

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2006 年 1 月 19 日 (19.01.2006)

PCT

(10) 国際公開番号
WO 2006/006232 A1

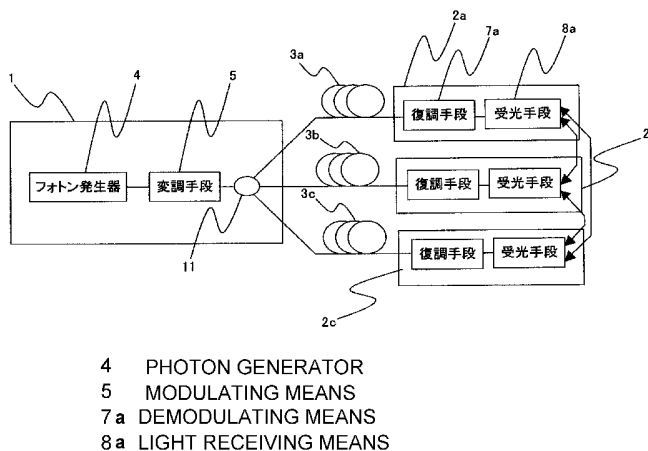
- (51) 国際特許分類⁷: H04L 9/12
- (21) 国際出願番号: PCT/JP2004/009931
- (22) 国際出願日: 2004 年 7 月 12 日 (12.07.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 安部 淳一 (ABE, Jun'ichi) [JP/JP]; 〒1008310 東京都千代田区丸の内二

- 丁目 2 番 3 号 三菱電機株式会社内 Tokyo (JP). 清水克宏 (SHIMIZU, Katsuhiko) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社内 Tokyo (JP).
- (74) 代理人: 酒井 宏明 (SAKAI, Hiroaki); 〒1006019 東京都千代田区霞が関三丁目 2 番 5 号 霞が関ビルディング 酒井国際特許事務所 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

/ 続葉有 /

(54) Title: QUANTUM ENCRYPTION KEY DELIVERY SYSTEM

(54) 発明の名称: 量子暗号鍵配送システム



(57) Abstract: A quantum encryption key delivery system wherein three or more users can easily and safely share a quantum encryption key and wherein a plurality of users can share a photon generator. There are provided transmitting means (1) comprising photon generating means (4) and modulating means (5); two or more receiving means (2a, 2b, 2c) comprising demodulating means (7a, 7b, 7c) connected to the respective ones of two or more transmission paths (3a, 3b, 3c) connected to the transmitting means (1). It is arranged that pulses transmitted to each transmission path do not include two or more photons. Modulation system information selected by the transmitting means is exchanged between the transmitting means and at least one of the receiving means. Demodulation system information selected by the receiving means and information indicative of whether a photon arrives are exchanged between the receiving means. When all the receiving means receive photons, and all the demodulation systems selected by the receiving means coincide with the modulation system selected by the transmitting means, the quantum encryption key is shared.

(57) 要約: 量子暗号鍵配送システムにおいて、3者以上の複数ユーザが量子暗号鍵を容易かつ安全に共有し、また、複数のユーザ間でフォトン発生器の共有を可能とすること。フォトン発生手段(4)および変調手段(5)を具備する送信手段(1)と、送信手段(1)に接続された2経路以上の伝送路(3a, 3b, 3c)のそれぞれに接続される復調手段(7a, 7b, 7c)を具備する2以上の受信手段(2a, 2b, 2c)とを備え、各伝送路に送出されるパルスには2つ以上のフォトンが

/ 続葉有 /

WO 2006/006232 A1



(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

含まれることがないように制御され、送信手段と、少なくとも一つの受信手段との間で送信手段が選択した変調系情報が交換され、各受信手段が選択した復調系情報と、フォトン到着の有無情報とが各受信手段の間で交換され、受信手段の全てがフォトンを受信し、かつ、各受信手段が選択した復調系の全てと、送信手段の選択した変調系とが一致した場合に量子暗号鍵が共有される。

明 細 書

量子暗号鍵配送システム

技術分野

- [0001] 本発明は、量子暗号鍵配送システムに関するものであり、特に、3者以上のユーザ間で量子暗号鍵を共有するための量子暗号鍵配送システムに関するものである。

背景技術

- [0002] 暗号鍵配送システムは送受信手段間でランダムなビット列(暗号鍵)を共有することを目的とするシステムである。近年、暗号鍵の中でも、攻撃者の計算能力によらず安全の保証された暗号鍵を配送することができる量子暗号鍵配送技術が注目されている。
- [0003] 量子暗号鍵配送にかかる従来技術としては、BB84方式として知られている単一光子光源を用いた量子暗号鍵配送技術が広く知られている(例えば、非特許文献1、2など)。これらの文献に開示されている量子暗号鍵配送技術は、量子信号ビットの不確定性(ランダム性)を利用して、盗聴者の盗聴を回避しつつ送信手段(送信者)と受信手段(受信者)との間で鍵を共有することができる。
- [0004] 量子暗号鍵配送技術のベースとなる量子暗号通信では、通信手段として光子(光子)が用いられ、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、その偏光および位相等の量子状態を知らずに任意の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。すなわち、従来技術にかかる量子暗号鍵配送技術では量子暗号鍵の共有と盗聴者の検出が物理的に保証されるという特徴を有している。
- [0005] 非特許文献1:C. H. Bennett, and G. Brassard, :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).

非特許文献2:C. H. Bennett, “Quantum Cryptography Using Any Two Nonorthogonal States,” Phys. Rev. Lett. 68, 3121 (1992).

発明の開示

発明が解決しようとする課題

[0006] しかしながら、上記の非特許文献1、2などに開示されたBB84方式では、送信者は1パルスあたり1フォトン以下の微小な光信号を精度よく送出する必要があるため、複雑で高価な光子発生器を持たなければならないという課題があった。

[0007] また、BB84方式においては、システムを利用するユーザ個々がフォトン発生器を持たなければならないという課題があった。

さらに、BB84方式では2者間にて量子暗号鍵を共有する仕組みを提供するが、3者以上の多者間での暗号鍵共有が難しいという課題があった。

[0008] このような状況に鑑み、本発明は、3者以上の複数ユーザが量子暗号鍵を容易かつ安全に共有することを可能とし、複数のユーザあるいは複数システム間でフォトン発生器の共有を可能とする量子暗号鍵配送システムを提供することを目的とする。

課題を解決するための手段

[0009] 本発明にかかる量子暗号鍵配送システムにあつては、量子暗号鍵を共有するための量子暗号鍵配送システムにおいて、フォトン発生手段と、選択可能な2系以上の変調系を有する変調手段と、を具備する送信手段と、前記送信手段に接続された2経路以上の伝送路と、前記2経路以上の伝送路のそれぞれに接続され、選択可能な2系以上の復調系を有する復調手段を具備する2以上の受信手段と、を備え、前記各伝送路に送出されるパルスには2つ以上のフォトンが含まれることがないように制御され、前記送信手段と前記2以上の受信手段のうちの少なくとも一つの受信手段との間で該送信手段が選択した変調系情報が交換され、前記2以上の受信手段のそれぞれが選択した復調系情報と、フォトン到着の有無情報とが該受信手段のそれぞれとの間で交換され、前記2以上の受信手段の全てがフォトンを受信し、かつ、該2以上の受信手段のそれぞれが選択した復調系の全てと、前記送信手段の選択した変調系とが一致した場合に前記量子暗号鍵を共有することを特徴とする。

[0010] 本発明によれば、各伝送路に送出されるパルスには2つ以上のフォトンが含まれる

ことがないように制御され、送信手段と2以上の受信手段のうちの少なくとも一つの受信手段との間で送信手段が選択した変調系情報が交換され、2以上の受信手段のそれぞれが選択した復調系情報と、光子到着の有無情報とが受信手段のそれぞれの間で交換され、2以上の受信手段の全てが光子を受信し、かつ、2以上の受信手段のそれぞれが選択した復調系の全てと、送信手段の選択した変調系とが一致した場合に2以上の受信手段の間で量子暗号鍵が共有される。

発明の効果

- [0011] 本発明にかかる量子暗号鍵配送システムによれば、2以上の受信手段の全てが光子を受信し、かつ、2以上の受信手段のそれぞれが選択した復調系の全てと、送信手段の選択した変調系とが一致した場合に量子暗号鍵を共有するようにしているので、送信者を含む3者以上の複数ユーザが量子暗号鍵を容易かつ安全に共有することができるという効果を奏する。

図面の簡単な説明

- [0012] [図1]図1は、本発明の実施の形態1にかかる量子暗号鍵配送システムの構成を示す概念図である。
- [図2]図2は、本発明の実施の形態2にかかる量子暗号鍵配送システムの構成を示す概念図である。
- [図3]図3は、本発明の実施の形態3にかかる量子暗号鍵配送システムの構成を示す概念図である。
- [図4]図4は、本発明の実施の形態4にかかる量子暗号鍵配送システムの構成を示す概念図である。
- [図5]図5は、本発明の実施の形態5にかかる量子暗号鍵配送システムの構成を示す概念図である。
- [図6]図6は、BB84方式を用いた従来技術にかかる量子暗号鍵配送システムの構成例を示す概念図である。
- [図7]図7は、図6に示した量子暗号鍵配送システムの変調手段5および復調手段7のそれぞれに位相変調器を用いた場合の構成例を示す図である。

符号の説明

- [0013] 1 送信手段
2, 2a, 2b, 2c, 2d, 2e 受信手段
3a, 3b, 3c 伝送路
4 フォトン発生器
5 変調手段
6a, 6b 信号処理手段
7 復調手段
8 受光手段
9 情報交換手段
10 誤り率検出手段
11, 11a, 11b 分波手段
12a, 12b, 12c 可変減衰器
13a, 13b 位相変調器
14a, 14b 合波手段

発明を実施するための最良の形態

- [0014] 以下に添付図面を参照して、本発明にかかる量子暗号鍵配送システムの好適な実施の形態を詳細に説明する。なお、この実施の形態により本発明が限定されるものではない。
- [0015] 実施の形態1.

まず、本発明の実施の形態1にかかる量子暗号鍵配送システムについて説明する。図1は、本発明の実施の形態1にかかる量子暗号鍵配送システムの構成を示す概念図である。この実施の形態の量子暗号鍵配送システムは、送信側で使用される送信手段1と、送信手段1に接続された3つの伝送路3a、3b、3cと、受信側の伝送路それぞれに接続された受信手段2a、2b、2cと、を備えるように構成される。送信手段1はフォトン発生器4、変調手段5、分波手段11を有し、それぞれの受信手段は復調手段7、受光手段8を具備する。ここで、変調手段5、復調手段7としては位相変調器、偏波変調器などを用いることができる。フォトン発生器4としては、例えば、レーザダイオードなどの光源を用いるのが一般的である。伝送波長は伝送路3に適した波長で

あれば、いかなる波長であっても構わない。分波手段11としては、例えば、光カップラなどを用いることができる。伝送路3a、3b、3cとしては、シングルモード光ファイバ、分散シフト光ファイバなどの各種光信号用伝送路を用いることができる。また、伝送路は必ずしも有線である必要はなく、空間伝送など無線伝送路でも構わない。

[0016] つぎに、上記に示した本発明にかかる量子暗号鍵配送システムの理解を容易にするため、BB84方式を用いた従来技術にかかる量子暗号鍵配送システムを例にとり、その動作について説明する。

[0017] 図6は、BB84方式を用いた従来技術にかかる量子暗号鍵配送システムの構成例を示す概念図である。同図において、送信手段1は、光子発生器4、変調手段5、信号処理手段6aを備える。ここでは、変調手段5として位相変調器を用いるものとして説明する。送信手段1では、 $[0, \pi]$ 系もしくは $[\pi/2, 3\pi/2]$ 系のいずれかの位相変調系が1パルスごとに選択され、“0”または“1”の信号が伝送路3に送信される。信号伝送に際し、2つの変調系が用いられ、1パルスあたり1光子しか使わないことが特徴である。一方、受信手段2は、復調手段7、受光手段8、信号処理手段6bを備える。受信手段2では、任意の復調系を用いて受信パルスが観測され、“0”、“1”、“光子無し”、のいずれであるかが判定される。また、送信手段1および受信手段2では、選択された変復調系情報と、パルスの到着の有無情報とが、盗聴されてもよい公衆回線などの情報交換手段9にて交換される。損失がある伝送路では、多くのパルスが“光子無し”という結果となる。受信手段2で光子が受信され、かつ、送受信間で系が一致した場合にのみ両者間でビット列が共有される。共有されたビット列は誤り率検出手段10にて、誤り検出、誤り訂正された後に、量子暗号鍵として使用される。

[0018] また、図7は、図6に示した量子暗号鍵配送システムの変調手段5および復調手段7のそれぞれに位相変調器を用いた場合の構成例を示す図である。同図において、変調手段5は、分波手段11a、位相変調器13a、合波手段14aから構成され、復調手段7は、分波手段11b、位相変調器13b、合波手段14bから構成される。いま、送信手段1が $[0, \pi]$ 系（“ π ”測定系）を選択する場合には、信号“0”に対して位相変調器13aは位相変調量“0”を発生し、信号“1”に対しては位相変調量“ π ”を発生す

る。送信手段1が $[\pi/2, 3\pi/2]$ 系(“ $\pi/2$ ”測定系)を選択する場合には、信号“0”に対して位相変調器13aは位相変調量“ $\pi/2$ ”を発生し、信号“1”に対しては位相変調量“ $3\pi/2$ ”を発生する。一方、受信手段2が復調器として $[0, \pi]$ 系(“ π ”測定系)を選択する場合には、位相変調器13bは位相変調量“0”を発生し、 $[\pi/2, 3\pi/2]$ 系(“ $\pi/2$ ”測定系)を選択する場合には位相変調器13bは位相変調量“ $\pi/2$ ”を発生する。送信手段1および受信手段2が、同一の変調・復調系を選択した場合にのみ、受光手段8は正しい信号を検出することができる。

[0019] 上述の処理のように、1パルスあたり1光子しか使用されないので、通信路に送出された信号を盗聴するためには、盗聴者は一度光子を抜き出して観測した後、その光子を再び通信路に戻さなければならない。しかし、量子力学の不確定性原理により、光子の量子状態に擾乱を与えずに観測を行うことはできないため、上述の Protokol では盗聴者が存在すると受信側において1/4の確率で誤りが生じることになる。例えば、送信手段1から $[0, \pi]$ 系の信号“0”が送信された場合、盗聴者が誤った $[\pi/2, 3\pi/2]$ 系を選択する確率が1/2であり、そのとき受信手段2が観測する偏光方向は $[\pi/2, 3\pi/2]$ に変化する。一方、受信手段2において、この偏光方向の信号が送信手段1において使用された測定系と同一の測定系である $[0, \pi]$ 系で観測された場合、信号“0”と信号“1”とが等確率で観測されるので、送信手段1が送信した信号“0”を受信手段2が信号“1”として観測する確率は1/4となる。

[0020] チェックビット数 m を十分に大きくすれば、大数の法則によって誤り率は必ず25%に近づくため、盗聴を検出できない確率は、無視できる程度に十分小さくできる。また、選択可能な変・復調系の数を3以上にすれば盗聴防止に要するチェックビット数 m を低減することができる。このように、送信側-受信側間で誤り検出を行うことにより、盗聴者の存在は必ず検知することができる。なお、このBB84方式は、量子暗号鍵の共有と盗聴者の検出が量子力学の原理である量子力学的相補性によって物理的に保証されていることに大きな意味がある。

[0021] つぎに、図1に戻り、この実施の形態の量子暗号鍵配送システムの動作に関し、変調手段5に位相変調器を用いた場合について説明する。送信手段1では、 $[0, \pi]$ 系もしくは $[\pi/2, 3\pi/2]$ 系のいずれかの位相変調系が1パルスごとに選択され

た同一信号が3つの伝送路3a、3b、3cに略同時に送信される。ここで重要なことは、いずれの伝送路においても、1パルスあたりのフォトン数は1以下となるように制御されることである。受信手段2a、2b、2cでは、それぞれが独立に任意の復調系にて受信パルスが観測され、“0”、“1”、“フォトン無し”、のいずれであるかが判定される。受信手段2a、2b、2cは、選択した復調系情報とパルスの到着の有無情報とが相互に交換される。また、これらの情報は、各受信手段が測定した測定結果情報ではなく、たとえ盗聴されたとしても量子暗号鍵共有の安全性を損なうことがないため、公衆回線を用いて送受することができる。

- [0022] 受信手段2a、2b、2cの全てがフォトンを受信し、かつ、3者が選択した受信系が全て送信手段の変調系に一致した場合にのみ3者間でビット列が共有される。受信手段の共有されたビット列は必要に応じて誤り検出、誤り訂正された後に、3者間の量子暗号鍵として使用される。量子暗号鍵を共有する3者がフォトン発生器を持つ必要がないことが特徴である。
- [0023] このとき、送信手段1は必ずしも受信手段2a、2b、2cが選択した復調系を知る必要はない。また、送信手段1は必ずしも受信手段2a、2b、2c全員と選択した変復調系情報を交換する必要はない。すなわち、受信手段2a、2b、2cのいずれかが、送信手段1の変調系情報を知ればよい。また、送信手段1は受信手段2a、2b、2cで共有された量子暗号鍵を知る必要はない。
- [0024] なお、図1では、受信手段数が3である例を示したが、受信手段数は2であってもよく、また、4以上であっても構わない。
- [0025] また、全ての受信手段がフォトンを受信し、かつ、全ての受信手段が同一の復調系を採用した場合にのみ、受信手段間でビット情報が共有されるため、受信手段数が増加すると、量子暗号鍵の共有速度は低下する。しかしながら、量子暗号鍵の共有速度は、情報の伝送速度とは無関係であり、多くの場合、量子暗号鍵の共有速度は一定以上であればあまり重要ではない。
- [0026] 以上説明したように、この実施の形態の量子暗号鍵配送システムによれば、各伝送路に送出されるパルスには2つ以上のフォトンが含まれることがないように制御され、送信手段と2以上の受信手段のうちの少なくとも一つの受信手段との間で送信手段

が選択した変調系情報が交換され、2以上の受信手段のそれぞれが選択した復調系情報と、光子到着の有無情報とが受信手段のそれぞれの間で交換され、2以上の受信手段の全てが光子を受信し、かつ、2以上の受信手段のそれぞれが選択した復調系の全てと、送信手段の選択した変調系とが一致した場合に量子暗号鍵を共有するようにしているので、送信者を含む3者以上の複数ユーザが量子暗号鍵を容易かつ安全に共有することができる。

[0027] 実施の形態2.

図2は、本発明の実施の形態2にかかる量子暗号鍵配送システムの構成を示す概念図である。同図に示す量子暗号鍵配送システムの図1との相違は、分波手段11の3つの各出力に可変減衰器12a、12b、12cを備えた点にある。なお、その他の構成については実施の形態1の構成と同一、あるいは同等であり、これらの部分については同一符号を付して示している。

[0028] 上述のように、量子暗号鍵配送システムでは、1パルスあたりの光子数が1以下となるように制御することが重要である。そこで、図2に示す量子暗号鍵配送システムでは、伝送路3a、3b、3cにそれぞれ送出される光信号が1パルスあたり1光子を超えないように、可変減衰器を12a、12b、12cをそれぞれ用いて制御している。また、受信手段2a、2b、2cで測定された結果と送信側の送信結果とが不一致となる要因として伝送路上のノイズが影響するので、伝送路3a、3b、3cのそれぞれに可変減衰器を12a、12b、12cを挿入し、各伝送路の伝送路特性に応じた減衰量の制御を可能とする構成としている。なお、可変減衰器12a、12b、12cの制御には、例えば、光強度などをモニタしたフィードバック回路を用いるように構成すればよい。

[0029] 以上説明したように、この実施の形態の量子暗号鍵配送システムによれば、送信手段に接続される2経路以上の伝送路に可変減衰器をさらに備えるように構成しているので、各伝送路にそれぞれ送出される光信号の1パルスあたりの光子数が1を超えないように制御することができ、量子暗号鍵の共有を確実かつ安定的に行うことができる。

[0030] 実施の形態3.

図3は、本発明の実施の形態3にかかる量子暗号鍵配送システムの構成を示す概

念図である。同図に示す量子暗号鍵配送システムの図1との相違は、送信手段1と受信手段2とが、それぞれの信号処理手段6a、6bを備え、送信手段1および受信手段2の一部(図3の例では受信手段2c)がその機能を共有する誤り率検出手段10を備えた点にある。なお、その他の構成については実施の形態1の構成と同一、あるいは同等であり、これらの部分については同一符号を付して示している。

[0031] 図3に示す量子暗号鍵配送システムでは、誤り率検出手段10によって送受信間の誤りが検出される。送信手段と受信手段間で誤りを検出することにより、BB84方式などの従来技術と同一原理により盗聴者の存在を確実に検出しつつ、量子暗号鍵の共有が可能となる。ただし、従来技術との大きな相違点は、誤り検出を送信手段と受信手段の一部とのみで行えばよいことにある。送信手段が全ての受信手段が選択した復調系を知る必要はないため、送信手段は受信手段が共有した量子暗号鍵を知らなくてもよい。

[0032] なお、全ての受信手段が送信手段との間で誤り検出を行うこともできるが、全ての受信手段が送信手段との間で誤り検出を行うことは必須ではない。また、受信手段同士が誤り検出を行うことを妨げるものでもない。

[0033] 以上説明したように、この実施の形態の量子暗号鍵配送システムによれば、2以上の受信手段の全てが光子を受信し、かつ、2以上の受信手段のそれぞれが選択した復調系の全てと、送信手段の選択した変調系とが一致した場合にのみ、送信手段と、2以上の受信者との間で共有したビット列の誤り率を検出するようにしているので、盗聴者の存在を確実に検出しつつ、量子暗号鍵の共有が可能となる。

[0034] 実施の形態4.

図4は、本発明の実施の形態4にかかる量子暗号鍵配送システムの構成を示す概念図である。同図に示す量子暗号鍵配送システムの図3との相違は、受信手段2a、2b、2cがそれぞれの信号処理手段6b-1、6b-2、6b-3を備え、受信手段2a、2b、2cのみ(送信手段は利用しない)がその機能を共有する誤り率検出手段10を備えた点にある。なお、その他の構成については実施の形態3の構成と同一、あるいは同等であり、これらの部分については同一符号を付して示している。

[0035] 図4に示す量子暗号鍵配送システムでは、送信手段1は送信変調系情報の送信を

行い、受信手段からの復調系の情報・光子受信などの一切の情報を受け取らない。また、受信手段間で誤りを検出することにより、BB84方式などの従来技術と同一原理により盗聴者の存在を確実に検出しつつ、3以上の受信手段を利用する受信者との間で量子暗号鍵の共有が可能となる。ただし、従来技術と大きく異なり、送信手段が受信手段の復調系を知る必要がなく、誤り検出を受信手段間のみで行えばよい。また、送信手段は、受信手段が共有した量子暗号鍵を知らなくてもよい。このような特徴から、送信手段を利用する送信者が絶対的に信頼できる対象でなくともよい。このような特徴を利用すれば、例えば、第3者が提供した量子通信路を利用して任意の受信者のみで量子暗号鍵の共有が可能となる。

[0036] 以上説明したように、この実施の形態の量子暗号鍵配送システムによれば、2以上の受信手段の全てが光子を受信し、かつ、2以上の受信手段のそれぞれが選択した復調系の全てと、送信手段の選択した変調系とが一致した場合にのみ、2以上の受信者との間で共有したビット列の誤り率を検出するようにしているので、誤り検出を受信手段間のみで行えばよく、また、送信手段にとって受信手段が共有した量子暗号鍵を知る必要がないので、任意の受信者のみで量子暗号鍵の共有が可能となる。

[0037] 実施の形態5.

図5は、本発明の実施の形態5にかかる量子暗号鍵配送システムの構成を示す概念図である。同図に示す量子暗号鍵配送システムの図1との相違は、受信手段の数が5となった点にある。なお、その他の構成については実施の形態3の構成と同一、あるいは同等であり、これらの部分については同一符号を付して示している。

[0038] 図5に示す量子暗号鍵配送システムでは、受信手段2a、2b、2cにて相互に選択した復調系情報とパルスの到着の有無情報とが交換され、これらの3者間で量子暗号鍵が共有される。略同時に、受信手段2d、2eも互いに選択した復調系情報とパルスの到着の有無情報とが交換され、これらの2者間で量子暗号鍵が共有される。ところが、すでに上述した量子通信の原理から明らかのように、受信手段2a、2b、2cと、受信手段2d、2eとが同一な送信手段1が送出する光パルスを受信したとしても、受信手段2a、2b、2cが共有する量子暗号鍵と、受信手段2d、2eが共有する量子暗号鍵とを異なる量子暗号鍵とすることが可能となる。したがって、同一の送信手段が送出す

る光パルスを用いて、複数のグループが略同時に量子暗号鍵を共有することができる。

[0039] また、かかる構成によれば、光子発生器を有する送信手段が送出する光パルスを複数のユーザ、複数のシステムで共有できるので、システムの構築が安価かつ簡易となるという効果が生ずる。

[0040] なお、図5のシステムにおいても、図3に示す実施の形態3の量子暗号鍵配送システムと同様に、各グループごとに誤り検出を行うことで、盗聴者の存在を確実に検出することが可能となる。

[0041] 以上説明したように、この実施の形態の量子暗号鍵配送システムによれば、光子発生手段を複数の量子暗号鍵配送システムで共有するようにしているので、複数のユーザあるいは複数システム間で光子発生器の共有が可能となり、システムの構成を安価、かつ簡易な構成とすることができる。

産業上の利用可能性

[0042] 以上のように、本発明にかかる量子暗号鍵配送システムは、複数のユーザあるいは複数システム間での量子暗号鍵の共有に有用であり、特に、送信者が絶対的に信頼できる対象でない場合や、複数のユーザグループごとに個別に量子暗号鍵を共有したい場合など、さまざまなニーズに柔軟に対応できる量子暗号鍵配送システムとして好適である。

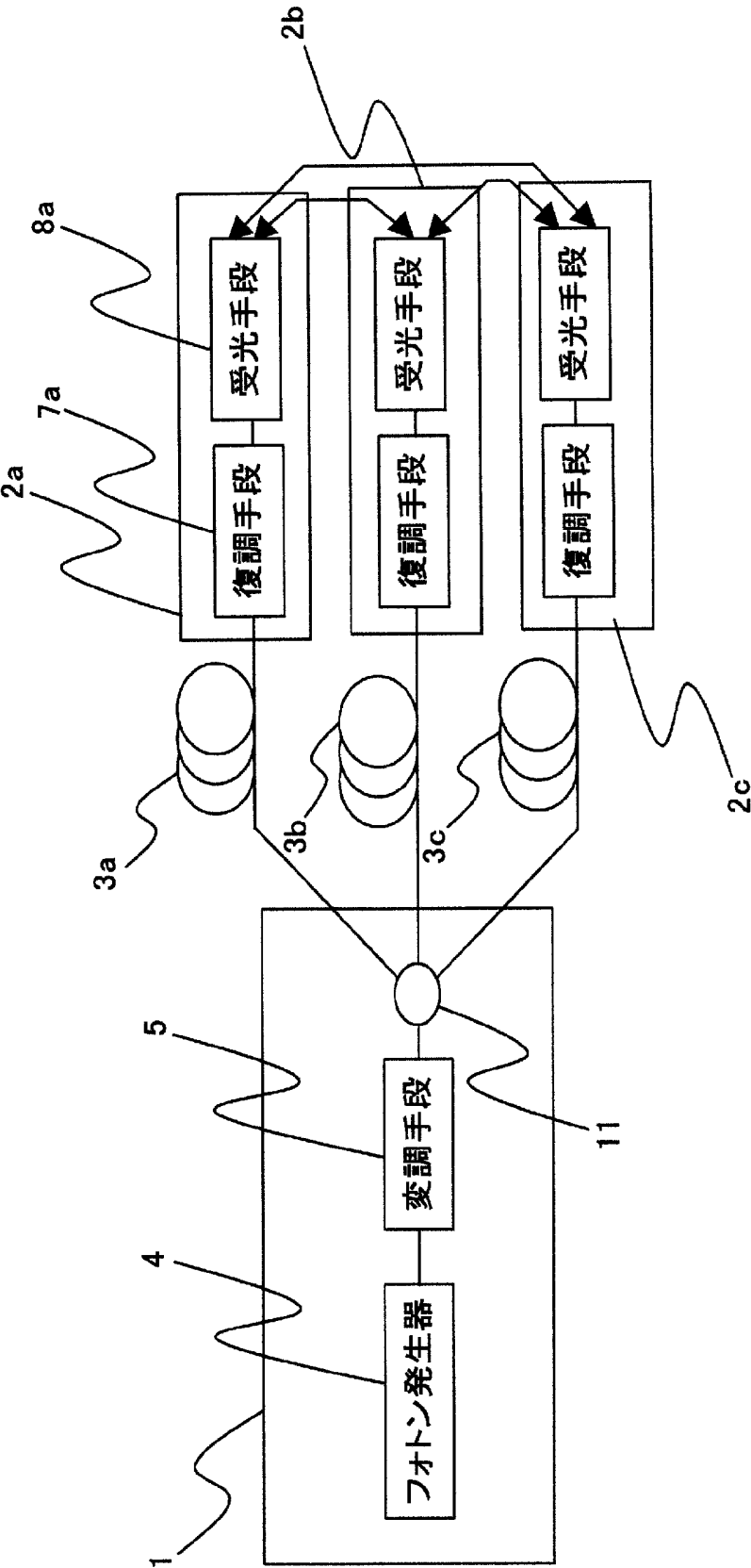
請求の範囲

- [1] 量子暗号鍵を共有するための量子暗号鍵配送システムにおいて、
光子発生手段と、選択可能な2系以上の変調系を有する変調手段と、を具備する送信手段と、
前記送信手段に接続された2経路以上の伝送路と、
前記2経路以上の伝送路のそれぞれに接続され、選択可能な2系以上の復調系を有する復調手段を具備する2以上の受信手段と、
を備え、
前記各伝送路に送出されるパルスには2つ以上の光子が含まれることがないように制御され、
前記送信手段と前記2以上の受信手段のうちの少なくとも一つの受信手段との間で該送信手段が選択した変調系情報が交換され、
前記2以上の受信手段のそれぞれが選択した復調系情報と、光子到着の有無情報とが該受信手段のそれぞれの間で交換され、
前記2以上の受信手段の全てが光子を受信し、かつ、該2以上の受信手段のそれぞれが選択した復調系の全てと、前記送信手段の選択した変調系とが一致した場合に前記量子暗号鍵を共有することを特徴とする量子暗号鍵配送システム。
- [2] 前記送信手段と、該送信手段に接続された2経路以上の伝送路との間にそれぞれ挿入される可変減衰器をさらに備えることを特徴とする請求項1に記載の量子暗号鍵配送システム。
- [3] 前記2以上の受信手段の全てが光子を受信し、かつ、該2以上の受信手段のそれぞれが選択した復調系の全てと、前記送信手段の選択した変調系とが一致した場合にのみ、該送信手段と、該2以上の受信者との間でビット列を共有し、該共有したビット列の誤り率を検出する誤り率検出手段をさらに備えることを特徴とする請求項1に記載の量子暗号鍵配送システム。
- [4] 前記2以上の受信手段の全てが光子を受信し、かつ、該2以上の受信手段のそれぞれが選択した復調系の全てと、前記送信手段の選択した変調系とが一致した場合にのみ、該2以上の受信者との間でビット列を共有し、該共有したビット列の誤り率

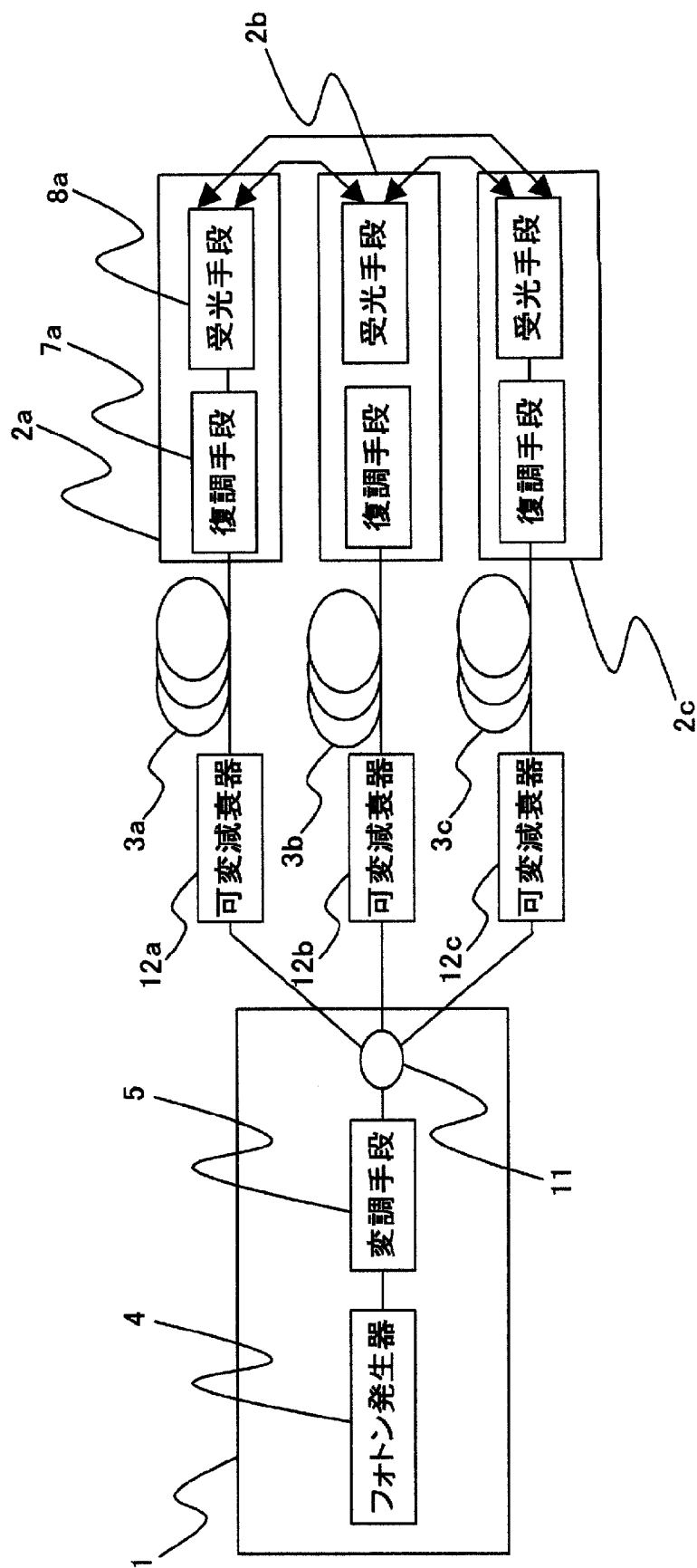
を検出する誤り率検出手段をさらに備えることを特徴とする請求項1に記載の量子暗号鍵配送システム。

- [5] 前記光子発生手段は、複数の量子暗号鍵配送システムで共有されることを特徴とする請求項1に記載の量子暗号鍵配送システム。
- [6] 変調系および復調系として位相変調器を用いることを特徴とする請求項1に記載の量子暗号鍵配送システム。
- [7] 変調系および復調系として偏波変調器を用いることを特徴とする請求項1に記載の量子暗号鍵配送システム。

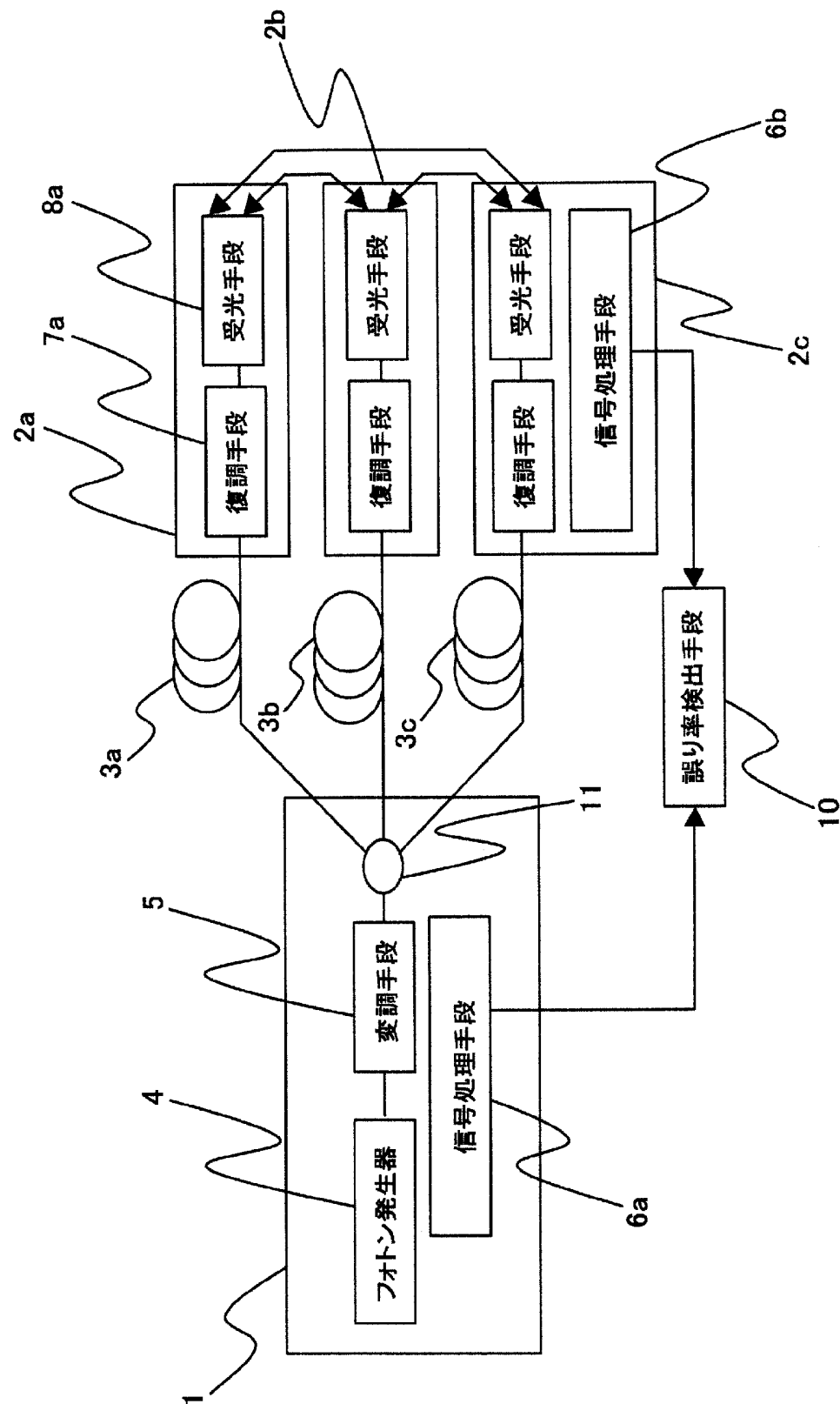
[図1]



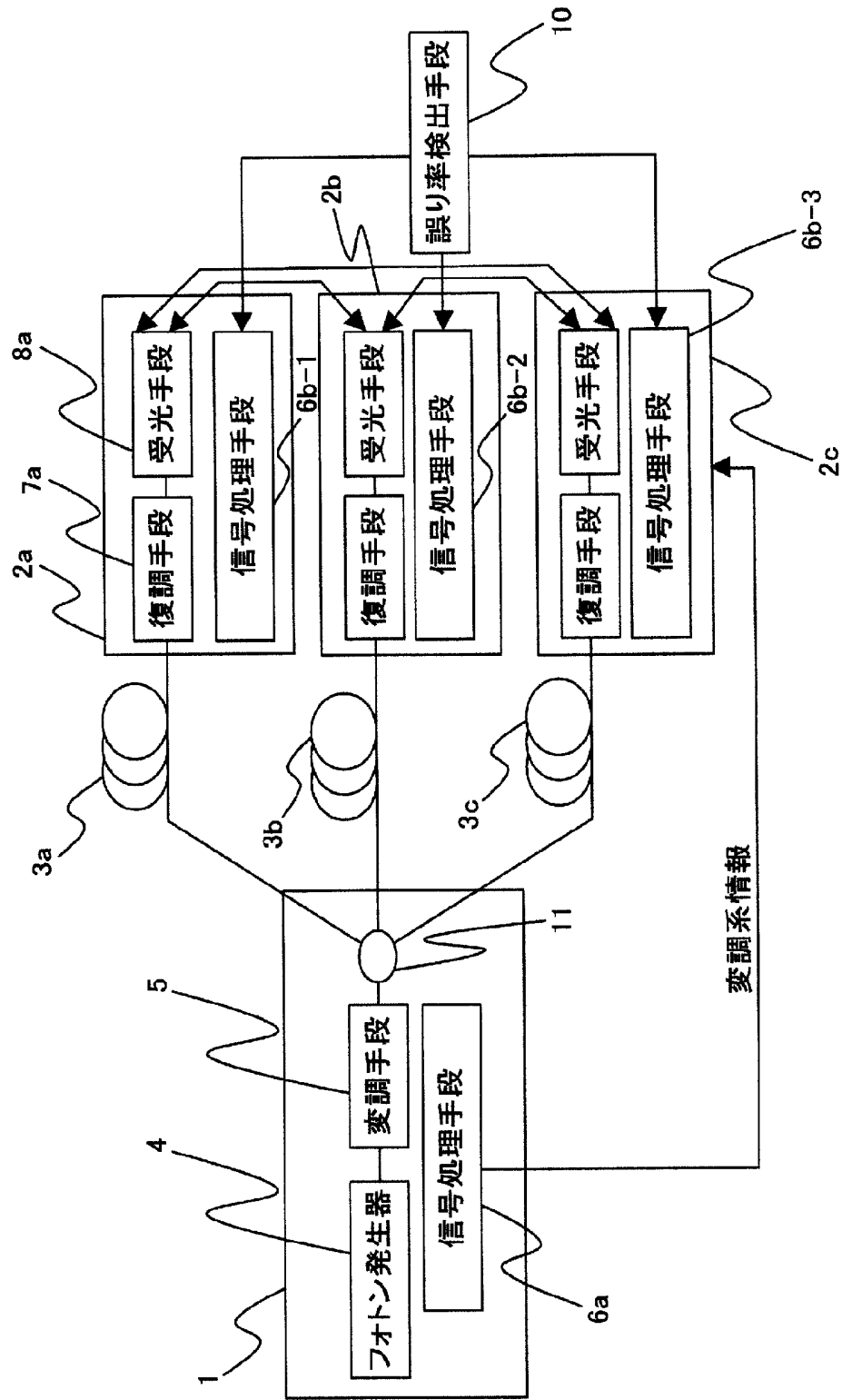
[図2]



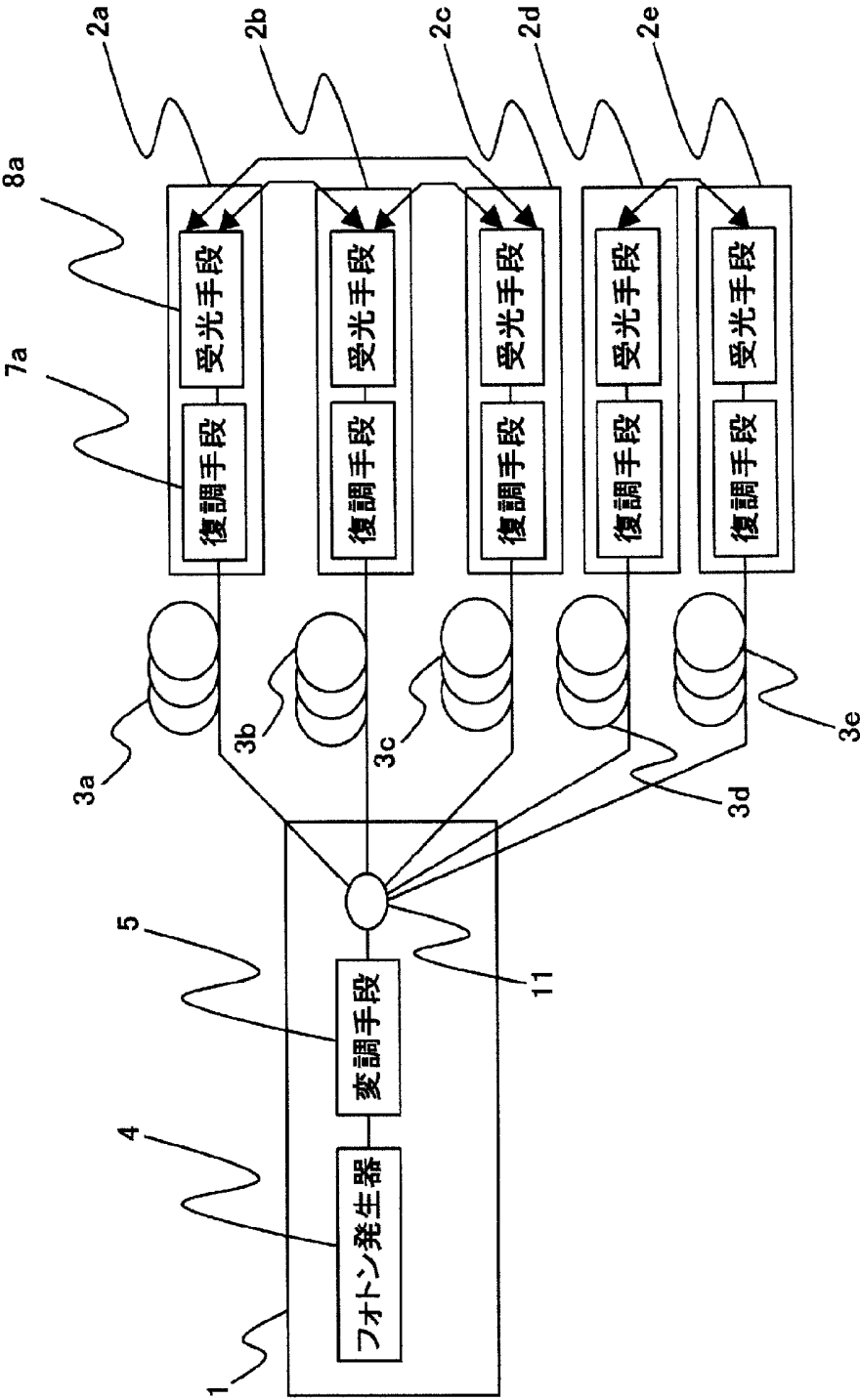
[図3]



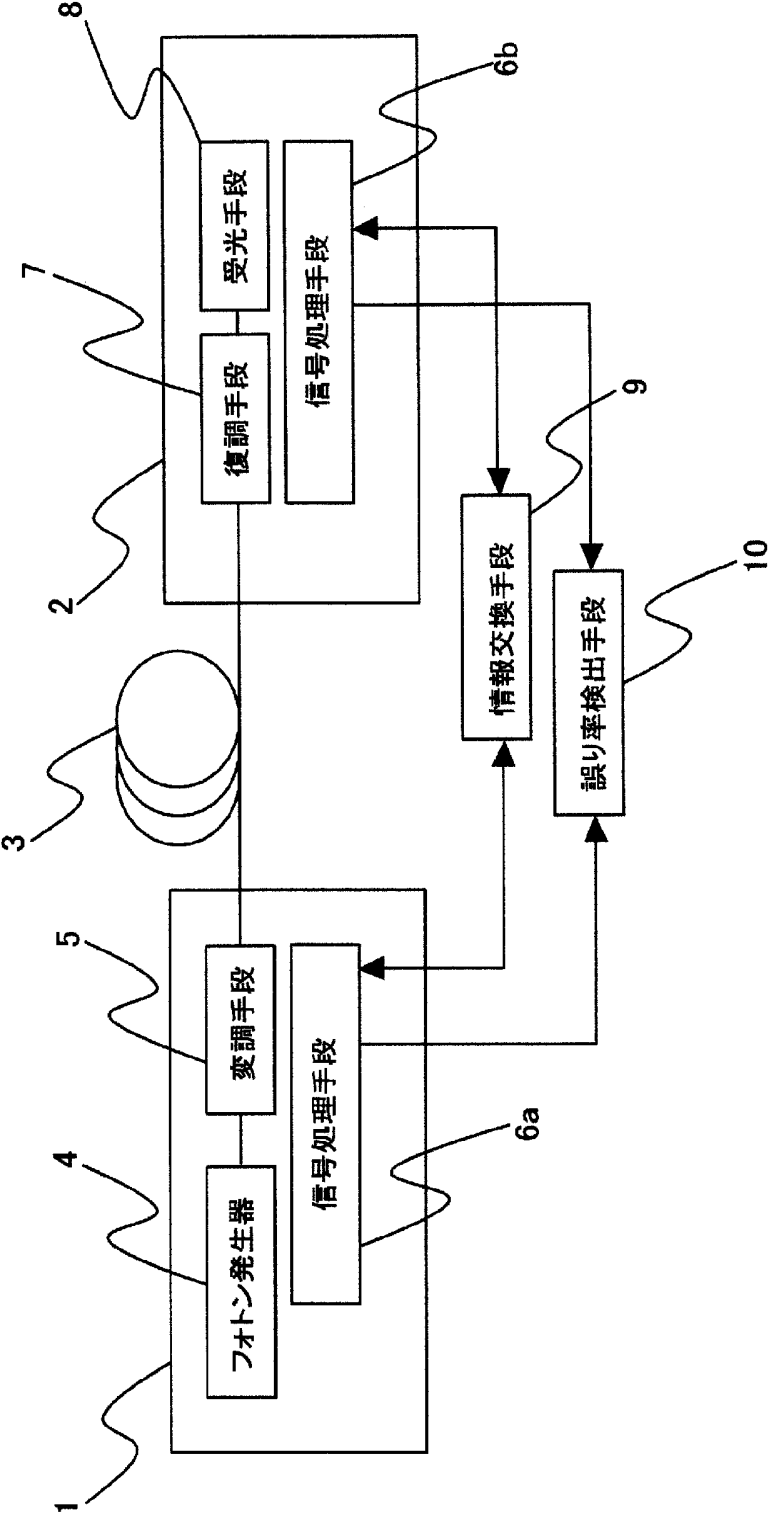
[図4]



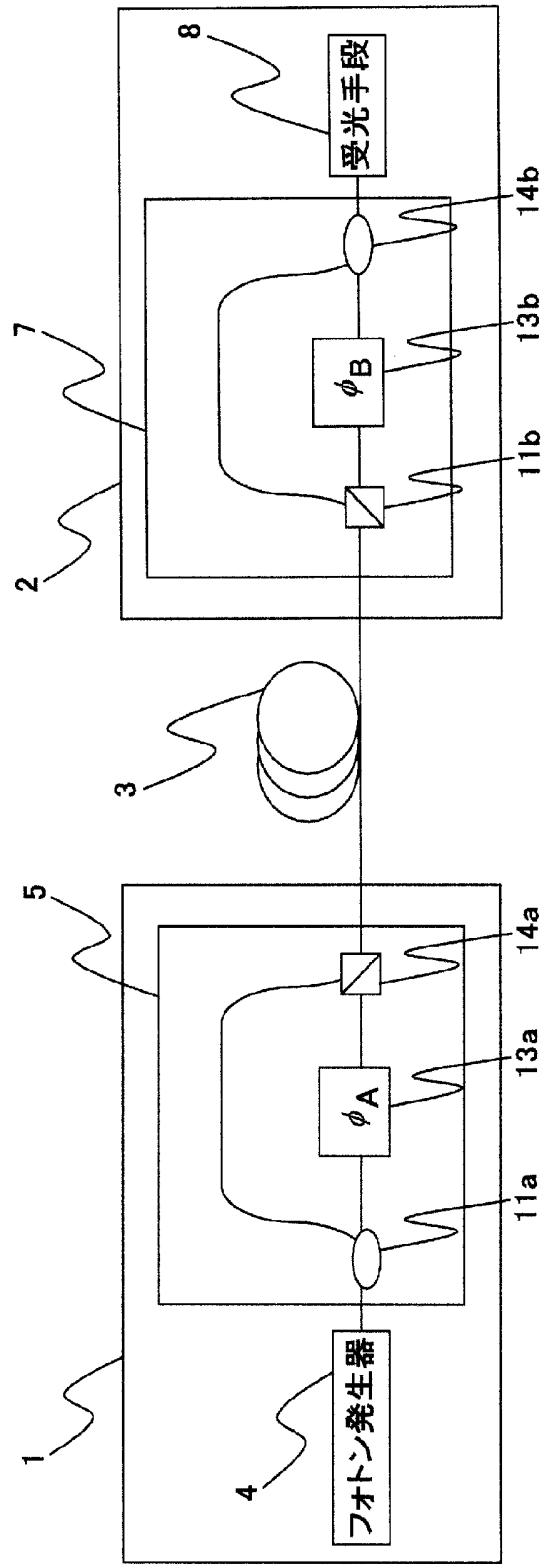
[図5]



[図6]



[図7]



送信者の変調 ϕ_A

" π "測定系 " $\pi/2$ "測定系

ビット	0	1
位相	0	π

ビット	0	1
位相	$\pi/2$	$3\pi/2$

受信者の変調 ϕ_B
(測定系を選択)

測定系	" π "	" $\pi/2$ "
位相	0	$\pi/2$

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/009931

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L9/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L9/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Y. MU, Y. ZHENG, Y. LIN, Multi-user quantum cryptography, In: Proceedings of International Symposium on Information Theory and Its Applications, 1994, pages 245 to 250	1, 3-7 2
Y	JP 2003-37593 A (Mitsubishi Electric Corp.), 07 February, 2003 (07.02.03), Par. Nos. [0003] to [0004]; Fig. 5 (Family: none)	2

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
25 August, 2004 (25.08.04)

Date of mailing of the international search report
14 September, 2004 (14.09.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/12

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/12

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2004年

日本国登録実用新案公報 1994-2004年

日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	Y. MU, Y. ZHENG, Y. LIN, Multi-user quantum cryptography, In: Proceedings of International Symposium on Information Theory and Its Applications, 1994, p.245-250	1,3-7
Y		2
Y	JP 2003-37593 A (三菱電機株式会社) 2003.02.07, 段落【0003】 - 【0004】, 図5 (ファミリーなし)	2

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

25.08.2004

国際調査報告の発送日

14.9.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5M

3365

電話番号 03-3581-1101 内線 3597