられ、量子ユニットの通信、基準クロックの送受信および制御部107のデータ通信は、それぞれ異なる波長により行われる。送信器10には波長合分波器110が設けられ、光ファイバ伝送路30から入射した光信号を分波して、光可変減衰器103、光受信器105および光送受信器108へ出力し、逆に、光可変減衰器103、光送信器106および光送受信器108から出射した光信号を合波して光ファイバ伝送路30へ送出する。すなわち、光ファイバ伝送路30には、量子ユニットで使用される量子チャネルと、光受信器105、光送信器106および光送受信器108でそれぞれ使用される古典チャネルとが波長多重されている。

20

【0032】

1. 2) 受信器 (Bob)

本実施形態における受信器20の量子ユニットは、光サーキュレータ203、光カップラ204、位相変調器205、PBS206および光検出器APD0、APD1を有する。光カップラ204とPBS206の間には長いパスと短いパスが並列に設けられている。位相変調器205は長いパスに設けられ、位相制御部210からの位相制御信号により位相変調の深さ(基底)と駆動タイミングとが制御される。光検出器APD0およびAPD1はアバランシェ・フォトダイオード(APD)であり、位相制御部210からの制御信号によりガイガーモード(Gated Geiger Mode)で駆動される(非特許文献5を参照)。

【0033】

30

受信器20には基準クロック源201が設けられ、レーザ源202は基準クロック源201により生成された基準クロックに従って駆動され、同時に、その基準クロックは光送信器208を通して送信器10へ送出される。送信器10では、その基準クロックを用いて同期タイミングを決定すると共に、その基準クロックをそのまま受信器20へ折り返す。送信器10から折り返された基準クロックは光受信器209によって受信され、受信器20の同期クロックとして位相制御部210へ供給される。位相制御部210は、制御部211の制御の下で、供給された基準クロックに同期するように位相変調器205の位相変調の深さおよび電圧印加タイミングを制御し、光検出器APD0およびAPD1に光子検出のための逆バイアス電圧の印加タイミングを制御する。

【0034】

40

また、受信器20は1個の乱数発生器(図示せず)を有し、制御部211は乱数発生器で基底情報(+/-)を生成してメモリ214に順次格納する。鍵生成フローが開始されると、制御部211はメモリ214から基底情報を順次読み出し、位相制御部210へ出力する。メモリ214には、高速アクセスが実現できるメモリが使用される(ここではSDRAM)。位相制御部210は、基準クロックに従って位相変調器205に対して当該基底に対応する電圧の位相制御信号を印加する。これによって、送信器10から伝送されてきた光パルスが位相変調器205を通過するタイミングに合わせて当該基底に対応した変調を施すことができる。

【0035】

後述するように送信器10の位相変調器101で変調された光パルスと受信器20の位

50

相変調器 205 で変調された光パルスとが光カプラ 204 で干渉し、それぞれの位相変調の深さの差に応じて光検出器 A P D 0 あるいは光検出器 A P D 1 で光子が検出される。光検出器 A P D 0 および A P D 1 のそれぞれの検出信号は生鍵として順次メモリ 213 に書き込まれる。なお、メモリ 213 に書き込まれる生鍵のビット番号およびメモリ 214 に格納される基底情報としての乱数のビット番号は、後述するようにそれぞれのメモリのアドレスを用いて管理される。メモリ 213 として、ここでは高速アクセスが実現できる S D R A M を使用する。また、メモリ 213 および 214 は同一メモリの別領域であってもよい。

【0036】

続いて、メモリ 213 に格納された生鍵のビット番号とそれらに対応するメモリ 214 に格納された基底情報とを送信器 10 の制御部 107 へ通知し、上述した基底照合を経て基底が不一致の乱数ビットが捨てられるが、その際、基底が一致したビットのうちメモリ 109 に格納された素データとメモリ 213 に格納された検出データとの一致／不一致も検出され、誤り率 Q B E R が算出される。モニタ 212 は誤り率 Q B E R をメモリ 213 に蓄積しつつ Q B E R の変化を常時監視し、制御部 211 は誤り率 Q B E R の値あるいはその変化量に応じて、後述する位相補正処理あるいはフレーム同期処理を適宜実行する。

【0037】

上述したように本実施形態では波長分割多重伝送が用いられ、量子ユニットの通信、基準クロックの送受信および制御部 211 の基底照合等のデータ通信は、それぞれ異なる波長により行われる。受信器 20 には波長合分波器 207 が設けられ、光ファイバ伝送路 30 から入射した光信号を分波して P B S 206、光受信器 209 および光送受信器 215 へ出力し、逆に、P B S 206、光送信器 208 および光送受信器 215 から出射した光信号を合波して光ファイバ伝送路 30 へ送出する。

【0038】

2. システム動作

基準クロック源 201 から供給されるクロック信号に従ってレーザ源 202 から出射した光パルス P は、光サーキュレータ 203 により光カプラ 204 へ導かれ、光カプラ 204 により 2 分割される。分割された一方の光パルス P 1 は短いパスを通過して直接 P B S 206 へ送られ、分割された他方の光パルス P 2 は長いパスに設けられた位相変調器 205 を通して P B S 206 へ送られる。これら光パルス P 1 および P 2 は P B S 206 で合波され、ダブルパルスとして波長合分波器 207 および光伝送路 30 を通して送信器 10 へ送信される。

【0039】

送信器 10 において、伝送路 30 から波長合分波器 110 および可変光減衰器 103 を通して到来したダブルパルス P 1 および P 2 は、P B S 102 でさらに分離され、時計回りのダブルパルス P 1_{CW} および P 2_{CW} と反時計回りのダブルパルス P 1_{CCW} および P 2_{CCW} の 4 つのパルス、すなわちカルテットパルスとなって位相変調器 101 をそれぞれ反対方向で通過し、それぞれ出射したポートとは反対の P B S ポートへ入射する。

【0040】

位相変調器 101 は、時計回りのダブルパルスの後方のパルス P 2_{CW} を前方のパルス P 1_{CW} に対して位相変調するとともに、反時計回りのダブルパルスと時計回りのダブルパルスとの間に π の位相差を与える。位相変調器 101 は位相制御部 104 の位相制御信号によってカルテットパルスの各パルスに任意の位相変調を施すようにタイミング制御される。

【0041】

こうして必要に応じて位相変調されたカルテットパルスは P B S 102 で合波され再びダブルパルスに戻る。上述したように後方のパルスのみが伝送情報により位相変調されたので、出射ダブルパルスを P 1 および P 2^{*a} と記す。このとき P B S ループ入射時に対して出射時は偏波が 90° 回転しているので、結果的にファラデーミラーと同等の効果が得られる。

10

20

30

40

50

【0042】

受信器20のPBS206は、送信器10から受信した光パルスP1およびP2^{*a}の偏光状態が90度回転していることから、これら受信パルスをそれぞれ送信時とは異なるパスへ導く。すなわち受信した光パルスP1は長いパスを通り、位相変調器205を通過するタイミングで指定された基底で位相変調され、位相変調された光パルスP1^{*b}が光カプラ204に到達し、他方、光パルスP2^{*a}は送信時とは異なる短いパスを通過して同じく光カプラ204に到達する。

【0043】

こうして送信器10で位相変調された光パルスP2^{*a}と受信器20で位相変調された光パルスP1^{*b}とが干渉し、その結果が光子検出器APD0またはAPD1により検出される。光子検出器APD0およびAPD1は、位相制御部210から供給されるクロック信号に従ってガイガーモードで駆動され、その検出データはメモリ213に順次格納される。そして基底照合の際に算出されたQBERがモニタ212により監視され、制御部211は、誤り率QBERと予め格納された閾値とを比較しながら、必要に応じてフレーム同期の復旧処理を実行する。以下、本発明の望ましい実施例によるフレーム同期制御方法について詳細に説明する。これら実施例によるフレーム同期制御方法は、送信器10の制御部107と受信器20の制御部211およびモニタ212とによって実行されるが、送信器10および受信器20のそれぞれのプログラム制御プロセッサ上でフレーム同期制御プログラムを実行することで同様の機能を実現してもよい。

【実施例1】

【0044】

1. 1) 装置間および装置内の処理ずれの定義

図2は、量子暗号鍵配布システムにおける装置間および装置内の伝搬遅延によりビット番号がずれる様子を示した模式図である。上述したように、データおよび基底のビット番号はメモリのアドレスにより管理される。

【0045】

送信器10のメモリ109には、暗号鍵の素データの乱数がアドレス(… i-3, i-2, i-1, i, i+1, …)に、基底情報の乱数がアドレス(… j-3, j-2, j-1, j, j+1, …)にそれぞれ格納され、iとjとが対応しているものとする。位相変調器101によって変調を施す時、制御部107はメモリ109のアドレスi, jからそれぞれデータおよび基底を読み出し、その組み合わせに対応した変調の深さで位相変調器101により光パルスの位相変調が行われる。ただし、装置内の等遅延設計により、アドレスiおよびjからの読み出しには遅延差がなく、i = jを常に満たすものと仮定する。

【0046】

送信器10から送出されたダブルパルスは、上述したように受信器20のPBS206で受信器20を出射したときは別のパスに導かれ、一方は短いパスを通してそのまま光カプラ204へ、他方は長いパスを通して位相変調器205で位相変調され光カプラ204へ到達する。位相変調器205によって変調を施す時、制御部211はメモリ214のアドレス(k)から基底を読み出し、それに対応した変調の深さで位相変調器205が光パルスに位相変調を行う。

【0047】

こうして光検出器APD0およびAPD1により検出されたデータはメモリ213のアドレスl(エル), mに順次書き込まれる。この場合も装置内の等遅延設計により、アドレスlおよびmへの書き込みには遅延差がなく、l = mを常に満たすものと仮定する。

【0048】

このように、送信器10におけるメモリ109の読み出しアドレスi, j、受信器20におけるメモリ214の読み出しアドレスkおよびメモリ213の書き込みアドレスl, mは全て異なる値となるが、送信側のどのビットが受信側のどのビットに対応するかを正しく認識するためには、これらのメモリの間でアドレスの対応関係を決定しておく必要がある。

【0049】

そこで、 $i = j$ および $l = m$ が常に満たされるとして、送信器 10 のメモリ 109 の変調アドレスと受信器 20 のメモリ 213 の検出アドレスとの差を装置間アドレス差分 $G_D (= l - i)$ 、受信器 20 の内部での変調アドレスと検出アドレスとの差を装置内アドレス差分 $G_I (= l - k)$ と呼ぶ。

【0050】

1. 2) フレーム同期ずれと QBER 劣化

装置間アドレス差分 G_D および／または装置内アドレス差分 G_I が温度変化等の原因で変動すると、QBER は次のように変動する。なお、簡単な為に Alice から送信したビットは全て Bob に誤り無く届くと仮定する。

10

【0051】

a) G_D , G_I 共に正しい場合

図 3 は、装置間アドレス差分 G_D と装置内アドレス差分 G_I とが共に正しい場合のビット対応を示す模式図である。QBER の計算では、Alice 及び Bob において施した変調の基底 (Basis) が一致するビットに関してデータの一致率を計算する。図 4 に示す様に、基底の一致しないビットに関しては誤り率に影響せず、基底の一致したビットでは Alice 側のデータ A と Bob 側のデータ B とは一致するので、QBER は 0 % となる。

【0052】

b) G_D が正しくない場合

図 4 は、装置間アドレス差分 G_D が正しくない場合のビット対応を示す模式図である。この場合には、基底照合の際に比較するビットが異なるので相関の無い乱数をずらして比較することとなり、QBER は約 50 % となる。しかしながら、QBER を計算する際のビット量によって、フレーム同期ずれが計算範囲の途中で生じたり計算結果そのもののばらつき等も生じたりする。したがって、これらも考慮して QBER 計算結果が 30 % ~ 60 % 程度の範囲内であれば、 G_D が正しくない場合のフレーム同期ずれが生じていると判断できる。この G_D 不正フレーム同期ずれを判定する基準として、装置間フレーム同期ずれ閾値 Q_{bit} を 30 % ~ 60 % の範囲内に設定する。

20

【0053】

c) G_I が正しくない場合

図 5 (A) は装置内アドレス差分 G_I が正しくない場合のビット対応を示す模式図であり、(B) はこの場合の QBER の推定範囲を説明するための図である。この場合には、図 5 (A) に示すように、Bob 内部で変調のための基底情報アドレスと検出信号の書き込みアドレスとがずれている。したがって、QBER 計算は上記 (a)、(b) の様に単純ではなく、図 5 (B) の様な場合分けで考える必要がある。

30

【0054】

まず、Alice において i ビット目で変調された光子が、Bob において $(i + 1)$ ビット目で変調され、 i ビット目で受信されたと仮定する。但し、Bob は i ビット目で変調したものと誤認している。

【0055】

Alice の i ビット目の基底 $Basis_{Ai}$ と Bob の i ビット目の基底 $Basis_{Bi}$ とが一致する確率も一致しない確率も共に 50 % である。ただし、 i ビット目の基底が一致しない場合 ($Basis_{Ai} \neq Basis_{Bi}$) は QBER に影響ないので、一致する場合 ($Basis_{Ai} = Basis_{Bi}$) のみ検討すればよい。

40

【0056】

上述したように、実際に Bob において光子が変調を受けた基底は $(i + 1)$ ビット目であるから、 $(i + 1)$ ビット目の基底 $Basis_{Bi+1}$ と i ビット目の基底 $Basis_{Bi}$ とが一致する場合 ($Basis_{Bi} = Basis_{Bi+1}$) は誤り無く受信することができ (100 %)、異なる場合 ($Basis_{Bi} \neq Basis_{Bi+1}$) は 50 % の確率で誤受信することになる。

【0057】

50

したがって、結果としてビットが誤りとなる確率は、 $50\% \times 50\% = 25\%$ となる。QBERを計算する際のビット量によって、フレーム同期ずれが計算範囲の途中で生じたり計算結果そのもののばらつき等も生じたりするので、これらを考慮してQBER計算結果が $15\% \sim 30\%$ 程度の範囲内であれば、 G_I が正しくない場合のフレーム同期ずれが生じていると判断できる。この G_I 不正フレーム同期ずれを判定する基準として、装置内フレーム同期ずれ閾値 Q_{in} を $15\% \sim 30\%$ の範囲内に設定する。

【0058】

上述した各ケースのフレーム同期ずれは、CPUの処理エラーやAlice/Bob間の通信エラー等の要因で引き起こされるが、次に説明するフレーム同期処理を実行することで劣化前のQBERに復旧可能である。

10

【0059】

1. 3) フレーム同期制御

以下、本実施例におけるフレーム同期制御について詳細に説明する。

【0060】

図6は、本発明の第1実施例による送信器および受信器の間で行われるフレーム同期制御の過程を示すシーケンス図である。まず、受信器(Bob)10の制御部211は装置内アドレス差分 G_I の概算値として G_I' を仮設定する。そしてメモリ213のアドレス l, m に対応するタイミングで光子を検出した場合(以下、「1ビット目」という。)、制御部211は、当該アドレスの検出データ(0/1)と、当該アドレスに対応するメモリ214のアドレス(k)の周りの所定範囲($l - G_I' \sim (l - G_I' + g_i)$)に格納された基底と、を送信器10へ送信する。ここで、 g_i は装置内アドレス差分 G_I の調整範囲を示す。

20

【0061】

送信器(Alice)10の制御部107は装置間アドレス差分 G_D の概算値として G_D' を仮設定する。受信器20から受信した1ビット目の検出データと($l - G_I' \sim (l - G_I' + g_i)$)ビット目の基底(Bob)の各々との組み合わせに対して、メモリ109における対応ビット($l - G_D'$)の周りの所定範囲($l - G_D' \sim (l - G_D' + g_d)$)に格納されたデータおよび基底(Alice)との照合を行い、それぞれQBERを算出する。ここで、 g_d は装置間アドレス差分 G_D の調整範囲を示す。このようにして最もQBERの低くなる G_D および G_I を決定することでフレーム同期を確立した後、これらの差分値を使用して暗号鍵抽出を行う。

30

【0062】

ここで誤り率QBERは、($l - G_D' \sim (l - G_D' + g_d)$)ビット目の基底(Alice)の各々と、($l - G_I' \sim (l - G_I' + g_i)$)ビット目の基底(Bob)の各々が同一であるビットに対して、それに対応するAlice側のメモリ109に格納された素データとBob側の1ビット目の検出データとの一致率を計算することで求めることができる。

【0063】

上述したように、本発明の第1実施例によれば、 G_D および G_I を総当たりに変化させ、QBERが最小値を示す G_D および G_I をフレーム同期を確立したアドレス差分として以後の暗号鍵生成プロセスで使用する。しかしながら、現実問題として、温度変動による光伝送路の伸縮や受信器内での電気回路の遅延変動などによってビット位置の同期が外れる可能性があるため、後述するように誤り率QBER等を監視項目として常時監視し、通信品質が劣化した場合には、上記フレーム同期処理を実行して G_D および G_I を再設定する必要がある。

40

【実施例2】

【0064】

図7は本発明の第2実施例によるフレーム同期制御を示すフローチャートである。本実施例では、 G_D および G_I を総当たりに変化させ、QBERがフレーム同期処理用閾値 Q_{bit} を下回る時の G_D および G_I をもってフレーム同期を終了する。

50

【0065】

図7において、量子鍵配布の後、 $G_I = G_I'$ および $G_D = G_D'$ と仮設定する（ステップS11）。ここで、 G_I' は装置内ビットずれ仮補正值（ $1-k$ の概算値）であり、 G_D' は装置間ビットずれ仮補正值（ $1-i$ の概算値）である。

【0066】

続いて、 $(1-G_D)$ ビット目のA l i c e側メモリ109の基底と $(1-G_I)$ ビット目のB o b側メモリ214の基底とが同一であるビットに対して、 $(1-G_D)$ ビット目のA l i c e側のメモリ109に格納された素データと1ビット目のB o b側メモリ213に格納された検出データとの一致率を計算することでQ B E Rを計算する（ステップS12）。

10

【0067】

次に、計算されたQ B E Rと装置間フレーム同期処理用閾値 Q_{bit} とが比較され（ステップS13）、Q B E Rが Q_{bit} 以上であれば（ステップS13のN o）、 G_D が調整範囲の下限（ $G_D' - g d$ ）まで到達したか否かが判断される（ステップS14）。 G_D がさらに調整可能であれば（ステップS14のN o）、 G_D を1減少させ（ステップS15）、ステップS12へ戻る。

【0068】

こうして、 G_D が（ $G_D' - g d$ ）に到達するまで1ずつ変化させながら、その都度Q B E Rを計算し、その間にQ B E R < Q_{bit} になれば（ステップS13のY e s）、フレーム同期処理を完了する。

20

【0069】

G_D が（ $G_D' - g d$ ）に到達すると（ステップS14のY e s）、 G_I が調整範囲の下限（ $G_I' - g i$ ）まで到達したか否かが判断される（ステップS16）。 G_I がさらに調整可能であれば（ステップS16のN o）、 G_I を1減少させるとともに G_D を初期の仮設定値 G_D' に戻し（ステップS17）、上記ステップS12～S15を繰り返す。すなわち、 G_I が（ $G_I' - g i$ ）に到達するまで1ずつ減少させながら、ステップS12～S15を繰り返し、その都度Q B E Rを計算し、その間にQ B E R < Q_{bit} になれば（ステップS13のY e s）、フレーム同期処理を完了する。

【0070】

このようにしてQ B E R < Q_{bit} になることなく G_I が（ $G_I' - g i$ ）に到達すると（ステップS16のY e s）、総当たりでもQ B E Rが改善されなかったこととなり、フレーム同期失敗と判断し鍵生成を中断する。

30

【実施例3】

【0071】

図8は本発明の第3実施例によるフレーム同期制御を示すフローチャートである。本実施例では、上述したように G_D が正しくない場合の誤り率Q B E Rが50%、 G_I のみ正しくない場合のQ B E Rが25%になることを利用し、 G_D を先に決定し、その後で G_I を決定する。

【0072】

図8において、量子鍵配布の後、 $G_I = G_I'$ および $G_D = G_D'$ と仮設定する（ステップS11）。続いて、 $(1-G_D)$ ビット目のA l i c e側メモリ109の基底と $(1-G_I)$ ビット目のB o b側メモリ214の基底とが同一であるビットに対して、 $(1-G_D)$ ビット目のA l i c e側のメモリ109に格納された素データと1ビット目のB o b側メモリ213に格納された検出データとの一致率を計算することでQ B E Rを計算する（ステップS12）。

40

【0073】

次に、計算されたQ B E Rと装置間フレーム同期処理用閾値 Q_{bit} とが比較され（ステップS13）、Q B E Rが Q_{bit} 以上であれば（ステップS13のN o）、 G_D が調整範囲の下限（ $G_D' - g d$ ）まで到達したか否かが判断される（ステップS14）。 G_D がさらに調整可能であれば（ステップS14のN o）、 G_D を1減少させ（ステップS15）、

50

ステップS12へ戻る。

【0074】

こうして、 G_D が $(G_D' - g_d)$ に到達するまで1ずつ変化させながら、その都度QBERを計算し、 $QBER < Q_{bit}$ になることなく G_D が $(G_D' - g_d)$ に到達すると（ステップS14のYes）、フレーム同期失敗と判断し鍵生成を中断する。

【0075】

$QBER < Q_{bit}$ になれば（ステップS13のYes）、続いてQBERと装置内フレーム同期処理用閾値 Q_{in} とが比較される（ステップS21）。QBERが Q_{in} 以上であれば（ステップS21のNo）、 G_I が調整範囲の下限 $(G_I' - g_i)$ まで到達したか否かが判断される（ステップS22）。 G_I がさらに調整可能であれば（ステップS22のNo）、 G_I を1減少させ（ステップS23）、QBERを計算して（ステップS24）、ステップS21へ戻る。

10

【0076】

こうして、 G_I が $(G_I' - g_i)$ に到達するまで1ずつ変化させながら、その都度QBERを計算し、 $QBER < Q_{in}$ になれば（ステップS21のYes）、フレーム同期を完了し、 $QBER < Q_{in}$ になることなく G_I が $(G_I' - g_i)$ に到達すると（ステップS22のYes）、フレーム同期失敗と判断し鍵生成を中断する。

【0077】

3. 適用例1

上述したように、本発明によれば、 G_D および G_I を変化させ、QBERが最小となる、あるいは所定閾値を下回る、 G_D および G_I をフレーム同期が確立したアドレス差分とし、以後の暗号鍵生成プロセスで使用する。しかしながら、現実問題として、温度変動による光伝送路の伸縮や受信器内での電気回路の遅延変動などによってビット位置の同期が外れる可能性があるので、誤り率QBER等を監視項目として常時監視し、通信品質が劣化した場合には上記フレーム同期処理を実行して G_D および G_I を再設定する必要がある。以下、本発明の第1適用例を説明する。

20

【0078】

図9（A）は本発明によるフレーム同期処理を利用したネットワーク監視制御の一例を示すフローチャートであり、（B）は誤り率QBERの変化に応じた位相補正およびフレーム同期処理の一例を示す模式的グラフである。本適用例では図9（A）のシーケンスに基づいてシステムの障害検出と復旧作業を行う。

30

【0079】

モニタ212は、上述したように、量子暗号鍵配布S101において算出されたQBERを監視し、制御部211はQBERとフレーム同期処理用の閾値 Q_{bit} とを比較し（ステップS102）、 $QBER < Q_{bit}$ であれば、さらに位相補正処理用の閾値 Q_{phase} と比較する（ステップS103）。 $QBER < Q_{phase}$ であれば（ステップS103のYes）、後続する鍵生成フロー、ここでは誤り訂正、残留誤り検出および秘匿増強の各処理が実行される（ステップS104）。

【0080】

これに対して、 $QBER < Q_{bit}$ であるが（ステップS102のYes）、位相補正処理用の閾値 Q_{phase} 以上に悪化している場合には（ステップS103のNo）、位相補正処理が実行される（ステップS105）。なお、「位相ずれ」とは光子の通過／到達タイミングとクロックタイミングとのずれをいう。「位相補正処理」としては、非特許文献6に記載された位相整合(Phase alignment)を用いる方法あるいは位相制御部を制御してクロックタイミングをシフトさせながらモニタ212で最小のQBERとなるタイミングに合わせる処理などがある。

40

【0081】

位相補正処理S105が終了すると、続いてフレーム同期処理を実行する（ステップS106）。すでに定義したように、「フレーム同期」とは送信側と受信側との間で情報ビットの同期が取れていること、すなわちビット対応の正しい認識が成立している状態をい

50

い、「フレーム同期ずれ」とはビット対応が誤認識されている状態をいう。また「フレーム同期処理」とは、ビット対応をシフトさせながらQBERが最小となるビット対応に再設定することであるが、具体的には後述するフレーム同期処理の項で説明する。

【0082】

フレーム同期処理S106が終了すると、制御部211は再計算されたQBERと盗聴検出用の閾値 Q_{Eve} とを比較する（ステップS107）。 $QBER < Q_{Eve}$ であれば（ステップS107のYes）、再びステップS102に戻る。

【0083】

他方、QBERがフレーム同期処理用の閾値 Q_{bit} 以上に悪化していれば（ステップS102のNo）、上述したフレーム同期処理（ステップS106）を行い、続いてステップS107を実行する。

10

【0084】

ここで位相補正処理S105を実行した後にフレーム同期処理S106を実行するのは、位相補正処理によってクロックの位相が変化し、フレーム同期ずれを誘発している可能性があるからである。また一般的に、フレーム同期処理と位相補正処理とを比べると、フレーム同期処理に要する時間の方が位相補正処理のそれと比べて格段に短いために、位相補正処理を行うに当たって、追加してフレーム同期処理を行うことに時間的な損失が大きくないからでもある。

【0085】

ステップS107においてQBERが Q_{Eve} 以上に悪化していれば（ステップS107のNo）、制御部211は $QBER < Q_{Eve}$ となるまで位相補正処理S105およびフレーム同期処理S106を所定回数（N）だけ連続して繰り返す（ステップS108）。所定回数繰り返してもQBERが改善しなければ（ステップS108のYes）、その時初めて暗号鍵生成フローを中断する（ステップS109）。その際、盗聴の可能性があることを示すアラームを生成することが望ましい。

20

【0086】

なお、QBERは確率的に定まる値であり有限の偏差を有する。したがってQBERの閾値 Q_{bit} や Q_{phase} を設定して「この値を超えると障害」と判断するだけではなく、「複数回連続して閾値を超えると障害」といった判断も必要である。

【0087】

量子鍵配布中に盗聴行為によって情報が漏れている場合にもQBERは劣化するが、この劣化はシステム復旧によって改善しない。したがって、所定回数連続して位相補正処理S105およびフレーム同期処理S106を繰り返しても復旧しない場合は、「盗聴の可能性有り」として暗号鍵の生成を中断する。

30

【0088】

ここで、非特許文献2および3に示した漏洩情報量推定手段を用いて盗聴された可能性のある情報量を破棄することにより暗号鍵生成は行うことができるが、ある誤り率の値を超えると安全な暗号鍵生成が行えなくなる。したがって、この値を盗聴検出用の閾値 Q_{Eve} として使用する。

【0089】

また、装置内に使用しているデバイス自体の故障により誤り率が増加することもあるが、本装置の最終目的は、第三者に漏洩することなく共有暗号鍵を生成することであるから、QBERに変化を及ぼさない障害は無視できる。従って、暗号鍵生成を中断するトリガは、システム復旧後でも閾値 Q_{Eve} を超えている場合として構わない。

40

【0090】

図9（B）は、一例として $Q_{bit} = 30\%$ 、 $Q_{phase} = 10\%$ 、 $Q_{Eve} = 10\%$ 強に設定した場合のQBERの変化と位相補正処理S105およびフレーム同期処理S106を模式的に示したものである。図示されているように、QBERが劣化しても位相補正処理S105およびフレーム同期処理S106を実行することで復旧できるかどうかをチェックし、復旧すれば、そのまま鍵生成フローを続行することができ、鍵生成効率を改善するこ

50

とができる。また、何回か試みても復旧できない場合に「盗聴の可能性有り」と判断して暗号鍵の生成を中断するので、鍵生成の効率性とともにも安全性も担保される。

【0091】

3. 1) 変調・検出位相ずれ

図1に示すような往復型の量子暗号鍵配布システムは、PMD(Polarization Mode Dispersion)やPDL(Polarization Dependent Loss)といった伝送路における偏波方向依存の擾乱を抑制すると共に、光子パルスに載せられた位相情報を読み取るために必要な光学干渉計を効率良く組織できる、という利点を有する。

【0092】

一方、往復型のシステムであるが故に、光子パルスに位相情報を載せるために用いる位相変調器を双方向で使用する必要が生じ、位相変調器を単一方向で使用する場合と比べて高い変調タイミング精度が必要になる。ここで、光子パルスが位相変調器を通過するタイミングと位相変調器を駆動するタイミングがずれると、所望量の位相変調を施すことができなくなり、干渉計の信号対雑音比(SN比)に対応する明瞭度が低下する。この低下は即ちQBERの劣化に対応する。

【0093】

上述したように、送信器10の位相変調器101によって通過光パルスに位相変調を施し、それを可変光減衰器103によって単一光子状態まで減衰させて受信器20へ送信する。受信器20では、単一光子状態の光パルスを位相変調器205によって位相変調し干渉させることで平衡型ゲートモード光子検出器APD0、APD1(非特許文献5)で光子検出を行う。一般的に、APDにゲート電圧を印加し始めた直後に光子が入射するようにタイミング調整するとAPD内部で最も雪崩増倍が起こりやすくなることが知られている。光子入射のタイミングとAPDへのゲート電圧印加タイミングとがずれると、その分、雪崩増倍が減少し、出力電流も減少してSN比が劣化する。この劣化は即ちQBERの劣化に対応する。

【0094】

このようなタイミングずれ、すなわち光子入射のタイミングと位相変調器/APDの駆動タイミングとのずれは、温度変化による光伝送路の遅延変動、電気回路の遅延変動によって引き起こされるので、変化の割合は比較的小さい。従って、クロック位相をシフトさせることで、光子入射のタイミングと位相変調器/APDの駆動タイミングとを最適位置に調整することができ、劣化前のQBERに復元させることができる。

【0095】

クロック位相の調整法はいくつか提案されている。非特許文献6には、クロック信号を可変遅延した補正クロック信号と光子検出信号との位相差を検出し、その位相差に応じてクロック信号の遅延量を変化させる温度補償遅延ロックループ(DLL)を用いた方法が記載されている(非特許文献6のFig. 2参照)。また、QBERをモニタしながらクロック位相を徐々にシフトさせ、QBERが最小となるクロック位相を最適位置として設定する方法も利用可能である。

【0096】

3. 2) 盗聴者の存在

非特許文献2および3に記載されている盗聴者Eveの情報量は、Incoherent Attack(Individual Attack)と呼ばれる盗聴法に基づいている。この盗聴法によれば、Eveは1度に1個の光子にだけ自分の持っている量子プローブをエンタングルさせる(絡ませる)ことによって光子パルスに載せられた乱数情報のある程度盗み、Alice/Bob間で基底照合のための通信が行われるまで当該量子プローブを保持する。基底公開後に適切な観測を行うことにより盗聴者は最大限の情報を得ることができる。

【0097】

非特許文献2および3によれば、QBERが11~15%以上になると、Eveの情報がBobの情報量を上回ることが導かれている。これらのQBER閾値は理論的に導かれたものであり、実世界における様々な制約を加味するとEveに漏れ得る情報量はより小

10

20

30

40

50

さくなるが、実装置の雑音指数を理論的に定量化することはできないために一般に上記 QBER 閾値を盗聴検出の閾値 Q_{Eve} として使用する。

【0098】

その他、より現実的な盗聴法として、Eve が一旦光子パルスを受光／観測してから観測結果に基づいて再度光子パルスを Bob へと送り直す Intercept/Resend Attack といった盗聴法もある。しかし、この盗聴法で Eve が光子ビットに残す痕跡の大きさは Incoherent Attack のそれと比べて大きいので、この盗聴が行われている場合には誤り率はより大きく劣化する。したがって、QBER 閾値 Q_{Eve} を 10% 強に設定しておけば、Incoherent Attack に加えてこの盗聴も検出できる。

【0099】

さらに、QBER は確率的に定まる値であり有限の偏差を有する。したがって QBER の閾値を設定して「この値を超えると障害」と判断するだけではなく、「複数回連続して閾値を超えると障害」といった判断が必要となる。具体的には、一定の長さの時間、一定の大きさの空間において、ごく稀な確率で発生する事象の確率分布はポアソン (Poisson) 分布に従うことが知られている。QBER が 10% とすると、1000 ビットの試験ビットの中に 100 ビット前後の誤りが含まれており、この誤り数は 10 ビット分の標準偏差を持つ。つまり誤り数は 90 ～ 110 ビットまで無為に揺らぎ、これに従って測定される QBER も 9% ～ 11% まで変化する。この確率的な誤差を小さくするためには、試験ビットを増やすか試験回数を増やすことが必要となる。

【0100】

盗聴行為によって生じた QBER 劣化は、いかなる復旧作業を施しても元に戻ることはない。したがって、システム復旧後に測定した QBER が盗聴閾値 Q_{Eve} より上回っている場合は「盗聴可能性有り」として暗号鍵生成を中断する。

【0101】

3. 3) 光源・受光器障害

光子パルスを生成するレーザ源および光子パルスを検出する受光器の障害によっても QBER は劣化する。レーザ光源のエネルギー変換効率が劣化すると、出力光強度が劣化し、それによって光子受信器に到達する光強度も劣化し、受信器での光子カウント数が減少する。一方、受信器でのノイズ量は入射光強度に依らず一定であるために、結果として暗号鍵の SN 比が劣化する。この劣化は即ち QBER の劣化に対応する。

【0102】

また、光子受信器でも光電変換効率の劣化やバイアス電圧の低下など様々な劣化要因があり、これによって同一光強度を受光していても光子カウント数は劣化する。一方、このようなデバイス劣化によってノイズ量も変化するが、一般的に SN 比が劣化することが大半である。つまり、光子受信器の障害によっても QBER は劣化する。

【0103】

以上のようなデバイスそのものの劣化に起因する QBER の劣化は復旧機構によって回復するものではない。したがって、本障害を検出した時にはアラームを上げ暗号鍵の生成を停止する。

【0104】

4. 適用例 2

本発明は、上記実施例の往復型だけでなく、単一方向型の量子暗号鍵配布システムにも同様に適用することができる。

【0105】

図 10 は本発明によるフレーム同期制御を適用した単一方向型量子暗号鍵配布システムの構成を示すブロック図である。ただし、本発明の動作に関するモニタやメモリおよび制御系は図 1 に示すものと同様であるから同一参照番号を付している。

【0106】

単一方向型量子暗号鍵配布システムにおいて、送信器 (Alice) 40 と受信器 (Bob) 50 とは光ファイバ伝送路 30 によって光学的に接続され、レーザ光源 401 およ

10

20

30

40

50

びクロック源 403 は送信器 40 に設けられている。

【0107】

レーザ光源 401 はクロック源 403 から供給される基準クロックに従って光パルス列を出射する。光パルスは光カプラ 402 で 2 分割され、一方のパルス P1 は短いパスに設けられた位相変調器 405 によって位相変調されて光カプラ 406 へ到達し、他方のパルス P2 は長いパス 407 を通って光カプラ 406 に到達する。したがって、位相変調された光パルス P1^{*A}と遅延した光パルス P2 とが時間的に相前後したダブルパルスとなり、可変光減衰器 408 および波長合分波器 409 を通して伝送路 30 へ送出される。

【0108】

位相制御部 404 はクロック源 403 からの基準クロックに従って位相変調器 405 へ位相制御信号を出力し、それに従って位相変調器 405 は通過する光パルス P1 に位相変調を施す。位相変調の深さは、第 1 実施例で述べたようにメモリ 109 に格納された（乱数、基底）の組み合わせに依存する。また、クロック源 403 の基準クロックは光送信器 410 によりレーザ源 401 とは異なる波長の光信号として波長合分波器 409 を通して伝送路 30 へ送出される。なお、第 1 実施例と同様に、送信器 40 の制御部 107 と受信器 50 の制御部 211 とは、光送受信器 108 および 215 を通して同様の波長多重伝送によりフレーム同期や位相補正に必要なデータや制御信号等をやり取りする。

【0109】

受信器 50 では、光パルス P1^{*A}および光パルス P2 が波長合分波器 501 を通して送信器 40 と同様の光学系に入射する。すなわち、それぞれの光パルスは、光カプラ 502 により 2 分割され、送信器 40 と同様の短いパスに設けられた位相変調器 503 と長いパス 504 とを通して光カプラ 507 で合波する。この場合、送信器 40 と受信器 50 との間の変調の深さの差に依存して光検出器 APD0 あるいは APD1 の一方で光パルスが検出できるのは、送信器 40 の短いパス（位相変調器 405）および受信器 50 の長いパス 504 を通った光パルス P1^{*A}と、送信器 40 の長いパス 407 および受信器 50 の短いパス（位相変調器 503）を通った光パルス P2^{*B}とが同時に光カプラ 507 に到達し干渉する場合である。

【0110】

位相制御部 506 は、送信器 40 から光受信器 505 を通して受信した基準クロックに従って位相変調器 503 へ位相制御信号を出力し、それに従って位相変調器 503 は通過する光パルスに位相変調を施す。位相変調の深さは、既に述べたようにメモリ 214 に格納された基底に依存する。

【0111】

こうして光検出器 APD0 および APD1 により検出されたデータはモニタ 212 を通してメモリ 213 に書き込まれる。モニタ 212 および制御部 211 の監視制御は、上述した実施例で説明したとおりである。

【産業上の利用可能性】

【0112】

本発明は、量子暗号鍵配布技術に代表される共通暗号鍵配布技術を用いた高秘匿通信に利用可能である。量子暗号鍵配布方法は、単一方向型・往復型を問わない。

【図面の簡単な説明】

【0113】

【図 1】本発明の一実施形態による Plug & Play 方式の量子暗号鍵配布システムの構成を示すブロック図である。

【図 2】量子暗号鍵配布システムにおける装置間および装置内の伝搬遅延によりビット番号がずれる様子を示した模式図である。

【図 3】装置間アドレス差分 G_D と装置内アドレス差分 G_I とが共に正しい場合のビット対応を示す模式図である。

【図 4】装置間アドレス差分 G_D が正しくない場合のビット対応を示す模式図である。

【図 5】（A）は装置内アドレス差分 G_I が正しくない場合のビット対応を示す模式図で

10

20

30

40

50

あり、(B)はこの場合のQBERの推定範囲を説明するための図である。

【図6】本発明の第1実施例による送信器および受信器の間で行われるフレーム同期制御の過程を示すシーケンス図である。

【図7】本発明の第2実施例によるフレーム同期制御を示すフローチャートである。

【図8】本発明の第3実施例によるフレーム同期制御を示すフローチャートである。

【図9】(A)は本発明によるフレーム同期処理を利用したネットワーク監視制御の一例を示すフローチャートであり、(B)は誤り率QBERの変化に応じた位相補正およびフレーム同期処理の一例を示す模式的グラフである。

【図10】本発明によるフレーム同期制御を適用した単一方向型量子暗号鍵配布システムの構成を示すブロック図である。

10

【図11】BB84プロトコルによる量子暗号鍵配布方法の概念を示す模式図である。

【図12】一般的な量子暗号鍵生成の流れを示すフローチャートである。

【符号の説明】

【0114】

10 送信器 (Alice)

20 受信器 (Bob)

30 光ファイバ伝送路

101 位相変調器

102 偏光ビームスプリッタ

103 可変光減衰器

104 位相制御部

105 光受信器

106 光送信器

107 制御部

108 光送受信器

109 メモリ

110 波長合分波器

201 クロック源

202 レーザ源

203 光サーキュレータ

204 光カプラ

205 位相変調器

206 偏光ビームスプリッタ

207 波長合分波器

208 光送信器

209 光受信器

210 位相制御部

211 制御部

212 モニタ

213 メモリ

214 メモリ

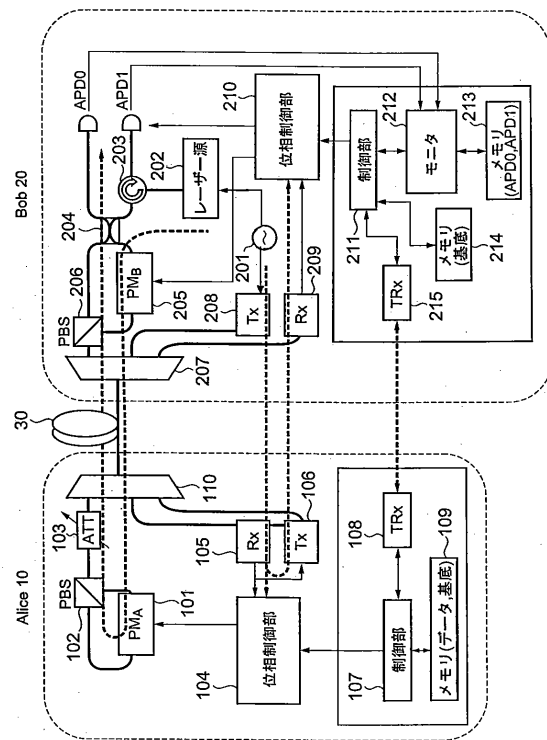
215 光送受信器

20

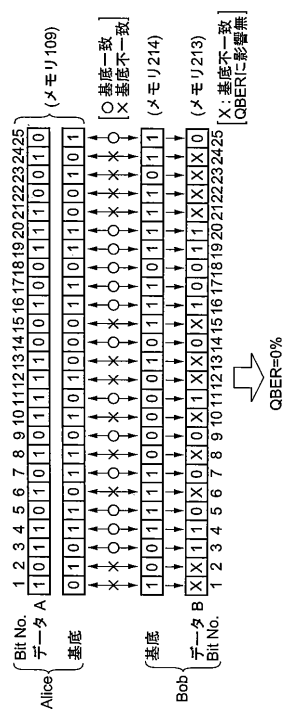
30

40

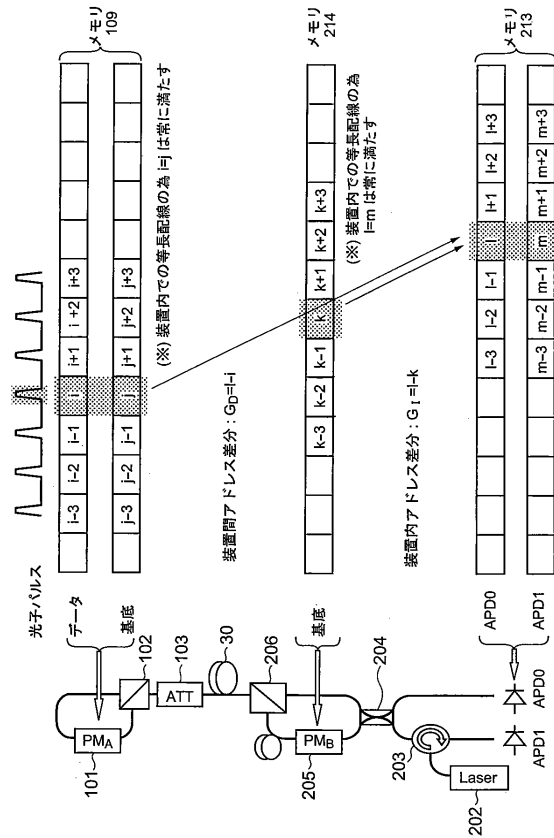
【図 1】



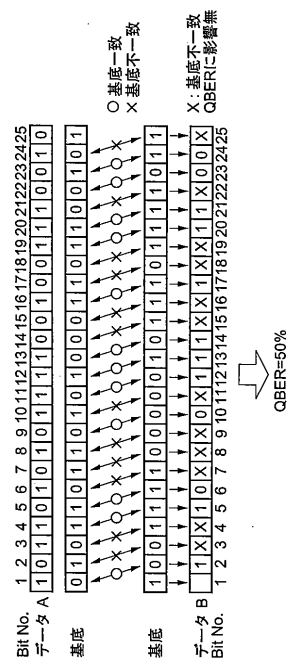
【図 3】



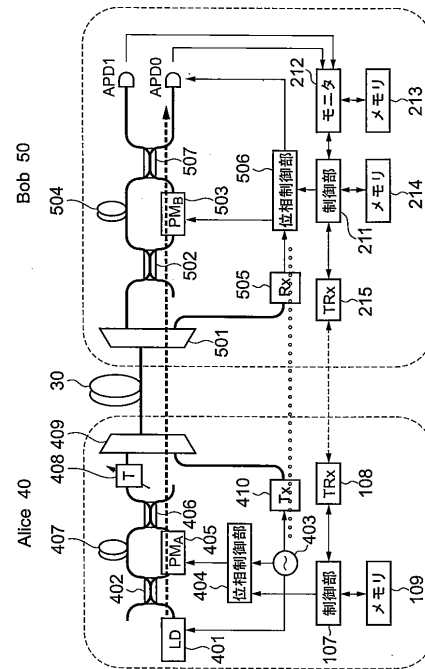
【図 2】



【図 4】



【図 10】



量子暗号通信

乱数1 (データ)	乱数2 (基底)	位相	乱数3 (基底)	位相	乱数4 (出力)
1	+	π	+	0	1
0	×	$\pi/2$	+	0	0 or 1
1	×	$3\pi/2$	×	$\pi/2$	1
0	+	0	×	$\pi/2$	0 or 1
0	+	0	+	0	0
1	×	$\pi/2$	×	$\pi/2$	0
0	×	$\pi/2$	+	0	0 or 1
1	+	π	+	0	1

ランダム

基底	乱数	位相
+	0	0
+	1	π
×	0	$\pi/2$
×	1	$3\pi/2$

ランダム

AliceとBobの位相が同じなら 0
 AliceとBobの位相が違うなら 1
 AliceとBobの基底が違うなら 0 or 1

フロントページの続き

(72)発明者 前田 和佳子
東京都港区芝五丁目7番1号 日本電気株式会社内

審査官 白井 亮

(56)参考文献 国際公開第2005/018185 (WO, A1)
特開平08-256086 (JP, A)
特開平09-200197 (JP, A)
特開2000-174747 (JP, A)
特開2004-112278 (JP, A)

(58)調査した分野(Int.Cl., DB名)
H04L 7/00-7/10