(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2019年6月6日(06.06.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/106971 A1

(51) 国際特許分類:
H04L 9/12 (2006.01)　*G02F 3/00* (2006.01)
G02F 1/01 (2006.01)　*H04B 10/70* (2013.01)

(21) 国際出願番号：　PCT/JP2018/037959

(22) 国際出願日：　2018年10月11日(11.10.2018)

(25) 国際出願の言語：　日本語

(26) 国際公開の言語：　日本語

(30) 優先権データ：
特願 2017-231240　2017年11月30日(30.11.2017) JP

(71) 出願人: 沖電気工業株式会社(**OKI ELECTRIC INDUSTRY CO., LTD.**) [JP/JP]; 〒1058460 東京都港区虎ノ門１丁目７番１２号 Tokyo (JP).

(72) 発明者: 荒平 慎 (**ARAHIRA, Shin**); 〒1058460 東京都港区虎ノ門１丁目７番１２号 沖電気工業株式会社内 Tokyo (JP).

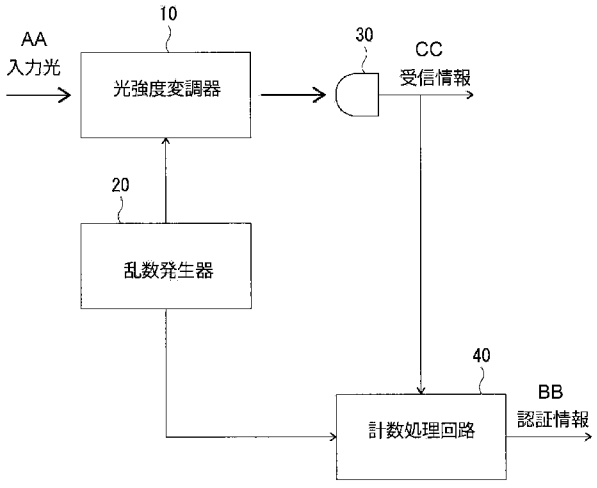
(74) 代理人: 伊藤 学, 外 (**ITO Manabu** et al.); 〒1600023 東京都新宿区新宿区西新宿7-5-14 井上ビル12号館2階 Tokyo (JP).

(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, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

(54) **Title:** SINGLE PHOTON DETECTION DEVICE AND QUANTUM KEY DELIVERY RECEIVING DEVICE

(54) 発明の名称： 単一光子検出装置及び量子鍵配送用受信装置

[図1]



10　Light intensity modulator
20　Random number generator
40　Counting processing circuit
AA　Input light
BB　Authentication information
CC　Reception information

(57) **Abstract:** [Problem] To eliminate hacking by a bright illumination attack on a quantum key delivery receiving device equipped with a single photon detector. [Solution] The present invention comprises: a random number generator that generates random number bit value information which includes a random number value i and the time at which the random number value i was generated; a light intensity modulator that modulates the intensity of light input from the outside at a transmittance T_i determined by the random number value i; a single photon detector

WO 2019/106971 A1

[続葉有]

NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告(条約第21条(3))

---

that receives input of the input light which was intensity-modulated by the light intensity modulator and generates, as reception information, a time at which a single photon was detected; and a counting processing circuit that calculates a determination value $S_i/(T_iM_i)$ for the random number value i from a photon detection rate S_i of the single photon detector, a mark rate M_i which is the percentage accounted for by the random number value i of the random number values generated by the random number value generator, and the transmittance T_i, and that outputs an authentication signal indicating authentication if the determination value satisfies a predetermined criteria or outputs an authentication signal indicating denial if the predetermined criteria is not satisfied.

(57) 要約:【課題】単一光子検出器を備える量子鍵配送用受信装置に対するＢｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃によるハッキングを排除する。【解決手段】ｎ値の乱数を発生させ、乱数値ｉと、乱数値ｉを発生させた時刻を含む乱数ビット値情報を生成する乱数発生器と、乱数値ｉによって定まる透過率Ｔ$_{i}$で外部からの入力光を強度変調する光強度変調器と、光強度変調器で強度変調された入力光が入力され、単一光子を検出した時刻を受信情報として生成する単一光子検出器と、前記乱数値ｉにおける、前記単一光子検出器の光子検出率Ｓ$_{i}$、乱数発生器で発生する乱数値のうち乱数値ｉが占める割合であるマーク率Ｍ$_{i}$、及び、透過率Ｔ$_{i}$から判定値Ｓ$_{i}$／（Ｔ$_{i}$Ｍ$_{i}$）を算出し、判定値が予め定めた基準を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路とを備える。

明　細　書

発明の名称 ： 単一光子検出装置及び量子鍵配送用受信装置

技術分野

[0001] この発明は、量子鍵配送システム等の量子情報通信技術で利用される、単一光子検出装置と、この単一光子検出装置を用いた量子鍵配送用受信装置に関する。

背景技術

[0002] 単一光子レベルの光を検出できる単一光子検出装置は、量子鍵配送システムなど量子情報通信技術の実用化に必要不可欠である。この単一光子検出装置に求められる特性としては、高い検出効率、低い暗電流雑音特性、低いアフターパルス発生確率、高速動作性等がある。一方、実用面を考えると、これら特性と低コスト性のバランスもまた重要な課題である。

[0003] 単一光子検出装置に含まれる、単一光子の検出を行う単一光子検出器として、これまで様々なものが提案されている。中でも、アバランシェフォトダイオード（ＡＰＤ：Ａｖａｌａｎｃｈｅ　ＰｈｏｔｏＤｉｏｄｅ）を利用した単一光子検出器は、実用面で最も有望なものの一つである。

[0004] 特に、ＡＰＤに定常電圧ではなくパルス電圧を印加して動作させる、いわゆるゲート動作型ガイガーモードＡＰＤ（Ｇａｔｅｄ　Ｇｅｉｇｅｒ　ｍｏｄｅ　ＡＰＤ）では、高い検出効率、低い暗電流雑音特性、及び、低いアフターパルス発生確率が実現される。上記のようなＧｅｔｅｄ　Ｇｅｉｇｅｒ　ｍｏｄｅ動作は、光通信波長帯（１．３μｍ／１．５μｍ）での単一光子検出器としてよく使用されているＩｎＧａＡｓ／ＩｎＰ－ＡＰＤに主に実装され、基礎実験や商用システム開発等で利用されている。

[0005] 図９を参照して、アクティブモジュレーション型の量子鍵配送用受信装置の一構成例を説明する。図９は、アクティブモジュレーション型の量子鍵配送用受信装置の一構成例の模式図である。

[0006] 量子鍵配送用受信装置は、偏波変調用乱数発生器１２０、偏波変調器１１

０、偏光ビームスプリッタ１４０、第１の単一光子検出部１３１、第２の単一光子検出部１３２、及び、生鍵生成回路１５０を備えて構成されている。

[0007] 送信側装置（以下、送信者と称する。）は、単一光子レベルの光子を発生させ、これに偏波変調を施したうえで、受信側装置（以下、受信者と称する。）に送信する。送信者が行う偏波変調は、例えば、縦偏光（Ｖ偏光）及び横偏光（Ｈ偏光）を一方の組とし、これらと非直交な右斜め直線偏光（Ｄ（＋）偏光）及び左斜め直線偏光（Ｄ（－）偏光）を他方の組とし、これら４つの偏光状態のいずれか１つを無作為（ランダム）に選択して行う。

[0008] 送信者は、Ｖ偏光又はＤ（＋）偏光を選んだときは、自らのビット値を「１」とし、Ｈ偏光又はＤ（－）偏光を選んだときは、自らのビット値を「０」とする。そして、Ｖ偏光又はＨ偏光を選んだときは、Ｈ／Ｖ送信基底を選択したものとし、Ｄ（＋）偏光又はＤ（－）偏光を選んだときは、Ｄｉａｇｏｎａｌ送信基底を選択したものとする。

[0009] 受信者が備える偏波変調用乱数発生器１２０は、２値の偏波変調器用乱数を発生させ、偏波乱数値ｋ（ｋは０又は１）と、偏波乱数値ｋを発生させた時刻を含む基底乱数情報を生成する。基底乱数情報は、偏波変調器１１０及び生鍵生成回路１５０に送られる。

[0010] 受信者が備える偏波変調器１１０は、偏波変調用乱数発生器１２０が発生した乱数の偏波乱数値ｋに応じて、通過する光の偏波状態を変更する。

[0011] 偏波乱数値が「０」であるとき、偏波変調器１１０は、入力光の偏光状態を変えない。この場合、受信者は、Ｈ／Ｖ受信基底を選択したものとする。

[0012] 偏波乱数値が「１」であるとき、偏波変調器１１０は、入力光の偏光状態を、Ｖ偏光又はＨ偏光を、それぞれＤ（＋）偏光又はＤ（－）偏光に変え、Ｄ（＋）偏光又はＤ（－）偏光をＶ偏光又はＨ偏光に変える。この場合、受信者は、Ｄｉａｇｏｎａｌ受信基底を選択したものとする。

[0013] 偏光ビームスプリッタ１４０は、第１及び第２の出力端を有している。偏光ビームスプリッタは、入力された光がＨ偏光の場合は、第１の出力端から出力して第１の単一光子検出部１３１に送り、Ｖ偏光の場合は、第２の出力

端から出力して第２の単一光子検出部１３２に送る。また、偏光ビームスプリッタ１４０は、入力された光がＤ（＋）偏光又はＤ（－）偏光の場合は、第１及び第２の出力端からランダムに出力する。

[0014] 第１及び第２の単一光子検出部１３１及び１３２は、それぞれ、いわゆるゲート動作型ガイガーモードＡＰＤ（以下、単にＡＰＤとも称する。）で構成され、光子を検出した時刻を第１及び第２の受信情報として、生鍵生成回路１５０に送る。

[0015] 生鍵生成回路１５０は、第１の単一光子検出部１３１で光子を検出した場合は、自らのビット値を「０」とし、第２の単一光子検出器で光子を検出した場合は、自らのビット値を「１」とする。また、偏波乱数値が「０」の場合は、Ｈ／Ｖ受信基底が選択され、「１」の場合は、Ｄｉａｇｏｎａｌ受信基底が選択されたものとする。生鍵生成回路１５０は、第１及び第２の単一光子検出器のいずれかでヒットした時刻での偏波乱数値から、受信者が受信した光の偏光状態が、Ｈ偏光、Ｖ偏光、Ｄ（－）偏光、Ｄ（＋）偏光のいずれかであるかを得ることができ、これが受信側での生鍵となる。

[0016] その後、秘密鍵蒸留部（図示を省略する。）において、送信者の生鍵と受信者の生鍵から、鍵蒸留プロセスが行われ、送信者と受信者とで最終的な秘密鍵が共有される。ここで、鍵蒸留プロセスには、例えば、シフト鍵生成、誤り訂正、及び、秘密増幅のプロセスが含まれる。

[0017] ここで、送信者と受信者の間に盗聴者が存在し、送信者が受信者に送った光子に対して盗聴者が何らかの操作をした場合、シフト鍵の誤り率が増加する。この誤り率の増加から盗聴者の存在を知り、場合によっては当該セッションを破棄することで、量子鍵配送システムでは安全な秘密鍵を共有できる。

[0018] 図９を参照して説明した量子鍵配送用受信装置はアクティブモジュレーション型であったが、偏波変調用乱数発生器、偏波変調器の代わりにハーフミラーと波長板を備えるパッシブモジュレーション型としてもよい。

[0019] 図１０を参照して、パッシブモジュレーション型の量子鍵配送用受信装置

の一構成例を説明する。図１０は、パッシブモジュレーション型の量子鍵配送用受信装置の一構成例の模式図である。

[0020] この量子鍵配送用受信装置は、ハーフミラー１１２、波長板１１４、第１及び第２の偏光ビームスプリッタ１４１及び１４２、第１～第４の単一光子検出部１３１～１３４、生鍵生成回路１５０を備えて構成されている。

[0021] ハーフミラー１１２は、第１及び第２の出力端を有していて、入力された光を２分岐して、第１及び第２の出力端から出力する。入力される光が単一光子の場合は、第１及び第２の出力端からランダムに出力される。

[0022] 第１の出力端から出力された光は、第１の偏光ビームスプリッタ１４１に送られ、第２の出力端から出力された光は、波長板１１４を経て、第２の偏光ビームスプリッタ１４２に送られる。

[0023] 第１の偏光ビームスプリッタ１４１は、第１及び第２の出力端を有している。第１の偏光ビームスプリッタ１４１は、入力された光がＨ偏光の場合は、第１の出力端から出力して第１の単一光子検出部１３１に送り、Ｖ偏光の場合は、第２の出力端から出力して第２の単一光子検出部１３２に送る。また、第１の偏光ビームスプリッタ１４１は、入力された光がＤ（＋）偏光又はＤ（－）偏光の場合は、第１及び第２の出力端からランダムに出力し、第１及び第２の単一光子検出部１３１及び１３２のいずれかでランダムに検出される。

[0024] 波長板１１４は、入力光の偏光状態を、Ｖ偏光又はＨ偏光を、それぞれＤ（＋）偏光又はＤ（－）偏光に変え、Ｄ（＋）偏光又はＤ（－）偏光をＶ偏光又はＨ偏光に変えて、第２の偏光ビームスプリッタ１４２に送る。

[0025] 第２の偏光ビームスプリッタ１４２は、第１及び第２の出力端を有している。第２の偏光ビームスプリッタ１４２は、入力された時点でＨ偏光の場合は、第１の出力端から出力して第３の単一光子検出部１３３に送り、Ｖ偏光の場合は、第２の出力端から出力して第４の単一光子検出部１３４に送る。また、第２の偏光ビームスプリッタ１４２は、入力された時点でＤ（＋）偏光又はＤ（－）偏光の場合は、第１及び第２の出力端からランダムに出力し

、第３及び第４の単一光子検出部１３３及び１３４のいずれかでランダムに検出する。

[0026] 第１～第４の単一光子検出部１３１～１３４は、それぞれ、ＡＰＤで構成され、光子を検出した時刻を第１～第４の受信情報として、生鍵生成回路１５０に送る。

[0027] 生鍵生成回路１５０は、第１の単一光子検出部１３１で光子を検出した場合は、Ｈ偏光、第２の単一光子検出部１３２で検出した場合は、Ｖ偏光、第３の単一光子検出部１３３で検出した場合は、Ｄ（＋）偏光、及び、第４の単一光子検出部１３４で検出した場合は、Ｄ（－）偏光として、これが受信側での生鍵となる。

[0028] その後、秘密鍵蒸留部（図示を省略する。）において、送信者の生鍵と受信者の生鍵から、鍵蒸留プロセスが行われ、送信者と受信者とで最終的な秘密鍵が共有される。ここで、鍵蒸留プロセスには、例えば、シフト鍵生成、誤り訂正、及び、秘密増幅のプロセスが含まれる。

先行技術文献

非特許文献

[0029] 非特許文献1：Ｌａｒｓ Ｌｙｄｅｒｓｅｎ，ｅｔ．ａｌ，”Ｈａｃｋｉｎｇ ｃｏｍｍｅｒｃｉａｌ ｑｕａｎｔｕｍ ｃｒｙｐｔｏｇｒａｐｈｙ ｓｙｓｔｅｍｓ ｂｙ ｔａｉｌｏｒｅｄ ｂｒｉｇｈｔ ｉｌｌｕｍｉｎａｔｉｏｎ”，Ｎａｔｕｒｅ ｐｈｏｔｏｎｉｃｓ，ｖｏｌ．４，Ｏｃｔｏｂｅｒ，ｐｐ．６８６－６８９（２０１０）

発明の概要

発明が解決しようとする課題

[0030] ここで、単一光子検出器としてＧａｔｅｄ Ｇｅｉｇｅｒ ｍｏｄｅ ＡＰＤを用いた場合、動作特性自体がセキュリティ上のループホールとなる可能性があることが知られている。その代表例として、量子鍵配送システムにおけるＢｒｉｇｈｔ Ｉｌｌｕｍｉｎａｔｉｏｎ攻撃がある（例えば、非特

許文献１参照）。

[0031] 図９を参照して説明したアクティブモジュレーション型の量子鍵配送用受信装置に対するＢｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃について、図１１Ａから図１１Ｆを参照して説明する。図１１Ａから図１１Ｆは、Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を説明するための模式図である。

[0032] 盗聴者は送信者からの光子を遮断する。盗聴者は連続光のバックグラウンド成分（P_{CW}）にピーク強度P_{pulse}の光パルスを重畳した光パルスを用意し、受信者に送る。ここで、P_{pulse}は単一光子レベルではなく、例えば数百μWの、レーザ光強度レベルの光である。また、光パルスは、送信者が送信した偏波状態（Ｈ偏光、Ｖ偏光、Ｄ（＋）偏光もしくはＤ（－）偏光）の何れかと同じ偏波状態とする（図１１Ａ）。

[0033] 受信者側では、ＡＰＤにおいて、強い光強度の入力により強いクエンチングが生じる。その結果、ＡＰＤに実際に印加される電圧が低減しブレークダウン電圧以下となる。これにより、ＡＰＤでは雪崩増幅が生じず、通常のリニアＰＤの動作モードになる。

[0034] リニアＰＤとなったＡＰＤの光入力－電気出力特性は線形となる。このとき、入力パルス強度がP_{pulse}であるときの出力電流をI_1とすると、入力光パルス強度がP_{pulse}／２であるときの出力は$I_2 = I_1/2$となる（図１１Ｂ）。

[0035] ＡＰＤでは、出力電流がしきい値I_{th}以上のときは信号検出（ｃｌｉｃｋ）、それ以下の時は信号検出なし（Ｎｏ　ｃｌｉｃｋ）とする。

[0036] ここで、盗聴者が$I_2 < I_{th} < I_1$となるように、光パルス強度P_{pulse}を制御する。このとき、ＡＰＤに入力される入力光パルス強度がP_{pulse}であれば、ＡＰＤは常にｃｌｉｃｋとなり、その半分（$P_{pulse}/2$）であるときは、常にＮｏ　ｃｌｉｃｋとなる。

[0037] 盗聴者の送信基底と、受信者の受信基底が一致しているとき、盗聴者が送った光パルスは一方のポートのみから出力される。例えば、盗聴者がＨ／Ｖ送信基底でＨ偏光の光パルスを送信し、受信基底がＨ／Ｖ受信基底である場

合、偏光ビームスプリッタ１４０の第１の出力端から出力され、第１の単一光子検出部１３１でｃｌｉｃｋとなる（図１１Ｃ）。一方、第２の単一光子検出部１３２では常にＮｏ　ｃｌｉｃｋとなる（図１１Ｄ）。

[0038] 一方、盗聴者の送信基底と、受信者の受信基底が不一致であるとき、盗聴者が送った光パルスは、偏光ビームスプリッタ１４０の第１及び第２の出力端から等分されて出力される。例えば、盗聴者がＨ／Ｖ送信基底でＨ偏光の光パルスを送信し、受信基底がＤｉａｇｏｎａｌ受信基底である場合、偏光ビームスプリッタ１４０の第１及び第２の出力端から出力され、第１及び第２の単一光子検出部１３１及び１３２にP_{pulse}／２の光強度で入力される。この場合、第１及び第２の単一光子検出部１３１及び１３２のいずれでも常にＮｏ　ｃｌｉｃｋとなる（図１１Ｅ及び図１１Ｆ）。

[0039] つまり、盗聴者は、盗聴者の送信基底と受信者の受信基底が一致する場合は、受信者に同じ偏光状態の光でｃｌｉｃｋとなり、盗聴者の送信基底と受信者の受信基底が不一致の場合は、受信者において、常にＮｏ　ｃｌｉｃｋとなるようにできる。

[0040] このような攻撃の結果、盗聴者は受信者の観測結果（生鍵）を自由に制御できるようになる。送信者と受信者がシフト鍵を作る際、受信者の受信基底情報は公開される。このため、盗聴者は受信者のシフト鍵に誤りを生じさせることなく、シフト鍵を取得することができる。

[0041] この場合、秘匿増幅などの後処理を行っても、送信者と受信者が、盗聴者の知らない秘密鍵を共有することは不可能である。

[0042] この攻撃は、盗聴者が生成する光パルスの強度を２倍にすれば、パッシブモジュレーション型の量子鍵配送用受信装置に対しても適用できる。

[0043] この発明は、上述の問題点に鑑みてなされたものである。この発明の目的は、Ｂｒｉｇｈｔ　Ｉｌｌｕｍｉｎａｔｉｏｎ攻撃によるハッキングを排除できる単一光子検出装置、及び、これを用いた量子鍵配送用受信装置を提供することにある。

課題を解決するための手段

[0044] 上述した目的を達成するために、この発明の単一光子検出装置は、ｎ（ｎは２以上の整数）値の乱数を発生させ、乱数値ｉ（ｉは０以上ｎ－１以下の整数）と、乱数値ｉを発生させた時刻を含む乱数ビット値情報を生成する乱数発生器と、乱数値ｉによって定まる透過率T_iで外部からの入力光を強度変調する光強度変調器と、光強度変調器で強度変調された入力光が入力され、単一光子を検出した時刻を受信情報として生成する単一光子検出器と、乱数値ｉにおける、単一光子検出器の光子検出率S_i、乱数発生器で発生する乱数値のうち乱数値ｉが占める割合であるマーク率M_i、及び、透過率T_iから判定値S_i／（$T_i M_i$）を算出し、判定値が予め定めた基準を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路とを備えて構成される。

[0045] また、この発明の他の好適実施形態に係る単一光子検出装置は、ｎ（ｎは２以上の整数）値の乱数を発生させ、乱数値ｉ（ｉは０以上ｎ－１以下の整数）と、乱数値ｉを発生させた時刻を含む乱数ビット値情報を生成する乱数発生器と、乱数値ｉによって定まる電圧値V_iのゲート電圧を生成するゲート電圧生成部と、外部からの入力光をゲート電圧の電圧値V_iで定まる検出効率η_iで検出する単一光子検出器と、乱数値ｉにおける、単一光子検出器の光子検出率S_i、乱数発生器で発生する乱数値のうち乱数値ｉが占める割合であるマーク率M_i、及び、検出効率η_iから判定値S_i／（$\eta_i M_i$）を算出し、判定値が予め定めた基準を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路とを備えて構成される。

[0046] また、この発明の他の好適実施形態に係る単一光子検出装置は、外部からの入力光を２分岐して、第ｊ（ｊは１又は２）の入力光を生成する光回路であって、当該光回路の出力強度の総和に対する第ｊの入力光の強度の割合をT_jとする光分岐部と、それぞれ、第ｊの入力光が入力され、単一光子を検出した時刻を受信情報として生成する第１及び第２の単一光子検出器と、第ｊの単一光子検出器の光子検出率S_j、及び、第ｊの入力光の強度の割合T_jか

ら判定値S_j/T_jを算出し、$S_1/S_2=T_1/T_2$を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路とを備えて構成される。

[0047] また、この発明の他の好適実施形態に係る単一光子検出装置は、外部からの、周期Δｔのパルス光である入力光を２分岐して、第ｊ（ｊは１又は２）の入力光を生成する光回路であって、当該光回路の出力強度の総和に対する第ｊの入力光の強度の割合をT_jとする光分岐部と、第１の入力光及び第２の入力光を合波して、入力合波光を生成する光合波部と、第２の入力光を遅延させて、光合波部で合波される第１の入力光及び第２の入力光の間にΔｔ／２の時間差を与える光遅延器と、入力合波光が入力され、単一光子を検出した時刻を受信情報として生成する単一光子検出器と、幅Δｔ／２の時間スロットに区切ったときの、奇数番目の時間スロットでの単一光子検出器における光子検出数をS_1、偶数番目の時間スロットでの単一光子検出器における光子検出数をS_2として判定値S_j/T_jを算出し、$S_1/S_2=T_1/T_2$を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路とを備えて構成される。

[0048] また、この発明の量子鍵配送用受信装置は、単一光子検出部として、上記の単一光子検出装置を備えて構成され、認証信号が承認を示す場合に生鍵を生成する。

発明の効果

[0049] この発明の単一光子検出装置及び量子鍵配送用受信装置によれば、レーザ光強度の光の入力と、単一光子レベルの光の入力を区別できるので、Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を容易に検知できる。

図面の簡単な説明

[0050] [図1]第１の単一光子検出装置を説明する模式図である。

[図2A]第１の単一光子検出装置の動作を説明する模式図（その１）である。

[図2B]第１の単一光子検出装置の動作を説明する模式図（その２）である。

[図2C]第１の単一光子検出装置の動作を説明する模式図（その３）である。

[図2D]第１の単一光子検出装置の動作を説明する模式図（その４）である。

[図3]第２の単一光子検出装置を説明する模式図である。

[図4]第３の単一光子検出装置を説明する模式図である。

[図5]第４の単一光子検出装置を説明する模式図である。

[図6]第４の単一光子検出装置の動作を説明する模式図である。

[図7]第１の量子鍵配送用受信装置を説明する模式図である。

[図8]第２の量子鍵配送用受信装置を説明する模式図である。

[図9]アクティブモジュレーション型の量子鍵配送用受信装置を説明する模式図である。

[図10]パッシブモジュレーション型の量子鍵配送用受信装置を説明する模式図である。

[図11A]Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を説明する模式図（その１）である。

[図11B]Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を説明する模式図（その２）である。

[図11C]Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を説明する模式図（その３）である。

[図11D]Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を説明する模式図（その４）である。

[図11E]Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を説明する模式図（その５）である。

[図11F]Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を説明する模式図（その６）である。

発明を実施するための形態

[0051] 以下、図を参照して、この発明の実施の形態について説明するが、各構成要素の形状、大きさ及び配置関係については、この発明が理解できる程度に概略的に示したものに過ぎない。また、以下、この発明の好適な構成例につき説明するが、単なる好適例にすぎない。従って、この発明は以下の実施の

形態に限定されるものではなく、この発明の構成の範囲を逸脱せずにこの発明の効果を達成できる多くの変更又は変形を行うことができる。

[0052] （第１の単一光子検出装置の構成）

図１を参照して、この発明の第１の実施形態に係る単一光子検出装置（以下、第１の単一光子検出装置とも称する。）を説明する。図１は、第１の単一光子検出装置を説明する模式図である。

[0053] 第１の単一光子検出装置は、乱数発生器２０、光強度変調器１０、単一光子検出器３０、及び、計数処理回路４０を備えて構成される。

[0054] 乱数発生器２０は、ｎ（ｎは２以上の整数）値の乱数を発生させ、乱数値ｉ（ｉは０以上ｎ－１以下の整数）と、この乱数値ｉを発生させた時刻を含む乱数ビット値情報を生成する。乱数ビット値情報は、光強度変調器１０と計数処理回路４０に送られる。

[0055] 光強度変調器１０は、乱数値ｉによって定まる透過率T_iで外部からの入力光を強度変調する。

[0056] 外部からの入力光は、光強度変調器１０で強度変調されたのち、単一光子検出器３０に送られる。単一光子検出器３０は、単一光子を検出した時刻を受信情報として生成する。この受信情報は、計数処理回路４０に送られる。

[0057] 計数処理回路４０は、乱数値ｉにおける、単一光子検出器３０での光子検出率S_i、乱数発生器２０で発生する乱数値のうち乱数値ｉが占める割合（マーク率）M_i、及び、光強度変調器１０の透過率T_iから、判定値S_i／（T_i M_i）を算出する。この判定値が予め定めた基準を満たしている場合、例えば判定値がある一定値に等しい場合、承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する。

[0058] （第１の単一光子検出装置の動作）

ｎが２の場合、すなわち、乱数発生器２０が２値の乱数を発生する場合の、第１の単一光子検出装置の動作を説明する。

[0059] この例では、乱数発生器２０は、乱数値「０」又は「１」を、等しい割合で生成する。すなわちマーク率M_0及びM_1をともに５０％とする。また、T_0

＝０．５、T_1＝１とする。

[0060] Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃の本質は、盗聴者が強い光パルスを送って、ピーク光強度P_{pulse}の光パルスが単一光子検出器に入力されたら単一光子検出器は常に光子検出（ｃｌｉｃｋ）となり、ピーク光強度がP_{pulse}／２の光パルスが単一光子検出器に入力されたら単一光子検出器は常に光子検出無（Ｎｏ　ｃｌｉｃｋ）となるように受信者を動作させることにある。これにより、Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃では、盗聴者は受信者の受信結果を制御する。

[0061] このとき、単一光子検出器３０には平均光子数が１よりも非常に大きい、レーザ光レベルの光が入力されている。従って、Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃によるハッキングを排除するには、受信者が持つ単一光子検出器３０に入力される光が単一光子レベルの極微弱光であるか否かを受信者が探知できれば良い。

[0062] 一般に、単一光子検出器の内部量子効率は１００％よりも小さく、例えば、ＩｎＧａＡｓ／ＩｎＰ－ＡＰＤの場合で、６０～７０％程度である。実際のデバイスとして用いる場合は、光入力系の光学損失等があるため、検出効率はせいぜい４０％程度である。この程度の検出効率の単一光子検出器では、複数回の検出により期待値を知ることはできるが、入力された光子の数を知ることはできない。従って、一般的には、最終的な出力電流にしきい値I_{th}を設けて、出力電流がしきい値I_{th}以上の時はｃｌｉｃｋ、それ以下の時はＮｏ　ｃｌｉｃｋとする、いわゆる、スレショルド型検出器として単一光子検出器を動作させる。

[0063] ＡＰＤでの信号検出率Ｓは以下の式（１）で与えられる。

[0064]

$$S = 1 - e^{-\mu\eta} \qquad (1)$$

ここで、μは入力光の平均光子数、ηはμが十分少ないときの検出効率で、一般的に単一光子検出器の検出効率として認識されている値である。ここでは入力光の光子数分布はポアソン分布と仮定している。

[0065] 上記式（１）は、μが十分小さいときには、Ｓ＝$\mu\eta$となり、μに比例した結果となる。一方、μがおおきくなるとＳは飽和していき、１に漸近していく。すなわち、Ｓがμに比例している場合、単一光子検出器に入力されている光は単一光子レベルの光であり、Ｓがμに比例せず飽和傾向にある場合、単一光子検出器に入力されている光はμ＞＞１の強い光であるといえる。

[0066] 光強度変調器１０は、乱数発生器２０が生成する乱数の乱数値に応じて透過率をランダムに変調する。この結果、光強度変調器１０に入力される光の平均光子数がμであるとき、単一光子検出器３０に入力される光の平均光子数はμT_0、μT_1になる。

[0067] μ＜＜１、すなわち、入力される光が単一光子レベルであるとき、光強度変調器の透過率T_0と、このときの光子検出率S_0、及び、光変調器の透過率T_1と、このときの光子検出率S_1の間には、$S_0/S_1=T_0/T_1$の関係が成立する。

[0068] 一方、μ＞＞１であるとき、$S_0/S_1=T_0/T_1$の関係が成立しなくなる。この例のように、$T_0<T_1$であるとき、高い透過率T_1に設定されたときの光子検出率S_1の飽和がより顕著になる。このため、一般に、$S_0/S_1>T_0/T_1$になる。

[0069] 図２Ａから図２Ｄは、上記の式（１）を用いて、μを変化させたときのS_1、S_0/S_1を計算した結果を示す図である。ここでは、T_0＝０．５、T_1＝１としている。図２Ａから図２Ｄでは横軸に平均光子数μを取って示し、左軸にS_1、右軸にS_0/S_1を取って示している。図２Ａ、図２Ｂ、図２Ｃ及び図２Ｄは、それぞれ検出効率ηが５％、１０％、２０％及び４０％の場合を示している。また、簡単のために、光学系での損失や単一光子検出器のクエンチング効果等は無視している。

[0070] 図２Ａから図２Ｄに示すように、μ＜＜１であるとき、S_0/S_1＝０．５（＝T_0/T_1）が成り立つのに対し、μを増加させるとS_0/S_1は増加していく。$\mu\eta$＝１のとき、概ね、S_0/S_1＝０．６２であり、μ＜＜１のときに比べ約１．２倍に増加する。すなわち、第１の単一光子検出装置では、S_0

／S_1を計算することで、入力された光が単一光子レベルであるか否かを判別できる。

[0071] 図９を参照して説明した、従来のアクティブモジュレーション型の量子鍵配送用受信装置において、第１及び第２の単一光子検出部に第１の単一光子検出装置を用いる場合を考える。

[0072] 先ず、送信者の送信基底と、受信者の受信基底が一致している場合を説明する。透過率がT_1（＝１）であるとき、一方の、例えば第１の単一光子検出部に入力される光パルスの強度はP_{pulse}であるので、第１の単一光子検出部の単一光子検出器は常にｃｌｉｃｋとなる。一方、透過率がT_0（＝０．５）であるとき、第１の単一光子検出器に入力される光パルスの強度はP_{pulse}／２であるので、第１の単一光子検出部の単一光子検出器は常にＮｏ ｃｌｉｃｋとなる。すなわち、送信者の送信基底と、受信者の受信基底が一致している場合、S_0／S_1＝０となる。このため、受信者は、Ｂｒｉｇｈｔ ｌｌｕｍｉｎａｔｉｏｎ攻撃を容易に探知できる。

[0073] T_0（＝０．５）であるときも単一光子検出器で常にｃｌｉｃｋとなるように、盗聴者が光強度を２倍にしたとする。しかし、このとき、S_0／S_1＝１となるため、やはり、受信者はＢｒｉｇｈｔ ｌｌｌｕｍｉｎａｔｉｏｎ攻撃を探知できる。また、盗聴者の送信基底と受信者の受信基底が不一致の場合、第１及び第２の単一光子検出器の両者にピーク光強度P_{pulse}の光パルスが入力され、ともにｃｌｉｃｋとなる。これは、シフト鍵に誤りを生じさせてしまうため、Ｂｒｉｇｈｔ ｌｌｕｍｉｎａｔｉｏｎ攻撃を成功させることはできない。

[0074] 量子鍵配送用受信装置の単一光子検出部として、第１の単一光子検出装置を用いると、盗聴者が乱数発生器の乱数ビット値情報を知らないとすれば、光強度を調整することができないため、盗聴者はS_0／S_1を受信者にとって適正な値に制御することができない。従って、受信者はＢｒｉｇｈｔ ｌｌｕｍｉｎａｔｉｏｎ攻撃を容易に探知できる。

[0075] なお、ここでは、光強度変調器の透過率としてT_0、T_1を、それぞれ５０

％の割合で生じさせるとしたが、この割合は５０％でなくてもよい。

[0076] 例えば、全体のうち、T_1が占める割合（マーク率）をＭとすれば、$\mu \ll 1$であるとき、$S_0/S_1 = \{(1-M) \times T_0\} / (M \times T_1)$の関係を満たすか否かを判別条件に用いればよい。

[0077] また、光強度変調器の透過率を３通り以上にしてもよい。判定条件を一般化すると、光強度変調器の透過率T_iのときのマーク率をM_iとした場合、$S_i / (M_i \times T_i)$が一定値という条件を満たせばよい。

[0078] 光強度変調器の透過率がT_0、T_1の２通りであり、それぞれ５０％の割合の場合は、$S_0/(0.5 \times T_0) = S_1/(0.5 \times T_1)$＝一定値となり、この場合、$S_0/S_1 = T_0/T_1$となる。また、光強度変調器の透過率が$T_0$、$T_1$の２通りであり、$T_1$が占める割合がＭの場合、$M_0 = 1 - M$及び$M_1 = M$であるので、$S_0/\{(1-M) \times T_0\} = S_1/(M \times T_1)$＝一定値となる。この場合、$S_0/S_1 = \{(1-M) \times T_0\} / (M \times T_1)$となる。

[0079] なお、光強度変調器の透過率を３通り以上にすると、T_iとS_iが比例関係にあるか否かを判別することができ、入力光が単一光子レベルであるか否かをより厳密に判断することができる。

[0080] （第２の単一光子検出装置の構成）

図３を参照して、この発明の第２の実施形態に係る単一光子検出装置（以下、第２の単一光子検出装置とも称する。）を説明する。図３は、第２の単一光子検出装置を説明する模式図である。

[0081] 第２の単一光子検出装置は、乱数発生器２０、ゲート電圧生成部５０、単一光子検出器３０、及び、計数処理回路４０を備えて構成される。

[0082] 乱数発生器２０は、ｎ（ｎは２以上の整数）値の乱数を発生させ、乱数値ｉ（ｉは０以上ｎ－１以下の整数）と、この乱数値ｉを発生させた時刻を含む乱数ビット値情報を生成する。乱数ビット値情報は、ゲート電圧生成部５０と計数処理回路４０に送られる。

[0083] ゲート電圧生成部５０は、乱数値ｉによって定まる電圧値V_iのゲート電圧を生成する。ゲート電圧生成部５０は、変調電圧源５２と定常電圧源５４を

備えて構成される。変調電圧源５２は、乱数値ｉによって定まる変調電圧を生成し、定常電圧源５４は、定常電圧を生成する。ゲート電圧生成部５０は、変調電圧と定常電圧を加算してゲート電圧を生成する。このように、ゲート電圧は、乱数発生器２０の乱数値に基づいて変調される。ゲート電圧は、単一光子検出器３０に送られる。

[0084] ここで、変調電圧源５２が発生する変調電圧が単一光子検出器３０でブレークダウン電圧を超えるほど十分大きな値であるときは、定常電圧源５４を省略し、変調電圧をそのままゲート電圧として用いてもよい。

[0085] 外部からの入力光は、単一光子検出器３０に送られる。単一光子検出器３０は、単一光子を検出した時刻を受信情報として生成する。この受信情報は、計数処理回路４０に送られる。Ｇａｔｅｄ Ｇｅｉｇｅｒ ｍｏｄｅ ＡＰＤの検出効率ηは、印加電圧によって変化することが知られている。従って、ＡＰＤに印加されるゲート電圧V_iが異なると、検出効率η_iも異なる。

[0086] 計数処理回路４０は、乱数値ｉにおける、単一光子検出器３０の光子検出率S_i、乱数発生器２０で発生する乱数値のうち乱数値ｉが占める割合（マーク率）M_i、及び、検出効率η_iから判定値$S_i/(\eta_i M_i)$を算出する。この判定値が予め定めた基準を満たしている場合、例えば判定値がある一定値に等しい場合、承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する。

[0087] （第２の単一光子検出装置の動作）

ｎが２の場合、すなわち、乱数発生器が２値の乱数を発生する場合の、第２の単一光子検出装置の動作を説明する。

[0088] この例では、乱数発生器２０は、乱数値「０」又は「１」を、等しい割合で生成する。すなわちマーク率M_0及びM_1をともに５０％とする。

[0089] 入力光の平均光子数をμとすると、$\mu \ll 1$であるとき、ＡＰＤに印加されるゲート電圧がV_1のときの信号検出率S_1は$\mu\eta_1$で与えられ、ゲート電圧がV_0のときの信号検出率S_0は$\mu\eta_0$で与えられる。このため、$S_0/S_1=\eta_0/\eta_1$の関係が成立する。

[0090] 一方、$\mu >> 1$であるときは、$S_0/S_1=\eta_0/\eta_1$の関係が成立しない。すなわち、S_0/S_1を計算することで、入力光が単一光子レベルであるか否かを判別できる。

[0091] なお、第２の単一光子検出装置においても、ｎを３以上に多値化して、$S_i/(M_i\times\eta_i)$が一定であるか否かで判別することにより、判別条件をより厳密化してもよい。また、乱数発生器のマーク率を任意に設定してもよい。

[0092] この、第２の単一光子検出装置によれば、第１の単一光子検出装置と同様にＢｒｉｇｈｔ　Ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を探知することができる。また、光強度変調器が不要なため、第２の単一光子検出装置は、第１の単一光子検出装置よりも装置を小型化することができる。

[0093] （第３の単一光子検出装置の構成）

図４を参照して、この発明の第３の実施形態に係る単一光子検出装置（以下、第３の単一光子検出装置とも称する。）を説明する。図４は、第３の単一光子検出装置を説明する模式図である。

[0094] 第３の単一光子検出装置は、光分岐部６０、第１の単一光子検出器３１、第２の単一光子検出器３２、及び、計数処理回路４０を備えて構成される。

[0095] 光分岐部６０は、外部からの入力光を２分岐して、第１及び第２の入力光を生成する。また、外部からの入力光に対して第１及び第２の入力光の強度の割合をそれぞれT_1、T_2とする。

[0096] 光分岐部６０は、例えば、ハーフミラー、第１の光減衰器、第２の光減衰器を備えて構成される。この場合、外部からの入力光はハーフミラーで２分岐されて、一方は透過率T_1の第１の光減衰器を経て、第１の入力光として出力され、他方は透過率T_2の第２の光減衰器を経て、第２の入力光として出力される。第１及び第２の入力光は、それぞれ、第１及び第２の単一光子検出装置に送られる。なお、$T_1=1$の場合は、第１の光減衰器を備えない構成にすることができる。

[0097] また、光分岐部６０として、分岐比が$T_1:T_2$の任意好適な光分岐回路を用いてもよい。

[0098] 第１の単一光子検出器３１は、入力された第１の入力光について、単一光子を検出した時刻を第１の受信情報として生成する。また、第２の単一光子検出器３２は、入力された第２の入力光について、単一光子を検出した時刻を第２の受信情報として生成する。

[0099] 計数処理回路４０は、第１の受信情報及び第２の受信情報に基づいて、第１の単一光子検出器の光子検出率S_1、第２の単一光子検出器の光子検出率S_2、第１の入力光の強度の割合T_1、及び第２の入力光の強度の割合T_2から、$S_1／S_2＝T_1／T_2$を満たしているか否かを判定する。計数処理回路４０は、$S_1／S_2＝T_1／T_2$を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する。

[0100] また、第３の単一光子検出装置を、量子鍵配送用受信装置の単一光子検出部に用いる場合は、第１の受信情報及び第２の受信情報の和集合を受信情報として生成し、生鍵生成回路に送ればよい。

[0101] 第１の単一光子検出装置は、１つの単一光子検出器を用いてT_1及びT_2に対する検出を順次行うのに対し、第３の単一光子検出装置では、入力光を２分岐して、２つの単一光子検出器を用いて、それぞれ、T_1及びT_2に対する検出を行う。

[0102] 第３の単一光子検出装置では、乱数発生器を備えておらず、ハーフミラーなど受動素子で構成される光分岐部の動作により自然乱数的に透過率を選択できるので、より安全なシステム構成を実現できる。

[0103] （第４の単一光子検出装置の構成）

図５を参照して、この発明の第４の実施形態に係る単一光子検出装置（以下、第４の単一光子検出装置とも称する。）を説明する。図５は、第４の単一光子検出装置を説明する模式図である。

[0104] 第４の単一光子検出装置は、光分岐部６０、単一光子検出器３０、光遅延器７０、光合波部８０、及び、計数処理回路４０を備えて構成される。

[0105] 光分岐部６０は、外部からの周期Δｔのパルス状の入力光を２分岐して、第１及び第２の入力光を生成する。また、外部からの入力光に対して第１及

び第２の入力光の強度の割合をそれぞれT_1、T_2とする。

[0106] 光分岐部６０は、第３の単一光子検出器の光分岐部と同様に構成することができるので、重複する説明を省略する。

[0107] 第１の入力光は光合波部８０に送られ、第２の入力光は光遅延器７０で所定の遅延を受けた後、光合波部８０に送られる。光合波部８０は、第１の入力光及び第２の入力光を合波して、入力合波光を生成する。光合波部８０は、例えば、ハーフミラーで構成される。なお、光遅延器７０は、光合波部８０で合波される第１の入力光及び第２の入力光の間にΔｔ／２の時間差を与えるように、第２の入力光に遅延を与える。

[0108] 単一光子検出器３０は、入力合波光が入力され、単一光子を検出した時刻を受信情報として生成する。

[0109] 計数処理回路４０は、幅Δｔ／２の時間スロットに区切ったときの、奇数番目の時間スロットでの単一光子検出器における光子検出数をS_1、偶数番目の時間スロットでの単一光子検出器における光子検出数をS_2として、$S_1/S_2=T_1/T_2$を満たしているか否かを判定する。満たしている場合、承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する。

[0110] 第４の単一光子検出装置では、１つの単一光子検出器を備える構成で第３の単一光子検出器と同様の効果を達成できる。

[0111] （第４の単一光子検出装置の動作）

図６を参照して、第４の単一光子検出装置の動作を説明する。図６は、第４の単一光子検出装置の動作を説明する模式図である。

[0112] 第４の単一光子検出装置では、単一光子検出器３０に印加されるゲート電圧の周期はΔｔ／２である。（図６（Ａ））。

[0113] また、入力光は周期Δｔのパルス状であり、光遅延器７０により、光合波部８０で合波される際の第１の入力光（図６（Ｂ））及び第２の入力光（図６（Ｃ））の間にΔｔ／２の時間差が与えられる。

[0114] 計数処理回路４０は、幅Δｔ／２の時間スロットに区切ったとき（図６（

Ｄ））の、奇数番目の時間スロットでの単一光子検出器３０における光子検出数を$Ｓ_{1}$、偶数番目の時間スロットでの単一光子検出器３０における光子検出数を$Ｓ_{2}$として、$Ｓ_{1}／Ｓ_{2}＝Ｔ_{1}／Ｔ_{2}$を満たしているか否かを判定する。満たしている場合、承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する。

[0115] （第１の量子鍵配送用受信装置）

図７を参照して、第１の量子鍵配送用受信装置について説明する。図７は、第１の量子鍵配送用受信装置の模式図である。

[0116] 第１の量子鍵配送用受信装置は、光強度変調器１０、乱数発生器２０、偏波変調用乱数発生器１２０、偏波変調器１１０、偏光ビームスプリッタ１４０、第１の単一光子検出部１３１、第２の単一光子検出部１３２、計数処理回路４０、及び、生鍵生成回路１５０を備えて構成されている。

[0117] 第１の量子鍵配送用受信装置は、従来のアクティブモジュレーション型の量子鍵配送用受信装置に、第１の単一光子検出装置の光強度変調器、乱数発生器及び計数処理回路を組み込んで構成される。従って、以下の説明において、従来のアクティブモジュレーション型の量子鍵配送用受信装置及び第１の単一光子検出装置と重複する説明を省略することがある。

[0118] 入力光は、乱数発生器２０が生成する乱数により、透過率をランダムに変化させる光強度変調器１０を経て、偏波変調用乱数発生器１２０で駆動された偏波変調器１１０に入力される。

[0119] 偏波変調用乱数発生器１２０は、２値の偏波変調器用乱数を発生させ、偏波乱数値ｋ（ｋは０又は１）と、偏波乱数値ｋを発生させた時刻を含む基底乱数情報を生成する。基底乱数情報は、偏波変調器１１０及び生鍵生成回路１５０に送られる。

[0120] 受信者が備える偏波変調器１１０は、偏波変調用乱数発生器１２０が発生した乱数の偏波乱数値ｋに応じて、通過する光の偏波状態を変更する。

[0121] 偏波乱数値が「０」であるとき、偏波変調器１１０は、入力光の偏光状態を変えない。この場合、受信者は、Ｈ／Ｖ受信基底を選択したものとする。

[0122] 偏波乱数値が「１」であるとき、偏波変調器１１０は、入力光の偏光状態を、Ｖ偏光又はＨ偏光を、それぞれＤ（＋）偏光又はＤ（－）偏光に変え、Ｄ（＋）偏光又はＤ（－）偏光をＶ偏光又はＨ偏光に変える。この場合、受信者は、Ｄｉａｇｏｎａｌ受信基底を選択したものとする。

[0123] 偏光ビームスプリッタ１４０は、第１及び第２の出力端を有している。偏光ビームスプリッタは、入力された光がＨ偏光の場合は、第１の出力端から出力して第１の単一光子検出部１３１に送り、Ｖ偏光の場合は、第２の出力端から出力して第２の単一光子検出部１３２に送る。また、偏光ビームスプリッタ１４０は、入力された光がＤ（＋）偏光又はＤ（－）偏光の場合は、第１及び第２の出力端からランダムに出力する。

[0124] 第１及び第２の単一光子検出部１３１及び１３２は、それぞれ、いわゆるゲート動作型ガイガーモードＡＰＤで構成され、光子を検出した時刻を第１及び第２の受信情報として、生鍵生成回路１５０に送る。

[0125] 生鍵生成回路１５０は、第１の単一光子検出部１３１で光子を検出した場合は、自らのビット値を「０」とし、第２の単一光子検出器で光子を検出した場合は、自らのビット値を「１」とする。また、偏波乱数値が「０」の場合は、Ｈ／Ｖ受信基底が選択され、「１」の場合は、Ｄｉａｇｏｎａｌ受信基底が選択されたものとする。生鍵生成回路１５０は、第１及び第２の単一光子検出器のいずれかでヒットした時刻での偏波乱数値から、受信者が受信した光の偏光状態が、Ｈ偏光、Ｖ偏光、Ｄ（－）偏光、Ｄ（＋）偏光のいずれかであるかを得ることができ、これが受信側での生鍵となる。

[0126] その後、秘密鍵蒸留部（図示を省略する。）において、送信者の生鍵と受信者の生鍵から、鍵蒸留プロセスが行われ、送信者と受信者とで最終的な秘密鍵が共有される。ここで、鍵蒸留プロセスには、例えば、シフト鍵生成、誤り訂正、及び、秘密増幅のプロセスが含まれる。

[0127] ここで、第１の量子鍵配送用受信装置では、計数処理回路４０が、乱数発生器２０から送られた乱数ビット値情報と、第１及び第２の単一光子検出部１３１及び１３２から送られた第１及び第２の受信情報を用いて、認証信号

を生成する。この認証信号は、計数処理回路４０が第１及び第２の単一光子検出部１３１及び１３２に入力される光が単一光子レベルであるか否かを判定し、単一光子レベルである場合は承認を示し、そうでない場合は否認を示す。認証信号は生鍵生成回路１５０に送られる。

[0128] 生鍵生成回路１５０は、認証信号が承認を示す場合は生鍵を生成し、否認を示す場合は、生鍵の生成を行わない。

[0129] このようにして、第１の量子鍵配送用受信装置では、Ｂｒｉｇｈｔ　Ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を排除する。

[0130] なお、計数処理回路４０で認証情報を生成するのに用いられる受信情報と、生鍵生成回路１５０で生鍵を生成するのに用いられる受信情報とは同じものを用いることができる。

[0131] （第２の量子鍵配送用受信装置）

図８を参照して、第２の量子鍵配送用受信装置について説明する。図８は、第２の量子鍵配送用受信装置の模式図である。

[0132] 第２の量子鍵配送用受信装置は、光強度変調器１０、乱数発生器２０、ハーフミラー１１２、波長板１１４、第１及び第２の偏光ビームスプリッタ１４１及び１４２、第１～第４の単一光子検出部１３１～１３４、計数処理回路４０、並びに、生鍵生成回路１５０を備えて構成されている。

[0133] 第２の量子鍵配送用受信装置は、従来のパッシブモジュレーション型の量子鍵配送用受信装置に、第１の単一光子検出装置の光強度変調器、乱数発生器及び計数処理回路を組み込んで構成される。従って、以下の説明において、従来のパッシブモジュレーション型の量子鍵配送用受信装置及び第１の単一光子検出装置と重複する説明を省略することがある。

[0134] 入力光は、乱数発生器２０が生成する乱数により、透過率をランダムに変化させる光強度変調器１０を経て、ハーフミラー１１２に入力される。

[0135] ハーフミラー１１２は、第１及び第２の出力端を有していて、入力された光を２分岐して、第１及び第２の出力端から出力する。入力される光が単一光子の場合は、第１及び第２の出力端からランダムに出力される。

[0136] 第１の出力端から出力された光は、第１の偏光ビームスプリッタ１４１に送られ、第２の出力端から出力された光は、波長板１１４を経て、第２の偏光ビームスプリッタ１４２に送られる。

[0137] 第１の偏光ビームスプリッタ１４１は、第１及び第２の出力端を有している。第１の偏光ビームスプリッタ１４１は、入力された光がＨ偏光の場合は、第１の出力端から出力して第１の単一光子検出部１３１に送り、Ｖ偏光の場合は、第２の出力端から出力して第２の単一光子検出部１３２に送る。また、第１の偏光ビームスプリッタ１４１は、入力された光がＤ（＋）偏光又はＤ（－）偏光の場合は、第１及び第２の出力端からランダムに出力し、第１及び第２の単一光子検出部１３１及び１３２のいずれかでランダムに検出される。

[0138] 波長板１１４は、入力光の偏光状態を、Ｖ偏光又はＨ偏光を、それぞれＤ（＋）偏光又はＤ（－）偏光に変え、Ｄ（＋）偏光又はＤ（－）偏光をＶ偏光又はＨ偏光に変えて、第２の偏光ビームスプリッタに送る。

[0139] 第２の偏光ビームスプリッタ１４２は、第１及び第２の出力端を有している。第２の偏光ビームスプリッタ１４２は、入力された時点でＨ偏光の場合は、第１の出力端から出力して第３の単一光子検出部１３３に送り、Ｖ偏光の場合は、第２の出力端から出力して第４の単一光子検出部１３４に送る。また、第２の偏光ビームスプリッタ１４２は、入力された時点でＤ（＋）偏光又はＤ（－）偏光の場合は、第１及び第２の出力端からランダムに出力し、第３及び第４の単一光子検出部１３３及び１３４のいずれかでランダムに検出する。

[0140] 第１～第４の単一光子検出部１３１～１３４は、それぞれ、ＡＰＤで構成され、光子を検出した時刻を第１～第４の受信情報として、生鍵生成回路１５０に送る。

[0141] 生鍵生成回路１５０は、第１の単一光子検出部１３１で光子を検出した場合は、Ｈ偏光、第２の単一光子検出部１３２で検出した場合は、Ｖ偏光、第３の単一光子検出部１３３で検出した場合は、Ｄ（＋）偏光、及び、第４の

単一光子検出部１３４で検出した場合は、Ｄ（－）偏光として、検出した偏光が受信側での生鍵となる。

[0142] その後、秘密鍵蒸留部（図示を省略する。）において、送信者の生鍵と受信者の生鍵から、鍵蒸留プロセスが行われ、送信者と受信者とで最終的な秘密鍵が共有される。ここで、鍵蒸留プロセスには、例えば、シフト鍵生成、誤り訂正、及び、秘密増幅のプロセスが含まれる。

[0143] ここで、第２の量子鍵配送用受信装置では、計数処理回路４０が、乱数発生器２０から送られた乱数ビット値情報と、第１～第４の単一光子検出部１３１～１３４から送られた第１～第４の受信情報を用いて、認証信号を生成する。この認証信号は、計数処理回路４０が、第１～第４の単一光子検出部１３１～１３４に入力される光が単一光子レベルであるか否かを判定し、単一光子レベルである場合は承認を示し、そうでない場合は否認を示す。認証信号は生鍵生成回路１５０に送られる。

[0144] 生鍵生成回路１５０は、認証信号が承認を示す場合は生鍵を生成し、否認を示す場合は、生鍵の生成を行わない。

[0145] このようにして、第２の量子鍵配送用受信装置では、Ｂｒｉｇｈｔ　Ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を排除する。

[0146] なお、計数処理回路４０で認証情報を生成するのに用いられる受信情報と、生鍵生成回路１５０で生鍵を生成するのに用いられる受信情報とは同じものを用いることができる。

[0147] （量子鍵配送用受信装置の他の構成例）

Ｂｒｉｇｈｔ　Ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を排除可能な量子鍵配送用受信装置は、上述の第１及び第２の量子鍵配送用受信装置の構成に限定されない。

[0148] 例えば、光強度変調器１０及び乱数発生器２０に換えて、第４の単一光子検出装置の光分岐部６０、光遅延器７０、及び、光合波部８０を設けてもよい。

[0149] また、図９を参照して説明したアクティブモジュレーション型の量子鍵配

送用受信装置の第１及び第２の単一光子検出部に、上述の第１～第４の単一光子検出装置を用いてもよいし、図１０を参照して説明したパッシブモジュレーション型の量子鍵配送用受信装置の第１～第４の単一光子検出部に、上述の第１～第４の単一光子検出装置を用いてもよい。

[0150] ここで、いずれか１つの単一光子検出部に、第１～４の単一光子検出装置のいずれかを設ければ、Ｂｒｉｇｈｔ　ｉｌｌｕｍｉｎａｔｉｏｎ攻撃を探知できるが、単一光子検出部に入力される光の対称性や、複数の単一光子検出部での認証による高い安全性を考えると、全ての単一光子検出部に同じ単一光子検出装置を用いるのが良い。

[0151] また、単一光子検出部の全てに第２の単一光子検出装置を用いる場合、１つの乱数発生器及びゲート電圧生成部を、全ての単一光子検出部で共有してもよい。

符号の説明

[0152]
１０　光強度変調器
２０　乱数発生器
３０、３１、３２　単一光子検出器
４０　計数処理回路
５０　ゲート電圧生成部
５２　変調電圧源
５４　定常電圧源
６０　光分岐部
７０　光遅延器
８０　光合波部
１１０　偏波変調器
１２０　偏波変調用乱数発生器
１３１、１３２、１３３、１３４　単一光子検出部
１４０、１４１、１４２　偏光ビームスプリッタ
１５０　生鍵生成回路

請求の範囲

[請求項1] ｎ（ｎは２以上の整数）値の乱数を発生させ、乱数値ｉ（ｉは０以上ｎ－１以下の整数）と、該乱数値ｉを発生させた時刻を含む乱数ビット値情報を生成する乱数発生器と、

前記乱数値ｉによって定まる透過率T_iで外部からの入力光を強度変調する光強度変調器と、

前記光強度変調器で強度変調された入力光が入力され、単一光子を検出した時刻を受信情報として生成する単一光子検出器と、

前記乱数値ｉにおける、前記単一光子検出器の光子検出率S_i、前記乱数発生器で発生する乱数値のうち前記乱数値ｉが占める割合であるマーク率M_i、及び、前記透過率T_iから判定値S_i／（$T_i M_i$）を算出し、該判定値が予め定めた基準を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路と

を備える、単一光子検出装置。

[請求項2] ｎ（ｎは２以上の整数）値の乱数を発生させ、乱数値ｉ（ｉは０以上ｎ－１以下の整数）と、該乱数値ｉを発生させた時刻を含む乱数ビット値情報を生成する乱数発生器と、

前記乱数値ｉによって定まる電圧値V_iのゲート電圧を生成するゲート電圧生成部と、

外部からの入力光を前記ゲート電圧の電圧値V_iで定まる検出効率η_iで検出する単一光子検出器と、

前記乱数値ｉにおける、前記単一光子検出器の光子検出率S_i、前記乱数発生器で発生する乱数値のうち前記乱数値ｉが占める割合であるマーク率M_i、及び、前記検出効率η_iから判定値S_i／（$\eta_i M_i$）を算出し、該判定値が予め定めた基準を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路と

を備える、単一光子検出装置。

[請求項3] 外部からの入力光を２分岐して、第ｊ（ｊは１又は２）の入力光を生成する光回路であって、当該光回路の出力強度の総和に対する第ｊの入力光の強度の割合をT_jとする光分岐部と、

それぞれ、第ｊの入力光が入力され、単一光子を検出した時刻を受信情報として生成する第１及び第２の単一光子検出器と、

前記第ｊの単一光子検出器の光子検出率S_j、及び、前記第ｊの入力光の強度の割合T_jから判定値S_j/T_jを算出し、$S_1/S_2=T_1/T_2$を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路と

を備える、単一光子検出装置。

[請求項4] 外部からの、周期Δｔのパルス光である入力光を２分岐して、第ｊ（ｊは１又は２）の入力光を生成する光回路であって、当該光回路の出力強度の総和に対する第ｊの入力光の強度の割合をT_jとする光分岐部と、

第１の入力光及び第２の入力光を合波して、入力合波光を生成する光合波部と、

前記第２の入力光を遅延させて、前記光合波部で合波される前記第１の入力光及び前記第２の入力光の間にΔｔ／２の時間差を与える光遅延器と、

前記入力合波光が入力され、単一光子を検出した時刻を受信情報として生成する単一光子検出器と、

幅Δｔ／２の時間スロットに区切ったときの、奇数番目の時間スロットでの前記単一光子検出器における光子検出数をS_1、偶数番目の時間スロットでの前記単一光子検出器における光子検出数をS_2として判定値S_j/T_jを算出し、$S_1/S_2=T_1/T_2$を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路と

を備える、単一光子検出装置。

[請求項5] ２値の偏波変調器用乱数を発生させ、乱数値ｋ（ｋは０又は１）と、該乱数値ｋを発生させた時刻を含む基底乱数情報を生成する偏波変調用乱数発生器と、

前記偏波変調用乱数発生器が発生した乱数の偏波乱数値ｋに応じて、通過する光の偏波状態を変更する偏波変調器と、

第１及び第２の出力端を有し、前記偏波変調器を通過した光が入力され、該光の偏波状態に応じて、第１及び第２の出力端から出力する偏光ビームスプリッタと、

前記偏光ビームスプリッタの第１の出力端から出力された光が入力され、単一光子を検出した時刻を第１の受信情報として生成する第１の単一光子検出部と、

前記偏光ビームスプリッタの第２の出力端から出力された光が入力され、単一光子を検出した時刻を第２の受信情報として生成する第２の単一光子検出部と、

前記第１及び第２の受信情報と、前記基底乱数情報に基づいて、生鍵を生成する生鍵生成回路と

を備え、

前記第１及び第２の単一光子検出部のいずれか一方又は双方が、請求項１に記載する単一光子検出装置であり、

前記生鍵生成回路は、前記計数処理回路が生成する認証信号が承認を示すときに生鍵を生成する、

量子鍵配送用受信装置。

[請求項6] ハーフミラーと、

前記ハーフミラーで２分岐された一方が入力され、第１及び第２の出力端を有し、前記ハーフミラーで２分岐された一方の光が入力され、該光の偏波状態に応じて、第１及び第２の出力端から出力する第１の偏光ビームスプリッタと、

前記ハーフミラーで２分岐された他方が入力される波長板と、

前記波長板を通過した光が入力され、該光の偏波状態に応じて、第３及び第４の出力端から出力する第２の偏光ビームスプリッタと、

それぞれ、前記第ｍ（ｍは１以上４以下の整数）の出力端から出力された光が入力され、単一光子を検出した時刻を第ｍの受信情報として生成する、第１～第４の単一光子検出部と、

第１～第４の受信情報に基づいて、生鍵を生成する生鍵生成回路とを備え、

前記第１～４の単一光子検出部のいずれか１つ又は複数が、請求項１に記載する単一光子検出装置であり、

前記生鍵生成回路は、前記計数処理回路が生成する認証信号が承認を示すときに生鍵を生成する、

量子鍵配送用受信装置。

[請求項7] ｎ（ｎは２以上の整数）値の乱数を発生させ、乱数値ｉ（ｉは０以上ｎ－１以下の整数）と、該乱数値ｉを発生させた時刻を含む乱数ビット値情報を生成する乱数発生器と、

前記乱数値ｉによって定まる透過率T_iで外部からの入力光を強度変調する光強度変調器と、

２値の偏波変調器用乱数を発生させ、乱数値ｋ（ｋは０又は１）と、該乱数値ｋを発生させた時刻を含む基底乱数情報を生成する偏波変調用乱数発生器と、

前記偏波変調用乱数発生器が発生した乱数の偏波乱数値ｋに応じて、前記光強度変調器を経て入力される光の偏波状態を変更する偏波変調器と、

第１及び第２の出力端を有し、前記偏波変調器を通過した光が入力され、該光の偏波状態に応じて、第１及び第２の出力端から出力する偏光ビームスプリッタと、

前記偏光ビームスプリッタの第１の出力端から出力された光が入力

され、単一光子を検出した時刻を第１の受信情報として生成する第１の単一光子検出器と、

前記偏光ビームスプリッタの第２の出力端から出力された光が入力され、単一光子を検出した時刻を第２の受信情報として生成する第２の単一光子検出器と、

前記乱数値ｉにおける、前記単一光子検出器の光子検出率S_i、前記乱数発生器で発生する乱数値のうち前記乱数値ｉが占める割合であるマーク率M_i、及び、前記透過率T_iから判定値S_i／（$T_i M_i$）を算出し、該判定値が予め定めた基準を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路と、

前記第１及び第２の受信情報と、前記基底乱数情報に基づいて、生鍵を生成する生鍵生成回路と

を備え、

前記生鍵生成回路は、前記計数処理回路が生成する認証信号が承認を示すときに生鍵を生成する、

量子鍵配送用受信装置。

[請求項8] ｎ（ｎは２以上の整数）値の乱数を発生させ、乱数値ｉ（ｉは０以上ｎ－１以下の整数）と、該乱数値ｉを発生させた時刻を含む乱数ビット値情報を生成する乱数発生器と、

前記乱数値ｉによって定まる透過率T_iで外部からの入力光を強度変調する光強度変調器と、

前記光強度変調器を通過する入力光が入力されるハーフミラーと、

前記ハーフミラーで２分岐された一方が入力され、第１及び第２の出力端を有し、前記ハーフミラーで２分岐された一方の光が入力され、該光の偏波状態に応じて、第１及び第２の出力端から出力する第１の偏光ビームスプリッタと、

前記ハーフミラーで２分岐された他方が入力される波長板と、

前記波長板を通過した光が入力され、該光の偏波状態に応じて、第３及び第４の出力端から出力する第２の偏光ビームスプリッタと、

それぞれ、前記第ｍ（ｍは１以上４以下の整数）の出力端から出力された光が入力され、単一光子を検出した時刻を第ｍの受信情報として生成する、第１～第４の単一光子検出器と、

前記乱数値ｉにおける、前記単一光子検出器の光子検出率S_i、前記乱数発生器で発生する乱数値のうち前記乱数値ｉが占める割合であるマーク率M_i、及び、前記透過率T_iから判定値$S_i/(T_iM_i)$を算出し、該判定値が予め定めた基準を満たしている場合は承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路と、

第１～第４の受信情報に基づいて、生鍵を生成する生鍵生成回路とを備え、

前記生鍵生成回路は、前記計数処理回路が生成する認証信号が承認を示すときに生鍵を生成する、

量子鍵配送用受信装置。

[請求項9] 外部からの、周期Δｔのパルス光である入力光を２分岐して、第ｊ（ｊは１又は２）の入力光を生成する光回路であって、当該光回路の出力強度の総和に対する第ｊの入力光の強度の割合をT_jとする光分岐部と、

第１の入力光及び第２の入力光を合波して、入力合波光を生成する光合波部と、

前記第２の入力光を遅延させて、前記光合波部で合波される前記第１の入力光及び前記第２の入力光の間にΔｔ／２の時間差を与える光遅延器と、

２値の偏波変調器用乱数を発生させ、乱数値ｋ（ｋは１又は２）と、該乱数値ｋを発生させた時刻を含む基底乱数情報を生成する偏波変調用乱数発生器と、

前記偏波変調用乱数発生器が発生した乱数の偏波乱数値ｋに応じて、前記入力合波光の偏波状態を変更する偏波変調器と、

第１及び第２の出力端を有し、前記偏波変調器を通過した光が入力され、該光の偏波状態に応じて、第１及び第２の出力端から出力する偏光ビームスプリッタと、

前記偏光ビームスプリッタの第１の出力端から出力された光が入力され、単一光子を検出した時刻を第１の受信情報として生成する第１の単一光子検出器と、

前記偏光ビームスプリッタの第２の出力端から出力された光が入力され、単一光子を検出した時刻を第２の受信情報として生成する第２の単一光子検出器と、

幅Δｔ／２の時間スロットに区切ったときの、奇数番目の時間スロットでの前記単一光子検出器における光子検出数をS_1、偶数番目の時間スロットでの前記単一光子検出器における光子検出数をS_2として判定値$S_j／T_j$を算出し、$S_1／S_2＝T_1／T_2$を満たしている場合承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路と、

前記第１及び第２の受信情報と、前記基底乱数情報に基づいて、生鍵を生成する生鍵生成回路と

を備え、

前記生鍵生成回路は、前記計数処理回路が生成する認証信号が承認を示すときに生鍵を生成する、

量子鍵配送用受信装置。

[請求項10] 外部からの、周期Δｔのパルス光である入力光を２分岐して、第ｊ（ｊは１又は２）の入力光を生成する光回路であって、当該光回路の出力強度の総和に対する第ｊの入力光の強度の割合をT_jとする光分岐部と、

第１の入力光及び第２の入力光を合波して、入力合波光を生成する

光合波部と、

前記第２の入力光を遅延させて、前記光合波部で合波される前記第１の入力光及び前記第２の入力光の間にΔｔ／２の時間差を与える光遅延器と、

前記入力合波光が入力されるハーフミラーと、

前記ハーフミラーで２分岐された一方が入力され、第１及び第２の出力端を有し、前記ハーフミラーで２分岐された一方の光が入力され、該光の偏波状態に応じて、第１及び第２の出力端から出力する第１の偏光ビームスプリッタと、

前記ハーフミラーで２分岐された他方が入力される波長板と、

前記波長板を通過した光が入力され、該光の偏波状態に応じて、第３及び第４の出力端から出力する第２の偏光ビームスプリッタと、

それぞれ、前記第ｍ（ｍは１以上４以下の整数）の出力端から出力された光が入力され、単一光子を検出した時刻を第ｍの受信情報として生成する、第１～第４の単一光子検出器と、

幅Δｔ／２の時間スロットに区切ったときの、奇数番目の時間スロットでの前記単一光子検出器における光子検出数をS_1、偶数番目の時間スロットでの前記単一光子検出器における光子検出数をS_2として判定値$S_j／T_j$を算出し、$S_1／S_2＝T_1／T_2$を満たしている場合承認を示す認証信号を出力し、満たしていない場合は否認を示す認証信号を出力する計数処理回路と、

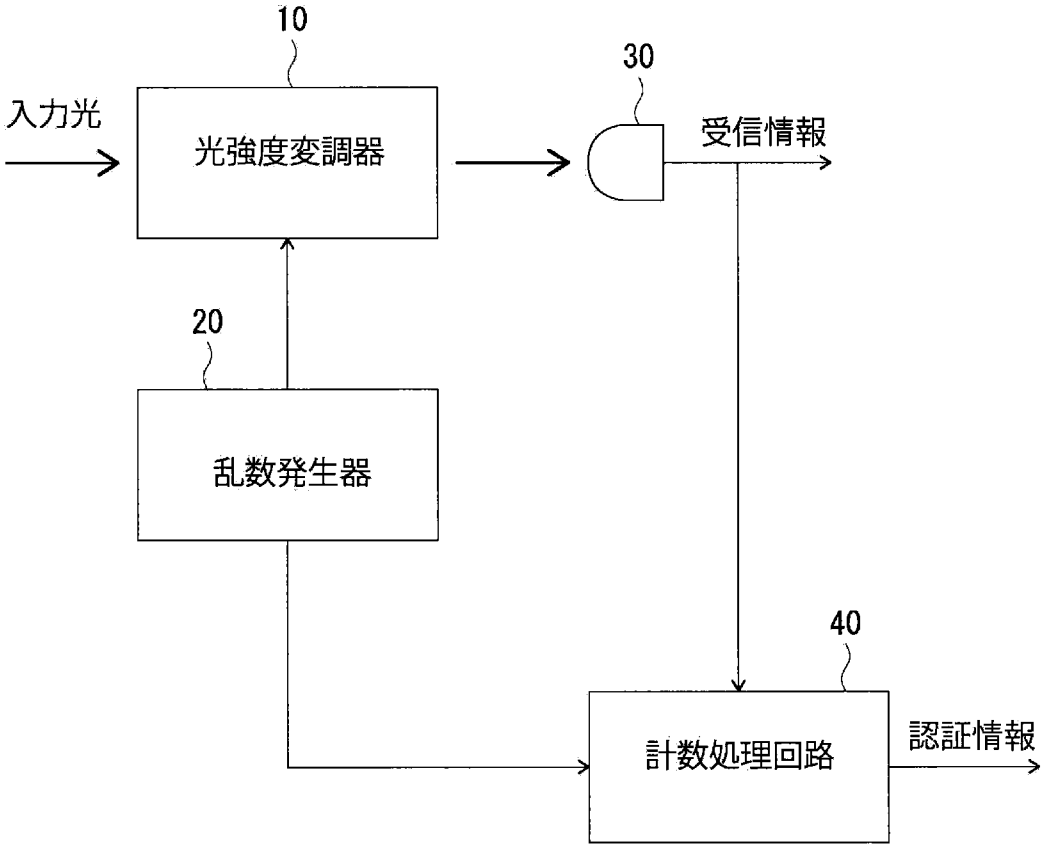
前記第１～第４の受信情報に基づいて、生鍵を生成する生鍵生成回路と

を備え、

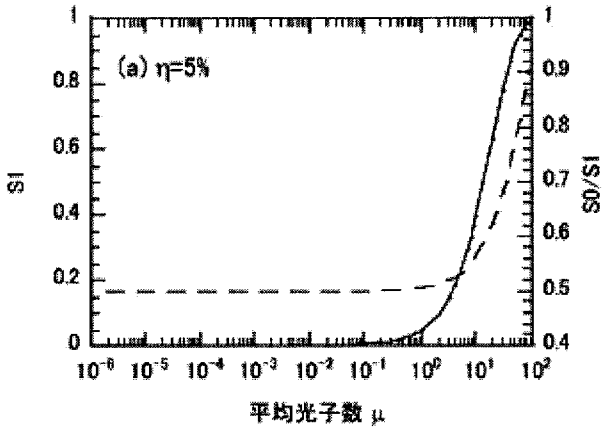
前記生鍵生成回路は、認証信号が承認を示すときに生鍵を生成する、

量子鍵配送用受信装置。

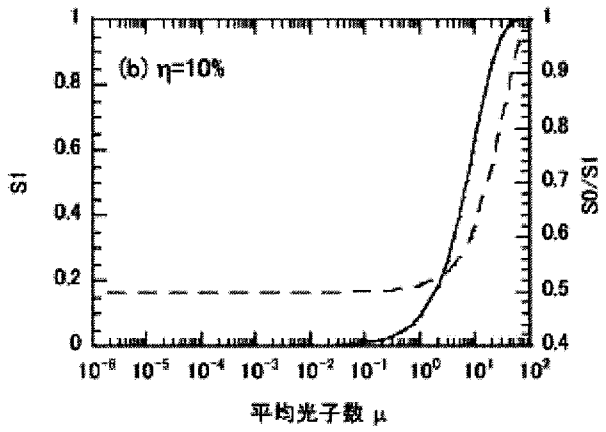
[図1]


10
入力光
光強度変調器
30
受信情報
20
乱数発生器
40
計数処理回路
認証情報

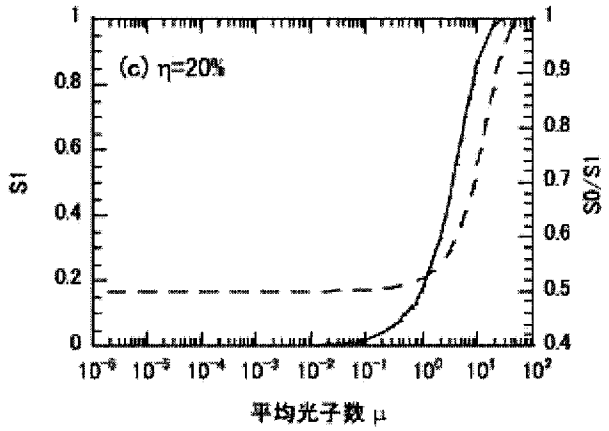
[図2A]


(a) η=5%
SI
S0/SI
平均光子数 μ

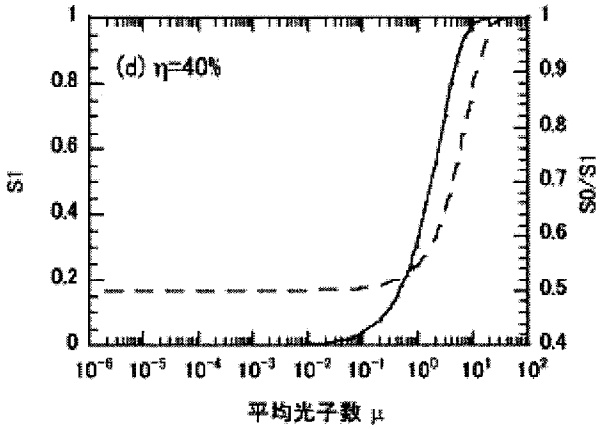
[図2B]


(b) η=10%
SI
S0/SI
平均光子数 μ

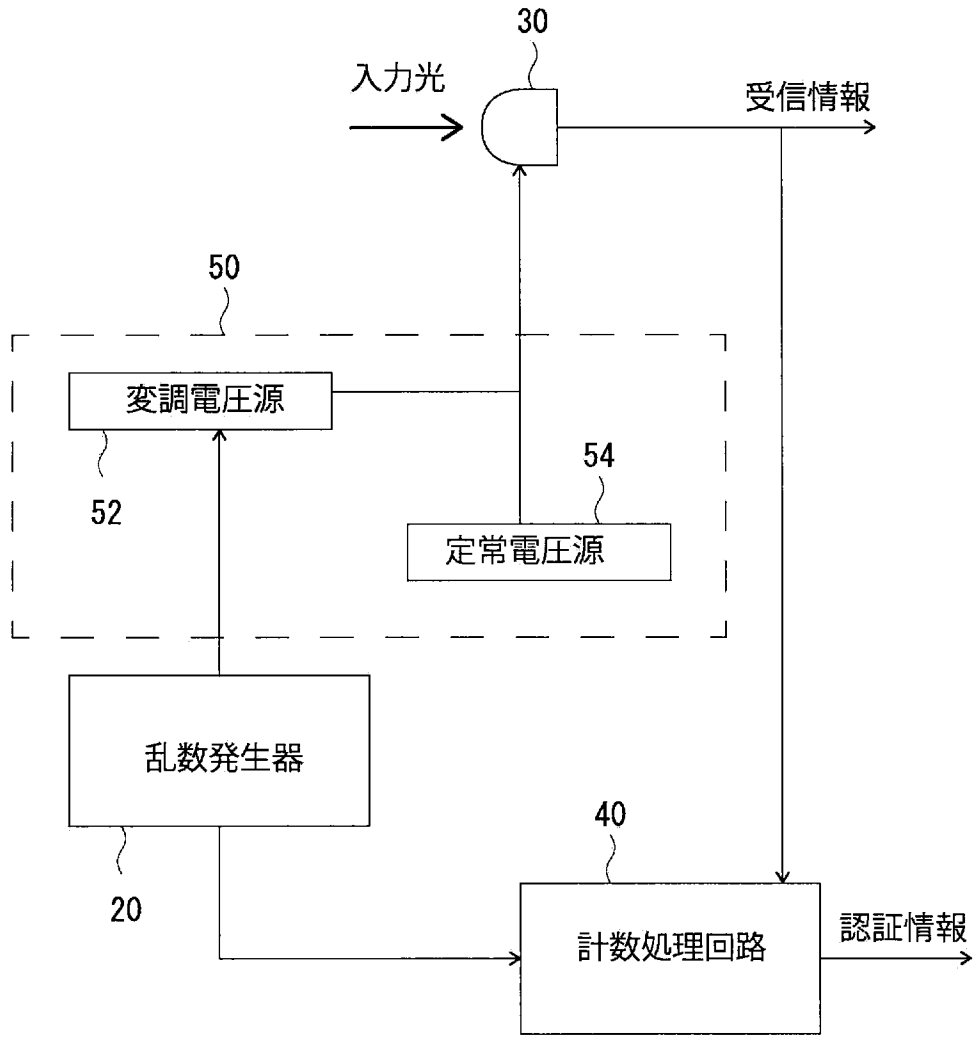
[図2C]



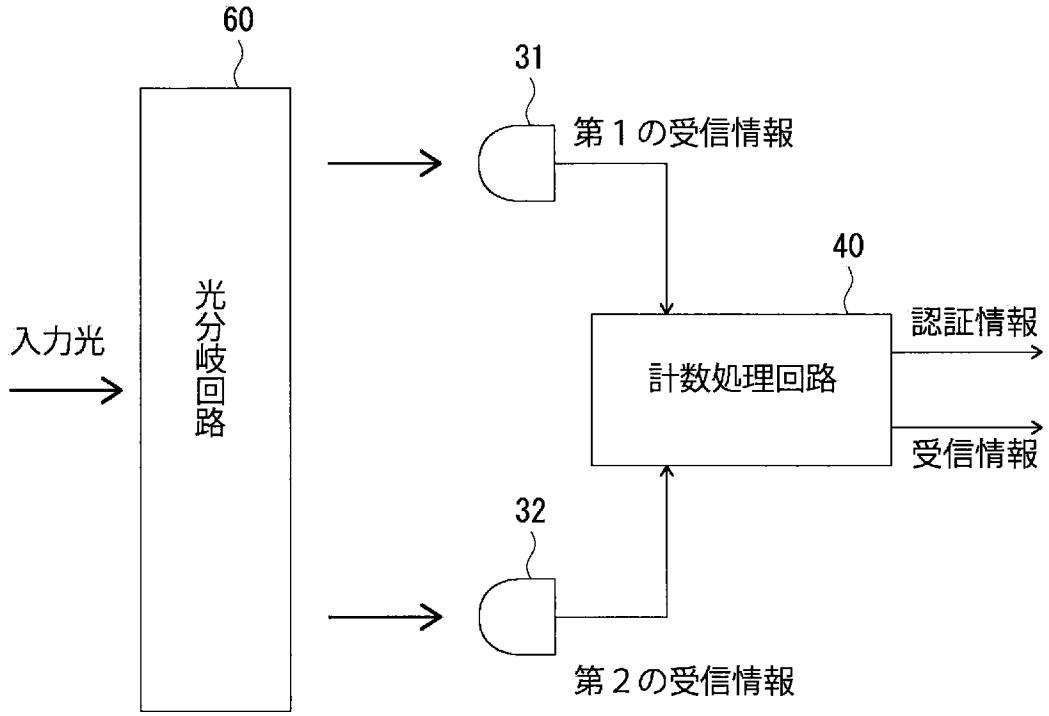
[図2D]



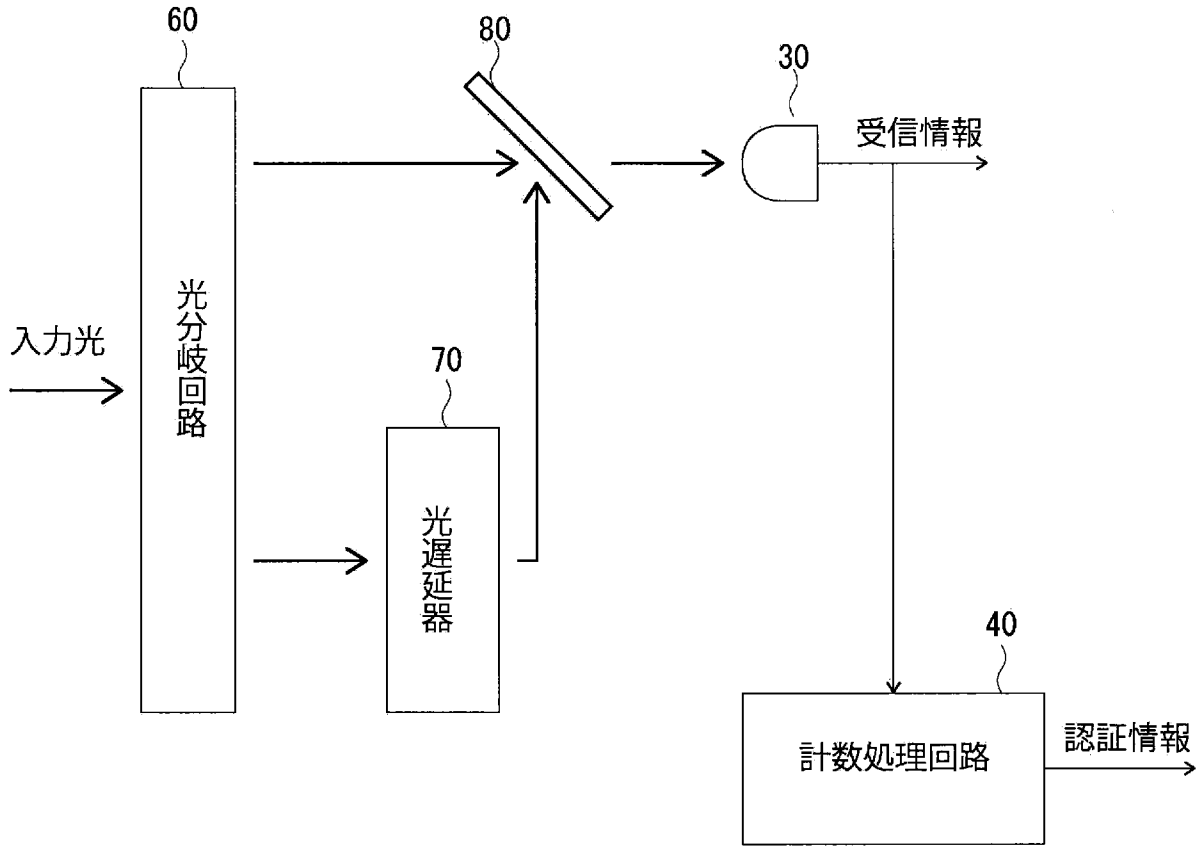
[図3]


30
入力光
受信情報
50
変調電圧源
52
54
定常電圧源
乱数発生器
20
40
計数処理回路
認証情報

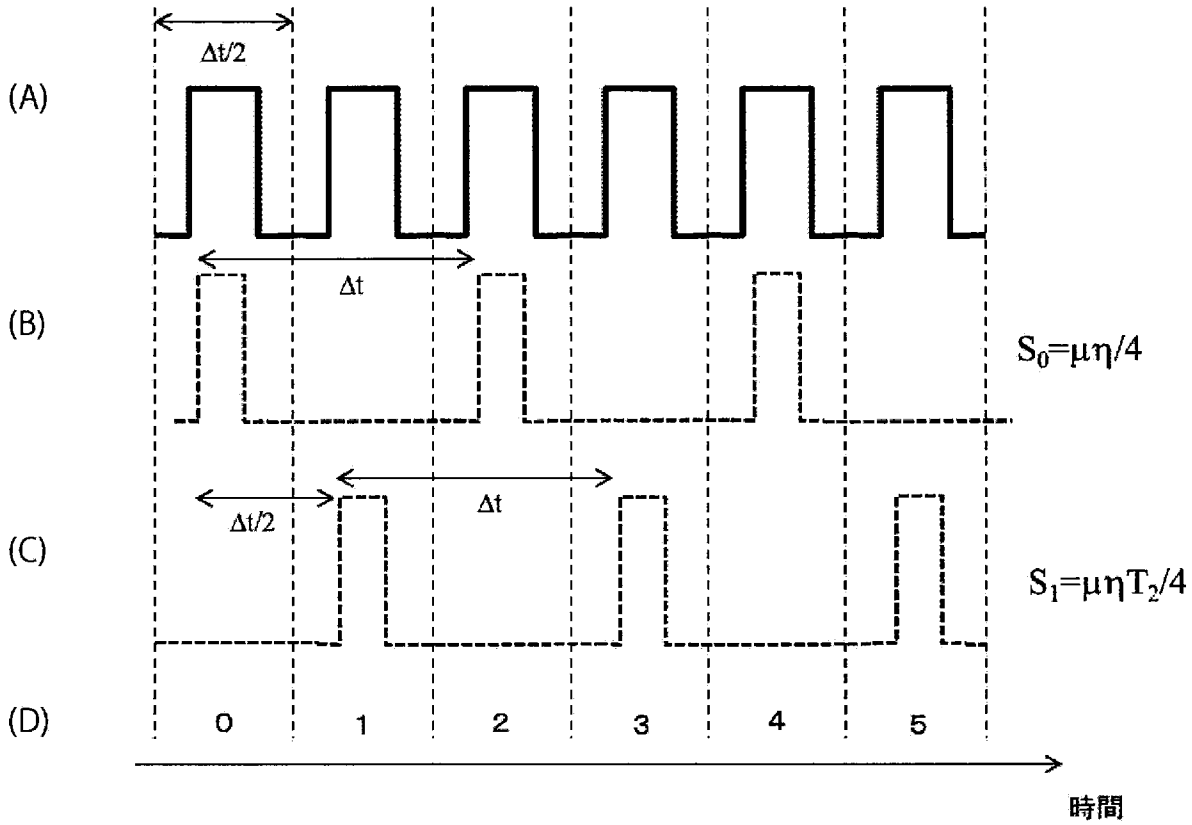
[図4]


60
31
第１の受信情報
40
入力光
光分岐回路
計数処理回路
認証情報
受信情報
32
第２の受信情報

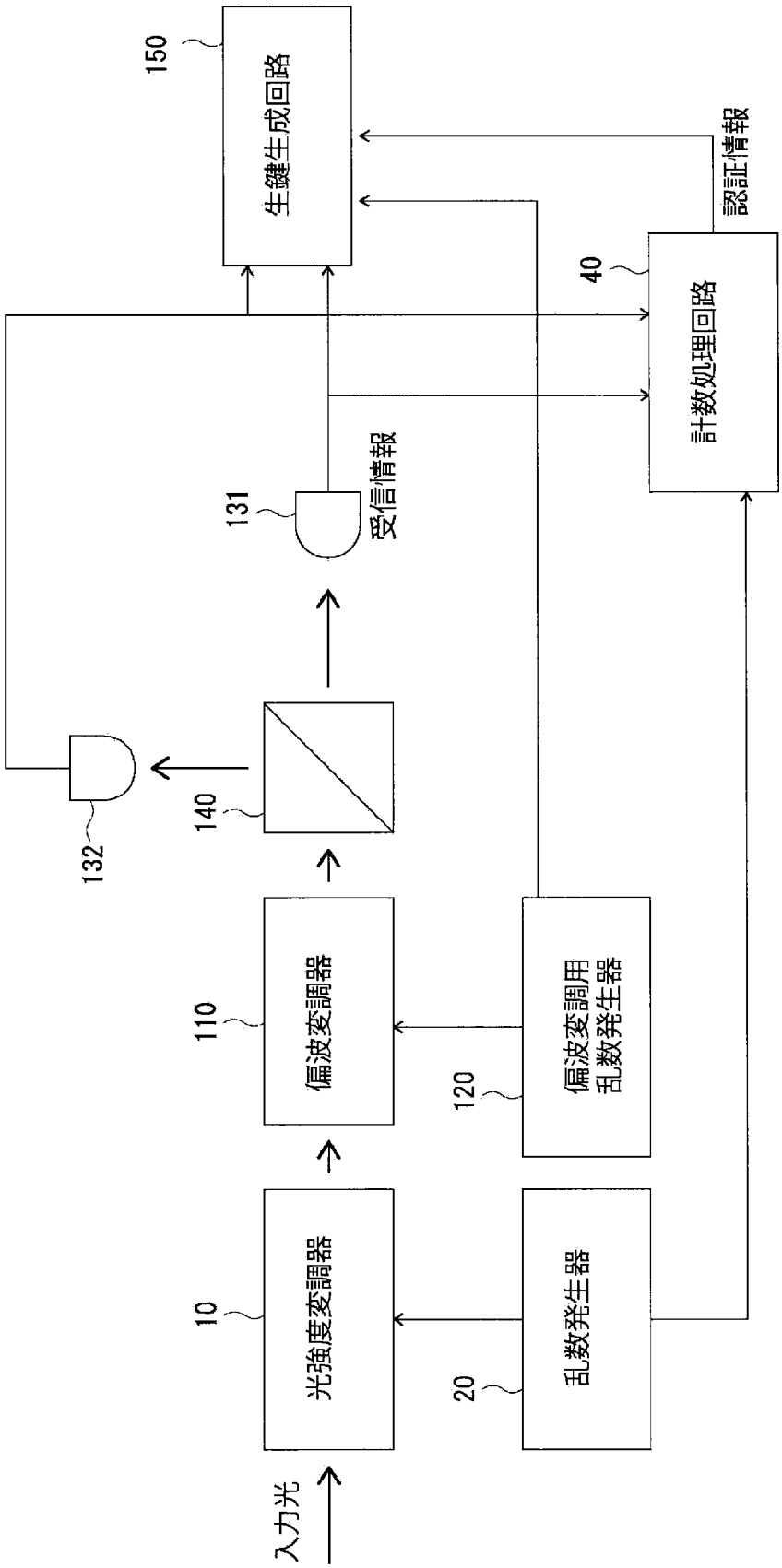
[図5]


60
80
30
受信情報
入力光
光分岐回路
70
光遅延器
40
計数処理回路
認証情報

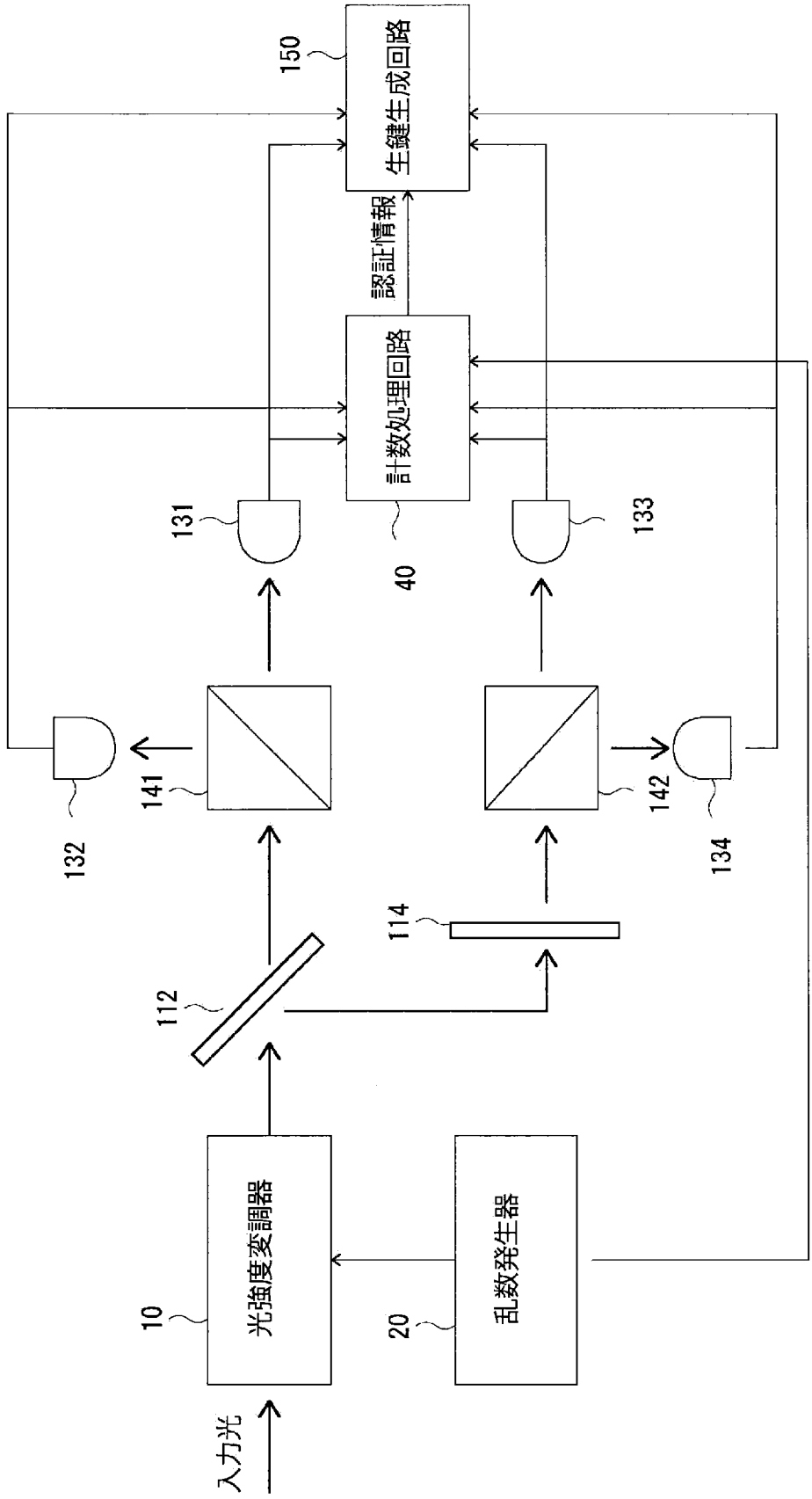
[図6]


(A)
Δt/2
(B)
Δt
$S_0=\mu\eta/4$
(C)
Δt/2
Δt
$S_1=\mu\eta T_2/4$
(D)
0
1
2
3
4
5
時間

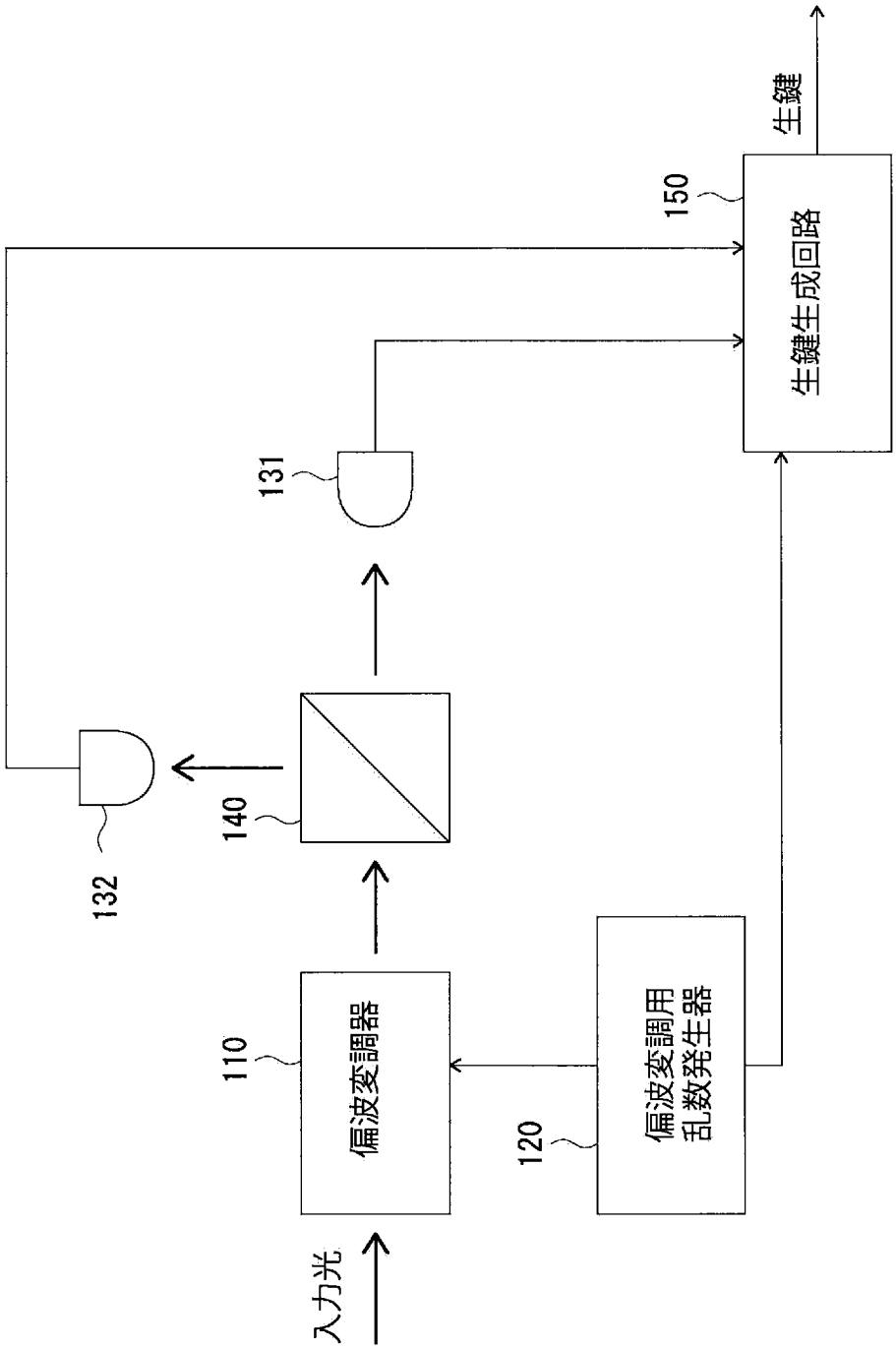
[図7]


150
生鍵生成回路
認証情報
40
計数処理回路
131
受信情報
132
140
110
偏波変調器
120
偏波変調用
乱数発生器
10
光強度変調器
20
乱数発生器
入力光

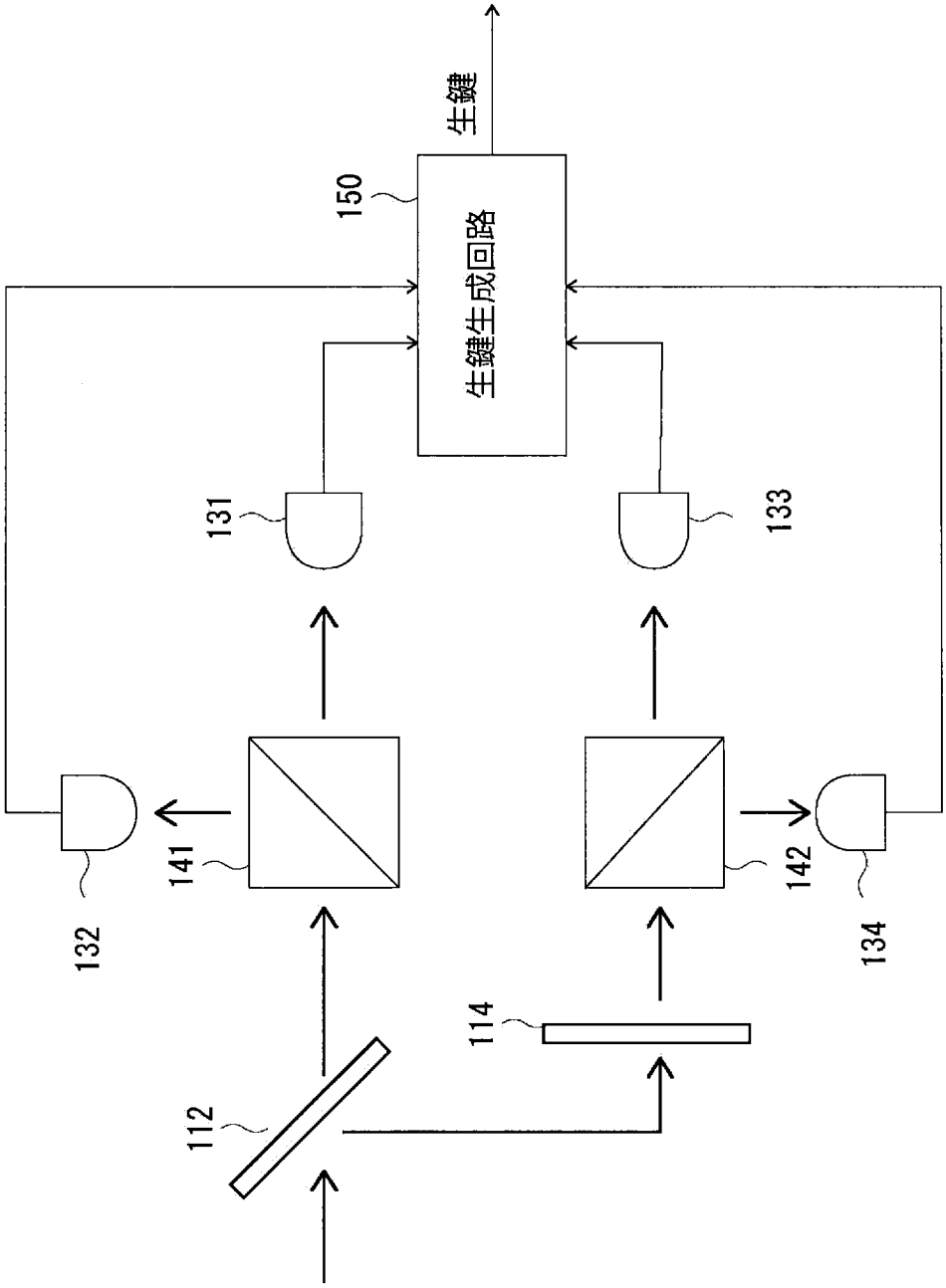
[図8]


150
生鍵生成回路
認証情報
計数処理回路
40
131
133
132
141
142
134
114
112
10
光強度変調器
20
乱数発生器
入力光

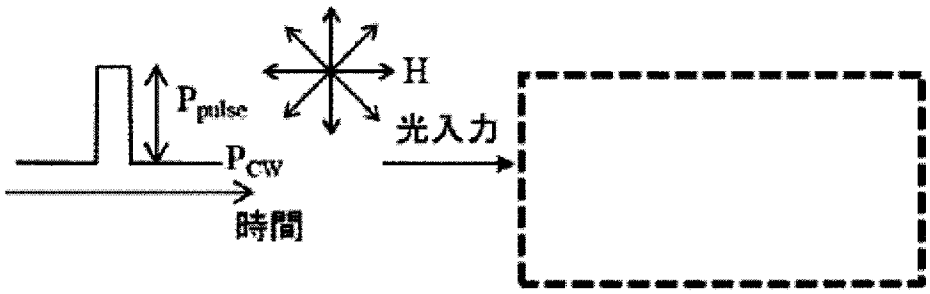
[図9]



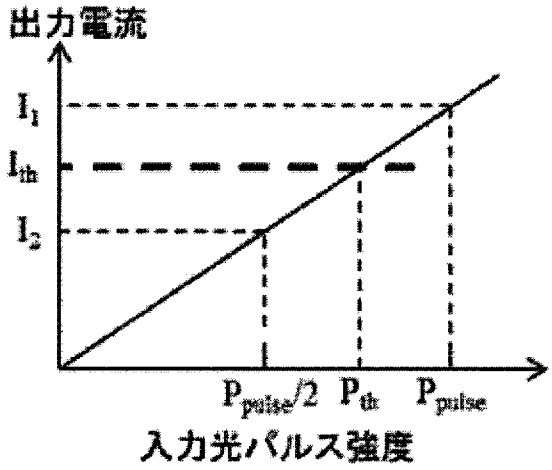
[図10]


生鍵
150
生鍵生成回路
131
133
141
142
132
134
114
112

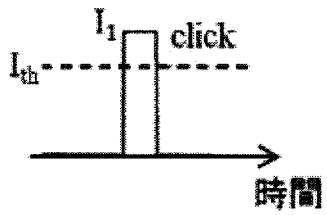
[図11A]


H
P_{pulse}
P_{CW}
光入力
時間

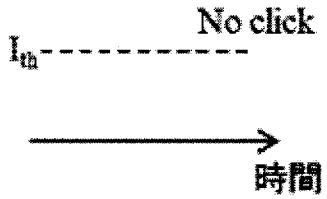
[図11B]



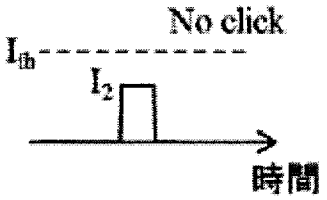
[図11C]



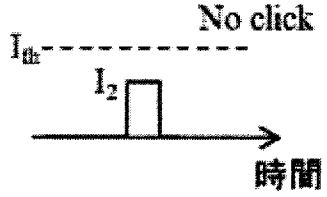
[図11D]



[図11E]



[図11F]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/037959

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. H04L9/12(2006.01)i, G02F1/01(2006.01)i, G02F3/00(2006.01)i, H04B10/70(2013.01)i

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. Cl. H04L9/12, G02F1/01, G02F3/00, H04B10/70

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2018
Registered utility model specifications of Japan 1996-2018
Published registered utility model applications of Japan 1994-2018

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.
A	HONJO, T. et al., Countermeasure against tailored bright illumination attach for DPS-QKD, Optics Express, vol. 21, no. 3, OSA Publishing, 11 February 2013, pp. 2667-2673, [online], [retrieved on 14 December 2018], Internet <URL: http://www.osapublishing.org/oe/abstract.cfm?uri=oe-21-3-2667>, <DOI:10.1364/OE.21.002667>	1-10
A	永田恒一ほか, ハンディ光パワーメータを用いるDPS-QKDブラインド攻撃対策, 2014年第61回応用物理学会春季学術講演会「講演予稿集」, 公益社団法人応用物理学会, 03 March 2014, p. 1 (NAGATA, Koichi, INOUE, Kyo. DPS-QKD with Handy Optical Power Meter against Tailored Bright Illumination Attack. Proceedings of the 61st JSAP Spring Meeting. The Japan Society of Applied Physics.)	1-10

☒ 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	Date of mailing of the international search report
14.12.2018	25.12.2018
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/037959

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2012-69944 A (TOSHIBA CORP.) 05 April 2012, paragraphs [0040]-[0071] & US 2012/0063789 A1, paragraphs [0054]-[0083]	1-10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／０３７９５９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/12(2006.01)i, G02F1/01(2006.01)i, G02F3/00(2006.01)i, H04B10/70(2013.01)i

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.Cl.　H04L9/12, G02F1/01, G02F3/00, H04B10/70

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	１９７１－２０１８年
日本国実用新案登録公報	１９９６－２０１８年
日本国登録実用新案公報	１９９４－２０１８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	関連する請求項の番号
A	HONJO, T. et al., Countermeasure against tailored bright illumination attack for DPS-QKD, Optics Express, vol.21, no.3, OSA Publishing, 2013.02.11, p.2667-2673, [online], [検索日 2018.12.14],インターネット<URL:http://www.osapublishing.org/oe/abstract.cfm?uri=oe-21-3-2667>,<DOI:10.1364/OE.21.002667>	1-10
A	永田恒一ほか，ハンディ光パワーメータを用いるＤＰＳ－ＱＫＤブラインド攻撃対策，２０１４年第６１回応用物理学会春季学術講演会「講演予稿集」，公益社団法人応用物理学会，2014.03.03，p.1	1-10

☑　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	国際調査報告の発送日
１４．１２．２０１８	２５．１２．２０１８

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
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）　５Ｓ　６３０４
行田　悦資
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　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	関連する請求項の番号
A	JP 2012-69944 A (株式会社東芝) 2012.04.05, 段落 0040－0071 & US 2012/0063789 A1, 段落 0054－0083	1-10