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

特許第4095536号
(P4095536)

(45)発行日　平成20年6月4日(2008.6.4)　(24)登録日　平成20年3月14日(2008.3.14)

(51)Int.Cl.			F I		
H04L	9/12	(2006.01)	H04L	9/00	631
G02F	1/39	(2006.01)	G02F	1/39	
G02F	2/00	(2006.01)	G02F	2/00	

請求項の数 7　(全 15 頁)

(21)出願番号　特願2003-370922(P2003-370922)
(22)出願日　平成15年10月30日(2003.10.30)
(65)公開番号　特開2005-136721(P2005-136721A)
(43)公開日　平成17年5月26日(2005.5.26)
審査請求日　平成17年2月9日(2005.2.9)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎

最終頁に続く

(54)【発明の名称】秘密鍵配布方法および秘密鍵配布装置

(57)【特許請求の範囲】

【請求項１】

秘密鍵となる関連づいた2つの乱数表を、場所Aと場所Bとの間にN箇所の中継所R(i)（i=1、2、…、N）を設けて、前記AとBの2箇所間に配布する秘密鍵配布方法であって、

光子発生部により、N+1組の、エンタングルメントで結ばれた光子P1(j)と光子P2(j)とからなる光子対PP(j)（j=1、2、…、N+1）を発生させ、

前記光子発生部に接続された光路を介して、光子対PP(1)のうち光子P1(1)をAに、光子P2(1)をR(1)に送り、光子対PP(k)のうち光子P1(k)をR(k-1)に、光子P2(k)をR(k)に送り（k=2、3、…、N）、光子対PP(N+1)のうち光子P1(N+1)をR(N)に、光子P2(N+1)をBに送り、

それぞれの光子がA、R(i)、およびBに到達した後、それぞれの光子を測定するためにA、R(i)、およびBに設けられた光子測定器に含まれる基底調整用光学素子の基底をAとR(1)、R(m)とR(m+1)（m=1、2、…、N-1)、R(N)とBとの間で切り替え信号発生器によって決め情報交換して、AとR(1)、R(m)とR(m+1)、R(N)とBのそれぞれの間で互いにエンタングルメントで結ばれた光子を同じ基底を用いて前記光子測定器に含まれる光検出器によって測定し、予め定めた対応関係に従って各光子の測定値に対応するビットをA、R(i)、およびBに設けられたデータ取り込み・演算・記憶装置で取得し、Aにおいて光子P1(1)の測定で取得したビットをB(P1(1))とし、R(i)において光子P2(i)の測定で取得したビットをB(P2(i))、光子P1(i+1)の測定で取得したビットをB(P1(i+1))とし、Bにおいて光子P2(N+1)の測定で取得したビットをB(P2(N+1))とし、

R(1)ではB(P2(1))とB(P1(2))に応じ、R(2)に対して、B(P2(2))を反転するか否かの情報

C(1)を送り、R(2)ではC(1)に従ってB(P2(2))をB(P2(2))'とし、
次いでR(m)ではB(P2(m))'とB(P1(m+1))に応じ、R(m+1)に対して、B(P2(m+1))を反転するか否かの情報C(m)を送り、R(m+1)ではC(m)に従ってB(P2(m+1))をB(P2(m+1))'とする、という操作をm=2、3、…、N-1に関してこの順で行い、
次いでR(N)ではB(P2(N))'とB(P1(N+1))に応じ、Bに対して、B(P2(N+1))を反転するか否かの情報C(N)を送り、BではC(N)に従ってB(P2(N+1))をB(P2(N+1))'とすることにより、Aにおいて取得したビットB(P1(1))とBにおいて取得したビットB(P2(N+1))'とを関連づけ、
以上の各操作によりAとBとで関連づいたビットを取得する手順を必要な回数だけ繰り返し、第q回目の手順により取得されるB(P1(1))とB(P2(N+1))'とをそれぞれAとBとで取得する乱数表の第q番目のビットとする
ことを特徴とする秘密鍵配布方法。

【請求項２】
秘密鍵となる関連づいた2つの乱数表を、場所Aと場所Bとの間にN箇所の中継所R(i)（i=1、2、…、N）を設けて、前記AとBの2箇所間に配布する秘密鍵配布方法であって、
Aに乱数列BA(r)（r=1、2、…）を用意し、
光子発生部により、N+1組の、エンタングルメントで結ばれた光子P1(j)と光子P2(j)とからなる光子対PP(j)（j=1、2、…、N+1）を発生させ、
前記光子発生部に接続された光路を介して、光子対PP(1)のうち光子P1(1)をAに、光子P2(1)をR(1)に送り、光子対PP(k)のうち光子P1(k)をR(k-1)に、光子P2(k)をR(k)に送り（k=2、3、…、N）、光子対PP(N+1)のうち光子P1(N+1)をR(N)に、光子P2(N+1)をBに送り、
それぞれの光子がA、R(i)、およびBに到達した後、それぞれの光子を測定するためにA、R(i)、およびBに設けられた光子測定器に含まれる基底調整用光学素子の基底をAとR(1)、R(m)とR(m+1)（m=1、2、…、N-1）、R(N)とBとの間で切り替え信号発生器によって決め情報交換して、AとR(1)、R(m)とR(m+1)、R(N)とBのそれぞれの間で互いにエンタングルメントで結ばれた光子を同じ基底を用いて前記光子測定器に含まれる光検出器によって測定し、予め定めた対応関係に従って各光子の測定値に対応するビットをA、R(i)、およびBに設けられたデータ取り込み・演算・記憶装置で取得し、Aにおいて光子P1(1)の測定で取得したビットをB(P1(1))とし、R(i)において光子P2(i)の測定で取得したビットをB(P2(i))、光子P1(i+1)の測定で取得したビットをB(P1(i+1))とし、Bにおいて光子P2(N+1)の測定で取得したビットをB(P2(N+1))とし、
Aでは乱数列BA(r)（r=1、2、…）のq番目のビットBA(q)とB(P1(1))に応じ、R(1)に対して、B(P2(1))を反転するか否かの情報C(A)を送り、R(1)ではC(A)に従ってB(P2(1))をB(P2(1))'とし、
R(1)ではB(P2(1))'とB(P1(2))に応じ、R(2)に対して、B(P2(2))を反転するか否かの情報C(1)を送り、R(2)ではC(1)に従ってB(P2(2))をB(P2(2))'とし、
次いでR(m)ではB(P2(m))'とB(P1(m+1))に応じ、R(m+1)に対して、B(P2(m+1))を反転するか否かの情報C(m)を送り、R(m+1)ではC(m)に従ってB(P2(m+1))をB(P2(m+1))'とする、という操作をm=2、3、…、N-1に関してこの順で行い、
次いでR(N)ではB(P2(N))'とB(P1(N+1))に応じ、Bに対して、B(P2(N+1))を反転するか否かの情報C(N)を送り、BではC(N)に従ってB(P2(N+1))をB(P2(N+1))'とすることにより、Aに用意した乱数列BA(r)のq番目のビットBA(q)とBにおいて取得したビットB(P2(N+1))'とを関連づけ、
以上の各操作によりAとBとで関連づいたビットを取得する手順を必要な回数だけ繰り返して、Aに用意した乱数列をBに配布する
ことを特徴とする秘密鍵配布方法。

【請求項３】
N+1組の光子対PP(j)が、PP(j)を構成する光子を前記光子測定器に含まれる光検出器によってある基底1で測定したときに観測される2種類の測定値をS1、S2として、その基底による光子P1(j)の互いに直交する2つの固有状態φ1(j,S1)およびφ1(j,S2)ならびに光子P2(j)の互いに直交する2つの固有状態φ2(j,S1)とφ2(j,S2)を用いて、φ1(j,S1)φ2（j,S2

)+exp(iθ)φ1(j,S2)φ2(j,S1)（θは任意の実数)と表され、
AとR(1)、R(m)とR(m+1)、R(N)とBのそれぞれの間で光子の測定に用いる共通の基底を、前記基底1または前記基底1と直交しない別の基底2とし、各光子の測定値と取得するビットとの対応関係を、基底1で測定したときに、S1が観測された場合のビットを0、S2が観測された場合のビットを１とし、基底2で測定したときに、観測される2種類の測定値をS1'、S2'として、S1'が観測された場合のビットを0、S2'が観測された場合のビットを1とし、
R(1)ではB(P2(1))とB(P1(2))とが同じであれば「B(P2(2))を反転しない」という情報C(1)、異なれば「B(P2(2))を反転する」という情報C(1)を、R(2)に対して送り、R(2)ではC(1)に従ってB(P2(2))をB(P2(2))'とし、
次いでR(m)ではB(P2(m))'とB(P1(m+1))が同じなら「B(P2(m+1))を反転しない」という情報C(m)、異なれば「B(P2(m+1))を反転する」という情報C(m)を、R(m+1)に対して送り、R(m+1)ではC(m)に従ってB(P2(m+1))をB(P2(m+1))'とする、という操作をm=2、3、…、N-1に関してこの順で行い、
次いでR(N)ではB(P2(N))'とB(P1(N+1))が同じなら「B(P2(N+1))を反転しない」という情報C(N)、異なれば「B(P2(N+1))を反転する」という情報C(N)を、Bに対して送り、BではC(N)に従ってB(P2(N+1))をB(P2(N+1))'とする
ことを特徴とする請求項１または２に記載の秘密鍵配布方法。

【請求項４】
それぞれの光子がA、R(i)、およびBに到達した後、前記光子測定器に含まれる前記基底調整用光学素子の基底をAとR(1)、R(1)とR(2)、R(m)とR(m+1)（m=2、3、…、N-1)、R(N)とBとの間で切り替え信号発生器によって決め情報交換して、測定を行うまでの間、A、R(1)、R(m)、およびBに設置した遅延路で光子を保持することを特徴とする請求項１または２に記載の秘密鍵配布方法。

【請求項５】
秘密鍵となる関連づいた2つの乱数表を、場所Aと場所Bとの間にN箇所の中継所R(i)（i=1、2、…、N）を設けて、前記AとBの2箇所間に配布する秘密鍵配布装置であって、
AとR(1)、R(m)とR(m+1)（m=1、2、…、N-1)、R(N)とBとの間にそれぞれ設けられ、光子対PP(1)、光子対PP(k)（k=2、3、…、N）、光子対PP(N+1)を発生させる光子発生部と、
各々の光子発生部から、光子対PP(1)のうち光子P1(1)をAに、光子P2(1)をR(1)に送り、光子対PP(k)のうち光子P1(k)をR(k-1)に、光子P2(k)をR(k)に送り（k=2、3、…、N）、光子対PP(N+1)のうち光子P1(N+1)をR(N)に、光子P2(N+1)をBに送るための光路と、
前記光子発生部から送られる光子P1(1)、光子P2(1)、光子P1(k)、光子P2(k)、光子P1(N+1)、光子P2(N+1)を測定するために、A、R(i)、Bにそれぞれ設けられた、遅延路、基底調整用光学素子および光子検出器を含む光子測定部と、
AとR(1)、R(m)とR(m+1)（m=1、2、…、N-1)、R(N)とBのそれぞれの間で、互いにエンタングルメントで結ばれた光子を同じ基底を用いて測定するように、前記基底調整用光学素子の基底を切り替える信号を発生する切り替え信号発生器と、
A、R(i)、Bにそれぞれ設けられ、前記光子測定部においてある基底で測定された各々の光子の測定値を取り込み、予め定めた対応関係に従って前記測定値に対応するビットを記憶するデータ取り込み・演算・記憶装置であって、さらに各中継所のデータ取り込み・演算・記憶装置はその中継所で取得される2つのビットに応じ、次に中継所またはBのデータ取り込み・演算・記憶装置に対し、1つのビットを反転するか否かの情報を演算して送り、前記情報が送られたデータ取り込み・演算・記憶装置は1つのビットを操作するように構成されているデータ取り込み・演算・記憶装置と
を具備したことを特徴とする秘密鍵配布装置。

【請求項６】
前記切り替え信号発生器は、A、R(1)、R(m)、R(m+1)、R(N)、Bの全てまたは一部の内部に設けられていることを特徴とする請求項５に記載の秘密鍵配布装置。

【請求項７】

前記切り替え信号発生器は、レーザー光源と、ビームスプリッターと、ビームスプリッターの2つの出口に設けられ、それぞれ前記基底調整用光学素子のドライバーに接続された2つの光子検出器とを有することを特徴とする請求項５または６に記載の秘密鍵配布装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、光子の量子状態に情報を載せ、盗聴することがほとんど不可能な量子通信と、量子通信で伝送されてきた情報をいったん古典情報にした後、再び量子通信で伝送する古典的な中継とを組み合わせた秘密鍵配布方法および秘密鍵配布装置に関する。

【背景技術】

【０００２】

量子暗号通信では、光子の量子状態に情報を担わせ、その状態の複製が原理的に不可能であることを利用して、安全な秘密鍵配布を行う。しかし、複製が不可能という性質は、安全上の利点である反面、光ファイバーなどの通信路で光子が減衰しても増幅ができないことを意味する。このように単純な信号増幅による中継ができないため、現在のところ量子暗号通信が可能なのは、一度発生した光子が減衰せずに届く距離に限られる。従来技術では、この距離は、10bps程度の通信速度を確保する場合に100㎞程度であるとされている。

【０００３】

そこで、遠距離間でエンタングルメントと呼ばれる量子相関を持つ量子系を生成し、このような量子系を利用して長距離間の量子暗号通信を実現する研究が進められている（非特許文献１、特許文献１、特許文献２参照)。原理的にほぼ完全な（無条件な）安全性を求める場合は、このような方法が有効である。

【０００４】

一方、必要な安全性の水準から判断して、中継所の安全性は十分確保されていると見なされる場合には、空間的に広がり完全な安全性の確保が困難な中継所間は量子通信を利用するが、中継所内では量子通信で伝送されてきた情報をいったん古典情報にして受け渡し、再び量子通信で伝送するという方法も実用的であり有用であると考えられる。

【０００５】

その際、最初の送信所と中継所の間、中継所間、中継所と最後の受信所間のそれぞれで量子暗号通信を行い、送りたい通信内容そのものを順次それぞれの場所の間で送るという方法が考えられる。しかし、この方法では、暗号通信したい場合には常に量子通信が必要となる。これに対して、もし秘密鍵（共通の乱数表）だけ予め共有しておけば、送りたい通信内容を暗号通信する際にその秘密鍵を用い、どこにいても利用し易い古典伝送路を経由して安全な暗号を送ることができ、都合がよい場合が多い。また、古典伝送路での通常の通信となるので、送りたい通信内容を送りたい時に速い通信速度で送れるという利点もある。そこで、秘密鍵の配布方法が重要になってくる。

【０００６】

古典的な中継所を利用して長距離通信用の秘密鍵を配布する際に、中継所間などでの量子通信に、現在盛んに実験が進められているエンタングルメントを利用しない秘密鍵配布の方法をそのまま適用しようとすると、中継のたびに（中継距離によらず）秘密鍵の数が1/2以下の一定の割合で減少するという問題があり、中継の意味がなくなる。この問題は以下のような理由によるものである。現在実験が行なわれている秘密鍵配布では、その安全性確保のために、秘密鍵の送信者が鍵を量子状態に載せて送信する際、および受信者が送られてきた鍵を量子状態の観測により受信する際に、それぞれ互いに関連しないランダムな基底を採用する。そして、送信および受信が終了した後に、送信者と受信者は互いの採用した基底の情報を古典通信路でやり取りして偶然基底が一致した場合の鍵だけ利用する。この方法では、たとえ互いの採用した基底の情報が漏れたとしても、すでに光子が量子伝送路（光ファイバーなど）を通過した後なので、量子伝送路から抜き出した光子をそ

の基底で観測し、秘密鍵の情報を得て同じ量子状態の光子を生成して量子伝送路に戻すというタイプの盗聴ができなくなる。しかし、その安全性と引き換えに基底が一致しなかったビットを捨てているため、上述したように中継のたびに秘密鍵の数が減少するという問題が生じる。

【０００７】

長距離通信用の秘密鍵そのものを、送りたい古典的な通信内容として、送信所と中継所の間、中継所間、中継所と受信所間のそれぞれで量子暗号通信を利用して送信するという方法も考えられる。この方法では、中継所間などで量子通信路と古典通信路を使って共有した秘密鍵を利用し、長距離間通信用の秘密鍵を安全に送るという操作を、次々と中継所間などで繰り返す。この場合、中継所間の量子暗号通信それぞれのために、基底の選択用とは別に、中継所間での量子暗号通信のために共有する秘密鍵の元となる乱数表も必要であり、大量の乱数を消費する。従って、質が高く効率のよい乱数生成機構が組み込まれていなければならないという問題がある。しかも、何度も秘密鍵を利用する必要があるので、無駄に捨てるビットを少なくしないと伝送速度を向上させることが困難である。

【０００８】

このように、中継所内の安全性は確保できると考えられる場合に、中継所間での安全な量子通信を繰り返すことにより遠距離間での秘密鍵配布を行おうとすると、中継のたびに秘密鍵の数が指数関数的に減少するか、または質の良い大量の乱数を効率よく生成しなければならなくなるという問題が生じる。しかし、従来はこれらの問題を解決する簡単な方法は知られていなかった。

【非特許文献１】L. -M. Duan et al., Nature, 414, 413(2001)

【特許文献１】特開平１１－３４６２１１号公報

【特許文献２】特開２０００－３３９３８７号公報

【発明の開示】

【発明が解決しようとする課題】

【０００９】

本発明の目的は、中継により秘密鍵の数が減少することがなく長距離化を実現することを可能にし、ビットの無駄がなく通信速度の高速化に有利で、質の良い乱数の効率良い生成機構を内蔵していることで安全性の高い秘密鍵配布方法および秘密鍵配布装置を提供することにある。

【課題を解決するための手段】

【００１０】

本発明の一態様に係る秘密鍵配布方法は、秘密鍵となる関連づいた2つの乱数表を、場所Aと場所Bとの間にN箇所の中継所R(i)（i=1、2、…、N）を設けて、前記AとBの2箇所間に配布する秘密鍵配布方法であって、

光子発生部により、N+1組の、エンタングルメントで結ばれた光子P1(j)と光子P2(j)とからなる光子対PP(j)（j=1、2、…、N+1）を発生させ、

前記光子発生部に接続された光路を介して、光子対PP(1)のうち光子P1(1)をAに、光子P2(1)をR(1)に送り、光子対PP(k)のうち光子P1(k)をR(k-1)に、光子P2(k)をR(k)に送り（k=2、3、…、N）、光子対PP(N+1)のうち光子P1(N+1)をR(N)に、光子P2(N+1)をBに送り、

それぞれの光子がA、R(i)、およびBに到達した後、それぞれの光子を測定するためにA、R(i)、およびBに設けられた光子測定器に含まれる基底調整用光学素子の基底をAとR(1)、R(m)とR(m+1)（m=1、2、…、N-1)、R(N)とBとの間で切り替え信号発生器によって決め情報交換して、AとR(1)、R(m)とR(m+1)、R(N)とBのそれぞれの間で互いにエンタングルメントで結ばれた光子を同じ基底を用いて前記光子測定器に含まれる光検出器によって測定し、予め定めた対応関係に従って各光子の測定値に対応するビットをA、R(i)、およびBに設けられたデータ取り込み・演算・記憶装置で取得し、Aにおいて光子P1(1)の測定で取得したビットをB(P1(1))とし、R(i)において光子P2(i)の測定で取得したビットをB(P2(i))、光子P1(i+1)の測定で取得したビットをB(P1(i+1))とし、Bにおいて光子P2(N+1)の測定で取得したビットをB(P2(N+1))とし、

R(1)ではB(P2(1))とB(P1(2))に応じ、R(2)に対して、B(P2(2))を反転するか否かの情報C(1)を送り、R(2)ではC(1)に従ってB(P2(2))をB(P2(2))'とし、
次いでR(m)ではB(P2(m))'とB(P1(m+1))に応じ、R(m+1)に対して、B(P2(m+1))を反転するか否かの情報C(m)を送り、R(m+1)ではC(m)に従ってB(P2(m+1))をB(P2(m+1))'とする、という操作をm=2、3、…、N-1に関してこの順で行い、
次いでR(N)ではB(P2(N))'とB(P1(N+1))に応じ、Bに対して、B(P2(N+1))を反転するか否かの情報C(N)を送り、BではC(N)に従ってB(P2(N+1))をB(P2(N+1))'とすることにより、Aにおいて取得したビットB(P1(1))とBにおいて取得したビットB(P2(N+1))'とを関連づけ、
以上の各操作によりAとBとで関連づいたビットを取得する手順を必要な回数だけ繰り返し、第q回目の手順により取得されるB(P1(1))とB(P2(N+1))'とをそれぞれAとBとで取得する乱数表の第q番目のビットとする
ことを特徴とする。

【００１１】

本発明の他の態様に係る秘密鍵配布方法は、秘密鍵となる関連づいた2つの乱数表を、場所Aと場所Bとの間にN箇所の中継所R(i)（i=1、2、…、N）を設けて、前記AとBの2箇所間に配布する秘密鍵配布方法であって、
Aに乱数列BA(r)（r=1、2、…）を用意し、
光子発生部により、N+1組の、エンタングルメントで結ばれた光子P1(j)と光子P2(j)とからなる光子対PP(j)（j=1、2、…、N+1）を発生させ、
前記光子発生部に接続された光路を介して、光子対PP(1)のうち光子P1(1)をAに、光子P2(1)をR(1)に送り、光子対PP(k)のうち光子P1(k)をR(k-1)に、光子P2(k)をR(k)に送り（k=2、3、…、N）、光子対PP(N+1)のうち光子P1(N+1)をR(N)に、光子P2(N+1)をBに送り、
それぞれの光子がA、R(i)、およびBに到達した後、それぞれの光子を測定するためにA、R(i)、およびBに設けられた光子測定器に含まれる基底調整用光学素子の基底をAとR(1)、R(m)とR(m+1)（m=1、2、…、N-1）、R(N)とBとの間で切り替え信号発生器によって決め情報交換して、AとR(1)、R(m)とR(m+1)、R(N)とBのそれぞれの間で互いにエンタングルメントで結ばれた光子を同じ基底を用いて前記光子測定器に含まれる光検出器によって測定し、予め定めた対応関係に従って各光子の測定値に対応するビットをA、R(i)、およびBに設けられたデータ取り込み・演算・記憶装置で取得し、Aにおいて光子P1(1)の測定で取得したビットをB(P1(1))とし、R(i)において光子P2(i)の測定で取得したビットをB(P2(i))、光子P1(i+1)の測定で取得したビットをB(P1(i+1))とし、Bにおいて光子P2(N+1)の測定で取得したビットをB(P2(N+1))とし、
Aでは乱数列BA(r)（r=1、2、…）のq番目のビットBA(q)とB(P1(1))に応じ、R(1)に対して、B(P2(1))を反転するか否かの情報C(A)を送り、R(1)ではC(A)に従ってB(P2(1))をB(P2(1))'とし、
R(1)ではB(P2(1))'とB(P1(2))に応じ、R(2)に対して、B(P2(2))を反転するか否かの情報C(1)を送り、R(2)ではC(1)に従ってB(P2(2))をB(P2(2))'とし、
次いでR(m)ではB(P2(m))'とB(P1(m+1))に応じ、R(m+1)に対して、B(P2(m+1))を反転するか否かの情報C(m)を送り、R(m+1)ではC(m)に従ってB(P2(m+1))をB(P2(m+1))'とする、という操作をm=2、3、…、N-1に関してこの順で行い、
次いでR(N)ではB(P2(N))'とB(P1(N+1))に応じ、Bに対して、B(P2(N+1))を反転するか否かの情報C(N)を送り、BではC(N)に従ってB(P2(N+1))をB(P2(N+1))'とすることにより、Aに用意した乱数列BA(r)のq番目のビットBA(q)とBにおいて取得したビットB(P2(N+1))'とを関連づけ、
以上の各操作によりAとBとで関連づいたビットを取得する手順を必要な回数だけ繰り返して、Aに用意した乱数列をBに配布する
ことを特徴とする。

【００１２】

本発明の他の態様に係る秘密鍵配布装置は、秘密鍵となる関連づいた2つの乱数表を、場所Aと場所Bとの間にN箇所の中継所R(i)（i=1、2、…、N）を設けて、前記AとBの2箇所

間に配布する秘密鍵配布装置であって、
AとR(1)、R(m)とR(m+1)（m=1、2、…、N-1)、R(N)とBとの間にそれぞれ設けられ、光子対PP(1)、光子対PP(k)（k=2、3、…、N）、光子対PP(N+1)を発生させる光子発生部と、
各々の光子発生部から、光子対PP(1)のうち光子P1(1)をAに、光子P2(1)をR(1)に送り、光子対PP(k)のうち光子P1(k)をR(k-1)に、光子P2(k)をR(k)に送り（k=2、3、…、N）、光子対PP(N+1)のうち光子P1(N+1)をR(N)に、光子P2(N+1)をBに送るための光路と、
前記光子発生部から送られる光子P1(1)、光子P2(1)、光子P1(k)、光子P2(k)、光子P1(N+1)、光子P2(N+1)を測定するために、A、R(i)、Bにそれぞれ設けられた、遅延路、基底調整用光学素子および光子検出器を含む光子測定部と、
AとR(1)、R(m)とR(m+1)（m=1、2、…、N-1)、R(N)とBのそれぞれの間で、互いにエンタングルメントで結ばれた光子を同じ基底を用いて測定するように、前記基底調整用光学素子の基底を切り替える信号を発生する切り替え信号発生器と、
A、R(i)、Bにそれぞれ設けられ、前記光子測定部においてある基底で測定された各々の光子の測定値を取り込み、予め定めた対応関係に従って前記測定値に対応するビットを記憶するデータ取り込み・演算・記憶装置であって、さらに各中継所のデータ取り込み・演算・記憶装置はその中継所で取得される2つのビットに応じ、次に中継所またはBのデータ取り込み・演算・記憶装置に対し、1つのビットを反転するか否かの情報を演算して送り、前記情報が送られたデータ取り込み・演算・記憶装置は1つのビットを操作するように構成されているデータ取り込み・演算・記憶装置とを具備したことを特徴とする。

【発明の効果】

【００１３】

本発明に係る秘密鍵配布方法および秘密鍵配布装置によれば、場所A、場所Bおよび中継所の安全性さえ確保できれば盗聴に関して安全な秘密鍵配布が実行でき、その際に中継ごとに秘密鍵が減少することなく長距離間での秘密鍵配布が可能であり、中継ごとに必要となる秘密鍵が組み込まれた質の良い物理乱数発生機構により自動的に生成され、しかもその秘密鍵生成において無駄に捨てるビットがないため伝送速度の高速化にも有利である。

【発明を実施するための最良の形態】

【００１４】

本発明の実施形態に係る秘密鍵配布方法の原理を説明する。
図１は、場所A（最初の送信所）、中継所、場所B（最後の受信所）の位置関係、生成させる光子対、および光子の分配を示す模式図である。図１に示すように、場所Aと場所Bの間には、N箇所の中継所R(i)（i=1、2、…、N）が設置されている。この図において、場所A、場所Bの2箇所間で、中継所での中継を行いながら、秘密鍵となるビットを1ビットずつ取得していく場合を考える。

【００１５】

まず、第1番目のビットを取得する手順を説明する。図１に示すように、N+1個のエンタングルメントで結ばれた光子対を生成させ、それぞれの光子対をPP(j)（j=1、2、…、N+1）とする。それぞれの光子対は、光子P1(j)と光子P2(j)で構成されているものとして、その片割れ同士を分配する。すなわち、光子対PP(1)のうち光子P1(1)をAに、光子P2(1)をR(1)に分配し、光子対PP(k)のうち光子P1(k)をR(k-1)に、P2(k)をR(k)に分配し（k=2、3、…、N)、光子対PP(N+1)のうちP1(N+1)をR(N)に、光子P2(N+1)をBに分配する。

【００１６】

次に、それぞれの光子がA、R(i)、Bに到達した後に、光子を測定する基底をAとR(1)、R(m)とR(m+1)（m=1、2、…、N-1)、R(N)とBの間でそれぞれ取り決める。この取り決めは通常の古典通信路を通して行っても安全性は損なわれない。なぜなら、たとえ盗聴されても、既にその基底で測定されるべき光子は安全なA、B、またはR(i)に到達しており、途中の量子伝送路（光ファイバーなど）から光子を抜き出し、その基底で観測して秘密鍵に関する情報を盗み、また改めて光子を挿入し、その盗聴を発覚しないようにするという攻撃ができないからである。

【００１７】

本発明では、光子が中継所などの安全な場所に入った後に、どの基底を使うかの情報をやりとりすればよい。このため、例えば片方の光子は中継所に入るとすぐに測定してしまい、その後にその光子の測定に利用した基底をもう片方の光子が保持されている中継所に教えるという方法を採用してもよい。遅延路で両方の光子を保持してもよいが、光子の保持は必須ではなく（少なくとも片方は保持しなくて良い場合があり）、むしろ保持しなくて済むのであれば保持しない方が好ましい。

【００１８】

A、B、またはR(i)に到達した光子は、到達後に決められた基底でそれぞれ測定され、その測定値に対して予め決められた対応関係によりビットに変換される。このようにして、A、B、R(i)のそれぞれで、最初のビットを得る。このとき得られるビットは、エンタングルメントという重ね合わせの状態の測定により確率的に波動関数の波束が収縮した結果として得られる値であり、物理的に完全に確率的な過程の結果であるため、乱数表や乱数生成装置を別に用意しなくても、自動的に質の良い乱数が得られる。また、光子対をなす個々の光子の測定値は予想不可能であるが、2つの光子の測定値の間にはエンタングルメントに基づく相関がある。

【００１９】

図２に、A、R(i)、Bのそれぞれで最初に取得されたビットを示す。図２に示すように、Aにおいて光子P1(1)の測定により取得されるビットをB(P1(1))とし、R(i)において光子P2(i)の測定により取得されるビットをB(P2(i))、光子P1(i+1)の測定により取得されるビットをB(P1(i+1))とし、Bにおいて光子P2(N+1)の測定により取得されるビットをB(P1(N+1))とする。図２において、破線で示した矢印は測定結果に（取得されるビット）に相関があることを示している。

【００２０】

B(P2(i))、B(P1(i+1))、B(P1(N+1))はいわば量子暗号における秘密鍵であり、これらを利用して、最初の中継所R(1)はAのビットを安全な秘密鍵を用いてR(2)に送り、R(2)はR(3)に送る、という具合に順次Bまで送ることが可能になる。ただし、本発明に係る方法では、秘密鍵によりエンコードした情報を送り、相手方でその情報により秘密鍵を操作して、送りたい情報に変化させるという形式をとる（すなわち、従来のように、秘密鍵によってエンコードした情報を送り、その情報を相手方の秘密鍵でデコードするという形式ではない）。

【００２１】

図３を参照して、実際に中継所において実施する操作を説明する。図３（上）に示すように、R(1)では、B(P2(1))とB(P1(2))に応じて予め定めた決まりに従い、次の中継所R(2)に対して、B(P2(2))を反転するか否かの情報C(1)（ここでC(1)＝f(B(P2(1)),B(P1(2)))と表される）を、古典伝送路を経由して送る。図３（中央）に示すように、R(2)では、C(1)に従い、B(P2(2))を反転させるかまたはそのまま反転させないで、B(P2(2))'とする。図３（下）に示すように、R(2)では、B(P2(2))'とB(P1(3))に応じて予め定めた決まりに従い、次の中継所R(3)に対して、B(P2(3))を反転するか否かの情報C(2)（ここでC(2)＝f(B(P2(2)'),B(P1(3)))と表される）を、古典伝送路を経由して送る。

【００２２】

一般化すると、R(m)（m=1、2、…、N-1)では、B(P2(m))'とB(P1(m+1))に応じて、次の中継所R(m+1)に対して、ビットB(P2（m+1))を反転するか否かの情報C(m)を送り、R(m+1)ではC(m)に従いB(P2（m+1))を反転させるかまたはそのまま反転させないでB(P2(m+1))'とする。そして、最後の中継所R(N)では、B(P2(N))'とB(P1(N+1))に応じて、Bに対して、ビットB(P2(N+1))を反転するか否かの情報C(N)を送り、BではC(N)に従いB(P2(N+1))を反転させるかまたはそのまま反転させないでB(P2(N+1))'とする。

【００２３】

上記の操作はある中継所においてAまたは1つ前の中継所のビットを暗号化して次の中継所またはBに送ることに相当し、m=1、2、…、N-1の順でR(m)とR(m+1)において実行し、最後にR(N)とBで実行することにより、Aのビット情報がBに送られることになる。これらの

操作において送られる情報C(m)、C(N)は古典伝送路で送っても盗聴者には何の情報も与えず安全である。

【００２４】

以上のようにしてAとBとで、第1番目のビットを取得することができる。以上の各操作によりAとBとで関連づいたビットを取得する手順を必要な回数だけ繰り返す。そして、第q回目の手順により取得されるB(P1(1))とB(P2(N+1))'とをそれぞれAとBとで取得する乱数表の第q番目のビットとする。こうした手順をL回繰り返せば、互いに関連づいたLビットの乱数列をAとBとで生成できる。その際2つの乱数列の関係は、A、R(i)、Bでの測定値とビットとの間に定められた対応関係、および各場所で取得されたビットとそれに応じて次の場所へ送るC(m)、C(N)、C(A)との間の定められた対応関係により決まる。

【００２５】

本発明に係る秘密鍵配布方法によれば、以下のような効果を得ることができる。すなわち、エンタングルメントで結ばれた光子対を構成する個々の光子を最初の送信所、中継所、最後の受信所の間に分配し、各中継所内などの安全な領域に到達した後に、光子を測定するための基底を隣接する送信所、中継所、受信所の間で決め、それぞれの場所で光子を観測することにより、従来のように偶然の一致を待つのではなく、毎回一致する基底で中継所間での安全な情報伝達に使う秘密鍵を取得することが可能になる。また、秘密鍵となる良質な乱数をエンタングルメントという重ね合わせの状態の観測により物理的に自動的に毎回生成させることが可能になる。さらに、従来の量子暗号通信の秘密鍵配布の手続きだけを中継所で古典的に中継して距離を伸ばすのではなく、一種の量子暗号で秘密鍵そのものを送ることに相当する手続きをとることができる。したがって、中継所間での安全な量子通信を繰り返して遠距離間での秘密鍵配布を行う際に、中継により秘密鍵の数が減少することがなく長距離化を実現することが可能であり、中継ごとに必要となる秘密鍵が組み込まれた質の良い物理乱数発生機構により自動的に生成され、しかもその秘密鍵生成において無駄に捨てるビットがないため伝送速度の高速化にも有利になる。

【００２６】

次に、光子の測定値と取得するビットとの対応関係、およびある中継所から次の中継所へ送る反転するか否かの情報について例を挙げて説明する。

【００２７】

いま、N+1組の光子対PP(j)が、ある基底1で測定したときに観測される2種類の測定値をS1、S2として、光子P1(j)の互いに直交する2つの固有状態φ1(j,S1)およびφ1(j,S2)ならびに光子P2(j)の互いに直交する2つの固有状態φ2(j,S1)とφ2(j,S2)を用いて、φ1(j,S1)φ2（j,S2)+exp(iθ)φ1(j,S2)φ2(j,S1)（θは任意の実数)と表されるものとする。

【００２８】

そして、たとえば、AとR(1)、R(m)とR(m+1)、R(N)とBのそれぞれの間で光子の測定に用いる共通の基底を、基底1、または基底1と直交しない別の基底2とし、各光子の測定値と取得するビットとの対応関係を、基底1で測定したときに、S1が観測された場合のビットを0、S2が観測された場合のビットを１とし、基底2で測定したときに、観測される2種類の測定値をS1'、S2'として、S1'が観測された場合のビットを0、S2'が観測された場合のビットを1とするように定める。

【００２９】

また、R(1)ではB(P2(1))とB(P1(2))とが同じであればB(P2(2))を反転しないという情報C(1)、異なればB(P2(2))を反転するという情報C(1)を、R(2)に対して送るようにし、R(2)ではC(1)に従ってB(P2(2))をB(P2(2))'とする。同様に、R(m)ではB(P2(m))'とB(P1(m+1))が同じならB(P2(m+1))を反転しないという情報C(m)、異なればB(P2(m+1))を反転するという情報C(m)を、R(m+1)に対して送り、R(m+1)ではC(m)に従ってB(P2(m+1))をB(P2(m+1))'とする。こうした操作をm=2、3、…、N-1に関してこの順で行う。さらに、R(N)ではB(P2(N))'とB(P1(N+1))が同じならB(P2(N+1))を反転しないという情報C(N)、異なればB(P2(N+1))を反転するという情報C(N)を、Bに対して送り、BではC(N)に従ってB(P2(N+1))をB(P2(N+1))'とする。このようにして本発明の方法を実施することができる。

【００３０】
なお、以上においては、AとBで確率的に自然に発生したビットを取得する場合について説明した。ただし、本発明の方法では、Aに乱数列BA(r)（r=1、2、…）を予め用意し、この乱数列BA(r)と関連づいた乱数列をBにおいて取得するようにしてもよい。
【００３１】
この場合、Aにおいて光子P1(1)の測定で取得したビットをB(P1(1))とし、R(i)において光子P2(i)の測定で取得したビットをB(P2(i))、光子P1(i+1)の測定で取得したビットをB(P1(i+1))とし、Bにおいて光子P2(N+1)の測定で取得したビットをB(P2(N+1))とした後、まずAでは乱数列BA(r)（r=1、2、…）のq番目のビットBA(q)とB(P1(1))に応じ、R(1)に対して、B(P2(1))を反転するか否かの情報C(A)を送り、R(1)ではC(A)に従ってB(P2(1))をB(P2(1))'とする。その後は、上述した操作を続けることにより、Aに用意した乱数列BA(r)と関連づいた乱数列をBにおいて取得することができる。
【００３２】
（実施例）
以下、図面を参照しながら、本発明の実施例を説明する。
【００３３】
（実施例1）
図４は本実施例の秘密鍵配布システムを示す構成図である。図４は場所Aと場所Bとの間に2つの中継所R(1)、R(2)を設置した場合を示している。これらの4箇所A、R(1)、R(2)、Bは互いに1km離れて直線上に並んでいるものとする。AとR(1)の間、R(1)とR(2)の間、R(2)とBの間の3箇所には、エンタングルメントで結ばれた光子対を発生させる光子対発生部100が設置されている。これらの光子対発生部をPPG(1)、PPG(2)、PPG(3)とする。
【００３４】
それぞれの光子対発生部100は、波長351.1nmのアルゴンイオンレーザー101、NDフィルター102、電気光学効果素子を用いたシャッター103、1/2波長板104、1/4波長板105、厚さ0.6mmの非線形BBO結晶106、虹彩絞り107、1/2波長板108、レンズ109を有する。
【００３５】
アルゴンイオンレーザー101から光を発し、NDフィルター102で光の強度を調整し、シャッター103でパルス幅約2ns、繰り返し周波数100Hzの光パルス列として切り出し、1/2波長板104および1/4波長板105で偏光した光を調整し、この偏光した光をBBO結晶106に照射する。このようにしてアルゴンイオンレーザーをtypeIIの位相整合をとってBBO結晶106に照射し、パラメトリック過程によるダウン・コンバージョンにより、702nmのエンタングルメントで結ばれた光子対を発生させる。このとき1パルスにつき大体１つの光子対が生成される強度になるようにNDフィルター102で調整している。
【００３６】
AとR(1)、R(1)とR(2)、R(2)とBの間の光子対発生部で生成した光子対をそれぞれPP(1)、PP(2)、PP(3)とし、PP(u)を構成する波長702nmの2つの光子をP1(u)、P2(u)（u=1、2、3）とする。このとき、P1(u)とP2(u)の2光子状態ψ(u)は、式(1)で表されるエンタングルメントで結ばれた状態となっている。
【００３７】
$$\psi(u)=\phi 1(u, V)\phi 2(u, H)+\exp(i\theta)\phi 1(u, H)\phi 2(u, V) \quad (1)$$
ただし、θは実数、φ1(u, H)は、P1(u)の偏光が0°の状態、φ1(u, V)はP1(u)の偏光が90°の状態、φ2(u, H)はP2(u)の偏光が0°の状態、φ2(u, V)はP2(u)の偏光が90°の状態を表す。
【００３８】
パラメトリック　ダウン・コンバージョンで発生した光束をそれぞれ虹彩絞り107で絞り、光子P1(u)、P2(u)（u=1、2、3）を取り出し、1/2波長板108で偏光を調整し、レンズ109で集光して、光ファイバー110に導入し、P1(1)はAへ、P2(1)はR(1)へ、P1(2)はR(1)へ、P2(2)はR(2)へ、P1(3)はR(2)へ、P2(3)はBへと導く。
【００３９】

A、R(1)、R(2)、Bには、それぞれの光子を測定するための光子測定部200が設けられている。これらの光子測定部をDP1(1)、DP2(1)、DP1(2)、DP2(2)、DP1(3)、DP2(3)とする。

【００４０】

それぞれの光子測定部200は、10kmの光ファイバー遅延路201、レンズ202、基底調整用光学素子としての電気光学効果素子を用いた偏光子203、偏光ビームスプリッター(PBS)204、偏光ビームスプリッター204の2つの出口にそれぞれ設けられた2つの光子検出器205、206を有する。光ファイバー遅延路201は入射した光子の偏光状態がファイバー端から出る際に入射時と同じになるように、全体で曲げおよびねじれによる偏光状態の変化が補償されるように設置される。光ファイバー遅延路201のファイバー端から出た光子を、レンズ202で集光し、電気光学効果素子を用いた偏光子203に通す。この偏光子203は、ドライバーからの印加電圧で偏光測定の基底を0°/90°または-45°/45°に切り替えられるようになっている。偏光子203を通過した光子を、偏光ビームスプリッター204を通して光子検出器205または206で検出する。

【００４１】

偏光子203による基底の切り替えは、それぞれの偏光子203に対応して設けられたドライバー210への切り替え信号に従って行われる。この切り替え信号は、それぞれR(1)、R(2)、Bに設置した切り替え信号発生器300により発生させる。これらの切り替え信号発生器をT(1)、T(2)、T(B)とする。

【００４２】

図５に切り替え信号発生器300の構成を示す。切り替え信号発生器300は、電源・ドライバー部301a付きの半導体レーザー301、50%-50%のビームスプリッター302、ビームスプリッター302の一方の出口に設けられた光子検出器(A)303、他方の出口に設けられた光子検出器(B)304を有する。なお、半導体レーザーからのパルス光をNDフィルターで弱めてほぼ単一パルス光源と見なせるようにしている。

【００４３】

上述した光子P1(1)、P2(1)、P1(2)、P2(2)、P1(3)、P2(3)を測定するときの基底を決定する電気光学効果を用いた偏光子203をそれぞれE01(1)、E02(1)、E01(2)、E02(2)、E01(3)、E02(3)とする。図４では、切り替え信号発生器T(1)はE01(1)とE02(1)の基底を、T(2)はE01(2)とE02(2)の基底を、T(B)はE01(3)とE02(3)の基底を、それぞれ切り替えるようにドライバー210へ信号を送る。たとえば、それぞれの切り替え信号発生器300において、光子検出器(A)303が光子検出した場合には0°/90°の基底で、光子検出器(B)304が光子検出した場合に-45°/45°の基底で測定するように切り替え信号を発生し、ドライバー210によって電気光学効果を用いた偏光子203を動作させる。

【００４４】

また、A、R(1)、R(2)、Bにはそれぞれ高速のデータ取り込み・演算・記憶装置400が設置されている。これらのデータ取り込み・演算・記憶装置を(A)、(1)、(2)、(B)とする。データ取り込み・演算・記憶装置400は、光子測定部200からある基底で測定された光子の測定値を取り込み、予め定めた対応関係に従って、対応するビットを取得して記憶する。このときの、対応関係の一例を表１に示す。

【表１】

基底	測定値	ビット
0° と 90°	0°	0
−45° と 45°	−45°	0
0° と 90°	90°	1
−45° と 45°	45°	1

【００４５】

データ取り込み・演算・記憶装置(A)は、P1(1)の偏光の測定結果をB(P1(1))として記憶

する。データ取り込み・演算・記憶装置(1)は、P2(1)の偏光の測定結果をビットB(P2(1))として記憶し、P1(2)の偏光の測定結果をビットB(P1(2))として記憶する。データ取り込み・演算・記憶装置(2)は、P2(2)の偏光の測定結果をビットB(P2(2))として記憶し、P1(3)の偏光の測定結果をビットB(P1(3))として記憶する。データ取り込み・演算・記憶装置(B)は、P2(3)の偏光の測定結果をビットB(P2(3))として記憶する。

【００４６】

データ取り込み・演算・記憶装置(A)と(1)の間、(1)と(2)の間、および同装置(2)と(B)の間は信号線で接続されている。データ取り込み・演算・記憶装置(1)は、データ取り込み・演算・記憶装置(2)に対し、B(P2(1))とB(P1(2))が同じならば「B(P2(2))のビットを反転しないでそのままB(P2(2))'とする」という命令を送り、異なれば「B(P2(2))のビットを反転しB(P2(2))'とする」という命令を送るように設定されている。データ取り込み・演算・記憶装置(2)は、データ取り込み・演算・記憶装置(B)に対し、B(P2(2))'とB(P1(3))が同じならば「B(P2(3))のビットを反転しないでそのままB(P2(3))'にする」という命令を送り、異なれば「B(P2(3))のビットを反転しB(P2(3))'とする」という命令を送るように設定されている。

【００４７】

それぞれの光子対発生部100のシャッター103、切り替え信号発生器300、データ取り込み・演算・記憶装置400は、制御装置500により動作時刻が制御される。

【００４８】

図４および図５に示した秘密鍵配布装置のシステムを用い、AとBで共通の乱数表を得る手順の一例を説明する。まず、各光子対発生部100で同時にエンタングルメントで結ばれた光子対PP(u)を生成させた。光子対PP(u)を構成する光子P1(u)、P2(u)がそれぞれA、R(1)、R(2)、Bに到達してから2μs後に、各切り替え信号発生器300を動作させ、各々の光子測定部200の電気光学効果を用いた偏光子203に切り替え信号を送信した。光子対発生から約30μs後に、偏光子203の基底と光子検出器205または206で検出された光子の測定値を、それぞれのデータ取り込み・演算・記憶装置400に記憶させた。次に、データ取り込み・演算・記憶装置(1)、(2)、(B)をこの順に動作させて、最終的にAでビットB(P1(1))、Bでビット B(P2(3))'を得た。上記と同様の操作によってビットを得る手順を10回繰り返し、得られたB(P1(1))およびB(P2(3))'を順次記録して数列を得たところ、A、Bのどちらでも「1、1、0、0、1、0、0、1、1、0」となり、共通の乱数表を得ることができた。ただし、光子が観測されるはずの時刻に光子が観測されなかった場合のデータは捨て、その回はやり直してカウントしないようにした。

【００４９】

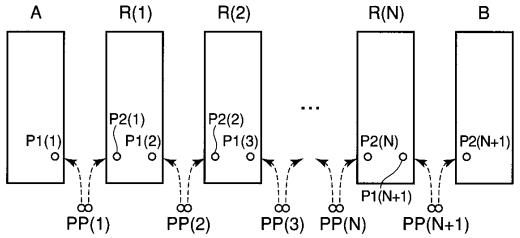
（実施例2）

実施例１のデータ取り込み・演算・記憶装置(A)に予め乱数列BA(r)（r=1、2、…、10）として数列「0、1、1、0、1、1、0、0、0、1」を記憶させた。また、データ取り込み・演算・記憶装置(A)は、AとBとで関連づいたビットを得るためのq回目の操作において、以下のように設定されている。すなわち、データ取り込み・演算・記憶装置(A)は、データ取り込み・演算・記憶装置(1)に対し、BA(q)とB(P1(1))が異なれば「B(P2(1))のビットを反転しないでそのままB(P2(1))'とする」という命令を送り、同じならば「B(P2(1))のビットを反転しB(P2(1))'とする」という命令を送るように設定されている。また、実施例1と同様に、データ取り込み・演算・記憶装置(1)は、データ取り込み・演算・記憶装置(2)に対し、B(P2(1))'とB(P1(2))が同じならば「B(P2(2))のビットを反転しないでそのままB(P2(2))'とする」という命令を送り、異なれば「B(P2(2))のビットを反転しB(P2(2))'とする」という命令を送るように設定されている。データ取り込み・演算・記憶装置(2)の設定も実施例1と同様である。このような設定で、AとBとで関連づいたビットを得るための操作を10回繰り返し、順次B(P2(3))'を記録したところ、BA(r)と同じ数列「0、1、1、0、1、1、0、0、0、1」を得ることができた。つまり、Aで予め用意した乱数列をBとの間で共有することができた。

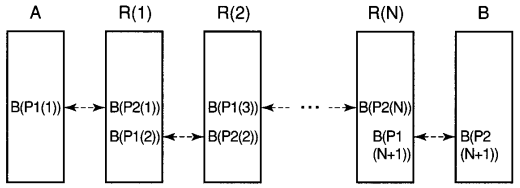
【図面の簡単な説明】

【００５０】
【図１】本発明に係る秘密鍵配布方法における、場所A、中継所、場所Bの位置関係と、生成させる光子対、および光子の分配を示す模式図。
【図２】本発明に係る秘密鍵配布方法において、A、R(i)、Bのそれぞれで最初に取得されたビットを示す図。
【図３】本発明に係る秘密鍵配布方法において、中継所において実施する操作を説明する図。
【図４】本発明の実施例1における秘密鍵配布装置を示す構成図。
【図５】本発明の実施例1における切り替え信号発生器を示す構成図。
【符号の説明】
【００５１】
100…光子対発生部、101…アルゴンイオンレーザー、102…NDフィルター、103…シャッター、104…1/2波長板、105…1/4波長板、106…BBO結晶、107…虹彩絞り、108…1/2波長板、109…レンズ、110…光ファイバー、200…光子測定部、201…光ファイバー遅延路、202…レンズ、203…電気光学効果素子を用いた偏光子（基底調整用光学素子）、204…偏光ビームスプリッター、205、206…光子検出器、210…ドライバー、300…切り替え信号発生器、301a…電源・ドライバー部、301…半導体レーザー、302…ビームスプリッター、303…光子検出器(A)、304…光子検出器(B)、400…データ取り込み・演算・記憶装置、500…制御装置。

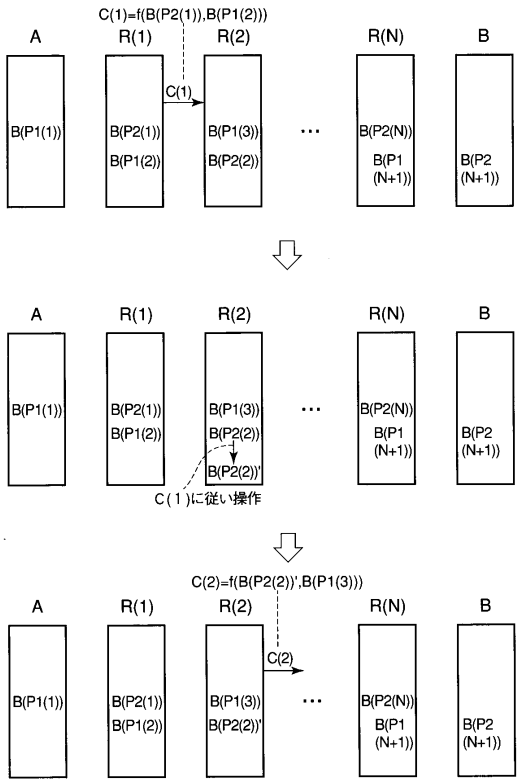
【図１】



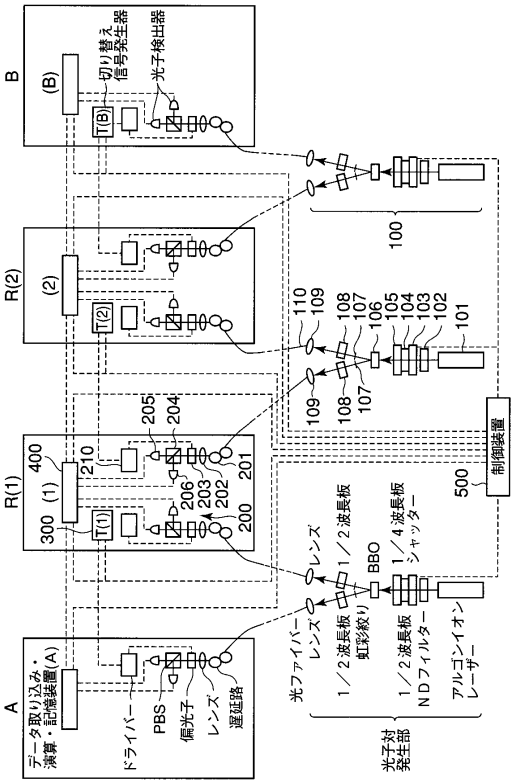
【図２】



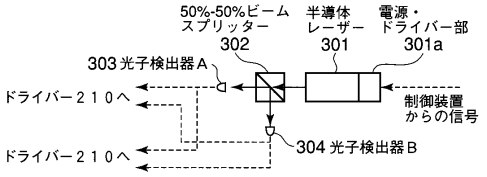
【図３】



【図４】


B
(B)
T(B)
切り替え信号発生器
光子検出器
R(2)
(2)
T(2)
R(1)
(1)
T(1)
100
101
102
103
104
105
106
107
108
109
110
200
201
202
203
204
205
206
210
300
400
500
制御装置
レンズ
1／2波長板
BBO
1／4波長板
シャッター
光ファイバー
レンズ
1／2波長板
虹彩絞り
1／2波長板
NDフィルター
アルゴンイオン
レーザー
光子対
発生部
A
データ取り込み・
演算・記憶装置(A)
ドライバー
PBS
偏光子
レンズ
遅延路

【図５】


50%-50%ビーム
スプリッター
302
半導体
レーザー
301
電源・
ドライバー部
301a
303 光子検出器A
ドライバー２１０へ
制御装置
からの信号
ドライバー２１０へ
304 光子検出器B

フロントページの続き

(72)発明者　市村　厚一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　塩川　教次
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　藤居　三喜夫
東京都府中市東芝町１番地　株式会社東芝府中事業所内
(72)発明者　鳥居　健太郎
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　大熊　建司
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

審査官　石田　信行

(56)参考文献　Briegel, Quantum Repeaters:The Role of Imperfect Local Operation in Quantum Communication, Physical Review Letters, 米国, １９９８年１２月２８日, Vol.81, No.26, 頁５９３２－頁５９３５
TAL MOR, Quantum memory in quantum cryptography, arXiv.org, 米国, １９９９年　６月２１日, ＵＲＬ, http://arxiv.org/PS_cache/quant-ph/pdf/9906/9906073v1.pdf

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　　９／１２
Ｇ０２Ｆ　　１／３９
Ｇ０２Ｆ　　２／００