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

特許第4504833号
(P4504833)

(45)発行日　平成22年7月14日(2010.7.14)　(24)登録日　平成22年4月30日(2010.4.30)

(51)Int.Cl.			F I		
H04L	9/12	(2006.01)	H04L	9/00	631
G02F	1/015	(2006.01)	G02F	1/015	
H04B	10/00	(2006.01)	H04B	9/00	Z

請求項の数 6　(全 22 頁)

(21)出願番号　特願2005-40977(P2005-40977)
(22)出願日　平成17年2月17日(2005.2.17)
(65)公開番号　特開2006-229608(P2006-229608A)
(43)公開日　平成18年8月31日(2006.8.31)
審査請求日　平成18年3月27日(2006.3.27)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　竹本　一矢
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　臼杵　達哉
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　新田　亮

最終頁に続く

(54)【発明の名称】秘密鍵配送システム

(57)【特許請求の範囲】
【請求項１】
単一光子を生成する単一光子源と、該単一光子に秘密鍵情報を付与する符号化部と、を有する送信機と、
前記単一光子から秘密鍵情報を取出す検出部とを有する受信機と、
前記送信機と受信機とを接続する光伝送路と、を備える秘密鍵配送システムであって、
前記送信機は、
前記単一光子源が波長の異なる複数の単一光子を同時に生成する量子ドット構造体を有し、
前記単一光子源と前記符号化部との間に、単一光子を波長毎に分岐させる光分波器を有し、
前記符号化部が単一光子の波長毎に設けられてなることを特徴とする秘密鍵配送システム。
【請求項２】
前記送信機は、符号化部と光伝送路との間に、波長の異なる複数の単一光子を合波し同時に光伝送路に送出する光混合器をさらに有し、
前記受信機は、光伝送路と検出部との間に該単一光子の各々を波長毎に分岐させる他の光分波器を有し、該検出部が単一光子の波長毎に設けられてなることを特徴とする請求項１記載の秘密鍵配送システム。
【請求項３】

前記送信機は、波長の異なる複数の単一光子を波長毎に光伝送路に送出して、複数の受信機に秘密鍵情報を送信することを特徴とする請求項１記載の秘密鍵配送システム。

【請求項４】

前記量子ドット構造体は、一つの半導体層の表面に、複数の互いに大きさの異なる量子ドットが設けられてなることを特徴とする請求項１～３のうち、いずれか一項記載の秘密鍵配送システム。

【請求項５】

１つの第１の受信機と複数の第２の受信機の各々とが秘密鍵情報を共有するための秘密鍵配送システムであって、

波長の異なる複数のエンタングル状態の単一光子対を生成する量子ドット構造体を有する単一光子対源と、該単一光子対を各々の単一光子に分離する光分離器と、分離された単一光子の一方でかつ波長の異なる単一光子を合波して同時に送出する光混合器とを有する送信機と、

前記合波された単一光子を受信する第１の受信機と、前記分離された単一光子の他方を波長毎に受信する複数の第２の受信機からなることを特徴とする秘密鍵配送システム。

【請求項６】

前記量子ドット構造体は、１．３μｍ～１．５５μｍの範囲から選択された波長の単一光子あるいは単一光子対を生成することを特徴とする請求項１～５のうち、いずれか一項記載の秘密鍵配送システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は秘密鍵配送システムおよび秘密鍵配送方法に関する。

【背景技術】

【０００２】

電子政府や電子商取引など次世代情報化社会の実現に向けて、安全・確実な暗号通信は必要不可欠である。暗号通信では、公開暗号鍵方式や秘密暗号鍵方式が用いられている。

現在広く用いられているＲＳＡ公開暗号鍵方式は、非常に大きな数の素因数分解を多項式で解くことは膨大な時間を必要とするので解読が困難であるという計算量的側面によってのみ、安全性を保証されている。したがって、非常に高速な並列計算を得意とする量子計算機が登場すれば、このような暗号を解読するのにかかる時間は飛躍的に短縮される。そのため、公開暗号鍵方式では公開鍵が解読されると、第三者によるデータの盗聴や改ざんのおそれがあり、その安全性は完全ではない。また、秘密暗号鍵方式では、情報の送信者と受信者が同一の秘密鍵を所有し、送信者が秘密鍵で暗号化したデータを受信者がその秘密鍵でデータを解読する。秘密暗号鍵方式では、秘密鍵自体をこれらの二者に配信する際に盗聴されるおそれがあり、その安全性は完全ではない。

【０００３】

こうした安全性の問題を解決する手段として期待されているのが量子暗号である。量子暗号として、ＢＢ８４（１９８４年にＣ．Ｈ．ＢｅｎｎｅｔｔとＧ．Ｂｒａｓｓａｒｄに提案された。）、Ｅ９１（１９９１年にＡ．Ｋ．Ｅｋｅｒｔによって提案された。）等様々な方式が提案されている。例えばＢＢ８４では、従来の光通信のような光子の集合体ではなく、光子一つ一つに情報を載せて伝送する。情報の１ビットを１つの光子に、例えば光子の偏光状態に付与すれば、各々の光子は、ハイゼンベルクの不確定性原理（共役する物理量は同時に正確に測定できないとする原理。）およびｎｏ－ｃｌｏｎｉｎｇ定理（量子状態を観測することなく複製することはできないといる定理。）に従うため、光子の状態を破壊することなしにビット情報を取出したり、複製することはできない。したがって、量子暗号では通信経路上の第三者による盗聴を防止することはできないが、情報の複製や改ざんを検出することができる。こうして二者間で共有された暗号鍵の安全性は、情報の担い手が単一光子である限り、計算量的困難性ではなく物理的原理に基づいて保証される。

【０００４】
近年、量子暗号システムが実用化されている。量子暗号システムは、送信者側が、１つの光子（単一光子）を生成する単一光子源と、光子に秘密鍵の情報を付与する偏光状態制御部とからなり、受信者側は、光子の情報を検出する単一光子検出器を有する。単一光子源には、通常、レーザ光源と減衰器が用いられている。かかる単一光子源では、レーザ光源からレーザパルス列を射出し、減衰器によりレーザパルス列の光の強度を減衰させ、１パルス当たり平均１個あるいはそれ以下の光子数になるようする。単一光子源はこのように疑似的に単一光子を生成している。
【特許文献１】特開２００３－２４９９２８号公報
【特許文献２】特開２０００－２１６７７５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上述した疑似的単一光子源では、１パルスに２つ以上の光子が含まれることがある。この場合、１パルスの２つ以上の光子に同じ情報が載せられるので、盗聴者がそのうちの１つの光子を抜き取っても受信者はその盗聴行為を検出できず、安全性が完全ではないという問題が生ずる。
【０００６】
そのため、１パルス当たりの平均光子数をさらに低減して、１パルス当たり複数の光子が存在する確率を極めて低く設定する必要がある。このような場合、安全性は向上するが、光子のないパルスが多くなり、転送レートが極めて低下するという問題がある。
【０００７】
そこで、本発明は上記問題点に鑑みてなされたもので、本発明の目的は、安全性が高く、高転送レートの秘密鍵配送システムおよび秘密鍵配送方法を提供するものである。
【０００８】
さらに、本発明の他の目的は、一つの送信機から複数の受信機に、秘密鍵情報あるいは秘密鍵情報生成するための媒体を同時に配送可能な秘密鍵配送システムおよび秘密鍵配送方法を提供するものである。
【課題を解決するための手段】
【０００９】
本発明の一観点によれば、単一光子を生成する単一光子源と、該単一光子に秘密鍵情報を付与する符号化部と、を有する送信機と、前記単一光子から秘密鍵情報を取出す検出部とを有する受信機と、前記送信機と受信機とを接続する光伝送路と、を備える秘密鍵配送システムであって、前記送信機は、前記単一光子源が波長の異なる複数の単一光子を同時に生成する量子ドット構造体を有し、前記単一光子源と前記符号化部との間に、単一光子を波長毎に分岐させる光分波器を有し、前記符号化部が単一光子の波長毎に設けられてなることを特徴とする秘密鍵配送システムが提供される。
【００１０】
本発明によれば、秘密鍵配送システムは、送信機が波長の異なる複数の単一光子を同時に生成する量子ドット構造体を有し、それらの単一光子に秘密鍵情報を付与して受信機に送信するので、秘密鍵情報を高転送レートで送信できる。また、量子ドット構造体は単一光子を生成するので、高いあるいは完全な安全性を有する秘密鍵配送システムが実現できる。なお、本明細書および特許請求の範囲において、単一光子は、１つの光子しか含まない光のパルスを意味する。
【００１２】
本発明によれば、送信機は、単一光子対源の量子ドット構造体から波長が異なる複数のエンタングル状態の単一光子対を同時に生成し、各々の波長の単一光子対を単一光子に分離して、分離された単一光子の一方を一方の受信機に送信し、分離された単一光子の他方を他方の受信機に送信する。分離された単一光子は、波長の異なる複数の単一光子であるので、同時に複数の単一光子が受信機の各々に送信される。受信機は、受けた単一光子を

媒体として秘密情報を生成する。したがって、エンタングル状態の単一光子が同時に波長多重化されているので、秘密鍵情報となる媒体を高転送レートで送信できる。また、量子ドット構造体はエンタングル状態にある単一光子と単一光子の対を生成するので、高いあるいは完全な安全性を有する秘密鍵配送システムが実現できる。なお、エンタングル状態は、２つ以上の粒子の量子状態（量子力学により記述される状態をいう。）が特定の組み合わせで相関を有する状態である。

【発明の効果】

【００１３】

本発明によれば、安全性が高く、高転送レートの秘密鍵配送システムおよび秘密鍵配送方法を提供できる。また、本発明によれば、一つの送信機から複数の受信機に、秘密鍵情報あるいは秘密鍵情報生成するための媒体を同時に配送可能な秘密鍵配送システムおよび秘密鍵配送方法を提供できる。

【発明を実施するための最良の形態】

【００１４】

以下図面を参照しつつ実施の形態を説明する。

【００１５】

（第１の実施の形態）

本発明の第１の実施の形態に係る秘密鍵配送システムは、送信機から受信機に量子暗号を用いて秘密鍵情報を送信するシステムである。

【００１６】

図１は、本発明の第１の実施の形態に係る秘密鍵配送システムの構成を示すブロック図である。

【００１７】

図１を参照するに、秘密鍵配送システム１０は、波長多重化された単一光子に秘密鍵情報を付与して光伝送路１１に送出する送信機２０と、光伝送路１１から受けた波長多重化された単一光子から秘密鍵情報を取出す受信機４０と、送信機２０と受信機４０とを接続する光伝送路１１から構成される。

【００１８】

秘密鍵配送システム１０は、二者間で秘密鍵情報を共有するために、秘密鍵情報を量子暗号により配送するシステムである。ここでは、秘密鍵情報を送信機２０により受信機４０に送信する場合について説明する。

【００１９】

以下、秘密鍵配送システム１０を構成する送信機２０について詳細に説明する。

【００２０】

送信機２０は、複数の異なる波長λ_1～λ_nの単一光子を生成する波長多重単一光子源２１と、単一光子を波長毎に分離する光分波器２２と、波長λ_1～λ_n以外の余分な光子を遮断するバンドパスフィルタ２３と、単一光子に秘密鍵情報を付与する位相変調器２４と、各波長λ_1～λ_nの単一光子を再び合波して光伝送路１１に送出する光混合器２５から構成される。

【００２１】

波長多重単一光子源２１は、波長多重化された単一光子、すなわち、互いに異なる波長を有する単一光子を生成する。単一光子は、１つの光子しか含まない光のパルスである。

【００２２】

図２は、第１の実施の形態の波長多重単一光子源の構成を示す図である。図２を参照するに、波長多重単一光子源２１は、レーザ光源２８と、光カプラ２９と、出力モニタ３０と、集光光学系３１と、量子ドット構造体５０と、冷凍機３５と、ローパスフィルタ３７と、これらを接続する光ファイバ３６等から構成される。

【００２３】

レーザ光源２８は、パルス列からなる励起光を出射するパルスレーザ、例えば、波長が７８０ｎｍのＴｉ：サファイアレーザからなる。レーザ光源２８のパルス時間幅は、後述

する量子ドットの発光寿命よりも短い時間幅に設定される。代表的な単一ドットの発光寿命は１ｎ秒である（Ｐｈｙｓ．　Ｒｅｖ．　Ｂ　Ｖｏｌ．　６４　（２００１）　ｐｐ．　２０１３０２－１　～　ｐｐ．　２０１３０２－４）。パルス幅をこのように設定することで、所望の波長の単一光子を生成できる。パルス時間幅は、１００ｐ秒以下の範囲に設定することが好ましく、一例として８０ｆ秒（80×10^{-15}秒）に設定される。

【００２４】

また、レーザ光源２８のパルス列の繰返し周波数は適宜選択されるが、例えば８０ＭＨｚに設定される。なお、繰返し周波数は、量子ドットの発光寿命の点から、最大１ＧＨｚに設定可能である。なお、レーザ光源２８は上記のパルス列からなる励起光を出射可能であれば特に制限されない。

【００２５】

なお、図示を省略するが、レーザ光源２８と光カプラ２９との間に、励起光の繰返し周波数を図１に示す受信機４０の検出器42_1～42_nの速度に合わせるためのパルスピッカーを設けてもよい。

【００２６】

レーザ光源２８のパルスの出力値は、後述する量子ドット構造体への１パルスの照射により、所定の波長毎に一つ光子が生成されるように設定される。すなわち、パルスの出力値が過度に高いと、同一の波長で２個以上の光子が生成され、単一光子でなくなる。また、パルスの出力値が過度に低いと、光子が生成されなくなる。なお、パルスの出力値は出力モニタ３０により監視される。

【００２７】

集光光学系３１は、光カプラ２９側から、集光レンズ３２、Ｓｉフィルタ３３、対物レンズ３４からなる。集光光学３１系は、光カプラ２９を介して送られてきた励起光としてのパルス列を量子ドット構造体５０に集光する。また、集光光学系３１は、量子ドット構造体５０から入射する波長λ_1～λ_nを有する単一光子を光ファイバ３６に集光して送出する。なお、その際、散乱した励起光をシリコンフィルタ３３により除去する。

【００２８】

量子ドット構造体５０は、冷凍機３５、例えばクライオスタット内に載置され、液体ヘリウムにより１０Ｋ程度の温度に冷却される。励起光は、クライオスタットに設けられた光学窓を介して、量子ドット構造体５０に照射される。

【００２９】

図３は、量子ドット構造体の模式的斜視図、図４は量子ドット構造体の要部断面図である。

【００３０】

図３及び図４を参照するに、量子ドット構造体５０は、図３に示すように山型の断面形状を有し、その頂上面が平らなメサ構造を有する。図４は、量子ドット構造体５０の頂上付近を拡大した断面図である。なお、図３に示す頂上面が、図４に示すＩｎＰキャップ層５６の表面に対応する。なお、量子ドット構造体５０は、山型のかわりに、高さが低く頂上面の面積が広い台地状の形状を有してもよい。

【００３１】

量子ドット構造体５０は、ＩｎＡｓ／ＩｎＰ量子ドットである。具体的には、量子ドット構造体５０は、ＩｎＰ基板５１上に形成されたＩｎＰバッファ層５２（膜厚２００ｎｍ）と、ＩｎＰバッファ層５２の表面に形成された複数のＩｎＡｓ量子ドット５３と、ＩｎＰバッファ層５２の表面とＩｎＡｓ量子ドット５３を覆う第１ＩｎＰダブルキャップ層５４（厚さ２ｎｍ）、および第２ＩｎＰダブルキャップ層５５（厚さ１８ｎｍ）と、その上に形成されたＩｎＰキャップ層５６（厚さ１００ｎｍ）からなる。

【００３２】

ＩｎＰバッファ層５２の表面には、複数の異なる底面直径を有するＩｎＡｓ量子ドット５３が形成されている。ＩｎＡｓ量子ドット５３は、ＩｎＰキャップ層５６側からの適当な励起光の照射により単一光子を発光する。この単一光子は励起光の入射側に進行するす

る。単一光子の波長は、ＩｎＡｓ量子ドット５３の底面直径および高さに対応して決定される。例えば、底面直径が大きいほど単一光子の波長は長くなる。また、ＩｎＡｓ量子ドット５３はレンズ状の形状を有し、その上面５３－１はほぼ平らに形成されている。ＩｎＡｓ量子ドット５３は高さ方向に数分子が積み上がって構成される。したがって、ＩｎＡｓ量子ドット５３の高さH_{QD}は離散的な値に設定されている。このように設定することで、ＩｎＡｓ量子ドット５３から発光される単一光子の波長が離散的になり、送信機で波長毎に単一光子に分離するのが容易になる。

【００３３】

本願発明者等の検討によれば、このような構造の量子ドット構造体５０のＩｎＡｓ量子ドット５３から、通信波長帯（波長１．３μｍ～１．５５μｍ）において離散的でかつ波長幅の狭い輝線が得られることが知得されている（Ｊｐｎ．Ｊ．Ａｐｐｌ．Ｐｈｙｓ．，Ｖｏｌ．４３ Ｎｏ．３Ａ，（２００４）ｐｐ．Ｌ３４９－Ｌ３５１）。さらに、量子ドット構造体からそのような輝線の波長の単一光子が得られることが知得されている（Ｊｐｎ．Ｊ．Ａｐｐｌ．Ｐｈｙｓ．，Ｖｏｌ．４３ Ｎｏ．７Ｂ，（２００４）ｐｐ．Ｌ９９３－Ｌ９９５）。

【００３４】

図５は、量子ドット構造体の１０Ｋでの光ルミネセンススペクトルの例を示す図である。図５は、４種類の量子ドット構造体の各々について（Ａ）から（Ｄ）に光ルミネセンススペクトルを示している。これらの量子ドット構造体は、上述した本実施の形態の量子ドット構造体と略同様の構成を有するが、量子ドット構造体当たり１つの量子ドットのみを有するものである。

【００３５】

図５を参照するに、（Ａ）から（Ｄ）のスペクトルにおいて、各々、離散的で、鋭いつまり波長幅の狭い輝線L_A～L_Dが認められる。これらの輝線L_A～L_Dの波長幅は１ｎｍよりも小さい。これらの輝線L_A～L_Dは、その各々にスペクトルに示される他の輝線（サテライト）と波長が離れているので容易に分離できる。また、このような輝線L_A～L_Dは高強度のため、励起光の波長および強度を調整することで、単一光子を容易に取出すことができる。さらにその際に他の強度の弱い発光線の発光を回避した状態で、単一光子を取出すことができる。

【００３６】

本実施の形態の量子ドット構造体は、このような輝線L_A～L_Dを示すＩｎＡｓ量子ドットを図３に示す一つのメサ構造のＩｎＰバッファ層５２上に２個以上、例えば１０個～２０個有するものである。このように複数の量子ドット設定することで、１パルスの励起光の照射で、所望の互いに異なる複数の波長の単一光子が得られる。

【００３７】

さらに、輝線L_A～L_Dの各々は、（Ａ）から（Ｄ）に向かって順に、通信波長帯域のＣ帯、Ｓ帯、Ｅ帯、Ｏ帯に存在する。これらの通信帯域はシングルモードの光ファイバが用いられる帯域であり、ギガビット伝送が可能なものである。したがって、単一光子を高転送レートで送信機から受信機に送信可能である。量子ドット構造体は、上記の各々の通信帯域内の輝線を複数有してもよい。量子ドット構造体は、図５に示すような輝線をｎ個有する発光を行うものとして以下の説明を行う。ここでｎは２以上の整数である。

【００３８】

図２に戻り、量子ドット構造体からの波長多重化された単一光子は、集光光学系３１を介して光ファイバ３６に集光され、光カプラ２９を介してローパスフィルタ３７に達する。

【００３９】

ローパスフィルタ３７は、励起光の波長に合わせて選択され、励起光を遮断するフィルタであれば特に限定されない。ローパスフィルタ３７を通過した多重化された単一光子は光ファイバ３６を介して光分波器に送出される。

【００４０】

図１に戻り、光分波器２２は、多重化された単一光子を各々の波長λ_1～λ_nに分岐させるものである。光分波器２２は、例えば、波長分割多重化（ＷＤＭ）結合器やＡＷＧ（Arrayed Waveguide Grating）波長合分波器を用いることができる。

【００４１】

バンドパスフィルタ２３は、所望の波長に近接した波長を有する光子を遮断し、所望の波長の単一光子のみを通過させる。バンドパスフィルタ２３は、光分波器２２で遮断しきれなかった光子を遮断するものである。バンドパスフィルタ２３の透過波長幅は、１ｎｍ程度に設定してもよい。バンドパスフィルタ２３は、例えば、誘電体多層膜フィルタや回折格子を用いることができる。

【００４２】

なお、バンドパスフィルタ２３はその透過波長および透過波長幅を調整可能なフィルタを用いてもよい。また、光分波器２２により所望の波長以外の波長を有する光子が除去される場合はバンドパスフィルタ２３を設けなくともよい。

【００４３】

位相変調器２４は、単一光子の各波長λ_1～λ_n毎に一つずつ設けられている。位相変調器２４は、各々の単一光子の位相状態に秘密鍵情報の要素を付与する符号化の機能を有する。例えば、位相変調器２４は、データ“１”に対してπだけ位相変調し、データ“０”に対して位相変調しない取決めの符号化を行う。なお、光子の位相は量子化されており、取りうる位相は０、π／２、π、３π／２の４状態のみである。

【００４４】

また、秘密鍵情報が例えばｍ行ｎ列の行列Ａで表されるとすると、その行列の成分A_{11}～A_{1n}の各々を位相変調器24_1～位相変調器24_nに割当てる。次いで、次に位相変調器が受ける単一光子に行列の成分A_{21}～A_{2n}の各々を位相変調器24_1～位相変調器24_nに割り当てる。このような動作を繰り返してA_{m1}～A_{mn}まで割り当てる。上記の取決めと秘密鍵情報の割り当てにしたがって単一光子に秘密鍵情報を付与する。このようにして秘密鍵情報を波長多重化した単一光子に付与して送信することで、秘密鍵情報の要素を並列に送信できるので、転送レートが高速になる。

【００４５】

光混合器２５は、各波長の単一光子を合波して光伝送路１１に送出する。光混合器２５は、光分波器２２と同様に、例えば、ＷＤＭ結合器やＡＷＧ波長合分波器を用いることができる。

【００４６】

次に、秘密鍵配送システム１０を構成する受信機４０について説明する。

【００４７】

受信機４０は、光伝送路１１から受けた波長多重化された単一光子を各波長λ_1～λ_nに分離する光分波器４１と、単一光子毎に秘密鍵情報を取り出す検出器42_1～42_nから構成される。

【００４８】

光分波器４１は、多重化された単一光子を各々の波長λ_1～λ_nに分岐させるものであり、送信機２０の分波器２２と同様にＷＤＭ結合器やＡＷＧ波長合分波器を用いることができる。

【００４９】

検出器42_1～42_nは、単一光子の波長λ_1～λ_n毎に設けられ、光分波器４１より受けた単一光子の位相状態を検出する。検出器42_1～42_nは、例えばマッハーツェンダ干渉計に単一光子検出器を接続したものを用いることができる。

【００５０】

検出器42_1～42_nでは、各波長λ_1～λ_n毎に単一光子の位相情報が検出され、各波長λ_1～λ_n毎にデータ“１”あるいはデータ“０”に復号化され、符号化された秘密鍵情報が例えばｍ行ｎ列の行列Ａで秘密鍵情報が得られる。

【００５１】

以上説明したように、第１の実施の形態に係る秘密鍵配送システム１０は、送信機２０が波長多重単一光子源２１を用いて波長が異なる複数の単一光子を同時に生成し、単一光子の各々に秘密鍵情報の要素を載せ、再び合波して光伝送路１１により送出する。受信機４０は、各波長毎に秘密鍵情報の要素を検出し、秘密鍵情報を再構成する。したがって、単一光子が波長多重化されているので、秘密鍵情報を高転送レートで送信できる。

【００５２】

さらに、波長多重単一光子源２１は励起光の１ショット毎に多重化された単一光子が生成される。したがって、従来の疑似的単一光子源よりも、効率良く単一光子が生成されるので、この点においても秘密鍵配送システム１０は秘密鍵情報を高転送レートで送信できる。

【００５３】

さらに、励起光の繰り返し照射周波数を１ＧＨｚ程度まで高めることができるので、秘密鍵情報をいっそう高転送レートで送信できる。

【００５４】

また、波長多重単一光子源２１は量子ドット構造体５０を有し、従来の疑似的単一光子源よりも、単一光子を正確にかつ効率良く生成でき、安全性が高まる。量子ドット構造体５０は１チップで形成されているので、単一波長の単一光子を発生する量子ドット構造体を複数配置するよりも、量子ドット構造体を冷却する冷凍機３５を小型化できる。さらに、冷凍機３５の低コスト化も図れる。

【００５５】

なお、図１に示す第１の実施の形態では、秘密鍵情報を付与する符号化手法として位相符号方式を用いた例を示したが、その代わりに偏光符号方式を用いてもよい。具体的には、図１に示す送信機１０の位相変調器24_1～24_nの代わりに偏光制御器を用いる。偏光制御器は、例えば、データ“１”に対して縦偏光（９０度偏光）、データ“０”に対して横偏光（０度偏光）を割当てる符号化を行う。この場合、受信機４０の検出器42_1～42_nは、偏光光子測定器および単一光子検出器を用いる。偏光光子測定器は例えば０度－９０度偏光測定器を用いることで、０度偏光の単一光子を検出し、復号化してデータ“０”を得る。なお、符号化および復号化においては上述した手法に限定されず、公知の手法を用いてもよい。

【００５６】

また、図１では、１本の光伝送路１１を用いる場合を例に挙げて説明したが、送信機２０の光混合器２５および受信機４０の光分波器４１を省略し、送信機２０の位相変調器24_1～24_nと、受信機４０の検出器40_1～40_nをｎ本の光伝送路で並列に接続してもよい。

【００５７】

次に、本実施の形態に係る量子ドット構造体の製造方法を図６および図７を参照しつつ説明する。実施の形態に係る量子ドット構造体は、有機金属化学気相成長（ＭＯＣＶＤ）法およびいわゆるダブルキャップ法を用いて以下のようにして形成される。

【００５８】

最初に、図６（Ａ）の工程では、Ｆｅをドープした（１００）面を主面とするＩｎＰ基板５１上に減圧ＭＯＣＶＤ法を用いてＩｎＰバッファ層５２を形成する。具体的には、トリエチルインジウムおよび水素化リンを前駆体、水素ガスをキャリアガスとして供給し、圧力５０Ｔｏｒｒに設定し、６００℃に加熱してＩｎＰバッファ層５２を成長させる。

【００５９】

図６（Ａ）の工程ではさらに、ＩｎＰバッファ層５２上に、減圧ＭＯＣＶＤ法を用いてＩｎＡｓ量子ドット前駆体５３ａを自己組織的に形成する。具体的には、トリエチルインジウムおよび水素化ヒ素を前駆体、水素ガスをキャリアガスとして供給し、圧力５０Ｔｏｒｒに設定し、５００℃に加熱して、例えば２．８分子のＩｎＡｓ量子ドット前駆体５３ａを成長させる。次いで、水素化ヒ素雰囲気で１５秒の加熱処理を行う。このようにして、ＩｎＡｓ量子ドット前駆体５３ａは、ＩｎＰバッファ層５２上にＳ－Ｋ（Ｓｔｒａｎｓ

ｋｉ－Ｋｒａｓｔａｎｏｗ）型の成長モードにより形成される。このようにして得られたＩｎＡｓ量子ドット前駆体５３ａは、底面直径および高さが分布を有する。上記条件では、ＩｎＡｓ量子ドット前駆体５３ａの底面直径は３５ｎｍ～７０ｎｍ、高さは３ｎｍ～１２ｎｍであった。また、ＩｎＡｓ量子ドット前駆体５３ａの密度は$1.8\times10^{10}cm^{-2}$であった。なお、Ｓ－Ｋ型の成長モードは、格子不整合系のヘテロエピタキシャル成長の初期に下地層上に成長島が自己組織的に形成される成長モードのことである。

【００６０】

次いで、図６（Ｂ）の工程では、図６（Ａ）の構造体の表面に第１ＩｎＰダブルキャップ層５４を形成する。具体的には、５００℃に加熱して、上述したＩｎＰバッファ層５２の形成条件と略同様にして、膜厚２ｎｍの第１ＩｎＰダブルキャップ層５４をＩｎＡｓ量子ドット前駆体５３ａおよびＩｎＰバッファ層５２の表面を覆うように形成する。ＩｎＡｓ量子ドット前駆体５３ａは、第１ＩｎＰダブルキャップ層５４の膜厚よりも高いので、その上部は露出する。

【００６１】

図６（Ｂ）の工程ではさらに、第１ＩｎＰダブルキャップ層５４およびＩｎＡｓ量子ドット前駆体５３ａの表面を水素化リンに１２０ｓ曝露する。この処理により、ＩｎＡｓ量子ドット前駆体５３ａは、第１ＩｎＰダブルキャップ層５４から露出した部分でその上面付近が水素化リンとの反応が生じ、ＩｎＰに置換される。これにより上面がＩｎＰ５３ｂに覆われたＩｎＡｓ量子ドット５３が形成される。すなわち、その結果、ＩｎＡｓ量子ドットのＩｎＡｓからなる部分、すなわちＩｎＡｓ量子ドットの高さが低下する。その高さH_{QD}はＩｎＡｓ分子の整数倍の高さとなる。したがって、ＩｎＡｓ量子ドットは離散的な高さを有するようになる。

【００６２】

次いで、図７（Ａ）の工程では、第１ＩｎＰダブルキャップ層５４およびＩｎＰに置換されたＩｎＡｓ量子ドット５３の表面に、第１ＩｎＰダブルキャップ層５４の形成条件と同様にして膜厚１８ｎｍの第２ＩｎＰダブルキャップ層５５を形成する。

【００６３】

図７（Ａ）の工程ではさらに、６００℃に加熱して、第２ＩｎＰダブルキャップ層５５上にＩｎＰバッファ層５２の形成条件と同様にして膜厚１００ｎｍのＩｎＰキャップ層５６を形成する。

【００６４】

次いで、図７（Ｂ）の工程では、このようにして形成された図７（Ａ）の構造体をエッチングする。エッチングは、図３に示すような山型、あるいは台地形状なるようにエッチングする。具体的には、フォトリソグラフィ法によりパターニングして、ウエットエッチング法によりエッチングする。このようにして頂上の直径が１００ｎｍ～５００ｎｍ程度のメサ構造を有する量子ドット構造体が形成される。

【００６５】

次いで、図示を省略するが、作製した量子ドット構造体のμ－光ルミネセンススペクトルを測定し、所望の波長λ_1～λ_nの輝線を示す量子ドット構造体を選別する。このようにして、本実施の形態を構成する量子ドット構造体が得られる。なお、上述した膜厚および加熱温度等は例として挙げたものであり、それらに限定されるものではない。

【００６６】

（第２の実施の形態）

本発明の第２の実施の形態に係る秘密鍵配送システムは、送信機からｎ個の受信機に量子暗号を用いて秘密鍵情報を送信するシステムである。第２の実施の形態に係る秘密鍵配送システムは、第１の実施の形態に係る秘密鍵配送システムの変形例である。

【００６７】

図８は、本発明の第２の実施の形態に係る秘密鍵配送システムの構成を示すブロック図である。図中、先に説明した部分に対応する部分には同一の参照符号を付し、説明を省略する。

【００６８】
図８を参照するに、第２の実施の形態に係る秘密鍵配送システム６０は、一つの送信機６１から秘密鍵情報をｎ個の受信機４０$_1$～４０$_n$の各々に量子暗号により同時に配送するシステムである。秘密鍵配送システム６０は、ｎ個の波長が多重化された単一光子列を用いて、受信機４０$_1$～４０$_n$の各々に送る秘密鍵情報を一の波長を有する単位光子列に載せ、これを同時にｎ個の受信機に対して行って送信する。
【００６９】
秘密鍵配送システム６０は、波長多重化された単一光子に秘密鍵情報を付与してｎ個の光伝送路１１$_1$～１１$_n$に送出する送信機６１と、ｎ個の光伝送路１１$_1$～１１$_n$と、各々の光伝送路１１$_1$～１１$_n$から受けた単一光子列から秘密鍵情報を取り出すｎ個の受信機４０$_1$～４０$_n$から構成される。
【００７０】
送信機６１は、光伝送路１１$_1$～１１$_n$に送出する前に光混合器を設けない以外は図１に示す第１の実施の形態の送信機と同様の構成を有する。送信機６１は、第１の実施の形態と同様の波長単一光子源２１を有するので、ｎ個の波長が多重化された単一光子列を正確に効率良く生成できる。
【００７１】
受信機４０$_1$～４０$_n$は各波長λ$_1$～λ$_n$毎に設けられている。受信機４０$_1$～４０$_n$は各々検出器４２$_1$～４２$_n$を有する。検出器４２$_1$～４２$_n$は図１に示す第１の実施の形態の検出器４２$_1$～４２$_n$と同様の構成を有する。
【００７２】
次に本実施の形態に係る秘密鍵配送システム６０の動作について説明する。秘密鍵配送システム６０は、送信機において、波長λ$_1$～λ$_n$に分けられた単一光子に秘密鍵情報の要素を付与して、秘密鍵情報を有する複数の単一光子からなる単一光子列として送信する。一波長を有する単一光子列は、対応する１個の受信機に送信される。このようにして、ｎ個の波長の単一光子列が各々受信機４０$_1$～４０$_n$に同時に送信される。
【００７３】
そして、受信機４０$_1$～４０$_n$の各々において単一光子列から秘密鍵情報が取り出される。このようにして、１個の送信機とｎ個の受信機の各々との間で秘密鍵情報が共有される。
【００７４】
第２の実施の形態に係る秘密鍵配送システム６０は、波長多重化単一光子源２１を用いることにより、従来では不可能であった１個の送信機６１から同時にｎ個の受信機４０$_1$～４０$_n$に秘密鍵情報を送信することが可能となる。秘密鍵配送システム６０は、第１の実施の形態に係る秘密鍵配送システムと同様に、従来の疑似的単一光子源を用いた秘密鍵配送システムよりも秘密鍵情報を高転送レートで送信でき、また、安全性も高い。
【００７５】
（第３の実施の形態）
本発明の第３の実施の形態に係る秘密鍵配送システムは、送信機が波長多重化されたエンタングル状態の単一光子対を分離して２つの受信機に送信し、２つの受信機が波長多重化された単一光子の量子状態に基づいて秘密鍵情報を生成して共有するものである。なお、エンタングル状態の単一光子対は、２つの単一光子の量子状態（量子力学により記述される状態をいう。）が特定の組み合わせを有する状態であることをいう。
【００７６】
図９は、本発明の第３の実施の形態に係る秘密鍵配送システムの構成を示すブロック図である。
【００７７】
図９を参照するに、秘密鍵配送システム７０は、波長多重化されたエンタングル状態の単一光子対を生成し、各波長毎にその単一光子対を２つの単一光子に分離し、２つに分離された各々の波長の単一光子を合波して光伝送路１１に送信する送信機８０と、２つの光

伝送路１１と、光伝送路１１から波長多重化された単一光子対の一方の単一光子を受信する２つの受信機９１、９２から構成される。

【００７８】

送信機８０は、波長多重化されたエンタングル状態の単一光子対を生成する単一光子対源８１と、波長多重化された単一光子対を波長毎に分離する光分波器２２と、波長毎に分離した単一光子対を所望の波長成分だけを通過させるバンドパスフィルタ２３と、単一光子対を各々の単一光子に分ける光カプラ２３と、分けられた各波長の単一光子を合波して光伝送路１１に送出する光混合器２５から構成される。

【００７９】

単一光子対源８１は、図２に示す波長多重単一光源２１と同様の構成を有する。すなわち、単一光子対源８１は、図２に示すように、レーザ光源２８と、光カプラ２９と、出力モニタ３０と、集光光学系３１と、量子ドット構造体５０と、冷凍機３５と、ローパスフィルタ３７と、これらを接続する光ファイバ３６等から構成される。本実施の形態では、第１の実施の形態の量子ドット構造体を用いて励起光の照射により波長が異なる複数のエンタングル状態の単一光子対（波長多重化されたエンタングル状態の単一光子対）を生成する。量子ドット構造体からのエンタングル状態の単一光子対の生成は、以下に述べるように理論的に予想されているものである。この理論と第１の実施の形態の量子ドット構造体とにより、波長が異なる複数のエンタングル状態の単一光子対を生成できるはずである。

【００８０】

図１０は、エンタングル状態の単一光子対の発生を説明するためのエネルギー状態図である。

【００８１】

図１０を参照するに、量子ドット構造体に励起光を照射するとＩｎＡｓ量子ドットでは二励起子状態E_2が生じる。二励起子状態E_2は、スピンの向きが異なる２つの電子正孔対が遷移したものである。二励起子状態E_2にある電子正孔対は一励起子状態E_1を介して基底状態E_0に遷移する際、２つの経路で遷移することが理論的に知られている（Ｐｈｙｓ．Ｒｅｖ．Ｌｅｔｔ．Ｖｏｌ．８４（２０００）ｐｐ．２５１３～ｐｐ．２５１６）。一方の経路では、二励起子状態E_2から一励起子状態E_1に遷移する際に右回り円偏光の単一光子σ^+を放出し、次いで、基底状態E_0に遷移する際に左回り円偏光の単一光子σ^-を放出する。他方の経路では、二励起子状態E_2から一励起子状態E_1に遷移する際に左回り円偏光の単一光子σ^-を放出し、次いで、基底状態E_0に遷移する際に右回り円偏光の単一光子σ^+を放出する。このように、単一光子σ^+および単一光子σ^-がこの順でカスケードに放射される単一光子対と、単一光子σ^-および単一光子σ^+がこの順でカスケードに放射される単一光子対がある。これらの単一光子対は、いずれも、一方の単一光子が右回り円偏光の場合、他方の単一光子は必ず左回り円偏光となる。したがって、単一光子対の各々の単一光子は相関を有し、エンタングル状態にある。

【００８２】

図９に戻り、このようにして、単一光子対源８１は、エンタングル状態にある単一光子対を放射する。さらに、単一光子対源８１は、量子ドット構造体に大きさの異なる量子ドットが形成されているので、波長が異なる複数のエンタングル状態にある単一光子対を同時に放射する。

【００８３】

光分波器２２およびバンドパスフィルタ２３は、第１の実施の形態と同様の構成を有し、波長多重化された単一光子対を波長λ_1～λ_n毎に分岐させ、所望の波長λ_1～λ_nの単一光子対のみを通過させる。

【００８４】

光カプラ８２は、単一光子対を単純分波することにより、右回り円偏光の単一光子と左回り円偏光の単一光子とに分離する。そして、各々の単一光子を各々の光混合器２５に送出する。光混合器２５は光カプラから送られてきた単一光子を合波して波長多重化し光伝

送路１１に送出する。すなわち、エンタングル状態の単一光子対は、単一光子に分離されて２つの受信機９１、９２に別々に送信される。

【００８５】

受信機９１、９２は、光伝送路から受けた波長多重化された単一光子を波長毎に分離する光分波器２２と、単一光子毎に右回りあるいは左回り円偏光を検出する検出器４２_{1}～４２_{n}から構成される。

【００８６】

光分波器２２は、送信機８０の光分波器２２と同様の構成を有し、多重化された単一光子を波長λ_{1}～λ_{n}毎に分岐させる。

【００８７】

検出器４２_{1}～４２_{n}は、例えば、アバランシェフォトダイオードを用いることができる。２つの受信機９１、９２では同じタイプの検出器を用いることが好ましい。

【００８８】

次に本実施の形態に係る秘密鍵配送システム７０の動作について説明する。秘密鍵配送システム７０では、以下のようにして秘密鍵が生成される。

【００８９】

送信機８０からエンタングル状態にある単一光子が受信機９１と受信機９２に送信される。説明の簡単のため、波長λ1を例に挙げる。例えば、一方の受信機９１の波長λ_{1}の検出器４２_{1}で右回り円偏光の単一光子が検出された場合、他方の受信機９２の波長λ_{1}の検出器４２_{1}では必ず左回り円偏光の単一光子が検出されることが確定する。

【００９０】

したがって、一方の受信機９１の検出器４２が単一光子の円偏光の向きを検出すると、他方の受信機９２の同じ波長の検出器４２では、受信機９１とは逆の向きの円偏光が検出されることが自ずと確定する。このようにして検出した波長λ_{1}～λ_{n}までの情報を復号化して秘密鍵情報とする。例えば、一方の受信機９１では右回り円偏光を“１”、左回り円偏光を“０”とする。他方の受信機９２では、右回り円偏光を“０”、左回り円偏光を“１”とする。このようにして、２つの受信機は秘密鍵を共有することができる。なお、λ_{1}～λ_{n}までの情報の総てを秘密鍵情報としてもよく、λ_{1}～λ_{n}までの情報の一部を秘密鍵情報としてもよい。また、これを時系列的に繰り返して、さらにビット数の多い秘密鍵情報としてもよい。

【００９１】

第三者が盗聴しているかどうか検知する場合は、秘密鍵情報の一部の情報を一方の受信機９１から他方の受信機９２に公開通信路（不図示）を介して送信する。他方の受信機９２は受け取った情報と自分が所有する情報とを照合する。もし、情報が一致しない割合が高い場合は盗聴された可能性が高い。このようにして、第三者の盗聴を検知できる。なお、この場合は秘密鍵情報全体を破棄し再度秘密鍵を入手する。

【００９２】

第３の実施の形態に係る秘密鍵配送システム７０は、送信機８０が単一光子対源８１から波長が異なる複数のエンタングル状態の単一光子対を同時に生成し、各々の波長の単一光子対を単一光子に分離して、２つの受信機に各々の単一光子を波長多重化して送信する。受信機９１、９２は、各波長の単一光子の円偏光の向きを検出し符号化して秘密鍵情報を生成する。したがって、エンタングル状態の単一光子が波長多重化されているので、秘密鍵情報となる媒体を高転送レートで送信できる。

【００９３】

さらに、単一光子対源８１は励起光の１ショット毎に波長多重化された単一光子対が生成される。この点においても秘密鍵配送システム７０は秘密鍵情報となる媒体を高転送レートで送信できる。

【００９４】

（第４の実施の形態）

本発明の第４の実施の形態に係る秘密鍵配送システムは、送信機が波長多重化されたエ

ンタングル状態の単一光子対を単一光子に分離して、１つの第１受信機とｎ個の第２受信機に送信し、第１受信機とｎ個の第２受信機の各々とが単一光子（あるいは単一光子列）の量子状態に基づいて秘密鍵情報を生成して共有するものである。第４の実施の形態に係る秘密鍵配送システムは、第３の実施の形態に係る秘密鍵配送システムの変形例である。

【００９５】

図１１は、本発明の第４の実施の形態に係る秘密鍵配送システムの構成を示すブロック図である。

【００９６】

図１１を参照するに、秘密鍵配送システム１００は、送信機１０１と、波長多重化された単一光子が供給される第１受信機９１と、波長毎に単一光子が供給されるｎ個の第２受信機９２_{1}～９２_{n}と、送信機１０１と第１受信機９１または第２受信機９２_{1}～９２_{n}とを接続する光伝送路１１、１２_{1}～１２_{n}から構成される。

【００９７】

送信機１０１は、ｎ個の第２受信機９２_{1}～９２_{n}が接続される側に、図９に示す光混合器２５が設けられていない点を除いては図９に示す送信機８０と略同様の構成からなる。すなわち、光カプラ８２で分離された単一光子の一方は、合波されない状態で、波長毎にｎ個の第２受信機９２_{1}～９２_{n}に送信される。

【００９８】

第１受信機９１は、波長毎に検出器４２_{1}～４２_{n}を備え、図９に示す受信機９１と同様の構成からなる。第２受信機９２_{1}～９２_{n}は、各々、図９に示す検出器４２と同様の検出器４２_{1}～４２_{n}を備える。

【００９９】

送信機１０１は、第１受信機９１に、エンタングル状態の単一光子対が分離された単一光子の一方を波長多重化して送信する。これは第３の実施の形態と同様である。送信機１０１は、第２受信機９２_{1}～９２_{n}の各々には、エンタングル状態の単一光子対が分離された単一光子の他方を波長毎に送信する。

【０１００】

第１受信機９１および第２受信機９２_{1}～９２_{n}は、第３の実施の形態と同様にして秘密鍵情報を生成する。例えば、第１受信機９１および第２受信機９２_{1}～９２_{n}は、割当てられた波長において、時間経過にしたがって受信する複数の単一光子からなる単一光子列から秘密鍵情報を生成する。この際、第１受信機９１および第２受信機９２_{1}～９２_{n}は、必要ならば単一光子を検出した時刻データを合わせて用いてもよい。この結果、第１受信機９１と第２受信機９２_{1}～９２_{n}の各々とが、それぞれ異なる秘密鍵情報を共有する。

【０１０１】

第４の実施の形態に係る秘密鍵配送システム１００は、送信機１０１の単一光子対源８１が波長の異なる複数のエンタングル状態の単一光子対を同時に生成し、各々の波長の単一光子対を単一光子に分離してその一方の単一光子を波長多重化して第１受信機９１に送信する。また、送信機１０１は、その他方の単一光子を波長毎にｎ個の第２受信機９２_{1}～９２_{n}の各々に送信する。そして、第１受信機９１および第２受信機９２_{1}～９２_{n}は、時間経過に従って受信する複数の単一光子（単位光子列）の各々から円偏光の向きを検出し、符号化して秘密鍵情報を生成する。したがって、秘密鍵配送システム１００は、１つの第１受信機９１とｎ個の第２受信機９２_{1}～９２_{n}の各々との間で、秘密鍵情報を生成するための媒体、つまりエンタングル状態の単一光子の各々を同時に配送可能である。従来は第１受信機とｎ個の第２受信機の各々との間で秘密鍵情報を生成するための媒体の送信をｎ回繰り返して行っていたが、秘密鍵配送システム１００は並列的に送信するため高速で行える。

【０１０２】

さらに、単一光子対源８１は励起光の１ショット毎に波長多重化された単一光子対が生成される。この点においても秘密鍵配送システム１００は秘密鍵情報となる媒体を効率良く、高転送レートで送信できる。

【０１０３】
（第５の実施の形態）
本発明の第５の実施の形態に係る秘密鍵配送システムは、送信機が波長多重化されたエンタングル状態の単一光子対を単一光子に分離して、ｎ個の第１受信機とｎ個の第２受信機に送信し、ｎ組の第１受信機と第２受信機とが単一光子（あるいは単一光子列）の量子状態に基づいて秘密鍵情報を生成して共有するものである。第５の実施の形態に係る秘密鍵配送システムは、第４の実施の形態に係る秘密鍵配送システムの変形例である。
【０１０４】
図１２は、本発明の第５の実施の形態に係る秘密鍵配送システムの構成を示すブロック図である。
【０１０５】
図１２を参照するに、秘密鍵配送システム１１０は、送信機１１１と、波長毎に単一光子が供給されるｎ個の第１受信機９１_{1}～９１_{n}と、波長毎に単一光子が供給されるｎ個の第２受信機９２_{1}～９２_{n}と、送信機１１１と第１受信機９１_{1}～９１_{n}または第２受信機９２_{1}～９２_{n}とを接続する光伝送路１１_{1}～１１_{n}、１２_{1}～１２_{n}から構成される。
【０１０６】
送信機１０１は、ｎ個の第１受信機９１_{1}～９１_{n}が接続される側に、図１１に示す光混合器２５が設けられていない点を除いては図１１に示す送信機１０１と略同様の構成からなる。すなわち、光カプラ８２で分離された単一光子の一方は、合波されない状態で、波長毎にｎ個の第１受信機９１_{1}～９１_{n}に送信される。
【０１０７】
第１受信機９１_{1}～９１_{n}は、波長毎に検出器４２_{1}～４２_{n}を備え、図１１に示す受信機９２と同様の構成からなる。第１受信機９２_{1}～９２_{n}は、各々、図１１に示す検出器４２_{1}～４２_{n}と同様の構成からなる。
【０１０８】
送信機１０１は、第１受信機９１_{1}～９１_{n}の各々に、エンタングル状態の単一光子対が分離された単一光子の一方を波長毎に送信する。また、送信機１０１は、第２受信機９２_{1}～９２_{n}の各々に、エンタングル状態の単一光子対が分離された単一光子の他方を波長毎に送信する。
【０１０９】
第１受信機９１_{1}～９１_{n}および第２受信機９２_{1}～９２_{n}は、第３の実施の形態と同様にして秘密鍵情報を生成する。例えば、第１受信機９１_{1}～９１_{n}および第２受信機９２_{1}～９２_{n}は、割当てられた波長において、時間経過にしたがって受信する複数の単一光子からなる単一光子列から秘密鍵情報を生成する。この際、第１受信機９１_{1}～９１_{n}および第２受信機９２_{1}～９２_{n}は、必要ならば単一光子を検出した時刻データを合わせて用いてもよい。この結果、同じ波長の単一光子を検出する１つの第１受信機と１つの第２受信機とが秘密鍵情報を共有する。すなわち、波長$λ_{1}$の単一光子を受信する第１受信機９１_{1}と第２受信機９２_{1}とが秘密鍵情報を共有する。したがって、ｎ組の第１受信機と第２受信機とが秘密鍵情報を共有する。なお、各々の組が有する秘密鍵情報はそれぞれ異なるものになるであろう。
【０１１０】
第５の実施の形態に係る秘密鍵配送システム１１０は、送信機１１１の単一光子対源８１から波長が異なる複数のエンタングル状態の単一光子対を同時に生成し、各々の波長の単一光子対を単一光子に分離してその一方を波長多重化して第１受信機９１に送信し、その他方を波長毎にｎ個の第２受信機９２_{1}～９２_{n}の各々に送信する。第１受信機９１および第２受信機９２_{1}～９２_{n}は、時間経過に従って受信する複数の単一光子（単位光子列）の各々から円偏光の向きを検出し、符号化して秘密鍵情報を生成する。
【０１１１】
第５の実施の形態に係る秘密鍵配送システム１１０は、送信機１１１の単一光子対源８１が波長の異なる複数のエンタングル状態の単一光子対を同時に生成し、各々の波長の単

一光子対を単一光子に分離してその一方を波長毎にｎ個の第１受信機９１$_1$～９１$_n$に送信し、その他方を波長毎にｎ個の第２受信機９２$_1$～９２$_n$の各々に送信する。第１受信機９１$_1$～９１$_n$および第２受信機９２$_1$～９２$_n$は、時間経過に従って受信する複数の単一光子（単位光子列）の各々から円偏光の向きを検出し、符号化して秘密鍵情報を生成する。したがって、秘密鍵配送システム１１０は、ｎ組の第１受信機と第２受信機に、秘密鍵情報を生成するための媒体、つまりエンタングル状態の単一光子の各々を同時に配送可能である。従来は第１受信機と第２受信機の各々との間で秘密鍵情報を生成するための媒体の送信をｎ回繰り返して行っていたが、秘密鍵配送システム１１０は並列的に送信するため高速で行える。

【０１１２】

さらに、単一光子対源８１は励起光の１ショット毎に波長多重化された単一光子対が生成される。この点においても秘密鍵配送システム１１０は秘密鍵情報となる媒体を効率良く、高転送レートで送信できる。

【０１１３】

以上本発明の好ましい実施の形態について詳述したが、本発明は係る特定の実施の形態に限定されるものではなく、特許請求の範囲に記載された本発明の範囲内において、種々の変形・変更が可能である。

【０１１４】

なお、以上の説明に関して更に以下の付記を開示する。

（付記１）　単一光子を生成する単一光子源と、該単一光子に秘密鍵情報を付与する符号化部と、を有する送信機と、

前記単一光子から秘密鍵情報を取出す検出部とを有する受信機と、

前記送信機と受信機とを接続する光伝送路と、を備える秘密鍵配送システムであって、

前記送信機は、

前記単一光子源が波長の異なる複数の単一光子を同時に生成する量子ドット構造体を有し、

前記単一光子源と前記符号化部との間に、単一光子を波長毎に分岐させる光分波器を有し、

前記符号化部が単一光子の波長毎に設けられてなることを特徴とする秘密鍵配送システム。

（付記２）　前記送信機は、符号化部と光伝送路との間に、波長の異なる複数の単一光子を合波し同時に光伝送路に送出する光混合器をさらに有し、

前記受信機は、光伝送路と検出部との間に該単一光子の各々を波長毎に分岐させる他の光分波器を有し、該検出部が単一光子の波長毎に設けられてなることを特徴とする付記１記載の秘密鍵配送システム。

（付記３）　前記送信機は、波長の異なる複数の単一光子を波長毎に光伝送路に送出して、複数の受信機に秘密鍵情報を送信することを特徴とする付記１記載の秘密鍵配送システム。

（付記４）　波長の異なる複数の単一光子を同時に生成する量子ドット構造体を有する単一光子源と、該単一光子の各々を波長毎に分岐させる光分波器と、該単一光子の各々に秘密鍵情報の要素を付与する符号化部と、該符号化部からの波長の異なる複数の単一光子を合波し、波長の異なる複数の単一光子を同時に光伝送路に送出するする光混合器と、を有する送信機と、

前記単一光子を波長毎に分岐させる他の分波器と、該単一光子の波長毎に設けられ、単一光子の各々から秘密鍵情報の要素を取出す検出部と、を有する受信機と、

前記通信機と受信機とを接続する光伝送路と、

を備える秘密鍵配送システム。

（付記５）　波長の異なる複数の単一光子を同時に生成する量子ドット構造体を有する単一光子源と、該単一光子の各々を波長毎に分岐させる光分波器と、該単一光子の各々に秘密鍵情報の要素の各々を付与する符号化部と、を有する送信機と、

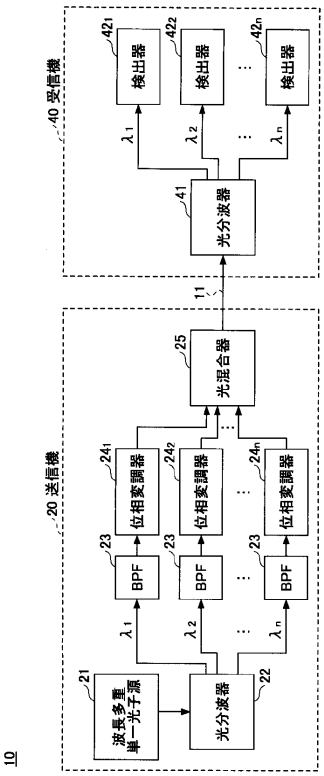
前記単一光子の各々から秘密鍵情報の要素を取出す検出部を有し、前記波長の数に対応する数の受信機と、
前記通信機と受信機の各々とを接続する光伝送路と、
を備える秘密鍵配送システム。
（付記６） 前記単一光子源はレーザ光源を有し、
前記量子ドット構造体はレーザ光源からの励起光の照射により単一光子を発光することを特徴とする付記１～５のうち、いずれか一項記載の秘密鍵配送システム。
（付記７） 前記量子ドット構造体は、一つの半導体層の表面に、複数の互いに大きさの異なる量子ドットが設けられてなることを特徴とする付記１～６のうち、いずれか一項記載の秘密鍵配送システム。
（付記８） 前記量子ドット構造体は、ＩｎＰ半導体層と、該ＩｎＰ半導体層上に形成されたＩｎＡｓからなる量子ドットからなることを特徴とする付記７記載の秘密鍵配送システム。
（付記９） 前記量子ドットは離散的な高さを有することを特徴とする付記７または８記載の秘密鍵配送システム。
（付記１０） 前記量子ドット構造体は、頂上が平坦な山型あるいは台地状の形状に形成されてなる付記７～９のうち、いずれか一項記載の秘密鍵配送システム。
（付記１１） 前記光分波器と符号化部との間に、所定の波長以外の光子を遮断するバンドパスフィルタを設けることを特徴とする付記１～１０のうち、いずれか一項記載の秘密鍵配送システム。
（付記１２） ２つの受信機が秘密鍵情報を共有するための秘密鍵配送システムであって、
エンタングル状態の単一光子対を生成する単一光子対源と、該単一光子対を各々の単一光子に分離する光分離器とを有する送信機と、
前記分離された単一光子のいずれか一方を受信して、秘密鍵情報を生成する２つの受信機と、
前記送信機と受信機の各々とを接続する光伝送路とを備え、
前記送信機は、
前記単一光子対源が波長の異なる複数のエンタングル状態の単一光子対を同時に生成する量子ドット構造体を有することを特徴とする秘密鍵配送システム。
（付記１３） 前記送信機は、
前記単一光子対源と光分離器との間に単一光子対を波長毎に分岐させる光分波器と、
単一光子の波長毎に設けられた前記光分離器と、
分離された波長の異なる複数の単一光子を合波する光混合器とを有し、
前記受信機は、
前記光伝送路と検出部との間に該単一光子の各々を波長毎に分岐させる他の光分波器と、
単一光子の波長毎に設けられた前記検出部とを有することを特徴とする付記１２記載の秘密鍵配送システム。
（付記１４） １つの第１の受信機と複数の第２の受信機の各々とが秘密鍵情報を共有するための秘密鍵配送システムであって、
波長の異なる複数のエンタングル状態の単一光子対を生成する量子ドット構造体を有する単一光子対源と、該単一光子対を各々の単一光子に分離する光分離器と、分離された単一光子の一方でかつ波長の異なる単一光子を合波して同時に送出する光混合器とを有する送信機と、
前記合波された単一光子を受信する第１の受信機と、前記分離された単一光子の他方を波長毎に受信する複数の第２の受信機からなることを特徴とする秘密鍵配送システム。
（付記１５） 組をなす１つの第１の受信機と１つの第２の受信機とが秘密鍵情報を共有し、複数の組の第１の受信機および第２受信機に秘密鍵情報を送信する秘密鍵配送システムであって、

波長の異なる複数のエンタングル状態の単一光子対を生成する量子ドット構造体を有する単一光子対源と、該単一光子対を各々の単一光子に分離する光分離器と、を有する送信機と、
前記分離された単一光子の一方を波長毎に受信する複数の第１の受信機と、前記分離された単一光子の他方を波長毎に受信する複数の第２の受信機とからなり、
前記組をなす第１の受信機および第２の受信機は、同一波長の単一光子を各々受信することを特徴とする秘密鍵配送システム。
（付記１６）　前記単一光子対源はレーザ光源を有し、
前記量子ドット構造体はレーザ光源からの励起光の照射によりエンタングル状態の単一光子対を発光することを特徴とする付記１２～１５のうち、いずれか一項記載の秘密鍵配送システム。
（付記１７）　前記量子ドット構造体は、１．３μｍ～１．５５μｍの範囲から選択された波長の単一光子あるいは単一光子対を生成することを特徴とする付記１～１６のうち、いずれか一項記載の秘密鍵配送システム。
（付記１８）　送信機と受信機とが秘密鍵情報を共有するための秘密鍵配送方法であって、
前記送信機において、量子ドット構造体に励起光を照射して波長の異なる複数の単一光子を同時に生成し、該単一光子の各々に秘密鍵情報の要素を付与して受信機に送信し、
前記受信機において、各々の単一光子から秘密鍵情報を取り出すことを特徴とする秘密鍵配送方法。
（付記１９）　前記送信機において、秘密鍵情報の要素が付与された波長の異なる複数の単一光子を合波して受信機に送信することを特徴とする付記１８記載の秘密鍵配送方法。
（付記２０）　前記受信機が複数からなり、
前記送信機は、前記単一光子の波長毎に秘密鍵情報を付与して波長毎に単一光子列を形成し、複数の受信機の各々に互いに異なる波長の単一光子列を送信することを特徴とする付記１８記載の秘密鍵配送方法。
（付記２１）　２つの受信機が秘密鍵情報を共有するための秘密鍵配送方法であって、
量子ドット構造体に励起光を照射して波長の異なる複数のエンタングル状態の単一光子対を同時に生成し、該単一光子対を各々の単一光子に分離して、分離された単一光子を受信機の各々に送信し、
各々の受信機において、単一光子の量子状態を検出して秘密鍵情報を生成することを特徴とする秘密鍵配送方法。
（付記２２）　１つの第１の受信機と複数の第２の受信機の各々とが秘密鍵情報を共有するための秘密鍵配送方法であって、
量子ドット構造体に励起光を照射して波長の異なる複数のエンタングル状態の単一光子対を同時に生成し、該単一光子対を各々の単一光子に分離して、分離された一方の単一光子でかつ波長の異なる単一光子を合波して第１の受信機に送信し、分離された他方の単一光子を波長毎に第２の受信機の各々に送信し、
第１および第２の受信機の各々において、単一光子の量子状態を検出して秘密鍵情報を生成することを特徴とする秘密鍵配送方法。
【図面の簡単な説明】
【０１１５】
【図１】本発明の第１の実施の形態に係る秘密鍵配送システムの構成を示すブロック図である。
【図２】第１の実施の形態の波長多重単一光子源の構成を示す図である。
【図３】量子ドット構造体の模式的斜視図である。
【図４】量子ドット構造体の要部断面図である。
【図５】量子ドット構造体の１０Ｋでの光ルミネセンススペクトルの例を示す図である。
【図６】（Ａ）～（Ｃ）は量子ドット構造体の製造工程図（その１）である。
【図７】（Ａ）および（Ｂ）は量子ドット構造体の製造工程図（その２）である。

【図８】本発明の第２の実施の形態に係る秘密鍵配送システムの構成を示すブロック図である。
【図９】本発明の第３の実施の形態に係る秘密鍵配送システムの構成を示すブロック図である。
【図１０】エンタングル状態の単一光子対の発生を説明するためのエネルギー状態図である。
【図１１】本発明の第４の実施の形態に係る秘密鍵配送システムの構成を示すブロック図である。
【図１２】本発明の第５の実施の形態に係る秘密鍵配送システムの構成を示すブロック図である。
【符号の説明】
【０１１６】
１０、６０、７０、１００、１１０　秘密鍵配送システム
１１、11_1～11_n、１２、12_1～12_n　光伝送路
２０、６１、８０、１０１、１１１　送信機
２１　波長多重単一光子源
２２　光分波器
２３　バンドパスフィルタ
２４、24_1～24_n　位相変調器
２５　光混合器
２８　レーザ光源
２９　光カプラ
３０　出力モニタ
３１　集光光学系
３５　冷凍器
３６　光ファイバ
３７　ローパスフィルタ
４０、40_1～40_n、91_1～91_n、９２、92_1～92_n　受信機
４１　光分波器
４２、42_1～42_n　検出器
５０　量子ドット構造体
５１　ＩｎＰ基板
５２　ＩｎＰバッファ層
５３　ＩｎＡｓ量子ドット
５３ａ　ＩｎＡｓ量子ドット前駆体
５４　第１ＩｎＰダブルキャップ層
５５　第２ＩｎＰダブルキャップ層
５６　ＩｎＰキャップ層
８１　単一光子対源
８２　光カプラ

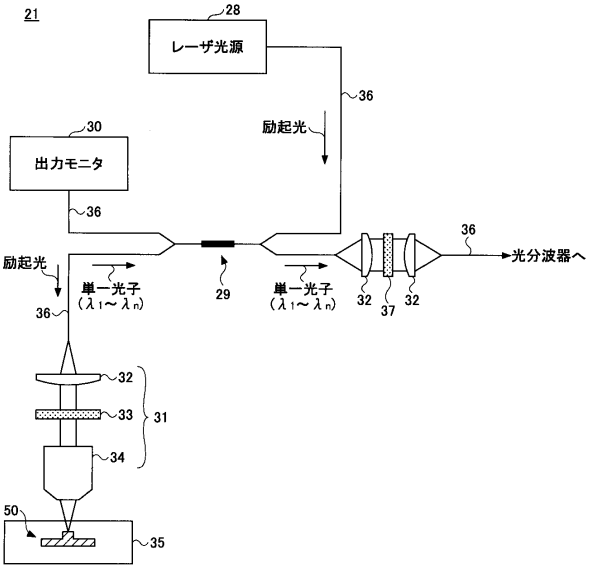
【図１】

本発明の第１の実施の形態に係る秘密鍵配送システムの構成を示すブロック図



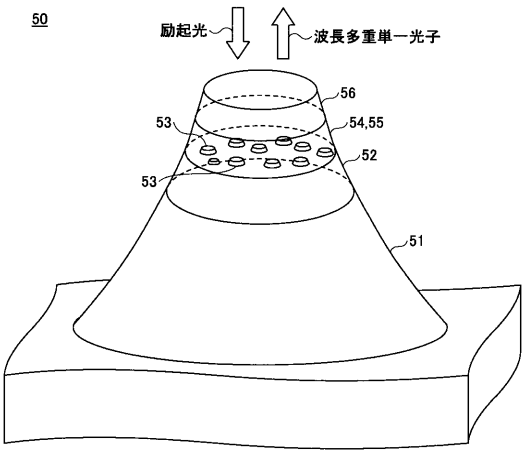
【図２】

第１の実施の形態の波長多重単一光子源の構成を示す図



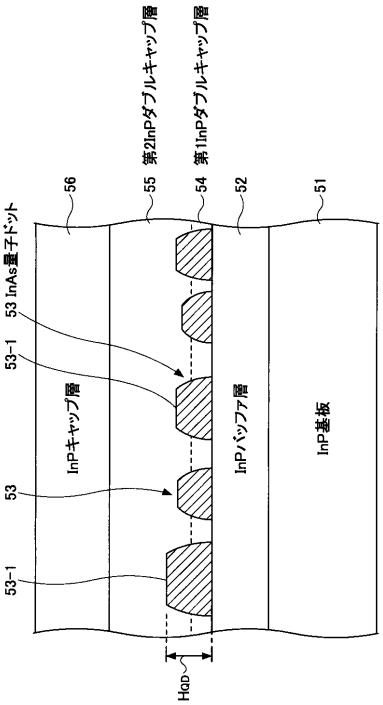
【図３】

量子ドット構造体の模式的斜視図



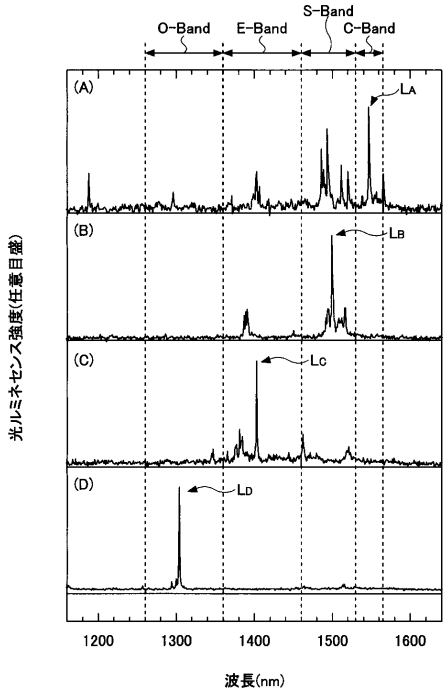
【図４】

量子ドット構造体の要部断面図



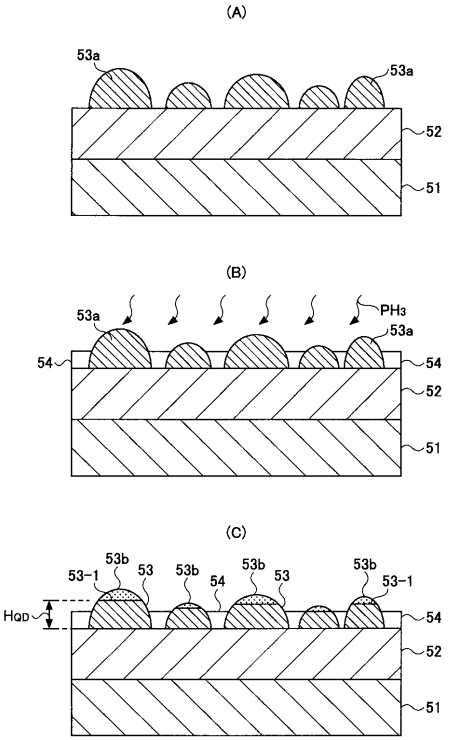
【図５】

量子ドット構造体の10Kでの光ルミネセンススペクトルの例を示す図



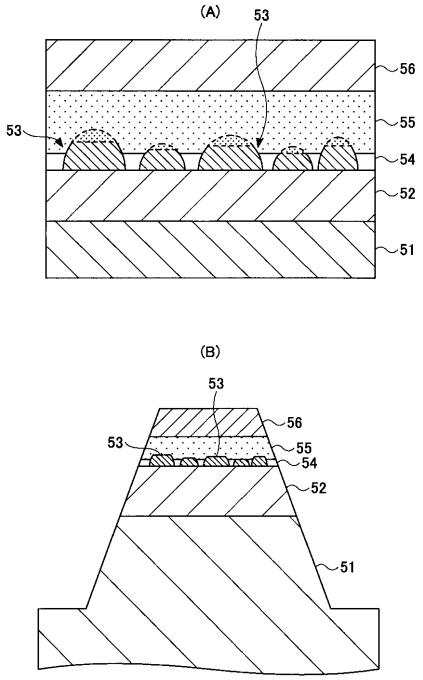
【図６】

(A)～(C)は量子ドット構造体の製造工程図(その1)



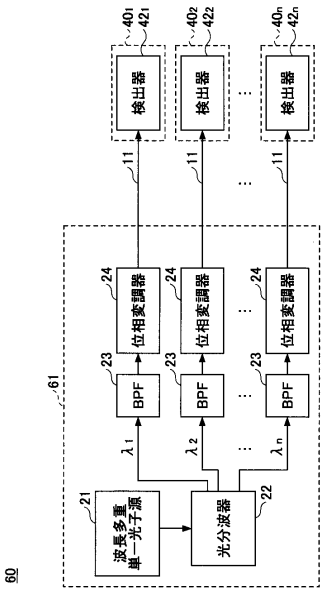
【図７】

(A)および(B)は量子ドット構造体の製造工程図(その2)



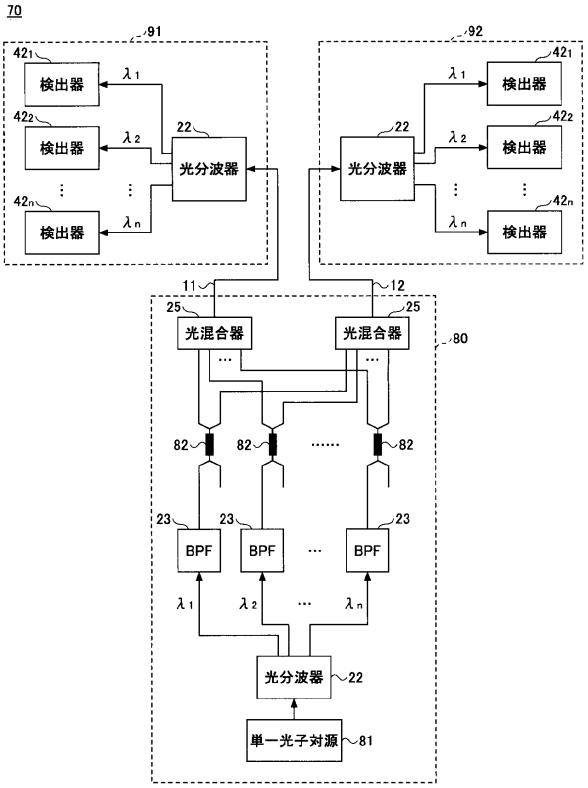
【図８】

本発明の第2の実施の形態に係る秘密鍵配送システムの構成を示すブロック図



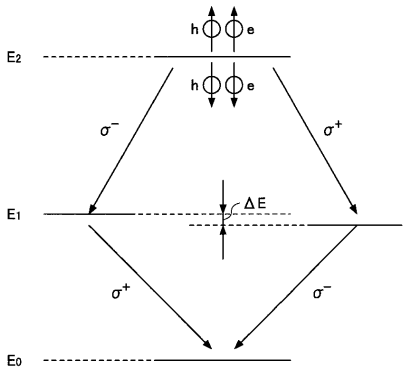
【図９】

本発明の第3の実施の形態に係る秘密鍵配送システムの構成を示すブロック図



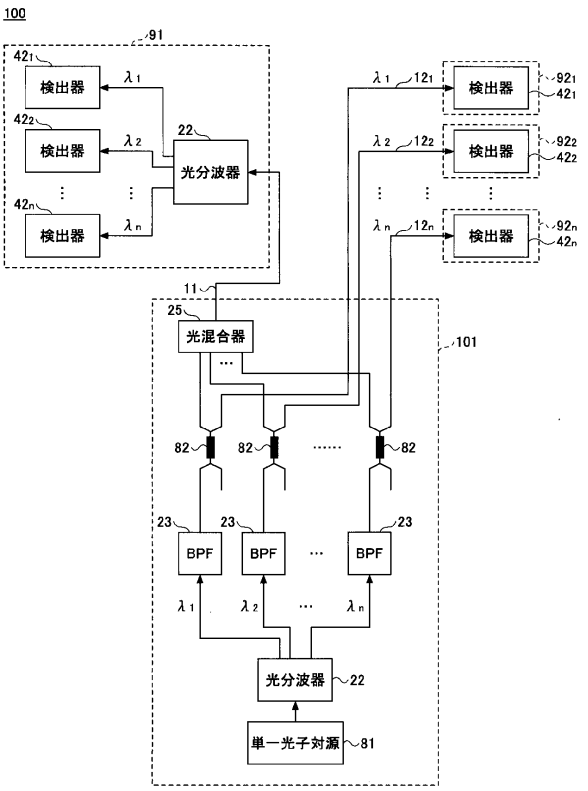
【図１０】

エンタングル状態の単一光子対の発生を説明するためのエネルギー状態図



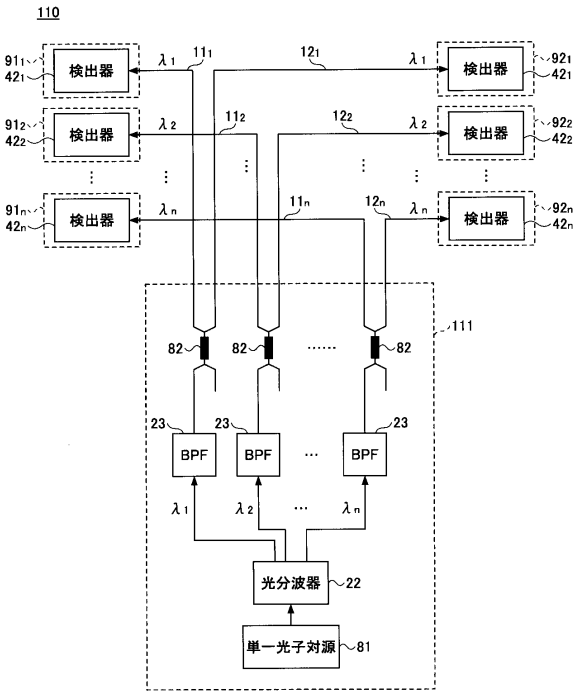
【図１１】

本発明の第4の実施の形態に係る秘密鍵配送システムの構成を示すブロック図



【図１２】

本発明の第5の実施の形態に係る秘密鍵配送システムの構成を示すブロック図



フロントページの続き

(56)参考文献 特開２００４－１８７２６８（ＪＰ，Ａ）
特開２００４－１５７３２６（ＪＰ，Ａ）
特開２００３－０１８１４４（ＪＰ，Ａ）
特開２００１－２３０４４５（ＪＰ，Ａ）
井上 恭 Kyo Inoue，電子情報通信学会２００４年エレクトロニクスソサイエティ大会講演論文集１ PROCEEDINGS OF THE 2004 IEICE ELECTRONICS SOCIETY CONFERENCE，２００４年 ９月，S17-S18
アンドリュー シールズ，傍受不能な光量子暗号通信を可能にする単一光子技術，東芝レビュー，２００２年，Vol.57 No.1，P.25-28，ＵＲＬ，http://www.toshiba.co.jp/tech/review/2002/01/57_01pdf/a07.pdf

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／１２
Ｇ０２Ｆ １／０１５
Ｈ０４Ｂ １０／００